Réseaux et transmissions

Protocoles, infrastructures et services

Stéphane Lohier
Maître de conférences en réseaux
à l'université de Marne-la-Vallée

Dominique Présent
Maître de conférences en réseaux
à l'université de Marne-la-Vallée

6e édition

DUNOD

Toutes les marques citées dans cet ouvrage
sont des marques déposées par leurs propriétaires respectifs.

Illustration de couverture :
Communication Cable © alexmat46 - Fotolia.com

5 rue Laromiguière, 75005 Paris
www.dunod.com

ISBN 978-2-10-074475-6

TABLE DES MATIÈRES

AVANT-PROPOS

La guerre des mondes

Hier, deux mondes coexistaient : le monde des télécommunications avec ses services propres et ses infrastructures fermées (« l'oligarchie » des opérateurs, Orange en tête) et le monde des informaticiens de l'Internet avec une organisation décentralisée, plus ouverte mais moins fiable (« l'anarchie » des protocoles).

Même si les informaticiens s'appuyaient parfois sur les infrastructures des « télécoms » pour échanger des données (les prémices d'Internet) chacun s'occupait jalousement de sa partie : le transport, la téléphonie et un peu d'échange de données pour l'un ; le courrier électronique, le transfert de fichiers et d'informations pour l'autre.

Aujourd'hui, devant la multiplication des services (téléphonie mobile, informations en temps réel, offres multimédia…) la tendance est à la convergence. Pour transporter des paquets d'un réseau à l'autre, plus d'alternative : c'est IP, un protocole finalement pas si anarchique, qui a gagné la guerre !

On en arrive même à un paradoxe : pour téléphoner, la voix est numérisée puis transportée dans des paquets IP, eux-mêmes envoyés après modulation sur le RTC (Réseau Téléphonique Commuté), pas du tout prévu au départ pour les paquets IP mais pour… le bon vieux téléphone analogique !

La voix, le son, les vidéos, les informations, tout est donc transporté dans des paquets IP grâce tout de même à des opérateurs de transport et des opérateurs de câblage qui continuent, dans l'ombre, à prendre en charge l'acheminement de ces précieux paquets. Ces opérateurs ne disposent la plupart du temps que de paires torsadées de qualité bien médiocre, celles précisément qui ont été posées il y a bien longtemps pour offrir dans une démarche d'utilité publique le téléphone à tout le monde. Ces fils de cuivre que l'on retrouve à l'extrémité du RTC, vers l'abonné (la fameuse boucle locale) permettent donc aujourd'hui de transporter bien d'autres informations que la voix mais au prix de prouesses techniques comme la modulation sophistiquée présente dans l'ADSL.

Les limites de ces techniques sont sans doute atteintes, les « hauts » débits proposés par l'ADSL2+ sont très rarement obtenus et nécessitent des distances de plus en plus réduites entre l'abonné et son répartiteur. Les hauts débits de demain, qui seront les bas débits d'après-demain, ne pourront être obtenus qu'avec de nouvelles infrastructures qui mélangeront probablement, suivant l'environnement rural ou urbain, des fibres optiques et des transmissions sans fil (avec WiMAX par exemple). Une

nouvelle guerre démarre, à un autre niveau, celle du nouveau câblage de la boucle locale !

Parallèlement, les protocoles développés par les informaticiens de l'Internet ont la vie dure : IP, TCP, et toute la gamme des protocoles applicatifs contrôlant l'échange d'information (HTTP, FTP, SMTP…) ont peu changé. Les évolutions se retrouvent plutôt au niveau des contenus (pages dynamiques, animations, vidéo en ligne…) et de la sécurité (antivirus, antispam, paiement en ligne…).

Enfin du côté des réseaux locaux, d'autres guerres se terminent. Dans le monde filaire, la technologie Ethernet a acquis une situation de quasi-monopole avec des débits sans cesse augmentés (1 Gbit/s aujourd'hui, 100 Gbit/s demain) sur des câblages en paire torsadée peu onéreux. Le sans fil et l'avènement du WiFi avec ses évolutions constantes (802.11n, 802.11ad…) propose aux entreprises et aux particuliers des performances satisfaisantes (jusqu'à 500 Mbit/s) dans les lieux où le câblage est difficile.

Objectifs de ce livre

Ce livre a pour but de vous présenter de manière pédagogique les différents concepts et technologies de ces différents mondes en perpétuelle évolution. Il s'adresse à des étudiants de niveau baccalauréat et ne nécessite aucune connaissance préalable dans le domaine.

Pour comprendre le rôle et le fonctionnement des protocoles en cours et de ceux à venir, il est en effet nécessaire de s'attacher avant tout aux principes de base plutôt qu'à la description détaillée de ces protocoles évolutifs : il est plus important de comprendre comment les informations circulent sur un câble entre deux ordinateurs que de connaître les spécifications du dernier commutateur Ethernet.

C'est pourquoi tout au long des chapitres, les concepts et les protocoles sont présentés très progressivement, comme des briques assemblées au fur et à mesure : comment comprendre le fonctionnement d'ADSL sans savoir ce qu'est une transmission série ?

Cette présentation se démarque de celle rencontrée dans la plupart des ouvrages sur les réseaux dans lesquels les notions sont abordées suivant leur appartenance à telle ou telle couche du modèle de référence OSI plutôt que suivant une démarche linéaire.

Contenu des chapitres

Les deux premiers chapitres présentent les concepts de base des transmissions entre deux ordinateurs. Pour chacun de ces concepts, des exemples concrets sont développés : le bus USB, le bus I2C…

Le chapitre 3 étend la description à des réseaux distants. Les transmissions ADSL et WiMAX sont développées L'explication de leur fonctionnement s'appuie sur celui de la transmission du signal numérique grâce aux modems, nécessaires sur les longues distances.

Les briques de base de la transmission entre ordinateurs proches ou distants étant posées, le chapitre 4 aborde la normalisation des réseaux avec le fameux modèle de référence en couches, mais toujours en présentant les concepts, parfois abstraits, à partir d'exemples concrets.

À partir de la connaissance de cette normalisation, le chapitre 5 décrit les réseaux locaux, filaires ou sans fil, avec leurs normes (Ethernet, WiFi…) et leurs caractéristiques (topologies, accès au support, débit…).

Toujours dans l'idée d'étendre au fur et à mesure la présentation des concepts, le chapitre 6 traite de l'interconnexion des réseaux avec les différents dispositifs (commutateurs, routeurs…), les différents protocoles (TCP/IP, ICMP) et les différentes techniques de routage entre machines.

Le chapitre 7 décrit davantage les infrastructures qui permettent d'étendre le réseau en présentant les réseaux d'opérateurs tels le RTC ou le réseau ATM.

Enfin le réseau Internet avec ses prestataires, ses services et ses protocoles (POP3, HTTP…) est décrit dans le chapitre 8.

Enfin, le chapitre 9 est dédié à la sécurité dans les réseaux avec une présentation des solutions matérielles (firewall, VPN…) et logicielles (chiffrement, hash…) de sécurisation et les protocoles associés.

Comment lire ce livre

Pour le lecteur novice dans le domaine, il est recommandé de respecter le caractère volontairement progressif des chapitres. Un lecteur familiarisé avec certains principes de base pourra aborder les chapitres dans un ordre différent, les concepts, protocoles et exemples étant bien séparés au sein de chaque chapitre. Par exemple un lecteur connaissant la modélisation des réseaux et les principes d'encapsulation pourra étudier directement le fonctionnement de TCP/IP au chapitre 6.

Pour valider les différentes étapes d'apprentissage, un résumé avec des mots-clés est proposé pour chacun des chapitres. Un QCM corrigé permet de vérifier rapidement la compréhension des concepts abordés. Des exercices corrigés de niveaux différents permettent au lecteur de vérifier ses connaissances et de les approfondir.

CONCEPTS DE BASE 1

PLAN

OBJECTIFS

- ➤ Connaître l'architecture générale des systèmes de télécommunication et des réseaux informatiques.
- ➤ Connaître les éléments de base d'une liaison série et comprendre comment les données sont codées et transmises.
- ➤ Comprendre la différence entre transmission asynchrone et synchrone.

1.1 SYSTÈMES DE COMMUNICATION

Les besoins de communication de données informatiques entre systèmes plus ou moins éloignés sont multiples : transmission de messages, partage de ressources, transfert de fichiers, consultation de bases de données, gestion de transactions, lecture de vidéos ou de musiques, réseaux sociaux, réservations en ligne…

Pour communiquer, ces systèmes disposent de trois blocs fonctionnels (figure 1.1) :

- les applications qui veulent échanger des données ;
- les fonctions destinées à établir et à gérer la communication ;
- les fonctions assurant la transmission des données.

Il est important de noter que ce sont les applications qui sont à l'origine de la demande et de la procédure de communication. En revanche, l'établissement de la connexion entre les systèmes informatiques s'effectue à partir du réseau.

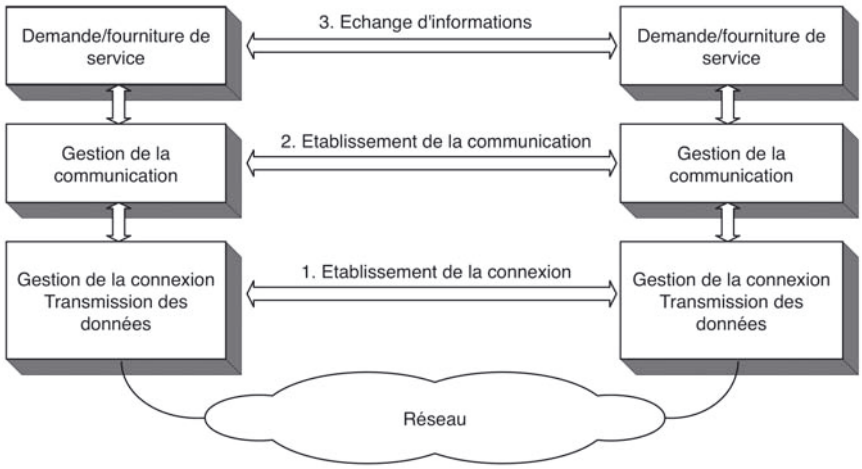


Figure 1.1 – Architecture des systèmes de communication.

C'est tout d'abord la connexion entre les deux systèmes qui est établie à travers le réseau (phase 1). Puis la communication est établie, vérifiant que les systèmes peuvent dialoguer : même « langage », mémoire disponible, services applicatifs présents (phase 2). Les applications peuvent alors échanger leurs informations (phase 3). Pour comprendre le rôle de chacun de ces blocs, une analogie simple avec le réseau téléphonique peut être faite :

- **phase 1 :**
  - ◇ à l'initiative de l'appelant, la demande de connexion est initiée par la prise du combiné (la tonalité confirme que le réseau est disponible) et la numérotation,
  - ◇ l'opérateur est chargé d'établir la connexion entre les deux postes téléphoniques,
  - ◇ le combiné distant sonne, informant le destinataire de la demande de connexion. Celui-ci répond en décrochant son combiné, **la connexion est établie** ;
- **phase 2 :** s'ils sont disponibles et s'ils parlent la même langue, les deux interlocuteurs peuvent être mis en relation par l'intermédiaire d'un secrétariat ou d'un standard par exemple, **la communication est établie** ;
- **phase 3 :** les deux interlocuteurs dialoguent.

On retrouve ces différents blocs fonctionnels, décomposés en couches, dans les modèles OSI et TCP-IP décrits dans le chapitre 4.

Matériellement, un réseau de transmission comprend des **équipements de raccordement** pouvant être externes (comme un modem, un routeur ou un point d'accès sans fil) ou internes (carte réseau Ethernet ou WiFi par exemple). Ces équipements sont connectés entre eux par des lignes ou **supports physiques** de transmission (figure 1.2).

Un **réseau** de transmission de données peut donc être défini comme l'ensemble des ressources liées à la transmission et permettant l'échange des données entre les différents systèmes éloignés.

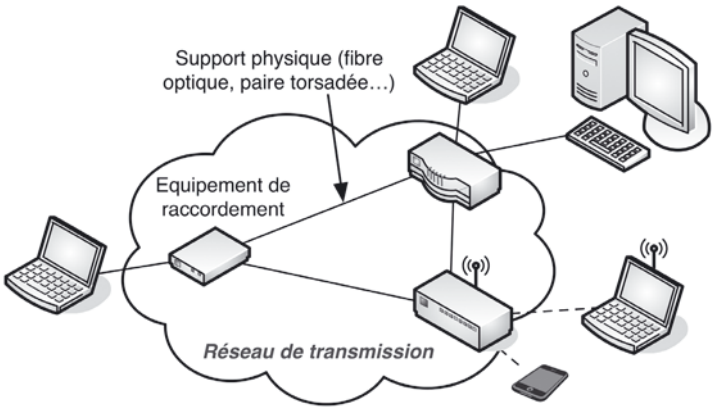


Figure 1.2 – **Architecture d'un réseau de transmission.**

Suivant leur organisation, ou architecture, les distances, les vitesses de transmission et la nature des informations transmises, les spécifications et les normes utilisées sont différentes. Les chapitres suivants analysent les principales normes utilisées dans les réseaux d'ordinateurs.

Les équipements de raccordement vont devoir mémoriser les informations, les coder et les transmettre en fonction des supports physiques et du réseau de transmission utilisés. Les paragraphes suivants ainsi que les chapitres 2 et 3 décrivent les modes de codage et de transmission.

La classification des réseaux de transmission est de plus en plus complexe. Mais deux familles de réseaux sont à distinguer. D'une part, les **réseaux informatiques** dont font partie les réseaux locaux étudiés aux chapitres 5 et 6 et qui sont à la **périphérie d'Internet**. Dans cette catégorie, les lignes de transmission et les équipements de raccordement sont le plus souvent la propriété de l'utilisateur.

D'autre part, les réseaux de télécommunication pour les liaisons longues distances présentés aux chapitres 7 et 8. Ces réseaux sont le plus souvent la propriété d'opérateurs de télécommunication (Orange, British Telecom, AT&T…) qui louent leur utilisation et des services aux clients. Les équipements de raccordement marquent alors la limite de propriété entre les équipements du client et ceux de l'opérateur. Ce sont ces réseaux qui permettent de relier entre eux les réseaux locaux informatiques et qui composent le **réseau cœur d'Internet**.

1.2 Éléments d'une liaison

La communication entre systèmes informatiques s'effectue *via* des liaisons dont les principaux éléments sont définis par les recommandations de l'**UIT-T** (Union Internationale des Télécommunications – secteur des Télécommunications). La figure 1.3 met en évidence ces différents éléments.

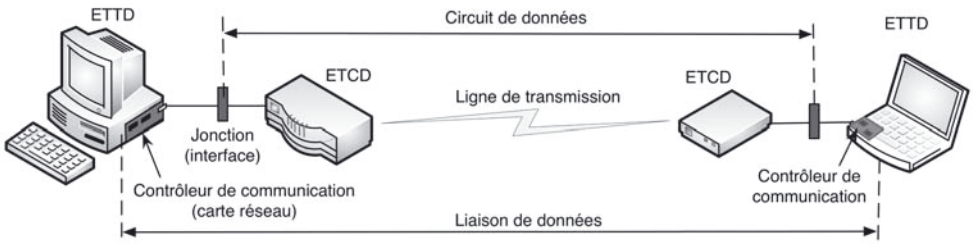


Figure 1.3 – Éléments d'une liaison.

Situé à l'extrémité de la liaison, l'**ETTD** (Équipement Terminal de Traitement de Données ou DTE : *Data Terminal Equipment*) qui intègre un contrôleur de communication peut être un ordinateur, un terminal, une imprimante ou plus généralement tout équipement qui ne se connecte pas directement à la ligne de transmission.

La transmission des données sur la ligne est assurée par l'**ETCD** (Équipement de Terminaison de Circuit de Données ou DCE : *Data Communication Equipment*) qui peut être un modem, un multiplexeur, un concentrateur ou simplement un adaptateur (pseudo-modem).

L'ETCD, la plupart du temps un modem, a deux fonctions essentielles :

- l'adaptation du signal binaire entre l'ETTD et la ligne de transmission, ce qui correspond généralement à un codage et à une modulation (ou une démodulation et un décodage suivant qu'il émet ou reçoit) ;
- la gestion de la liaison comprenant l'établissement, le maintien et la libération de la ligne à chaque extrémité.

La **jonction** constitue l'interface entre ETCD et ETTD et permet à ce dernier de contrôler le circuit de données (établissement et libération, initialisation de la transmission…).

1.3 Modes d'exploitation

Le transfert d'informations entre deux systèmes informatiques peut s'effectuer, en fonction des besoins et des caractéristiques des éléments, suivant trois modes d'exploitation de la liaison.

1.3.1 Liaison simplex

L'un des systèmes est un émetteur, l'autre est un récepteur, les données sont transmises dans un seul sens (figure 1.4). L'exploitation en mode unidirectionnel est justifiée pour les systèmes dont le récepteur n'a jamais besoin d'émettre (liaisons radio ou télévision).

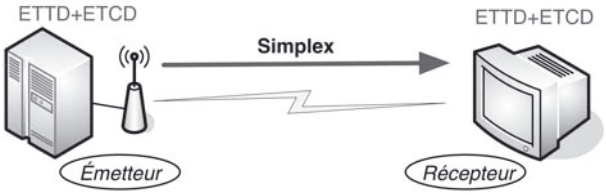


Figure 1.4 – **Liaison simplex.**

1.3.2 Liaison semi-duplex (*half duplex*)

La transmission est possible dans les deux sens mais non simultanément, l'exploitation est en mode bidirectionnel à l'alternat (figure 1.5). Ce type de liaison est utilisé lorsque le support physique est commun aux deux sens de transmission (cas des lignes téléphoniques) et ne possède pas une largeur de bande suffisante pour permettre des liaisons bidirectionnelles simultanées par modulation de deux fréquences porteuses différentes ; des procédures particulières permettent alors d'inverser le sens de transmission (talkies-walkies, liaison WiFi).

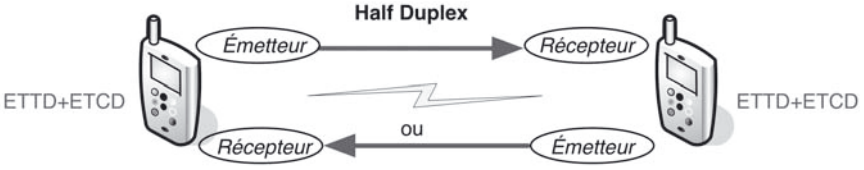


Figure 1.5 – **Liaison *half duplex*.**

1.3.3 Liaison duplex intégral (*full duplex*)

Les données peuvent être émises ou reçues simultanément dans les deux sens, l'exploitation est en mode bidirectionnel simultané (figure 1.6). À chaque sens de transmission correspond un canal de communication propre ; lorsque le support physique est commun aux deux sens de transmission, chaque canal est défini dans une bande de fréquence spécifique. Ainsi, une transmission sur Internet entre deux PC par l'intermédiaire de modems ADSL est de type *full duplex* asymétrique : la communication est possible dans les deux sens simultanément, mais pas avec les mêmes débits.

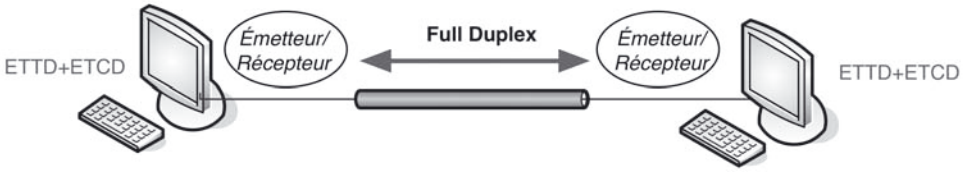


Figure 1.6 – **Liaison *full duplex*.**

1.4 Codage et transmission série

Dans la plupart des réseaux d'ordinateurs, les informations sont de nature numérique mais leur transmission sur le support physique d'interconnexion (« la ligne ») peut être réalisée, suivant les besoins et les caractéristiques du support, sous forme analogique (RTC, Réseau Téléphonique Commuté) ou numérique (réseaux locaux Ethernet).

Dans les deux cas, une adaptation à la ligne est nécessaire. Pour une transmission analogique, cette adaptation consiste en une conversion numérique-analogique par modulation. Pour une transmission numérique, un simple codage est suffisant. Ces notions sont développées dans le chapitre 3.

Les informations numériques traitées et transmises dans les réseaux d'ordinateurs correspondent à une association d'éléments binaires ou bits (bit est la contraction de *binary digit*). Suivant le type de traitement réalisé et la nature des informations (texte, fichier vidéo, programme…), les éléments binaires sont regroupés pour former un ensemble significatif (octet, caractère sur 7 ou 8 bits…).

Le codage est l'opération qui fait correspondre à chaque caractère ou groupe de bits une valeur numérique déterminée exprimée le plus souvent en décimal ou en hexadécimal (code ASCII, ISO 8859…). Les éléments binaires composant un caractère codé sont généralement transmis les uns à la suite des autres, « sur un fil », ce qui correspond à une transmission série (figure 1.7).

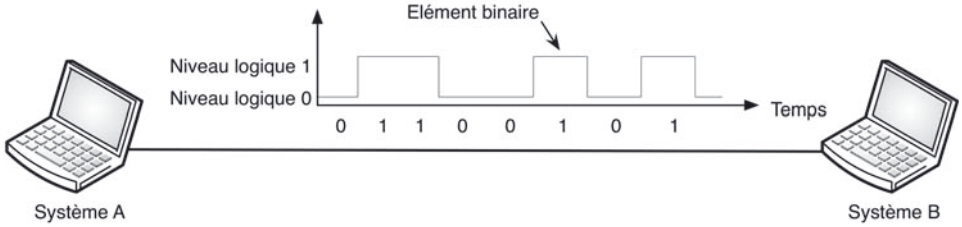


Figure 1.7 – Transmission série numérique entre deux systèmes.

Les *n* bits d'un message sont ainsi transmis séquentiellement au rythme d'une horloge de période *T*, la durée de transmission des bits étant alors égale à *nT*. La vitesse de transmission, ou débit, correspond au nombre de bits transmis par unité de temps. Les débits sont exprimés en bit/s ou bps (*bit per second*).

1.5 Transmissions asynchrones et synchrones

Les informations traitées sous forme parallèle dans les systèmes informatiques sont transmises sous forme série sur le réseau. Cela suppose une conversion parallèle/série (ou série/parallèle) cadencée par un signal d'horloge de référence dont la fréquence correspond à la vitesse de transmission.

En émission, les données et l'horloge sont générées par l'émetteur. En réception, l'horloge de synchronisation peut provenir de l'émetteur si celui-ci la transmet sur la ligne ou être interne au récepteur.

Dans le premier cas, on parle de transmission synchrone car l'émetteur et le récepteur sont synchronisés sur la même horloge de référence. Ce mode est beaucoup plus fréquent dans les réseaux courte ou longue distance car il permet des débits beaucoup plus importants.

Dans le deuxième cas, la transmission est dite asynchrone ou arythmique, le récepteur doit synchroniser sa propre horloge sur la séquence des bits successifs émis (figure 1.8). Le mode asynchrone est orienté pour une transmission par caractères, ceux-ci peuvent être émis à tout moment, la synchronisation à la réception se faisant pour chacun d'eux.

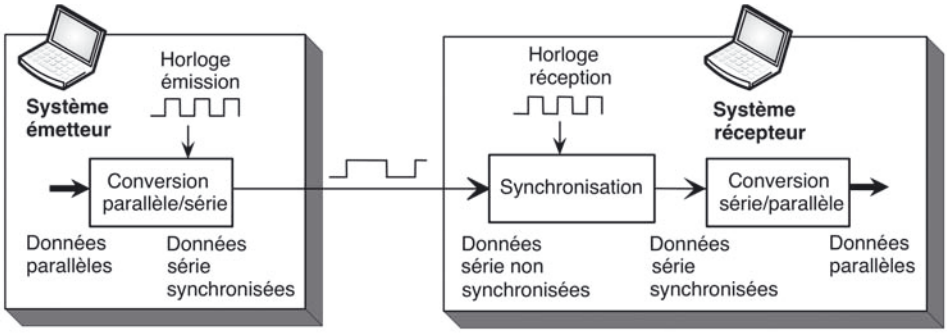


Figure 1.8 – Synchronisation en réception.

1.5.1 Transmission asynchrone

La trame asynchrone (figure 1.9) correspond à la transmission d'un octet ou d'un caractère ; dans ce dernier cas, la longueur dépend du codage utilisé (généralement ASCII pour les caractères alphanumériques) et est limitée à 7 ou 8 bits. Un certain nombre de bits sont associés à chaque caractère pour former la trame. Entre l'émission de deux trames, la ligne est au repos pour une durée quelconque.

L'état de « repos » correspond au niveau logique haut. Un caractère émis sur la ligne est précédé d'un bit de départ (*start bit*) correspondant à l'état actif et à un niveau logique bas ; cette transition haut-bas va indiquer au récepteur qu'un caractère est émis et va permettre sa synchronisation. La fin de l'émission d'un caractère est indiquée par un ou plusieurs bits d'arrêt (*stop bits*) correspondant au niveau logique haut soit à l'état « repos », ce qui permet la distinction avec les bits de départ du caractère suivant. Cette structure est parfois nommée « start-stop ».

Le bit de parité, facultatif, est généré à l'émission et testé à la réception. Deux types de parité existent :

- parité paire (*even*) : la parité est dite paire si le nombre de bits (bits de donnée et bit de parité compris) au niveau logique 1 est pair, le bit de parité est donc positionné dans l'émetteur en conséquence (cas de la figure 1.9) ;
- parité impaire (*odd*) : la parité est dite impaire pour un nombre impair de bits à 1.

Le contrôle à la réception consiste à calculer la parité sur le caractère reçu et à la comparer à la valeur du bit transmis par l'émetteur. Il faut donc que le choix de la parité soit le même à l'émission et à la réception.

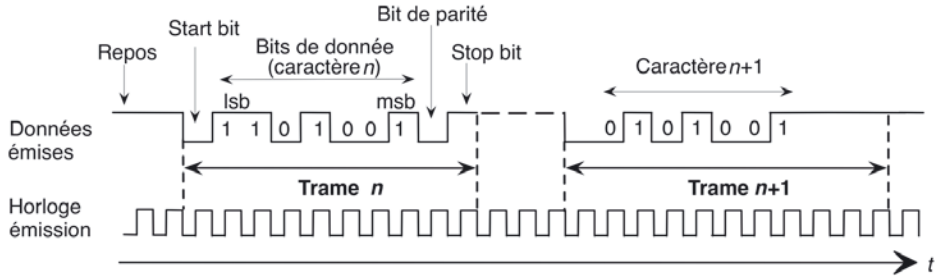


Figure 1.9 – **Trame asynchrone.**

La durée entre chaque bit étant constante et la synchronisation se faisant sur le bit de départ, le déphasage entre l'horloge de réception et les instants correspondant aux changements de bits est d'autant plus grand que ces derniers sont éloignés du bit de départ et que la fréquence de l'horloge de réception est éloignée de celle de l'horloge d'émission. Ceci limite, d'une part, le nombre de bits par trame et, d'autre part, les vitesses de transmission (débit maximum de l'ordre de 56 kbit/s sur une transmission asynchrone).

Il est à remarquer que les débits asynchrones ne correspondent pas aux vitesses effectives de transmission des informations dans la mesure où chaque caractère est encadré par plusieurs bits de contrôle (dans un codage ASCII sur 7 bits avec 1 bit de départ, 1 bit de parité et 1 bit de stop, 10 bits sont transmis pour 7 utiles).

Par ailleurs, le récepteur dispose d'une mémoire tampon permettant le stockage au rythme de l'émission avant traitement. Lorsque cette mémoire est saturée ou sur le point de l'être, le récepteur doit demander à l'émetteur de suspendre son émission pour éviter de perdre des caractères. Il devra également demander la reprise d'émission lorsque la mémoire tampon sera libérée, après traitement des données mémorisées. Cette procédure de **contrôle de flux** peut être réalisée en utilisant des signaux spécifiques (par exemple, le récepteur fait passer le signal RTS/CTS au niveau haut en cas de saturation) ou des caractères spécifiques (par exemple, le caractère Xoff demande l'arrêt de l'émission, le caractère Xon demande la reprise).

1.5.2 Transmission synchrone

Lors d'une transmission synchrone, le signal d'horloge de l'émetteur est transmis sur la ligne au récepteur ou reconstitué par ce dernier, ce qui évite une nouvelle synchronisation en réception et garantit des instants d'échantillonnage en phase quelle que soit la position relative du bit dans la séquence (figure 1.10).

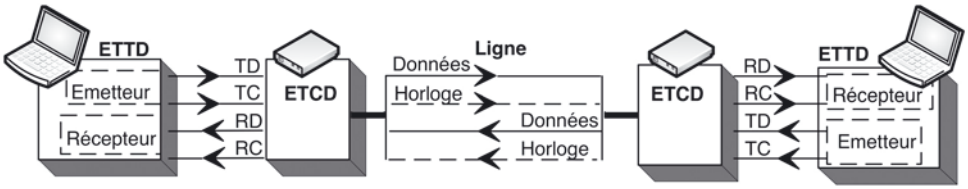


Figure 1.10 – Liaison synchrone *full duplex*.

En pratique, l'horloge de synchronisation en réception peut être élaborée de plusieurs façons :

- directement à partir de l'horloge d'émission si celle-ci est transmise sur une ligne séparée, cas des transmissions synchrones en bande de base ou par modem sur quatre fils ;
- par reconstitution dans le modem de l'horloge d'émission à partir des instants de transition du signal de données et suivant le type de modulation ;
- en utilisant des caractères de synchronisation situés au début des trames transmises et présentant des successions de 0 et de 1, cas des transmissions synchrones en bande de base sur réseaux locaux avec une ligne de données.

Dans la mesure où la fréquence de l'horloge d'émission est rigoureusement égale à celle de l'horloge de réception, les débits peuvent être plus importants. De même, la longueur des trames n'est plus limitée à un caractère comme pour la transmission asynchrone mais est quelconque, ce qui réduit l'importance relative des bits servant au contrôle par rapport aux bits utiles.

En transmission synchrone, une trame est donc composée d'un ensemble de bits pouvant être regroupés par caractères ou octets.

Le début d'une trame est annoncé par un ou plusieurs caractères de synchronisation codés suivant le protocole utilisé. Suivent ensuite un champ de service pouvant contenir l'adresse de l'émetteur et du récepteur ou d'autres informations sur le type de trame ou la structure du message (début de fichier, début ou longueur de bloc…), un champ de données correspondant au message, un champ de contrôle permettant la détection des erreurs de transmission suivi éventuellement d'un ou plusieurs caractères de fin de trame (figure 1.11).

Figure 1.11 – Structure générale d'une trame synchrone.

Contrairement à la transmission asynchrone, la synchronisation au niveau bit et la synchronisation au niveau trame sont indépendantes et correspondent à deux niveaux distincts du modèle OSI (voir chapitre 4) : respectivement le niveau physique et le niveau liaison de données.

1.6 Réseaux informatiques

Suivant la localisation, les distances entre systèmes informatiques et les débits maximums, on peut distinguer trois types de réseaux (figure 1.12) :

- les réseaux locaux ou **LAN** (*Local Area Network*) qui correspondent par leur taille aux réseaux intra-entreprise ou domestiques et qui permettent l'échange de données informatiques ou le partage de ressources ;
- les réseaux métropolitains ou **MAN** (*Metropolitan Area Network*) qui permettent l'interconnexion de plusieurs sites à l'échelle d'une ville ou d'un campus, chacun des sites pouvant être équipé d'un réseau local ;
- les réseaux longues distances ou **WAN** (*Wide Area Network*), généralement réseaux d'opérateurs, et qui assurent la transmission des données numériques sur des distances à l'échelle d'un pays. Le support utilisé peut être terrestre (réseau maillé du type réseau téléphonique ou ligne spécialisée en fibre optique) ou hertzien (transmission par satellite).

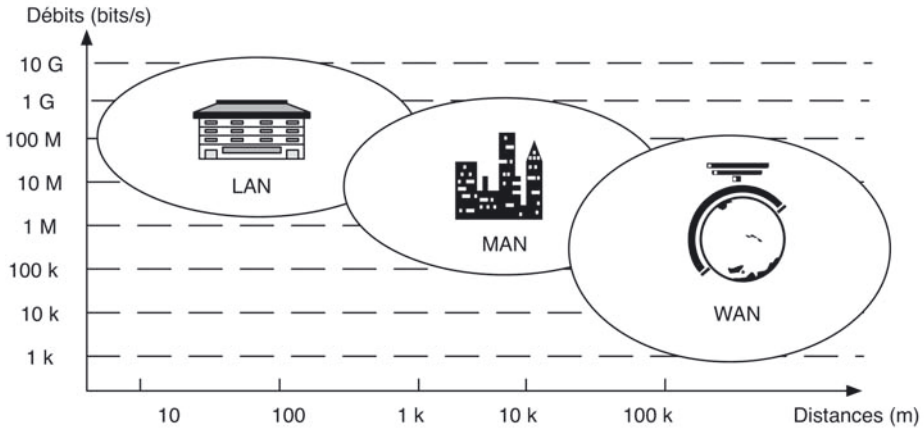


Figure 1.12 – **Types de réseaux.**

Ces réseaux sont généralement associés pour permettre une gestion ouverte et décentralisée des ressources informatiques au sein d'une entreprise. **Internet** (voir chapitre 8) qui relie aujourd'hui la grande majorité des ordinateurs peut être considéré comme une interconnexion à l'échelle mondiale de ces différents types de réseaux.

La figure 1.13 illustre ce que pourrait être l'organisation informatique au niveau d'une banque nationale où l'accès à l'information serait possible à partir de tout établissement ou pour tout client. Les agences correspondent à des LAN, l'ensemble formant un MAN ou un WAN suivant les distances.

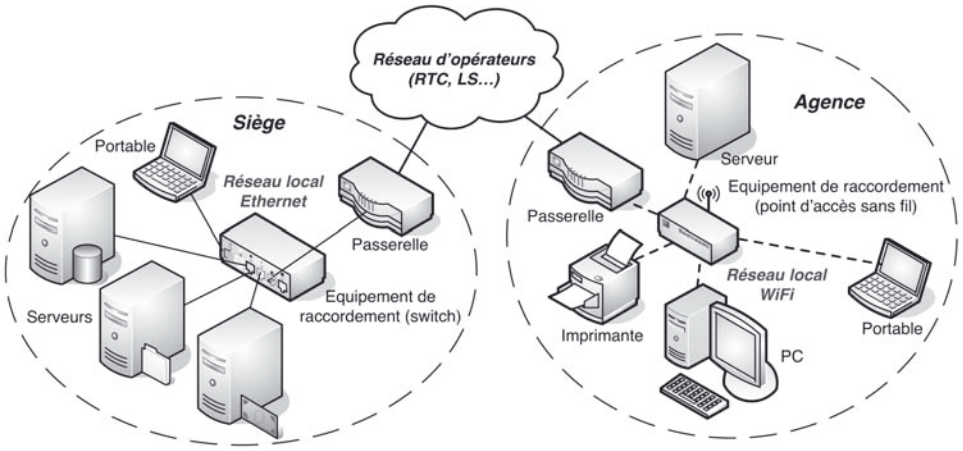


Figure 1.13 – **Exemple d'organisation d'un réseau bancaire.**

1.7 Notion de protocole

Dans le monde des réseaux, un protocole définit un ensemble de règles suivies par les équipements pour se mettre en relation ou pour échanger des informations. Pour chacun des blocs fonctionnels décrits précédemment, un ensemble de protocoles sont définis :

- au niveau de la gestion de la **connexion**, des protocoles décrivent les opérations qui s'enchaînent pour assurer l'ouverture, la gestion et la fermeture de cette connexion (l'internaute connecte son modem ADSL, son FAI – Fournisseur d'Accès Internet – l'authentifie puis lui fournit un accès…) ;
- au niveau de la **communication**, des protocoles tels TCP (voir chapitre 6) gèrent le transport des données entre deux machines en s'appuyant sur la connexion précédemment établie ;
- au niveau du **service**, des protocoles décrivent les commandes et les réponses permettant de transférer et de traiter les données. Par exemple, dans le cas de http, il s'agit de l'envoi d'une page web d'un serveur vers le navigateur d'un client.

Résumé

- Les systèmes disposent de trois blocs fonctionnels : les applications qui veulent **échanger des données** ; les fonctions destinées à **établir et à gérer la communication** et les fonctions assurant la **transmission des données**.
- Un réseau de transmission comprend des **équipements de raccordement** (switch, point d'accès sans fil, routeur, modem…) reliés par des **lignes de transmission**. Il existe deux familles de réseaux : les **réseaux locaux informatiques** à la périphérie d'Internet et les **réseaux de télécommunication** qui composent le réseau cœur d'Internet.
- Les systèmes informatiques communicants sont composés d'**ETTD** pour le traitement des données et d'**ETCD** pour le raccordement à la ligne. Ces deux éléments essentiels sont reliés par une **jonction** normalisée.
- Les systèmes distants peuvent communiquer dans un seul sens – **mode simplex** –, dans les deux sens alternativement – ***half duplex*** – ou dans les deux sens simultanément – ***full duplex***.
- Le codage fait correspondre à chaque caractère une valeur binaire. Les éléments binaires sont transmis les uns après les autres : c'est la **transmission série**. La transmission des informations nécessite leur **mémorisation** et leur **codage**.
- Si l'émetteur transmet son signal d'horloge vers le récepteur, la transmission est dite **synchrone**. Sinon, la transmission est **asynchrone**. En transmission **synchrone**, le signal d'horloge peut être transmis séparément ou codé dans les données, les débits peuvent être beaucoup plus importants. Les données sont regroupées en trames pouvant contenir plusieurs milliers d'octets.
- Suivant la distance entre systèmes informatiques, on distingue les **LAN**, les **MAN** et les **WAN** respectivement à l'échelle d'une **entreprise**, d'une **ville**, de la **planète**.
- Un **protocole** décrit un ensemble de règles utilisées par les équipements pour établir une communication ou échanger des données. Ces protocoles peuvent concerner la **connexion** des équipements, la gestion de la **communication** ou la nature des **informations** échangées.

Exercices corrigés

QCM

Q1.1 Quel bloc fonctionnel est à l'origine de la demande de communication ?

a) L'application b) La gestion de la communication

c) La transmission des données

Q1.2 Indiquer deux des fonctions assurées par un équipement de raccordement.

a) Coder b) Assembler c) Mémoriser
d) Transmettre e) Numéroter

Q1.3 Citer les deux familles de réseaux.

a) LAN b) MAN c) Informatique
d) WAN e) Télécommunication

Q1.4 Dans le cas du raccordement d'un réseau local sur un réseau d'opérateur, quel équipement marque la limite entre les deux réseaux ?

a) De raccordement b) De transmission
c) De connexion d) De routage

Q1.5 Quelle opération fait correspondre une valeur binaire à un caractère ?

a) L'assemblage b) Le codage
c) La transmission d) La numérotation

Q1.6 Indiquer le rôle du bit de parité dans une trame asynchrone :

a) Synchronisation b) Délimitation de fin
c) Contrôle d'erreur

Q1.7 Sur un support physique dans un réseau, les bits d'un message sont transmis :

a) Simultanément b) Séquentiellement

Q1.8 Citer trois types de réseaux informatiques que l'on distingue en fonction de la distance entre les systèmes raccordés.

a) LAN b) MAN c) Informatique
d) WAN e) Télécommunication

Q1.9 À quel type de réseau correspond un réseau d'opérateur ?

a) LAN b) MAN c) WAN

Q1.10 Dans l'exemple du réseau bancaire (figure 1.13), citer une fonction assurée par le réseau d'opérateur.

a) Partage de ressources b) Gestion des clients
c) Interconnexion de sites

Q1.11 Les équipements cités font-ils partie de la catégorie des ETTD ?

a) PC b) Modem
c) Téléphone cellulaire d) Imprimante

Q1.12 Les équipements cités font-ils partie de la catégorie des ETCD ?

a) Terminal b) Téléphone cellulaire
c) Routeur d) Carte réseau

Q1.13 Quel est le mode d'exploitation utilisé dans une communication par téléphone cellulaire ?

a) Simplex b) *Half duplex* c) *Full duplex*

Exercices

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

1.1 (*) Peut-on connecter un ETTD directement sur le réseau téléphonique commuté ?

1.2 (*) Quel est le mode d'exploitation illustré par la figure suivante ?

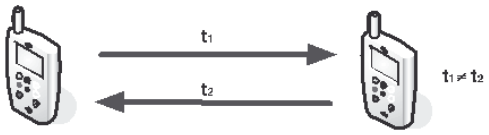


Figure 1.14

1.3 (*) Combien de fils au minimum sont nécessaires, au niveau de la jonction, pour réaliser une transmission en *full duplex* ?

1.4 (**) Même question au niveau de la ligne de transmission.

1.5 (**) Quelle est la durée minimale de transmission d'un fichier de 3 Ko à 2 Mbit/s ?

1.6 (**) Quelle est la différence entre une transmission série et une transmission parallèle ? Dans quels cas cette dernière est-elle encore utilisée ?

1.7 (*) Dans une transmission asynchrone à 56 000 bit/s, quelle est la durée entre l'émission de deux caractères ?

1.8 (**) Quel type de parité est utilisé dans la trame de la figure suivante ?

Figure 1.15

1.9 (*) Dans une transmission asynchrone, quel est le nombre maximum de bits correspondant à une trame ?

1.10 (*) Lors d'une transmission synchrone par modem, comment le signal d'horloge de niveau bit est-il transmis ?

1.11 (**) Dans une transmission synchrone, combien d'octets de données peuvent être transmis par trame ?

1.12 (**) Votre réseau local domestique utilise des transmissions sans fil WiFi. Quels sont les débits usuels ? Quelles sont les portées usuelles ?

Solutions

QCM

Q1.1 : a **Q1.2** : a-d **Q1.3** : c-e **Q1.4** : a **Q1.5** : b

Q1.6 : c **Q1.7** : b **Q1.8** : a-b-d **Q1.9** : b-c **Q1.10** : c

Q1.11 : a-d **Q1.12** : b-d **Q1.13** : c

Exercices

1.1 Les signaux de sortie d'un ETTD sont généralement numériques (sur la prise Ethernet par exemple). Les lignes téléphoniques transmettent des signaux analogiques. Il est donc nécessaire d'interposer un modem.

1.2 Il s'agit d'une liaison en mode unidirectionnel (*half duplex*). Les informations peuvent être échangées dans les deux sens mais à des instants différents (t_1 et t_2).

1.3 Il faut au moins deux fils (TD et RD) pour assurer une liaison en *full duplex*, plus la masse commune.

1.4 Il faudra deux fils si la bande passante est réduite ou un seul fil si la bande passante permet l'utilisation de deux porteuses distinctes, plus la masse commune.

1.5 **Attention** : les tailles de fichier utilisent des puissances de 2 (grandeur traitée dans l'ordinateur), les débits utilisent des puissances de 10 (grandeur traitée sur la ligne). Il s'agit d'une durée minimale car elle ne tient pas compte du temps dédié au contrôle.

$$t = \frac{3 \times 2^{10} \times 8}{2 \times 10^{6}} = 12{,}288 \text{ ms}$$

1.6 Dans une transmission série, les bits sont transmis à la suite ; dans une transmission parallèle, ils sont transmis en même temps, il faut donc autant de fils sur le câble que de bits (un câble en nappe peut être composé de 16 fils pour les données et un fil pour la masse commune). Une transmission parallèle peut donc être utilisée pour obtenir des débits élevés sur de très courtes distances.

1.7 Dans une transmission asynchrone, la durée séparant l'émission de deux caractères peut être quelconque.

1.8 Le nombre de bits à 1 est de 5. Il s'agit donc d'une parité impaire.

1.9 Le nombre de bits sur une trame asynchrone est généralement limité à 11, ce qui correspond aux deux formats suivants :

- 1 bit de départ, 8 bits de données, 1 bit de parité et 1 bit de stop ;
- 1 bit de départ, 7 bits de données, 1 bit de parité et 2 bits de stop.

1.10 Le signal d'horloge n'est pas transmis, il est reconstitué à la réception à partir des signaux de données.

1.11 Ce nombre dépend de la technologie utilisée mais il est généralement de plusieurs centaines d'octets (1 500 octets par exemple dans le cas d'un réseau Ethernet).

1.12 Il s'agit d'un réseau de type WLAN (*Wireless Local Area Network*). La norme WiFi la plus utilisée à l'heure actuelle (IEEE 802.11g) autorise des débits théoriques de 54 Mbit/s. Les portées dépendent largement de la nature et de la géométrie des lieux (murs, planchers, portes…), ils sont de quelques dizaines de mètres.

LES LIAISONS SÉRIE 2

PLAN

OBJECTIFS

- Connaître les principales caractéristiques des liaisons série normalisées.
- Comprendre le fonctionnement de la liaison USB.
- Comprendre le protocole de transmission des bus électroniques I2C et SPI.

2.1 LIAISONS NORMALISÉES

Les principales normes électriques, mécaniques et fonctionnelles rencontrées dans les liaisons séries entre systèmes sont définies par les avis et les recommandations de l'UIT-T, par l'ISO (*International Standardization Organization*), par l'association américaine EIA (*Electrical Industry Association*) ainsi que par l'IEEE (*Institute of Electrical and Electronic Engineers*).

Certaines de ces normes sont équivalentes mais font l'objet de différentes appellations. Ainsi, la norme **RS232C** définie par l'EIA pour des transmissions série bas débit (inférieures à 20 kbit/s) correspond aux avis V24 et V28 de l'UIT-T et à la norme ISO 2110 qui fixent respectivement les caractéristiques fonctionnelles, électriques et mécaniques des liaisons. La norme EIA **RS422** permet des transmissions série du même type mais pour des distances et des débits plus grands. La norme EIA **RS485** est une autre extension qui permet des liaisons multipoints et donc la formation de réseaux de plusieurs machines.

Le standard **USB** fut à l'origine développé par Compaq, Digital, IBM, Intel, Microsoft, Nec et Northern Telecoms. C'est une norme de fait décrite dans un forum : l'USB-IF (*USB Implementers Forum* – http://www.usb.org), créé en 1995 par les sept fondateurs. Les liaisons série USB sont largement utilisées pour la

connexion de périphériques standards, tels les souris, claviers, clés de stockage ou disques durs (voir section 2.3).

Les bus électroniques **I2C** et **SPI** décrits à la fin du chapitre utilisent des liaisons série pour échanger des données sur de très courtes distances entre des modules électroniques. Ils sont définis par des normes proposées au départ par des constructeurs : Philips pour le bus I2C et Motorola pour le bus SPI.

2.2 La liaison RS232/V24

Conçue à l'origine pour la connexion d'équipements avec des réseaux de télécommunication de type analogique (réseau téléphonique), la norme RS232 définit les caractéristiques fonctionnelles de la jonction entre un ETTD et un ETCD (ordinateur-modem) pour un connecteur 25 broches (DB25) ou 9 broches (DB9).

Bien que la liaison RS232 (les anciens ports « COM ») soit remplacée par l'USB sur les PC, elle reste encore très utilisée dans l'industrie, en particulier dans les systèmes automatisés (machines à commande numériques par exemple) et sur les périphériques réseau tels les routeurs ou les commutateurs pour leur configuration. Elle permet des débits jusqu'à 20 kbit/s pour des distances limitées à une dizaine de mètres.

Les données sont transmises de manière asynchrone, en *full duplex* grâce aux lignes TD (*Transmitted Data*) et RD (*Received Data*), trois fils minimum sont nécessaires (TD, RD et la masse). Les autres lignes peuvent être utilisées pour le contrôle entre l'ordinateur et le modem : DCD (*Data Carrier Detect*) pour indiquer que le modem reçoit bien une porteuse sur la ligne, RTS/CTS (*Request To Send/Clear To Send*) pour une demande d'émission de l'ordinateur et une confirmation du modem…

Cette liaison est également utilisée pour la connexion entre deux ETTD, par exemple un terminal ou un PC pour configurer un routeur. Dans ce cas, un câble croisé est nécessaire (figure 2.1).

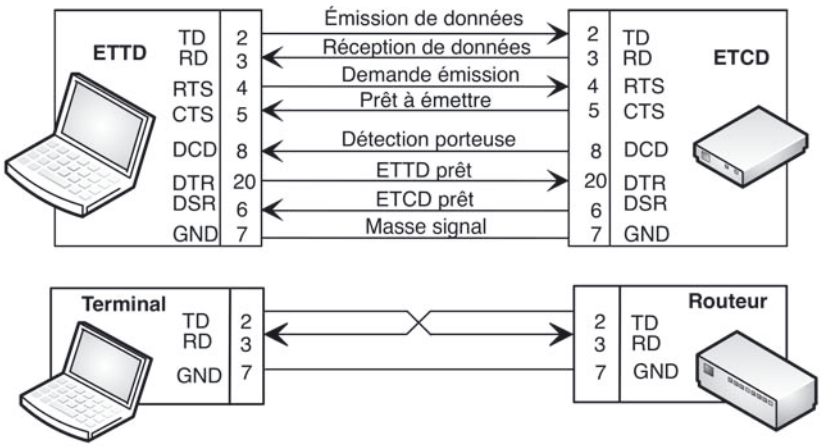


Figure 2.1 – **Liaisons RS232 standard et croisée.**

2.3 Les liaisons RS422 et RS485

La norme EIA RS422 est utilisée pour des transmissions sur de plus grandes distances (supérieure à 1 000 m) et pour des débits plus élevés (supérieurs à 20 kbit/s).

Elle est équivalente à la norme V11 qui définit les caractéristiques électriques des signaux sur un support de transmission différentiel : deux fils correspondant à des niveaux complémentaires sont utilisés pour chaque signal (TD et RD), ce qui assure, dans tous les cas, une tension différentielle équilibrée et limite l'influence des sources de bruits extérieurs et des masses.

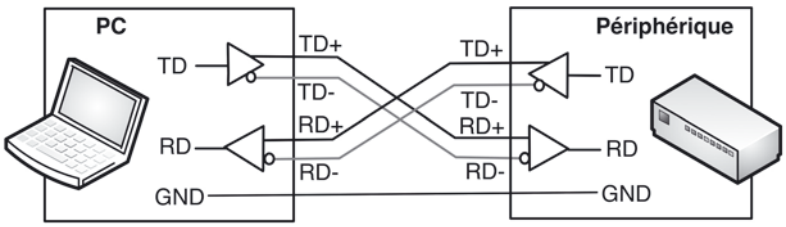


Figure 2.2 – **Liaison différentielle RS422.**

La norme EIA RS485 intègre en plus des circuits trois états, le troisième état « haute impédance » permettant de désactiver les sorties non actives sur le bus partagé. Cette norme autorise donc des liaisons multipoints avec un maximum de 64 nœuds, elle est fréquemment utilisée dans les réseaux locaux industriels.

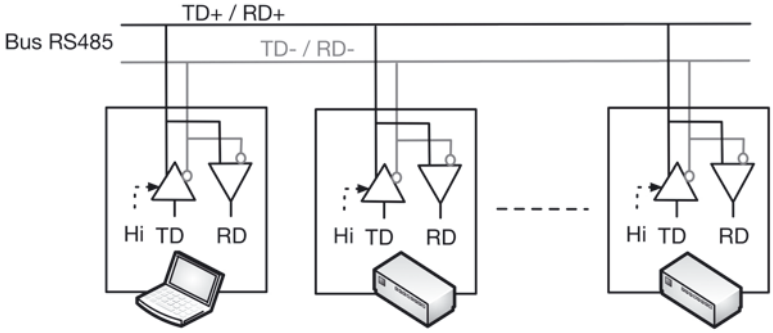


Figure 2.3 – **Liaison différentielle trois états RS485.**

2.4 La liaison USB

2.4.1 Introduction

La norme USB (*Universal Serial Bus*) a été mise au point par Compaq, Digital, IBM, Intel, Microsoft et Nec pour simplifier et augmenter le nombre et les performances des raccordements série sur micro-ordinateur de type PC.

Cette technologie *plug & play* permet de connecter en série jusqu'à 127 périphériques (souris, clavier, imprimante, scanner…) sur un même canal et autorise dans sa version initiale un taux de transfert maximum de 12 Mbit/s (1,5 Mbit/s pour les périphériques lents). La version 2 de la norme, la plus courante aujourd'hui, permet d'obtenir des débits de 120 à 480 Mbit/s pour la connexion de périphériques plus rapides (disques durs, lecteur DVD, clés USB…). La version 3, présente depuis 2010 sur certains équipements rapides (disques durs, clés USB…) propose des débits jusqu'à 4,8 Gbit/s.

En standard, les transferts USB sont effectués entre un hôte, généralement un PC, et un périphérique. Le PC est équipé de plusieurs connecteurs USB permettant de raccorder directement le clavier et la souris par exemple. Les autres périphériques (*functions*) doivent passer par un boîtier de raccordement USB (un *hub*) si le nombre de ports s'avère insuffisant pour réaliser le chaînage de tous les périphériques (figure 2.4).

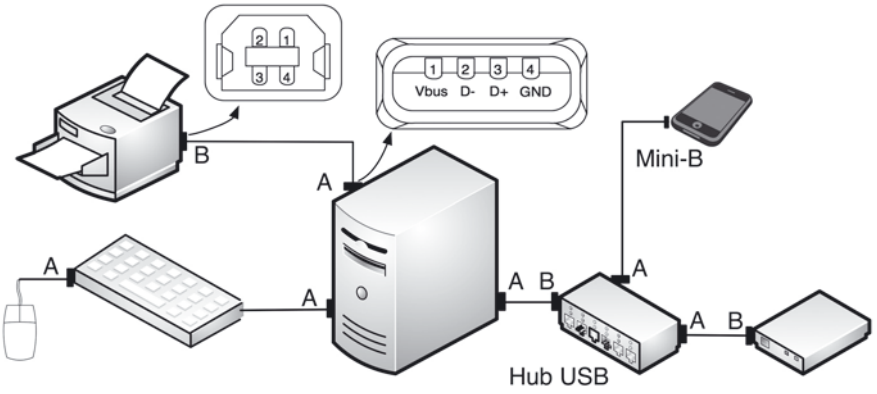


Figure 2.4 – Exemple de chaînage USB.

Deux types de connecteurs USB existent (figure 2.4) :

- type A (*downstream*) sur l'hôte et les sorties du hub ;
- type B (*upstream*) en entrée du hub et sur les périphériques (certains sont équipés en plus d'un connecteur de type A pour le chaînage sans hub).

Il est donc possible en théorie de chaîner jusqu'à 127 éléments les uns après les autres selon l'organisation du bus, et de débrancher n'importe lequel « à chaud » (*hot swap*).

Les cordons de liaison sont de type AB. Ils sont constitués de 4 fils, 2 pour l'alimentation des périphériques (Vbus et GND) et 2 pour les signaux sur paire torsadée (D+ et D–), sa longueur peut atteindre 5 m, son impédance caractéristique est de 80 Ω.

La transmission des signaux sur les deux fils est de type différentielle, avec des tensions inférieures à 0,3 V pour le niveau bas, et supérieures à 2,8 V pour le niveau haut (alimentation en + 5 V sur Vbus).

Les transmissions sur le bus sont de type synchrone ou isochrone (transferts à intervalles de temps réguliers pour des périphériques de type audio ou téléphonique) suivant un codage NRZI (voir chapitre 3).

Bien que l'usage d'une liaison USB soit le plus souvent en mode point à point entre un ordinateur et un périphérique, il s'agit bien, comme l'indique l'appellation USB, d'un bus avec un partage de l'accès au support physique dans le cadre d'une liaison multipoint. Ce qui, du point de vue fonctionnel, est comparable aux architectures de réseaux locaux en bus de type Ethernet notamment (voir chapitre 5).

2.4.2 Connexion d'un périphérique

Lors de la connexion « à chaud » du périphérique à l'hôte, ce dernier détecte l'ajout du nouveau périphérique grâce au changement de la tension entre les fils D+ et D–. À ce moment, l'ordinateur envoie un signal d'initialisation au périphérique pendant 10 ms, puis lui fournit du courant grâce aux fils GND et VBUS (jusqu'à 100 mA). Le périphérique est alors alimenté en courant électrique et récupère temporairement l'adresse par défaut (l'adresse 0).

L'étape suivante consiste à lui fournir son adresse définitive (c'est la procédure d'énumération). Pour cela, l'ordinateur hôte interroge les périphériques déjà branchés (le cas échéant) pour connaître leur adresse et en attribue une au nouveau, qui en retour s'identifie. L'hôte, disposant de toutes les caractéristiques nécessaires est alors en mesure de charger le pilote approprié…

L'adresse est codée sur 7 bits, 128 périphériques (2^7) peuvent être connectés simultanément à un port de ce type. Il convient en réalité de ramener ce chiffre à 127 car l'adresse 0 est une adresse réservée.

Par défaut, chaque connecteur USB ne peut fournir que 100 mA. Avec un hub passif, les ports supplémentaires devront se partager 100 mA, ce qui pour des périphériques gourmands peut être insuffisant. Sur le marché, on trouve donc trois types de hub USB :

- *Low power*, *bus-powered functions hubs* ou *Self-powered functions hubs* (100 mA sur la totalité des ports avec un hub passif) ;
- *Bus-powered hubs* (500 mA sur la totalité des ports) ;
- *High power*, *bus-powered functions hubs* ou *Self-powered hubs* (500 mA sur chaque port).

2.4.3 Protocole de transmission

Le PC hôte initie tous les transferts de données, l'accès au bus se fait lors d'une élection par consultation (*polling*). L'hôte émet un signal de début de séquence chaque milliseconde, intervalle de temps pendant lequel il va donner successivement la « parole » à chacun des périphériques. Cette invitation à la communication correspond à l'envoi successif par le PC hôte à chaque périphérique d'un paquet « Jeton » (*Token packet*) contenant la direction et l'adresse du périphérique USB consulté.

Le périphérique adressé peut alors participer au transfert. La source (PC hôte ou périphérique suivant la direction précisée dans le paquet Jeton) transmet ses paquets de données ou indique qu'il n'a pas de données à transmettre. La destination répond avec un paquet d'acquittement si le transfert a abouti. Un contrôle de flux est réalisé lors de la transmission de plusieurs paquets.

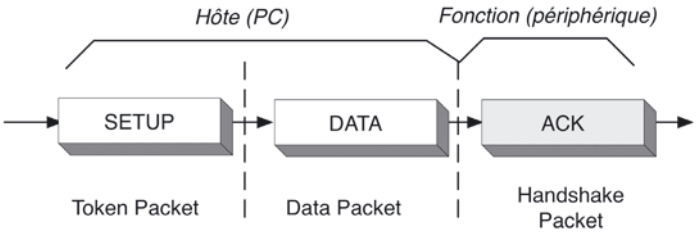


Figure 2.5 – Paquets USB.

Pour chaque périphérique concerné, les transactions USB se font donc par l'intermédiaire de l'émission d'une succession de paquets (figure 2.5) :

- un paquet Jeton (*Token*) envoyé par le PC hôte dans lequel figurent le type de transaction (lecture ou écriture), l'adresse du périphérique de destination et la terminaison désignée (voir ci-dessous) ;
- un paquet de données (*Data*) qui contient les informations réellement utiles dans la transaction (charge utile ou *payload*) ;
- un paquet d'état (*Handshake*) qui indique si l'échange s'est correctement déroulé.

a) Les terminaisons (EndPoints)

Comme l'indique la figure 2.6, chaque périphérique USB est décomposé en plusieurs sous-blocs, possédant chacun un rôle différent dans la communication. Nous pouvons distinguer trois sous-blocs principaux :

- la partie qui décode l'adresse émise par l'hôte dans le paquet Jeton et qui permet au périphérique de savoir que c'est bien à lui que l'hôte s'adresse ;
- la partie terminaison ;
- la partie réalisant la fonction USB proprement dite.

Les terminaisons peuvent être vues comme des intermédiaires, des tampons entre le bus et la fonction USB. En effet, il n'est pas possible pour le bus d'écrire directement dans la fonction, et pour la fonction d'écrire directement sur le bus. Les

données sont donc stockées temporairement (jusqu'à ce que l'hôte ou le périphérique les lisent) dans les terminaisons. C'est pour cette raison que, dans le paquet Jeton, l'hôte précise la terminaison à laquelle il veut s'adresser.

On peut remarquer qu'une même fonction USB peut utiliser plusieurs terminaisons. Dans la spécification USB 1.1, le nombre de paires de terminaisons est limité à 2, c'est-à-dire que les communications peuvent se faire *via* EP0 In, EP0 Out, EP1 In et EP1 Out (EP = EndPoint). La paire de terminaisons utilisée par défaut par l'hôte pour dialoguer avec le périphérique est EP0.

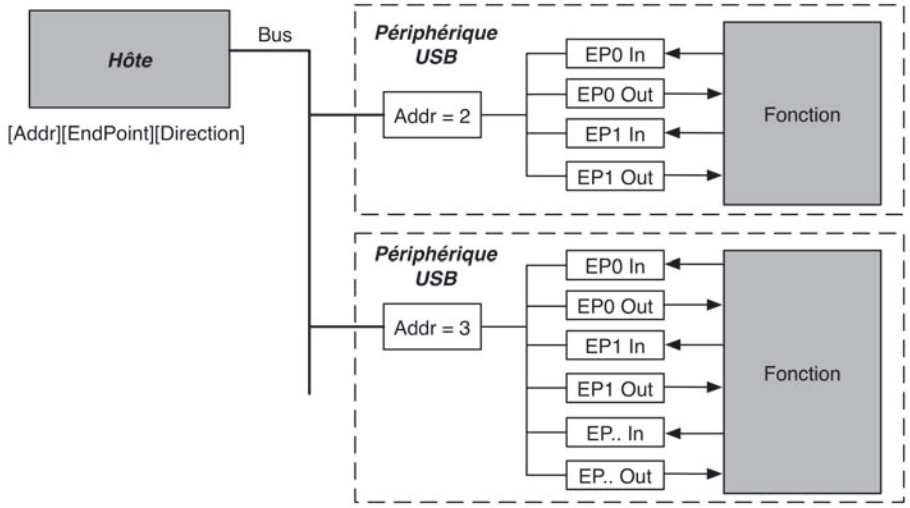


Figure 2.6 – Blocs fonctionnels USB et terminaisons (EP).

b) Les types de transfert

La spécification USB définit quatre types de transferts entre l'hôte et les périphériques :

- **Les transferts de commande (*control*)** : ce sont les transferts généralement utilisés pour les opérations de commande et d'état, par exemple l'énumération du périphérique lors de sa connexion (voir section 2.4.2). Suivant le débit utilisé, la taille des paquets de commande peut être de 8 à 64 octets. Le transfert de commande est fiable : en cas d'erreur sur un paquet, il est répété.
- **Les transferts d'interruption (*interrupt*)** : ce type de transfert est très utilisé, puisque c'est celui qui est mis en œuvre pour les souris, les claviers et tous les périphériques qui n'ont pas une activité permanente mais qui ont besoin d'une prise en compte rapide d'un événement. Dans ce cas, le périphérique signalera à l'hôte qu'il a une information urgente à transférer en utilisant une terminaison spécifique (ce n'est donc pas réellement un mécanisme d'interruption au sens informatique du terme dans la mesure où le périphérique attend le dialogue avec l'hôte et ne force pas l'interruption d'un autre transfert en cours).

- **Les transferts isochrones (*isochronous*)** : c'est le mode de transfert le plus efficace en termes de débit, de disponibilité et de délai d'attente. Mais c'est aussi le plus complexe. Il est utilisé principalement pour des données de type audio ou vidéo avec de fortes contraintes de temps. Ce type de transfert assure un débit minimum, mais il peut arriver que certains paquets soient erronés.
- **Les transferts en bloc (*bulk*)** : ce type de transfert est utilisé quand il faut transférer une grande quantité d'informations pendant un temps relativement court. Par exemple, un appareil photo ou une caméra numérique utilisent ce type de transfert pendant lequel 90 % de la bande passante du bus est attribuée au périphérique et les paquets erronés sont répétés.

c) Les descripteurs USB

Ce point est essentiel pour le fonctionnement correct du bus. En effet, chaque périphérique possède des caractéristiques propres qui le différencient du voisin. L'hôte (le PC) doit être en possession de toutes ces caractéristiques pour initier une communication avec le périphérique en question. Pour cela, chaque périphérique possède une série de descripteurs (données enregistrées sur une mémoire morte) qui précisent complètement son identité, la façon de communiquer avec lui, sa compatibilité USB 2 ou 3…

L'hôte accède aux différents champs des descripteurs par un jeu de requêtes décrites dans la partie logicielle de la spécification USB.

Le mode veille est obligatoire sur tous les appareils USB. Un périphérique USB entrera en veille lorsqu'il n'y a aucune activité sur le bus pendant plus de 3 ms. Il dispose ensuite de 7 ms supplémentaires pour confirmer ce mode et ne consommer que le courant de veille nominal (500 µA) nécessaire à son éventuelle reprise d'activité.

2.4.4 Norme USB 2

Comme indiqué précédemment, l'apport de la norme USB 2.0 se situe essentiellement au niveau du débit augmenté. Ce dernier permet des transferts d'informations volumineuses avec des périphériques performants tels les disques durs externes ou les appareils photos et caméras numériques. Typiquement, un transfert de 10 Go (Giga-octets) entre un PC et un disque dur externe prendra environ 3 minutes à 480 Mbit/s (USB 2.0) contre près de 2 heures à 12 Mbit/s (USB 1.1) !

Un classement en fonction du débit utilisé et du type de périphérique a été introduit. Trois classes de performances sont ainsi proposées : *Low-Speed*, *Full-Speed* et *High-Speed* (figure 2.7). Lors d'une connexion entre un hôte et un périphérique USB, si l'un des deux ne supporte pas la nouvelle norme USB 2.0, le transfert se fera automatiquement à bas débit suivant la norme USB 1.1 (rétrocompatibilité).

Enfin, la norme USB 2.0 s'est enrichie d'une fonctionnalité appelée *On-The-Go* (OTG) pour pouvoir effectuer des échanges de données « d'égal à égal » (*peer to peer*) entre deux périphériques sans avoir à passer par un hôte du type PC. Un périphérique OTG peut donc se connecter à un autre périphérique OTG, à un

Performance	*Applications*	*Caractéristiques*
Low-Speed · Périphériques interactifs · 10 - 100 Kbps	Clavier, souris, périphériques de jeux, périphérique type réalité virtuelle.	Faible coût, usage simple, branchement/débranchement dynamique, périphérique multiples.
Full-Speed · Téléphonie, audio, vidéo compressée · 500 Kbps – 10 Mbps	Téléphones standard, périphériques audio, microphone.	Faible coût, usage simple, branchement/débranchement dynamique, périphérique multiples, bande passante garantie, latence garantie.
High-Speed · Vidéo, stockage · 25 – 400 Mbps	Périphériques vidéo, disques durs, lecteurs DVD.	Faible coût, usage simple, branchement/débranchement dynamique, périphérique multiples, bande passante garantie, latence garantie, bande passante élevée.

Figure 2.7 – Classes de débit USB.

périphérique (non-OTG) ou à un hôte. Les applications de cette extension sont par exemple la connexion directe d'un appareil photo avec une imprimante ou la connexion d'un téléphone cellulaire avec un lecteur MP3.

Pour cette fonctionnalité, des prises mini A et B, des câbles mini USB et des câbles convertisseurs mini-standards sont définis. Dans le cas d'une connexion OTG-OTG, c'est le type de prise, min A ou B, qui va permettre de déclarer lequel des deux périphériques OTG va prendre provisoirement le rôle d'hôte. Ensuite, il peut se produire un renversement des rôles suite à une étape de négociation entre les deux systèmes OTG (protocole HNP).

2.4.5 Norme USB 3

L'USB 3.0 propose un débit supérieur pouvant aller jusqu'à 4,8 Gbit/s (*Super-Speed* USB). Les nouveaux périphériques utilisent des connecteurs de type A ou B munis d'une double rangée de contacts superposés, la partie supérieure (USB 3 - *SuperSpeed*) permettant les transferts haut débit avec des lignes différentielles pour l'émission et la réception.

La compatibilité ascendante avec les versions antérieures est assurée : les câbles USB 1.1/2.0 peuvent être utilisés sur des prises USB 3.0 et les protocoles de transfert restent compatibles. En revanche, la compatibilité descendante est impossible : les câbles USB 3.0 ne pouvent se connecter directement sur les prises USB 1.1/2.0 (des adaptateurs sont disponibles).

L'autre amélioration importante proposée par l'USB 3 est la gestion de l'énergie. Des procédures sont prévues pour mettre en veille automatiquement les équipements, notamment les hubs, en cas de cessation d'activité.

2.5 Les bus série I2C et SPI

2.5.1 Les bus électroniques

Ces bus font partie de la catégorie des bus électroniques. Ce sont donc des bus série synchrones destinés à transférer à faible débit et faible distance (à l'échelle d'une carte, d'un connecteur ou d'un câble de quelques centimètres) des données entre une carte mère et d'autres modules électroniques (microcontrôleur, mémoire, CAN, afficheur LCD, coupleur sans fil…).

Les liaisons étant multipoint sur le bus, une électronique de commande est nécessaire pour déconnecter (état haute impédance) les sorties inactives.

2.5.2 Le bus I2C

a) Introduction

Le bus I2C a été développé au début des années 1980 par Philips Semiconductors pour permettre de relier facilement à un microprocesseur les différents circuits d'un téléviseur moderne.

Le bus I2C est un bus série synchrone qui permet de faire communiquer entre eux des composants électroniques très divers grâce à seulement trois lignes (figure 2.8) :

- un signal de donnée **SDA** (*Signal DAta*) ;
- un signal d'horloge **SCL** (*Signal CLock*) ;
- un signal de référence électrique (GND).

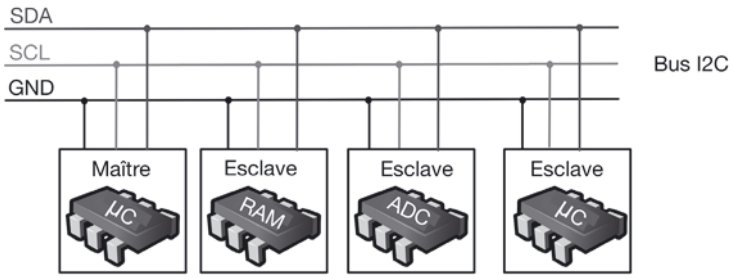


Figure 2.8 – **Architecture du bus I2C.**

Chaque périphérique connecté au bus I2C a une adresse unique et peut agir comme un récepteur et/ou un émetteur. Un afficheur LCD sera récepteur seulement alors qu'une mémoire sera réceptrice et émettrice.

Le bus I2C est un bus multimaître : plusieurs microcontrôleurs (µC) peuvent être les initiateurs d'une transmission de données. L'initiateur est considéré comme le maître du bus et tous les autres comme des esclaves.

Les signaux SDA et SCL sont initialement bidirectionnels. Ce qui signifie qu'ils peuvent être émis par le µC qui a la main (le maître) comme par les autres périphériques (les esclaves). Toutefois, seul un circuit de type µC peut générer le signal

d'horloge. Comme pour le bus RS485 décrit précédemment, afin d'éviter les conflits électriques entre les sorties des modules connectés sur le bus multipoint, les entrées/sorties SDA et SCL sont de type trois états.

Les données sont transmises en série à 100 kbits/s en mode standard et jusqu'à 400 kbits/s en mode rapide (d'autres modes jusqu'à 5 Mbps existent).

La variété des circuits disponibles disposant d'un port I2C est grande : ports d'E/S bidirectionnels, convertisseurs A/N et N/A, mémoires (RAM, EPROM, EEPROM...), circuits Audio (égaliseur, contrôle de volume…) et autre drivers (LED, LCD…). Le nombre de composants qu'il est ainsi possible de relier est essentiellement limité par la charge capacitive des lignes SDA et SCL : 400 pF.

b) Protocole de transmission

Le protocole I2C définit la succession des états logiques possibles sur SDA et SCL, et la façon dont doivent réagir les circuits en cas de conflits. Le bus est toujours dans l'un des états suivants : START, ADDRESS, ACKNOWLEDGE, DATA, STOP). Ces états correspondant à des conditions uniques.

Le cycle de fonctionnement normal est le suivant (figure 2.9) :

- le bus est initialement au repos (SDA et SCL à « 1 ») ;
- le µC qui doit réaliser une transmission prend le contrôle du bus en envoyant une condition de départ (START) à tous les périphériques connectés à l'écoute. Le µC devient le maître, c'est lui qui génère le signal d'horloge ;
- le µC envoie l'adresse du périphérique (ADDRESS) concerné avec l'information lecture ou écriture (R/W) ;
- tous les périphériques vont comparer l'adresse émise avec leur propre adresse :
  - ◇ si ce n'est pas son adresse, le périphérique va se mettre en attente de la condition STOP,
  - ◇ si c'est son adresse, le périphérique va acquitter (ACKNOWLEDGE) ;
- dès que le µC reçoit l'acquittement, il peut transmettre ou recevoir les données, suivant la valeur de R/W ;
- quand il a terminé la transmission, il envoie la condition d'arrêt (STOP). Le bus est alors libre et tous les contrôleurs peuvent démarrer une nouvelle transmission.

Figure 2.9 – États du bus I2C.

c) Lecture/écriture d'une donnée

Pour une écriture de données, les états successifs des lignes SDA et SLC sont les suivants (figure 2.10) :

- après avoir imposé la condition de départ (SDA passe à « 0 », SCL reste à « 1 »), le maître applique sur SDA le bit d'adresse de poids fort A6 (les adresses sont

codées sur 7 bits). Il valide ensuite la donnée en appliquant pendant un instant un niveau « 1 » sur la ligne SCL ;

- lorsque SCL revient à « 0 », il recommence l'opération jusqu'à ce que l'adresse complète soit transmise. Il envoie ensuite le bit R/W à « 0 » pour signifier qu'il s'agit d'une écriture ;
- le maître envoie alors un bit ACK à « 1 » tout en scrutant l'état réel de SDA. L'esclave doit alors imposer un niveau « 0 » pour signaler au maître que la transmission s'est effectuée correctement. Les sorties étant de type « collecteur ouvert », si l'esclave impose un « 0 », c'est un « 0 » qui sera relu par le maître (état dominant) ;
- la transmission des 8 bits de données et de l'acquittement correspondant s'effectue de la même manière ;
- lorsque le maître a terminé son écriture sur un ou plusieurs octets, il envoie la condition d'arrêt (SDA passe à « 1 », SCL reste à « 1 »).

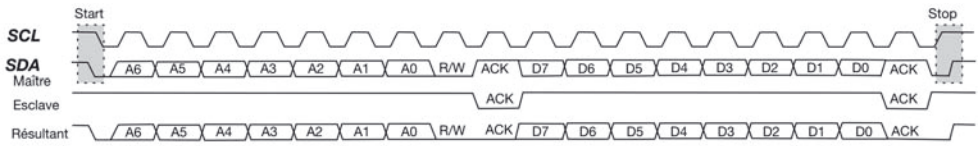


Figure 2.10 – Écriture d'une donnée.

Pour une lecture, la séquence est sensiblement la même. Le bit R/W est positionné à « 1 ». Après la lecture d'un octet, le maître positionne ACK à « 0 » s'il veut lire la donnée suivante (cas d'une mémoire par exemple) ou à « 1 » pour envoyer la condition d'arrêt.

d) Gestion des conflits

Si plusieurs contrôleurs sont connectés au bus, chacun pouvant prendre possession du bus dès que celui-ci est libre, il existe une probabilité pour que deux contrôleurs prennent le contrôle simultanément. Si cela ne pose pas de problème d'un point de vue électrique (sorties « collecteur ouvert »), il faut pouvoir détecter ce conflit pour éviter d'obtenir des niveaux erronés sur le bus.

Chaque contrôleur vérifie en permanence l'état des lignes SDA et SCL, y compris lorsqu'il est lui-même en train d'envoyer des données. On distingue alors deux cas :

- un contrôleur impose un « 0 » sur le bus. Il relira forcément un « 0 » (état dominant) et continuera à transmettre. Il ne peut pas alors détecter un éventuel conflit avec un autre contrôleur ;
- un contrôleur cherche à imposer un « 1 » sur le bus. S'il ne relit pas un « 1 », c'est qu'un autre contrôleur a pris la main dans le même temps. Le premier perd alors immédiatement le contrôle du bus et devient esclave pour ne pas perturber la transmission du second, qui, lui, devient maître.

2.5.3 Le bus SPI

a) Introduction

Le bus SPI (*Serial Peripheral Interface*) est un standard établi par Motorola et intégré dans de nombreux microcontrôleurs (Motorola, Atmel, Microchip, Texas Instruments…). Il permet des transferts jusqu'à 20 Mbit/s.

Comme le bus I2C, il est dédié aux communications inter-composants (mémoires, DSP, CAN, CNA, CODEC…), voir inter-cartes, au sein d'un même système. Il s'agit donc d'un bus série synchrone avec quelques particularités :

- deux lignes de données pour des transferts *full duplex* ;
- un seul maître possible sur le bus ;
- une ligne dédiée pour la sélection de l'esclave plutôt qu'un adressage.

Le bus SPI décrit sur la figure 2.11 contient quatre signaux logiques, plus la masse non représentée ici :

- un signal d'horloge généré par le maître **SCLK** (ou SCK) ;
- un signal de données généré par le maître **MOSI** (*Master Output / Slave Input,* parfois noté SDO) ;
- un signal de données généré par l'esclave **MISO** (*Master Input / Slave Output,* parfois noté SDI) ;
- un ou plusieurs signaux de sélection de l'esclave, actifs à l'état bas, généré par le maître *SS* (*Slave Select*, ou CS).

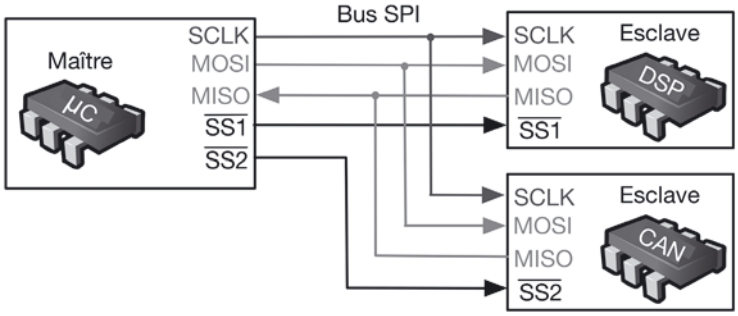


Figure 2.11 – Signaux SPI.

b) Protocole de transmission

Le maître a l'initiative des échanges : il sélectionne l'esclave (activation de la ligne SS), génère l'horloge SCLK, et les données (MOSI et MISO) sont échangées dans les deux sens simultanément. Le maître ne tient pas compte de la donnée reçue dans le cas d'un échange « écriture seule » ou alors il envoie un octet sans importance (0xFF) dans le cas d'un échange « lecture seule ».

Les données sont échangées par octet. Suivant la configuration choisie, chaque bit est transmis sur un front montant ou descendant de l'horloge (figure 2.12). En

fonction du mode de synchronisation de l'esclave, le type d'horloge est choisi sur le contrôleur grâce à une combinaison de 2 bits dans le registre de contrôle SPCON (*Serial Peripheral CONtrol register*) :

- le bit **CPOL** (*Clock POLarity*) détermine le niveau logique de la ligne SCLK au repos ;
- le bit **CPHA** (*Clock PHAse*) détermine le front sur lequel la donnée est modifiée et le front sur lequel la donnée va être lue.

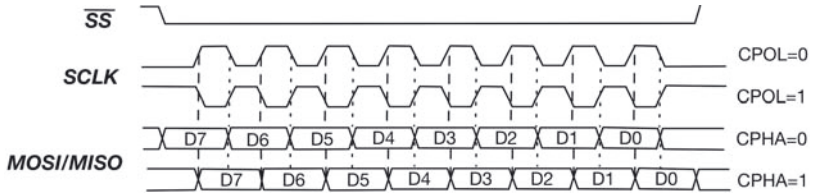


Figure 2.12 – **Synchronisation SPI.**

Par ailleurs, la vitesse de transmission est paramétrable dans le registre de contrôle SPCON. La fréquence d'horloge est choisie parmi sept fréquences (3 bits dans le registre de contrôle) obtenues par division de la fréquence de fonctionnement du microcontrôleur.

c) Comparaison I2C

Les avantages du bus SPI par rapport à l'I2C sont ses transferts *full duplex*, un débit plus important et une consommation moindre dans la mesure où les sorties ne sont pas de type « trois états ». Ses inconvénients sont l'impossibilité de sélectionner un maître parmi plusieurs, le nombre limité d'esclaves (beaucoup de contrôleurs SPI ne possèdent qu'une ligne de sélection) et l'absence d'acquittement.

Résumé

- La norme **RS232** définit une jonction sur un connecteur 25 ou 9 broches (DB25 ou DB9) pour des communications série, asynchrone et *full duplex* limitées à **20 kbit/s**. Trois lignes minimum sont nécessaires (Td, RD et GND). Ses extensions **RS422** et **RS485** permettent respectivement des distances plus élevées et des connexions multipoints.
- La liaison **USB** permet le raccordement « à chaud » de périphériques standards à un ordinateur. Elle offre des débits jusqu'à 480 Mbit/s (USB2) et potentiellement 4,8 Gbit/s (USB3). Le périphérique connecté est généralement alimenté par la liaison USB et autoconfiguré. Le PC hôte initie tous les transferts de données, l'accès au bus se faisant lors d'une élection par consultation (*polling*). Dans la mesure où les périphériques peuvent être très variés (souris, disque dur, smartphone…), ces derniers possèdent en mémoire morte des descripteurs lus par le PC hôte lors de l'initialisation et permettant d'adapter la communication (compatibilité USB2 ou 3, transferts par blocs possibles, modes veille…).
- Les bus I2C et SPI sont des **bus électroniques** synchrones prévus pour des transferts entre les différents modules d'un système informatique (microcontrôleur vers une mémoire, un convertisseur numérique-analogique, une interface sans fil…).
- Le bus **I2C** est un bus multipoint utilisant seulement trois lignes (données, horloge et masse). Il peut exister plusieurs contrôleurs sur le bus mais, à un instant donné, seul un maître a le contrôle du bus. Lors d'une séquence de transmission, le maître envoie successivement l'adresse de l'esclave sur 7 bits, un bit R/W pour indiquer s'il s'agit d'une lecture ou d'une écriture. Suivent les octets de données transmis par le maître ou l'esclave sélectionné. Ce dernier acquitte à l'aide d'un bit spécifique l'adresse et les données reçues.
- Le bus **SPI** a un fonctionnement plus simple et permet des débits plus élevés. En plus de l'horloge, deux lignes de données sont prévues pour des transmissions *full duplex*. Des lignes spécifiques (généralement de 1 à 3) permettent de sélectionner les esclaves. Il n'y a pas la possibilité de choisir parmi plusieurs maîtres.

Exercices corrigés

QCM

Q2.1 Quels sont les débits usuels sur une liaison USB ?

a) 1 Mbit/s b) 12 Mbit/s c) 480 Mbit/s d) 4,8 Gbit/s

Q2.2 Combien peut-on, en théorie, connecter de périphériques sur un connecteur USB d'ordinateur ?

a) 10 b) 32 c) 64 d) 127

Q2.3 Combien de paquets sont nécessaires pour une transaction USB ?

a) 2 b) 4 c) 1 d) 3

Q2.4 Quelle est la durée du transfert d'un fichier de 4 Go vers une clé USB2 ?

a) 5 mn b) 20 mn c) 60 s d) 5 s

Q2.5 Sur quel type de liaison peut-on réaliser des transferts isochrones ?

a) RS232 b) RS485 c) USB d) I2C

Q2.6 Combien de fils sont présents sur une liaison USB ?

a) 2 b) 3 c) 4 d) 6

Q2.7 Le bus I2C est-il un bus ?

a) synchrone b) asynchrone c) isochrone

Q2.8 Combien d'esclaves peuvent être connectés sur un bus I2C ?

a) 16 b) 32 c) 64 d) 127

Q2.9 Comment le début d'une transmission est-il signalé sur le bus I2C ?

a) bit de START b) préambule c) SDA =0, SCL = 1

Q2.10 Sur quel(s) bus les données sont-elles acquittées ?

a) USB b) RS485 c) SPI d) I2C

Q2.11 Sur quelle(s) liaison(s) les transferts sont-ils *full duplex* ?

a) RS232 b) USB c) I2C d) SPI

Q2.12 Sur quelle(s) liaison(s) la transmission des signaux est-elle de type différentiel ?

a) SPI b) I2C c) RS422 d) USB

Q2.13 Combien peut-il y avoir de maîtres potentiels sur un bus SPI ?

a) 1 b) 2 c) n

Q2.14 Sur le bus SPI, les données sont lues sur un front d'horloge :

a) montant b) descendant c) l'un ou l'autre

Exercices

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

2.1 (*) Pourquoi une liaison différentielle de type RS422 permet-elle des distances plus élevées ?

2.2 (*) Comment un périphérique USB signifie-t-il au PC que le transfert d'un paquet de données a réussi ?

2.3 (**) Comparer les temps de transfert d'un fichier de 3 Go sur liaison USB 2 et sur une liaison de type FireWire à 3,2 Gbit/s.

2.4 (***) La norme Serial ATA (*Advanced Technology Attachment*) permet de connecter en série des disques durs en interne avec un débit théorique de 150 Mo/s, supérieur au débit obtenu avec une connexion parallèle de type Parallel ATA 133 (133 Mo/s). Comment expliquer ce gain ?

2.5 (*) Sur une liaison USB, comment le PC détecte-t-il la présence d'un périphérique au moment de la connexion ?

2.6 (**) Comment les adresses sont-elles affectées lorsque plusieurs périphériques sont connectés sur le même port USB ?

2.7 (**) Sur une liaison USB comprenant plusieurs périphériques, comment la parole est-elle distribuée ?

2.8 (*) Comment le PC hôte sait-il qu'une transmission USB vers un périphérique connecté s'est déroulée sans erreur ?

2.9 (**) Plusieurs types de transferts sont possibles sur une liaison USB. Quel est le type le plus adapté pour regarder une vidéo à partir d'une clé USB ? Quel est le type à privilégier pour le stockage d'un fichier volumineux sur un disque dur USB ?

2.10 (***) Sur le bus I2C, lorsque plusieurs contrôleurs sont connectés, comment la prise de contrôle du bus par l'un d'eux est-elle réalisée ? Que se passe-t-il si plusieurs contrôleurs prennent le contrôle au même instant ?

2.11 (***) Comment est effectué l'acquittement des données sur le bus I2C ? Comment un esclave peut-il être sûr que le maître a bien reçu les données ?

2.12 (***) Établir le chronogramme des lignes SCL et SDA du bus I2C pour un transfert d'un octet de valeur B2 vers un esclave d'adresse 7C.

2.13 (**) Comment les esclaves sont-ils adressés sur un bus SPI ? Combien d'esclaves peut-on avoir au maximum ?

2.14 (**) Pour quelle(s) raison(s) les débits peuvent-ils être plus importants sur un bus SPI que sur un bus I2C ?

Solutions

QCM

Q2.1 : b-c-d **Q2.2** : d **Q2.3** : d **Q2.4** : c **Q2.5** : c

Q2.6 : c **Q2.7** : a **Q2.8** : d **Q2.9** : c **Q2.10** : a-d

Q2.11 : a-d **Q2.12** : c-d **Q2.13** : a **Q2.14** : c

Exercices

2.1 Sur une liaison différentielle deux fils correspondant à des niveaux complémentaires sont utilisés pour chaque signal, contrairement à une liaison standard sur laquelle chaque signal est référencé par rapport à une masse commune. Une tension différentielle reste donc équilibrée et limite l'influence des sources de bruits extérieurs et des masses.

2.2 Un acquittement (ACK) est envoyé dans un paquet d'état (*Handshake Packet*) par le périphérique vers le PC pour confirmer la bonne réception du paquet de données.

2.3 Sur une liaison USB2 à 480 Mbit/s, le temps théorique de transfert est de $t_{USB} = 3 \times 2^{30} \times 8 / 480 \times 10^6 = 53{,}68$ s. Sur une liaison FireWire à 3 200 Mbit/s : $t_{FW} = 3 \times 2^{30} \times 8 / 3\,200 \times 10^6 = 8$ s. Ces temps sont théoriques car ils ne tiennent pas compte d'une part du temps nécessaire au contrôle de la liaison (en-têtes, Jeton, acquittement…) et d'autre part de l'éventuel partage de la bande passante dans le cas de la liaison USB.

2.4 Sur une interface où les données sont envoyées en parallèle (16 bits à la fois pour ATA 133), l'augmentation de la fréquence pose des problèmes d'interférence électromagnétique liée à la proximité des fils sur la nappe, chacun des fils portant des informations différentes. Ces interférences sont limitées par la multiplication des fils de masse intercalés avec les fils de donnée.

Sur une interface *Serial ATA*, le câble rond est limité à sept fils (trois fils pour la masse et deux paires pour les données) et présente donc une bien meilleure indépendance des signaux.

2.5 Le PC détecte l'ajout du nouveau périphérique grâce au changement de la tension entre les fils D+ et D– présents sur le connecteur.

2.6 Le PC interroge les périphériques déjà connectés pour connaître leurs adresses (codées sur 7 bits) et attribue l'adresse suivante disponible au nouveau périphérique. Il n'y a donc pas de relation entre l'adresse et le type de périphérique.

2.7 Le PC donne successivement la « parole » à chacun des périphériques en envoyant un paquet « Jeton » contenant la direction et l'adresse du périphérique USB consulté. L'accès au bus se fait donc lors d'une élection par consultation (*polling*).

2.8 Le PC transmet un paquet de données au périphérique connecté, ce dernier confirme la bonne réception avec un paquet spécifique d'acquittement.

2.9 La lecture en continu de données vidéo nécessite une gestion rigoureuse du temps, les transferts isochrones sont dans ce cas adaptés. Pour le stockage sur disque dur, le débit est à privilégier, les transferts en bloc sont dans ce cas les plus performants.

2.10 Le contrôleur qui souhaite réaliser une transmission prend le contrôle du bus en envoyant une condition de départ (START : SDA passe à « 0 », SCL reste à « 1 ») à tous les périphériques connectés. Le contrôleur devient le maître, les autres contrôleurs deviennent esclaves. Les contrôleurs lisent en permanence l'état des lignes ; si un contrôleur relit une valeur, par exemple sur un bit d'adresse, qui ne correspond pas à ce qu'il a envoyé, il laisse la main et devient aussitôt esclave. L'état « 0 » étant l'état dominant, cette détection n'est possible que si le premier contrôleur envoie un « 1 » et relit un « 0 ».

2.11 Pour une écriture, le maître envoie, après les données, un bit ACK à « 1 » tout en scrutant l'état réel de SDA. L'esclave doit alors imposer un niveau « 0 » pour acquitter la transmission. Dans le cas d'une lecture, l'esclave ne gère pas l'état du bit ACK, il ne peut donc pas savoir directement si le maître a bien reçu les données. La lecture de l'état du bit ACK lui permet seulement de savoir si un nouvel octet est demandé (ACK = 0) ou si c'est la fin de la transmission (ACK = 1). En cas d'erreur sur une lecture, le maître peut toujours demander une retransmission.

2.12 La ligne SDA représentée correspond au signal résultant, les bits ACK sont à « 03 ».

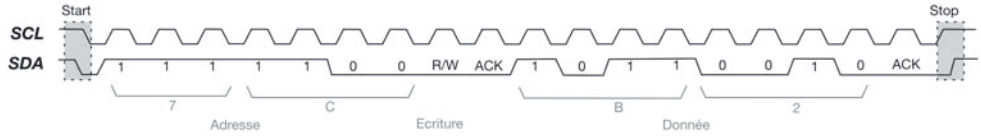


Figure 2.13

2.13 L'adresse n'est pas envoyée sur la ligne de données comme pour le bus I2C, une ligne spécifique SS (*Slave Select*), active à l'état bas, permet de sélectionner un esclave. Certains microcontrôleurs possèdent jusqu'à trois lignes de sélection (SS1, SS2, SS3). Au-delà de trois esclaves, une logique supplémentaire commandée à partir d'autres sorties numériques doit être câblée.

2.14 Le bus SPI utilise des sorties logiques simples et non des sorties « 3 états » comme sur le bus I2C, les temps de commutation sont donc beaucoup plus faibles. Par ailleurs, seuls les octets de données sont envoyés, le bus I2C envoie en plus l'adresse et des bits de contrôle. Enfin, les transmissions sont *full duplex*, ce qui améliore le débit global.

TRANSMISSION DU SIGNAL NUMÉRIQUE

3

PLAN

OBJECTIFS

- ➤ Connaître les principes de base de la transmission en bande de base et en bande transposée.
- ➤ Comprendre le fonctionnement des modulations de type PSK+AM utilisées dans la plupart des liaisons sans fil ou longue distance.
- ➤ Savoir caractériser une voie de transmission (capacité, débit, valence, multiplexage).
- ➤ Étudier les caractéristiques des transmissions ADSL, sur fibre et WiMAX.

3.1 TRANSMISSION EN BANDE DE BASE

3.1.1 Principe

Lorsque la longueur de la liaison ne dépasse pas quelques centaines de mètres, les informations peuvent être transmises sur le support de liaison sans transformation du signal numérique en signal analogique.

Ce type de transmission sans transposition de fréquence par modulation est appelé transmission en bande de base (figure 3.1).

La transmission en bande de base rencontrée principalement dans les réseaux locaux permet d'obtenir des circuits de données à grand débit et faible portée (débits supérieurs à 1 Mbit/s pour des distances inférieures à 1 km), en utilisant directement des supports physiques de type métallique (paires torsadées ou câble coaxiaux) ou optique avec éventuellement l'adjonction de répéteurs disposés sur des intervalles allant de 500 mètres à quelques kilomètres.

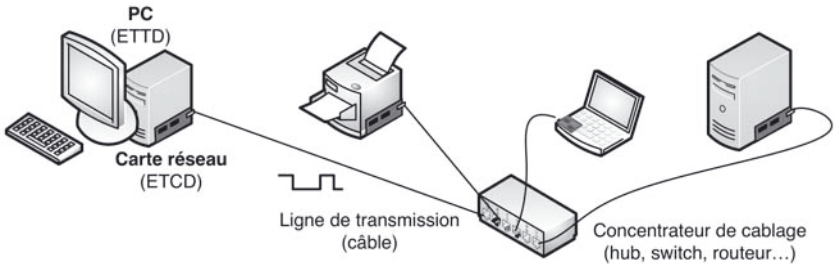


Figure 3.1 – Transmission en bande de base.

En général, le signal binaire n'est pas transmis directement sur la ligne et différents codages numériques sont utilisés pour différentes raisons :

- la récupération de l'horloge nécessaire en transmission synchrone est facilitée par des séquences qui présentent des changements d'état fréquents et évitent ainsi les longues suites de 1 ou de 0 ;
- le spectre d'un signal binaire est concentré sur les fréquences basses qui sont les plus affaiblies sur la ligne ;
- les perturbations subies par un signal sont proportionnelles à la largeur de sa bande de fréquence.

Les codages en bande de base vont donc essentiellement avoir pour rôle de diminuer la largeur de bande du signal binaire et de transposer celle-ci vers des fréquences plus élevées (figure 3.6). C'est l'ETCD, la carte réseau intégrée dans le PC ou le routeur, qui réalise ce codage en bande de base.

3.1.2 Principaux codages

a) Code NRZ (*No Return to Zero*)

Le signal binaire est simplement transposé en tension pour éviter une composante continue non nulle, source de consommation (figure 3.2).

Le code NRZI (*No Return To Zero Inverted*) présente les mêmes caractéristiques mais pour éviter les successions de 0, le signal reste dans le même état pour coder un 0 et change d'état pour coder un 1.

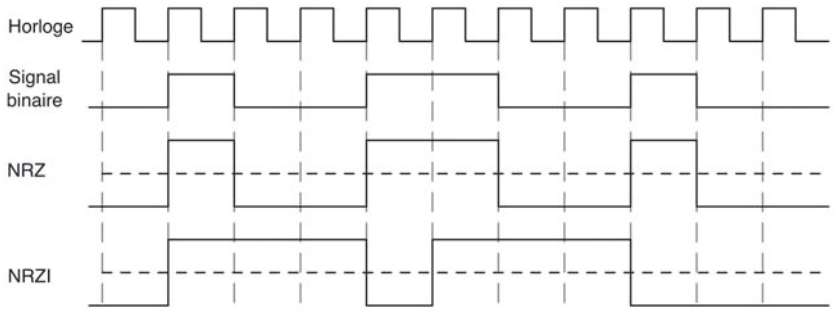


Figure 3.2 – Codes NRZ et NRZI.

b) Code biphase ou code Manchester

Pour augmenter les changements d'états, une transition systématique est réalisée au milieu de chaque bit du signal binaire : une transition négative lorsque le signal binaire est à 1 et une transition positive lorsque le signal binaire est à 0 (figure 3.3).

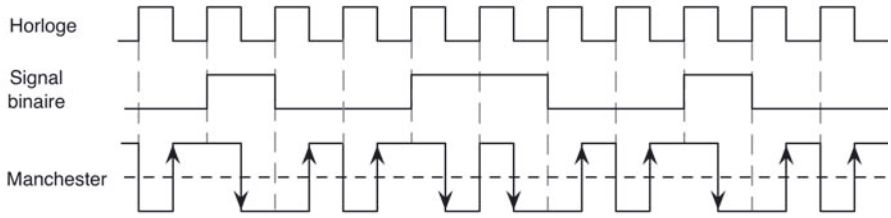


Figure 3.3 – Code Manchester.

c) Code biphase différentiel ou Manchester différentiel

Une transition systématique est réalisée au milieu de chaque bit. Pas de transition pour coder un bit à 1, une transition pour coder un bit à 0 (figure 3.4).

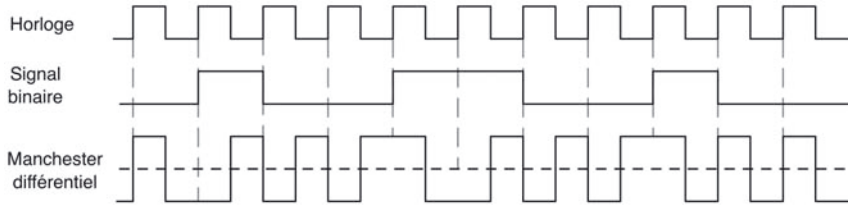


Figure 3.4 – Code Manchester différentiel.

d) Code de Miller ou Delay Mode

Une transition au milieu du bit pour un 1, pas de transition en milieu de bit pour un 0. Une transition à la fin du bit pour un 0 si le bit suivant est aussi un 0 (figure 3.5).

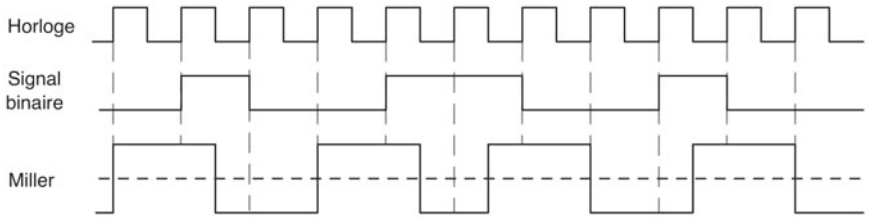


Figure 3.5 – Code de Miller.

La figure 3.6 donne l'allure des spectres en puissance des différents codes.

Le code Manchester, fréquemment utilisé, présente un spectre limité à 1,5 f_0 (f_0 étant la fréquence du signal d'horloge). Le code de Miller, plus complexe à mettre en œuvre, possède un spectre plus étroit et est adapté à des transmissions sur des supports dont la bande passante est limitée.

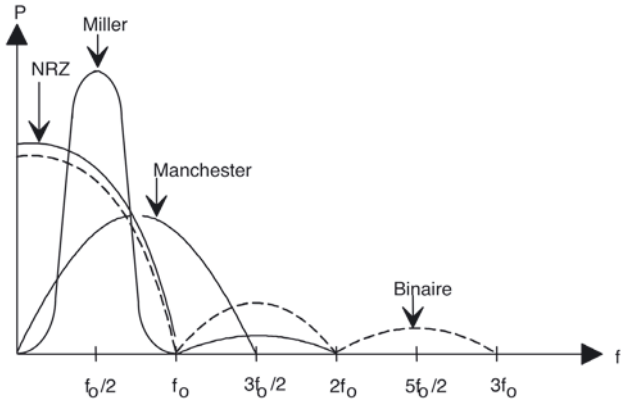


Figure 3.6 – **Spectres en puissance des principaux codes.**

3.2 Modulation/démodulation

Différentes raisons rendent impossible la transmission en bande de base à des vitesses élevées et sur de grandes distances :

- pas de propagation pour les fréquences en dehors de la bande passante du support ;
- pertes et affaiblissements sur la ligne ;
- impossibilité de différencier plusieurs communications sur un même support ;
- bruit, diaphonie…

Pour les transmissions longues distances utilisant comme support le réseau téléphonique commuté dont la bande passante est initialement comprise entre 300 Hz et 3 400 Hz, les débits sont limités à environ 20 kbit/s. Des débits plus importants peuvent être obtenus avec l'ADSL mais sur des fréquences plus élevées (voir paragraphe 3.4).

Toutes ces raisons imposent la transformation des données numériques à transmettre en un signal analogique modulant une onde porteuse, signal adapté au support de transmission. Les opérations de modulation en émission et de démodulation en réception sont réalisées par l'ETCD couramment appelé **modem** (**mod**ulateur-**dém**odulateur).

Les trois principaux types de modulation utilisés dans les transmissions sont les modulations par saut de fréquence, par saut de phase et par saut d'amplitude. Les plus efficaces, en termes de débit et de fiabilité sont les modulations qui combinent les sauts de phase et d'amplitude.

On retrouve par ailleurs ces modulations sur les transmissions sans fil (voir chapitre 5) qui sont par définition des transmissions par porteuse.

3.2.1 Modulation par saut de fréquence (FSK, *Frequency Shift Keying*)

Une porteuse sinusoïdale dont la fréquence F_0 est modulée par deux valeurs opposées de fréquences ($+f_1$ et $-f_1$) permet la représentation des deux niveaux logiques. Pour permettre une liaison *full duplex* sur un même support physique, on utilise la technique du partage de bande : une voie correspondant à une bande de fréquence ($F_0 - f_1$; $F_0 + f_1$) servira à l'émission, une autre voie correspondant à une autre bande ($F_0' - f_2$; $F_0' + f_2$) servira à la réception. La figure 3.7 décrit la modulation FSK *full duplex* correspondant à la recommandation UIT-T V21.

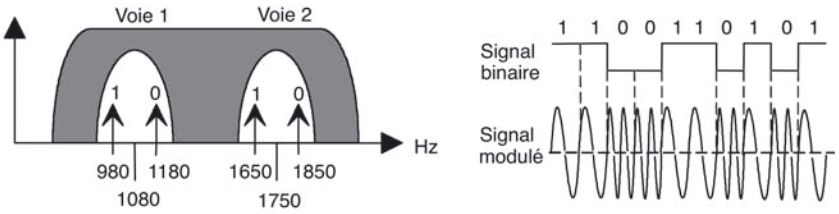


Figure 3.7 – Exemple de modulation FSK.

3.2.2 Modulation par saut de phase (PSK, *Phase Shift Keying*)

La modulation par saut de phase ou PSK associe à un code binaire une valeur de la phase ϕ de la porteuse sinusoïdale $V\sin(\omega t + \phi)$. En utilisant des codes binaires de 2, 3 bits ou plus, on peut ainsi augmenter la vitesse de transmission sans augmenter la fréquence de modulation.

La modulation PSK permet ainsi d'obtenir des vitesses de transmission plus élevées que la modulation FSK avec les mêmes limitations en bande passante du support de transmission.

De plus, dans ce type de modulation, le saut de phase peut ne pas avoir une valeur constante et dépendre de l'état de phase précédent. Il s'agit alors d'une modulation différentielle (DPSK, *Differential Phase Shift Keying*).

La figure 3.8 décrit la modulation DQPSK (*Differential Quadrature Phase Shift Keying*) utilisée dans un modem V22. Chaque état de phase est codé sur 2 bits. La fréquence de la porteuse est de 1 200 Hz ou 2 400 Hz suivant la voie utilisée.

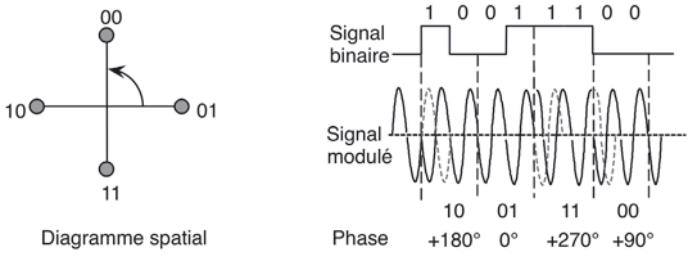


Figure 3.8 – Exemple de modulation DQPSK.

3.2.3 Modulation par saut de phase et d'amplitude (PSK + AM)

Pour obtenir des vitesses de transmission encore plus élevées dans une modulation de type PSK, il est nécessaire de multiplier le nombre d'états de phase (couramment 4, 8, 16 états ou plus). Les différences de phase entre états vont être réduites (les points correspondants du diagramme spatial vont être d'autant rapprochés), ce qui augmentera l'influence relative du bruit sur la transmission.

En combinant une modulation de phase à une modulation d'amplitude, on obtient une meilleure répartition des points sur le diagramme spatial et donc une meilleure immunité au bruit.

La figure 3.9 décrit la modulation mise en œuvre dans un modem V.29 utilisé à 7 200 bit/s. Dans cet exemple, chacun des huit états de phase est codé sur 3 bits ; deux valeurs d'amplitude (valeurs relatives 3 et $\sqrt{2}$) sont utilisées. La fréquence de la porteuse est de 1 700 Hz.

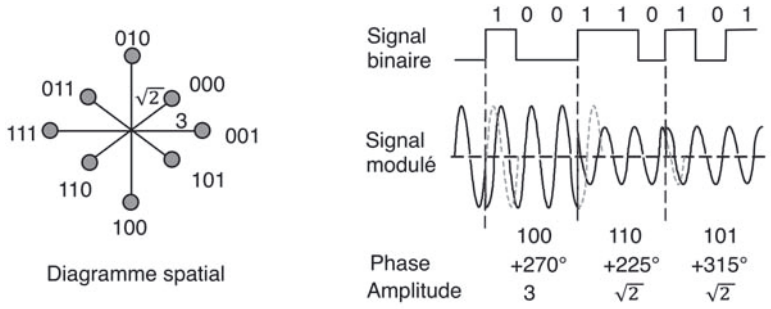


Figure 3.9 – **Exemple de modulation de phase et d'amplitude.**

La modulation en amplitude avec porteuse en quadrature est un cas particulier. Ce type de modulation, encore appelé **QAM** (*Quadrature Amplitude Modulation*) ou MAQ (Modulation d'Amplitude en Quadrature), permet de coder jusqu'à 4 bits par état de phase mais est fortement dépendant de la qualité des lignes utilisées.

La figure 3.10 décrit une modulation QAM 16. Pour chacun des groupes de 4 bits, les deux bits de poids faibles sont codés de façon différentielle en fonction de la combinaison précédente.

Les modems rapides utilisent une autre variante, la modulation codée en treillis **TCM** (*Trellis Coded Modulation*). Chaque groupe de bit est également codé en fonction des états antérieurs suivant un algorithme complexe intégrant une correction d'erreurs.

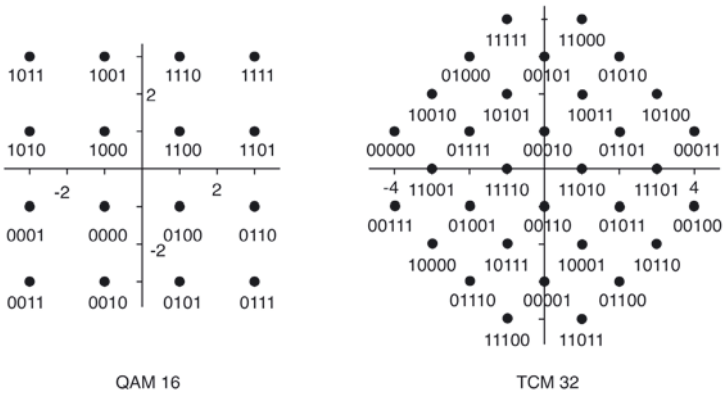


Figure 3.10 – **Exemple de codages QAM et TCM.**

3.2.4 Débit binaire, vitesse de modulation et valence

La vitesse de transmission ou **débit binaire Db** exprimée en bit/s correspond au nombre de bits transmis en une seconde.

La **vitesse de modulation** ou débit de symbole **Ds** exprimée en bauds correspond au nombre d'intervalles de modulation ou de symboles par seconde (on appelle intervalle de modulation la durée d'un état de la modulation).

Si l'intervalle de modulation correspond à la durée d'un bit, alors les deux unités sont équivalentes (cas de la modulation FSK). Si plusieurs bits sont codés sur un intervalle de modulation, les unités ne sont pas équivalentes (cas des modulations PSK, QAM et TCM ; si 2 bits sont codés par état de phase, la vitesse de transmission sera par exemple de 1 200 bit/s pour une vitesse de modulation de 600 bauds). Pour la transmission en bande de base, les unités sont équivalentes.

Le nombre d'états ou de symboles est appelé **valence M** de la modulation. La modulation QAM16, par exemple, est caractérisée par une valence de 16.

Débit binaire et débit de symbole sont liés par la relation :

$$Db = \log_2(M) \times Ds$$

On vérifie par exemple qu'avec 4 symboles et 2 bits par symbole, le débit binaire est le double du débit de symbole :

$$Db = \log_2(4) \times Ds = 2\ Ds$$

3.3 Caractéristiques d'une voie de transmission

3.3.1 Capacité

Les grandeurs caractéristiques d'une voie de transmission sont liées par un certain nombre de relations dérivées de la loi de Shannon.

Une voie de transmission ayant une largeur de bande de B Hz ne peut transmettre des signaux dont la vitesse de modulation est supérieure à $2B$ bauds.

Ainsi, le réseau téléphonique dont la largeur de bande est de 3 100 Hz (300 à 3 400 Hz) permet théoriquement des vitesses de modulation maximales de 6 200 bauds.

Le débit binaire maximum ou **capacité** C d'une ligne de transmission peut être défini suivant les caractéristiques de la ligne par la relation :

$$C = B\log_2\left(1 + \frac{S}{N}\right)$$

S/N étant le rapport signal/bruit en puissance du signal, généralement exprimé sous la forme $10 \log_{10} S/N$ en décibel (dB).

En reprenant l'exemple du réseau téléphonique et pour un rapport signal/bruit typique de 1 000 (30 dB), on obtient une capacité maximale de l'ordre de 31 000 bit/s. Cette valeur théorique est rarement atteinte à cause des diverses imperfections de la voie (le débit moyen sur un modem V90 est souvent inférieur à 28 800 bit/s).

3.3.2 Temps de propagation et temps de transmission

Le temps de propagation T_p est le temps nécessaire à un signal pour parcourir un support d'un point à un autre, ce temps dépend donc de la nature du support, de la distance et également de la fréquence du signal.

Pour une transmission radioélectrique par satellite, ce temps est calculé à partir de la vitesse de propagation qui est égale à celle de la lumière, soit 300 000 km/s. Sur le réseau téléphonique utilisant des paires métalliques, ce temps de propagation peut être compris entre 10 et 40 µs par kilomètre. Pour des liaisons locales à grand débit sur paire torsadée, telles que celles mises en œuvre sur le réseau Ethernet, le temps de propagation est estimé à environ 4 µs/km.

Le temps de transmission T_t est le délai qui s'écoule entre le début et la fin de la transmission d'un message sur une ligne, ce temps est donc égal au rapport entre la longueur du message et le débit de la ligne.

Le temps de traversée ou **délai d'acheminement** sur une voie est égal au temps total mis par un message pour parvenir d'un point à un autre, c'est donc la somme des temps T_p et T_t.

Pour évaluer l'importance relative du temps de propagation T_p, il est nécessaire de comparer celui-ci au temps de transmission T_t du message sur la ligne.

Ainsi pour un message de 100 bits transmis à 2 400 bit/s sur une paire torsadée d'une longueur de 100 km avec un temps de propagation de 10 µs/km, on obtient :

$$T_t = 100/2\,400 = 42 \text{ ms}$$

$$T_p = 10 \times 100 = 1\,000 \text{ µs} = 1 \text{ ms}$$

Pour un message de 10 000 bits sur un réseau Ethernet à 100 Mbit/s et sur une distance de 100 m, on obtient :

$$T_t = 10\,000/100\,000\,000 = 100\ \mu s$$

$$T_p = 4 \times 0{,}1 = 0{,}4\ \mu s$$

Dans la plupart des cas, le temps de propagation pourra donc être négligé devant le temps de transmission.

3.3.3 Partage d'une ligne (multiplexages)

Lorsque plusieurs liaisons de données sont nécessaires entre deux sites, il est généralement plus économique d'utiliser une seule ligne partagée sur laquelle seront transmis les messages des différents équipements plutôt que de réaliser autant de liaisons point à point (figure 3.11).

Le partage peut être réalisé suivant deux types d'allocation :

- l'**allocation statique** lorsqu'une fraction de la capacité de transmission de la ligne est mise de façon permanente à la disposition de chaque voie ou canal de transmission ;
- l'**allocation dynamique** lorsque les durées d'allocation sont variables suivant le trafic de chaque voie.

Le partage statique met en œuvre des équipements de type multiplexeur. Le multiplexage peut être fréquentiel, temporel ou statistique.

Le partage dynamique peut être réalisé à partir d'équipements spécialisés de type concentrateurs pour des liaisons point à point (pour des liaisons multipoints, les caractéristiques de ce mode de partage sont décrites dans les chapitres suivants). Le concentrateur intègre de plus une logique programmée permettant la gestion des protocoles de communication de niveaux supérieurs.

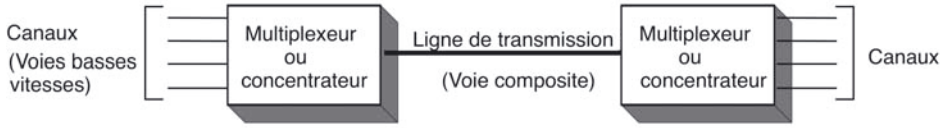


Figure 3.11 – Partage avec multiplexage ou concentration.

a) Multiplexage fréquentiel

Le multiplexage en fréquence, encore nommé **MRF** (Multiplexage par Répartition en Fréquence) ou **FDM** (*Frequency Division Multiplexing*), consiste à diviser la bande passante de la ligne en sous-bandes ou canaux à l'aide de filtres passe-bande, chaque circuit de données correspond alors à un canal (figure 3.12).

La modulation associée permet de positionner chaque canal dans la bande passante de la ligne. En pratique, pour limiter les interférences, une bande de garde est nécessaire entre chaque bande de fréquence des différents canaux.

Ce type de multiplexage est généralement utilisé pour la transmission de signaux analogiques par câble, par voie hertzienne ou par satellite dans des applications de type téléphonique, radiodiffusion et télévision.

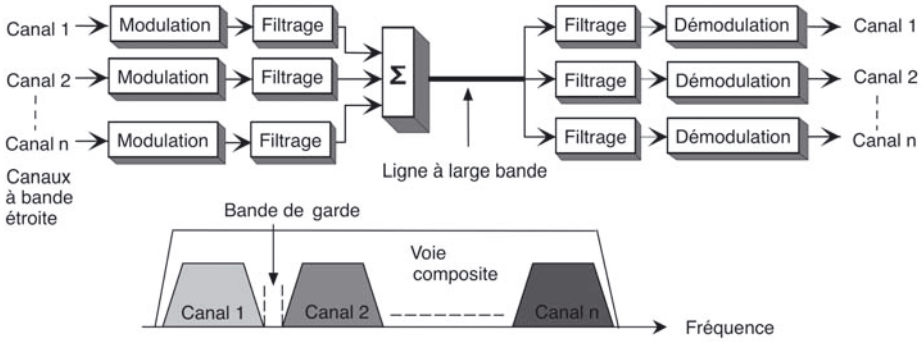


Figure 3.12 – Principe du multiplexage en fréquence.

À l'origine, le réseau téléphonique fonctionnait sur ce modèle : un certain nombre de voies multiplexées sur un support de transmission à large bande. Ces circuits large bande appelés circuits MRF (Multiplex à Répartition de Fréquence) correspondent à des liaisons interurbaines ou longue distance (tableau 3.1).

Une structure hiérarchique est ainsi définie suivant les distances et le nombre de voies regroupées :

- les groupes primaires rassemblent douze canaux (douze lignes d'abonnés) de 4 kHz dans la bande 60-108 kHz ;
- les groupes secondaires rassemblent cinq groupes primaires dans la bande 312-552 kHz…

Tableau 3.1 – Multiplexage hiérarchique du RTC.

Groupes	Nbre de voies (nbre de groupes)	Bande passante
Groupe primaire	12	60-108 kHz = 48 kHz
Groupe secondaire	60 (12 × 5)	312-552 kHz = 240 kHz
Groupe tertiaire	300 (60 × 5)	812-2 044 kHz = 1 232 kHz
Groupe quaternaire	900 (300 × 3)	8 516-12 338 kHz = 3 872 kHz

b) Multiplexage temporel

Dans un multiplexage temporel, encore nommé **MRT** (Multiplexage à Répartition dans le Temps) ou TDM (*Time Division Multiplexing*), l'allocation complète de la ligne aux différentes voies est effectuée périodiquement et pendant des intervalles de temps constants. Ce type de multiplexage est réservé aux signaux numériques. Les éléments des messages de chaque voie sont mémorisés sous forme de bits ou d'octets dans des mémoires tampon, puis transmis séquentiellement sur la voie composite. Les éléments sont ainsi assemblés pour former des trames multiplexées (figure 3.13).

La vitesse de transmission des voies bas débit (d) est fonction de la vitesse de transmission de la ligne (D) et du nombre de voies n. La période T des trames est fonction du nombre de voies et de l'intervalle de temps élémentaire IT (*slot time*).

$$d = \frac{D}{n} \qquad T = n \times IT$$

Ce type de multiplexage est particulièrement adapté aux transmissions asynchrones dans la mesure où les deux extrémités basse vitesse ne sont pas synchronisées.

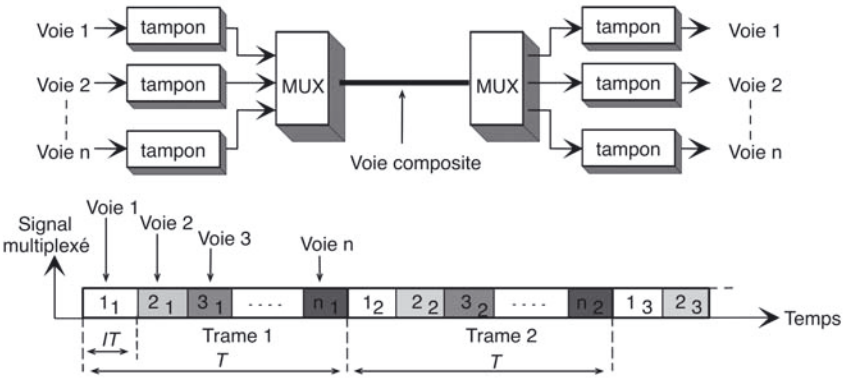


Figure 3.13 – Principe du multiplexage temporel.

- *Multiplexage MIC*

Le multiplexage temporel est également utilisé pour la transmission de la voix sur liaison téléphonique. Ce système de multiplexage est appelé **MIC** (Modulation par Impulsions Codées) ou **PCM** (*Pulse Code Modulation*) et comporte trois fonctions principales (figure 3.14) :

- l'échantillonnage des signaux analogiques de chacune des voies ;
- le multiplexage temporel des échantillons des différentes voies ;
- la quantification et le codage des échantillons multiplexés pour obtenir un signal numérique.

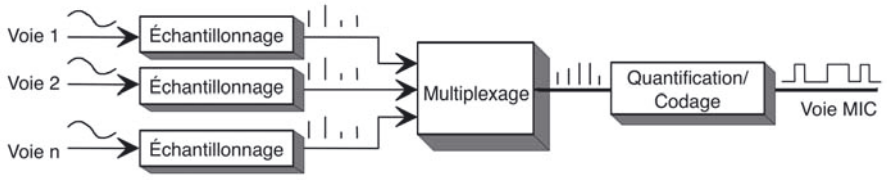


Figure 3.14 – **Principe de la transmission MIC.**

L'ensemble du dispositif qui effectue la conversion numérique-analogique sur la ligne est appelé CODEC (COdeur DECodeur).

La figure 3.15 décrit le principe d'un codage sur 4 bits des échantillons d'une des voies, le codage est en fait réalisé sur une seule ligne après multiplexage des voies.

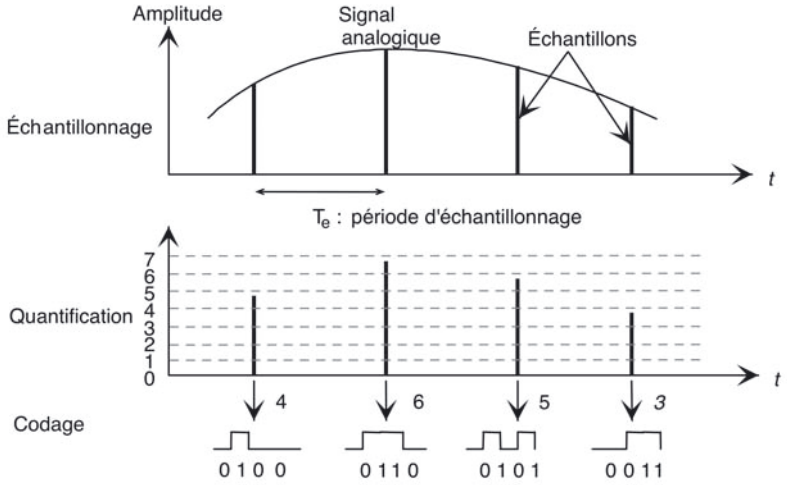


Figure 3.15 – **Codage du signal analogique.**

La figure 3.16 décrit le principe du multiplexage des échantillons qui sont ensuite codés pour former un ensemble de trames multiplexées.

La transmission MIC de base est définie pour un ensemble de trente voies (plus deux voies de synchronisation et de signalisation). L'échantillonnage est réalisé avec une fréquence de 8 kHz (période de 125 µs). Les échantillons multiplexés dans le temps sont codés sur 8 bits (7 bits aux États-Unis).

Le débit d'une voie est de 64 kbit/s (56 kbit/s aux États-Unis), ce qui correspond à un débit effectif sur la ligne de 2 048 kbit/s (32 voies).

Ces valeurs sont justifiées, d'une part, par la possibilité de convertir sans perte notable de qualité le signal analogique en signal numérique à 64 kbit/s et, d'autre part, par le fait qu'il est possible de transmettre des données binaires avec des débits de l'ordre de 2 Mbit/s sur une voie numérique longue distance. Le passage au numérique

permet donc d'acheminer simultanément par multiplexage temporel une trentaine de communications téléphoniques sur une seule ligne.

Le RTC fonctionne en grande partie sur ce modèle. Dans la mesure où la liaison à l'abonné (la boucle locale) reste encore très souvent analogique, la conversion en numérique et le multiplexage auront lieu au niveau du centre local de rattachement (CL ou CAA).

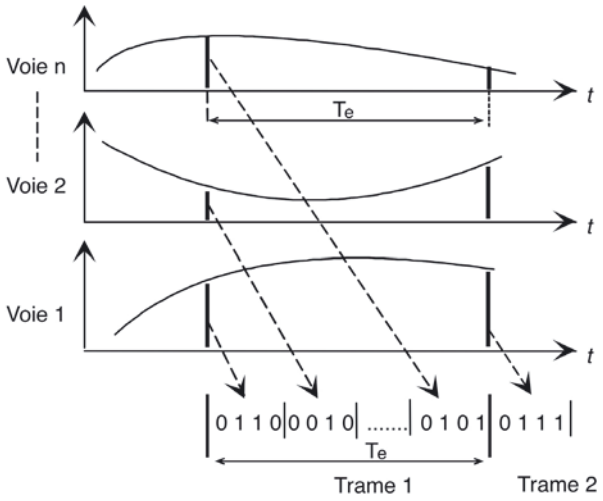


Figure 3.16 – Multiplexage temporel des échantillons.

c) Multiplexage temporel statistique

Dans un multiplexage temporel simple, les tranches de temps fixes allouées aux différentes voies ne sont pas toujours utilisées. Dans ce cas, des bits ou des caractères de remplissage sont insérés.

Le multiplexage temporel statistique ou asynchrone (ATDM : *Asynchronous Time Division Multiplexing*) consiste à allouer dynamiquement des tranches de temps aux seules voies qui ont des données à transmettre à un instant donné.

Le multiplexeur a donc pour rôle de détecter les tampons non vides, de prélever les données mémorisées, de supprimer les bits non significatifs dans le cas d'une transmission asynchrone (start, stop, parité), de comprimer éventuellement les données et de les insérer dans les trames de la voie composite (figure 3.17).

Ce type de multiplexage permet de raccorder plusieurs équipements sur une seule ligne, même si le débit cumulé de chaque voie est supérieur au débit maximum de la ligne (cas des terminaux de saisie par exemple).

De plus, le multiplexeur qui intègre un microprocesseur et des mémoires tampon permet des débits et des paramètres de transmission différents sur chaque voie ou sous-canal et à chaque extrémité. Généralement, les équipements raccordés sont de type asynchrone et la transmission sur la voie composite est synchrone.

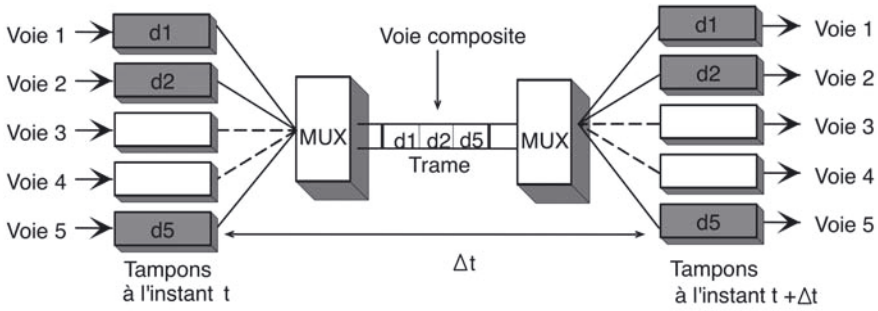


Figure 3.17 – Principe du multiplexage statistique.

Les multiplexeurs statistiques, du fait du caractère dynamique de la répartition temporelle entre les différentes voies, sont souvent confondus avec les concentrateurs.

3.3.4 Multiplexage par porteuses orthogonales (OFDM)

a) Principe

L'OFDM (*Orthogonal Frequency Division Multiplexing*) est une technique de multiplexage par répartition en fréquences orthogonales. Le principe consiste à répartir sur un grand nombre de sous-porteuses à différentes fréquences le signal numérique que l'on veut transmettre.

Pour que le signal modulé ait une grande efficacité spectrale (optimisation de la bande allouée), il faut que les fréquences des sous-porteuses soient les plus proches possibles, tout en garantissant que le récepteur soit capable de les séparer et de retrouver le symbole numérique émis sur chacune d'entre elles. Ceci est vérifié avec des sous-porteuses orthogonales : les spectres des différentes sous-porteuses se chevauchent mais, grâce à l'orthogonalité, les signaux n'interfèrent pas entre eux.

Précisons qu'avec un codage orthogonal, l'espacement entre chaque sous-porteuse doit être égal à $\Delta f = k/(T_U)$, où T_U est la durée utile d'un symbole (correspondant à la taille de la fenêtre de capture du récepteur), et k est un entier positif, généralement égal à 1. Par conséquent, avec n sous-porteuses, la largeur totale de la bande passante sera de $B \approx n \cdot \Delta f$ (figure 3.18).

Chaque sous-porteuse est ensuite modulée indépendamment en utilisant des modulations classiques : QPSK, QAM-16, QAM-64… Pour améliorer la fiabilité, le signal à transmettre peut également être répété sur plusieurs sous-porteuses.

L'OFDM limite donc les interférences intersymboles et est particulièrement bien adapté aux transmissions mobiles à haut débit et longues distances rencontrées notamment dans :

- la radiodiffusion pour la télévision numérique terrestre (DVB-T, DVB-H) et la radio numérique terrestre régionale DAB et mondiale DR.M ;

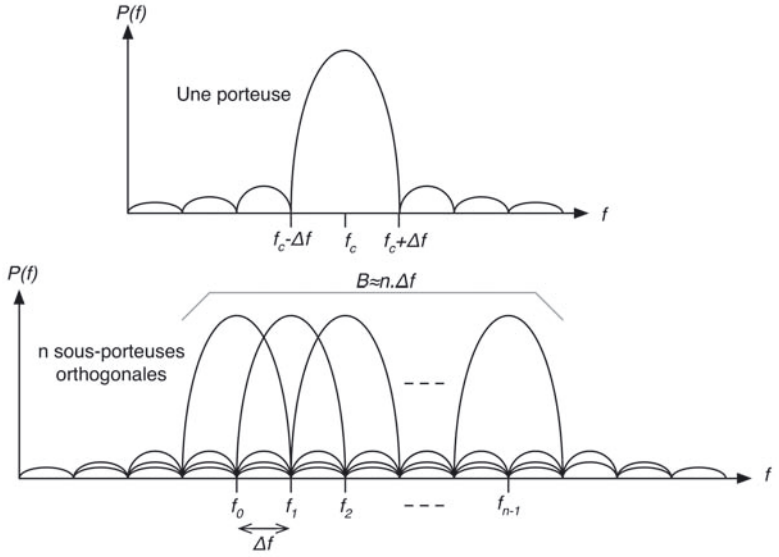


Figure 3.18 – Exemple de sous-porteuses orthogonales.

- les réseaux sans fil basé sur les normes IEEE 802.11a, 802.11g (WiFi) et 802.16 (WiMAX) ;
- les réseaux mobiles de nouvelle génération (4G) ;
- les liaisons filaires : ADSL, VDSL, modem sur courant porteur (CPL), modem câble (Docsis).

b) Exemple simple de multiplexage OFDM

Soit le signal binaire à transmettre : 1100 1110 1000 0100 0110 0011…

Le signal est multiplexé sur quatre sous-porteuses orthogonales (tableau 3.2).

Tableau 3.2 – Exemple de multiplexage sur sous-porteuses OFDM.

f_1	f_2	f_3	f_4
1	1	0	0
1	1	1	0
1	0	0	0
0	1	0	0
0	1	1	0
0	0	1	1

Chaque sous-porteuse doit transmettre sa propre séquence. Le signal de sous-porteuse f_1 sera ainsi modulé par la séquence 111000. Dans la figure 3.19, le signal est modulé avec une modulation simple BPSK. Le signal de sous-porteuse f_2, qui est

la fréquence orthogonale suivante, sera modulé par la séquence 110110. Les signaux de porteuse f_3 et f_4 seront modulés par les séquences respectives 010011 et 000001.

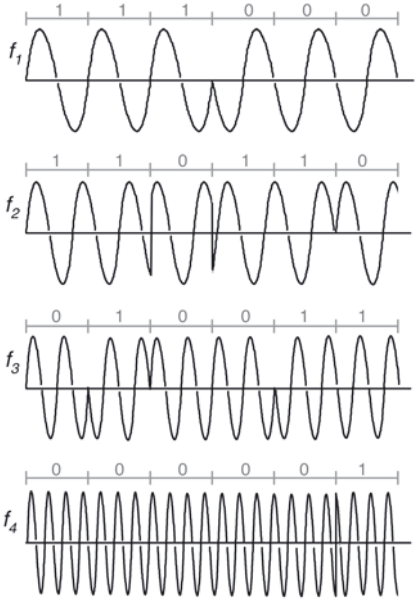


Figure 3.19 – **Sous-porteuses modulées en BPSK.**

Les bits successifs du signal binaire à transmettre sont donc multiplexés dans le temps pour moduler les différentes sous-porteuses orthogonales qui seront transmises simultanément (figure 3.20). Dans cet exemple simple, un bit seulement est transmis par état de phase pour chaque sous-porteuse grâce à une modulation BPSK. Dans la réalité, les modulations utilisées en OFDM sont beaucoup plus performantes (8PSK, QAM 16…).

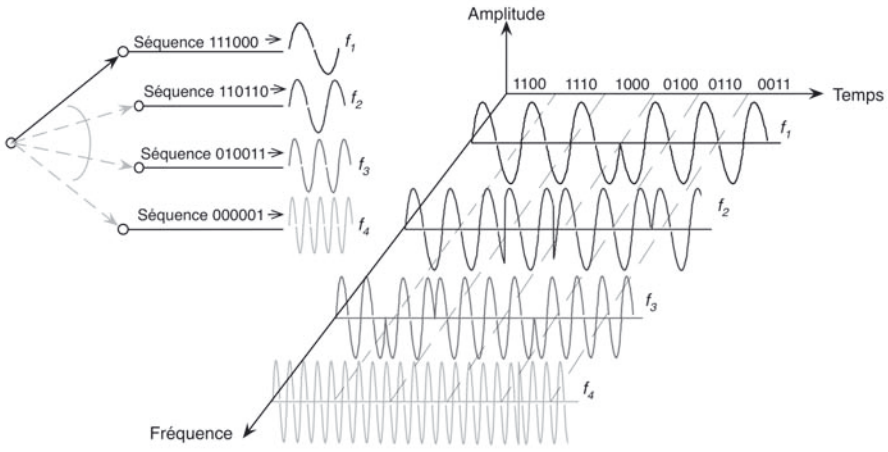


Figure 3.20 – **Multiplexage dans le temps du signal binaire.**

3.4 Transmission ADSL

3.4.1 Principe

La capacité des lignes téléphoniques en paires torsadées cuivre est limitée, d'une part, par la bande passante et, d'autre part, par l'atténuation du signal, proportionnelle à la longueur et à la section du câble. La distance critique à prendre en compte est celle qui sépare l'abonné de son commutateur local ou plus communément appelé répartiteur. Les relais du RTC au-delà du répartiteur sont reliés à l'heure actuelle, pour l'ADSL au moins, par de la fibre optique permettant des débits de plusieurs gigabits par seconde (Gbit/s). Pour des distances limitées à quelques kilomètres, en travaillant sur des fréquences plus élevées et en améliorant le rapport signal/bruit, il est possible de dépasser les débits de quelques dizaines de kbit/s obtenus avec les modulations étudiées section 3.2.

La technique utilisée dans l'*Asymetric Digital Subscriber Line*, permet d'atteindre des débits de plusieurs Mbit/s sur des distances inférieures à 5 km. Pour connaître les performances potentielles de la ligne ADSL, l'atténuation peut être mesurée par des équipements placés à chaque bout de la ligne. L'affaiblissement est l'atténuation totale de la ligne. D'après les principaux opérateurs, une ligne affichant un affaiblissement théorique de moins de 35 dB est considérée comme bonne et devrait permettre un débit ADSL de plus de 8 Mbit/s. En dessous de 20 dB, les lignes peuvent être considérées comme excellentes, le débit peut atteindre 20 Mbit/s. La limite actuelle pour avoir l'ADSL est de 70 dB.

L'ADSL est donc une solution permettant aux abonnés du RTC d'accéder, par l'intermédiaire d'un fournisseur d'accès, à Internet à des débits élevés. Un filtre permet si besoin d'assurer une communication téléphonique simultanément aux transferts de données (figure 3.21). Le filtre n'est plus nécessaire si l'abonné utilise la téléphonie sur IP (voir chapitre 8) et donc la même bande de fréquence que pour les données. Au-delà du répartiteur, le DSLAM (*Digital Subscriber Line Acces Multiplexer*) est un multiplexeur qui regroupe le trafic des différentes lignes d'abonnés qui lui sont raccordées et le redirige vers le réseau de l'opérateur ou du fournisseur d'accès selon le principe du multiplexage temporel où les données sont transportées en IP ou en ATM. Géographiquement, le DSLAM se situe à la terminaison de la boucle locale, après le répartiteur. Plus précisément, le NRA (Nœud de Raccordement d'Abonné) vers lequel aboutissent les lignes téléphoniques des abonnés comprend deux parties :

- une salle dédiée au répartiteur ;
- une salle de dégroupage ou salle de co-localisation dans laquelle le FAI installe et gère le DSLAM.

Le fonctionnement d'ATM qui sert souvent de réseau de collecte pour les liens ADSL multiplexés est décrit en section 7.4.

Même si l'ADSL peut être considéré comme une étape dans la numérisation complète du réseau téléphonique, les améliorations successives des techniques de modulation et donc des débits permettent de retarder le remplacement de millions de

lignes téléphoniques d'abonnés (le coût de ce remplacement est estimé par certains experts à 1 000 € par abonné). L'ADSL est donc une technologie encore très primée par les différents opérateurs de télécommunication.

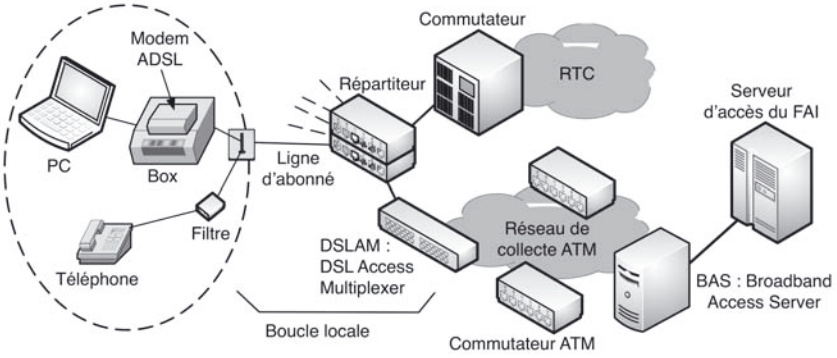


Figure 3.21 – **Équipements d'une connexion d'ADSL.**

3.4.2 La modulation

Compte tenu des objectifs, les débits dans le sens abonné vers réseau (flux montant ou *upstream*) sont moins élevés que dans le sens réseau vers abonné (flux descendant ou *downstream*). Les valeurs typiques de débit pour l'ADSL de base sont de 640 kbit/s pour le flux montant et de 500 kbit/s à 8 Mbit/s pour le flux descendant (figure 3.22).

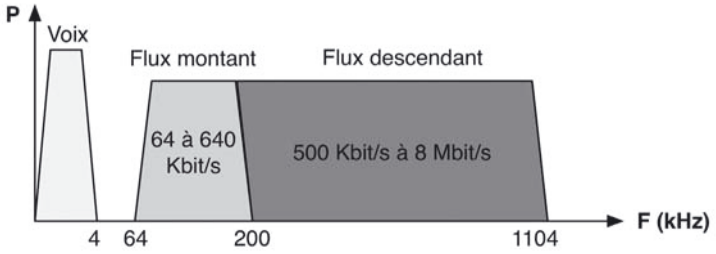


Figure 3.22 – **Utilisation de la bande passante du support.**

Pour obtenir de tels débits, la bande des fréquences utilisées sur les paires téléphoniques va de 0 Hz à 1,1 MHz (pour des lignes supportant de telles fréquences sur des distances courtes). La bande de 0 Hz à 4 kHz reste réservée aux communications de type voix analogique. La bande de 64 kHz à 1,1 MHz est utilisée pour la transmission des données en deux bandes distinctes, une pour chaque flux.

Cette bande de fréquence est divisée en canaux de 4 kHz (auxquels s'ajoutent des canaux de contrôle). Chaque canal utilise une modulation de type QAM avec une vitesse de modulation de 4 kbauds. Les données sont codées à l'aide d'une technique de codage par porteuses multiples DMT (*Discrete MultiTone*) (figure 3.23). Cette

technique de codage DMT utilise des porteuses orthogonales et donc un multiplexage de type OFDM (*Orthogonal Frequency Division Multiplexing*). Ce dernier est décrit dans la section 3.3.4.

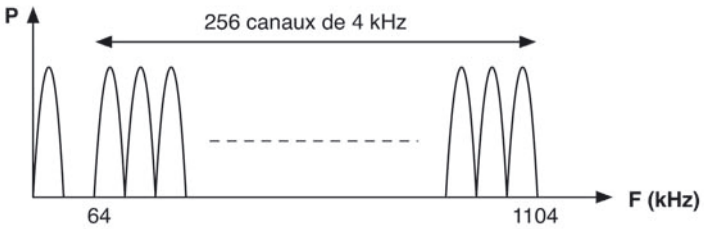


Figure 3.23 – Codage par porteuses multiples (*Discrete MultiTone*).

Cette solution revient à disposer de 256 modems synchronisés entre eux, se répartissant la transmission des données, comme l'illustre la figure 3.24.

Débit total = (nbre de canaux) × (nbre de bits/intervalle de modulation) × (vitesse de modulation)

Avec un maximum de 8 bits de données par intervalle de modulation, le débit total théorique atteint 8 Mbit/s, mais pour atteindre un tel débit, les canaux doivent être exploités au mieux :

- chaque canal sera exploité avec une constellation adaptée au bruit rencontré sur le canal (certains canaux pourront fournir un débit important, tandis que d'autres en fourniront très peu, voire pas du tout). Cette méthode flexible permet d'exploiter au mieux la ligne même dans un milieu hostile ;
- une répartition spatiale des données sera effectuée sur l'ensemble des canaux concernés (le flux de données sera découpé en tranche, chaque tranche étant acheminée par un canal différent).

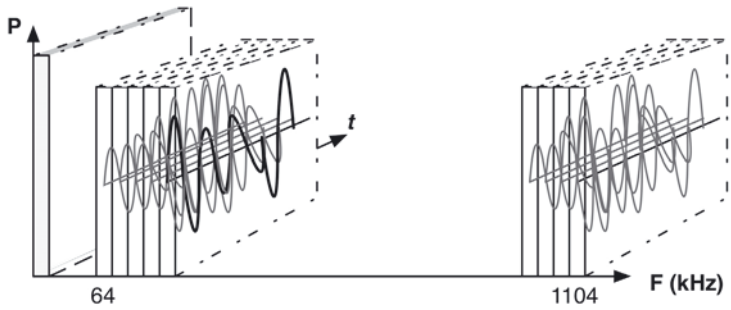


Figure 3.24 – Représentation de la modulation sur les canaux de données.

3.4.3 ADSL2+ et les évolutions

Si dans sa première version l'ADSL est limité à 8 Mbit/s en flux descendant pour des distances maximales de 5 km, l'ADSL2+ permet d'atteindre 20 Mbit/s pour des distances maximales de 2 km. Ce gain est obtenu essentiellement en utilisant une bande de fréquences allouées jusqu'à 2,2 MHz avec les mêmes techniques de modulation. Comme pour la version précédente, l'affaiblissement du signal est proportionnel à la distance parcourue depuis l'équipement de raccordement, le DSLAM : *DSL Access Multiplexer* (figure 3.25). De plus, cette évolution impose une mise à jour des équipements, notamment un modem compatible à la norme, et la mise à niveau des DSLAM.

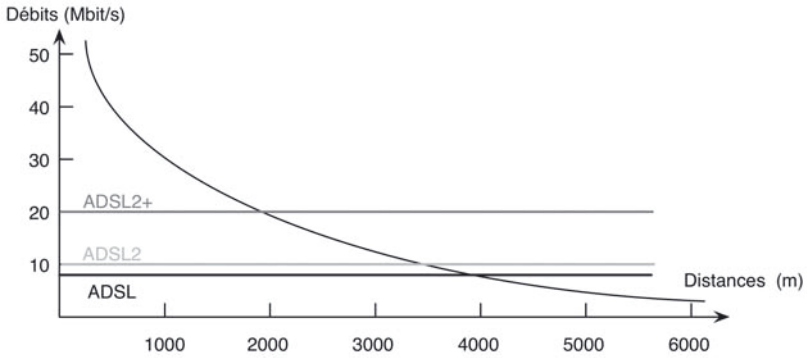


Figure 3.25 – Débit théorique sur une paire torsadée en fonction de la longueur.

ADSL reste un moyen technologiquement très sophistiqué, pour exploiter au mieux une installation existante, inadaptée au départ à la transmission haut débit. Dans l'avenir, pour continuer à utiliser des technologies xDSL, il faudra reconstruire toute l'architecture de la boucle locale pour assurer autant de services que ce que peut déjà assurer le câble TV par exemple.

Ainsi, en utilisant une bande de fréquence encore plus large et plus haute, le VDSL (*Very high bit-rate DSL*) permettra d'atteindre un débit de 52 Mbit/s en réception et de 12 Mbit/s en émission. La déclinaison VDSL2 permettra théoriquement de doubler ces débits et ouvrira l'accès à des applications requérant une bande passante conséquente : la vidéo de haute qualité en premier lieu (HDTV et vidéo à la demande), mais aussi les services interactifs ou la transmission de données à grande échelle.

Cette technologie peut constituer le raccord entre un réseau de fibre optique et l'équipement terminal d'un foyer ou d'un bureau qui pourront continuer à utiliser leur ligne téléphonique à fil de cuivre. La contrepartie est la faible portée (la distance entre le réseau à haut débit et le terminal de l'utilisateur) qui est limitée à 300 mètres en configuration de flux descendant maximal. Une contrainte qui restreint considérablement le nombre d'abonnés pouvant être raccordés directement *via* le réseau de distribution. Son utilisation est donc réservée aux internautes dont le domicile est proche d'un des 12 000 centraux téléphoniques de Orange (moins d'un foyer sur deux).

La solution proposée par Orange est de rapprocher les abonnées en installant les DSLAM (multiplexeurs d'accès) nécessaires au VDSL dans les sous-répartiteurs proches des habitations.

Mais les problèmes sont nombreux :

- il y a environ 120 000 sous-répartiteurs ;
- le VDSL dans les sous-répartiteurs perturbe l'ADSL existant ;
- il n'y a pas de place pour les équipements concurrents…

3.5 Transmission sur fibre optique

Compte tenu de ses performances et de son coût de déploiement en diminution constante, la fibre optique est de plus en plus utilisée dans les réseaux de télécommunications. Elle est présente depuis de nombreuses années dans le réseau cœur, pour interconnecter les routeurs sur des liaisons longue distance. Elle est par ailleurs de plus en plus déployée sur le réseau d'accès de l'utilisateur comme solution de remplacement de l'ADSL, dans les zones suffisamment peuplées pour que le déploiement soit rentable.

D'un point de vue physique, une fibre optique est constituée d'une fibre de verre très fine (le cœur) entourée d'une gaine protectrice (figure 3.26).

Du côté du système émetteur, un transpondeur optique est chargé de convertir les impulsions électriques générées par le système informatique en signaux optiques. Ce transpondeur intègre donc un émetteur optique du type LED (*Light Emitting Diode*) ou laser suivant la puissance et la longueur d'onde utilisées.

Le cœur de la fibre ayant un indice de réfraction légèrement plus élevé que celui de la gaine, la lumière est réfléchie à l'interface entre les deux matériaux et l'information lumineuse peut ainsi être propagée par des réflexions successives sur des longueurs importantes et avec très peu de pertes. Sur de très longues distances, par exemple sur les câbles transocéaniques (plusieurs milliers de km), des amplificateurs sont néanmoins nécessaires pour régénérer le signal optique.

Pour pouvoir transmettre des données binaires, le signal généré par l'émetteur est codé par une variation d'intensité lumineuse permettant, grâce à un codage en bande de base, de transmettre une grande quantité d'informations par unité de temps.

À l'autre bout de la chaîne de transmission, les récepteurs sont généralement des photodiodes qui réalisent l'opération inverse.

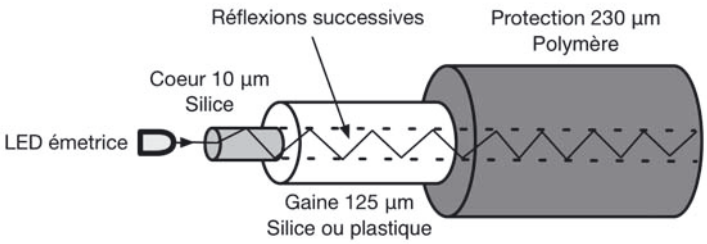


Figure 3.26 – Principe de la transmission sur fibre.

Deux types de fibres sont aujourd'hui utilisés. Les fibres multimodes capables de transporter plusieurs signaux lumineux présentent un diamètre de fibre plus important (de l'ordre 50 µm) et une dispersion modale plus importante. Elles sont donc réservées à des transmissions à plus faible débit et faible distance (moins de 10 Gbit/s sur quelques km). Les fibres monomodes utilisent des fibres plus fines (moins de 10 µm) et présentent donc moins de pertes dues aux réflexions. Elles sont utilisées sur des réseaux à haut débit et sur de très longues distances (de l'ordre de 100 Gbit/s sur une centaine de kilomètres), par exemple entre les grandes villes ou sur des liaisons intercontinentales par câbles sous-marins.

Enfin, pour optimiser le nombre de communication sur une même fibre, un multiplexage en longueur d'onde peut être utilisé (WDM - *Wavelenght Division Multiplexing*), chaque communication utilisant une longueur d'onde différente. Les systèmes WDM commercialisés aujourd'hui comportent jusqu'à 80 canaux optiques, ce qui permet d'atteindre une capacité de 800 Gbit/s avec un débit nominal de 10 Gbit/s. La technologie U-DWDM (Ultra-Dense WDM) offre une capacité de 4 000 Gbit/s (4 Tbit/s) avec 400 canaux optiques à 10 Gbit/s.

3.6 Transmission sans fil WiMAX

WiMAX (*Worldwide Interoperability for Microwave Access*) est un standard de transmission sans fil permettant, comme l'ADSL, de transporter des signaux numériques sur des distances de plusieurs kilomètres. L'objectif principal est de couvrir la zone dite du « dernier kilomètre », encore appelée boucle locale radio, particulièrement dans des endroits où l'abonné est situé trop loin de son équipement de raccordement, rendant l'ADSL inexploitable. Le WiMAX qui est souvent comparé à un « ADSL sans fil » permet donc de fournir un accès haut débit à l'Internet dans les zones non couvertes par les technologies filaires classiques ou encore permet de raccorder à l'Internet une zone équipée localement en ADSL (figure 3.27).

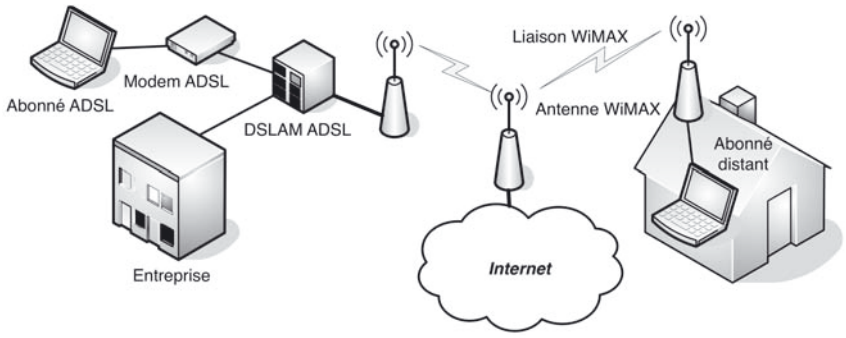


Figure 3.27 – Utilisation du WiMAX pour la connexion Internet.

Une autre exploitation possible est l'utilisation du WiMAX comme réseau d'interconnexion entre des réseaux locaux sans fil, utilisant par exemple le standard WiFi. Comme l'illustre la figure 3.28, le WiMAX permet, dans ce cas, de relier entre

elles différentes cellules (différents « hotspots ») afin de créer un réseau maillé (*mesh network*).

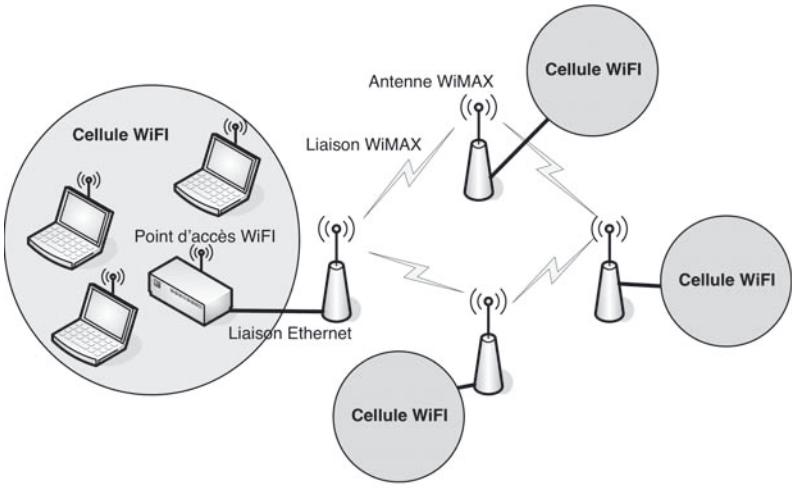


Figure 3.28 – Utilisation du WiMAX pour relier des réseaux WiFi.

Concernant la transmission radio, WiMAX est une norme basée sur le standard IEEE 802.16. Ce standard permet théoriquement d'émettre et de recevoir des données dans les bandes de fréquences radio de 2 à 66 GHz avec un débit maximum théorique de 70 Mbps sur une portée de 50 km. En pratique, WiMAX permet d'atteindre 12 Mbps sur une portée de 20 km.

Les révisions du standard IEEE 802.16 se déclinent en deux catégories :

- **WiMAX fixe**, également appelé IEEE 802.16-2004, est prévu pour un usage fixe avec une antenne montée sur un toit, à la manière d'une antenne TV. Le WiMAX fixe opère dans les bandes de fréquence 2,5 GHz et 3,5 GHz, pour lesquelles une licence d'exploitation est nécessaire, ainsi que la bande libre des 5,8 GHz ;
- **WiMAX mobile**, également baptisé IEEE 802.16e, prévoit la possibilité de connecter des clients mobiles au réseau Internet. Le WiMAX mobile ouvre ainsi la voie à la téléphonie mobile sur IP ou plus largement à des services mobiles haut débit.

Comme pour WiFi, la technologie WiMAX est organisée autour de la station de base, c'est-à-dire l'antenne centrale chargée de communiquer avec les antennes d'abonnés (*subscribers antennas*). On parle dans ce cas d'architecture Point-To-Multipoint (PMP) : 1 antenne émettrice, *n* antennes réceptrices.

Bien qu'il s'agisse de transmissions sans fil, les techniques de modulation et de codage sont très proches de celles utilisées pour l'ADSL : transposition en fréquence des données suivant un codage de type OFDM et modulation en phase et amplitude (QAM) des différents canaux.

Le **WiMAX2** qui correspond à la dernière norme IEEE 802.16m permet des débits théoriques descendants de plus de 300 Mbit/s. Ce nouveau standard a mis plus de quatre ans avant d'aboutir et arrive dans un contexte très concurrentiel (LTE/4G). Cette norme combine les dernières technologies permettant d'augmenter le débit (multiplexage OFDMA, antennes MIMO, utilisation de femtocells…)

En France, le WiMax est principalement exploité pour couvrir les zones « blanches », oubliées du haut débit. Mais cette technologie est fortement concurrencée par l'arrivée de la 4G/LTE (voir chapitre 7). Seules quelques offres existent, proposées par des opérateurs comme Iliad, Bolloré Telecom ou Axione dans certains départements (Axione propose par exemple ses réseaux WiMAX à 10 Mbit/s en réception dans le Finistère et les Hautes-Pyrénées).

Aux États-Unis, de grands opérateurs comme Sprint déploient des solutions WiMAX2 sur les réseaux WiMAX existants mais ces opérateurs qui fournissent également de la 4G seront sans doute également amenés à faire des choix compte tenu des coûts importants liés au déploiement des infrastructures.

Résumé

- Pour de faibles distances (inférieures au kilomètre sur des réseaux locaux), la transmission du signal numérique peut se faire en **bande de base**, sans transposition de fréquence. Le signal reste numérique et des débits importants peuvent être atteints (10 Gbit/s).
- Pour assurer une meilleure synchronisation et limiter l'affaiblissement, un **codage en bande de base** est appliqué au signal binaire (codage NRZ, Manchester, Miller…).
- Pour des distances plus importantes, à l'échelle des MAN ou des WAN, les performances du support imposent généralement une transformation du signal numérique en un signal analogique par **modulation**. Les **modems** réalisent cette opération de **mod**ulation à l'émission et de **dém**odulation à la réception.
- La modulation par **saut de phase et d'amplitude (PSK + AM ou QAM)** est la plus utilisée. Elle permet, en multipliant le nombre de bits codés par état de phase, d'augmenter les débits sans augmenter la bande passante du support.
- La voie de transmission qui relie les systèmes, généralement par l'intermédiaire de modems, est caractérisée par son débit maximum ou **capacité** exprimée en bit/s. Celle-ci est fonction de la bande passante et du rapport signal/bruit de la ligne.
- Le **délai d'acheminement** d'un message sur une voie est composé du **temps de transmission**, fonction du volume du message et du débit de la voie, et du **temps de propagation** lié à la nature du support.
- Une ligne de transmission peut être partagée en plusieurs voies ou canaux suivant un **multiplexage fréquentiel ou temporel**. Le multiplexage MIC permet ainsi de passer 32 voies à 64 kbit/s sur une ligne numérique d'une capacité de 2 048 kbit/s.

- Le multiplexage fréquentiel **OFDM** permet de répartir sur plusieurs sous-porteuses le code binaire à transmettre. Les fréquences des sous-porteuses sont orthogonales, ce qui permet d'une part de limiter la bande passante globale et d'autre part d'éviter que les signaux n'interfèrent entre eux.
- La transmission **ADSL** permet d'atteindre des débits de plusieurs Mégabit/s sur des distances inférieures à 5 km. Les paires téléphoniques classiques sont, dans ce cas, exploitées sur des fréquences allant jusqu'à 2,2 MHz avec les techniques de modulation et de partage étudiées précédemment.
- La transmission sur **fibre optique** est utilisée partout sur le réseau cœur d'Internet et de plus en plus comme solution de remplacement pour offrir « le très haut débit » sur la boucle locale. Les débits sur les fibres monomodes vont jusqu'à 100 Gbit/s et jusqu'à plusieurs Tbit/s lorsqu'un multiplexage en longueur d'onde est utilisé.
- Le standard **WiMAX** est utilisé pour des transmissions sans fil destinées à relier l'utilisateur à l'Internet sur le « dernier kilomètre » dans des endroits où une liaison ADSL filaire est inexploitable. Cette technique permet des débits théoriques maximums de 80 Mbit/s pour des distances jusqu'à 50 km. Les techniques de modulation sont semblables à celles utilisées pour l'ADSL.

Exercices corrigés

QCM

Q3.1 Sur quels types de support la transmission en bande base est-elle possible ?

a) Paire torsadée b) Fibre optique c) Réseaux sans fil

Q3.2 Dans une modulation PSK avec 3 bits par état de phase, quelle est la valeur élémentaire des déphasages ?

a) 90° b) 45° c) 22,5°

Q3.3 Sachant que le RTC présente une vitesse de modulation maximale de 6 200 bauds, quelle est la vitesse maximale de transmission si l'on utilise une modulation à huit états ?

a) 18 600 bit/s b) 28 800 bit/s c) 49 600 bit/s

Q3.4 Quelle est la valence d'une modulation à 4 bits par état de phase ?

a) 4 b) 16 b) 32 c) 64

Q3.5 Quel est le temps de transmission d'un fichier de 1 Mo sur une ligne à 1 Mbit/s ?

a) 8 s b) 1 s c) 10 s d) 8,4 s

Q3.6 Quel est le débit d'une voie dans un multiplexage TDM à 16 Mbit/s avec 8 voies ?

a) 1 Mbit/s b) 0,5 Mbit/s c) 2 Mbit/s

Q3.7 Dans un multiplexage OFDM avec 8 sous-porteuses et des modulations QAM 16, combien de bits peuvent être transmis simultanément ?

a) 8 b) 16 c) 32 d) 64

Q3.8 Dans une transmission ADSL, les signaux sont numériques :

a) Entre le PC et le modem b) Entre le modem et le DSLAM

c) Sur tout le réseau

Q3.9 Quelles sont les fréquences utilisées dans une transmission ADSL ?

a) 300-3 400 Hz b) 2-20 Mhz c) 64-1 100 Hz

Q3.10 Dans une transmission ADSL, où est situé le DSLAM ?

a) Chez le FAI b) Derrière la prise de l'abonné c) Après le répartiteur

Q3.11 Quel type de fibre permet les débits les plus élevés ?

a) La fibre multimode b) La fibre monomode

c) La fibre monomode avec WDM

Exercices

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

3.1 (**) En l'absence de transmission, le niveau binaire est en permanence à « 1 », coder ce signal en code Manchester, en code Manchester différentiel et en code Miller. Expliquer l'intérêt de ces codages pour le récepteur.

3.2 (**) Parmi les différents codages, quel est celui présentant le plus large spectre de fréquence, le spectre le plus étroit ? Quel est l'intérêt de réduire le spectre de fréquence ?

3.3 (**) Soit une modulation 16 PSK utilisant un code de Gray (deux symboles adjacents ne diffèrent que par un bit).

a) Dessinez le diagramme spatial correspondant.

b) Quel est le débit possible avec une fréquence de 4 méga-symbole/s ?

c) Pourquoi une modulation de type QAM est-elle mieux adaptée dans ce cas ?

3.4 (*) Calculer la capacité d'une ligne dont la bande passante est de 100-275 kHz et pour un rapport signal sur bruit évalué à 17 dB.

3.5 (*) Calculer le temps de transmission et le temps de propagation d'un fichier de 20 Ko sur un réseau Ethernet à 100 Mbit/s et pour des distances de 10 m, 100 m et 1 km.

3.6 (**) Quelles sont les trois étapes de la numérisation d'un signal analogique (ex. : parole) ? Quel est le débit de base du signal de parole numérisé ?

3.7 (*) Pour une transmission MIC à 2 048 kbit/s, calculer la période d'échantillonnage, la durée d'émission d'une trame, le nombre de bits par trames et la durée d'un intervalle de temps élémentaire.

3.8 (***) Quatre terminaux asynchrones sont connectés à un multiplexeur statistique permettant des débits composites maximums de 19 200 bit/s et intégrant des tampons d'un format de 8 bits. Les débits des terminaux sont respectivement de 9 600 bit/s, 4 800 bit/s, 4 800 bit/s et 4 800 bit/s. Calculer le débit effectif sur la voie composite et la durée d'une trame dans les différents cas si seulement trois terminaux sont actifs simultanément. Conclusion ?

3.9 (**) On désire transmettre un son HiFi stéréophonique de bande passante 20 Hz-20 kHz.

a) Peut-on transmettre ce signal tel quel sur le réseau téléphonique commuté (RTC) ? Justifier votre réponse.

b) On numérise ce signal par un échantillonnage à 44 kHz. On obtient alors pour chaque voie 8 bits à émettre toutes les 22,7 µs. Quel est le débit nécessaire ?

c) Ce débit est-il compatible avec les débits des modems actuels ?

3.10 (**) On veut utiliser la bande 64 kHz - 200 kHz pour assurer un débit de 544 kbit/s sur le flux montant d'un modem ADSL. Combien faut-il transmettre de bits par intervalle de modulation ?

3.11 (*) L'un des câbles transatlantiques, nommé TAT40, qui relie les États-Unis à l'Europe, est composé de deux ensembles de quatre paires de fibres. Chaque fibre peut fournir 40 canaux de 10 Gbit/s avec un multiplexage WDM. Quelle est la capacité du câble pour une exploitation bidirectionnelle ?

3.12 (*) Quels sont les domaines d'utilisation du WiMAX fixe et du WiMAX mobiles ?

Solutions

QCM

Q3.1 : a-b **Q3.2** : b **Q3.3** : a **Q3.4** : b **Q3.5** : d

Q3.6 : c **Q3.7** : c **Q3.8** : a **Q3.9** : c **Q3.10** : c

Q3.11 : b-c

Exercices

3.1

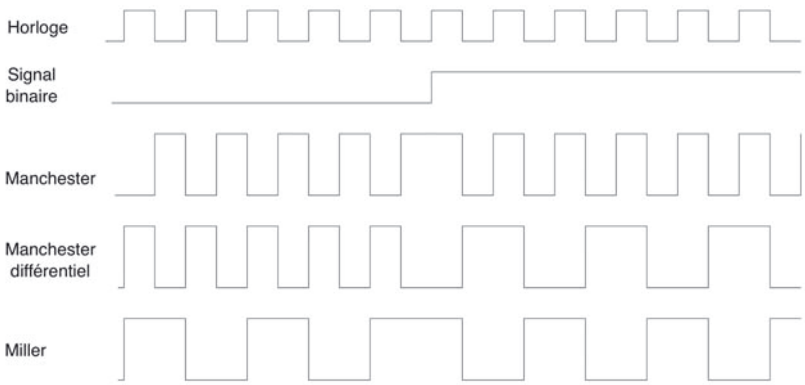


Figure 3.29

3.2 Le codage de Miller présente un spectre étroit donc moins exposé aux perturbations. Le codage Manchester a un spectre plus large mais sur des fréquences plus élevées donc moins affaiblies sur la ligne.

3.3

a)

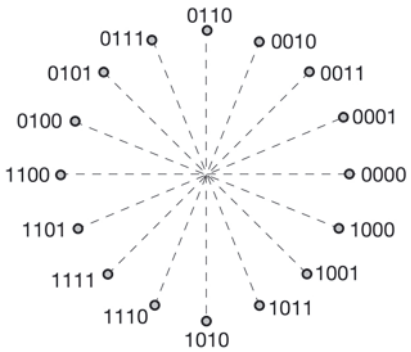


Figure 3.30

b) Le débit est de 4 bits par symboles, donc 16 Mbit/s.

c) L'utilisation conjointe de modulations par saut de phase et par saut d'amplitude permet une meilleure répartition des points dans le diagramme spatial et donc un taux d'erreur bit (BER) moins important à la réception.

3.4

$$C = 175 \cdot 10^3 \log_2(1 + 10^{1,7}) = 993 \text{ kbit/s}$$

3.5

$$T_t = \frac{20 \times 1024 \times 8}{100 \times 10^6} = 1{,}64 \text{ ms}$$

Tp = 4 µs pour 1 km ; Tp = 0,4 µs pour 100 m ; Tp = 0,04 µs pour 10 m.

3.6

- Étape 1 : échantillonnage (prélèvement périodique d'échantillons). Pour la parole, Fe = 8 000 Hz soit 8 000 échantillons/sec.
- Étape 2 : quantification (attribution de valeurs décimales aux échantillons prélevés).
- Étape 3 : codage en binaire des valeurs décimales précédentes. Pour la parole, le codage se fait sur 8 bits.

$$d = 8\,000 \times 8 \text{ bits/s} = 64\,000 \text{ bits/s} = 64 \text{ kbits/s}$$

3.7 La période d'échantillonnage est de $1/8 \cdot 10^3 = 125$ µs. Le temps de transmission d'une trame correspond au temps nécessaire pour multiplexer les échantillons de toutes les voies, soit 125 µs. Le nombre de bits par trame est de $32 \times 8 = 256$ bits ($2\,048 \cdot 10^3 \times 125 \cdot 10^{-6}$). La durée de l'intervalle de temps *IT* correspond au temps nécessaire pour transmettre les 8 bits d'un échantillon soit 125 µs / 32 = 3,9 µs.

3.8 Suivant les débits des terminaux actifs, deux calculs peuvent être effectués :

$$d = 3 \times 4800 = 14400 \text{ bit/s et } T_c = \frac{3 \times 8}{3 \times 4800} = 1{,}67 \text{ ms}$$

$$d = 2 \times 4800 + 9600 = 19200 \text{ bit/s et } T_c = \frac{3 \times 8}{2 \times 4800 + 9600} = 1{,}25 \text{ ms}$$

Pour le deuxième cas, le débit calculé est juste égal au débit composite maximum du multiplexeur. Si la voie composite est synchrone, le nombre de bits pouvant être transmis sur une trame sera supérieur au total des bits de chaque voie asynchrone dans la mesure où les bits de contrôle (start, stop, parité) sont supprimés.

3.9

a) Non. La bande passante du support utilisé sur le RTC (paire téléphonique) est de 300-3 400 Hz. Toutes les fréquences inférieures et supérieures seront fortement atténuées et donc non reçues par le récepteur.

b) En stéréophonie, il y a deux voies, soit 16 bits toutes les 22,7 µs. Débit : $16 / 22{,}7 \cdot 10^{-6} = 705$ kbit/s.

c) Un modem ADSL peut permettre un tel débit si la qualité de la ligne téléphonique est suffisante.

3.10 La bande allouée (64 kHz – 200 kHz) peut être divisée en 34 canaux de 4 kHz. Pour un débit total de 544 kbit/s, le nombre de bits par intervalle de modulation est de 544 000 / (4 000 × 34), soit 4 bits.

3.11 C = 2 × 4 × 40 ×10 Gbit/s = 3,2 Tbit/s.

3.12 Le WiMAX fixe est initialement prévu pour raccorder à l'Internet un usager à domicile en utilisant une transmission radio. Le WiMAX mobile prévoit la possibilité de connecter des clients mobiles à l'Internet, par exemple pour la téléphonie. La commutation entre les différentes antennes WiMAX devra dans ce cas être assurée lorsque l'utilisateur se déplace.

ARCHITECTURE DES RÉSEAUX

4

PLAN

OBJECTIFS

- Comprendre le rôle des différents équipements constituant un réseau.
- Connaître les principaux types de commutation dans le réseau cœur.
- Connaître le modèle OSI et savoir associer un protocole réseau à une couche de ce modèle.
- Comprendre le principe de l'encapsulation/décapsulation des données.
- Connaître les caractéristiques des principaux supports physiques présents dans les réseaux.

4.1 LIAISONS DE DONNÉES

Les liaisons et éléments associés faisant l'objet des normalisations décrites dans les chapitres précédents ne concernent que des transferts entre deux systèmes téléinformatiques distants, ce sont des **liaisons point à point**. Ce type de liaison existe par exemple entre un abonné et son fournisseur d'accès Internet et est matérialisé par la connexion entre les deux modems distants. Un protocole spécifique de type PPP (*Point to Point Protocol*) est alors utilisé pour le dialogue entre les deux modems (figure 4.1).

Pour une liaison point à point, le taux d'activité est généralement faible et le support physique sous-utilisé. Pour pallier cet inconvénient, une même ligne peut servir à la connexion de plusieurs systèmes, on parle alors de **liaison multipoint**. Ce type de liaison implique des techniques de raccordement et des méthodes de partage du support plus complexes. C'est une liaison multipoint que l'on retrouve par exemple dans un réseau local Ethernet pour lequel toutes les stations communiquent sur un même support par l'intermédiaire d'un équipement d'interconnexion (commutateur ou *switch*).

Précisons que, sur une liaison multipoint, la configuration peut varier entre deux situations extrêmes. Dans la configuration la plus simple, un seul système central (ou station primaire) donne le droit de transmettre à l'un des autres systèmes (ou stations secondaires). Toutes les données passent par le système central. La gestion est alors centralisée. À l'inverse, lorsque chaque station est susceptible d'être station primaire et donc de transmettre sur la liaison multipoint, la gestion est distribuée. Il faut alors définir quelle station va avoir le droit d'émettre sur le support partagé à un instant donné. Ce sont les méthodes d'accès au support qui vont permettre de décider quand une station a le droit d'émettre et qui permettront de résoudre éventuellement les erreurs de transmission en cas de demandes simultanées non résolues ou de mauvaises conditions sur la liaison. Ces méthodes d'accès au support sont décrites dans le chapitre sur les réseaux locaux (accès par élection ou par compétition, méthodes déterministes ou aléatoires).

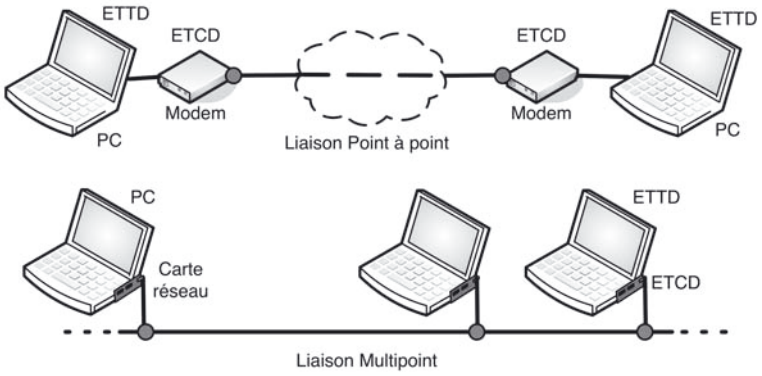


Figure 4.1 – **Liaisons point à point et multipoint.**

4.2 Éléments d'un réseau

Les éléments constitutifs d'un réseau local ou public peuvent être regroupés en trois familles : les équipements terminaux, les équipements d'interconnexion, les contrôleurs de communication.

Les éléments sont reliés entre eux par des lignes de transmission courte ou longue distance de type point à point ou multipoint.

La différence au niveau des lignes de transmission entre réseau local et réseau public, outre les valeurs caractéristiques des distances et des débits, se situe dans la nature des liaisons :

- dans un réseau local, les liaisons entre éléments sont généralement permanentes ;
- dans un réseau public, les liaisons entre éléments sont le plus souvent limitées à la durée des communications et utilisent des circuits de type commutés (voir section 4.3).

La figure 4.2 illustre un exemple de réseau privé faisant intervenir ces différents éléments. Les terminaux, les ordinateurs centraux ou serveurs symbolisent les ressources principales. Les routeurs et commutateurs du réseau cœur sont des équipements d'interconnexion.

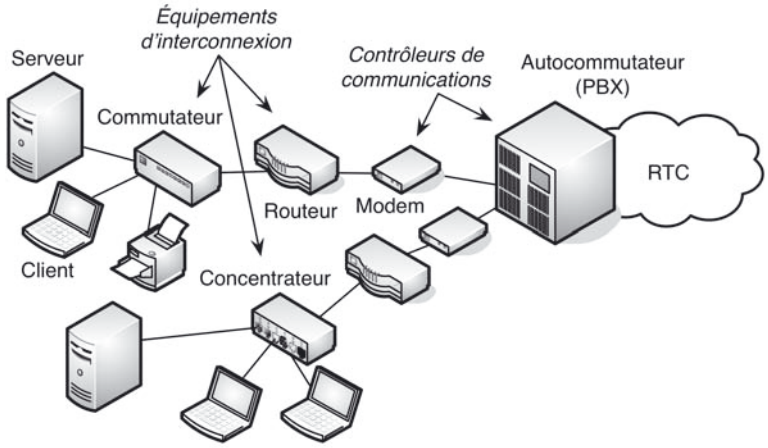


Figure 4.2 – Éléments d'un réseau informatique.

4.2.1 Équipements terminaux

La fonction principale d'un équipement terminal est de permettre à l'utilisateur d'accéder aux ressources du réseau par l'intermédiaire d'une interface, généralement multipoint, filaire ou sans fil. C'est l'équipement à l'extrémité de la liaison de données auquel l'utilisateur a directement accès. La famille des terminaux comprend les terminaux spécifiques (smartphone, terminal bancaire, terminal de paiement…), les ordinateurs de type PC (*Personnal Computer*), qui peuvent être des clients dans une organisation client-serveur, et les serveurs.

Les premiers réseaux locaux informatiques suivaient une organisation essentiellement client-serveur avec des terminaux (des stations) très limités, de type écran-clavier, et des serveurs qui concentraient toutes les ressources en termes de calcul et de stockage. De nos jours, les PC sont suffisamment puissants pour être autonomes et les serveurs sont utilisés pour l'authentification sur le réseau, le stockage sécurisé, ou la gestion de services spécifiques (mail, web fichier, bases de données…). Certaines entreprises utilisent également des « clients légers » qui sont alors des PC avec une architecture minimaliste (un processeur limité et pas de disque dur), les applications étant exécutées sur les serveurs. Cette organisation client-serveur permet de simplifier l'administration du parc de machine et d'éviter les stockages non sécurisés sur les PC mais n'est possible que si le réseau est performant.

4.2.2 Équipements d'interconnexion

Ils assurent les connexions nécessaires entre deux ou plusieurs équipements terminaux. Parmi les plus courants :

- Les **multiplexeurs** permettent le partage statique (allocation fixe et permanente) des ressources de la ligne entre les équipements terminaux qu'ils connectent. Le multiplexage peut être fréquentiel si la ligne large bande est divisée en canaux à bande de fréquence étroite, temporel ou statistique si chaque élément occupe la ligne successivement (voir chapitre 3).
- Les **concentrateurs** (*hub*) sont généralement passifs et permettent l'interconnexion au réseau de plusieurs équipements. Les hubs Ethernet qui sont progressivement remplacés par des switchs (voir chapitre 5) sont les plus répandus. Les hubs USB (voir chapitre 2) permettent également la connexion de plusieurs esclaves sur le même port USB d'un maître.
- Les **commutateurs** (*switch*) établissent les liaisons entre les équipements terminaux, le temps de la transmission des données. À titre d'exemple, le terminal (combiné téléphonique) de chaque abonné du réseau téléphonique est raccordé à un commutateur de rattachement de l'opérateur de boucle locale. La liaison n'est établie que le temps de la communication. Les **commutateurs Ethernet** sont un cas particulier, ils permettent de regrouper sur un même segment, un même bus, les stations d'un réseau local liées par un trafic important.
- Les **routeurs** permettent l'interconnexion des réseaux ou des sous-réseaux entre eux et sont décrits au chapitre 6.

4.2.3 Contrôleurs de communication

Les contrôleurs de communication gèrent l'accès d'un équipement terminal à la ligne de transmission. Suivant la nature des liaisons (débits, distances…), ces contrôleurs réalisent un simple codage en bande de base ou une modulation complexe. Dans le cas d'une liaison multipoint, le contrôleur gère également le partage de l'accès au support.

a) Cartes d'interface réseau (carte coupleur)

Ces cartes équipent la plupart des PC ou des serveurs et sont généralement intégrées à la carte mère. Elles permettent leur intégration dans un réseau local en gérant une partie du protocole. Ces cartes sont spécifiques au réseau local utilisé (cartes Ethernet, WiFi, Bluetooth…). Les routeurs intègrent également des cartes réseau, le plus souvent Ethernet.

b) Cartes d'interface série asynchrones ou synchrones

Ce sont les cartes qui équipent certains ordinateurs, routeurs et terminaux spécifiques. Elles intègrent un ou plusieurs circuits d'interfaçage asynchrone ou synchrone (voir chapitre 3). Ces cartes permettent le raccordement au réseau éventuellement *via*

l'utilisation d'un modem pour des liaisons distantes. Un automate intègre par exemple une carte RS485 pour être relié au reste du réseau de l'atelier.

c) Contrôleurs pour raccordement aux réseaux publics

Ce type de contrôleur dont l'architecture est comparable à celle d'un micro-ordinateur permet la transmission des données entre deux sites à travers les circuits commutés du réseau public utilisé (RTC, ATM…) ; un contrôleur équivalent doit donc exister à l'autre extrémité. Ces contrôleurs gèrent une partie du protocole lié au réseau et intègrent des tampons permettant la mémorisation temporaire des trames, des paquets ou des cellules (voir chapitre 7). Les modems et les cartes ATM font partie de cette catégorie.

4.3 Réseaux à commutation

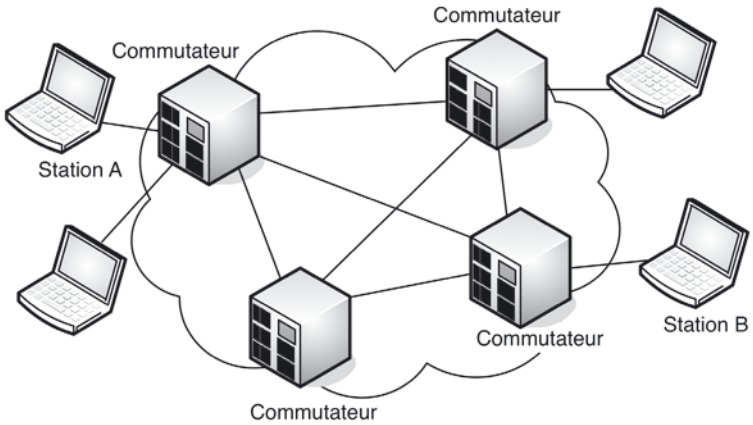


Figure 4.3 – Réseaux à commutation.

Les réseaux à commutation permettent à tout équipement informatique connecté de communiquer directement avec tout autre équipement à travers un réseau de type maillé (système ouvert).

Ce type de réseau, généralement public, est formé d'un ensemble d'ETTD (stations) interconnectés par des lignes de communication. Les liaisons sont gérées par des commutateurs ou nœuds de commutation chargés de trouver un chemin entre les stations communicantes et d'établir la liaison entre elles (figure 4.3). Ces réseaux sont souvent opposés aux réseaux locaux dans lesquels les liaisons entre stations sont permanentes.

On distingue pour ces réseaux trois types de commutation :

- la commutation de circuits ;
- la commutation de paquets ou de messages ;
- la commutation de cellules.

Pour comparer ces trois types de commutation, il convient de définir les grandeurs utilisées pour caractériser le trafic téléinformatique.

a) Intensité du trafic ou taux de connexion

L'intensité du trafic E exprimée en erlangs est définie par la relation :

$$E = \frac{N \times T}{3600}$$

N est le nombre de sessions ou périodes de communication à l'heure.

T est la durée moyenne en secondes des sessions.

Le taux de connexion E caractérise donc le volume du trafic mesuré pendant une période d'observation d'une heure. Pour des applications de type interactif, E sera proche de 1. Pour des applications de type messagerie ou transfert de fichiers, les valeurs de E seront relativement faibles.

b) Taux d'activité

Le taux d'activité σ exprimé en pourcentage (%) est défini par la relation :

$$\sigma = \frac{T_t}{T}$$

T_t est le temps de transmission et T la durée d'une session de communication.

Le paramètre σ caractérise donc le rapport entre le temps réellement utilisé pour la transmission et le temps d'ouverture de la liaison.

c) Délai d'acheminement

C'est le temps qui s'écoule entre le début de la transmission d'un message sur le réseau et la fin de sa réception par le destinataire.

Ce délai est fonction du temps de transmission T_t, du temps de propagation T_p, des temps d'attente dans les commutateurs et du nombre de commutateurs traversés (voir chapitre 3).

4.3.1 Commutation de circuits

Les données sont transmises sur un circuit, matérialisé par une continuité électrique, établi provisoirement entre 2 ETTD (figure 4.4). Les caractéristiques principales de ce type de commutation sont :

- un temps d'établissement de la commutation constant et court ;
- des formats d'information libres ;
- pas de stockage des informations communiquées dans le réseau ;
- des taux de connexion et d'activité faibles.

La commutation de circuits est utilisée principalement sur les réseaux téléphoniques. Pour des communications grandes distances, la liaison est établie par une série de commutateurs hiérarchisés et situés dans les différents centres de transit (centres locaux, centres interurbains, centres nationaux – voir chapitre 7).

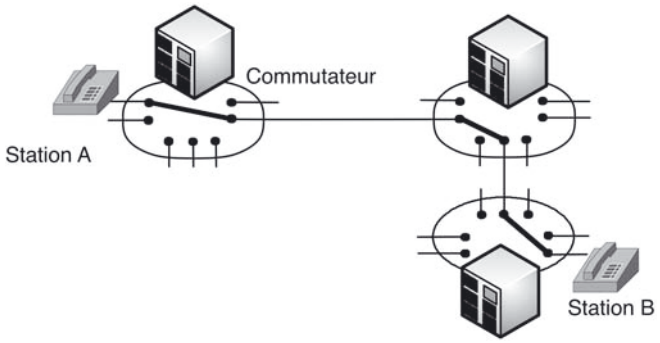


Figure 4.4 – **Commutation de circuits.**

4.3.2 Commutation de paquets

Un message est découpé en paquets de longueur fixe. Les paquets sont transmis de commutateur en commutateur jusqu'à l'ETTD destinataire (figure 4.5). À leur arrivée dans un commutateur, chaque paquet est mémorisé dans des tampons alloués et transmis vers le commutateur suivant lorsqu'un tampon de celui-ci est disponible. Les tampons d'un commutateur peuvent donc contenir à un instant donné les paquets de différents messages.

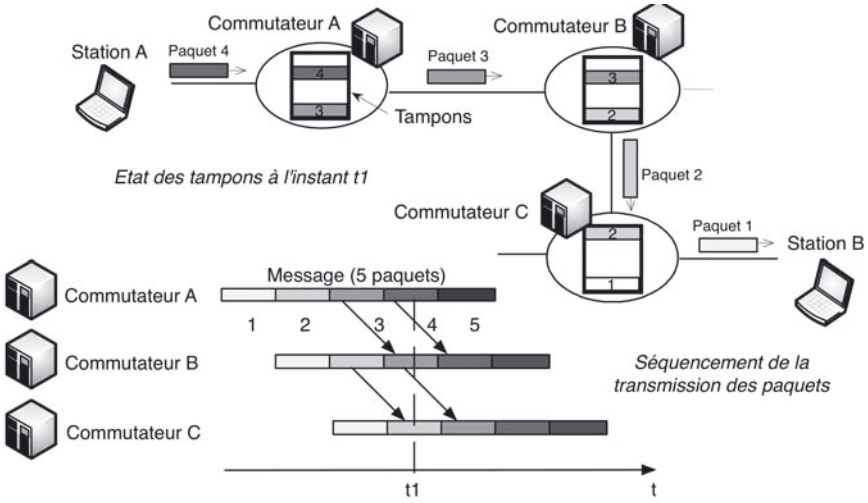


Figure 4.5 – **Commutation de paquets.**

Les caractéristiques de la commutation de paquets sont :

- un multiplexage temporel des paquets de plusieurs messages dans les commutateurs (optimisation des commutateurs) ;
- une possibilité de reprise en cas d'erreur de transmission d'un paquet ;
- une gestion des transmissions (acquittement ou demande de retransmission) et un contrôle de flux ;

- une politique de routage (choix des chemins suivant la capacité et l'état du réseau) ;
- des taux de connexion et d'activité proches de 1.

Ce type de commutation utilisé dans les anciens réseaux X.25 et Frame Relay est peu à peu abandonné au profit de la commutation de cellules ou de la technologie MPLS (voir chapitre 7).

4.3.3 Commutation de cellules

Dans la commutation de paquets, la taille de ceux-ci ne permet pas de prévoir le délai de transmission des informations, ce qui est incompatible avec le transport de la voix ou de la vidéo. Pour pallier cet inconvénient, l'OSI a normalisé une technique de commutation de cellules de longueur constante, émises à intervalle de temps constant sur des voies de communication. Cette technique est principalement exploitée dans le réseau ATM (*Asynchronous Transfer Mode*) qui a remplacé le réseau à commutation de paquets X25.

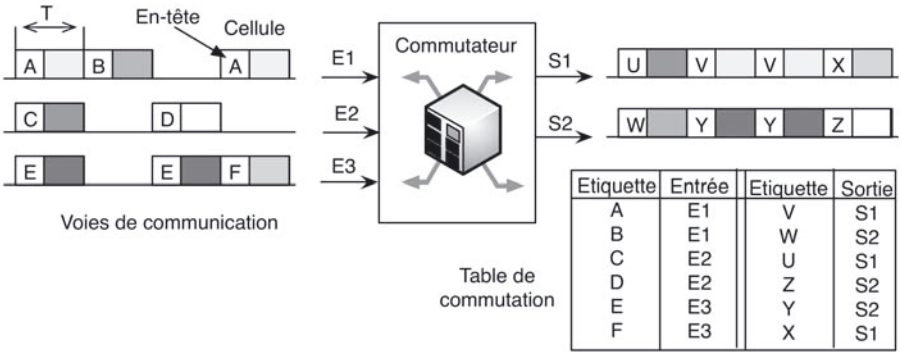


Figure 4.6 – **Commutation de cellules.**

Les stations transmettent leurs données sous forme de cellules dans des voies de communication communes. Chaque cellule est identifiée en entrée et en sortie du commutateur par une étiquette comprise dans son en-tête et sera redirigée vers une voie de sortie suivant une table de commutation (figure 4.6). Les commutateurs n'ont pas de fonctions de mémorisation, ils permettent d'optimiser les trafics en créant des chemins virtuels regroupant les différentes voies actives. Comme pour les réseaux à commutation de paquets, une première cellule spécifique est transmise pour tracer le circuit virtuel et poser les étiquettes dans les commutateurs. Les performances (cellules commutées par seconde) demandées aux commutateurs doivent être très élevées pour satisfaire à la contrainte du temps de transit qui doit rester constant dans le réseau, notamment pour le transfert de la voix.

4.4 Normalisation

4.4.1 Le modèle OSI

Un réseau est un ensemble complexe qui nécessite une décomposition des systèmes interconnectés en éléments matériels ou logiciels directement réalisables.

La décomposition en sept couches superposées, sept sous-ensembles fonctionnels, proposée par l'ISO (*International Standardization Organization*), définit les caractéristiques physiques et logicielles pour l'interconnexion en réseau des systèmes ouverts. Les fonctionnalités de chaque couche sont assurées par des fonctions logicielles, à l'exception des couches 1 et 2, réalisées par des composants matériels.

Ce modèle d'architecture en couches, dénommé modèle OSI (*Open System Interconnection*), est décrit par la figure 4.7. Dans ce modèle, ce sont les applications (couche 7) des systèmes d'extrémité (systèmes A et B) qui ont besoin d'échanger des données. Les autres couches ne sont là que pour permettre cet échange. Lorsque des systèmes intermédiaires, commutateurs ou routeurs par exemple, sont nécessaires, ils ne contiennent que les couches nécessaires à l'acheminement et au transfert des informations (en général, les couches 1, 2 et 3).

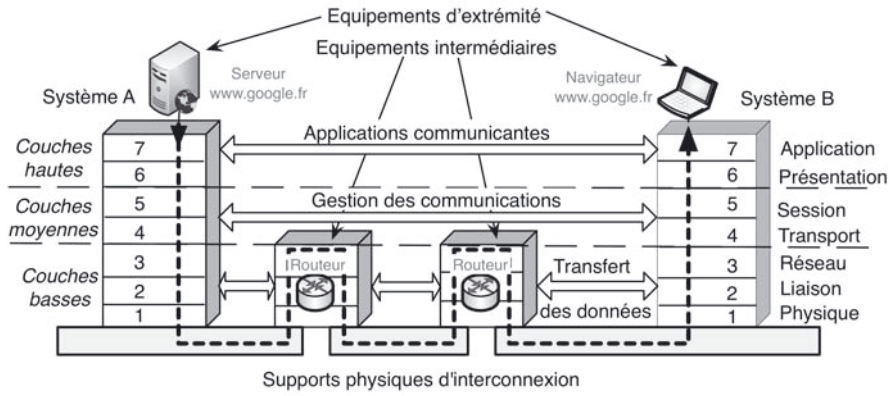


Figure 4.7 – Le modèle OSI.

Les fonctions assurées par l'ensemble des couches vont de l'exécution de l'application mise en œuvre par l'usager (niveau 7) jusqu'à la transmission physique des données sur la ligne ou support physique d'interconnexion (niveau 1).

Lors d'une communication, les échanges entre deux niveaux *N* (symbole ⟺ sur la figure) sont réglés suivant le protocole *N*. Les informations échangées lors de ce dialogue transitent verticalement par les niveaux inférieurs (symbole ◄- - ►), de couche en couche.

Par exemple, une application entre un serveur web et un navigateur utilise le protocole http au niveau 7 et les données correspondant à la page web sont transmises de couche en couche jusqu'au support physique.

4.4.2 Description des couches

Les sept couches peuvent être regroupées en trois blocs fonctionnels (voir les concepts de base au paragraphe 1). Les couches 1, 2 et 3 sont les **couches basses**. Elles assurent la transmission et l'acheminement des informations à travers le réseau sur le support (câbles, transmissions sans fil…).

Les couches 4 et 5 sont les **couches moyennes**. Elles gèrent les communications et les ressources (processus et mémoire) nécessaires à l'échange des messages entre équipements terminaux (stations ou serveurs). Les couches 6 et 7, **couches hautes**, traitent les données échangées (exécution de commandes, mise en forme, affichage…).

a) Les couches basses

Elles se trouvent dans tous les équipements connectés sur le réseau, équipement terminal, d'interconnexion ou contrôleur de communication.

- *Couche physique (couche 1)* : réalise la transmission des éléments binaires constitutifs des trames sur le support suivant des caractéristiques physiques, électriques, optiques et mécaniques définies par des normes (Ethernet, WiFi…). La couche physique définit donc l'interface, les connecteurs, le câblage et la nature des signaux utilisés.
- *Couche liaison (couche 2)* : assure un service de transport de trames sur une ligne et dispose de moyens de détection d'erreur et éventuellement de correction. La couche liaison définit également une méthode d'accès au support lorsque plusieurs stations sont en concurrence pour transmettre des données sur un support partagé (cas des liaisons multipoint).
- *Couche réseau (couche 3)* : assure l'adressage et le routage (choix des chemins à partir des adresses) des données groupées en paquets au travers du réseau (voir protocole IP). D'autres fonctions telles l'interconnexion de réseaux hétérogènes et le contrôle de congestion peuvent être réalisées dans cette couche.

b) Les couches moyennes

Elles assurent le dialogue entre les équipements terminaux, indépendamment du (ou des) réseau(x) utilisé(s). Elles comportent les règles de transfert de l'information, de contrôle de flux et de l'intégrité des données transmises.

- *Couche transport (couche 4)* : responsable du contrôle du transfert des informations de bout en bout, réalise le découpage des messages en paquets pour le compte de la couche réseau ou le réassemblage des paquets en messages pour les couches supérieures. Le contrôle de flux et la résolution de pertes sont le plus souvent réalisés par cette couche (voir protocole TCP).
- *Couche session (couche 5)* : sert d'interface entre les fonctions liées à l'application et celles liées au transport des données. Elle assure l'ouverture et la fermeture des sessions pour le compte des applications, définit les règles d'organisation et de synchronisation du dialogue entre les abonnés. Cette couche est rarement utilisée, ses fonctionnalités sont souvent assurées par la couche transport.

c) Les couches hautes

- *Couche présentation (couche 6)* : met en forme les informations échangées pour les rendre compatibles avec l'application destinatrice, dans le cas de dialogue entre systèmes hétérogènes (comporte des fonctions de traduction, de compression, d'encryptage…). Cette couche n'est pas indispensable.
- *Couche application (couche 7)* : est chargée de l'exécution de l'application et de son dialogue avec la couche 7 du destinataire en ce qui concerne le type ou la signification des informations à échanger (page web, transfert de fichier, messagerie, interrogation de base de données…).

4.4.3 Protocoles et services

Le modèle OSI définit également trois notions supplémentaires (figure 4.8) :

- les protocoles qui sont les règles qui définissent le dialogue entre couches de même niveau (protocole IP au niveau 3 par exemple) ;
- les services fournis par chaque couche $N - 1$ aux couches N par l'intermédiaire de primitives de service ;
- les primitives de service qui sont des fonctions logicielles qui définissent le dialogue entre couches adjacentes et qui peuvent concerner des demandes, des réponses, des échanges d'informations ou des confirmations d'états.

Les services sont fournis à la frontière entre deux couches au niveau de points d'accès (SAP, *Service Access Point*).

L'une des caractéristiques de la description par couche est de limiter le nombre de primitives et de protocoles qu'une couche doit connaître. La couche N d'un système n'a à connaître que les primitives de service correspondant à la couche N - 1 du même système et le protocole N des systèmes distants.

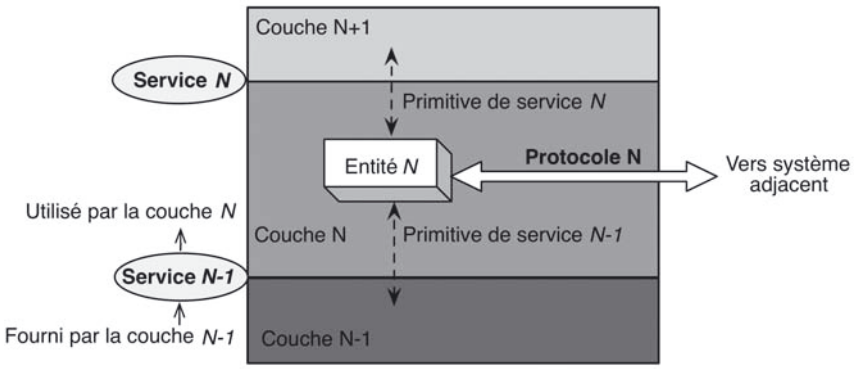


Figure 4.8 – Protocoles et services.

La notion de protocole a déjà été abordée dans le chapitre 1, il s'agit ici de protocoles réseau tels IP au niveau 3, TCP au niveau 4, http au niveau 7…

Pour illustrer la notion de service, la figure 4.9 décrit, en liaison avec le modèle OSI, les quatre primitives échangées à l'interface entre les couches transport et les couches réseau des deux systèmes susceptibles de communiquer. Chaque primitive fait référence à un service particulier, par exemple l'établissement d'une connexion au niveau transport. Ces primitives, qui correspondent dans ce cas à des fonctions logicielles standards, sont associées chacune à des paramètres, comme les adresses de l'appelant et de l'appelé pour la primitive *T_Connect_Request*. Cette dernière permet la demande d'un service à la couche réseau de la part de la couche transport. En réponse, la primitive *T_Connect_Confirm* indique à la couche transport que le service est établi.

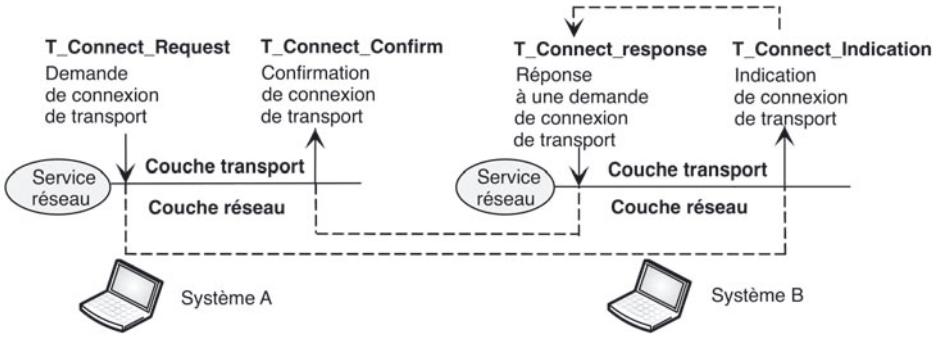


Figure 4.9 – Exemple d'échange de primitives de service aux niveaux 3 et 4.

La figure 4.10 décrit plus généralement le principe d'échange d'informations entre couches successives (seul le système source est représenté) :

- la couche $N + 1$, utilisatrice des services de niveau N, adresse à la couche N des unités de données de service de niveau N ou SDU (*Service Data Unit*) ;
- des informations de contrôle de protocole ou PCI (*Protocol Control Information*) sont ajoutées aux données entrantes constituées par les SDU ;
- l'ensemble ainsi formé constitue des unités de données de protocole ou PDU (*Protocol Data Unit*) ;
- la couche N utilisatrice des services de niveau $N - 1$ adresse à son tour à la couche $N - 1$ des $(N - 1)$ SDU.

La communication entre les deux entités de niveau N s'effectue donc par un échange des (N) PDU suivant le protocole N. Cet échange est effectué, après une demande de service $N - 1$ (à l'aide d'une primitive) à la couche $N - 1$, par transmission verticale des $(N - 1)$ SDU et ainsi de suite jusqu'au niveau physique.

L'échange d'informations des couches basses vers les couches hautes se fait suivant le même principe sur le système récepteur, à l'aide de primitives de service. Les PCI sont dans ce cas retranchées des PDU entrantes (figure 4.11).

Le procédé qui consiste, pour une couche donnée, à ajouter ou à retrancher des informations de contrôle pour former une nouvelle unité de données est nommé « encapsulation » ou « décapsulation ».

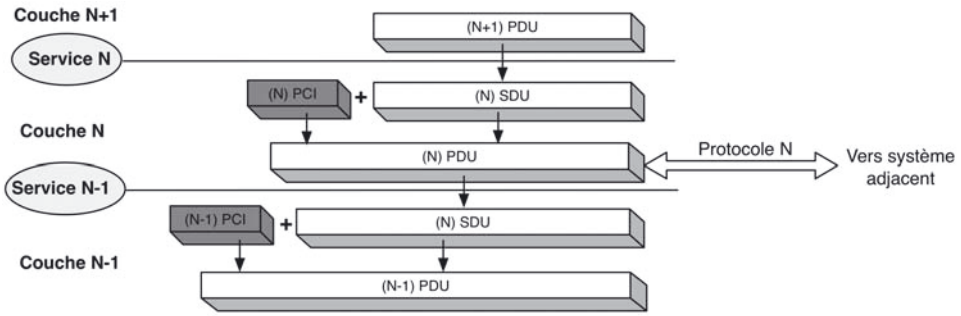


Figure 4.10 – Échange d'informations entre couches.

La figure 4.11 donne un exemple d'échange d'informations entre deux systèmes sur un réseau local Ethernet. À l'émission, les données sont découpées en fragments par la couche transport pour former des segments TCP. Ces segments sont encapsulés dans les paquets IP de la couche réseau, lesquels sont encapsulés à leur tour dans les trames Ethernet de la couche liaison. Ces trames sont ensuite codées et mises en forme pour être transmises sous forme d'éléments binaires sur le support physique.

Notons que chaque unité de donnée désignée de manière générique PDU (*Protocol Data Unit*) prend dans cet exemple un nom particulier suivant la couche concernée : segment, paquet, trame et bit. Le passage d'une couche à l'autre se fait par ajout d'informations de contrôle PCI (*Protocol Control Information*), c'est-à-dire successivement : l'en-tête TCP, l'en-tête IP, l'en-tête Ethernet.

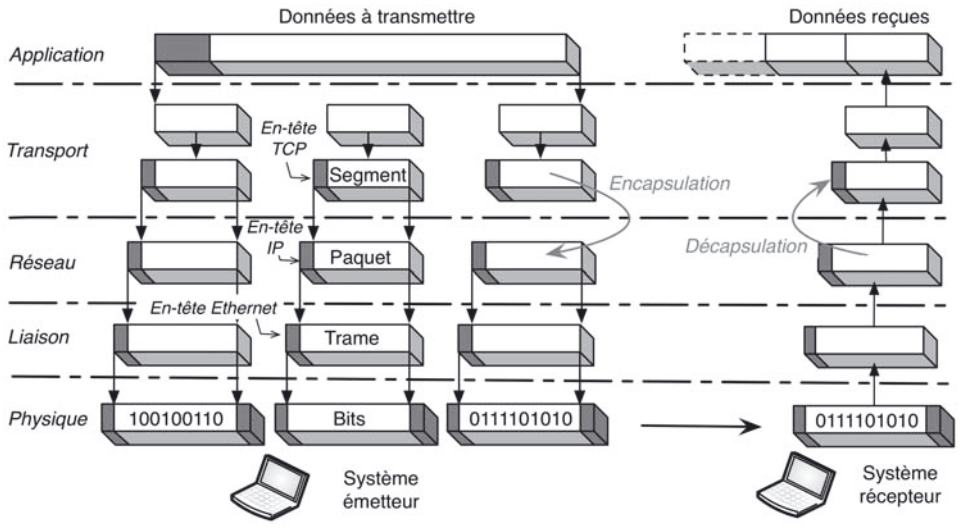


Figure 4.11 – Échange de données sur un réseau Ethernet.

4.5 Le support physique d'interconnexion

Le choix du support est fonction de critères interdépendants parmi lesquels :

- la distance maximum entre stations ;
- le débit minimum et maximum ;
- le type de transmission (numérique ou analogique) ;
- la nature des informations échangées (données, voix, vidéo…) ;
- la connectique ;
- la fiabilité, le coût…

Le tableau 4.1 donne l'ordre de grandeur des débits nécessaires en fonction de la nature des informations à transmettre.

Tableau 4.1 – Valeur des débits suivant la nature des informations.

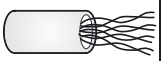
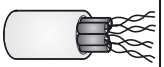
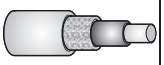
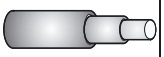
Nature des informations	Débits
Page A4 de texte transmise en 1 s	10 kbit/s
Fichier de 10 Mo transmis en 1 s	80 Mbit/s
Voix échantillonnée sur 8 bits à 8 kHz	64 kbit/s
Son stéréo échantillonnée sur 16 bits à 44,1 kHz	1,4 Mbit/s
Image N&B non compressée (50 images/s)	12,5 Mbit/s
Image N&B compressée	500 kbit/s
Image couleur non compressée (50 images/s)	200 Mbit/s
Image couleur compressée	2 Mbit/s

Les différents supports physiques sont :

- les fils de cuivre en paire torsadée utilisés pour la transmission locale en bande de base ou pour de faibles fréquences et sur de courtes distances ;
- les paires torsadées blindées utilisées en réseau local ou urbain pour des transmissions numériques ;
- les câbles coaxiaux utilisés dans les réseaux locaux en bande de base ou pour la transmission urbaine et interurbaine à moyen et haut débit ;
- les fibres optiques utilisées dans les réseaux locaux à haut débit, sur les liaisons interurbaines et sur les liaisons d'abonnés des réseaux publics numériques ;
- les supports hertziens (ondes radioélectriques) pour les applications urbaines et interurbaines de télécommunication (réseaux cellulaires ou boucle locale WiMAX par exemple) ainsi que pour les réseaux locaux sans fil (WLAN au standard WiFi) ou encore l'interconnexion des équipements personnels de type smartphone ou appareil photo (WPAN au standard Bluetooth) ;
- les liaisons satellitaires de télécommunication et de télédiffusion.

Le tableau 4.2 résume les caractéristiques principales des supports usuels pour des transmissions en bande de base.

Tableau 4.2 – Caractéristiques des différents supports.

Type de support		Débit max.	Distance max. (sans répéteurs)	Temps de propagation	Immunité au bruit	Remarques
Paire torsadée non blindée (0,2 mm)		1 Gbit/s	1 km	≈ 5,3 µs/km	Faible	Affaiblissements importants
Paire torsadée blindée (0,2 à 1 mm)		10 Gbit/s	1 km (56 m à 10 Gbit/s)	≈ 5,3 µs/km	Bonne	Liaisons multifils
Câble coaxial (2,6/9,5 mm ou 1,2/4,4 mm)		100 Mbit/s	1 km	≈ 4,1 µs/km	Très bonne	Impédance caractéristique de 50 Ω ou 75 Ω B ≈ 500 MHz
Fibre optique		10 Gbit/s	10 km	≈ 5 µs/km	Excellente	Débits en progression B = 10 GHz pour 1 km

Pour des distances de transmission supérieures à celles indiquées, l'utilisation de répéteurs est nécessaire. Les distances moyennes de répétition sont de 3 km pour le câble coaxial, ce qui autorise des débits de 10 Mbit/s, et de 50 km pour la fibre optique avec des débits supérieurs à 100 Mbit/s.

Pour les transmissions longues distances en bande de base ou par modem, l'utilisateur doit employer les ressources des télécommunications, en empruntant le RTC, les réseaux urbains câblés ou en louant des lignes spécialisées à un opérateur réseau. Ces lignes électriques ou optiques proposent des débits de quelques dizaines de kilobits par seconde à quelques gigabits par seconde.

Dans le cas particulier des transmissions sans fil par ondes radio, le débit dépend fortement de la bande de fréquence utilisée. Par exemple, pour des transmissions locales utilisant le standard WiFi 802.11n (voir chapitre 5), la bande ISM (Industrie, Science et Médecine) des 2,4 GHz utilisée et les modulations associées permettent des débits jusqu'à 100 Mbit/s pour des distances limitées à quelques centaines de mètres. Par ailleurs, le standard WiMAX 802.16 (voir chapitre 3) permet théoriquement d'émettre et de recevoir des données dans les bandes de fréquences radio de 2 à 66 GHz avec un débit maximum théorique de 70 Mbps sur une portée de 50 km.

De par leur nature, les supports sans fil sont naturellement plus sensibles aux perturbations extérieures, telles les interférences provoquées par d'autres émissions dans les mêmes bandes de fréquence (les micro-ondes générées dans un four

peuvent perturber des transmissions 802.11…) ou les obstacles entre les antennes émettrice et réceptrice. Ces supports présentent donc globalement une moins bonne immunité aux bruits que les supports filaires.

Résumé

- Les réseaux utilisent des **liaisons multipoints** sur des supports partagés. Les **méthodes d'accès** au support définissent comment un système peut émettre à un instant donné sur le support partagé.
- Trois types d'équipement existent dans les réseaux : les **terminaux** (PC, smartphone, serveur), les **équipements d'interconnexion** (hub, switch, routeur) et les **contrôleurs de communication** (carte Ethernet, carte Wifi, modem).
- Dans un **réseau local**, les liaisons entre les équipements sont généralement permanentes. Dans un **réseau public**, les liaisons entre les équipements sont limitées à la durée de la communication.
- Trois types de commutation sont utilisés dans les réseaux :
  – la commutation de **circuits** qui ne nécessite pas de stockage des informations dans le réseau, mais qui entraîne un faible taux d'activité ;
  – la commutation de **paquets** qui nécessite le stockage de chaque paquet dans les tampons des commutateurs. Elle permet des taux d'activité élevés ;
  – la commutation de **cellules** qui permet de diminuer le délai de transmission nécessaire à la voix et à la vidéo.
- Le **modèle OSI** décompose le fonctionnement des systèmes interconnectés en 7 couches fonctionnelles. Les couches peuvent être regroupées en 3 blocs fonctionnels : les couches basses gèrent la connexion et l'acheminement des informations, les couches moyennes gèrent la communication, les couches hautes traitent les données.
- Les **protocoles** définissent les dialogues de couche N à couche N, les **primitives de service** sont utilisées entre une couche $N-1$ et la couche adjacente N.
- À l'unité de donnée de service **SDU** (*Service Data Unit*) reçue, une couche N ajoute des informations de contrôle **PCI** (*Protocol Control Informations*) pour former une unité de données de protocole **PDU** (*Protocol Data Uni*t). Cette opération est nommée **encapsulation**. À la réception, les PCI sont traitées par la couche N et seul le **SDU** est remonté à la couche $N+1$, c'est la **décapsulation**.
- Les supports physiques utilisés dans les réseaux sont : les paires torsadées, les câbles coaxiaux, les fibres optiques et les supports sans fil par ondes radio. Ces supports sont caractérisés par le débit maximum, la portée et l'immunité aux bruits.

Exercices corrigés

QCM

Q4.1 À quel type d'élément appartient une carte d'interface réseau ?

a) terminaux b) équipements d'interconnexion

c) contrôleurs de communication

Q4.2 Quel est le type de commutation utilisé par le RTC ?

a) de circuit b) de paquets c) de cellules

Q4.3 Quel est le type de commutation utilisé par le réseau ATM ?

a) de circuit b) de cellules c) de paquets

Q4.4 Quel type de commutation ne nécessite pas le stockage des données dans le réseau ?

a) de circuit b) de paquets c) de cellules

Q4.5 Quelles couches du modèle OSI gèrent les communications ?

a) couches basses b) couches moyennes c) couches hautes

Q4.6 La couche réseau fait partie :

a) des couches basses b) des couches moyennes

c) des couches hautes

Q4.7 Quelle couche gère le contrôle de flux ?

a) Physique b) Réseau c) Transport d) Session

Q4.8 Quelle couche est responsable du routage ?

a) Liaison b) Réseau c) Transport d) Session

Q4.9 Dans quels équipements la couche réseau est-elle présente ?

a) Hub b) Switch c) Routeur d) Serveur

Q4.10 Le dialogue entre couches adjacentes est assuré par :

a) les protocoles b) les services c) les primitives de service

Q4.11 L'unité de données passée par une couche N à une couche $N-1$ est :

a) SDU b) PCI c) PDU

Q4.12 Un raccordement à l'aide d'une paire torsadée non blindée permet des débits maximums de :

a) 1 Gbit/s b) 10 Mbit/s c) 500 kbit/s

Q4.13 Un raccordement par fibre optique permet des débits maximums de :

a) 1 Gbit/s b) 10 Gbit/s c) 100 Mbit/s

Exercices

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

4.1 (*) Quel est le temps de transmission d'un fichier de 350 Mo sur une connexion ADSL à 12 Mbps ?

4.2 (***) Calculer le délai d'acheminement d'un message de 1 000 octets pour les deux types de réseaux :

a) réseau à commutation de paquets de 1 000 octets ;

b) réseau à commutation de paquets de 100 octets.

Dans les deux cas, le nombre de commutateurs traversés est de 3, le débit du réseau est de 9 600 bit/s et les temps de propagation et d'attente dans les commutateurs seront négligés.

4.3 (*) Pour une application de type transfert de fichiers sur réseau commuté, on transmet toutes les heures des fichiers de 1 Mo sur une ligne à 9 600 bit/s. Calculer le taux d'activité et le taux de connexion si la ligne est commutée pour des sessions de 20 min.

4.4 (**) Quel est le débit nécessaire pour transmettre des images d'une définition de 800 × 600 × 16 bits avec une fréquence image de 70 Hz pour un taux de compression de 20 ? Quels sont les supports physiques compatibles avec de tels débits ?

4.5 (*) Calculer le débit nécessaire pour transmettre un son stéréo numérisé sur 16 bits à 40 kHz. Quels sont les supports physiques compatibles avec ce débit ?

4.6 (***) Vous disposez d'un accès ADSL à 1 024 kbit/s et vous devez transférer un fichier de 300 Mo.

a) Calculez, en première approximation, le temps moyen mis pour transférer ce fichier.

b) Le fichier est en fait découpé en blocs de 1 460 octets. Pour chaque protocole sont ajoutés des en-têtes : 20 octets pour TCP, 20 octets pour IP et 30 pour les différents protocoles de niveau liaison présents sur ADSL. Calculez le temps effectif de transfert du fichier.

c) Compte tenu de l'heure et du nombre de clients connectés simultanément, les connexions de votre FAI sont saturées. Que devient le temps de transfert du fichier ?

d) À quel niveau OSI correspond le débit annoncé par les FAI ? Qu'en concluez-vous ?

4.7 (**) Votre réseau local est relié à votre FAI par un modem ADSL, à quelles couches OSI correspondent les différents matériels ou protocoles ?

Tableau 4.3

Entités	Couche OSI
Modem ADSL	
Câble Ethernet	
E-mail	
TCP	
IP	
Page web	
Compression	
Éléments binaires	
Trame	
Segment	

4.8 (**) Quel est le rôle des couches basses ? Quel est le rôle des couches moyennes ? Quel est le rôle des couches hautes ?

4.9 (**) Les couches moyennes sont dites « de bout en bout ». Que signifie cette expression ?

4.10 (***) Quel est l'intérêt de l'encapsulation de données ?

4.11 (**) Comment les informations sont-elles échangées entre deux couches de même niveau sur deux systèmes distants ?

4.12 (***) Votre PC est relié à un LAN Ethernet. Le format de l'information qui passe sur le médium de communication est le suivant, ce qui est en gras correspond à l'en-tête Ethernet :

Tableau 4.4

Adresse destination	**Adresse source**	**Type**	Données	**CRC**
6 octets	6 octets	2 octets	46 à 1 500 octets	4 octets

a) À quelle couche OSI correspondent les champs en gras ? Quelle est la longueur minimum d'une trame ?

b) Quelle est la longueur maximum de la charge utile (*payload*) ? À quelle couche correspondent ces données ?

c) Voici la trace hexadécimale prélevée par un analyseur de protocoles lors d'une communication. Les différents octets affichés correspondent à la trame Ethernet définie précédemment. Retrouver les trois premiers champs de la trame Ethernet dans la trace hexadécimale.

```
0800 2018 ba40 aa00 0400 1fc8 0800 4500
0028 e903 4000 3f06 6a5c a3ad 2041 a3ad
80d4 0558 0017 088d dee0 ba77 8925 5010
7d78 1972 0000 0000 0000 0000 0000 0000
```

Solutions

QCM

Q4.1 : c **Q4.2** : a **Q4.3** : b **Q4.4** : a **Q4.5** : b
Q4.6 : b **Q4.7** : c **Q4.8** : b **Q4.9** : c-d **Q4.10** : c
Q4.11 : c **Q4.12** : a **Q4.13** : b

Exercices

4.1 La taille en bits du fichier est : $350 \times 2^{20} \times 8$ (1 méga-octet fait 2^{20} octets). Le temps est donc :

$$T_t = (350 \times 2^{20} \times 8)/12 \times 10^6 = 268{,}43 \text{ secondes} = 4 \text{ min et } 28{,}43 \text{ s}$$

4.2

a) Commutation de paquets de 1 000 octets :

$$D_a = \frac{(4 \times 1\,000) \times 8}{9\,600} = 3{,}33 \text{ s}$$

b) Commutation de paquets de 100 octets :

$$D_a = \frac{(3 \times 100) \times 8}{9\,600} = 1{,}08 \text{ s}$$

4.3

$$E = \frac{20 \times 60}{3\,600} = 0{,}33 \qquad T_t = \frac{1\,024^2 \times 8}{9\,600} = 873{,}81 \text{ s}$$

$$\sigma = \frac{873{,}81}{20 \times 60} = 73\ \%$$

Les valeurs trouvées justifient l'emploi d'une liaison commutée.

4.4 Taille d'une image :

$$800 \times 600 = 480 \cdot 10^3 \text{ pixels soit } 480 \cdot 10^3 \times 16 = 7{,}28 \cdot 10^6 \text{ bits}$$

Après compression :

$$7{,}68 \cdot 10^6 / 20 = 384 \cdot 10^3 \text{ bits par image}$$

Pour avoir 70 images par seconde, il faut :

$$384 \cdot 10^3 \times 70 = 26{,}88 \text{ Mbits/s}$$

Les supports compatibles sont : le câble coaxial ou la fibre optique. La paire torsadée catégorie 5 peut être utilisée sur une distance inférieure à 500 m.

4.5 Débit nécessaire : $2 \times 16 \times 40 = 1\,280$ kbit/s. Tous les supports sont compatibles.

4.6

a) $T_1 = 300 \times 2^{20} \times 8/1\,024 \times 10^3 \approx 2\,458$ s ≈ 40 min 58 s

b) Nombre de blocs : $300 \times 2^{20}/1\,460 = 215\,461$

Pour chaque bloc, il faut rajouter 20 + 20 + 30 = 70 octets d'en-têtes

$$T_2 = 215\,461 \times (1\,460 + 70) \times 8/1\,024 \times 10^3 \approx 2\,575 \text{ s} \approx 42 \text{ min } 55 \text{ s}$$

c) Le temps peut être significativement allongé…

d) Il s'agit du débit sur la ligne, donc au niveau physique ou au niveau liaison lorsque le FAI spécifie par exemple qu'il s'agit du « débit ATM ». Le débit utilisateur obtenu au niveau de l'application, pour un transfert de fichier par exemple, peut être légèrement inférieur si le réseau est très fluide et que l'on ne tient compte que de la surcharge due aux en-têtes ou beaucoup plus faible si le réseau est encombré…

4.7

Tableau 4.5

Entités	Couche OSI
Modem ADSL	1-2
Câble Ethernet	1
E-mail	7
TCP	4
IP	3
Page web	7
Compression	6
Éléments binaires	1
Trame	2
Segment	4

4.8 Les couches basses se trouvent dans tous les équipements connectés sur le réseau, équipement terminal ou équipement d'interconnexion. Elles assurent la transmission et l'acheminement des informations à travers le réseau.

Les couches moyennes assurent le dialogue entre les équipements terminaux, indépendamment du (ou des) réseau(x) utilisé(s). Elles comportent les règles de transfert de l'information, de contrôle de flux et de l'intégrité des données transmises.

Les couches hautes définissent et traitent les données échangées (exécution de commandes, mise en forme, affichage…).

4.9 Les couches moyennes sont dites « de bout en bout » car elles assurent le dialogue entre les équipements terminaux, indépendamment du réseau ou de la route utilisée. Elles sont donc présentes sur les PC ou les serveurs mais ne sont pas gérées par les routeurs.

4.10 Pour chaque couche et donc chaque protocole associé, des informations de contrôle (PCI) sont ajoutées aux données issues de la couche supérieure (PDU). Cet ajout d'en-tête correspond à l'encapsulation : une nouvelle unité de données est formée et les données de la couche supérieure (SDU) sont alors sans signification pour la couche concernée. Les en-têtes contiennent des informations de contrôle relatives au protocole : par exemple, les adresses des stations source et destination pour le protocole IP défini sur la couche réseau.

4.11 La communication entre deux couches de même niveau est dite « horizontale et virtuelle » en référence au modèle OSI. Les échanges entre deux couches *N* sont réglés suivant le protocole *N* même si, physiquement, les informations échangées lors de ce dialogue transitent verticalement par les niveaux inférieurs, de système en système, en utilisant l'encapsulation/décapsulation.

4.12

a) La trame Ethernet est définie au niveau Liaison. Avec 46 octets de données, la trame minimum Ethernet comprend 64 octets.

b) 1 500 octets maximum de données peuvent être transportés dans une trame Ethernet. Ces données correspondent au paquet de niveau 3 encapsulé, donc au paquet IP.

c) Les champs de la trame Ethernet sont présents au début du relevé :

◇ `0800 2018 ba40` correspond à l'adresse destination sur 6 octets ;

◇ `aa00 0400 1fc8` correspond à l'adresse source sur 6 octets ;

◇ `0800` donne le type de protocole utilisé au niveau 3, en l'occurrence IP.

LES RÉSEAUX LOCAUX 5

PLAN

OBJECTIFS

- Connaître les topologies et les méthodes d'accès usuelles sur les réseaux locaux.
- Étudier l'architecture et les propriétés des réseaux Ethernet.
- Étudier les caractéristiques et les normes associées aux réseaux WiFi.
- Connaître les caractéristiques principales des réseaux Bluetooth.
- Étudier la technologie IEEE 802.15.4 et les réseaux associés ZigBee et 6LowPAN.

5.1 INTRODUCTION

Un réseau local ou **LAN** (*Local Area Network*) peut être défini comme l'ensemble des ressources téléinformatiques permettant l'échange à haut débit (100 kbit/s à 10 Gbit/s) de données entre équipements au sein d'une entreprise, d'une société ou de tout autre établissement.

Les équipements connectés sont variés : micro-ordinateurs, imprimantes, terminaux, serveurs, smartphones, tablettes, stations graphiques, matériel audio ou vidéo, automates pour les réseaux locaux industriels…

Le type et le volume des informations à transmettre, ainsi que le nombre d'utilisateurs simultanés, constituent la charge du réseau et vont déterminer le débit minimum nécessaire, et donc les types de support possibles (paire torsadée, fibre optique ou liaison sans fil).

Les besoins d'échange sont divers : consultation de bases de données, transfert de fichiers, partage de ressources, transmission de messages, contrôle de processus industriel par des stations réparties, échanges d'informations vidéo ou audio (streaming, vidéoconférence)… On peut ainsi distinguer deux types d'informations :

- **les informations de type informatique ou multimédia.** Il s'agit de fichiers textes, de fichiers programmes, de fichiers graphiques, de sons et d'images fixes ou animées dont le volume peut varier de quelques kilo-octets à quelques centaines de méga-octets. Pour ces informations, le trafic est **asynchrone**, les données sont transférées de façon irrégulière avec des débits variables ;
- **les informations de type temps réel.** Il s'agit principalement de la voix, de la vidéo dans le cadre du streaming ou de la VoD et du contrôle de processus industriel.

Ces informations doivent être transmises et traitées dans des délais fixés par l'application. Les trafics sont **synchrones** lorsqu'un débit moyen constant doit être garanti ou **isochrones** lorsque des transmissions à intervalles de temps constants sont nécessaires, par exemple pour la voix.

5.2 Topologie des réseaux locaux

Chaque équipement informatique est relié au support physique (paire torsadée, câble coaxial, fibre optique…) par l'intermédiaire d'un contrôleur de communication (généralement une carte d'interface réseau).

La topologie représente la manière dont les équipements sont reliés entre eux par le support physique. Elle est donc caractérisée par la figure géométrique que réalisent les liaisons établies entre les équipements. Les trois topologies possibles sont l'étoile, le bus et l'anneau. La topologie en étoile utilisée dans la technologie Ethernet est de loin la plus usuelle aujourd'hui.

5.2.1 Topologie en étoile

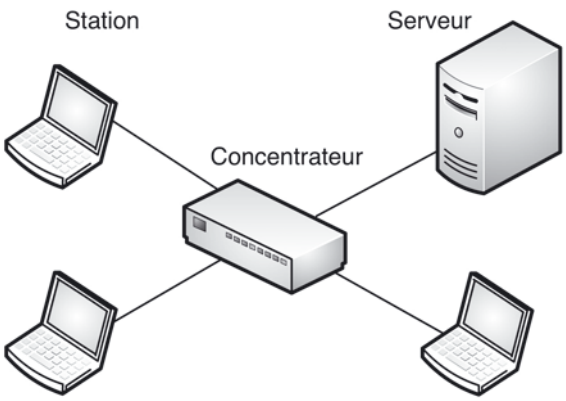


Figure 5.1 – **Topologie en étoile.**

Tous les équipements sont reliés directement à un concentrateur qui constitue le nœud central par lequel transitent toutes les transmissions (figure 5.1). Cette topologie permet d'ajouter aisément des équipements (un câble par équipement) dans la limite de la capacité du concentrateur.

La gestion du réseau se trouve facilitée par le fait que toutes les transmissions passent par le concentrateur. Par ailleurs, une défaillance d'un équipement terminal ne met pas en cause le fonctionnement du reste du réseau. En revanche, elle peut entraîner des longueurs importantes de câbles et, surtout, une panne sur le concentrateur immobilise tout le réseau.

Le câblage des réseaux récents Ethernet et des autocommutateurs privés (PABX) correspondent à cette topologie.

5.2.2 Topologie en bus

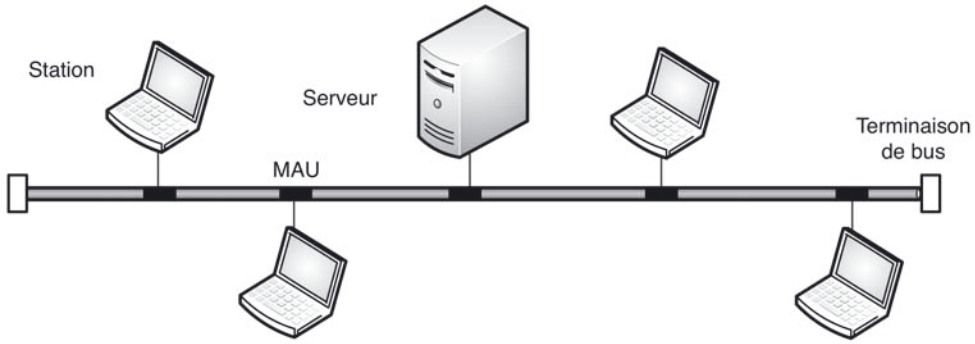


Figure 5.2 – **Topologie en bus.**

Chaque équipement est relié à un câble commun à tous, c'est une extension de la liaison multipoint (figure 5.2).

Sur câbles coaxiaux, les connexions au niveau du câble commun sont assurées par des unités de raccordement ou MAU (*Medium Attachment Unit*) passives limitant ainsi les risques de pannes. En revanche, sur fibres optiques, ces connexions sont le plus souvent réalisées par des équipements actifs.

Deux types de bus peuvent exister :

- **bus unidirectionnel :** les informations ne peuvent circuler que dans un sens et la transmission à toutes les stations est assurée par l'existence de deux canaux séparés (deux câbles distincts ou un seul câble et deux canaux multiplexés) ;
- **bus bidirectionnel :** les informations peuvent circuler dans les deux sens mais non simultanément sur un câble unique. Lorsqu'une station émet, le signal se propage dans les deux sens, de part et d'autre de la connexion, vers toutes les autres stations.

Cette topologie est économique en câblage. Dans le cas d'un support de type câble coaxial ou paire torsadée, elle permet facilement l'extension du réseau par ajout d'équipements (un câble et un connecteur par équipement) dans la limite de la

capacité de gestion du système d'exploitation. Si le support est de type optique, cette opération s'avère plus délicate, car elle nécessite la coupure de la fibre optique à l'endroit de la connexion.

En ce qui concerne la fiabilité, le dysfonctionnement d'une station ou d'un serveur ne met pas en cause le fonctionnement du reste du réseau. De même, en cas de rupture d'un câble ou de mauvais contact sur un connecteur, seul l'équipement connecté par ce câble sera privé des ressources du réseau (une panne sur un câble reliant deux équipements d'interconnexion de type commutateur affectera davantage de stations). La topologie en bus est celle adoptée par la plupart des réseaux locaux industriels.

Dans le cas particulier des architectures Ethernet (voir section 5.6), le câble coaxial utilisé dans les anciennes installations correspondait à une topologie en bus. Dans toutes les installations récentes, la paire torsadée plus simple à câbler et moins chère à fabriquer impose l'utilisation d'un concentrateur de câblage (*hub*), ou un commutateur (*switch*). La topologie « physique » est donc en étoile même si, d'un point de vue « logique », toutes les transmissions passent par un support commun, matérialisé par le hub (figure 5.3).

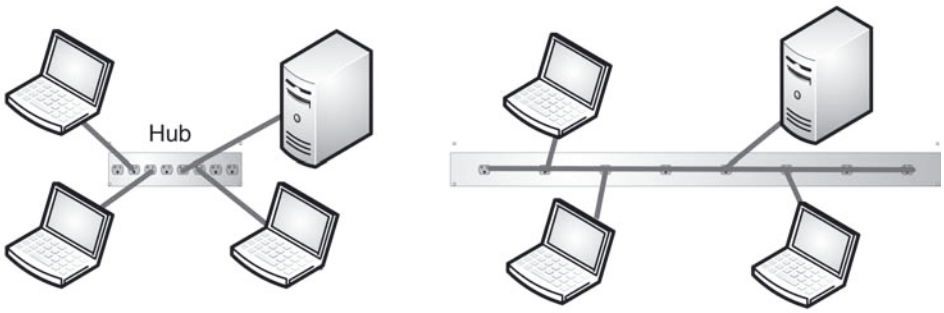


Figure 5.3 – **Topologie physique en étoile et topologie logique en bus.**

5.2.3 Topologie en anneau

Chaque équipement est relié à deux équipements voisins de telle sorte que l'ensemble constitue une boucle fermée (figure 5.4).

Dans cette topologie, les informations transitent d'équipement en équipement jusqu'à destination. Les MAU sont donc des éléments actifs chargés de recevoir les informations en provenance de la station précédente et de les retransmettre vers la station suivante.

L'insertion de nouveaux équipements sur l'anneau (un câble et un MAU par équipement) nécessite la coupure de l'anneau aux points d'insertion.

Deux événements peuvent bloquer le réseau dans son intégralité : une panne de l'un des MAU actifs, ou la rupture du câble en un point quelconque de l'anneau.

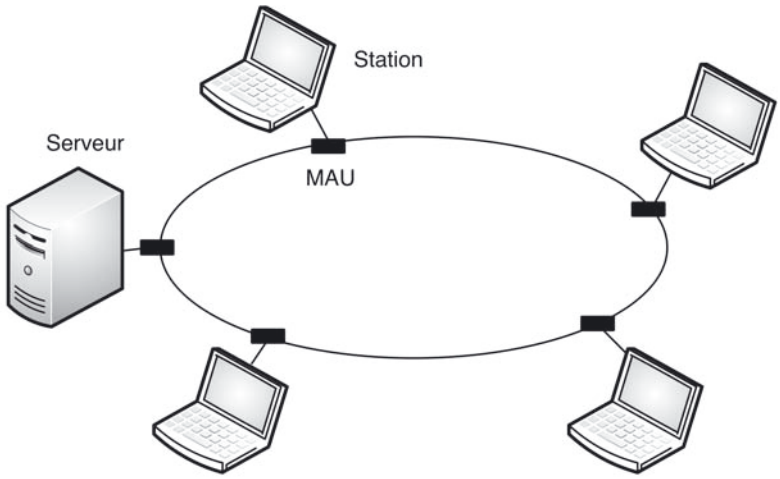


Figure 5.4 – **Topologie en anneau.**

Dans le premier cas, le fonctionnement partiel du réseau peut être assuré en court-circuitant le MAU en cause, la station associée est alors déconnectée. Dans le second cas, il est possible de limiter le blocage par l'utilisation d'un double anneau.

L'ancien réseau *Token Ring* initialement proposé par IBM et le réseau en fibre optique FDDI utilisent respectivement les topologies en anneau et double anneau.

5.3 Normalisation des réseaux locaux

Le transfert d'informations de l'émetteur vers le récepteur nécessite sur un réseau :

- la mise en forme des informations à émettre ;
- l'identification du récepteur ;
- le décodage par le récepteur des informations reçues ;
- l'annonce de la fin de transmission.

Il va de soi que si le récepteur ne connaît ni le format de l'information transmise, ni la méthode utilisée par l'émetteur pour lui signaler un envoi, il ne peut y avoir de transmission. Il s'avère donc indispensable d'établir un protocole de communication entre émetteurs et récepteurs d'un même réseau.

Pour réglementer l'émission d'une station sur le support, des protocoles ont donc été définis dans un premier temps sous l'égide de l'IEEE (*Institute of Electrical and Electronic Engineers*). Ces protocoles ont été repris et complétés par l'ISO (*International Standardization Organization*).

La correspondance entre les couches du modèle OSI (voir chapitre 4) et les sous-couches IEEE est représentée sur la figure 5.5. Les principales normes IEEE concernant les sous-couches LLC, MAC et PHY sont également évoquées.

La norme IEEE 802.2 correspondant à la sous-couche LLC (*Logical Link Control*) n'est pas liée à une architecture particulière ; elle offre des fonctionnalités d'ouverture et de fermeture de connexion, de contrôle de flux et de gestion des erreurs de transmission. Cette sous-couche est peu à peu abandonnée, ses fonctionnalités étant assurées par les couches supérieures, notamment la couche transport.

Les caractéristiques des sous-couches MAC et PHY et des normes associées (IEEE 802.3, 802.11, 802.15…) sont décrites dans l'étude des architectures Ethernet et sans fil. Les protocoles de niveau MAC (*Medium Access Control*) de l'architecture IEEE définissent essentiellement la méthode utilisée par une station pour accéder au support physique partagé ainsi que la structure de la trame associée.

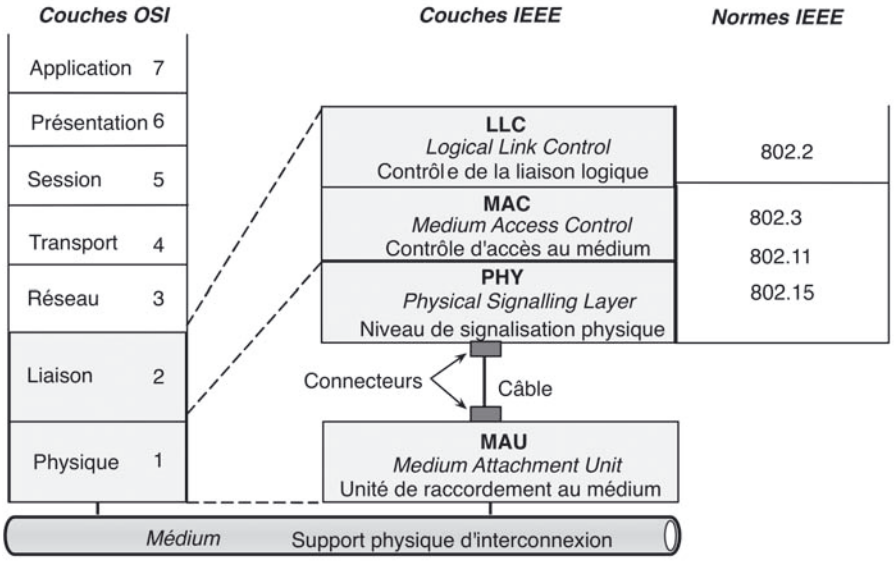


Figure 5.5 – **Correspondance OSI - IEEE.**

5.4 Méthodes d'accès

Plusieurs machines se partageant un même canal, un même support physique, il faut définir une méthode régissant les accès multiples à ce canal, plusieurs stations ne pouvant y accéder simultanément. Cette méthode est implémentée au niveau de la couche MAC. Il existe différentes méthodes, plus ou moins équitables vis-à-vis des possibilités d'accès au support.

La figure 5.6 présente une classification de ces méthodes. D'autres classifications existent suivant le caractère statique ou dynamique de l'allocation ou encore en distinguant accès par consultation et accès par compétition.

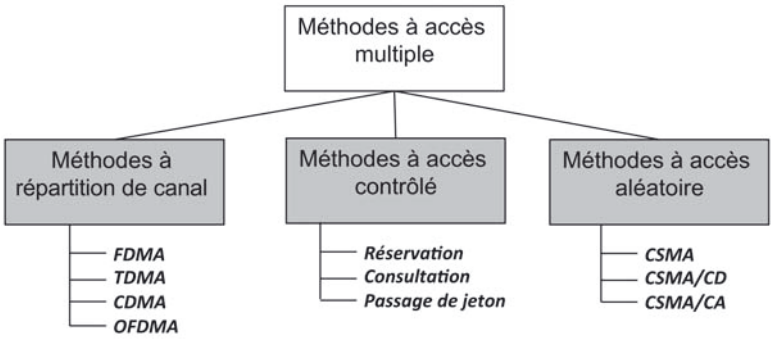


Figure 5.6 – **Classification des méthodes d'accès au canal.**

5.4.1 Méthodes à répartition de canal

Les méthodes de type **FDMA** (*Frequency Division Multiple Access*) et **TDMA** (*Time Division Multiple Access*) sont basées sur les multiplexages fréquentiels (FDM) et temporels (TDM) décrits au chapitre 3. Chaque équipement peut donc bénéficier à un instant donné d'une sous-bande de fréquence ou d'un intervalle de temps dans la trame, les communications simultanées sont donc possibles. Les accès multiples **CDMA** (*Code Division Multiple Access*) et **OFDMA** (*Orthogonal Frequency Division Multiple Access*) sont notamment utilisés dans le cadre de la téléphonie cellulaire et sont décrits dans le chapitre 7.

5.4.2 Méthodes à accès contrôlé

Ces méthodes sont caractérisées par une allocation dynamique, à la demande, de la bande passante. Ces méthodes sont souvent considérées comme déterministes car, si l'on connaît la séquence d'accès des stations et éventuellement leurs priorités, il est possible de prévoir les temps d'attente et de transmission pour chaque station.

Dans le contrôle centralisé par **réservation**, utilisé notamment dans les réseaux IEEE 802.15.4, une trame spécifique est échangée avant le début des transmissions de données pour que les stations esclaves puissent effectuer une réservation vers le maître.

Dans l'exemple illustré figure 5.7, les stations 1, 3 et 4 (cinq stations en tout) ont effectué une réservation dans la première trame. L'en-tête généré par le maître permet de spécifier quelles sont les réservations. Dans la deuxième trame, seule la station 1 transmet des données.

Dans le contrôle centralisé par **consultation** ou par **scrutation** (*polling*), c'est la station maître, ou station primaire, qui gère l'accès au support :

- elle sollicite les stations secondaires (esclaves) concernées pour envoyer ses propres données (figure 5.8a) ;
- elle invite les esclaves à émettre en leur envoyant une proposition (*poll*) selon un ordre établi dans une table de scrutation (figure 5.8b).

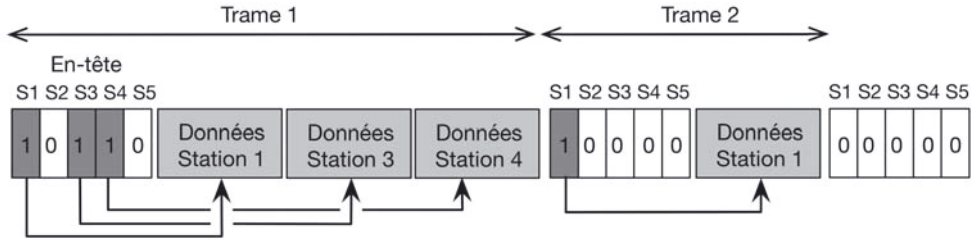


Figure 5.7 – **Exemple de réservation.**

Le maître peut être défini une fois pour toutes (contrôle centralisé) ou chaque esclave peut devenir maître à un instant donné (contrôle distribué).

Cette méthode est utilisée notamment dans les réseaux Bluetooth.

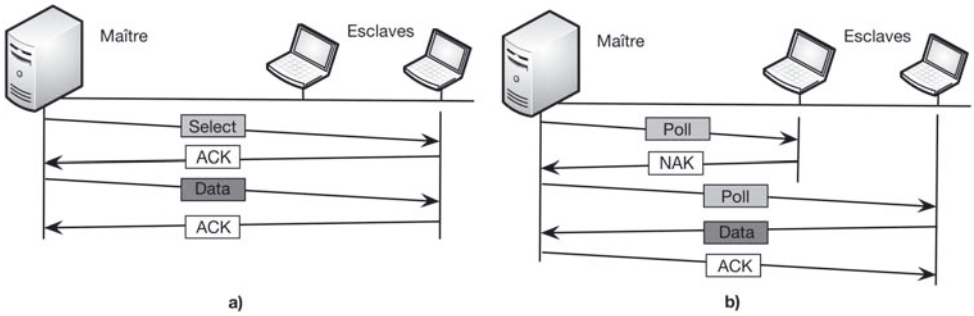


Figure 5.8 – **Exemple de scrutation.**

Les **méthodes à jeton** sont basées sur la circulation d'une trame vide de station en station contenant le jeton (*token*). Une station souhaitant émettre « prend » le jeton (changement d'état du bit correspondant), et émet sa trame. Des priorités ou des réservations peuvent être ajoutées. Ces méthodes sont liées à une topologie en anneau peu performante et sont très peu utilisées.

5.4.3 Méthodes à accès aléatoire

Les stations peuvent transmettre à tout moment, donc de manière aléatoire du point de vue de l'ensemble du réseau, mais avec des risques de collision (plusieurs trames peuvent être émises simultanément sur le support partagé). Plusieurs variantes existent pour limiter ou résoudre les collisions.

Le protocole **CSMA** (*Carrier Sense Multiple Access*) limite grâce à l'écoute le risque de collision : une station désirant émettre commence par « écouter » le support pour détecter une transmission en cours (*Carrier Sense*) ; la station transmet sa trame dès qu'elle ne détecte plus de signaux sur le support.

Le protocole **CSMA/CD** ajoute une détection de collision : si, malgré l'écoute du support, une collision intervient, les stations sont capables de la détecter (*Collision Detection*) et de relancer une transmission après un temps d'attente aléatoire. Ce protocole utilisé dans les réseaux Ethernet est décrit dans le paragraphe suivant.

Contrairement aux transmissions sur un support filaire, l'émission et la réception simultanée sont impossibles sur un support sans fil. Une station en émission ne peut donc pas détecter une collision. Le protocole **CSMA/CA** utilisé notamment sur les réseaux WiFi est basé sur l'évitement de collision (*Collision Avoidance*) : lorsqu'une station détecte un support libre, la station anticipe et commence par attendre un temps aléatoire pour éviter les risque d'émissions simultanées.

La fonction principale des protocoles d'accès au support est donc d'autoriser une seule station à émettre ses trames sur le support physique partagé. Les méthodes assurant cette fonction sont liées à la topologie du réseau. Quatre des méthodes définies par les normes 802 de l'architecture IEEE sont résumées dans le tableau 5.1.

Tableau 5.1 – Normes IEEE 802.

Norme	802.3	802.11	802.15.1	802.15.4
Méthode d'accès	CSMA/CD (compétition)	CSMA/CA (compétition)	TDMA (sélection)	TDMA et CSMA/CA
Type	Aléatoire	Aléatoire	Déterministe	Déterministe et aléatoire
Exemple	Ethernet	WiFi	Bluetooth	ZigBee

Certaines de ces méthodes permettent de prévoir et de calculer avec exactitude l'instant où une station aura accès au support, ces méthodes sont dites **déterministes**. Les autres, pour lesquelles l'instant d'accès au support ne peut être déterminé que d'une manière probabiliste, sont dites **aléatoires** ou non déterministes.

5.5 L'architecture Ethernet

5.5.1 Caractéristiques principales

Mise au point dans les années 1980 par Xerox, Intel et DEC, l'architecture Ethernet permet l'interconnexion de matériels divers avec de grandes facilités d'extension, les caractéristiques principales sont :

- débit de 10 Mbit/s à 10 Gbit/s ;
- transmission en bande de base, codage Manchester ;
- topologie en étoile (en bus sur les anciens réseaux) ;
- méthode d'accès suivant la norme IEEE 802.3 (CSMA/CD) ;
- longueur des trames comprise entre 64 et 1 518 octets ;

- support de type câble coaxial, paire torsadée ou fibre optique ;
- gestion des couches 1 et partiellement 2 du modèle OSI (sous-couches PHY et MAC) ;

Les fonctionnalités d'Ethernet correspondent donc aux deux sous-couches PHY et MAC définies par la norme IEEE 802.3 en liaison avec le support *via* l'unité de raccordement MAU (figure 5.9).

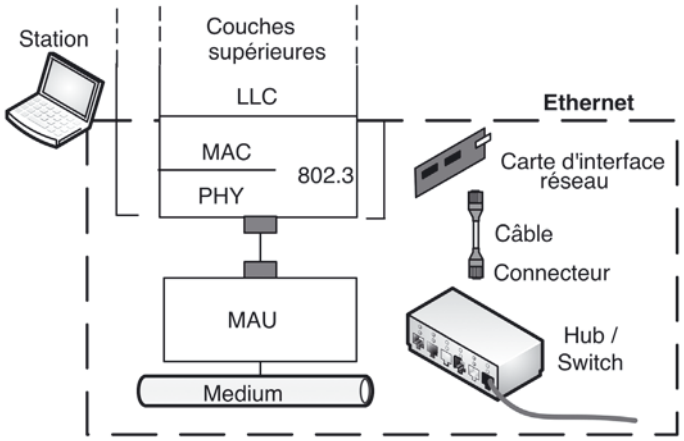


Figure 5.9 – **Fonctionnalités d'Ethernet.**

5.5.2 Méthode d'écoute de la porteuse : CSMA/CD

Dans la méthode d'accès aléatoire CSMA (*Carrier Sense Multiple Access*), plusieurs stations peuvent tenter d'accéder simultanément au support (*Multiple Access*).

Cette possibilité d'accès multiple impose pour chaque station l'écoute et la détection du signal sur le réseau (*Carrier Sense*). Elle utilise une topologie logique en bus, le support peut être une paire torsadée, un câble coaxial, ou une fibre optique suivant le débit souhaité et la longueur du bus.

Une station ayant des trames à émettre, détecte au préalable la présence ou non d'un signal sur le bus. Dans l'affirmative, cela signifie qu'une station est en train d'émettre, elle diffère son émission. Dans la négative, elle transmet sa trame.

Cette technique n'évite pas les collisions. En effet, dans l'exemple décrit figure 5.10, à l'instant t_0, le canal étant libre, la station A transmet sa trame. À l'instant $t_0 + T/5$ (T représentant le temps de propagation maximum d'une extrémité à l'autre du réseau), la station B ne détectant pas de porteuse, émet sa trame. Les deux trames se rencontrent à l'instant $t_0 + 5T/10$. Il y a collision et les trames sont altérées, donc perdues.

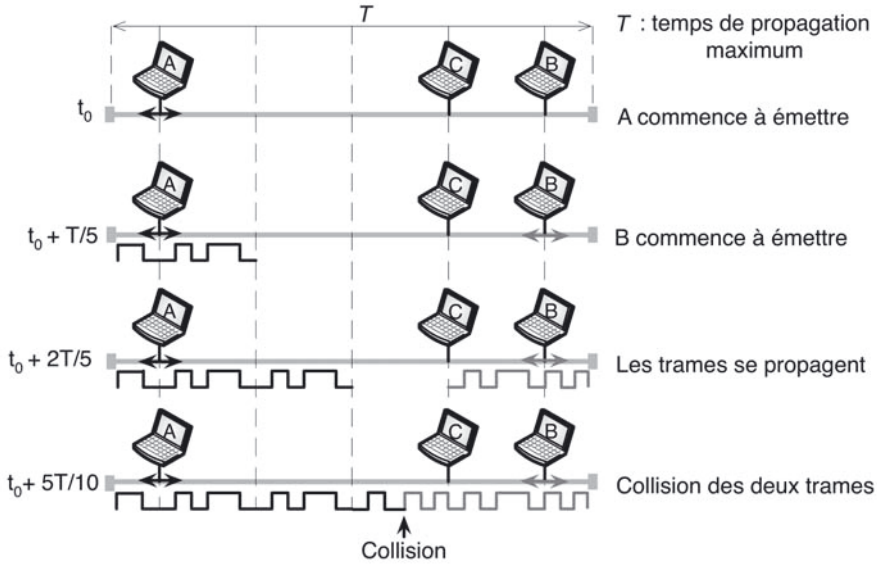


Figure 5.10 – **CSMA – collisions non détectées.**

Pour diminuer les pertes de trames, la norme prévoit une détection des collisions (CSMA/CD : *Carrier Sense Multiple Access with Collision Detection*). Une fois sa trame émise, la station écoute le support pendant un temps au moins égal au double du temps mis par la trame pour se propager jusqu'au point le plus éloigné du bus (si une collision intervient en ce point, il faut ajouter au temps de propagation de la trame le temps mis par la trame altérée pour revenir et être détectée).

Au bout de ce temps, deux cas peuvent se présenter :

- la trame émise n'est pas altérée, il n'y a pas eu de collision. La station peut poursuivre sa transmission (figure 5.11) ;
- la station détecte une trame altérée car les niveaux de tension mesurés sur l'interface sont erronés, il y a eu collision (figure 5.12). La station reprend la transmission de cette trame après un temps d'attente aléatoire (voir paragraphe 5.5.4).

Le temps de transmission d'une trame doit être supérieur au double du temps de propagation entre les deux points les plus éloignés du réseau, car pour qu'une station puisse détecter une collision, c'est-à-dire recevoir une trame altérée, il faut qu'elle soit en émission.

Il n'est pas nécessaire d'avoir une station de contrôle du support (superviseur). En revanche, il est clair que le nombre de collisions augmente avec le nombre de stations voulant émettre, pouvant même conduire à une saturation du support. Le nombre de réémissions des trames augmentant, le débit réel diminue (nombre d'informations binaires arrivant à destination par unité de temps). Par contre, lorsque le nombre de stations voulant émettre est faible, cette méthode réduit les temps d'attente.

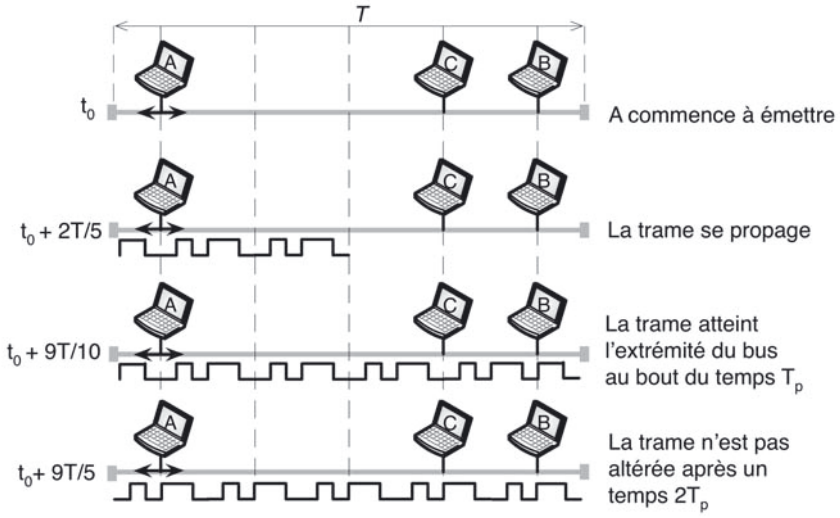


Figure 5.11 – **CSMA/CD – pas de collision.**

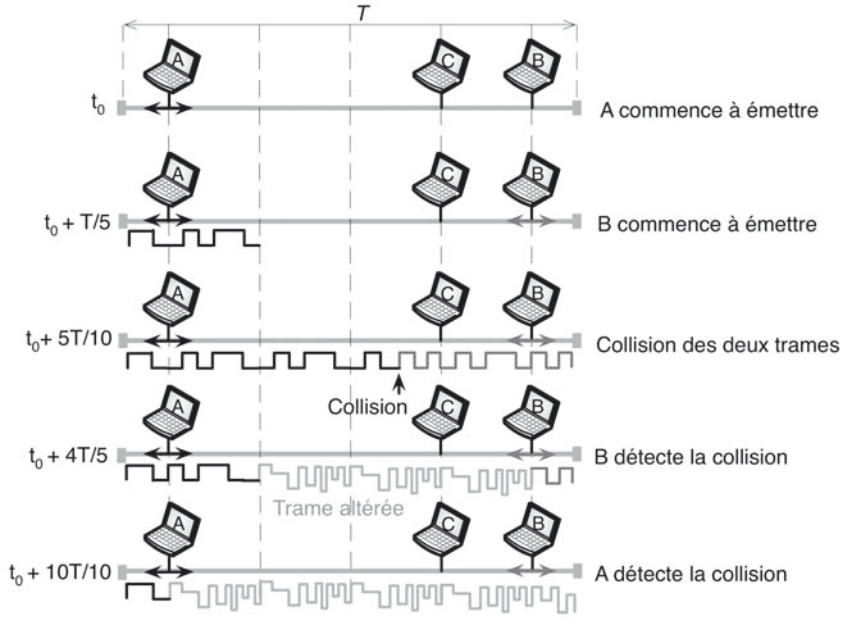


Figure 5.12 – **CSMA/CD – détection d'une collision.**

5.5.3 L'Ethernet commuté

Sur les anciens réseaux Ethernet en câble coaxial, la station était directement reliée au réseau par l'intermédiaire d'un connecteur. Pour des liaisons sur paires torsadées (10BaseT, 100BaseT ou 1000BaseT) ou sur fibre optique (100BaseF ou 1000BaseF), il est nécessaire d'utiliser des équipements d'interconnexion spécifiques : *hub* ou *switch*.

Le rôle du ***hub*** consiste à assurer la communication entre les stations comme si elles étaient reliées à un bus bien que physiquement la topologie soit de type étoile. Il intervient donc uniquement au niveau de la couche 1 du modèle OSI. Pour augmenter le nombre de connexions, les *hubs* (généralement 8, 12, 16 ou 24 ports) peuvent être mis en cascade. Toutes les machines reliées par ces *hubs* font partie du même domaine de collision. Il s'agit donc d'un **Ethernet partagé** dans lequel les performances peuvent être rapidement dégradées en cas de fort trafic. Les *hubs* sont peu à peu abandonnés au profit des ***switchs*** qui permettent un **Ethernet commuté.**

Le commutateur Ethernet ou ***switch*** possède les mêmes fonctionnalités que le *hub* et permet en plus de regrouper dans un même segment les stations liées par des trafics importants (plusieurs serveurs sur une dorsale ou un serveur et des stations d'un même groupe de travail) et augmente ainsi la bande passante du réseau (figure 5.13). Le *switch* intervient au niveau des couches 1 et 2. Chaque port à 10, 100 Mbit/s ou 1 Gbit/s fait partie d'un seul domaine de collision et apprend dynamiquement les adresses MAC des équipements qui lui sont connectés.

Un *switch* peut donc être considéré comme une matrice de connexion qui permet d'interconnecter simultanément des segments ou des appareils fonctionnant éventuellement à différents débits. Il possède un *buffer* circulaire interne travaillant entre 1 et 10 Gbits/s qui distribue les paquets entrants aux ports de destination s'il y a concordance avec l'adresse apprise dynamiquement par celui-ci.

Certains *switchs* reconnaissent automatiquement les ports 10 Mbit/s, 100 Mbit/s et 1 Gbit/s (*auto sensing*) et sont configurables à l'aide d'un protocole standard, généralement SNMP (*Simple Network Management Protocol*). La configuration

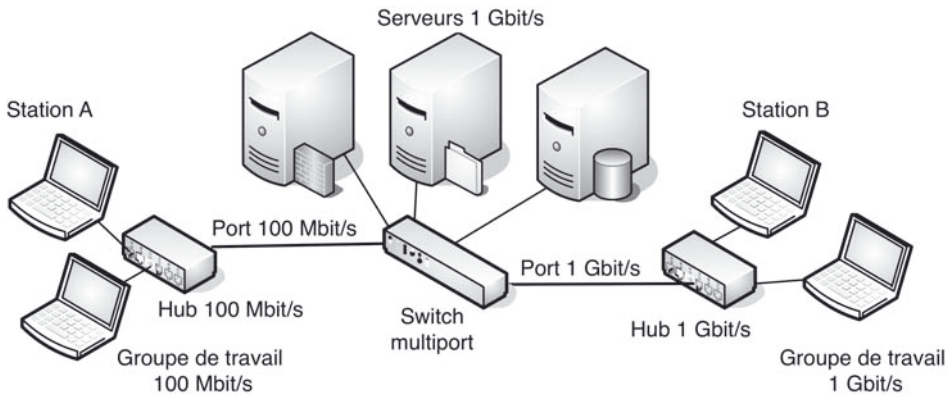


Figure 5.13 – Exemple de réseau Ethernet commuté.

n'est pas forcément nécessaire dans la mesure où les *switchs* gèrent dynamiquement les adresses MAC, elle peut cependant permettre de relier ou d'isoler des ports particuliers pour réaliser des réseaux locaux virtuels (voir section 5.6, les VLAN).

Dans la figure 5.13, la station A qui veut émettre vers la station B envoie une trame avec son adresse source et l'adresse destination de B. Le *switch* lit l'adresse destination et commute la trame sur le port de sortie approprié dans la mesure où il a appris dynamiquement toutes les adresses MAC des machines connectées sur ses ports. Dans l'exemple, les stations B et C sont connectées sur le même port du *switch*, par l'intermédiaire d'un *hub*. Pour que la commutation soit possible, il faut au préalable que la station B ait généré du trafic pour que le *switch* ait eu l'occasion d'apprendre son adresse. Par ailleurs, pour que la station A connaisse l'adresse de B, il faut au préalable qu'elle ait envoyé une requête à destination de tous les équipements du LAN (trame de diffusion). Cette requête doit être relayée par le *switch*, seule la station B répond (voir protocole ARP au paragraphe 6.3.1).

L'Ethernet commuté tant à prendre la place de l'Ethernet partagé conçu à l'origine. Le prix et les performances des *switchs* permettent de s'orienter vers un réseau totalement commuté en utilisant un port par machine connectée et donc d'éviter totalement les collisions.

Différentes techniques de commutation existent :

a) Commutation « *On the Fly* » ou « *Cut through* »

À l'arrivée de la trame, le commutateur lit seulement l'en-tête et commute la trame vers le port de sortie en fonction de l'adresse de destination. Les principaux avantages sont un temps de latence très faible (de l'ordre de 1 µs à 100 Mbit/s) et une commutation indépendante de la longueur de la trame. Parmi les inconvénients, on note la retransmission des erreurs (CRC, fragments de collision) et l'impossibilité de commuter entre un port 10 Mbit/s et un port 100 Mbit/s.

b) Commutation « *Store and Forward* »

Dans ce cas, la trame est stockée avant sa commutation sur le port de sortie. Cette technique permet le traitement des erreurs et est adaptée aux commutations 10/100 Mbit/s. En revanche, les temps de latence sont plus importants et fonction de la longueur de la trame.

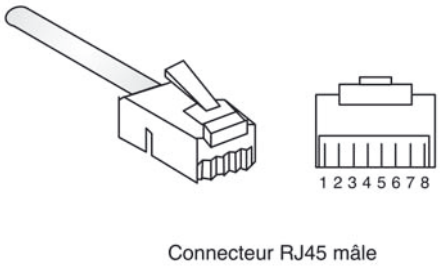
5.5.4 Normes et débits sur Ethernet

a) La connectique

La liaison en 10BaseT, 100BaseT ou 1000BaseT au *hub* ou au *switch* est réalisée par des connecteurs à huit contacts de type RJ45 (figure 5.14) et par des câbles de différentes catégories suivant le débit, seules deux paires torsadées par câble sont utilisées : une pour l'émission et une pour la réception. La communication bidirectionnelle entre deux stations nécessite que la paire d'émission de l'une (paire 2) soit reliée à la paire de réception de l'autre (paire 3) et réciproquement. Pour relier directement deux

stations, il faut donc inverser les fils sur l'un des connecteurs (paire 2 vers paire 3 et inversement), il s'agit alors d'un câble croisé. Pour éviter cette inversion qui complique le câblage, les équipements d'interconnexion (*hub*, *switch*, routeur) réalisent en interne le croisement et un câble droit peut être utilisé pour relier la station à l'équipement.

Par ailleurs, seul le câble de catégorie 5 non blindé (UTP, *Unshielded Twisted Pairs*) ou blindé (STP, *Shielded Twisted Pairs*) permet d'atteindre des débits de 100 Mbit/s ou 1 Gbit/s dans certains cas particuliers. Les câbles plus performants de catégorie 6a permettent d'atteindre les débits de 10 Gbit/s définis par la norme 10GBaseT.



Broche	Signal	Paire
1	TD+	1 Emission
2	TD-	
3	RD+	2 Réception
6	RD-	
4		3
5		
7		4
8		

Figure 5.14 – **Connecteur et câblage RJ45.**

b) Fast Ethernet (100 Mbit/s) – 100BaseT (802.3u)

Directement dérivée du 10BaseT, cette norme reprend la méthode d'accès CSMA/CD avec un codage 4B/5B (représentation sur 5 bits d'une série de 4 bits) et NRZI.

Elle reprend également le câblage avec trois variantes :

- 100BaseTX utilise un connecteur RJ45 et un câble à deux paires de catégorie 5 ;
- 100BaseT4 utilise un connecteur RJ45 et un câble à quatre paires de catégorie 3, 4 ou 5.
- 100BaseFX utilise un câble duplex fibre optique multimode.

Les longueurs maximales des segments sont de 100 m en paire torsadée et 2 km en fibre.

Une des particularités des liaisons point à point 100BaseTX est de pouvoir exploiter le mode *full duplex* en utilisant simultanément la paire dédiée à l'émission et la paire dédiée à la réception. Cette solution nécessite une modification minime des cartes d'interface (inhibition de la détection de collision au niveau de la couche MAC) et n'ajoute aucune nouvelle contrainte sur le câblage. C'est l'équipement d'interconnexion, un commutateur capable de gérer cette fonctionnalité, qui a alors la charge de traiter l'arrivée de plusieurs trames simultanément. Ce fonctionnement en *full duplex* offre donc une bande passante théorique de 200 Mbit/s (100 Mbits/s en émission et 100 Mbits/s en réception).

c) Fast Ethernet (100 Mbit/s) – 100BaseVG (802.12)

La méthode CSMA/CD est abandonnée au profit d'une demande d'émission de la station au *hub*. Ce dernier autorise les stations à émettre à tour de rôle (*Polling Round Robin*), évitant ainsi les pertes de temps dues aux collisions et retransmissions. Deux niveaux de priorité garantissent des niveaux de service pour les applications critiques. Le câblage utilise des paires torsadées non blindées de type 3, 4 ou 5, équipées de connecteurs RJ45 ou des fibres optiques. L'émission se fait par quartet sur 4 paires (soit 25 Mbit/s par paire) avec un codage de type NRZ-5B6B.

d) Gigabit Ethernet (1 Gbit/s)

Dérivé directement de *Fast Ethernet* et compatible avec ce dernier, le *Gigabit Ethernet* est destiné dans un premier temps à remplacer les commutateurs 10 ou 100 Mbit/s sur une dorsale. Il fait l'objet d'une normalisation IEEE 802.3z pour support en fibre optique ou paires torsadées (1000BaseSX, 1000BaseLX et 1000BaseCX). Une autre norme (IEEE 802.3ab) permet d'utiliser des câbles en cuivre de catégorie 5 (1000BaseT) sur des distances plus importantes (100 m) à l'aide d'un codage spécifique sur 4 paires.

Dans tous les cas, le Gigabit Ethernet est commuté en *half duplex* ou *full duplex*.

e) Ethernet 10 Gbit/s

L'Ethernet 10 Gbit/s est utilisé pour la connexion de serveurs gérant des grands flux de données, comme les serveurs de sauvegarde ou pour raccorder un LAN sur la boucle locale vers Internet.

Cette norme fonctionne en *full duplex* uniquement et essentiellement sur fibre optique bien que les câbles en paire torsadée de catégorie 6a soient compatibles.

5.5.5 La sous-couche MAC

La sous-couche MAC gère l'accès au support selon les principes CSMA/CD de la norme IEEE 802.3 et offre un ensemble de services à la couche réseau.

a) Trame 802.3

Le bloc d'information ou trame (MAC PDU : MAC *Protocol Data Unit*) est composé de huit champs (figure 5.15) :

- le préambule, composé de 7 octets formés d'une succession de 0 et de 1, assure la synchronisation du récepteur sur la trame émise ;
- le délimiteur de début de trame permet de trouver le début du champ des adresses ;
- les adresses destination et source sur 6 octets caractérisent l'interface réseau. Chaque carte possède une adresse unique appelée parfois adresse physique ou adresse MAC, les trois octets de poids forts identifient le constructeur ;
- le nombre d'octets de données provenant de la sous-couche LLC. Si cette dernière n'est pas utilisée (cas des trames Ethernet II), le champ longueur est remplacé par

le champ « type » qui donne la nature du protocole utilisé au niveau supérieur (par exemple 0800_H pour le protocole IP) ;
- des bits de « bourrage » si la longueur de la trame est inférieure à la limite imposée par la norme ;
- une somme de contrôle (*Frame Check Sequence*) calculée suivant un code de redondance cyclique (CRC).

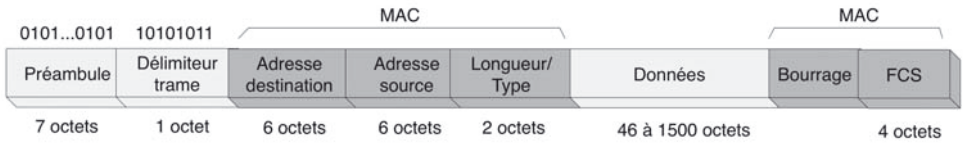


Figure 5.15 – Structure de la trame 802.3.

La norme 802.3 fixe également les valeurs par défaut des principaux paramètres de fonctionnement :
- temps de base (*slot time*) égal à la durée d'émission de 512 bits (ce temps sert de base aux différents temporisateurs utilisés) ;
- temps inter-trames de 9,6 µs pour des débits de 10 Mbit/s ou de 0,96 µs pour des débits de 100 Mbit/s ;
- nombre maximal de retransmissions égal à 16 ;
- tailles minimale et maximale des trames respectivement de 64 octets et 1 518 octets.

Notons que la taille minimale de la trame est calculée pour la première version de la norme IEEE 802.3 (10Base5) qui spécifiait une longueur maximale L de 2,5 km, une vitesse de propagation v de 230 000 km/s et un débit D de 10 Mbit/s. Rappelons que, pour pouvoir détecter une collision au point le plus éloigné du réseau, la station doit être en émission. La durée d'émission de la plus petite trame N_{min} doit par conséquent être égale au double du temps de propagation T_p au point le plus éloigné. Il faut donc résoudre l'équation :

$$2T_p = 2\frac{L}{v} = \frac{N_{min}}{D}$$

Le calcul donne une valeur de N_{min} de 217 bits, ce qui est inférieur aux 512 bits (64 octets) choisis pour la norme initiale.

Le problème se pose pour les débits plus importants des nouvelles normes : pour un débit de 100 Mbit/s, il faut diviser par 10 la longueur L du réseau, soit L = 250 m, si l'on conserve N_{min} = 512 bits.

Pour le Gigabit Ethernet, il faudrait réduire la longueur à 25 m. La solution retenue est de conserver des longueurs de 200 m (on parle de diamètre de collision de 200 m car le Gigabit Ethernet est commuté), ce qui impose de multiplier par un facteur 8 (8 × 25 = 200) le nombre de bits à émettre. La trame minimale passe donc à 512 octets (8 × 64) pour pouvoir détecter la collision. Plutôt que d'ajouter des bits de bourrage et de reformater les trames à chaque changement de débit, la technique d'extension de porteuse (*Carrier Extension*) est utilisée. Cette technique spécifie un

ajout de bits après le FCS pour atteindre si nécessaire 512 octets ; la trame Ethernet n'est donc pas modifiée et l'extension peut être enlevée lors du passage sur un segment à 100 Mbit/s.

Pour les modes *full duplex* du Gigabit Ethernet et du 10 Gigabits, les collisions ne peuvent avoir lieu et la taille initiale de trame peut être conservée.

b) Fonctions 802.3

Pour décrire les fonctionnalités de la sous-couche MAC, trois fonctions peuvent être distinguées : émission, réception et traitement des collisions.

- *Fonction émission*

À la réception d'une demande d'émission provenant de la couche supérieure, généralement la couche réseau, cette fonction doit :

- lire un bloc de données provenant de la couche réseau ;
- lire l'adresse de destination transmise par la couche réseau ;
- fabriquer la trame (adresses, longueur des données, données, CRC) ;
- attendre l'indication d'absence de porteuse provenant de la sous-couche PHY ;
- émettre la trame ;
- indiquer le succès de la transmission à la couche réseau ou, le cas échéant, traiter la collision signalée par la sous-couche PHY.

Ces séquences sont répétées jusqu'à ce que toutes les données soient transmises. Pour cela, les blocs de données sont retirés de la file d'attente de la couche réseau au fur et à mesure de la transmission des trames.

- *Fonction réception*

La lecture des trames passant sur le support est effectuée en permanence. Lorsqu'une trame est lue, la fonction réception exécute les séquences suivantes :

- lecture de la trame ;
- décodage de l'adresse de destination ;
- comparaison de celle-ci et de l'adresse de la station ;
- si les deux adresses sont identiques :
  - ◇ vérification du CRC ;
  - ◇ vérification de la longueur de trame ;
  - ◇ envoi d'un état de réception à la couche réseau ;
  - ◇ si le CRC et la longueur sont valides :
    - – communication des données à la couche réseau ;
    - – communication de l'adresse source à la couche réseau.

- *Fonction traitement de collisions*

Dans le cas où une indication de collision est transmise par la sous-couche PHY, la sous-couche MAC doit, dans un premier temps, transmettre une séquence de bourrage (*jam*) permettant de prolonger la collision pour que toutes les stations en émission puissent la détecter.

La sous-couche MAC doit ensuite tenter de retransmettre la trame après un délai d'attente aléatoire T_a déterminée par l'algorithme BEB (*Binay Exponential Backoff*) :

$$\text{si } N \leq 16 \text{ alors } T_a = R \times T_b$$

- N : nombre de tentatives de retransmission déjà effectuées ;
- R : nombre aléatoire tel que $0 \leq R \leq 2^k$ avec $k = \min(N, 10)$;
- T_b : temps de base ;
- N est initialisé à 1 et incrémenté à chaque tentative échouée. Si $N > 16$, la retransmission est ajournée et un rapport d'anomalie est communiqué à la couche supérieure.
- La borne supérieure 2^k utilisée pour le tirage du nombre aléatoire R est doublée à chaque tentative (*Binary Exponential*), ce qui limite la probabilité pour qu'une autre station tire le même nombre.

Le temps de base est égal au temps nécessaire pour émettre les 64 octets (512 bits) de la trame la plus courte, soit $T_b = 51{,}2$ µs à 10 Mbit/s et $T_b = 5{,}12$ µs à 100 Mbit/s. Ce temps correspond au temps de propagation aller et retour entre les deux points les plus éloignés du réseau.

5.6 Les VLAN Ethernet

Les réseaux locaux virtuels (VLAN : *Virtual Local Area Network*) permettent de regrouper des machines (serveurs, stations imprimantes…) en se basant sur l'organisation de l'entreprise plutôt que sur la localisation géographique. Certains PC d'un bureau situé au deuxième étage d'une entreprise pourront ainsi faire partie du même réseau local, qui devient alors virtuel car sans appartenance à un lieu précis, que d'autres PC localisés au premier étage. L'objectif étant de regrouper les utilisateurs ou les ressources qui communiquent le plus fréquemment indépendamment de leur emplacement ; l'aspect sécurité peut également être un facteur de regroupement.

Le concept de ces réseaux locaux virtuels repose sur la définition de domaines de diffusion (domaines de *broadcast*) indépendamment de l'endroit où se situent les systèmes. Il suffit d'indiquer au niveau des commutateurs (*switchs*) quelles sont les machines censées communiquer entre elles à l'exclusion des autres.

L'organisation des réseaux virtuels consistera donc à définir sur les différents commutateurs quels sont les ports correspondant aux différents VLAN. Il existe ainsi plusieurs niveaux de VLAN.

a) VLAN de niveau 1

Les VLAN de niveau 1 ou VLAN par port (*Port-Based VLAN*) regroupent les stations connectées en se basant sur les numéros de port des commutateurs. Quand une trame arrive sur le commutateur, celui-ci détermine le VLAN à partir du port d'arrivée. L'avantage est la simplicité : quand un utilisateur se déplace vers un autre port, il suffit d'affecter son VLAN au nouveau port, le changement est transparent

pour l'utilisateur. L'inconvénient est la nécessité pour l'administrateur de gérer manuellement les changements.

b) VLAN de niveau 2

Les VLAN de niveau 2 ou VLAN MAC (*MAC Address-Based VLAN*) associent les stations aux VLAN par leurs adresses MAC selon des tables de correspondance introduites par l'administrateur (figure 5.16). Lorsque le commutateur reçoit une trame sur un port, il analyse l'adresse source puis parcourt la table MAC/VLAN pour associer la trame à un VLAN. Il analyse ensuite l'adresse destination de la trame et parcourt à nouveau la table MAC/VLAN. Si l'adresse MAC appartient au même VLAN, il parcourt la table MAC/Port (gérée dynamiquement). Si l'association existe, il transmet la trame sur le port ; si elle n'existe pas, il transmet la trame sur tous les ports associés au VLAN. Si l'adresse destination n'appartient pas au même VLAN, il ne transmet pas la trame (cas théoriquement impossible car le PC ne peut obtenir l'adresse MAC d'une carte ne se trouvant pas sur son VLAN). Contrairement à un VLAN de niveau 1, aucune modification n'est nécessaire quand un utilisateur se déplace vers un autre port : son adresse MAC reste associée au même VLAN.

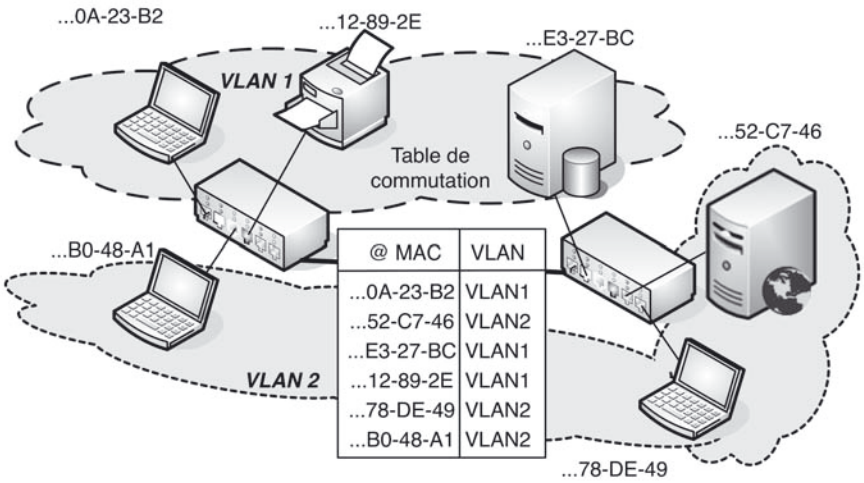


Figure 5.16 – Exemple de commutation dans des VLAN de niveau 2.

Les VLAN de niveau 2 qui s'étendent sur plusieurs commutateurs peuvent être de deux types :

- les VLAN implicites : lorsqu'une trame passe d'un commutateur à un autre, la table de correspondance MAC/VLAN partagée indique au commutateur d'arrivée à quel VLAN, et donc à quel port, le message doit être communiqué (figure 5.18) ;
- les VLAN explicites ou « taggés » : une étiquette (tag ou VLAN ID) d'appartenance à un VLAN est apposée sur chaque trame Ethernet. Cette dernière est commutée sur le port concerné. Dans la mesure où les étiquettes permettent

d'aiguiller les trames entre les commutateurs, ce sont ces derniers qui ajoutent les étiquettes et les retirent avant de délivrer les trames aux PC. Cette solution est intéressante lorsque les trames sont amenées à traverser de nombreux commutateurs. Dans ce cas, le temps mis pour gérer les étiquettes en entrée et en sortie est rentabilisé par rapport à un VLAN implicite où les tables de commutation sont consultées à chaque passage dans un commutateur.

Les VLAN niveau 1 ou 2 peuvent également regrouper des stations WiFi par l'intermédiaire de commutateurs reliés à des points d'accès WiFi ou intégrant ces derniers.

c) VLAN de niveau 3

Les VLAN de niveau 3 ou VLAN d'adresses réseaux (*Network Address-Based VLAN*) regroupent les stations par leurs adresses IP (un ensemble d'adresses ou une adresse de sous-réseau). Dans ce cas, le principe de la modélisation OSI n'est pas respecté car le commutateur doit inspecter l'intérieur de la trame pour analyser l'adresse réseau.

Les normes 802.1q et 802.1p décrivent respectivement les VLAN et la qualité de service associée. Quatre octets sont insérés dans la trame MAC des réseaux 802.3 juste après l'adresse source (figure 5.17) :

- le champ TPID (*Tag Protocol Identifier*) sur 2 octets, équivalent du champ « Type », 8100_H pour les trames « taggées » ;
- le champ *User Priority* sur 3 bits (8 niveaux de priorité) ;
- un bit CFI (*Canonical Format Indicator*) qui indique si la trame transporte des données autres qu'Ethernet ;
- un champ VID (VLAN ID) sur 12 bits qui identifie le VLAN destination.

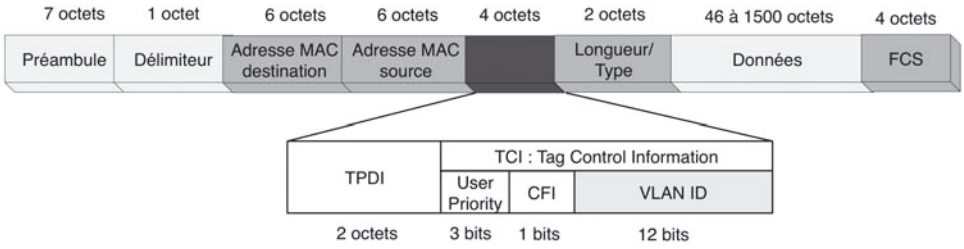


Figure 5.17 – Insertion d'une étiquette dans la trame Ethernet.

Finalement, trois types de trames peuvent traverser un commutateur prévu pour gérer les VLAN (« VLAN-aware ») :

- **Trame non taggée**, absence d'en-tête (TPDI+TCI) après l'adresse MAC source. Dans ce cas, c'est l'adresse MAC source ou éventuellement d'autres champs comme l'adresse IP qui permettent de déterminer le VLAN d'appartenance et de commuter la trame vers le port correspondant.

- **Trame taggée de priorité** (VID = 0). Le VID n'est pas signifiant, la trame ne transporte que des infos de priorité. Du point de vue du processus de transmission, elle est considérée comme une trame non taggée.
- **Trame taggée de VLAN**. TIPD = 8100_H, CFI = 0 et VID entre 1 et 4094. Dans ce cas, le commutateur utilise le VID pour déterminer vers quel port commuter la trame.

5.7 L'architecture sans fil 802.11 (WiFi)

Cette technologie permet de relier dans un réseau local sans fil ou **WLAN** (*Wireless LAN*) des équipements de type PC portable, tablette ou smartphone en utilisant les ondes radio. Les performances atteintes (11 à 300 Mbit/s pour des portées de l'ordre d'une centaine de mètres) permettent d'envisager le remplacement partiel de réseaux filaires de type Ethernet et d'éviter ainsi les contraintes du câblage. Des ponts sont prévus pour se relier aux réseaux locaux filaires ou à l'Internet.

Le standard d'interopérabilité WiFi (*Wireless Fidelity*) facilite la commercialisation de produits à la norme IEEE 802.11.

5.7.1 La norme IEEE 802.11

La norme IEEE 802.11 concerne la couche MAC du modèle IEEE associée à différentes normes de transmission radio (FHSS/DSSS/OFDM).

Couches OSI	Couches IEEE	Normes
Liaison	LLC (*Logical Link Control*)	802.2
	MAC (*Medium Access Control*)	802.11
Physique	PHY (*Physical Signalling Layer*)	FHSS DSSS OFDM

Figure 5.18 – **Modèle IEEE 802.11.**

Deux catégories d'équipements sont définies par cette norme :

- les stations sans fil (*wireless station*) : PC portable ou smartphone équipés d'une WNIC (*Wireless Network Interface Card*) ;
- les points d'accès (AP, *Access Point*) qui coordonnent les transmissions et servent de pont entre le réseau câblé et le WLAN.

L'organisation du réseau sans fil est basée sur une topologie cellulaire (le système est subdivisé en cellules) où chaque cellule (BSS, *Basic Service Set*) est contrôlée par un AP.

La norme 802.11 implémente deux modes de fonctionnement.

- **Le mode infrastucture** (*Infrastructure Mode*) illustré figure 5.19. Dans la plupart des installations, le WLAN est composé de plusieurs cellules où chaque AP de cellule est interconnecté aux autres par une dorsale (*backbone*) câblée (DS,

Distribution System). Cette interconnexion correspond à un ensemble étendu de cellules (ESS, *Extended Service Set*).

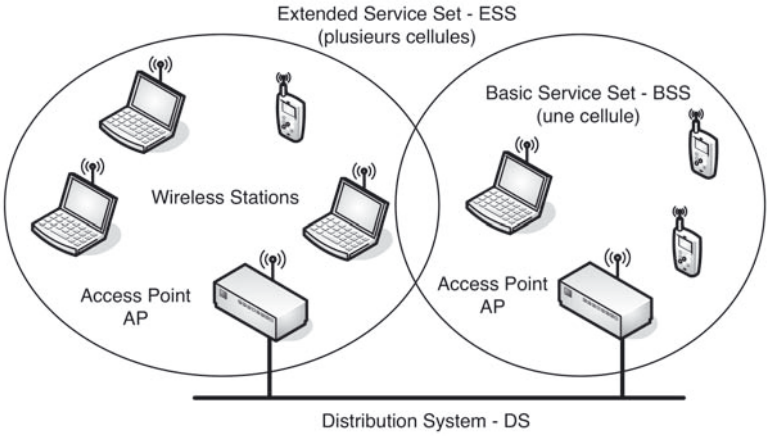


Figure 5.19 – **Mode infrastructure.**

- **Le mode *ad hoc*** (figure 5.20), également appelé mode sans infrastructure ou IBSS (*Independent Basic Service Set*), permet à des stations de communiquer directement entre elles sans utiliser un point d'accès. Ce mode simplifié permet de réaliser rapidement une communication entre deux stations sans fil. Pour pouvoir fonctionner sur un réseau étendu, ce mode doit être associé à un protocole de routage *ad hoc* permettant à une station de communiquer avec une station éloignée par l'intermédiaire de stations faisant office de routeur.

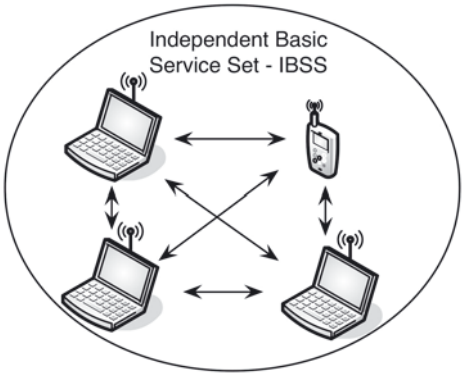


Figure 5.20 – **Mode *ad hoc*.**

5.7.2 La couche physique

Le standard définit actuellement une seule couche MAC qui interagit avec deux couches physiques (une troisième couche FHSS – *Frequency Hopping Spread Spectrum* – développée à l'origine est aujourd'hui abandonnée).

- **DSSS** (*Direct Sequence Spread Spectrum*). La bande sans licence ISM (Industrie, Science et Médecine) des 2,4 GHz (2,4000 – 2,4835 Ghz) est divisée en 14 canaux de 20 MHz chacun. La transmission ne se fait que sur un seul canal par BSS. Pour compenser le bruit, une technique de *chipping* qui consiste à convertir chaque bit de données en une séquence de 11 bits est utilisée. Cette technique permet une co-localisation théorique de 3 BSS, soit trois canaux (figure 5.21).
- **OFDM** (*Orthogonal Frequency Division Multiplexing*). Cette technique utilisée entre autres par l'ADSL permet de répéter le signal à transmettre sur différentes fréquences porteuses orthogonales dans le but d'augmenter le débit global. Suivant la norme associée, 802.11a ou 802.11g, le multiplexage OFDM utilise respectivement la bande U-NII (*Unlicensed-National Information Infrastructure*) dans les 5 Ghz ou la bande ISM des 2,4 GHz.

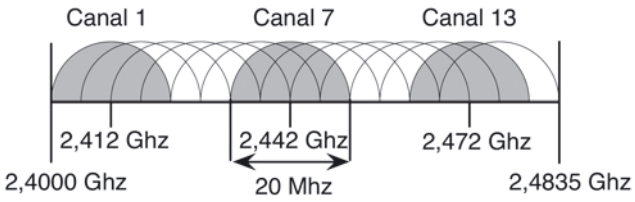


Figure 5.21 – Canaux 802.11 dans la bande ISM.

Les modulations à saut de phase appliquées aux séquences permettent d'obtenir des débits différents. La BPSK (*Binary Phase Shift Keying*) pour un débit de 1 Mbit/s et la QPSK (*Quadrature Phase Shift Keying*) pour un débit de 2 Mbit/s.

Dans le standard 802.11b, pour pouvoir supporter les débits de 5,5 Mbit/s et 11 Mbit/s, la technique DSSS High-rate est utilisée. Cette augmentation des débits est réalisée en ajoutant à une modulation QPSK une technique de codage CCK (*Complementary Code Keying*). Pour une réception satisfaisante, la portée de l'émetteur ne doit pas dépasser 100 m dans un environnement de bureau et 400 m sans obstacles. En pratique, on limite les distances à 50 m pour garder une qualité de réception optimale.

Pour le standard 802.11g qui permet des débits théoriques jusqu'à 54 Mbit/s, la modulation OFDM est utilisée. Chaque porteuse est ensuite modulée indépendamment en utilisant une modulation de type 64QAM (*64-level Quadrature Amplitude Modulation*) associée à un codage CCK. La compatibilité avec le standard 802.11b est assurée avec des débits de repli de 11 ou 5,5 Mbit/s. Pour obtenir des débits maximums, la portée en intérieur doit être réduite à quelques dizaines de mètres.

5.7.3 Association et *handover*

Quand une station veut s'associer à une cellule existante et donc accéder à un BSS ou à un IBSS, soit après un démarrage, un passage en mode veille ou un déplacement, la station a besoin d'informations de synchronisation de la part du point d'accès (ou des autres stations dans le cas du mode *ad hoc*). La station peut obtenir ces informations suivant deux méthodes choisies en fonction de la puissance des signaux reçus ou de la consommation d'énergie engendrée par l'échange :

- **écoute passive** : la station attend de recevoir une trame « balise » (*Beacon Frame*) envoyée périodiquement par l'AP et contenant les informations de synchronisation ;
- **écoute active** : la station essaie de rejoindre un AP en transmettant une trame de requête (*Probe Request Frame*) et attend la réponse du point d'accès.

La phase d'association se poursuit par un processus d'authentification qui peut être sécurisé par un échange de trames cryptées. Le processus se termine par un échange d'informations concernant les caractéristiques de la cellule et la station peut alors transmettre et recevoir des trames de données. L'émission périodique de trames balises assure la synchronisation tout au long des échanges.

Le ***handover*** est le processus de déplacement d'une station d'une cellule vers une autre sans interruption de la communication. Ce processus n'est pas directement géré par 802.11 mais les mécanismes d'association permettent de supporter cette mobilité. La station teste la puissance du signal de l'AP et, si celui-ci s'affaiblit, elle se réassocie avec un nouvel AP sur un autre canal. Ce processus dynamique d'association et de réassociation avec les AP permet de mettre en place des WLAN de couverture importante en créant une série de cellules se recouvrant (figure 5.22). Il faut alors éviter de configurer deux AP voisins avec le même canal pour éviter les interférences. Lors d'un déplacement en mode *ad hoc*, les stations testent de la même façon la présence d'autres stations sur différents canaux.

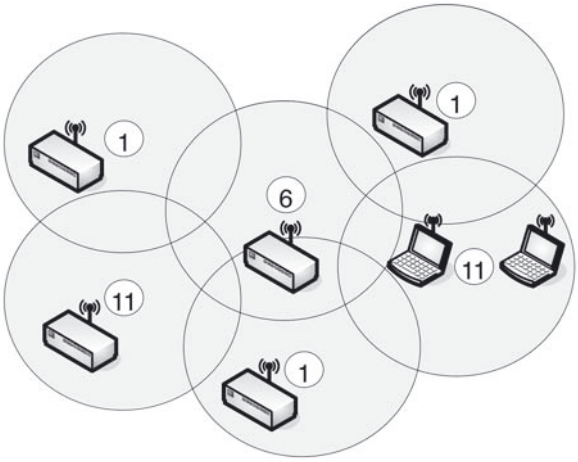


Figure 5.22 – **Affectation des canaux aux BSS ou IBSS.**

5.7.4 La sous-couche MAC

a) Méthode d'accès

La sous-couche MAC est unique au protocole 802.11. Elle définit une fonction de coordination des échanges distribuée (DCF : *Distributed Coordination Function*) dans laquelle toutes les stations ont une chance égale d'accéder au support.

Les liaisons radio n'étant pas *full duplex*, une méthode de détection de collision de type CSMA/CD ne peut être utilisée dans la mesure où une station ne peut être à l'écoute du support pendant son émission. Un mécanisme d'écoute de porteuse avec évitement de collision et acquittement est donc utilisé. DCF correspond à la méthode d'accès **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*).

Une station voulant transmettre écoute le support. S'il est occupé, la transmission est différée. Si le support est libre pendant un temps supérieur au **DIFS** (*DCF Inter Frame Spacing*), la station est autorisée à transmettre. La station réceptrice va vérifier le CRC du paquet reçu et renvoie un accusé de réception **ACK**. La réception de l'ACK indiquera à l'émetteur qu'aucune collision n'a eu lieu. Si l'émetteur ne reçoit pas l'accusé de réception, alors il retransmet la trame jusqu'à ce qu'il l'obtienne ou abandonne au bout d'un certain nombre de retransmissions (7 par défaut).

Pour séparer les transmissions au sein d'un même dialogue (données, ACK…), un temps inter-trame plus faible **SIFS** (*Short IFS*) est suffisant dans la mesure où seule une station est susceptible d'émettre à cet instant (émetteur ou récepteur en cours).

Pour éviter une collision, les stations qui entendent une transmission en cours utilisent un temporisateur régulièrement mis à jour : le **NAV** (*Network Allocation Vector*) calculé en fonction du champ délai contenu dans les trames émises. Les stations voulant émettre et trouvant le support encore occupé après le temps DIFS attendent donc un temps correspondant au NAV (durée théorique de l'occupation) augmenté d'un nouveau DIFS (figure 5.23).

Au bout de ce temps d'attente, les stations ne cherchent pas à émettre toutes en même temps et évitent les collisions en attendant chacune un temps supplémentaire aléatoire suivant un algorithme de type BEB (*Binay Exponential Backoff*).

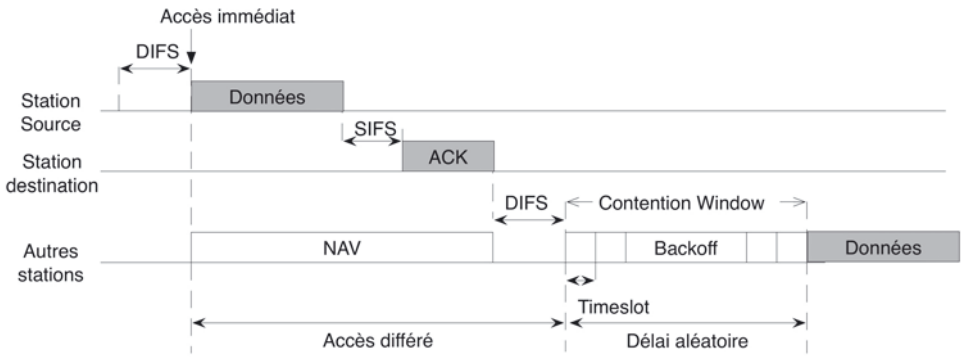


Figure 5.23 – Accès au support CSMA/CA.

L'algorithme BEB, proche de celui utilisé dans Ethernet, est basé sur la gestion de *timeslots* correspondant à des tranches de temps fixées par la couche physique :

- la station tire un nombre aléatoire *n* compris entre 0 et CW_i. CW_i est la fenêtre de contention (*Contention Window*) bornée à CW_{max} (1023 pour 802.11b et 802 .11g) et *i* est le nombre de tentatives de retransmission ;
- la station attend *n* x *Tslot* (*Tslot* est la durée prédéterminée du *timeslot*) et émet si le canal est libre (si le canal est occupé, c'est qu'une autre station a tiré un nombre inférieur de *timeslot*) ;
- la taille de la fenêtre de contention est doublée (*Binary Exponential*) à chaque tentative de retransmission : $CW_i = 2^{k+i} - 1$. *k* est un entier définissant la valeur de CW_{min} ($k = 4$ et $CW_{min} = 15$ pour 802.11g).

La figure 5.24 illustre l'accroissement de la fenêtre de contention CW_i en fonction du nombre de tentatives de retransmission.

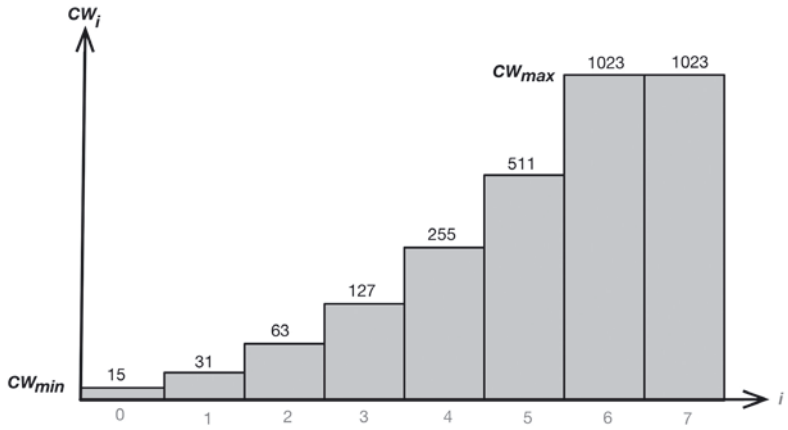


Figure 5.24 – Évolution de CW_i.

Si deux stations tirent le même nombre de *timeslots*, la collision ne peut être évitée, elle est alors détectée par l'absence de réponse ACK.

En définitive, l'algorithme de *back off* exponentiel est exécuté dans les cas suivants :

- quand la station écoute le support avant la première transmission d'un paquet et que le support est occupé pendant un temps supérieur au DIFS ;
- après chaque retransmission ;
- après une transmission réussie ;
- après une détection de collision.

Le seul cas où ce mécanisme n'est pas utilisé est quand la station décide de transmettre un nouveau paquet et que le support a été libre pour un temps supérieur au DIFS.

b) Problème de la station cachée

Une station A émet vers une station B ; une autre station C qui est hors de portée de la station A n'entend pas l'émission et risque de vouloir émettre à son tour vers la station B et donc de provoquer une collision qui ne peut être évitée par la méthode CSMA/CA (voir figure 5.25).

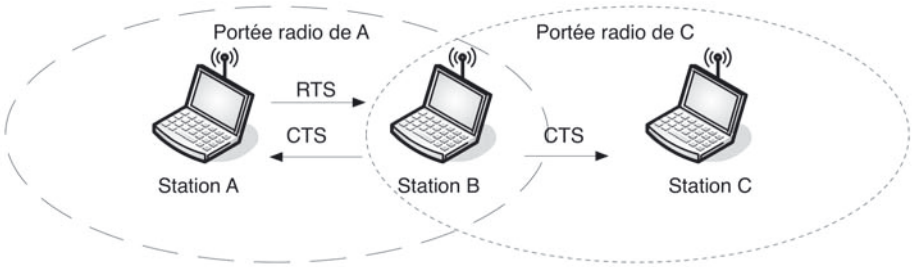


Figure 5.25 – **Station cachée et détection virtuelle de porteuse par RTS/CTS.**

Pour résoudre ce problème, la norme 802.11 a défini le mécanisme de **VCS** (*Virtual Carrier Sense*). Il est basé sur l'un des premiers protocoles développés pour les WLAN : MACA (*Multiple Access with Collision Avoidance*). Ce mécanisme virtuel de détection de porteuse au niveau MAC est comparable à l'écoute du support effectué au niveau physique (PCF, *Physical Carrier Sense*).

Une station voulant émettre transmet d'abord une petite trame (30 octets) de contrôle RTS (*Request To Send*). Toutes les stations qui entendent le RTS mettent à jour leurs NAV en fonction du champ durée du RTS. La station destination concernée répond après attente d'un temps SIFS avec une trame courte CTS (*Clear To Send*). Le NAV est de nouveau mis à jour par les stations entendant le CTS. Après réception du CTS par la station source, celle-ci est assurée que le support est réservé pour sa transmission pendant un temps au moins égal au NAV (voir figure 5.26). Par ailleurs, les stations cachées hors de portée de l'émetteur seront prévenues d'une émission en cours (dans l'exemple précédent, la station C qui aura entendu le CTS émis par B différera sa transmission). Ce mécanisme permet donc d'une part de

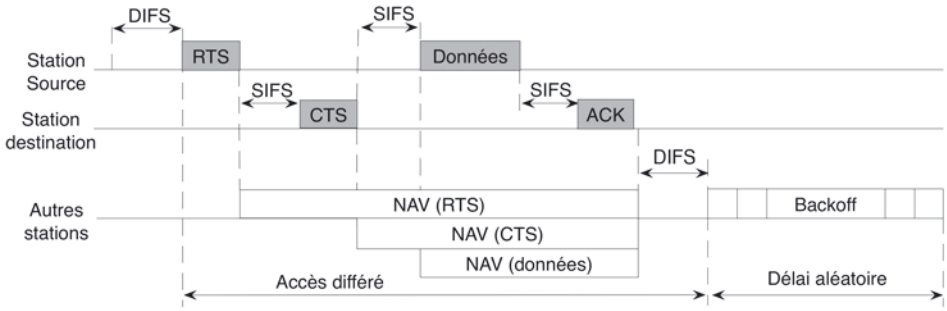


Figure 5.26 – **Réservation de support avec les trames RTS/CTS.**

réserver le support pendant un temps paramétrable et de résoudre le problème de la station cachée. Il n'évite cependant pas les collisions de RTS ou de CTS, mais celles-ci sont moins coûteuses que des collisions de longues trames de données.

c) Trames IEEE 802.11

Il y a trois principaux types de trames :

- les trames de données qui encapsulent les paquets IP ;
- les trames de contrôle utilisées pour contrôler l'accès au support (RTS, CTS, ACK) ;
- les trames de gestion, utilisées pour les phases d'association et d'authentification.

La structure de base des trames est commune et comporte les différents champs (figure 5.27) :

- le préambule est dépendant de la couche PHY et correspond à une séquence permettant de synchroniser et de définir le début de trame ;
- l'en-tête PLCP (*Physical Layer Convergence Protocol*) est utilisé par la couche PHY pour décoder la trame, il contient des informations sur la longueur de la trame et le débit des données.

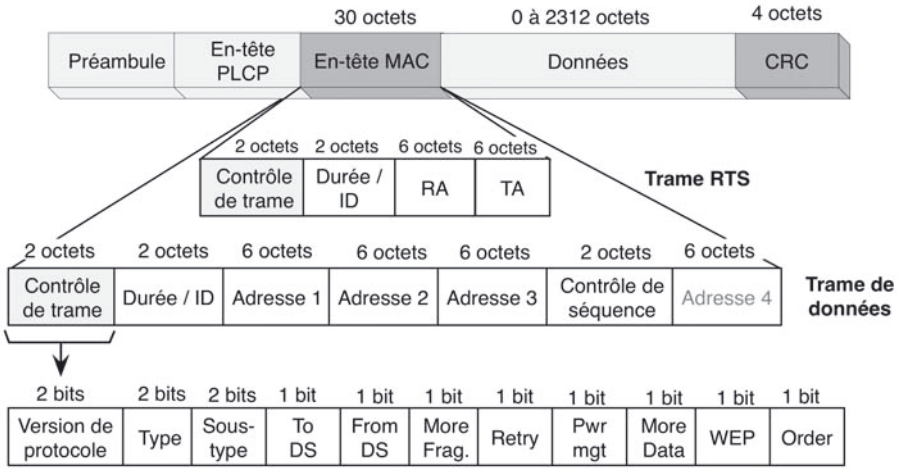


Figure 5.27 – Structure de base des trames 802.11.

Les trames de données et de gestion comportent un certain nombre de champs dans l'en-tête MAC :

- les deux octets de contrôle de trame donnent des indications telles la version du protocole, le type de trame, la direction de la trame (bit *To DS* à 1 lorsque l'AP doit relayer la trame vers le système de distribution DS ; bit *From DS* à 1 lorsque la trame vient d'une station), une fragmentation, une retransmission, un cryptage WEP…
- le champ Durée donne la valeur utilisée pour le calcul du NAV ;

- les champs Adresse ont différentes significations suivant les valeurs des bits *To DS* et *From DS*. Trois adresses sont nécessaires pour désigner la station émettrice, la station destinatrice et le point d'accès qui relaie les données (la quatrième adresse optionnelle est utilisée pour désigner un deuxième point d'accès intermédiaire). Adresse 1 et Adresse 2 correspondent toujours aux adresses du récepteur et de l'émetteur qui peuvent être une station ou le point d'accès intermédiaire ;
- le champ de Contrôle de séquence est utilisé pour représenter l'ordre des différents fragments appartenant à la même trame et pour reconnaître les paquets dupliqués.

Les trames de contrôle les plus courantes ont un format limité. Pour la trame RTS (figure 5.27), RA est l'adresse du récepteur de la prochaine trame de données ou de gestion et TA est l'adresse de l'émetteur.

La valeur de la durée est le temps, en microsecondes, nécessaire à la transmission d'une trame CTS, d'une trame de gestion ou de données et d'une trame ACK augmenté de trois intervalles SIFS (voir NAV-RTS figure 5.26).

La structure des trames CTS et ACK est similaire. Dans la mesure où ce sont des trames de réponses, les six octets TA sont absents.

5.7.5 Versions 802.11

Le tableau 5.2 résume les versions en cours et les évolutions futures de la norme. Les versions commercialisées à l'heure actuelle sont la 802.11g à 54 Mbit/s, la 802.11n jusqu'à 300 Mbit/s et la 802.11ac jusqu'à 1 Gbit/s. Le mécanisme de réservation de support avec les trames RTS/CTS est rarement implanté sur les cartes et l'algorithme de chiffrement WEP est considéré comme peu robuste.

Les évolutions portent surtout sur les débits qui doivent être associés à d'autres types de codage ou de transmission. Par exemple, la norme 802.11n utilise la technologie MIMO (*Multiple Input Multiple Output*) qui repose sur l'utilisation de plusieurs antennes sur le même canal pour transmettre davantage de données à la

Tableau 5.2 – Versions 802.11.

Version	802.11b ou WiFi	802.11g	802.11a ou WiFi5	802.11e	802.11f	802.11i	802.11n	802.11ac
Débit	2-11 Mbit/s	2-54 Mbit/s	6-54 Mbit/s	2-54 Mbit/s			54-300 Mbit/s	1 Gbit/s
Bande	ISM 2,4 GHz	ISM 2,4 GHz	U-NII 5GHz	ISM ou U-NII			ISM et U-NII	ISM et U-NII
Couche PHY	DSSS-highRate	OFDM	OFDM	DSSS ou OFDM			OFDM+ MIMO	OFDM+ MIMO
QoS	Non	Non	Non	Oui	Non	Non	Non	Non
Handover	Non	Non	Non	Non	Oui	Non	Non	Non
Sécurité	WEP	WEP/WPA	WEP	WEP	WEP	AES	WEP/WPA	WEP/WPA

fois en exploitant la différence des temps de propagation des signaux. La dernière norme 802.11ac (Gigabit WiFi) est basée sur trois améliorations : la largeur de bande (jusqu'à 160 MHz), la densité de modulation (256 QAM) et la multiplication du MIMO (jusqu'à 8 flux). Les autres évolutions portent sur la qualité de service QoS (802.11e), une meilleure gestion du *handover* (802.11f) ou de la sécurité (802.11i).

5.8 L'architecture sans fil 802.15.1 (Bluetooth)

Cette technologie est destinée à relier par ondes radio et sur de courtes distances (1-10 m) des équipements légers de type téléphone cellulaire, smartphone, lecteurs audio, appareils domestiques ou encore PC portables. Ces équipements reliés forment un réseau personnel sans fil ou **WPAN** (*Wireless Personal Area Network*) avec des débits inférieurs à 1 Mbit/s.

La simplicité d'intégration et les faibles ressources nécessaires sont les atouts majeurs de cette technologie. Le coupleur gérant l'accès au support suivant la norme IEEE 802.15 est très miniaturisé et se limite à une simple puce de faible coût, de faible encombrement et de faible consommation (0,1 W) pouvant être intégrée dans de nombreux appareils du réseau personnel.

5.8.1 La norme IEEE 802.15.1

La norme IEEE 802.15.1 concerne la couche MAC du modèle IEEE associée à une transmission physique par ondes radio dans la bande sans licence ISM des 2,4 GHz.

Couches OSI	Couches IEEE	Normes
Liaison	LLC (*Logical Link Control*)	802.2
	MAC (*Medium Access Control*)	802.15.1
Physique	PHY (*Physical Signalling Layer*)	FHSS + GFSK

Figure 5.28 – **Modèle IEEE 802.15.1.**

Dans la mesure où il n'existe pas d'infrastructure préexistante, les réseaux formés d'équipements Bluetooth sont dits *ad hoc*. Ils sont basés sur la formation de picoréseaux (piconets) contenant un maître (initiateur de la connexion) gérant les échanges et au plus sept esclaves actifs pouvant communiquer. Plusieurs piconets peuvent être associés par l'intermédiaire de l'un des équipements pour former un *scatternet* (figure 5.29).

Très souvent, le réseau est limité à un maître (un PC ou un smartphone) et un esclave (une souris ou un écouteur).

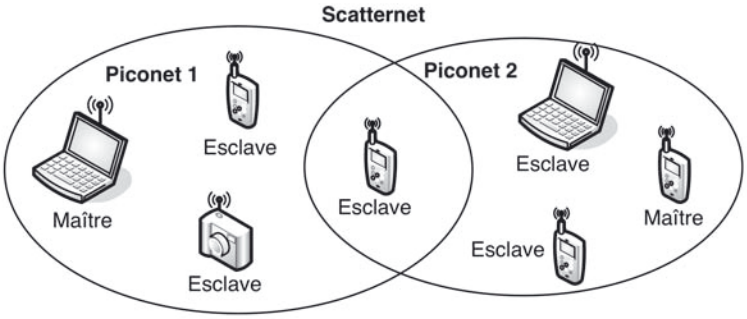


Figure 5.29 – **Organisation théorique d'un réseau Bluetooth.**

5.8.2 La couche physique

Comme pour WiFi, les transmissions utilisent la bande sans licence ISM de 2,4 GHz. Celle-ci est divisée en 79 canaux de 1 MHz chacun (limité à 23 canaux en France) avec une technique de saut de fréquence (FHSS, *Frequency Hopping Spread Spectrum*). Une modulation à saut de fréquence de type GFSK (*Gaussian Frequency Shift Keying*) est utilisée pour coder les différentes séquences numériques.

On peut distinguer deux types de communication *full duplex* entre les terminaux :

- **SCO** (*Synchronous connection-oriented*) : communications synchrones à 64 kbit/s pour la voix et les données. Trois communications de ce type peuvent être établies simultanément) ;
- **ACL** (*Asynchronous connection-less*) : communications asynchrones asymétriques avec une voie descendante à 723,2 kbit/s et une voie montante à 57,6 kbit/s pour une liaison Internet par exemple.

5.8.3 La sous-couche MAC

a) Méthode d'accès

Contrairement aux méthodes d'accès de type CSMA des normes 802.3 et 802.11, la méthode est déterministe et les échanges sont réglés par la station maître du piconet qui alloue à un esclave demandeur un temps de parole (*pooling*). Pour identifier les stations (maître ou esclave), une adresse MAC unique sur 48 bits est gravée sur la puce Bluetooth.

Lors d'une transmission, le temps est découpé en tranches ou *timeslot*. Chaque *slot* correspond à une durée de 625 µs, soit 1 600 *slots* par seconde. Les *slots* pairs sont réservés pour l'émission du maître, les *slots* impairs pour les esclaves. Pour chaque slot, un saut de fréquence (FHSS) sur un des canaux de la bande est réalisé suivant une séquence transmise au préalable par le maître à chaque station. Le maître peut allouer 1, 3 ou 5 *slots* pour la transmission suivant la taille du paquet de données. La figure 5.30 montre un enchaînement de communications synchrones (SCO) et asynchrones (ACL) sur *slots* de temps avec 3 esclaves.

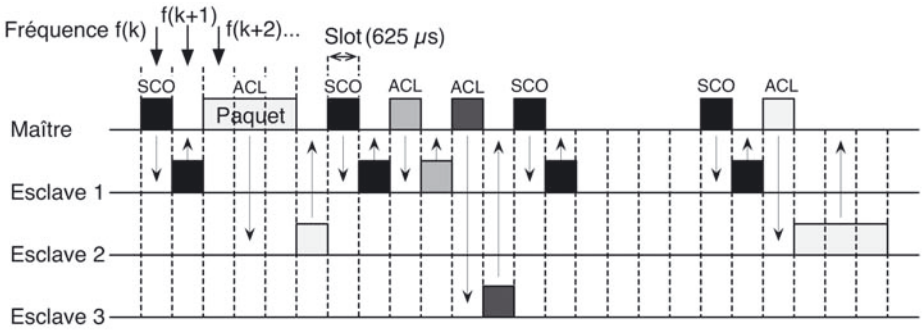


Figure 5.30 – **Transmissions sur *slot time*.**

b) Trames IEEE 802.15.1

Une structure de trame unique est utilisée par le maître ou l'esclave, elle comprend trois parties (figure 5.31) :

- le code d'accès de 72 ou 68 bits, lui-même composé de trois parties :
  - ◇ 4 bits de préambule pour la détection du début de trame,
  - ◇ 64 bits pour la synchronisation et l'identification dont la signification dépend de l'état en cours (code dérivé de l'adresse MAC pour l'état *page* ; code commun pour permettre à une station de s'associer pour l'état *inquiry* ; code unique identifiant le piconet pour l'état *connected*),
  - ◇ 4 bits de fin lorsque l'en-tête de paquet est présent ;
- l'en-tête de paquet sur 18 bits suit un encodage de type FEC (*Forward Error Correction*) avec des séquences de répétition limitant les risques d'erreur et formant un ensemble de 54 bits (3 × 18) :
  - ◇ l'adresse membre est attribuée par le maître (7 esclaves possibles),
  - ◇ le type de message précise s'il s'agit d'un contrôle, d'une communication synchrone ou asynchrone,
  - ◇ le bit flow permet le contrôle de flux en asynchrone,
  - ◇ les bits SEQN (*SEQuence Number*) et ARQN (*Automatic Repeat reQuest sequence Number*) permettent de numéroter et d'acquitter les trames,
  - ◇ le champ HEC (*Header Error Check*) correspond à une somme de contrôle.

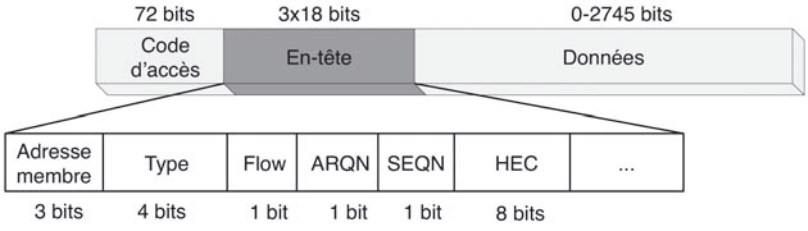


Figure 5.31 – **Structure des trames 802.15.1.**

5.8.4 Bluetooth *Low Energy*

Bluetooth LE ou BLE ou Bluetooth 4.0 permet en théorie une consommation dix fois moindre pour le même débit de 1 Mbit/s et une portée jusqu'à 60 m.

Cette réduction d'énergie est obtenue par l'activation systématique du mode veille en dehors des périodes de transmission et par la réduction des consommations : 0,5 µA en mode veille et moins de 15 mA en mode transmission. Cette économie permet à une puce BLE de fonctionner de plusieurs mois à plus d'un an avec une simple pile bouton.

Les couches basses de la pile protocolaire (PHY et MAC) restent les mêmes, les couches hautes chargées de gérer les applications et les profils d'utilisation sont simplifiées.

Les applications sont dans le domaine du sport, de la santé, du contrôle d'accès et de la domotique.

5.9 L'architecture sans fil 802.15.4

La norme IEEE **802.15.4** définit les couches basses, MAC et PHY, utilisées dans des réseaux de type **WPAN** à faible débit et faible consommation. Les principaux avantages par rapport à d'autres technologies sans fil sont une très faible consommation d'énergie en mode veille et la faible taille du code de la pile de protocoles à embarquer, ce qui permet le développement de composants miniaturisés à très faible coût.

L'un des objectifs de cette norme est la constitution de **réseaux de capteurs sans fil** (WSN : *Wireless Sensor Network*). Ces capteurs, regroupés en champs (*sensor fields*), font remonter les données *via* des passerelles (*sink*) vers un ordinateur central pour un traitement des informations (figure 5.32).

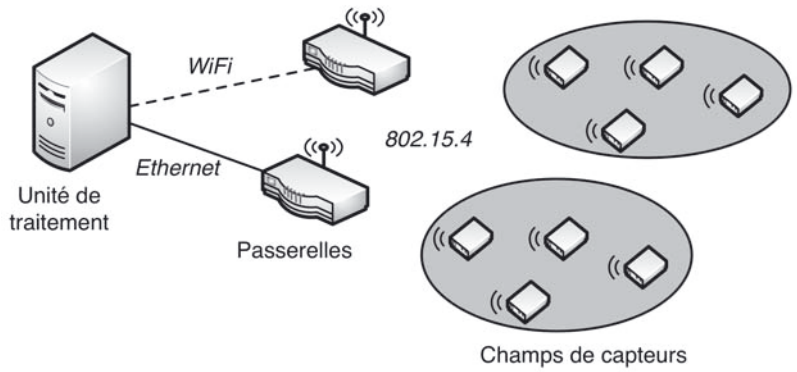


Figure 5.32 – **Principe d'organisation d'un réseau de capteurs sans fil.**

Les WSN ont de nombreuses applications, parmi lesquelles : la domotique (détection d'intrusions, identification) ; le contrôle de l'environnement (mesure d'ozone, pollution de l'air), l'agriculture (mesure d'humidité du sol, gestion du bétail), la surveillance médicale (mesure en temps réels de paramètres cardiaques, sanguins, respiratoires).

Cette norme est associée depuis sa conception à une architecture de réseau WPAN complète, l'architecture **ZigBee**, qui définit les couches supérieures, notamment les couches réseau et application (figure 5.33). Plus récemment, elle a été choisie pour fournir les couches basses au réseau **6LowPAN** destiné à étendre les réseaux locaux WPAN et à permettre la connexion des capteurs sans fil à l'échelle d'Internet. Ces deux architectures sont décrites dans les paragraphes suivants.

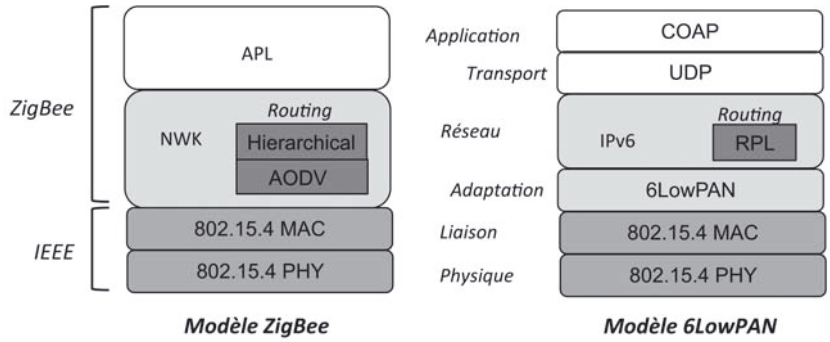


Figure 5.33 – Architectures à base de 802.15.4.

5.9.1 La norme IEEE 802.15.4

Les caractéristiques principales de cette norme sont un débit jusqu'à 250 kbit/s, une portée jusqu'à 100 m et une consommation en mode veille inférieure à 0,01 mA. Le protocole d'accès au support est de type CSMA/CA avec la possibilité pour un équipement d'obtenir des tranches de temps garanties.

Topologies

La norme IEEE définit deux types de périphérique :

- le FFD (*Full Function Device*) peut assurer trois rôles dans un réseau : coordinateur PAN, routeur ou simple capteur ;
- le RFD (*Reduced Function Device*) est un simple capteur terminal avec un module de transmission ; il ne possède pas suffisamment de ressources pour faire office de routeur.

À partir de ces différents rôles, trois topologies peuvent être déployées (figure 5.34). Les topologies maillées (*mesh*) et en arbre (*cluster tree*) sont des extensions de la topologie en étoile. Pour les topologies multisaut, un protocole de routage doit être fourni par la couche réseau.

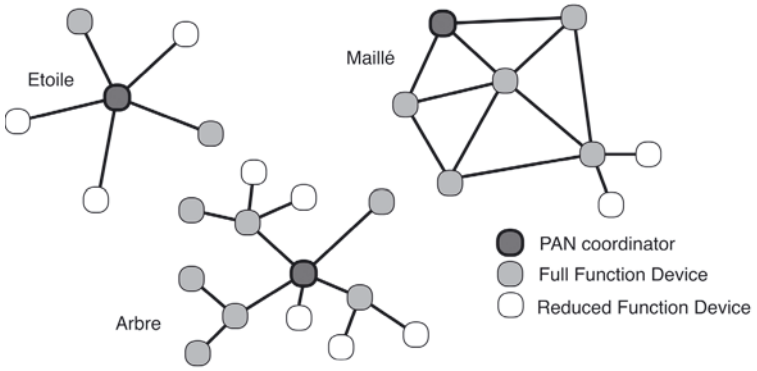


Figure 5.34 – Topologies 802.15.4.

Une fois son rôle déterminé (suivant le profil applicatif et ses propres ressources), les équipements 802.15.4 s'associent au réseau de manière hiérarchique : les routeurs et les simples périphériques terminaux envoient des paquets de découverte et s'associent au réseau par l'intermédiaire de son coordinateur ou d'un routeur intermédiaire. Lorsque plusieurs routeurs répondent, le routeur choisi est celui présentant la meilleure qualité sur la liaison (LQI : *Link Quality Indication*).

5.9.2 La couche physique

Les principales fonctions de la couche PHY sont :

- activation et désactivation de l'interface radio ;
- détection d'énergie (ED : *Energy Detection*) ;
- mesure de la qualité de la liaison (LQI : *Link Quality Indication*) ;
- estimation de disponibilité du canal (CCA : *Clear Channel Assessment*).

Le standard 802.15.4 propose deux couches physiques fonctionnant sur deux bandes de fréquences distinctes : 868/915 MHz et 2,4 GHz (bande ISM). La bande des 2,4 GHz, la plus courante, permet d'utiliser 16 canaux distincts (16 réseaux WPAN peuvent donc cohabiter dans la même zone) d'une largeur de 5 MHz chacun.

Suivant les bandes de fréquence utilisées, les modulations sont de type BPSK (*Binary Phase Shift Keying*) ou O-QPSK (*Orthogonal - Quadrature Phase Shift Keying*).

5.9.3 La sous-couche MAC

La sous-couche MAC 802.15.4 intègre les fonctionnalités suivantes :

- émission des trames balise si le périphérique est un coordinateur ;
- gestion de la synchronisation aux trames « balise » ;
- support des associations et désassociations au réseau à l'initiative des couches supérieures ;
- gestion de la méthode générale d'accès au médium CSMA/CA ;
- gestion du mécanisme spécifique d'accès avec durée garantie GTS (*Guaranteed Time Slot*).

a) Méthode d'accès

Suivant la configuration du réseau, la sous-couche MAC autorise deux types d'accès :

- un accès CSMA/CA standard dans un réseau asynchrone sans trames « balise » ;
- un accès multiplexé pour lequel les données sont transmises dans des tranches de temps calibrées (*timeslot*) dans un réseau synchronisé par des trames balise (*beacon*).

Pour la configuration avec trame « balise », la supertrame (*superframe*) comprise entre 2 *beacons* permet de définir les différents *slots* (figure 5.35). Sa structure est décidée par le coordinateur. Deux périodes de transmission des données sont possibles :

- période avec contentions (CAP : *Contention Access Period*) : les périphériques sont en compétition pour accéder au canal suivant la méthode CSMA/CA mais dans des *slots* de temps ;
- période sans contention (CFP : *Contention Free Period*) : certains périphériques (faible batterie, priorités…) ont acquis le droit de transmettre sur des *slots* de temps garantis de la trame (GTS : *Guaranteed Time Slot*).

La période d'inactivité de durée variable qui suit correspond à un mode basse consommation du coordinateur pendant laquelle le dialogue avec les autres périphériques est suspendu.

La synchronisation est nécessaire pour tous les accès au canal et les transferts de données. Chaque périphérique prêt à émettre des données sera en compétition pour l'obtention du canal et devra savoir quand la période d'accès par contention (CAP) débute. C'est le rôle du *beacon* de donner cette indication (voir structure de la trame « balise »). Dans le cas où le périphérique souhaite transmettre exclusivement en mode garanti (GTS), les informations transmises par le coordinateur dans le *beacon* permettront également de préciser dans quels *slots*.

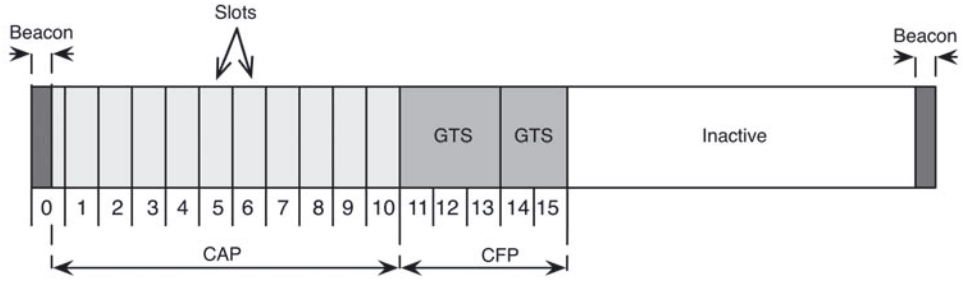


Figure 5.35 – Supertrame 802.15.4.

b) Trames IEEE 802.15.4

Pour gérer les différents mécanismes d'accès et de transmission des données, quatre types de trames sont utilisés :

- trame « balise » (*Beacon Frame*) ;
- trame de données (*Data Frame*) ;

- trame d'acquittement (*Acknowledgement Frame*) ;
- trame de commande (*Command Frame*).

L'en-tête MAC (*Mac Header*) est commun aux différentes trames, seuls les deux premiers champs sont utilisés pour les trames d'acquittement. La charge de niveau MAC (*MAC Payload*) varie suivant le type de trame avec des champs particuliers pour les trames « balise » et les trames de commande (figure 5.36). Pour les trames de données, cette charge utile est au maximum de 102 octets si l'en-tête MAC est de 25 octets, sachant que la taille maximale de la trame 802.15.4 est de 127 octets.

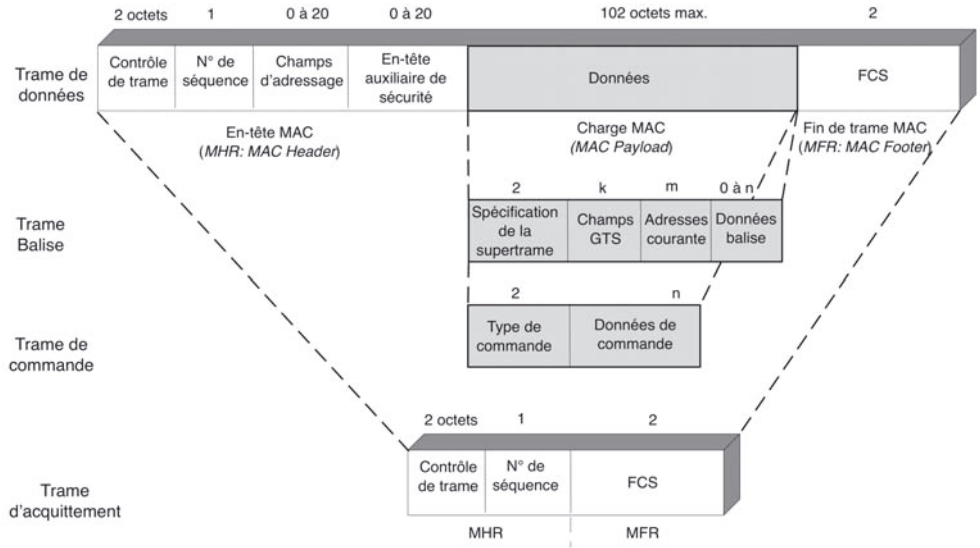


Figure 5.36 – Structure des trames 802.15.4.

Le champ de contrôle commun aux différentes trames précise :

- le type de trame ;
- l'utilisation ou non d'un champ supplémentaire dans l'en-tête pour gérer la sécurité au niveau MAC ;
- l'utilisation ou non d'acquittement de trame ;
- la présence ou non d'un adressage de niveau MAC dans l'en-tête (un adressage MAC existe toujours dans les trames balises) ;
- le numéro de séquence permet de synchroniser les trames de données et les trames balises aux acquittements correspondants ;
- le champ d'adressage, lorsqu'il est présent, spécifie l'adresse du réseau (*PAN identifier*) sur 2 octets et les adresses MAC source et destination d'un transfert sur 2 ou 8 octets chacune (dans le cas d'une trame « balise », seule l'adresse source correspondant au coordinateur est présente).

La charge de niveau MAC est particulière pour les trames balise. Elle permet de décrire l'organisation de la supertrame (voir paragraphe précédent) et contient :

- les valeurs qui déterminent les différentes durées de transmission et d'inactivité ;
- un champ qui spécifie le nombre de slots de temps alloués pour la période avec contentions (CAP) ;
- un descripteur pour les périodes sans contention (GTS) qui spécifie la liste des périphériques concernés avec pour chacun : la direction du transfert (coordinateur vers périphérique ou l'inverse), l'adresse du périphérique et le nombre de slots de temps alloués ;
- la liste des périphériques ayant un dialogue en cours avec le coordinateur.

5.9.4 Les réseaux ZigBee

ZigBee est une norme de réseau sans fil de type WPAN sécurisé à faible débit et faible consommation. Cette norme qui s'appuie sur la spécification IEEE 802.15.4 est promue par l'Alliance ZigBee : un consortium d'entreprises telles que Philips, Honeywell, Mitsubishi, Motorola et Samsung.

Les domaines d'application sont la domotique, le contrôle de bâtiments, la gestion de l'énergie, les télécommandes, la robotique et les réseaux de capteurs en général.

Le modèle ZigBee fournit :

- une couche réseau qui permet un adressage hiérarchique simple et un routage hiérarchique ou réactif ;
- une couche application permettant de définir des profils d'application pour les différents objets connectés et des associations entre ces objets ;
- un service de sécurité aux niveaux application et réseau qui intègre du cryptage et du contrôle d'intégrité.

a) La couche réseau

On retrouve les trois topologies définies par la norme 802.15.4 : étoile, arbre et maillée. Le rôle des différents équipements ZigBee correspond aux rôles attribués au niveau de la sous-couche MAC :

- **ZC**, coordinateur ZigBee, forcément un FFD ;
- **ZR**, routeur ZigBee, forcément un FFD ;
- **ZED**, périphérique de fin ZigBee, un FFD ou un RFD.

- *Assignation des adresses*

Les adresses de niveau réseau (adresses logiques) sont sur 2 octets et correspondent au format court des adresses MAC, ce qui permet d'adresser en théorie 65 535 périphériques. Les adresses MAC sur 8 octets correspondent aux adresses physiques des périphériques.

Trois paramètres sont utilisés pour définir la profondeur du réseau (le nombre maximum de sauts en partant du coordinateur), le nombre maximum de chaque type (ZC, ZR et ZED) et par suite l'assignation des adresses :

- ***Lm*** (MaxLayer) : spécifie la profondeur (*depth*) maximum du réseau ZigBee ;
- ***Cm*** (MaxChildren) : définit le nombre maximum d'enfants de type ZR ou ZED qu'un parent peut avoir ;
- ***Rm*** (MaxRouters) : définit le nombre maximum d'enfants de type ZR qu'un parent peut avoir.

À partir de *Lm*, *Cm* et *Rm*, une fonction ***Cskip(d)*** est utilisée pour calculer le décalage entre deux adresses de routeurs enfant. *Cskip(d)* correspond à la taille du sous-bloc d'adresse qui sera assigné par chaque parent à ses enfants routeurs.

$$Cskip(d) = \begin{cases} 1 + C_m \cdot (L_m - d - 1), & \text{si } R_m = 1 \\ \dfrac{1 + C_m - R_m - C_m \cdot R_m^{L_m - d - 1}}{1 - R_m}, & \text{sinon} \end{cases}$$

Un parent assigne une adresse à son premier enfant en incrémentant de 1 sa propre adresse. Les adresses des enfants routeurs suivants seront séparées d'une valeur égale à *Cskip(d).* Pour les enfants non-routeurs, la $n_{\text{ième}}$ adresse sera calculée comme suit :

$$A_n = A_{parent} + Cskip(d) \cdot R_m + n$$

Exemple : avec les paramètres suivants : *Lm* = 3 ; *Cm* = 4 et *Rm* = 4, la valeur de la fonction *Cskip(d)* peut être calculée pour les différentes profondeurs :

Tableau 5.3

Depth d	0	1	2	3
***Cskip*(d)**	21	5	1	0

Si un périphérique ZigBee obtient une valeur nulle de *Cskip(d)*, cela signifie qu'il n'est pas capable, à cette profondeur, d'accepter des enfants et sera donc forcément un ZED.

La figure 5.37 donne les valeurs d'adresse calculées avec les paramètres précédents, seule une partie des périphériques possibles dans cette configuration est représentée. On vérifie qu'à chaque niveau un routeur reçoit un bloc d'adresse suffisant pour pouvoir alimenter ses enfants routeurs ou simples terminaux.

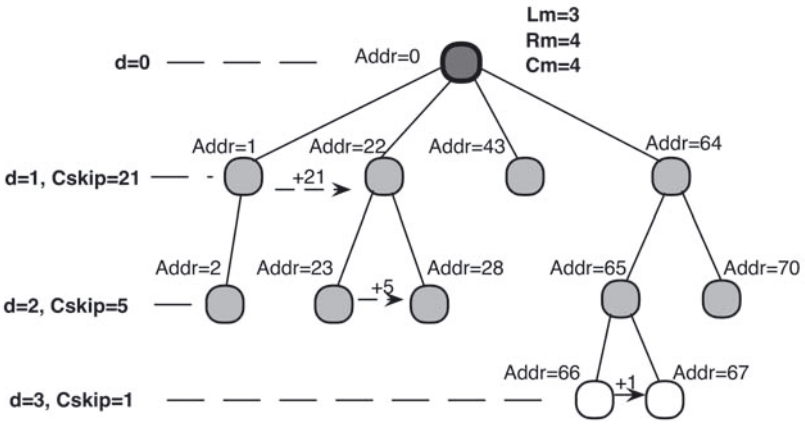


Figure 5.37 – **Exemple d'adressage ZigBee.**

- *Routage*

Trois processus de routage sont possibles dans un réseau ZigBee :

- **routage direct** (*no routing*) : dans une topologie en étoile, le ZC connaît tous ses ZED et communique directement avec eux ;
- **routage hiérarchique ou arborescent** : dans une topologie en arbre, tout nœud a au plus un père (tous en ont un et un seul sauf le coordinateur). Le routage utilise la structure arborescente définie lors de l'attribution des adresses.
  L'avantage est l'absence de tables de routage et donc la rapidité. L'inconvénient est que tous les messages à destination d'une autre branche passent par le ZC (figure 5.38) ;
- **routage réactif de type AODV** (*Adhoc On-demand Distance Vector routing*) mis en œuvre dans les réseaux *ad hoc*. Un paquet de découverte de route est envoyé en broadcast par l'émetteur. Lorsque le récepteur répond en *unicast*, la route est tracée. L'avantage est que tous les chemins directs sont possibles. L'inconvénient est que beaucoup de paquets sont échangés et qu'il est nécessaire de gérer des tables de routage.

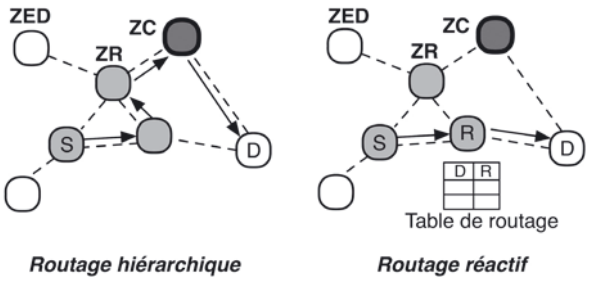


Figure 5.38 – **Exemple de routage ZigBee.**

b) La couche application

Avant de pouvoir transmettre des commandes ou des données à son voisinage, un équipement ZigBee doit d'abord connaître ce dernier. La phase de découverte de périphériques qui intervient aux niveaux MAC et réseau est donc suivie d'une phase de découverte de services au niveau applicatif (capteur de température sur l'équipement voisin, commande de volet…). Pour découvrir ces services, un équipement doit émettre des messages de requête vers les équipements voisins choisis pour obtenir en retour des descripteurs sur les propriétés du périphérique interrogé.

Une fois les services voisins découverts, les profils d'application qui définissent les messages et les traitements vont permettre aux équipements d'envoyer des commandes, de demander des données ou de traiter ces commandes ou ces données. Par exemple, un thermostat sur un équipement ZigBee peut interagir avec un chauffage distant muni d'une interface ZigBee suivant un processus préétabli (sensibilité en température, périodes d'allumage…). L'ensemble formant un profil d'application de régulation de température.

Ces profils d'application sont un moyen d'unifier les solutions techniques d'interopérabilité des constructeurs avec le standard ZigBee.

5.9.5 Les réseaux 6LowPAN

6LowPAN est l'acronyme de IPv6 *Low power Wireless Personal Area Networks*. Le groupe de travail 6LoWPAN a défini les mécanismes d'encapsulation, de fragmentation et de compression d'en-têtes permettant aux paquets au format IPv6 (voir chapitre 7) d'être envoyés ou reçus sur des réseaux IEEE 802.15.4.

L'objectif à large échelle est de pouvoir adresser les capteurs ou les actionneurs des réseaux 802.15.4 qui seront vus comme des objets « IPv6 ».

Un réseau 6LowPAN est donc composé de nœuds partageant le même préfixe IPV6, généralement avec un seul routeur de bord connecté à d'autres réseaux IP (figure 5.39). Le routeur de bord gère la compression et la fragmentation des en-têtes. Un réseau 6LowPAN étendu comprend plusieurs routeurs de bord reliés par une dorsale.

6LowPAN définit une couche d'adaptation sur la passerelle et sur les capteurs pour pouvoir adresser ceux-ci en IPv6 à partir de n'importe quel PC (voir le modèle 6LowPAN, figure 5.33).

Le rôle de la couche d'adaptation 6LowPAN est de résoudre le problème lié à la faible taille des trames 802.15.4 qui est de 127 octets : en retranchant les 25 octets de la sous-couche MAC, les 21 octets pour le cryptage AES, l'en-tête IPv6, l'en-tête UDP (ou TCP), il ne reste que 33 octets (21 avec TCP) pour les données utiles, ce qui ne permet pas de respecter les spécifications d'IPv6 qui imposent un MTU (*Maximum Transfer Unit*) minimal de 1 280 octets (figure 5.40).

La solution est d'une part d'utiliser la fragmentation des paquets Ipv6 et d'autre part d'utiliser la compression des en-têtes IPV6 et UDP.

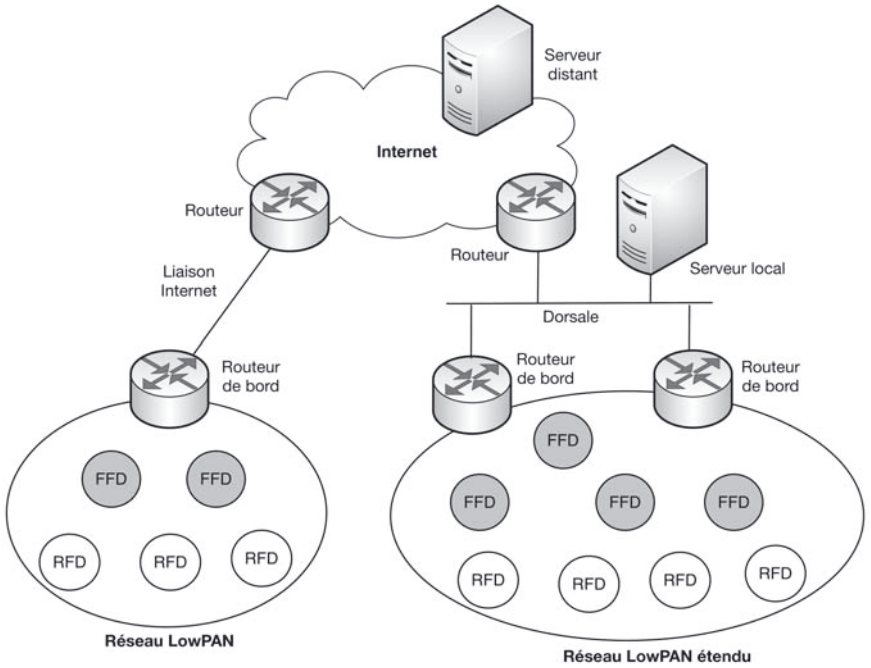


Figure 5.39 – **Architecture 6LowPAN.**

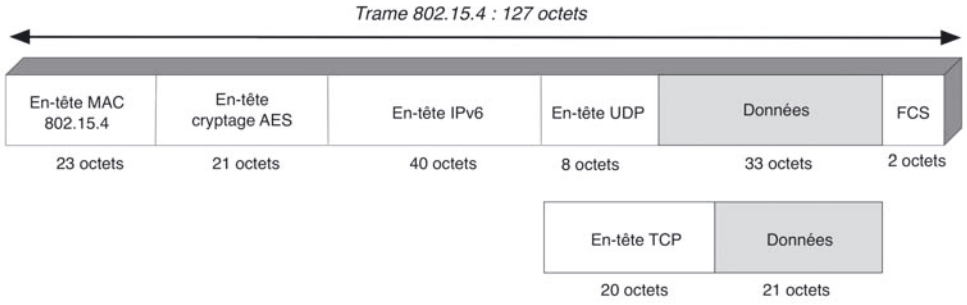


Figure 5.40 – **Trame 802.15.4 / 6LowPAN.**

Pour les couches supérieures, des protocoles spécifiques sont développés :

- COAP (*Constrained Application Protocol*) est destiné à gérer la communication avec les capteurs et les actionneurs à ressources réduites en minimisant les messages. Les commandes/réponses COAP peuvent être simplement traduites en commandes/réponses HTTP ;
- RPL *(Routing Protocol for Low power and Lossy Networks)* est un protocole de routage IPv6 à vecteur de distance économe en mémoire et en énergie.

Résumé

- Les **réseaux locaux** sont formés par l'interconnexion d'équipements divers (micro-ordinateurs, smartphones, imprimantes, matériel audio ou vidéo, automates…) au sein d'une entreprise. Les distances sont limitées à quelques km et les débits à 10 Gbit/s.
- Les **informations échangées** sont de type informatique (transfert de fichiers, images fixes…) ou temps réel (contrôle de processus, voix, images vidéo…). Le type de trafic (asynchrone, synchrone ou isochrone) et les débits utilisés sont bien sûr liés à la nature des informations.
- La **topologie** caractérise la manière dont les équipements sont connectés, il en existe trois principales : la topologie en étoile, la plus utilisée ; la topologie en bus, et la topologie en anneau. Chacune a ses caractéristiques propres en termes de facilité de connexion, de support physique, de fiabilité et de maintenance.
- La **normalisation proposée par l'IEEE** rajoute à la modélisation OSI deux sous-couches au niveau 2 : la sous-couche MAC et au-dessus, la sous-couche LLC. La **sous-couche MAC** définit essentiellement la méthode d'accès au support et la structure des trames. Les normes IEEE 802.3 à 802.15 correspondent à différentes méthodes d'accès et architectures filaires ou sans fil.
- Les **méthodes d'accès** au support définissent la façon dont une station, parmi d'autres, acquiert le droit de transmettre à un instant donné. On distingue les méthodes par répartition de canal (TDMA, FDMA…) ; les méthodes à accès contrôlé (par réservation ou consultation) et les méthodes à accès aléatoires utilisées notamment dans les réseaux Ethernet et WiFi.
- L'architecture **Ethernet** utilisée dans la majorité des réseaux locaux filaires couvre les couches 1 et 2 du modèle OSI. La topologie est en étoile, les débits vont de 10 Mbits/s à 10 Gbit/s pour des transmissions en bande de base (codage Manchester) sur paires torsadées, câble coaxial ou fibre optique.
- La **norme IEEE 802.3** associée définit une méthode d'accès aléatoire au support de type **CSMA/CD** ainsi qu'une structure de trame synchrone présentant un maximum de 1 518 octets.
- Pour un câblage en paires torsadées, les équipements de raccordement de type ***hub*** ou ***switch*** permettent d'optimiser la bande passante en utilisant des débits plus importants sur certains segments et en regroupant dans un même domaine de collision les stations liées par des échanges fréquents.
- Les **VLAN** permettent de regrouper dans un même réseau local dit virtuel des machines situées dans des locaux éloignés mais qui ont des besoins fréquents d'échange d'informations. Les machines appartenant à un même VLAN sont identifiées dans les commutateurs traversés grâce à leurs adresses MAC. Les **VLAN tagués** utilisent en plus une étiquette insérée dans la trame pour identifier le VLAN.

- **L'architecture sans fil 802.11 ou WiFi** permet de relier des équipements de type PC portables ou smartphones à l'aide de liaisons radio pour des débits jusqu'à 300 Mbit/s et des portées de 50 m. Pour chaque cellule correspondant à un regroupement de stations, une bande de fréquence spécifique est définie. Les cellules peuvent être reliées entre elles et à l'Internet par un réseau filaire. La méthode d'accès CSMA/CA est de type aléatoire avec un mécanisme d'évitement de collisions.
- **L'architecture sans fil 802.15.1 ou Bluetooth** est conçue pour relier sur des courtes distances (quelques mètres) des équipements légers de type smartphones, lecteurs audio ou GPS. Les débits sont limités à 1 Mbit/s. Un multiplexage temporel TDMA est utilisé pour offrir aux stations des transferts synchrones ou asynchrones.
- **La norme 802.15.4** définit les couches basses pour des réseaux sans fil faible coût et faible consommation. Les équipements peuvent être reliés en étoile, en arbre ou sur un réseau maillé. Suivant les besoins des applications, plusieurs méthodes d'accès sont possibles : déterministe de type TDMA ou aléatoire de type CSMA/CA.
- **Les réseaux ZigBee** intègrent une pile protocolaire complète basée sur le standard 802.15.4 pour les couches basses, sur une couche réseau offrant adressage et routage et sur une couche applicative qui définit des services et des profils permettant l'interaction des équipements. Ces réseaux sont destinés à la domotique et au contrôle de bâtiments.
- **Les réseaux 6LowPAN** s'appuient également sur les couches basses 802.15.4 avec pour objectif de connecter sur Internet, à l'aide d'un adressage IPv6, un ensemble de capteurs et d'actionneurs qui pourront alors être consultés ou commandés à partir de n'importe quel PC.

Exercices corrigés

QCM

Q5.1 Quels sont les débits courants sur un réseau local ?

a) 100 kbit/s b) 10 Mbit/s c) 100 Mbit/s d) 9 600 bit/s

Q5.2 Quel est le débit nécessaire pour transmettre le son avec une qualité de type CD ?

a) 234 Mbit/s b) 64 kbit/s c) 1,4 Mbit/s d) 10 Mbit/s

Q5.3 Quelle topologie est la plus économique en câblage ?

a) Étoile b) Bus c) Anneau

Q5.4 Quelles méthodes d'accès permettent aux stations d'émettre à un instant quelconque ?

a) CSMA b) CSMA/CD c) CSMA/CA d) Jeton sur anneau

Q5.5 Dans un réseau de dix stations utilisant la méthode d'accès CSMA/CD, pour quel débit les collisions seront-elles moins fréquentes ?

a) 10 Mbit/s b) 100 Mbit/s c) 1 Gbit/s

Q5.6 Quel équipement permet de séparer des segments de différents débits sur un réseau Ethernet ?

a) Le *hub* b) Le transceiver c) Le MAU d) Le *switch*

Q5.7 Quel type de câblage permet les débits les plus élevés sur un réseau Ethernet ?

a) Câble coaxial b) UTP c) STP d) Fibre optique

Q5.8 Quels sont les éléments pouvant être pris en compte pour constituer des VLAN ?

a) Les ports des commutateurs b) Les adresses MAC

c) Les adresses IP

Q5.9 Quel est le débit maximum pour l'ensemble des versions 802.11 ?

a) 1 Mbit/s b) 11 Mbit/s c) 300 Mbit/s d) 54 Mbit/s

Q5.10 Quelle méthode d'accès utilise le réseau Bluetooth ?

a) CSMA/CA b) TDMA c) FDMA d) Polling

Q5.11 Quelles sont les topologies possibles dans un réseau 802.15.4 ?

a) Bus b) Étoile c) Arbre d) Mesh

Q5.12 Quel type d'accès est possible dans un réseau 802.15.4 ?

a) Aléatoire b) Déterministe c) Synchrone

Q5.13 Quel type d'adressage utilise un réseau ZigBee ?

a) IPv4 b) IPv6 c) Hiérarchique d) Multicast

Q5.14 Quel est le rôle de la couche d'adaptation 6LowPan ?

a) Cryptage b) Routage c) Fragmentation d) Compression

Exercices

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

5.1 (*) Un réseau local est destiné à transférer deux types d'informations :

- des fichiers texte de 100 ko maximum nécessitant un temps de transmission minimal de 5 s ;

- des messages interactifs de cent caractères au maximum transmis en moins de 5 ms.

Calculer la capacité du support pour une transmission en bande de base.

5.2 (*) Dans un réseau local, quelles sont les conséquences, suivant la topologie utilisée, d'une rupture du câble?

5.3 (**) Citer les trois types de méthode d'accès possibles sur les LAN et WLAN. Indiquer leurs caractéristiques principales.

5.4 (*) Dans une méthode d'accès par réservation, comment se passe le processus de réservation ?

5.5 (**) Sur un réseau de huit stations utilisant la méthode d'accès CSMA, calculer la période de vulnérabilité, temps pendant lequel une station risque de ne pas détecter l'émission d'une trame. On donne :

- distance moyenne entre stations : 15 m ;
- vitesse de propagation : 200 000 km/s.

5.6 (*) Sur un réseau Ethernet, comment les collisions sont-elles détectées ? Que se passe-t-il après une détection de collision ?

5.7 (*) Déterminer la durée minimale d'occupation du bus par une trame sur un réseau Ethernet à 100 Mbit/s.

5.8 (***) Un réseau à 100 Mbit/s utilisant la méthode d'accès CSMA/CD est composé de trois stations A, B et C.

a) Calculer le temps de propagation maximum t_p entre les deux stations les plus éloignées pour une trame de 64 octets.

b) À l'instant t_0, la station A veut émettre vers B ; quelle est la durée minimale d'écoute pour pouvoir détecter une collision ?

c) À l'instant $t_0 + t_p/3$, la station C veut émettre vers B ; à quel instant la collision se produit-elle ?

d) À quel instant la collision est-elle détectée par C et par A ?

5.9 (**) Un *switch* Ethernet permet de connecter quatre stations appartenant à des VLAN de niveau 2. S1 et S4 sont dans le VLAN1, S2 et S3 sont dans le VLAN2. Pour simplifier, les adresses MAC sont représentées sur 1 octet au lieu de 6.

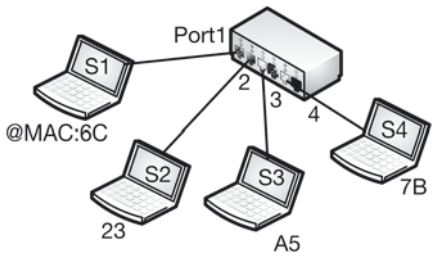


Figure 5.41

a) Établir les tables MAC/VLAN et PORT/VLAN du *switch*. Comment ces tables sont-elles construites dans la réalité ?

b) Quelle table l'administrateur doit-il modifier s'il souhaite changer une station de VLAN ?

5.10 (**) Dans l'exemple décrit par la figure 5.16, quel serait l'avantage d'utiliser un VLAN taggé ?

5.11 On considère le réseau sans fil ci-dessous. Il applique le protocole CSMA/CA. La station A décide d'émettre vers B.

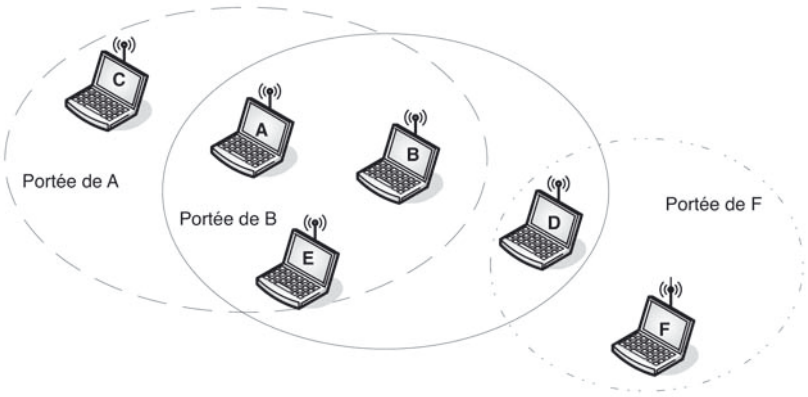


Figure 5.42

a) En l'absence de trames d'avertissement RTS/CTS, quelles stations peuvent détecter la transmission de A vers B ? Quelles sont les stations qui risquent de provoquer une collision ?

b) Dès que les stations A et B ont échangé les trames RTS et CTS, toute collision avec leurs données est-elle impossible ? Expliquez.

c) La station D a-t-elle le droit d'émettre vers la station F pendant la communication entre les stations A et B ?

5.12 (***) Un réseau WiFi 802.11b est composé de 4 stations A, B, C et D. À partir d'un instant initial t_0, la station A veut émettre ; à t_0 + 300 µs, les stations B et D veulent émettre ; à t_0 + 500 µs, la station C veut émettre.

Les temps inter-trames sont évalués à 10 µs pour le SIFS et 50 µs pour le DIFS. La durée du *timeslot* est de 20 µs. Les nombres de *timeslots* tirés par les stations B, C et D lors de la contention sont respectivement 5, 2 et 6.

a) Calculer les temps de transmission des trames de données et d'acquittement pour des paquets de 1 000 octets.

b) Établir un diagramme des temps faisant apparaître les transmissions des trames (première trame de chaque station) et les contentions.

c) Déterminer l'instant de début de transmission pour chacune des stations.

d) Calculer le débit moyen global (rapport du nombre total de bits transmis au temps total de transmission).

5.13 (**) Compte tenu de la taille des en-têtes des trames Bluetooth, quel est le rapport charge utile/charge totale pour des paquets asynchrones de 123 octets ?

En déduire le débit utile au niveau paquet si le débit trame pour une communication asynchrone est de 433,9 kbit/s.

5.14 La figure suivante illustre une transmission Bluetooth entre le maître et un esclave.

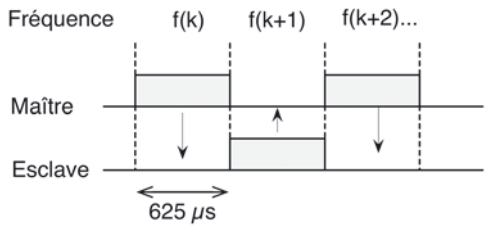


Figure 5.43

a) De quel type de multiplexage s'agit-il ?

b) Quelle méthode d'accès au support est utilisée ?

c) Les collisions entre maître et esclave ou entre esclaves peuvent-elles exister ?

d) Quel est l'intérêt de changer de canal de fréquence à chaque slot de transmission (f(k), f(k+1…) ?

5.15 (*) Les méthodes d'accès de type CSMA/CA utilisées dans les technologies 802.11 et 802.15.4 sont-elles comparables ?

5.16 (***) Calculez pour la topologie hiérarchique représentée ci-dessous les valeurs des adresses ZigBee. Rappelons que pour chaque niveau, les adresses sont affectées d'abord aux routeurs.

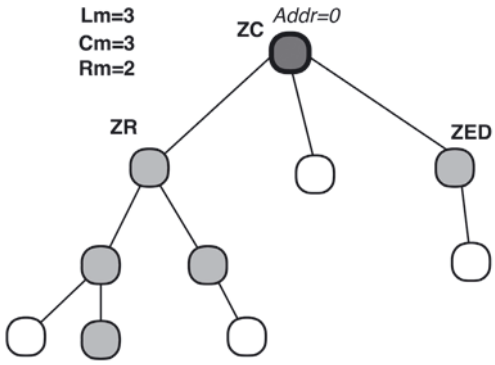


Figure 5.44

Solutions

QCM

Q5.1 : a-b-c **Q5.2** : c **Q5.3** : b **Q5.4** : a **Q5.5** : c

Q5.6 : d **Q5.7** : d **Q5.8** : a-b-c **Q5.9** : c **Q5.10** : b

Q5.11 : b-c-d **Q5.12** : a-b-c **Q5.13** : c **Q5.14** : c-d

Exercices

5.1 Débit nécessaire à la transmission des fichiers :

$$100 \times 1\,024 \times 8/5 = 164 \text{ kbit/s}$$

Débit nécessaire à la transmission des messages :

$$100 \times 8/5 \cdot 10^{-3} = 160 \text{ kbit/s}$$

Capacité du support : 164 kbit/s.

5.2 Pour une topologie en étoile, y compris pour un réseau Ethernet en paire torsadée, seule la station dont le câble de raccordement est rompu est inaccessible. S'il s'agit du câble entre deux hubs ou commutateurs, les deux domaines sont isolés.

Pour des topologies en bus ou en anneau, tout le réseau est bloqué.

5.3 Répartition de canal, accès contrôlé et accès aléatoire. Le premier type est basé sur le multiplexage fréquentiel ou temporel, chaque station possède un canal ou un slot de temps dédié. Dans les accès contrôlés, les stations doivent réserver le support ou attendre une invitation du contrôleur. Les accès aléatoires permettent aux stations d'émettre à tout moment mais avec des risques de collision.

5.4 Un dialogue préalable entre le maître et l'esclave souhaitant effectuer la réservation est nécessaire. Généralement, l'esclave envoie une trame spécifique spécifiant ses besoins en termes de durée ou débit d'émission, le maître acquitte ou refuse la demande.

5.5 Dans le cas le plus défavorable, la période de vulnérabilité est égale au double du temps de propagation entre les deux stations les plus éloignées, soit :

$$2 \times 7 \times 15 / 2 \cdot 10^{8} = 1{,}05 \text{ µs}$$

5.6 Les détections de collision se font par détection d'une surtension sur le support. Dans l'affirmative, la station attend avant une nouvelle tentative pendant un temps calculé suivant un tirage aléatoire dans lequel la borne supérieure double à chaque retransmission.

5.7 La taille minimale d'une trame est de 64 octets. La durée d'émission de cette trame est : 64 x 8/100.10^6 = 5,12 µs.
À cette durée, il faudrait ajouter le temps de propagation sur le support.

5.8

a)

$$t_{p\,max} = \frac{1}{2}\frac{64 \times 8}{100.10^6} = 2{,}56\ \mu s$$

b) Durée minimale d'écoute : 2 t_p = 5,12 µs

c) et d)

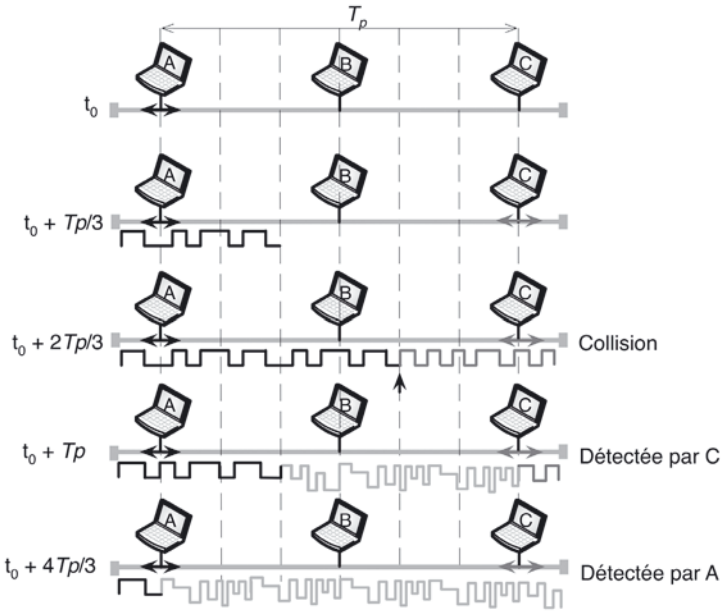


Figure 5.45

5.9 a)

Tableau 5.4

VLAN1	VLAN2
6C	23
7B	A5

PORT	VLAN
1	VLAN1
2	VLAN2
3	VLAN2
4	VLAN1

La table MAC/VLAN est établie par l'administrateur qui décide le VLAN d'appartenance de chaque station. La table PORT/VLAN est construite dynamiquement, lorsqu'une trame arrive sur un port, l'adresse MAC source est associée à un port et ce dernier est associé au VLAN correspondant.

b) L'administrateur doit modifier la table MAC/VLAN, la table PORT/VLAN sera modifiée automatiquement.

5.10 Pour un réseau local constitué seulement de deux commutateurs et de moins d'une dizaine de machines, le temps nécessaire pour que les commutateurs insèrent et éliminent les étiquettes sur les trames Ethernet sera perdu dans la mesure où il n'y a pas de commutateurs intermédiaires traversés. Il est dans ce cas plus simple d'utiliser une VLAN implicite avec des tables de commutation relativement légères.

5.11

a) Toutes les stations qui sont dans la zone de portée de A, c'est-à-dire C, E, peuvent détecter la transmission. La station D qui est dans la zone de portée de B ne pourra détecter l'émission de A vers B (station cachée) et risque de provoquer une collision si elle décide d'émettre. La station F n'est pas concernée.

b) La station A qui veut émettre envoie une trame d'avertissement RTS. Les stations C et E détectent cette trame et diffèrent leurs éventuelles émissions. La station B destinatrice répond avec une trame CTS pour prévenir les stations à sa portée. La station D qui a reçu une trame CTS venant de B différera son éventuelle émission. La station F, hors de portée de B, ne détecte pas la trame CTS mais son éventuelle émission ne perturbe pas B qui est hors de sa zone de portée. En conclusion, les collisions sont évitées.

c) Non car une émission de la station D serait détectée par B et provoquerait donc une collision lorsque A émet vers B (problème de la station cachée). Avec le mécanisme RTS/CTS, le problème est évité car la station D a détecté la trame CTS venant de B et va donc différer toute émission y compris vers F.

5.12

a) Une trame de donnée comporte 1 000 octets et 34 octets d'enveloppe MAC, d'où le temps de transmission :

$$T_{\text{Données}} = \frac{(1\,000 + 34) \times 8}{12 \cdot 10^6} \approx 689{,}33\,\mu\text{s}$$

Pour un acquittement de 14 octets, le temps est :

$$T_{\text{ACK}} = \frac{14 \times 8}{12 \cdot 10^6} \approx 9{,}33\,\mu\text{s}$$

La durée totale d'une transmission en ajoutant le temps inter-trame SIFS (figure 5.25) est donc :

$$T_{\text{Trans}} = T_{\text{Données}} + T_{\text{SIFS}} + T_{\text{ACK}} \approx 708{,}67\ \mu\text{s}.$$

b)

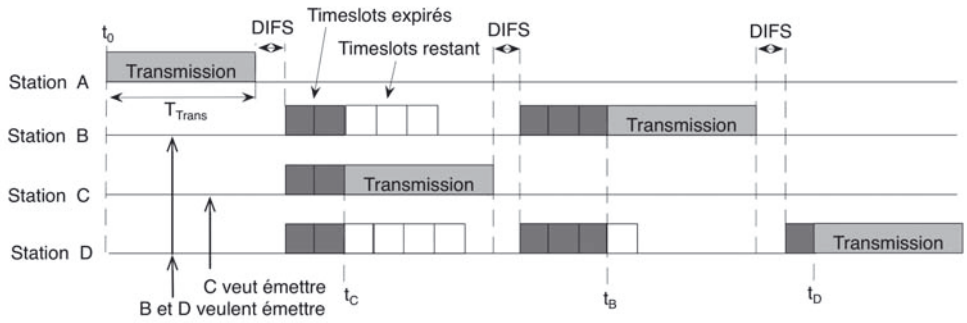


Figure 5.46

c) Les instants de début d'émission sont :

$$t_c = t_0 + T_{Trans} + T_{DIFS} + 2 \times T_{Slot} \approx t_0 + 798{,}68\ \mu s$$

$$t_B = t_c + T_{Trans} + T_{DIFS} + 3 \times T_{Slot} \approx t_0 + 1\ 617{,}34\ \mu s$$

$$t_D = t_B + T_{Trans} + T_{DIFS} + 1 \times T_{Slot} \approx t_0 + 2\ 396\ \mu s$$

d) Débit moyen global :

$$8 \times (4 \times 1\ 034 + 4 \times 14) / (2\ 396 \cdot 10^{-6} + 708{,}67 \cdot 10^{-6}) \approx 10{,}8 \text{ Mbit/s.}$$

5.13 Les champs « code d'accès » et « en-tête » de la trame Bluetooth occupent respectivement 72 et 54 octets. Pour une charge de 123 octets, le rapport est donc de 123 / (72 + 54 + 123) = 49,4 %.

Le débit au niveau paquet est dans ce cas de 49,4 % × 422,9 kbit/s, soit 214,34 kbit/s.

5.14

a) Multiplexage temporel (TDMA).

b) La méthode d'accès est déterministe de type *polling* : le maître donne la parole aux esclaves. Le maître émet sur des slots pairs, l'esclave sur des slots impairs.

c) Il ne peut y avoir collision entre le maître et un esclave (distinction entre slots pairs et impairs) et deux esclaves ne peuvent émettre simultanément car un esclave n'émet qu'en réponse à un paquet reçu du maître.

d) La technique des sauts de fréquences vise à limiter la durée des interférences toujours présentes dans les bandes partagées.

5.15 Dans un réseau 802.15.4 sans *beacon*, les méthodes sont comparables.

Dans un réseau 802.15.4 avec *beacon*, CSMA/CA résout les contentions dans la période CAP. Lorsqu'une station a gagné le droit d'occuper le support, elle le fait sur des slots de temps imposés par le coordinateur et non sur des durées variables comme en 802.11.

5.16

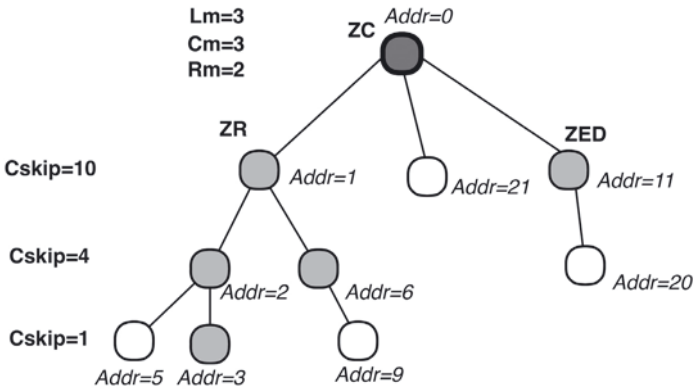


Figure 5.47

INTERCONNEXION DE RÉSEAUX

6

PLAN

OBJECTIFS

- Connaître le rôle des équipements d'interconnexion des réseaux.
- Étudier les fonctionnalités du protocole IP et en particulier l'adressage sur Internet.
- Comprendre le routage sur Internet et connaître les caractéristiques des principaux protocoles de routage dynamique.
- Étudier les fonctionnalités et les mécanismes du protocole TCP.

6.1 ÉQUIPEMENTS ET PROTOCOLES

6.1.1 Équipements d'interconnexion

L'interconnexion de deux réseaux d'architecture différente nécessite un équipement d'interconnexion spécifique dont la dénomination varie suivant les différentes couches où des modifications d'en-tête doivent être apportées.

a) Répéteur et concentrateur

Il sert à raccorder deux segments de câbles (deux segments de bus Ethernet par exemple) ou deux réseaux identiques qui constitueront alors un seul réseau logique. Il a pour fonctions :

- la répétition des bits d'un segment sur l'autre ;
- la régénération du signal pour compenser l'affaiblissement ;
- le changement de support physique (paires torsadées et fibre optique par exemple).

Le répéteur n'aura aucune fonction de routage ni de traitement des données, ni d'accès au support. Ainsi, le débit de retransmission est le même que le débit de réception. La trame n'est modifiée en aucune façon lors de la traversée du répéteur.

De la même façon, le concentrateur ou ***hub*** est un équipement passif qui permet, notamment sur les réseaux Ethernet, de connecter en paires torsadées ou fibres optiques les stations du réseau.

b) Pont et commutateur

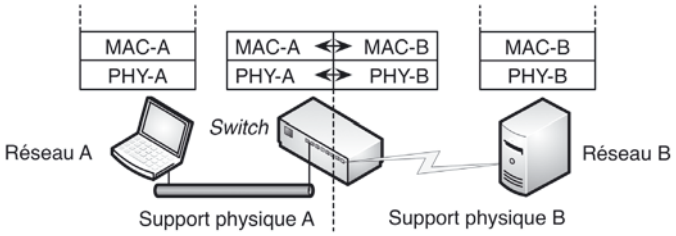


Figure 6.1 – Architecture d'un pont ou d'un commutateur.

Comme décrit figure 6.1, lorsqu'une station du réseau A veut transmettre des trames vers une station du réseau B, les en-têtes de la trame MAC sont décodés par **le pont** (*bridge*) qui les modifie de façon à les rendre compatibles avec les normes ou les contraintes du réseau B (pont Ethernet/WiFi par exemple).

Les principales fonctions des ponts sont donc :

- d'assurer la conversion du format de la trame et d'adapter sa longueur ;
- de filtrer éventuellement les trames en fonction de l'adresse du destinataire ;
- de positionner certains bits tels que ceux donnant la longueur de la trame ;
- de segmenter le trafic et d'éliminer la congestion sur une partie du réseau.

Pour assurer la communication d'un réseau à l'autre, le pont est capable de mémoriser dynamiquement (auto-apprentissage) les adresses de toutes les stations connectées. Le niveau physique peut également être différent entre les deux réseaux.

Le **commutateur Ethernet** (*switch*) présent sur les réseaux locaux Ethernet est également un dispositif d'interconnexion qui intervient au niveau 2 (voir chapitre 5). Son rôle est de commuter les trames sur les différents ports en fonction des adresses MAC de destination. Contrairement au pont, le commutateur ne fait que lire les adresses MAC sans modifier les en-têtes, sauf dans le cas particulier des VLAN tagués où il insère une étiquette d'identification du VLAN.

c) Routeur

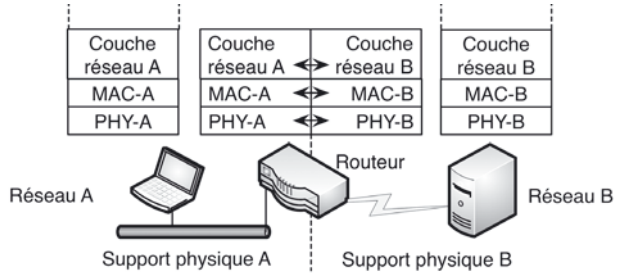


Figure 6.2 – Architecture d'un routeur.

Le rôle essentiel du routeur est d'effectuer le routage des paquets, c'est-à-dire le choix du chemin à partir de l'adresse de destination portée par le paquet. Dans un routeur, les en-têtes des paquets sont donc analysés et adaptés aux normes et aux contraintes du réseau sur lequel la trame est retransmise (figure 6.2).

Les routeurs ne sont pas capables d'apprendre les adresses comme les *switchs*, ils doivent tenir compte des différents protocoles réseau à gérer. La plupart des routeurs gèrent de plus les fonctions de niveau 2.

Les routeurs peuvent être administrés par un terminal ou un PC connecté et utiliser un protocole standard d'administration tel SNMP (*Simple Network Management Protocol*) ou encore à partir d'un ensemble de menus accessibles par des pages web stockées sur le routeur.

d) Passerelle

La passerelle (*gateway*), malgré sa complexité, est un élément essentiel dans les installations informatiques mettant en œuvre plusieurs types de réseaux. Les passerelles associées à des services ou des types de flux de données constituent un dispositif de conversion complet (ex. : passerelle VoIP/RTC, passerelle SMS/e-mails). Pour cela, elle possède une pile complète des sept couches OSI pour chacun des réseaux qu'elle sert.

6.1.2 La pile TCP/IP

À l'origine, les protocoles TCP/IP (*Transmission Control Protocol/Internet Protocol*) font partie de la hiérarchie des protocoles ARPA (*Advanced Research Project Agency*), sous l'égide du DOD (*Department Of Defense*) aux États-Unis. Ils sont intégrés dans tous les systèmes d'exploitation et constituent des protocoles de référence pour l'interconnexion des réseaux locaux à l'échelle d'une entreprise ou d'Internet.

Les protocoles TCP et IP servent de base à une famille de protocoles de niveau supérieur définis dans les RFC (*Requests For Comments*), documents publiés par l'IETF (*Internet Engineering Task Force*). Chaque protocole ou procédure lié à TCP/IP fait l'objet d'une RFC référencée : RFC 791 pour IP, RFC 793 pour TCP, RFC 2616 pour HTTP…

Ces protocoles sont antérieurs aux travaux de normalisation de l'OSI, mais une correspondance est généralement admise entre les couches du modèle TCP/IP et celles du modèle OSI (figure 6.3). Les couches 5 et 6 du modèle OSI, peu utilisées, ne sont pas représentées et les couches 1 et 2 sont regroupées dans la couche « *Network Access* », ce qui à l'époque était justifié car très peu d'architectures physiques de réseau existaient.

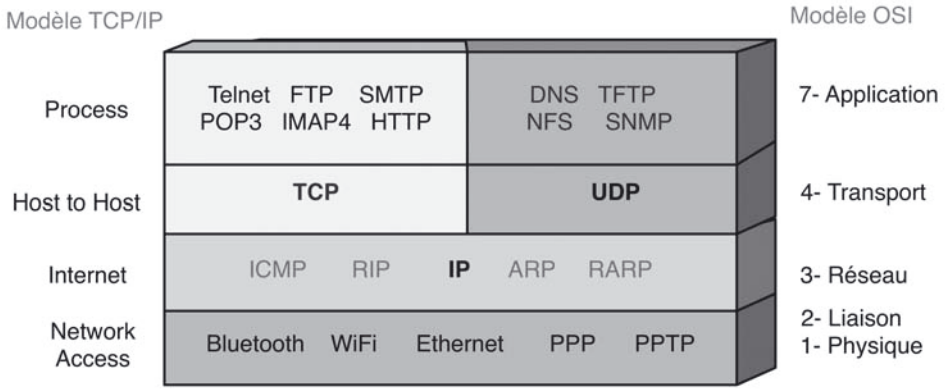


Figure 6.3 – **Correspondance entre les modèles TCP/IP et OSI.**

Aux niveaux 1 et 2, se trouvent les protocoles liés aux architectures **Ethernet**, **WiFi** ou autres décrites dans le chapitre 5.

Les protocoles **PPP** (*Point to Point Protocol*) et **PPTP** (*Point to Point Tunnelling Protocol*) sont des cas particuliers permettant d'adapter le réseau ou la station à une communication série asynchrone par l'intermédiaire d'un modem avec un serveur distant (cas du réseau Internet).

Au niveau 3, se trouve l'implantation du protocole IP (*Internet Protocol*) qui tient son nom de la nécessité d'interconnecter les réseaux (***Inter****connection* ***net****work*). Ce protocole, en mode datagramme, va offrir des fonctions d'adressage et de routage.

La couche 3 contient quatre autres protocoles :

- **ARP** (*Address Resolution Protocol*) permet de faire la correspondance entre les adresses logiques (Internet) et les adresses physiques (MAC). Les adresses MAC sont par construction uniques (numéro du constructeur, numéro de fabrication), mais leur allocation peut être vue comme aléatoire sur le réseau. Les adresses IP sont, elles, logiquement distribuées et permettent d'envoyer des données à une machine située n'importe où sur le réseau alors que les adresses physiques n'ont que la portée du réseau local. Il est donc plus simple pour l'administrateur réseau de référencer ses machines avec une adresse IP. Les mécanismes ARP permettent de faire la recherche de l'adresse MAC correspondante.
- **ICMP** (*Internet Control Message Protocol*) n'est pas à proprement parler un protocole de niveau 3, puisqu'il utilise l'encapsulation IP. Mais il sert à la gestion du protocole IP. Il permet, par exemple, de collecter les erreurs qui surviennent lors de l'émission de messages (réseau coupé, échéances temporelles…).
- **DHCP** (*Dynamic Host Configuration Protocol*) utilise les encapsulations IP et UDP et peut donc être considéré comme un protocole applicatif. Il est cependant traité dans ce chapitre car son rôle, très fortement lié à IP, est de permettre l'allocation dynamique par un serveur des adresses IP aux clients demandeurs dans le but de fédérer et de simplifier la gestion de ces adresses.

- **RIP** (*Routing Information Protocol*) est un protocole de routage, parmi d'autres, utilisant le principe de la multidiffusion. Les routeurs utilisant RIP diffusent périodiquement leurs tables de routage aux autres routeurs du réseau.

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

Le niveau 7 regroupe les différentes applications courantes au-dessus de TCP/IP (voir chapitre 8).

6.2 Le protocole IP (*Internet Protocol*)

Le protocole Internet est un protocole de niveau réseau. Il est responsable de :

- la transmission des données en mode sans connexion ;
- l'adressage et le routage des paquets entre stations par l'intermédiaire de routeurs ;
- la fragmentation des données.

Lors de l'**émission**, les fonctionnalités assurées sont :

- identification du paquet ;
- détermination de la route à suivre (routage) ;
- vérification du type d'adressage (station ou diffusion) ;
- fragmentation de la trame si nécessaire.

À la **réception**, les fonctionnalités sont :

- vérification de la longueur du paquet ;
- contrôle des erreurs ;
- réassemblage en cas de fragmentation à l'émission ;
- transmission du paquet réassemblé au niveau supérieur.

6.2.1 Format du paquet IP

Le paquet IP, ou datagramme IP, est organisé en champs de 32 bits (figure 6.4), c'est le format des adresses IP. Les fonctionnalités IP se retrouvent dans chaque groupement de bits de l'en-tête :

- Version : numéro de version du protocole IP (actuellement 4) ;
- Longueur de l'en-tête codée sur 4 bits et représentant le nombre de mots de 32 bits (généralement 5) ;
- Type de service (TOS) : désigne la qualité de service qui doit être utilisée par le routeur. Par exemple, pour un transfert de fichier important, il est préférable de privilégier le débit par rapport au délai de transmission. Pour une session interactive, le délai de propagation sera primordial ;
- Longueur totale : longueur totale du fragment (en-tête et données) exprimée en nombre d'octets ;

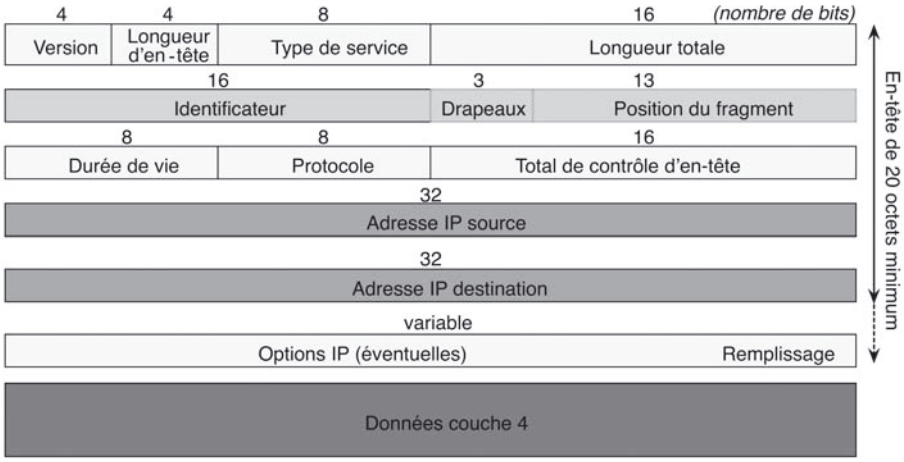


Figure 6.4 – **Format du paquet IP.**

- **Identificateur** : identifie le paquet pour la fragmentation (tous les fragments d'un même paquet portent le même numéro) ;
- **Drapeaux** : gère la fragmentation sur 3 bits suivant le format 0 DF MF :
  - ◇ le bit DF (*Don't Fragment*) demande au routeur de ne pas fragmenter le paquet ;
  - ◇ le bit MF (*More Fragment*) est positionné à 1 dans tous les fragments, sauf le dernier ;
- **Position du fragment** (*fragment offset*) : indique par multiple de 8 octets la position du fragment dans le paquet courant. Tous les fragments du paquet, sauf le dernier, doivent donc avoir pour longueur des multiples de 8 octets. Avec un codage sur 13 bits, le maximum pour un paquet est de 8 192 fragments ;
- **Durée de vie** (TTL, *Time To Live*) : indique en nombre de sauts la durée de vie d'un paquet. La valeur initiale à la création du paquet est de 32 ou 64 suivant la taille supposée du réseau (LAN ou WAN). La valeur est décrémentée à chaque passage dans un routeur. Si le TTL passe à 0, alors le paquet doit être détruit par le routeur, ce qui évite la circulation infinie de paquets à la recherche de destinations inexistantes ;
- **Protocole** : code qui indique le protocole de la couche supérieure (1 pour ICMP, 6 pour TCP, 17 pour UDP) ;
- **Options** : utilisées pour le contrôle ou la mise au point.

La figure 6.5 représente une trame capturée et décomposée couche par couche par un analyseur de protocole. Elle encapsule un paquet IP dont l'en-tête est analysé en détail. Ce paquet encapsule lui-même un segment TCP contenant une unité de données FTP. La fenêtre basse de l'analyseur de protocole présente en hexadécimal le contenu brut de la trame. On peut ainsi suivre l'analyse : le premier octet de l'en-tête IP est égal à 45_H. Le 4 représente la version du protocole, le 5 le nombre de mots de 32 bits, soit 20 octets. Les drapeaux analysés nous informent de l'absence de

fragmentation. Un peu plus loin, les adresses source et destination correspondent en hexadécimal aux valeurs décimales analysées (C0 A8 00 83 pour 192.168.0.131).

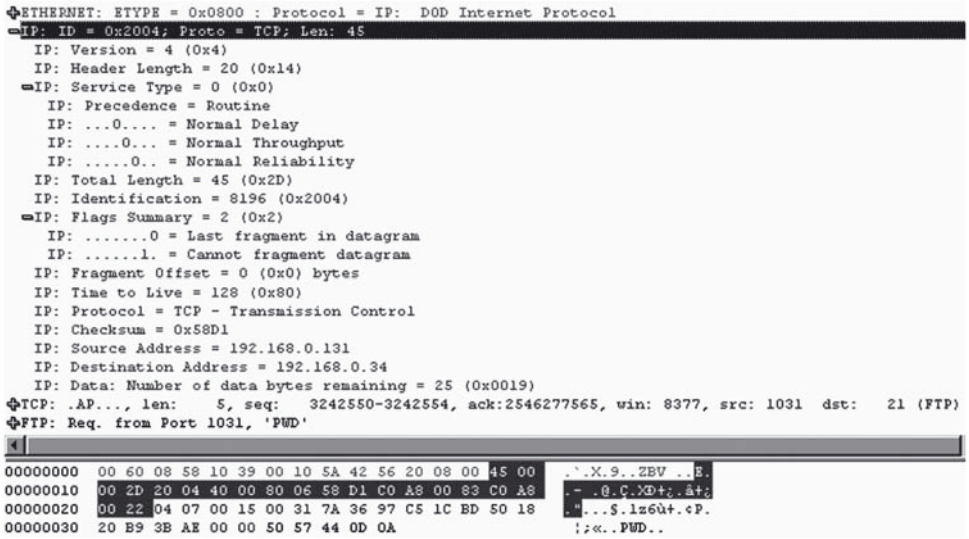


Figure 6.5 – **Exemple d'analyse IP.**

6.2.2 L'adressage Internet

a) Le format des adresses

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

Une autorité internationale, l'ICANN (*Internet Corporation for Assigned Names and Numbers*) attribue des numéros à chaque réseau. Les adresses codées sur 32 bits comportent deux parties : le numéro de réseau (*Net_id*) et le numéro de la machine sur le réseau (*Host_id*). L'ICANN n'alloue que les numéros de réseau. L'affectation des *Host_id* est à la charge des administrateurs des réseaux locaux. Suivant l'importance du réseau, plusieurs classes d'adressage sont possibles (figure 6.6).

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

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

- **classe A** : 1.0.0.0 à 126.0.0.0, soit 126 réseaux ($2^{8-1} - 2$) et 16 777 214 machines par réseau ($2^{32-8} - 2$) ;

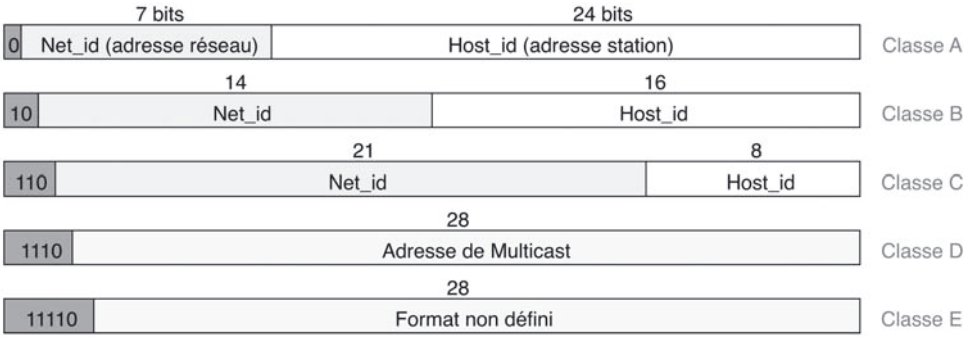


Figure 6.6 – **Format des adresses IP.**

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

La classe A représente donc les réseaux de grande envergure (ministère de la Défense, réseaux d'IBM, AT&T, DEC…) dont la plupart se trouvent aux États-Unis. **La classe B** désigne les réseaux moyens (universités, centres de recherches…). La **classe C** représente les petits réseaux régionaux, les PME/PMI et en règle générale les sites comprenant moins de 254 machines.

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

Les autres adresses sont particulières ou réservées :

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

Le nombre d'attribution d'adresses IP a suivi ces dernières années une croissance presque exponentielle, ce qui a conduit à une saturation. Au moment de la conception d'IP, l'adressage sur 32 bits qui offrait une capacité théorique de 2^{32} = 4,29 milliards d'adresses semblait suffisant… L'organisation en classes, justifiée au départ, a de plus généré un gaspillage important, notamment dans le cas des classes A sous-utilisées.

L'organisation en classe n'est donc plus guère utilisée et une ré-attribution des blocs d'adresses inutilisés grâce à des protocoles plus souples comme **CIDR** (*Classless InterDomain Routing*) ou l'utilisation multiple d'adresses privées et de système de translation d'adresses **NAT** (*Network Adress Translation*) permet de pallier, en partie, la pénurie. Parallèlement, la norme **IPv6** tente de remplacer la version 4 actuelle du protocole IP pour offrir un codage des adresses sur 128 bits (voir paragraphes suivants).

b) L'adressage de sous-réseaux (subneting) et les masques

Il peut être utile de segmenter le réseau en plusieurs sous-réseaux dans le but :

- de réduire le nombre de communications sur un même segment ;
- de connecter des réseaux d'architectures hétérogènes ;
- de regrouper les ordinateurs en domaines ou sous-domaines.

En cas de segmentation, les sous-réseaux seront interconnectés par des routeurs et les adresses des sous-réseaux correspondront à un sous-ensemble des adresses du réseau (voir exemple figure 6.7).

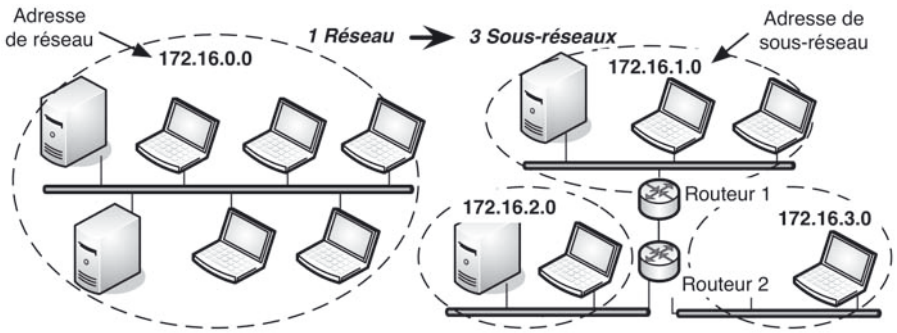


Figure 6.7 – Exemple de segmentation en sous-réseaux.

Les techniques d'adressage IP devront permettre de déterminer si un paquet est destiné à :

- une machine du même réseau ;
- une machine d'un sous-réseau différent sur le même réseau ;
- une machine sur un autre réseau.

Plus précisément, lorsqu'une segmentation en sous-réseaux est nécessaire, la partie de l'adresse Internet administrée localement (*host id* initial) peut être découpée en deux parties (figure 6.8) :

- une adresse de sous-réseau (*subnet_id*) ;
- un numéro de la machine dans le sous-réseau (*host_id*).

Figure 6.8 – Réorganisation du *host_id*.

Dans l'exemple de la figure 6.7, le troisième octet est utilisé entièrement pour numéroter les sous-réseaux (*subnet_id*), le quatrième octet correspond à la partie *host_id*.

Le système d'exploitation doit déterminer l'information désignant le sous-réseau et l'information désignant la machine. Cette structuration est employée, par exemple, dans les algorithmes de routage pour savoir si deux machines se trouvent sur le même sous-réseau.

Un **masque** de sous-réseau ou *netmask* a le même format qu'une adresse Internet. Les bits à 1 désignent la partie réseau (*net*) et sous-réseau (*subnet*) de l'adresse et les bits à 0 la partie numérotation des machines (*host*) sur le sous-réseau (figure 6.9). Il n'y a aucune raison pour que les bits à 1 soient contigus, mais le non-respect de cette règle entraînerait des difficultés de gestion inutiles.

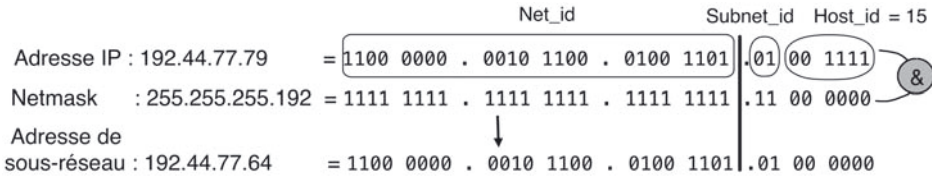


Figure 6.9 – Exemple d'utilisation du masque.

Un « ET logique » appliqué entre l'adresse de la machine et le masque permet de déterminer l'adresse du sous-réseau et donc de savoir si une destination est comprise dans ce sous-réseau ou doit être recherchée à travers un routeur.

Dans cet exemple de réseau de classe C, les 2 bits de poids fort des 8 bits disponibles sont utilisés pour identifier le sous-réseau. Il est ainsi possible de distinguer quatre adresses de sous-réseaux :

- 192.44.77.**00**000 0000 = 192.44.77.0
- 192.44.77.**01**00 0000 = 192.44.77.64
- 192.44.77.**10**000 0000 = 192.44.77.128
- 192.44.77.**11**00 0000 = 192.44.77.192

La première adresse est parfois exclue pour ne pas la confondre avec l'adresse du réseau, la dernière également pour éviter de confondre son *broadcast* avec le *broadcast* du réseau mais dans ce cas beaucoup d'adresses de machines sont inutilisées…

En l'absence de segmentation en sous-réseaux (*subnetting*), les masques sont ceux par défaut des classes standards :

- classe A : 255.0.0.0
- classe B : 255.255.0.0
- classe C : 255.255.255.0

Pour alléger la notation, les masques sont souvent notés sous forme de suffixe, ce dernier correspond au nombre de bits à 1.

Exemple

193.127.32.0 & 255.255.255.0 est équivalent à 193.127.32.0 / **24**.

c) Les masques de longueur variable VLSM

Lorsque la segmentation est utilisée, le masque de sous-réseau peut être de longueur variable si tous les sous-réseaux ne font pas la même taille. Il s'agit alors d'un masque de type VLSM (*Variable Lenght Subnet Mask*).

Dans ce cas, pour éviter les blocs d'adresses non alloués, on alloue les sous-blocs du plus grand au plus petit et on fait en sorte que les sous-blocs soient contigus.

Exemple

Un routeur possède trois interfaces pour connecter trois réseaux N1, N2 et N3. L'administrateur réseau impose les conditions suivantes :
– capacité d'adressage de N1, 40 stations ;
– capacité d'adressage de N2, 80 stations ;
– capacité d'adressage de N3, 140 stations ;
– utilisation au mieux du bloc 128.203.0.0 / 20.

La première étape consiste à trouver le nombre de bits pour la partie *host_id*, ce qui correspond à la puissance de 2 immédiatement supérieure au nombre de stations :
– N1 : 40 stations donc 6 bits (25 < 40 < 26) ;
– N2 : 80 stations donc 7 bits (26 < 80 < 27) ;
– N3 : 140 stations donc 8 bits (27 < 140 < 28).

Les masques sont donc :
– N1 : 255.255.255.192 (/26) ➔ 26 bits à 1 ; 6 bits à 0 ;
– N2 : 255.255.255.128 (/25) ➔ 25 bits à 1 ; 7 bits à 0 ;
– N3 : 255.255.255.0 (/24) ➔ 24 bits à 1 ; 8 bits à 0.

On alloue ensuite les blocs d'adresse du plus grand au plus petit :

– Premier bloc, le plus grand : N3.
Masque 255.255.255.0 soit 128.203.0.0/24.
Espace d'adressage de N3 : 128.203.0.0 à 128.203.0.255 (254 stations).

– Deuxième bloc : N2.
Masque 255.255.255.128 (/25).
On utilise le sous-bloc contigu à N3, donc : 128.203.1.0/25.
Espace d'adressage de N2 : 128.203.1.0 à 128.203.1.127 (126 stations).

– Le plus petit sous-réseau : N1.
Masque 255.255.255.192 (/26).
On utilise le sous-bloc contigu à N2, soit : 128.203.1.128/26.
Espace d'adressage de N1 : 128.203.1.128 à 128.203.1.191 (62 stations).

En utilisant cet algorithme, l'adressage IP est optimisé au maximum, C'est la façon dont les ISP gèrent, en principe, leurs espaces d'adressage IP.

d) La division des classes d'adresse avec CIDR

Comme indiqué précédemment, en attendant la généralisation d'IPv6 et des adresses sur 128 bits (voir paragraphe sur l'adressage IPv6), une solution est de s'affranchir des classes d'adresse et donc de mieux utiliser les adresses existantes.

Seules des classes C peuvent désormais être attribuées et beaucoup de sociétés ont besoin de plus de 256 adresses. Le protocole **CIDR (***Classless Inter Domain Routing*) permet d'agréger des classes C ou d'affecter une partie seulement d'une classe B en utilisant des préfixes pour indiquer aux routeurs qu'un seul sous-réseau correspond à trois classes C par exemple. On s'affranchit ainsi du découpage arbitraire et peu flexible en classes : l'allocation des ressources est plus fine et les tables de routages sont allégées au cœur du réseau.

Avec CIDR, toutes les adresses de réseaux sont annoncées avec leur préfixe qui correspond au nombre de bits à 1 du masque et remplace celui-ci. Par exemple :

- 193.127.32.0 & 255.255.255.0 ↔ 193.127.32.0 / 24
- 193.127.33.0 & 255.255.255.0 ↔ 193.127.33.0 / 24

Les deux réseaux explicites 193.127.32.0 et 193.127.33.0 peuvent être agrégés en 193.127.32.0 & 255.255.254.0. L'agrégat est noté 193.127.32.0 / 23, il désigne le couple préfixe/nombre de bits à 1 du masque.

Dans le cas d'une agrégation avec CIDR, on parle de ***supernetting***. On peut en effet considérer qu'il s'agit de l'opération inverse du *subnetting* : les réseaux ou sous-réseaux sont agrégés et non segmentés.

Les préfixes réseau étant de taille variable, les fournisseurs d'accès Internet peuvent allouer à leurs clients un espace d'adressage adapté à leur besoin. Imaginons le cas d'un fournisseur disposant du bloc d'adresses 206.0.64.0/18, soit 2^{14} (16 384) adresses individuelles ou 64 réseaux de 256 machines. Si un client demande 800 adresses, il peut se voir assigner soit une classe B (environ 64 700 adresses sont alors perdues), soit quatre classes C (et devoir rentrer quatre routes dans ses tables de routage). Avec CIDR, le fournisseur peut assigner à son client le bloc 206.0.68.0/22, soit 1 024 adresses.

e) Les réseaux privés et la translation d'adresses NAT

Une autre solution pour pallier à la pénurie d'adresses IPv4 est d'utiliser l'un des espaces d'adressage réservés aux réseaux privés isolés de l'Internet.

Le réseau de classe A 10.0.0.0, les réseaux de classe B allant de 172.16.0.0 à 172.31.0.0, ainsi que ceux de classe C allant de 192.168.0.0 à 192.168.255.0 sont définis par la RFC 1918 comme non attribués sur l'Internet et réservés à un usage privé. Il est alors possible de relier ces réseaux à l'Internet public en utilisant un dispositif de translation d'adresses ou **NAT** (*Network Address Translator*) proposé par la plupart des routeurs. Ces derniers vont attribuer à la volée une adresse publique aux machines internes qui souhaitent établir une connexion avec l'Internet, et effectuer une traduction automatique des adresses IP dans l'en-tête des paquets.

Dans l'exemple de la figure 6.10, le LAN privé n'est plus limité par le nombre d'adresses (jusqu'à 16 millions pour la classe A privée 10.0.0.0). Si l'entreprise dispose de la classe C publique 193.55.45.0, le NAT pourra affecter dynamiquement aux machines qui souhaitent accéder à l'Internet l'une des 254 adresses de la classe C. Le NAT garde une trace de toutes les connexions en cours en enrichissant dynamiquement une table de translation.

Ce mécanisme est particulièrement utilisé chez les particuliers qui possèdent plusieurs PC reliés en réseau et qui désirent partager une connexion Internet. Compte tenu du faible nombre de machines, c'est plutôt la classe C privée 192.168.0.0 qui est utilisée dans ce dernier cas.

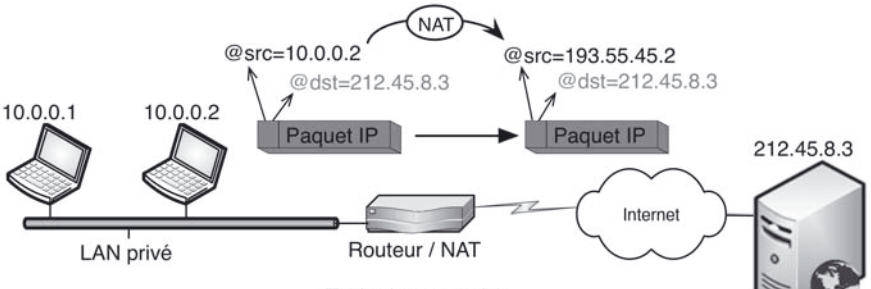


Table de translation

Interne		Externe	
@src	@dst	@src	@dst
10.0.0.2	212.45.8.3	19.55.45.2	212.45.8.3

Figure 6.10 – Exemple de translation d'adresses.

Si les 254 adresses possibles sont prises et que d'autres machines veulent établir une connexion vers l'extérieur, elles devront partager une adresse IP publique. Le NAT sera chargé de différentier les connexions en se basant sur les numéros de port TCP. Si ces numéros de port sont également identiques, les deux connexions ne pourront être différentiées (voir exemple de la figure 6.11). C'est pourquoi on utilise

systématiquement la translation de port associée à la translation d'adresse, on parle alors de **NAPT** (*Network Address and Port Translation*).

Dans l'exemple, les deux PC privés utilisent le même port source pour établir une connexion vers le même serveur externe. Après translation avec la même adresse source externe, si le port source n'est pas translaté, rien ne permet de différencier les paquets sortants et par suite de rediriger les réponses vers le bon PC. Le rôle de la table de translation est de garder en mémoire les correspondances des valeurs d'adresse et de port avant et après translation.

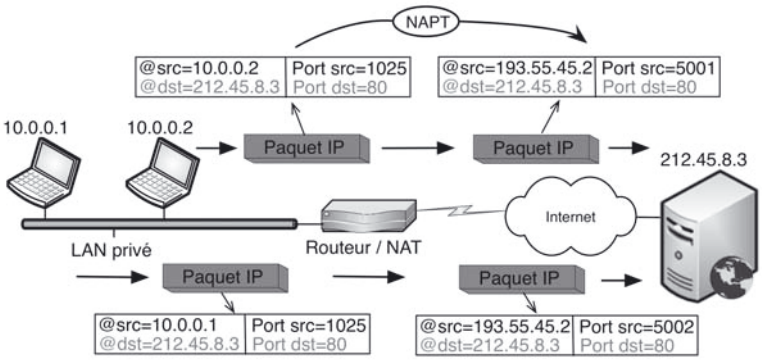


Table de translation

Interne				Externe			
@src	@dst	Port src	Port dst	@src	@dst	Port src	Port dst
10.0.0.1	212.45.8.3	1025	80	193.55.45.2	212.45.8.3	5001	80
10.0.0.2	212.45.8.3	1025	80	193.55.45.2	212.45.8.3	5002	80

Figure 6.11 – Exemple de translation d'adresse et de port.

f) L'adressage IPv6

L'un des principaux apports d'IPv6 consiste en l'augmentation massive du nombre d'adresses disponibles. De 32 bits, le système d'adressage passe à 128 bits ($2^{128} = 3{,}4 \cdot 10^{38}$), soit une réserve en principe suffisante d'adresses pour tous les usages.

Cette augmentation entraîne un passage de quatre « blocs » de 256 adresses pour IPv4 (en ne prenant pas compte des différents types d'adressage) à 16 blocs de taille équivalente pour IPv6 :

- **IPv4** : 212.180.62.226
- **IPv6** : 12.156.21.34.125.22.254.42.65.124.38.89.212.180.62.226

Afin de simplifier la période transitoire, IPv6 a été conçu pour être compatible avec IPv4, notamment en mettant en place un schéma autorisant l'imbrication d'adresses IPv4 au sein d'une structure IPv6 : les 128 bits de l'un pouvant facilement contenir les 32 bits nécessaires à l'autre. Dans ce cadre, les 32 bits de l'adresse originale sont placés en fin d'adresse IPv6, et tous les autres blocs sont mis à zéro.

Par ailleurs, pour faciliter la lecture et l'écriture de ces adresses, IPv6 définit une notation mixte pouvant prendre plusieurs formes. Tout en gardant les 32 bits finaux en décimal, les 96 bits précédents prennent une forme hexadécimale, et ne sont plus séparés par des points mais par des deux-points. Douze blocs en notation décimale deviennent ainsi six blocs en hexadécimal :

805B:2D9D:DC28:1080:200C:FC57:212.180.62.226

Précisons que chaque bloc de quatre chiffres hexadécimaux correspond à 16 bits, ce qui donne bien 6 × 16 bits + 32 bits = 128 bits.

Dans le cas d'une imbrication IPv4, on obtiendrait une suite de 0 précédant l'adresse originale :

0000:0000:0000:0000:0000:0000:212.180.62.226

Celle-ci est simplifiable en :

0:0:0:0:0:0:212.180.62.226

Elle peut également s'écrire :

::212.180.62.226

Les deux « deux-points » indiquent qu'il s'agit d'une adresse IPv6, et que tous les blocs précédents sont égaux à zéro. Ce principe s'applique bien sûr aux adresses normales IPv6 et permet de raccourcir certaines adresses contenant des blocs vides :

805B:2D9D:0000:DC28:12F7:000A:765C:D4C8

peut se simplifier en 805B:2D9D::DC28:12F7:A:765C:D4C8

Les longues chaînes de zéro peuvent également être combinées :

FE80:0000:0000:0000:0000:0000:0000:0001

donne FE80::1 en version abrégée.

Par ailleurs, lorsque l'on veut préciser l'adresse du réseau (net_id) et de la machine (host_id) une adresse se représente avec son préfixe (notation CIDR). Par exemple, la machine A200:E8FF:FE65:DF9A sur le réseau FEDC:6482:CAFE:BA05 :

FEDC:6482:CAFE:BA05:A200:E8FF:FE65:DF9A / 64

Si l'adressage est le principal apport d'IPv6, d'autres fonctionnalités sont également proposées. Le nouveau protocole simplifie le format d'en-tête des messages en rendant certains champs optionnels, voire en les supprimant. Il propose également des méthodes pour garantir la qualité et la complétude de l'information transmise, autorise des connexions facilitées pour les terminaux mobiles ainsi que les services multicast.

g) L'adressage multicast

Cet adressage, encore appelé envoi de groupe, consiste à émettre le même datagramme vers un groupe désigné de machines. Contrairement au mode diffusion (*broadcast*), le paquet n'est pas destiné à tous les hôtes d'un réseau, seulement à quelques machines qui n'appartiennent pas nécessairement au même réseau mais qui font partie d'un même groupe, identifié par une adresse IP.

Le *multicast* est utilisé par les applications nécessitant la transmission d'une même donnée vers de multiples destinations : VoD, retransmission d'événements, enseignement à distance, diffusion d'informations à une communauté…

Comparativement à la transmission *unicast*, le *multicast* permet d'économiser les ressources de la source et du réseau. Tandis qu'une source *unicast* émet autant de datagrammes qu'il existe de destinations, la source *multicast* génère un unique paquet. Les routeurs l'acheminent en limitant sa transmission aux réseaux qui contiennent un membre du groupe ou qui doivent être traversés pour en atteindre un, ce qui limite la congestion du réseau.

Les adresses de classe D sont réservées au multicast. Elles se caractérisent par les bits de poids fort 1110 et définissent la plage d'adresses 224.0.0.0 à 239.255.255.255. Elles sont uniquement utilisées comme adresse de destination.

Le *multicast* nécessite une méthode d'adressage, des protocoles de construction des groupes comme IGMP (*Internet Group Management Protocol*) ainsi que des protocoles de routage et de signalisation spécifiques.

6.3 Les autres protocoles de niveau 3

6.3.1 Le protocole ARP

Le **protocole ARP** (*Address Resolution Protocol*) permet de faire la correspondance entre les adresses logiques (IP) et les adresses physiques (MAC). Le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les deux types d'adresses dans une mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte sa table. Si l'adresse demandée ne s'y trouve pas, une recherche est réalisée suivant le principe (figure 6.12) :

- le module ARP envoie une requête ARP dans une trame avec une adresse MAC de diffusion générale (*broadcast*) pour que toutes les machines du réseau puissent la recevoir ;
- la couche ARP de la machine visée reconnaît que cette requête lui est destinée et répond par une réponse ARP contenant son adresse MAC (les autres machines l'ignorent) ;
- la réponse ARP est reçue par l'émetteur qui l'intègre dans sa mémoire cache et peut donc envoyer directement les paquets suivants avec la bonne adresse MAC de destination.

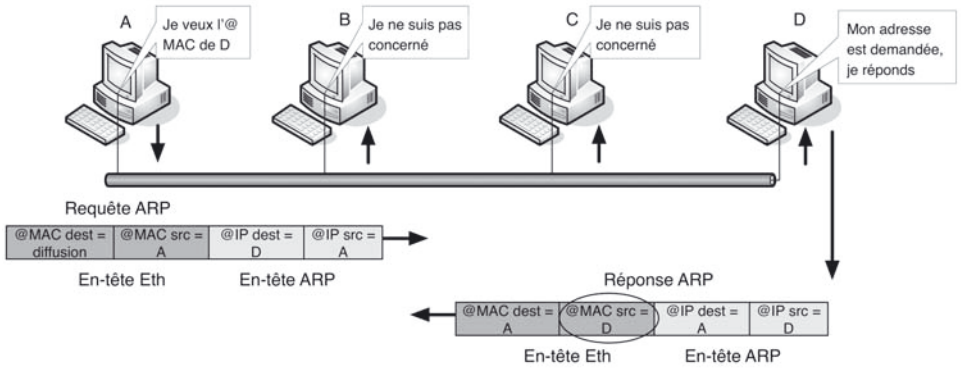


Figure 6.12

L'en-tête ARP présenté figure 6.13 comporte des indications sur la taille et la nature des adresses physiques et logiques qui sont la plupart du temps aux formats Ethernet et IP. Le code ARP précise l'opération effectuée : requête ou réponse.

Figure 6.13 – **Format de l'en-tête ARP.**

6.3.2 Le protocole ICMP

Le **protocole ICMP** (*Internet Control Message Protocol*) est utilisé pour gérer les informations contrôlant le trafic IP ; il permet notamment aux routeurs d'envoyer des messages de contrôle ou d'erreur vers d'autres ordinateurs ou routeurs connectés.

Les principales fonctions réalisées par ICMP sont :

- **contrôle de flux** : lorsque les datagrammes arrivent trop rapidement pour être traités, la destination renvoie un message de congestion qui indique à la source de suspendre temporairement l'envoi ;
- **détection de destination inaccessible** : lorsqu'une destination s'avère inaccessible, le système qui détecte le problème envoie un message « *destination unreachable* » vers la source ;
- **redirection des voies** : une passerelle envoie un message de redirection afin d'indiquer à une machine d'utiliser une autre passerelle qui constitue un meilleur choix ;
- **vérification des machines à distance** : une station peut envoyer le message d'écho ICMP par une commande de type « ping » pour vérifier que l'adresse et la couche IP du système distant sont opérationnelles ;

- **détection de temps expiré** : les paquets qui circulent en boucle sont identifiés grâce au champ TTL de l'en-tête IP ;
- **détection de paramètre incorrect** : la structure du paquet IP n'est pas conforme.

La figure 6.14 décrit le format du paquet ICMP qui comprend les différents champs :

- **Type** : indique le type de message de contrôle ICMP (*Echo Request*, *Echo Reply*, *Destination unreachable*, *Time Exceeded*…) ;
- **Code** : donne des informations complémentaires sur le message. Par exemple, le code 0 pour un paquet de type 3 (*Destination unreachable*), signifie Network unreachable, ce qui implique un routeur ou un lien en panne ; le code 1 signifie Host unreachable ;
- ***Checksum*** : permet une détection d'erreur sur l'en-tête ICMP ;
- **Paramètres** : dépend du type de message. Par exemple le type 3 n'utilise pas ce champ, les types 8 (*Echo Request*) et 0 (*Echo Reply*) l'utilisent pour stocker un identifiant et un numéro de séquence ;
- **Données** : recopie par défaut l'en-tête IP et les 64 premiers bits du datagramme original (celui ayant déclenché le message ICMP). La séquence est quelconque dans les messages de type « Echo », par exemple les premières lettres de l'alphabet.

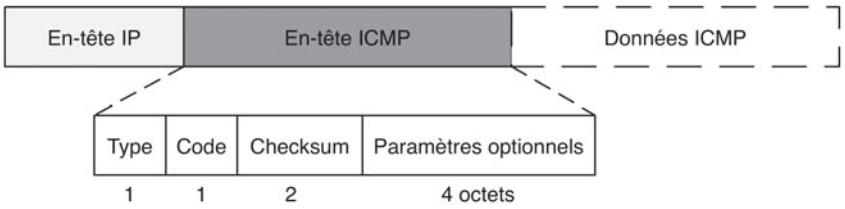


Figure 6.14 – **Format du paquet ICMP.**

6.3.3 Le protocole DHCP

DHCP (*Dynamic Host Configuration Protocol*) est un protocole de configuration dynamique d'hôte qui permet d'allouer à la demande des adresses IP aux machines se connectant au réseau. Il présente les avantages suivants :

- une gestion centralisée des adresses IP ;
- les ordinateurs clients ne requièrent pas de configuration IP manuelle ;
- le nombre d'adresses IP disponibles peut être supérieur au nombre de machines du réseau.

Un serveur DHCP est configuré dans le réseau, il possède une table d'adresses IP valides localement et attribue dynamiquement une adresse IP disponible à une nouvelle machine se connectant au réseau. La base de données du serveur DHCP contient les informations suivantes :

- une table d'adresses IP valides et des adresses IP réservées qui seront affectées manuellement ;

- des paramètres de configuration valides pour tous les clients du réseau (masques, adresses particulières…) ;
- la durée des baux (le bail définit la période de temps durant laquelle l'adresse IP attribuée peut être utilisée).

Le processus d'attribution dynamique d'une adresse IP se déroule en quatre étapes (figure 6.15) :

- **découverte** (*discover*) : le client envoie une trame de diffusion sur le réseau vers un serveur DHCP (l'adresse IP du client en attente d'attribution est l'adresse réservée 0.0.0.0) ;
- **offre** (*offer*) : tous les serveurs DHCP répondent au client en lui faisant une offre ;
- **demande** (*request*) : le client répond à un serveur DHCP en lui précisant qu'il accepte l'offre proposée ;
- **accusé de réception** (*ACK*) : le serveur DHCP confirme le bail avec sa durée et les options associées.

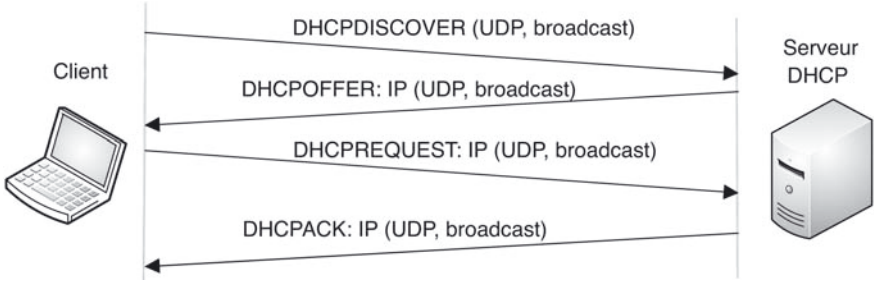


Figure 6.15 – Échange DHCP.

Une fois une adresse affectée, le client devra renouveler le bail avant son expiration s'il souhaite continuer à l'utiliser. Ce renouvellement passe par les étapes suivantes :

- à 50 % de la durée du bail, émission d'un DHCPREQUEST (*unicast*) contenant l'adresse attribuée :
  - ◇ le serveur ne répond pas : la demande devra être réémise en *broadcast* à 87,5 % de la durée du bail,
  - ◇ le serveur répond défavorablement (DHCPNAK) : le client doit cesser d'utiliser cette adresse mais peut recommencer le processus d'obtention,
  - ◇ le serveur répond favorablement (DHCPACK) : ce message indique une nouvelle durée du bail ;
- la demande à 87,5 % de la durée du bail diffère de la précédente par la destination (*broadcast*). Si aucun serveur ne répond, aucune nouvelle demande ne doit être émise et le client devra cesser d'utiliser l'adresse à expiration du bail.

Lorsqu'un client n'a plus besoin d'une adresse (déplacement d'une station sur un autre réseau par exemple), il doit la libérer (DHCPRELEASE).

6.4 Le routage

6.4.1 Principe

Le routage d'un paquet consiste à trouver le chemin de la station destinatrice à partir de son adresse IP. Si le paquet émis par une machine ne trouve pas sa destination dans le réseau ou sous-réseau local, il doit être dirigé vers un routeur qui rapproche le paquet de son objectif. Il faut par conséquent que toutes les stations du réseau possèdent l'adresse du routeur par défaut. La machine source applique le masque de sous-réseau (*netmask*) pour savoir si le routage est nécessaire.

Chaque routeur doit donc connaître l'adresse du routeur suivant lorsque la machine de destination n'est pas sur les réseaux ou sous-réseaux qui lui sont raccordés. Le routeur intègre au moins deux interfaces réseau avec une adresse IP dans chaque réseau connecté. Il doit gérer une table de routage de manière statique ou dynamique.

La figure 6.16 présente un exemple de réseaux interconnectés. Le routeur A possède quatre interfaces Ethernet et autant d'adresses IP, celles-ci étant généralement choisies dans les premières adresses du réseau connecté.

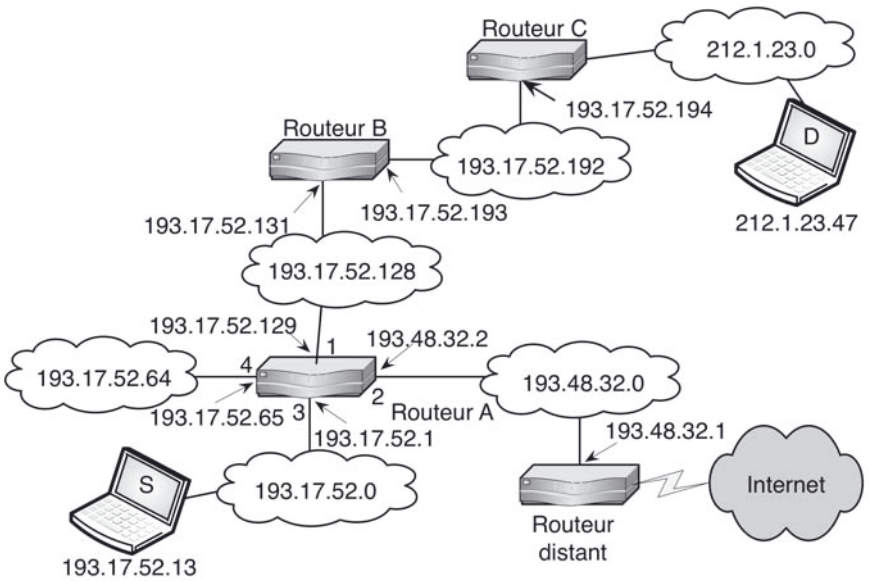


Figure 6.16 – **Exemple d'interconnexion.**

La table de routage du routeur A est donnée tableau 6.1. Les quatre premières lignes correspondent à des réseaux directement connectés sur le routeur A, on retrouve donc les adresses de celui-ci pour chacun des ports Ethernet. Le réseau 193.17.52.0 est décomposé en quatre sous réseaux (193.17.52.0, 193.17.52.64,

193.17.52.128 et 193.17.52.192). Les masques permettent de préciser les plages d'adresses concernées des réseaux destination.

Tableau 6.1 – Exemple de table de routage.

Adresse du réseau destination	Masque du réseau destination	Adresse du prochain routeur	Interface empruntée	Nombre de sauts
193.17.52.128	255.255.255.192	193.17.52.129	Ethernet 1	0 (direct)
193.48.32.0	255.255.255.0	193.48.32.2	Ethernet 2	0 (direct)
193.17.52.0	255.255.255.192	193.17.52.1	Ethernet 3	0 (direct)
193.17.52.64	255.255.255.192	193.17.52.65	Ethernet 4	0 (direct)
193.17.52.192	255.255.255.192	193.17.52.131	Ethernet 1	1
212.1.23.0	255.255.255.0	193.17.52.131	Ethernet 1	2
0.0.0.0	0.0.0.0	193.48.32.1	Ethernet 2	0

La cinquième ligne indique que lorsque le routeur A reçoit un paquet dont l'adresse de destination est sur le réseau 193.17.52.192, le paquet doit être envoyé au routeur B d'adresse 193.17.52.131 qui assurera le relais. Dans la mesure où le paquet devra traverser un routeur supplémentaire, le nombre de sauts est incrémenté de 1. La sixième ligne définit sur le même principe la route vers le réseau 212.1.23.0 qui passera par les routeurs B et C avec un nombre de sauts égal à 2. La dernière entrée définit le routage par défaut : si aucune des routes définies précédemment ne convient, le paquet est renvoyé vers la machine 193.48.32.1 qui est un routeur distant. Le nombre de sauts est dans ce cas à zéro, car non connu.

Si la station 193.17.52.13 veut envoyer un paquet à la station 212.1.23.47, le routage va se dérouler en quatre phases :

- la station source S connaissant sa propre adresse et son masque en déduit que l'adresse destination se trouve dans un autre réseau, elle adresse donc le paquet au routeur A qui est son routeur par défaut ;
- le routeur A qui reçoit le paquet lit l'adresse de destination et consulte sa table de routage, il dirige en conséquence le paquet vers le routeur B ;
- le routeur B suit le même processus et transmet le paquet au routeur C ;
- le routeur C peut enfin délivrer le paquet à la destination D qui se trouve sur un de ses réseaux connectés.

Par ailleurs, dans la mesure où le routeur A n'a pas les moyens de connaître les réseaux non directement connectés et le nombre de sauts pour les atteindre, des informations de routage doivent être échangées entre les routeurs (B devra par exemple indiquer à A qu'il est directement connecté au réseau 192.17.52.192 et qu'il connaît par C le réseau 212.1.23.0). C'est le principe du routage dynamique et des protocoles associés.

6.4.2 Les algorithmes de routage

Dans le cas du **routage statique**, la table est établie et modifiée manuellement. Ce type de routage simple peut être utilisé pour un petit réseau local avec une connexion externe.

Pour le **routage dynamique**, la table est mise à jour périodiquement et automatiquement à l'aide de protocoles spécifiques. Les routeurs envoient régulièrement la liste des réseaux ou des sous-réseaux que l'on peut atteindre par eux. Ce qui permet aux autres routeurs de mettre à jour leurs tables de routage. Pour les réseaux maillés, ils évaluent dynamiquement la meilleure route vers chaque réseau ou sous-réseaux.

Deux types d'algorithmes de routage dynamique existent :

- les **algorithmes à vecteurs de distance** (*Vector-Distance*) pour lesquels les informations échangées permettent pour chaque routeur de retenir la plus courte distance (le plus petit nombre de sauts) pour atteindre une destination ;
- les **algorithmes à état de lien** (*Link-State*) basés sur la transmission d'une carte complète des liens possibles entre les routeurs, ceux-ci doivent ensuite localement calculer les meilleures routes pour une destination.

a) Algorithmes à vecteur de distance

Ils sont basés sur l'algorithme de Belman-Ford :

- un routeur diffuse régulièrement à ses voisins les routes qu'il connaît ;
- une route est composée d'une adresse destination, d'une adresse de routeur et d'une métrique indiquant le nombre de sauts nécessaires (la distance) pour atteindre la destination ;
- un routeur qui reçoit ces informations compare les routes reçues avec ses propres routes connues et met à jour sa table de routage :
  - ◇ si une route reçue comprend un plus court chemin (nombre de sauts +1 inférieur),
  - ◇ si une route reçue est inconnue.

Dans l'exemple donné figure 6.17, le routeur A reçoit à un instant donné le vecteur contenant les routes connues par le routeur voisin J. Le routeur A examine chaque route transmise et effectue si nécessaire une mise à jour de sa table de routage. Ainsi, l'entrée pour atteindre le réseau 4 est modifiée car le routeur J connaît une route plus courte. Le nombre de sauts transmis est de 3, le routeur A ajoute 1 saut pour aller jusqu'à J. Une nouvelle entrée pour atteindre le réseau 21 est également ajoutée.

Ce type d'algorithme que l'on retrouve dans le protocole **RIP** à l'avantage de la simplicité pour des réseaux limités mais présente plusieurs inconvénients parmi lesquels :

- la taille des informations de routage est proportionnelle au nombre de routeurs interconnectés ;

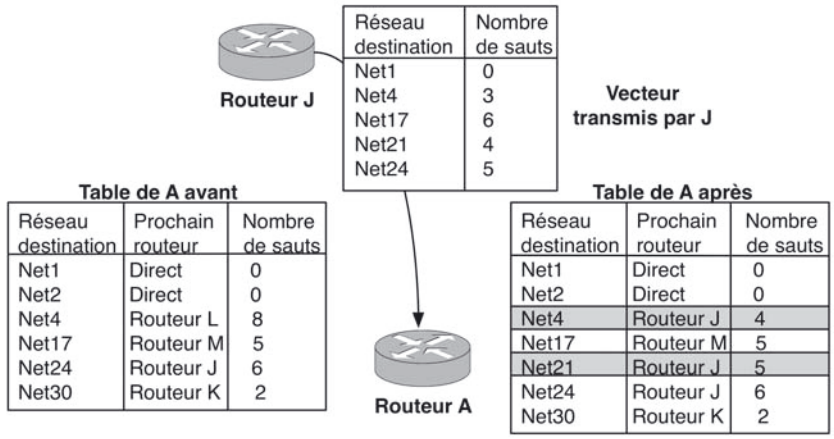


Figure 6.17 – Exemple d'application de l'algorithme *Vector-Distance*.

- la métrique de distance est difficilement utilisable sur des réseaux étendus car elle présente une grande lenteur de convergence (beaucoup d'échanges sont nécessaires avant d'obtenir des valeurs de distance optimisées et stables) ;
- des bouclages peuvent exister, éventuellement à l'infini (le routeur A transmet une route erronée au routeur B qui la retransmet à A avec un coût augmenté de 1…) ;
- il ne peut y avoir de chemins multiples.

b) Algorithmes à état des liens

Ils sont basés sur la technique du plus court chemin (SPF, *Shortest Path First*) :

- les routeurs maintiennent une carte complète du réseau et calculent les meilleurs chemins localement en utilisant cette topologie ;
- les routeurs ne communiquent pas la liste de toutes les destinations connues (contrairement aux algorithmes *Vector-Distance*) ;
- un routeur basé sur l'algorithme SPF teste périodiquement l'état des liens qui la relient à ses voisins, puis diffuse périodiquement ces états (*Link-State*) à tous les autres routeurs du domaine ;
- les messages diffusés ne spécifient pas des routes mais simplement l'état (*up*, *down*) entre deux routeurs ;
- lorsqu'un message parvient à un routeur, celui-ci met à jour la carte de liens et recalcule localement, pour chaque lien modifié, la nouvelle route selon l'algorithme de Dijkstra (*Shortest Path Algorithm*) qui détermine le plus court chemin pour toutes les destinations à partir d'une même source.

La figure 6.18 montre un exemple d'application de cet algorithme. Tous les routeurs possèdent à un instant donné la même table des liens. Si le routeur A veut envoyer un paquet vers le routeur C, il calcule le plus court chemin vers C et sélectionne en conséquence le routeur B pour lui envoyer le paquet ; B trouve à son tour le plus court chemin vers C qui est direct.

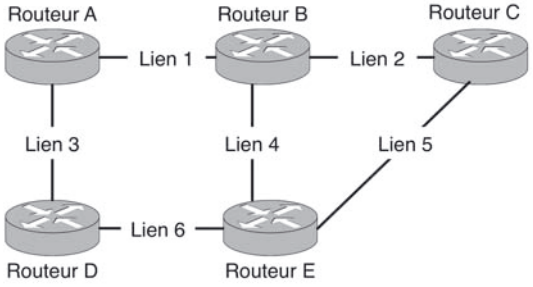


Table des liens

De	à	Lien	Distance
A	B	1	1
A	D	3	1
B	A	1	1
B	C	2	1
B	E	4	1
C	B	2	1
C	E	1	1
D	A	3	1
D	E	6	1
E	B	4	1
E	C	5	1
E	D	6	1

Figure 6.18 – **Exemple d'application de l'algorithme *Link-State*.**

Ce type d'algorithme présente plusieurs avantages :

- la convergence est rapide et sans boucle ;
- les chemins multiples sont possibles ;
- les métriques ne sont pas limitées à la distance (par exemple, la distance peut être remplacée par le débit et la meilleure route calculée sera celle présentant le meilleur débit) ;
- chaque routeur calcule ses routes indépendamment des autres ;
- les messages diffusés sont inchangés d'un routeur à l'autre et permettent un contrôle aisé en cas de dysfonctionnement ;
- les messages ne concernent que les liens directs entre routeurs et ne sont donc pas proportionnels au nombre de réseaux dans le domaine.

OSPF (*Open Shortest Path First*) est un protocole à état des liens qui possède la particularité de pouvoir utiliser des déclarations de lien entre sous-réseau IP et routeur (il n'est pas nécessaire de déclarer tous les liens entre toutes les stations du sous-réseau et le routeur). C'est un protocole plus efficace que **RIP**, en revanche les calculs locaux peuvent être assez lourds et les formats des messages ainsi que les échanges sont relativement complexes.

En conclusion, les algorithmes *Link-State* sont plus complexes mais plus performants et mieux adaptés au facteur d'échelle que les algorithmes *Vector-Distance*.

6.4.3 Le routage sur Internet

Pour l'Internet, qui est constitué par l'interconnexion d'une grande quantité de réseaux, une organisation hiérarchique est établie pour séparer des domaines de routage (figure 6.19) :

- le routage à l'intérieur de **systèmes autonomes** (AS, *Autonomous System*) qui correspondent à un domaine de routage lié à un découpage de l'Internet et sous la responsabilité d'une autorité unique (un AS est identifié par un numéro unique attribué par l'ICANN) ;

- le routage d'interconnexion entre les AS.

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

- les protocoles de routage interne **IGP** (*Interior Gateway Protocols*) tels que **RIP** et **OSPF** qui concernent les routeurs internes ;
- les protocoles de routage externe comme **EGP** (*Exterior Gateway Protocol*) ou **BGP** (*Border Gateway Protocol*) utilisés par les routeurs externes ou routeurs de bord (*border routers*).

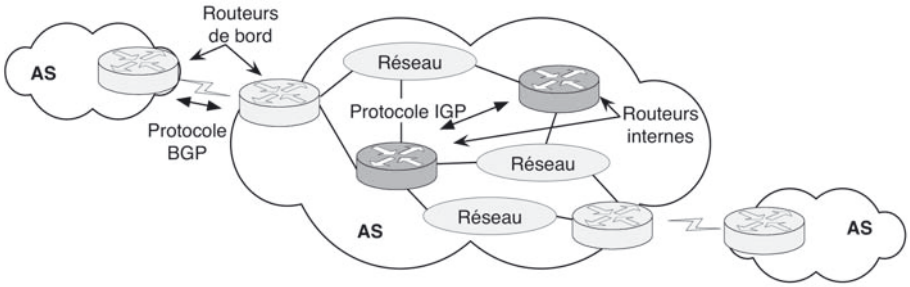


Figure 6.19 – **Organisation hiérarchique du routage.**

6.4.4 Le protocole RIP

RIP (*Routing Information Protocol*) est un protocole à vecteur de distance qui utilise une technique de diffusion (*broadcast*) périodique. Les transferts se font à l'aide de datagrammes UDP émis toutes les 30 secondes. La distance évaluée (la métrique) est le nombre de sauts, exprimée comme un nombre entier variant de 1 à 15 ; la valeur 16 correspond à l'infini. Si une route n'est pas annoncée au moins une fois en 3 minutes, la distance correspondante devient « infinie ».

Les messages au format RIP (figure 6.20) commencent par un mot de 32 bits comportant le code de la commande et un numéro de version, suivi par un ensemble de couples adresse/métrique occupant 5 mots de 32 bits.

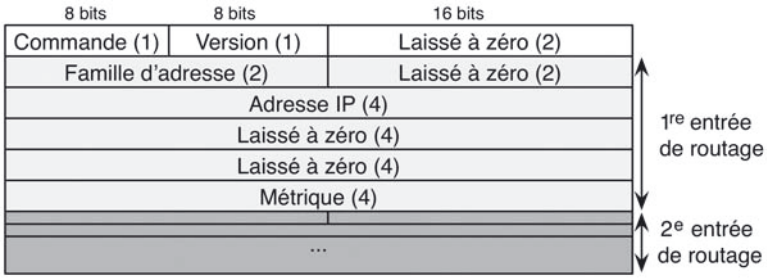


Figure 6.20 – **Format des messages RIP.**

Les messages peuvent être de deux types :

- une requête (champ commande à 1) permet de demander à l'autre routeur d'envoyer tout ou partie de sa table de routage ;
- une réponse (champ commande à 2) contient tout ou partie de la table de routage de la machine émettrice.

Chacun des couples adresse/métrique permet la mise à jour des tables de routage du routeur recevant le message suivant l'algorithme de Belman-Ford décrit précédemment ; le champ « famille d'adresse » est par défaut à 2 pour les adresses IP. Le message RIP peut comporter jusqu'à 25 entrées de routage de 20 octets chacune (la taille totale du message reste inférieure à 512 octets).

Suivant l'état du routeur, différentes séquences sont mises en œuvre :

- *Initialisation*. Le routeur envoie sur chacune de ses interfaces une requête pour demander la table complète des routeurs connectés (le champ « address family » est à 0 et la métrique à 16) ;
- *Requête reçue*. Pour une requête d'initialisation, la table de routage intégrale est transmise. Sinon, pour chaque route demandée, la métrique en cours est renvoyée (16 pour une route inconnue) ;
- *Réponse reçue*. Le routeur peut mettre à jour sa table de routage en ajoutant, modifiant ou détruisant les différentes entrées ;
- *Mises à jour périodiques*. Toutes les 30 s une partie ou l'intégralité de la table est envoyée aux routeurs adjacents par diffusion (*broadcast*) ou sur une liaison point à point entre deux routeurs ;
- *Mises à jour déclenchées*. Lorsque la métrique d'une route varie, les entrées concernées sont transmises aux routeurs voisins.

Une deuxième version de RIP propose un ensemble d'améliorations : le routage par sous-réseau, le support de CIDR, l'authentification des messages et la transmission multipoint. Elle utilise les espaces vides prévus dans le format des messages de la première version.

RIP est géré par tous les routeurs et sa simplicité permet une implémentation rapide. Les risques d'erreur sont limités et le résultat global satisfaisant si la topologie du réseau reste simple et les liaisons fiables. Mais pour des réseaux complexes, chaque changement de topologie n'est corrigé que lentement (convergence lente). Pendant le temps nécessaire au calcul, le réseau est dans un état intermédiaire où il peut y avoir des boucles pouvant causer des congestions temporaires.

La figure 6.21 présente une analyse de message RIP relevée sur un réseau Ethernet. Le port UDP 520 correspondant à RIP est utilisé pour la source et la destination. Il s'agit d'une réponse et le deuxième couple adresse/métrique est détaillé : deux sauts sont nécessaires pour atteindre le réseau 10.0.0.12/30 à partir du routeur 10.0.0.2.

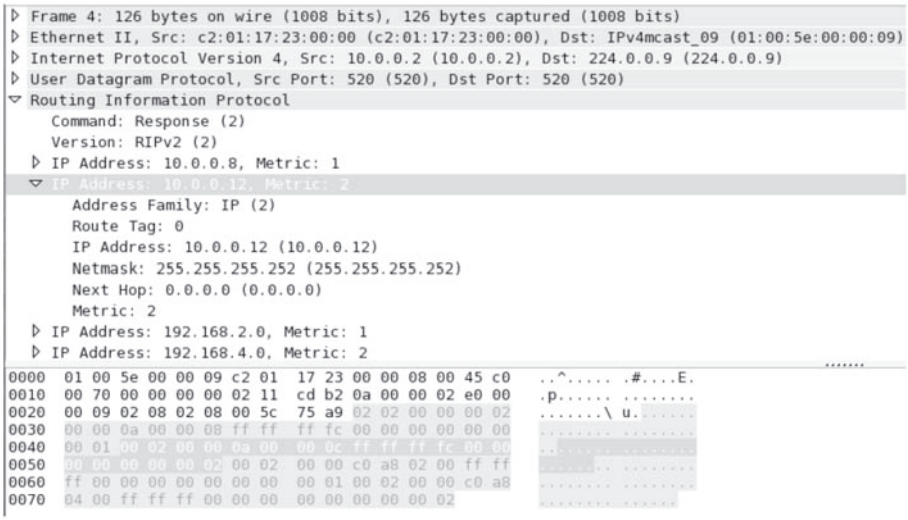
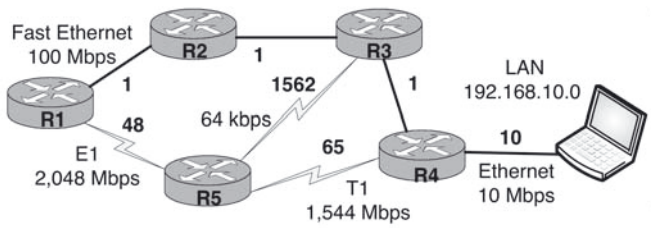


Figure 6.21 – **Exemple d'analyse RIP.**

6.4.5 Le protocole OSPF

OSPF (RFC 2328) est un protocole à état des liens globalement plus efficace que RIP et qui tend à remplacer ce dernier pour le routage interne. En revanche, les calculs locaux peuvent être assez lourds et les formats des messages ainsi que les échanges sont relativement complexes.

OSPF utilise l'algorithme SPF (*Shortest Path First*) afin d'élire la meilleure route, celle présentant le coût cumulé le plus faible sur l'ensemble de ses liens, vers une destination donnée. Dans l'exemple décrit à la figure 6.22, il s'agit d'atteindre le réseau local 192.168.10.0 à partir du routeur R1. Avec le protocole RIP, la route la plus courte en nombre de sauts passe par R5. Si certains liens présentent un débit plus élevé que d'autres, le choix de RIP n'est pas forcément pertinent. Le protocole OSPF attribue un coût à chaque lien afin de privilégier l'élection de certaines routes. Dans l'exemple, la métrique choisie est le débit. Suivant la table des liens et les coûts associés, la route OSPF passera par R2, R3 et R4 avec un coût total de 13 (1+1+1+10) et un débit minimum de 10 Mbit/s sur toute la route.



Lien	Coût
R1-R2	1
R1-R5	48
R2-R3	1
R3-R4	1
R3-R5	1562
R4-R5	65
R4 LAN	10

Figure 6.22 – **Exemple de coût sur les liens OSPF.**

Un réseau OSPF est divisé en plusieurs zones (*Areas*) qui se connectent à une zone centrale de distribution, *Area 0*, appelée aussi le *backbone*. À terme, tous les routeurs auront la même base de données sur l'état des liens de tous les autres routeurs appartenant à la même zone. Avant de pouvoir effectuer leur travail de routage à l'intérieur de cette même zone, les routeurs OSPF doivent préalablement remplir les tâches décrites ci-dessous.

a) Établir la liste des routeurs voisins à l'aide de messages hello

Des paquets de données *hello* sont envoyés périodiquement (par défaut toutes les 10 s) sur chaque interface du routeur où le processus de routage dynamique a été activé. L'adresse *multicast* 224.0.0.5 est utilisée, tout routeur OSPF se considère comme destinataire. Les paquets *hello* permettent à chaque routeur de s'annoncer auprès de ses voisins (deux routeurs sont dits voisins s'ils ont au moins un lien en commun) et d'intégrer leurs adresses IP dans une base de données appelée « base d'adjacences » (*adjacencies database*), en vérifiant que le lien est bien symétrique. Ce processus est généralisé à l'ensemble des routeurs de la zone qui à terme connaîtront les adresses IP de tous leurs voisins.

b) Élire le routeur désigné

Dans une zone OSPF, il est nécessaire d'élire un routeur désigné (DR, *Designated Router*) qui servira de référent pour la base de données topologique (la carte des liens) représentant le réseau. Cette élection répond à trois objectifs :

- réduire le trafic lié à l'échange d'informations sur l'état des liens (il n'y a pas d'échange entre tous les routeurs mais entre chaque routeur et le DR) ;
- améliorer l'intégrité de la base de données topologique (cette base de données doit être unique) ;
- accélérer la convergence, c'est-à-dire le temps mis pour que tous les routeurs aient la même table complète et à jour (point faible de RIP).

Par convention, le DR est celui qui a la priorité (*Router Priority*) la plus élevée, celle-ci est codée sur 8 bits et fixée par défaut à 1 sur tous les routeurs OSPF. L'administrateur codera une valeur supérieure sur le routeur qu'il veut privilégier. L'élection du DR se fait à l'aide d'échange de paquets *hello* qui contiennent l'adresse et la valeur de priorité du routeur émetteur.

c) Découvrir les routes

Pour constituer la base de données topologique, les routeurs doivent communiquer les liens qu'ils connaissent. Sur une interface sans DR (liaison point à point par exemple), les mises à jour OSPF sont envoyées directement au voisin. Sur une interface avec un DR, les routeurs « non DR » envoient leurs mises à jour au DR en utilisant l'adresse *multicast* 224.0.0.6. Le DR relaie les mises à jour à tous les routeurs OSPF en utilisant l'adresse *multicast* 224.0.0.5.

Dans un premier temps, le routeur émetteur (le plus souvent le DR) commence par transmettre un résumé de sa base de données topologique *via* des paquets de

données appelés DBD (*DataBase Description*). Plus précisément, ces paquets contiennent un extrait des enregistrements LSA (*Link State Advertisement*) qui comprend essentiellement l'identificateur du lien et un numéro de séquence. Ce numéro permet de déterminer l'ancienneté des informations reçues. Si les LSA reçus sont plus récents que ceux dans sa base topologique, le routeur récepteur demande une information plus complète par un paquet LSR (*Link State Request*).

Le routeur émetteur répond par des paquets LSU (*Link State Update*) contenant l'intégralité du LSA demandé et notamment le coût du lien ou des liens si le routeur en possède plusieurs (figure 6.23). Au bout d'un certain nombre d'échanges de LSAs, chaque routeur possédera la table complète d'état des liens à un instant donné. Un changement d'état sur un lien est ensuite signalé si besoin par le routeur possédant l'interface correspondante.

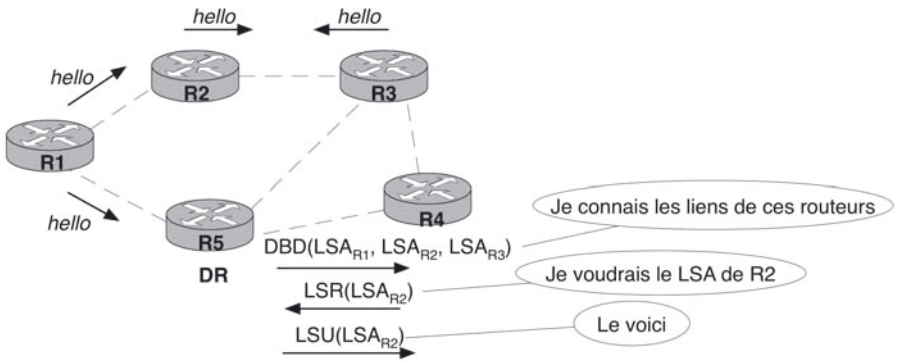


Figure 6.23 – Exemple de construction de la topologie OSPF.

d) Sélectionner les bonnes routes

Chaque routeur possédant la table à jour des liens est capable de calculer au besoin la nouvelle route vers une destination selon l'algorithme de Dijkstra (*shortest path algorithm*).

e) Maintenir la base topologique

Quand un changement survient sur un lien, les routeurs doivent avertir leurs voisins. Les paquets *hello* sont envoyés par défaut toutes les 10 s : au bout de 40 s de silence, un lien sera considéré comme non actif. Le routeur envoie alors un paquet LSU contenant l'information du nouvel état du lien au DR (224.0.0.6) qui fera passer le message aux autres routeurs (224.0.0.5). Une fois reçu le LSU, les routeurs mettent à jour leur base de données d'état de lien. Si aucun changement d'état n'intervient dans le réseau, les informations seront quand même mises à jour périodiquement, la période d'existence par défaut des LSA est fixée à 30 minutes.

La figure 6.24 montre un exemple d'analyse OSPF pour un paquet de type LSU comprenant deux LSA. L'information provient du DR 10.3.3.3 et est destinée à tous les routeurs non DR (224.0.0.5). Le type du premier LSA (*Router-LSA*) indique que

le LSA décrit les états de toutes les interfaces du routeur, dans ce cas, l'identificateur du lien (*Link State ID*) a même valeur que celle du routeur à l'origine du LSA (*Advertising Router*). Le premier LSA décrit 7 liens avec, pour chacun, le type de lien, l'identificateur et le coût (*metric*).

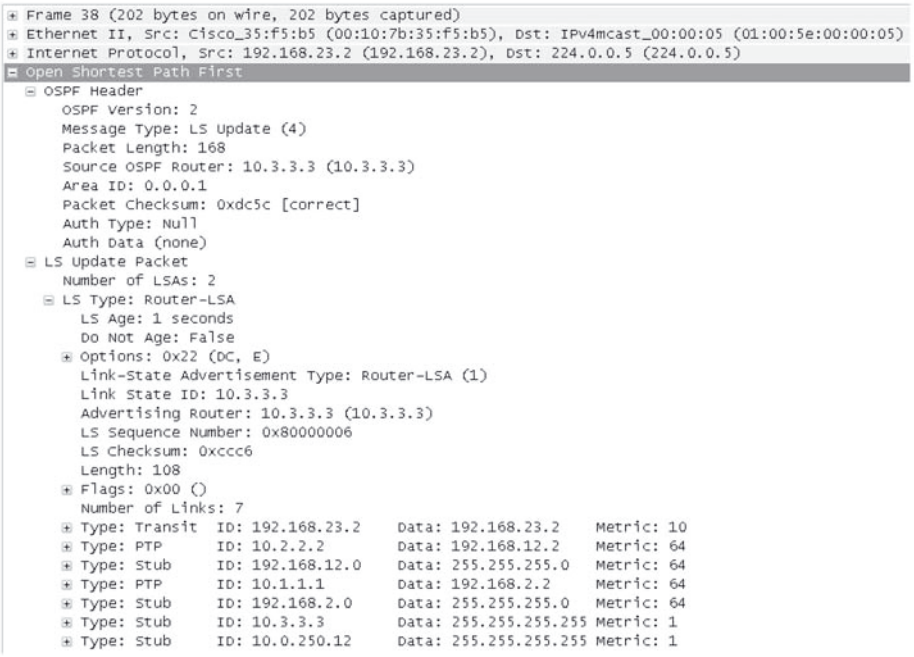


Figure 6.24 – Exemple d'analyse d'un paquet LSU.

6.4.6 Le protocole BGP

BGP (RFC 4271) est utilisé par les routeurs de bord des AS pour échanger de grandes quantités d'informations sur les réseaux qu'ils connaissent et pour lesquels ils proposent du transit (figure 6.25). Des attributs associés à ces réseaux internes sont également échangés pour permettre par exemple d'éviter les boucles ou d'élire la meilleure route. Contrairement aux protocoles de routage interne, BGP n'utilise pas de métrique classique mais base les décisions de routage sur la succession d'AS et de réseaux internes du chemin, sur les attributs de ces réseaux internes et sur un ensemble de règles de sélection définies par l'administrateur de l'AS. BGP est un protocole à vecteur de chemin (*path vector*).

Pour échanger les données de routage entre AS, deux types de partage (*peering*) entre deux routeurs voisins BGP (*peers*) existent (figure 6.25) :

- *customer-provider peering* : il s'agit d'une relation asymétrique dans laquelle un client (un domaine de routage) achète une connectivité à l'Internet auprès d'un FAI (un autre domaine de routage). Dans ce cas, le client envoie ses routes

internes et les routes apprises de ses propres clients au fournisseur. Ce dernier annoncera ces routes sur tout l'Internet. Le fournisseur annonce à son client toutes les routes qu'il connaît et le client est capable en principe d'atteindre n'importe quelle adresse sur l'Internet ;

- *shared-cost peering* : il s'agit d'une relation symétrique où deux domaines de routage acceptent d'échanger gratuitement leurs paquets à travers un point d'interconnexion. Chaque *peer* BGP envoie à l'autre ses propres routes et celles de ses clients. Le point d'interconnexion sera utilisé par chaque *peer* BGP pour atteindre les destinations des clients de l'autre.

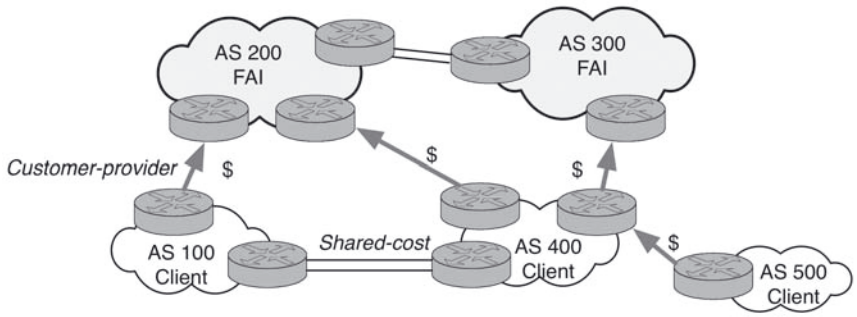


Figure 6.25 – **Les deux types de partage BGP.**

D'un point de vue protocolaire, la connexion entre deux routeurs *peers* est initiée par l'un des deux routeurs en utilisant TCP sur le port 179 (BGP est le seul protocole de routage à utiliser TCP comme protocole de transport). Ensuite, les différentes phases du protocole BGP sont les suivantes :

- chaque routeur BGP échange avec ses voisins des messages *Open* pour ouvrir et négocier les paramètres de la session BGP (numéros d'AS respectifs, capacités de chacun des *peers*…) ;
- les routeurs BGP échangent les informations concernant l'accessibilité des préfixes IP (réseaux destinations) qu'ils connaissent par l'intermédiaire de messages *Update*. Ces informations contiennent des attributs comme l'adresse du prochain nœud (attribut *Next_hop*), la liste des AS du chemin (attribut *AS_Path* : liste ordonnée des AS traversés) ou des contraintes sur les routes internes (attribut *Local_Preference* : métrique destinée aux routeurs externes pour privilégier certaines routes internes). Les routeurs BGP vont alors pouvoir prendre leurs décisions de routage et construire un graphe formé d'AS (sans boucle) sur lequel une politique de routage pourra être appliquée pour contraindre ou favoriser certains chemins suivant les attributs reçus et les restrictions ou préférences locales (voir exemple décrit à la figure 6.26) ;
- après avoir échangé la totalité des informations de routage, les routeurs BGP ne transmettent que les modifications (nouvelles routes ou retrait de routes) par des messages *Update* ;

- des messages *Keepalive* sont transmis périodiquement pour maintenir ouverte la session BGP ;
- des messages *Notification* sont utilisés pour fermer une session BGP suite à une erreur.

Dans l'exemple décrit par la figure 6.26, les contraintes suivantes sont mises en place par l'administrateur de l'AS 100 dans les routeurs R3 et R4 :

- pour arriver au réseau 172.30.0.0/22 depuis l'extérieur, il faut forcément passer par R4 ;
- pour aller du réseau 10.2.0.0/16 au réseau 172.18.0.0/20, il n'y a pas de possibilité de passage par l'AS 100 ;
- tous les paquets venant de l'AS 200 à destination de l'AS 300 passent par R4 ;
- tous les paquets à destination de l'AS 200 venant de l'AS 300 passent par R3.

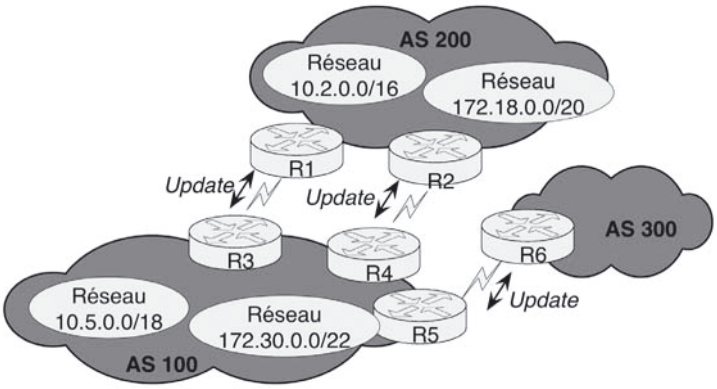


Figure 6.26 – Exemple de contraintes de routage BGP.

D'un point de vue fonctionnel, BGP se rapproche davantage d'un protocole à vecteur de distance que d'un protocole à état de liens mais avec des différences importantes :

- mémorisation de toutes les routes vers toutes les destinations ;
- le chemin suivi est décrit explicitement à l'aide de la liste des AS traversés ;
- les attributs des réseaux internes traversés permettent de donner un poids au chemin vers une destination (*path vector*) ;
- pas de transmission périodique des meilleures routes, mais uniquement des modifications ;
- construction de routes sans boucle.

6.5 Le protocole TCP

6.5.1 Le transport de bout en bout

La couche transport est essentiellement définie par les protocoles TCP et UDP. Contrairement à la couche réseau, cette couche est une couche de bout en bout dans la mesure où elle est présente uniquement dans les équipements d'extrémité, PC ou serveurs. Elle est absente dans les équipements intermédiaires : les segments ne sont pas « ouverts » par les routeurs, seule l'en-tête IP est analysé. Ce contrôle réalisé aux extrémités est illustré par la figure 6.27 : le segment TCP généré par le serveur n'est traité que par le PC à l'autre extrémité.

C'est donc TCP qui apporte la fiabilité sur Internet en veillant à ce que tous les paquets arrivent à destination et soient retransmis en cas de perte ou de saturation d'un routeur.

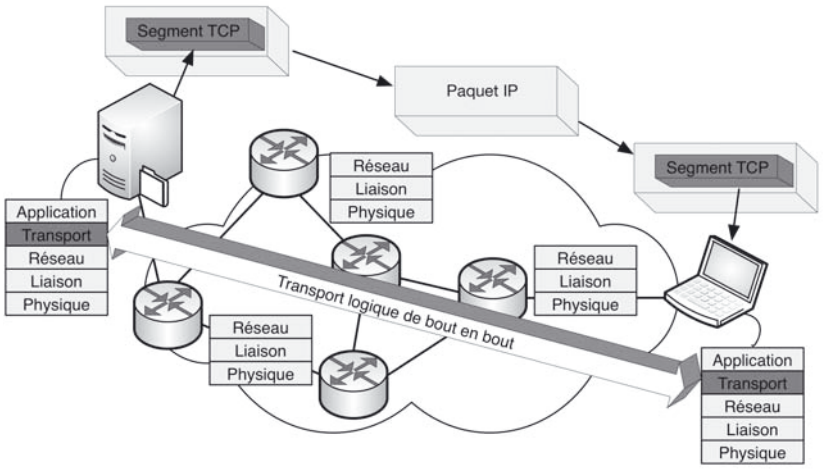


Figure 6.27 – Présence de la couche transport.

6.5.2 TCP et UDP

Contrairement à TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*) est un protocole sans connexion et non fiable. Il permet à une application d'envoyer des messages à une autre application avec un minimum de fonctionnalités (pas de garanties d'arrivée, ni de contrôle de séquencement) mais avec des temps de traitement courts. UDP n'apporte donc pas de fonctionnalités supplémentaires par rapport à IP et permet simplement de désigner les numéros de port correspondant aux applications envisagées. Il est par exemple utilisé pour des requêtes d'adressage dynamique DHCP ou des échanges d'informations de routage RIP qui pourront simplement être réitérés en cas d'échec.

Un message UDP est désigné dans un paquet IP par une valeur du champ protocole égal à 17. L'en-tête UDP est décrit à la figure 6.28.

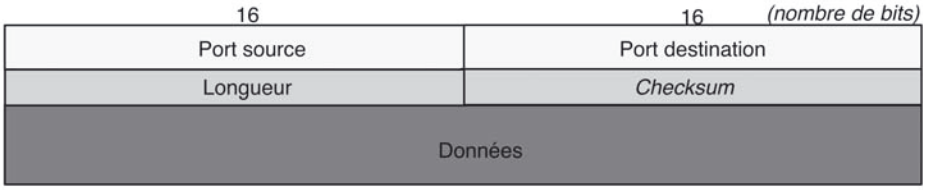


Figure 6.28 – **Format d'un message UDP.**

La longueur totale du message (données et en-tête) est donnée en octets.

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

Le port source et le port destination permettent de référencer les applications (*process*) qui s'exécutent sur les machines locales et distantes dans une communication de type client-serveur (figure 6.29) :

- une application serveur « écoute » sur un port qui lui est propre ;
- une application cliente A qui veut communiquer avec une application serveur B « parle » par le port de B.

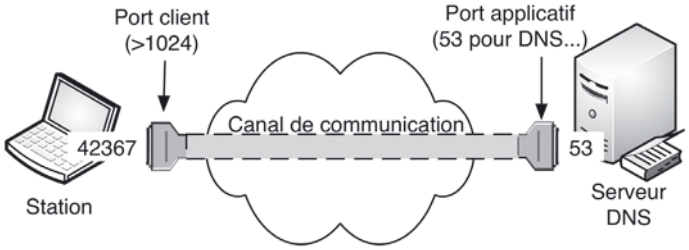


Figure 6.29 – **Affectation des numéros de port client et serveur.**

Les numéros de port de quelques applications usuelles sont donnés dans le tableau 6.2.

Tableau 6.2 – **Numéros de port UDP et TCP usuels.**

N° de port	7	20	21	22	25	53	80	110	161
Process	Echo	FTP-data	FTP	SSH	SMTP	DNS	HTTP	POP3	SNMP

Les valeurs supérieures à 1 024 correspondent généralement à des ports clients et sont affectées à la demande par la machine qui effectue la connexion TCP pour référencer cette dernière.

6.5.3 Le segment TCP

Le protocole TCP recouvre globalement les fonctionnalités des communications de niveau transport avec connexion. Il est identifié par la valeur 6 dans le champ protocole du paquet IP. Ses principales caractéristiques sont :

- établissement et fermeture de la connexion virtuelle ;
- segmentation et ré-assemblage des données (S-PDU) ;
- séquencement des segments (re-séquencement des paquets si la couche IP ne les délivre pas dans l'ordre) ;
- gestion de pertes : acquittement des segments reçus et retransmission sur absence d'acquittement ;
- contrôle de flux.

L'en-tête TCP est constitué par défaut de 20 octets organisés en mot de 32 bits (figure 6.30) :

- les numéros de port permettent de référencer les applications (voir protocole UDP) ;
- le numéro de séquence indique le numéro du premier octet transmis dans le segment ;
- le numéro d'acquittement contient le numéro de séquence du prochain octet attendu par l'émetteur ;
- la longueur de l'en-tête est codée sur 4 bits et donne le nombre de mots de 32 bits ;
- les bits de contrôle permettent de définir la fonction des messages ainsi que la validité de certains champs :
  - ◇ URG = 1 si le champ des priorités est utilisé (pour des demandes d'interruption d'émission par exemple) ;
  - ◇ ACK = 1 si la valeur du champ acquittement est significative ;
  - ◇ EOM (ou PSH) indique une fin de message (*End of Message*), les données doivent être transmises (*pushed*) à la couche supérieure ;
  - ◇ RST (*Reset*) : demande de réinitialisation de la connexion ;
  - ◇ SYN : demande d'ouverture de connexion (les numéros de séquence doivent être synchronisés) ;
  - ◇ FIN : fin de connexion ;
- le champ fenêtre (*Windows*) indique le nombre d'octets que le récepteur peut accepter à partir du dernier numéro d'acquittement ;
- le champ *checksum* correspond à une somme de contrôle de l'en-tête et du message ;
- le champ priorité contient lors d'une interruption d'émission (URG = 1) un pointeur sur les octets de données à traiter en priorité ;
- le champ options permet de définir, par exemple, la taille maximale d'un segment.

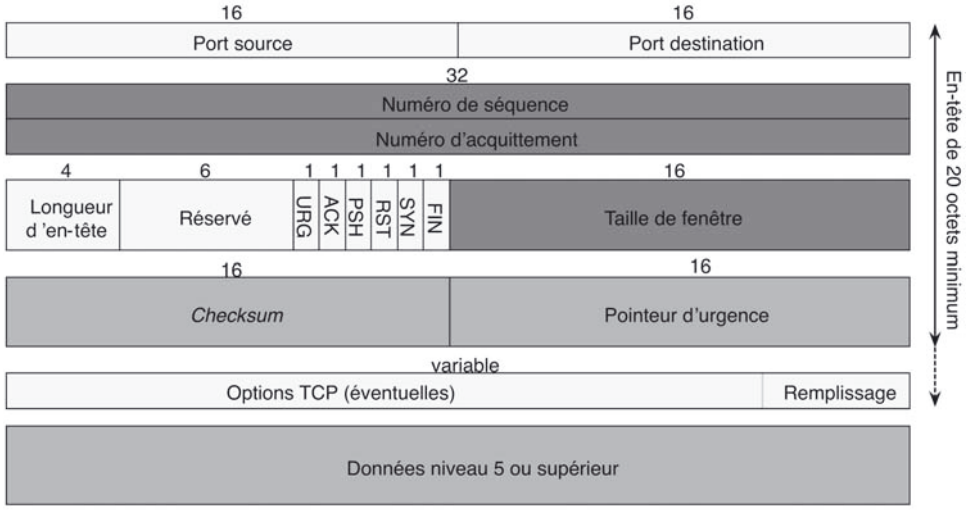


Figure 6.30 – **Format des segments TCP.**

6.5.4 Les états TCP

a) Ouverture d'une connexion

Après autorisation locale sur chaque station et déclaration d'un identificateur permettant à l'application de référencer la connexion, la demande d'ouverture de connexion est transmise à la couche transport qui positionne son bit SYN à 1 (figure 6.31). Le numéro de séquence initial à l'émission (*Initial Send Sequence number,* ISS) est délivré, au moment de la demande, par un compteur incrémenté toutes les 4 ms (la taille du champ séquence étant de 32 bits, la période du compteur est supérieure à 4 heures). Dans l'exemple, la valeur de ISS au moment de la connexion est à 350 pour la station A.

La station sollicitée répond avec les bits SYN et ACK à 1 et une dernière confirmation est effectuée par la station initiatrice avec le bit ACK à 1.

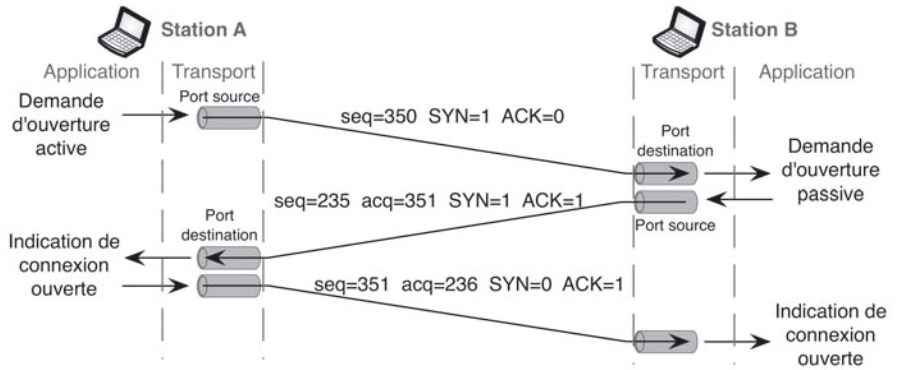


Figure 6.31 – **Exemple de connexion réussie.**

b) Transfert de données

Le transfert de données peut alors commencer avec les numéros de séquence en cours. Le contrôle de flux est réalisé dans les deux sens par les numéros d'acquittement (le bit ACK est alors positionné à 1). Chaque accusé de réception indique le nombre d'octets correctement reçus.

Dans l'exemple de la figure 6.32, le numéro d'acquittement 362 renvoyé par la station B indique à l'émetteur que les 10 octets de 352 à 361 ont été reçus et que les prochains octets, à partir du numéro 362, peuvent être transmis. Simultanément, la station B qui est aussi émettrice envoie un numéro de séquence à 236 correspondant au premier des 20 octets transmis vers la station A. Cette dernière acquittera donc avec un numéro à 256. Notons que les numéros qui contrôlent le flux dans les deux sens sont indépendants, ils sont générés par chacun des émetteurs (ISS) au moment de l'ouverture de la connexion TCP. La taille de la fenêtre de réception sans acquittement (le nombre d'octets qu'il peut encore recevoir) est transmise par le destinataire lors de chaque acquittement en fonction de la place restante dans son tampon de réception**.** Dans l'exemple, la taille de la fenêtre est toujours supérieure au nombre d'octets émis.

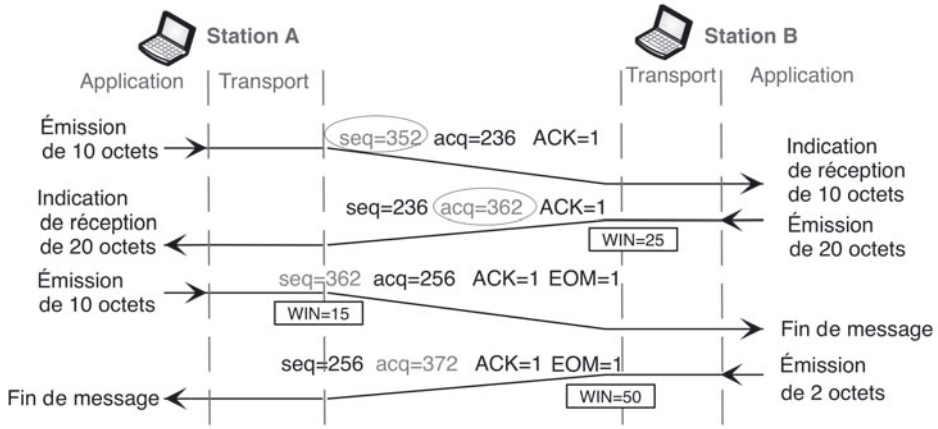


Figure 6.32 – Exemple d'échange TCP.

Une fois la taille de la fenêtre de réception transmise, l'émetteur connaît à tout moment le nombre d'octets émis et acquittés et le nombre d'octets en attente d'acquittement. Dès réception d'un acquittement sur un nombre variable d'octets, la fenêtre d'émission est déplacée ou glissée (*sliding window*) sur les octets suivants à émettre. Dans l'exemple de la figure 6.33, la taille de la fenêtre de réception est initialement de 10 octets et passe à 12 octets lorsque le récepteur acquitte les 4 premiers octets.

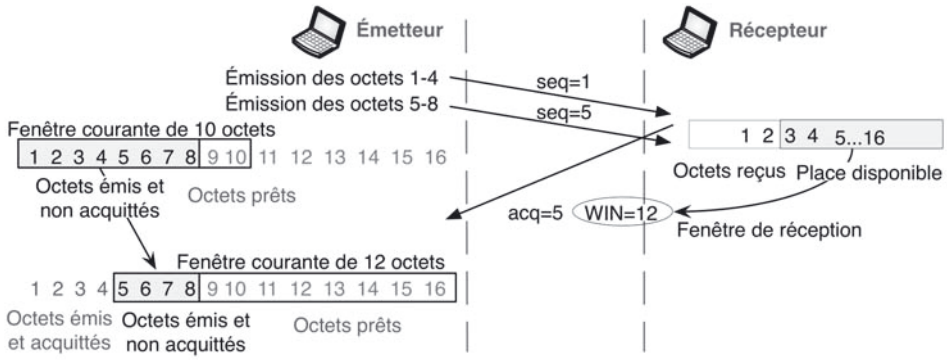


Figure 6.33 – **Gestion de la fenêtre d'émission.**

c) Fermeture d'une connexion

La demande de fermeture d'une connexion est initiée lorsqu'une des stations reçoit un en-tête TCP dont le bit FIN est positionné à 1 (figure 6.34). Dans l'exemple de la figure 6.34, après acquittement par la station B de la demande de fermeture, la connexion est à demi fermée. Cet état intermédiaire permet à des données en transit d'arriver jusqu'à la station A avant que B n'effectue à son tour une demande de fermeture suivie d'une confirmation.

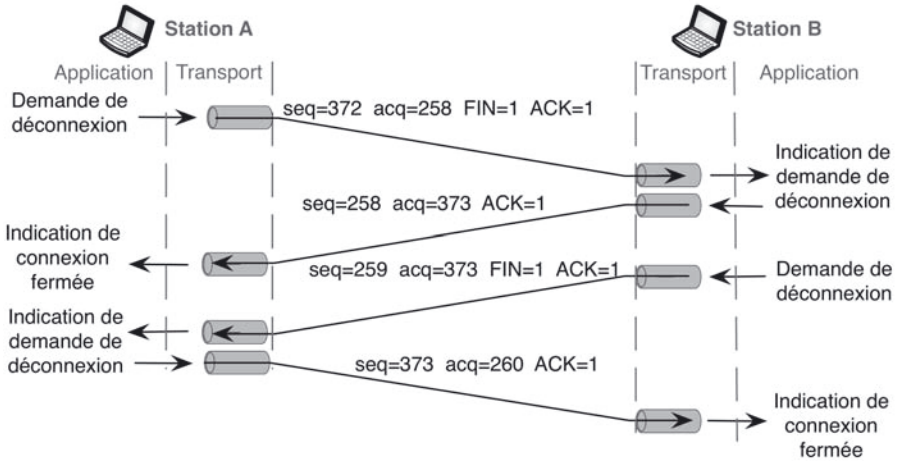


Figure 6.34 – **Exemple de fermeture réussie.**

6.5.5 Retransmission en cas de perte

Pour chaque émission de segment, TCP arme un temporisateur. En cas de perte de ce segment ou de l'acquittement correspondant, TCP retransmet le segment lorsque le temporisateur expire (RTO, *Retransmission TimeOut*).

Pour assurer un maximum d'efficacité, le dimensionnement de ce temporisateur RTO dépend de la réactivité du réseau et plus précisément du RTT (*Round Trip Time*), c'est-à-dire du temps aller-retour entre l'instant d'émission d'un segment et la réception de l'acquittement correspondant, ce temps pouvant être évalué par l'émetteur.

La figure 6.35 illustre ce problème : dans le premier cas, le RTO est correctement dimensionné par l'émetteur et la perte est efficacement résolue ; dans le deuxième cas, le RTO est trop faible, ce qui conduit à une retransmission inutile et une perte de temps (un RTO légèrement supérieur au RTT aurait permis de transmettre le troisième segment juste après la réception du premier acquittement).

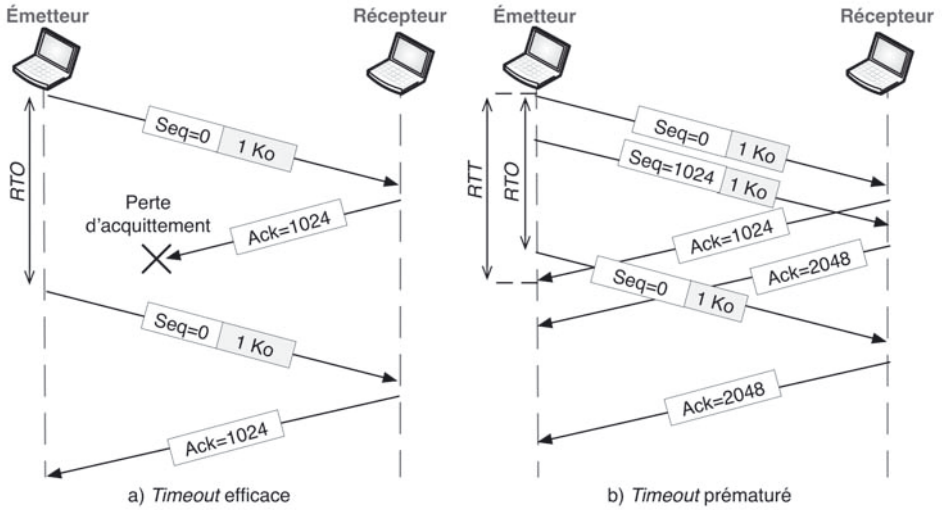


Figure 6.35 – Scénarios de retransmission.

La façon la plus simple est de calculer le RTO à partir d'un temps d'aller-retour RTT moyen. Dans l'algorithme simplifié de Jacobson, un RTT lissé est d'abord calculé en effectuant une pondération entre la précédente estimation et la dernière mesure du RTT :

$$RTT_{lissé} = (1-\alpha)\ RTT_{t-1} + \alpha\ RTT_{mesuré}$$

α est un facteur de lissage compris entre 0 et 1 permettant de donner plus ou moins d'importance à la dernière mesure du RTT (une valeur de α proche de 1 sera utilisée dans un réseau peu stable avec des temps de transmission très variables). Le

RTO est ensuite calculé en multipliant le RTT lissé par un coefficient de variance de délai β ayant une valeur recommandée de 2 :

$$RT0 = \beta\ RTT_{lissé}$$

Jacobson a montré par la suite qu'un calcul basé sur la déviation moyenne lissée *D* (approximation de la déviation standard) donnait de meilleurs résultats pour d'importantes variations du RTT :

$$D = (1-\beta)\ D + \beta\ |RTT_{mesuré} - RTT_{lissé}|$$

$$RT0 = RTT_{lissé} + 4D$$

6.5.6 Contrôle de flux et de congestion

Comme indiqué précédemment, TCP intègre des mécanismes de contrôle et donc des variables permettant d'adapter le rythme de l'émetteur aux capacités du récepteur et aux performances du réseau (figure 6.36).

Le **contrôle de flux** est réalisé par rapport au **récepteur** : l'émetteur adapte le nombre de segments envoyés à la taille du tampon de réception. Ce contrôle de bout en bout est réalisé grâce :

- aux numéros d'acquittement ;
- à la fenêtre ***window*** transmise par le récepteur.

Quand le récepteur veut ralentir la source, il peut ralentir l'envoi des acquittements et/ou envoyer une valeur de fenêtre faible ou nulle.

Le **contrôle de congestion** est réalisé par rapport au **réseau** : l'émetteur adapte le débit des données envoyées à la bande passante instantanée du réseau. Celle-ci peut tendre vers zéro lorsqu'un routeur intermédiaire est saturé (perte de segment ou d'acquittement).

Ce contrôle est géré, côté émetteur, grâce au dimensionnement dynamique d'une fenêtre de congestion ***cwnd*** (*congestion window*) dont la valeur augmente ou diminue suivant le nombre et la valeur des acquittements reçus.

Finalement, pour connaître le nombre d'octets ou de segments pouvant encore être envoyés sans attente, l'émetteur utilise une fenêtre d'émission ***Twindow*** (figure 6.36) qui est fonction des deux variables précédentes :

- *cwnd* qui dépend de la congestion du réseau ;
- *window* qui dépend de la disponibilité du récepteur.

$$Twindow = \min(cwnd, window)$$

La plupart du temps, le tampon de réception est correctement dimensionné et la fenêtre transmise par le récepteur (*window*) est supérieure à la fenêtre de congestion (*cwnd*). Dans ce cas, *Twindow* = *cwnd* et l'émetteur s'adapte à l'évolution de *cwnd*, donc au réseau.

La fenêtre de congestion *cwnd* sert donc à déterminer, suivant l'état du réseau, le nombre d'octets ou de segments pouvant être envoyés sans attente.

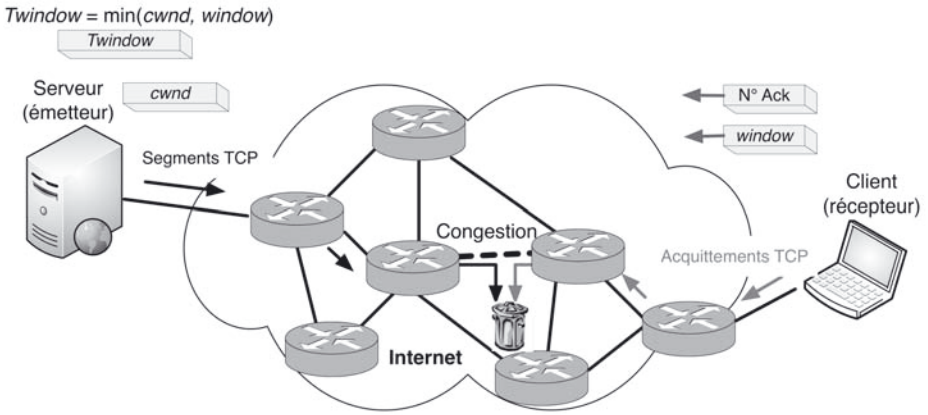


Figure 6.36 – **Variables TCP côté émetteur et côté récepteur.**

Pour optimiser le taux d'utilisation du canal, différents algorithmes de gestion de cette fenêtre peuvent être utilisés. L'algorithme TCP de base est le suivant :

- après établissement de la connexion, *cwnd* suit un démarrage lent (*slow start*) : à chaque réception d'acquittement, *cwnd* = *cwnd* + 1 segment ;
- lorsque *cwnd* atteint le seuil de démarrage lent (*ssthreshold: slow start threshold*), l'évolution est ralentie pour éviter une congestion (*congestion avoidance*) : à chaque réception d'acquittement, *cwnd* = *cwnd* + 1/*cwnd* ;
- en cas de congestion (un ou plusieurs segments non acquittés dans un temps *RTO*) :
  - ◇ réduction du seuil : *ssthreshold* = *cwnd*/2,
  - ◇ redémarrage lent : *cwnd* = 1,
  - ◇ retransmission du (ou des) segment(s).

Cet algorithme est illustré sur la figure 6.37. Pour simplifier, l'évolution de *cwnd* est notée en nombre de segments et non en nombre d'octets. L'échelle des temps est graduée en RTT, ce qui correspond au délai entre l'envoi d'un segment et la réception d'un acquittement. Dans la phase de démarrage lent, la valeur de *cwnd* est doublée pour chaque RTT (si par exemple *cwnd* = 2 et que les deux acquittements correspondants sont reçus dans un temps RTT, *cwnd* = *cwnd* + 2 = 4). Le seuil de démarrage lent est fixé initialement à 16 segments dans l'exemple. Dans la phase d'évitement de congestion, la valeur de *cwnd* est augmentée de 1 segment pour chaque RTT (si par exemple *cwnd* = 16 et que les 16 acquittements correspondants sont reçus dans un temps RTT, *cwnd* = *cwnd* + 16/*cwnd* = 17).

L'inconvénient principal de cet algorithme de base est que *cwnd* est réinitialisée à 1 pour chaque congestion. Lorsque celles-ci sont fréquentes, l'émetteur envoie très peu de segments à la fois avec pour chaque émission un temps d'attente d'acquittement qui peut être important (juste inférieur au RTO). Le débit moyen peut être considérablement ralenti.

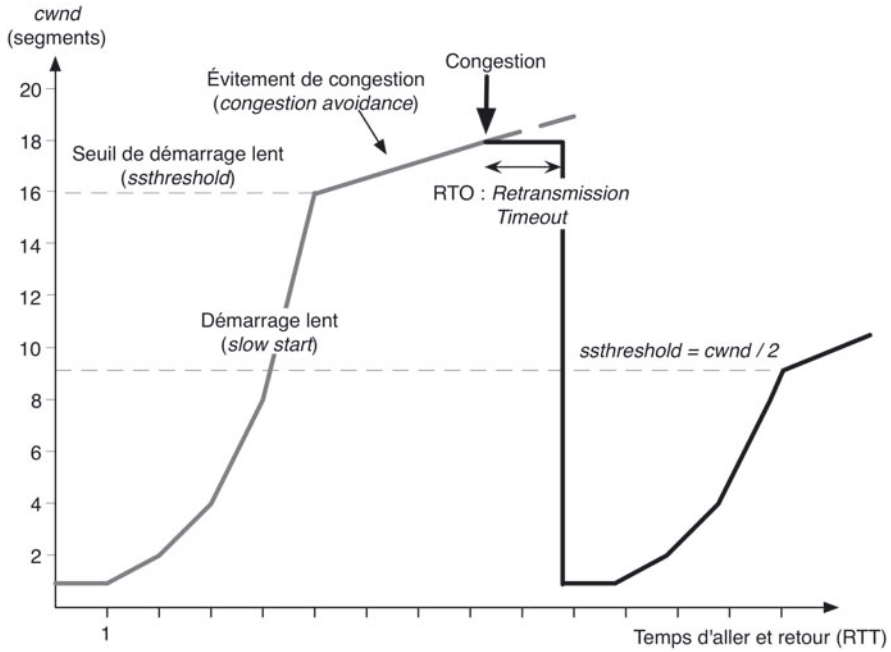


Figure 6.37 – **Algorithme TCP de base.**

Beaucoup d'améliorations ont été proposées pour accélérer la retransmission (*fast retransmit*) en cas de perte ou pour repartir avec un nombre de segments supérieur à 1 (*fast recovery*). L'algorithme TCP *new Reno*, le plus utilisé à l'heure actuelle, apporte une troisième amélioration en cas de pertes multiples non contiguës dans le même flux.

Résumé

- Les équipements d'interconnexion des réseaux interviennent à différents niveaux : le **répéteur** ou le ***hub*** pour la couche physique ; le **pont** ou le **commutateur Ethernet** pour la couche liaison ; le **routeur** pour la couche réseau et la **passerelle** pour l'ensemble des 7 couches.
- Les protocoles **TCP et IP** situés respectivement dans les **couches 4 et 3** du modèle OSI sont utilisés sur la majorité des équipements pour l'interconnexion des réseaux locaux et à l'échelle d'Internet.
- **IP** est un protocole de niveau réseau responsable de la fragmentation des données, de la transmission des datagrammes en mode sans connexion, de l'adressage et du routage des paquets entre stations par l'intermédiaire de routeurs.

- Les **adresses IPv4**, codées sur 32 bits, sont exprimées en décimal et séparées par des points (137.15.223.2). Chaque machine possède dans son réseau une adresse unique. Le **masque** de réseau permet de préciser le nombre de bits dédiés à l'identification du réseau (*net_id*) et le nombre de bits réservés pour la numérotation des machines (*host_id*). Organisés à l'origine suivant la dimension en quatre classes (A, B, C et D), les réseaux IP sont aujourd'hui désignés grâce au couple adresse/préfixe (137.15.128.0/19) qui permet de désigner simplement l'importance du réseau. Pour pallier à la pénurie d'adresses IPv4, l'**adressage IPv6** permet d'étendre le nombre d'adresses en les codant sur 128 bits et en utilisant une notation du type :
805B:2D9D:0000:DC28:12F7:000A:765C:D4C8
- D'autres protocoles sont associés à IP : **ARP** pour la correspondance entre les adresses IP et les adresses physiques ; **ICMP** pour le contrôle du trafic IP ; **DHCP** pour la transmission dynamique des adresses IP aux clients.
- Le **routage** consiste à trouver des chemins dans les réseaux interconnectés à partir des adresses de destination. Les routeurs concernés doivent être capables de gérer ces chemins dans leurs tables de routage et de maintenir ces dernières à jour à l'aide de protocoles de routage spécifiques (RIP, OSPF, BGP…).
- Deux niveaux de **protocoles de routage** sont distingués : les **IGP** qui interviennent à l'intérieur des systèmes autonomes (AS) et les **EGP** ou **BGP** qui permettent l'échange entre les routeurs de bords des AS.
- Les **IGP** sont eux-mêmes classés suivant l'algorithme utilisé. Un protocole tel **RIP** utilise un algorithme à **vecteur de distance,** les informations échangées permettent pour chaque routeur de retenir le plus petit nombre de sauts vers une destination. Le protocole **OSPF** utilise un algorithme à **état de lien** basé sur la transmission d'une carte complète des liens possibles entre les routeurs.
- Le protocole de niveau transport **UDP** est non connecté et non fiable. Il permet de désigner simplement les numéros de port des applications utilisées avec des temps de réponse courts.
- Le protocole de transport **TCP** fonctionne en mode connecté, ses principales caractéristiques sont la segmentation et le réassemblage des messages, la retransmission en cas d'échec et le contrôle de flux.
- On distingue principalement **trois phases TCP** : l'ouverture de la connexion, le transfert des données et la fermeture. Des bits dans l'en-tête TCP (*flags*) des segments envoyés et reçus permettent de savoir dans quel état se trouve la machine émettrice ou réceptrice.
- Des **numéros de séquence et d'acquittement** dans l'en-tête TCP permettent à tout moment de connaître, dans les deux sens, le nombre d'octets envoyés et le nombre d'octets acquittés et donc de réguler le flux des données et de provoquer une retransmission en cas de perte.

Exercices corrigés

QCM

Q6.1 Quel élément d'interconnexion travaille sur les adresses MAC ?

a) Le répéteur b) Le commutateur

c) Le routeur d) La passerelle

Q6.2 Un routeur analyse les adresses IP et modifie au passage :

a) L'adresse IP source b) L'adresse IP destination

c) Aucune

Q6.3 Quels sont les protocoles qui fonctionnent en mode connecté ?

a) IP b) ARP c) UDP d) TCP

Q6.4 Quelle est la valeur possible du champ TTL de l'en-tête IP après traversée de trois routeurs par un paquet ?

a) 65 b) 124 c) 61 d) 30

Q6.5 Quelle classe d'adresses IP permet d'avoir plus de 1 000 hôtes par réseau ?

a) A b) B c) C d) D

Q6.6 Combien de sous-réseaux peut-on distinguer avec un masque égal à 255.255.255.224 sur un réseau de classe C ?

a) 2 b) 4 c) 8 d) 16

Q6.7 Quelle est la taille minimale en octets d'un en-tête TCP ?

a) 16 b) 20 c) 24 d) 64

Q6.8 Sur un réseau Ethernet utilisant les protocoles TCP/IP, à quel niveau est réalisé le contrôle de flux ?

a) MAC b) DHCP c) IP d) TCP

Q6.9 Lors d'un transfert de données utilisant TCP, quel numéro de séquence peut transmettre l'émetteur s'il vient de recevoir un numéro d'acquittement à 1356 ?

a) 1356 b) 1357 c) 1376 d) 2856

Q6.10 Un routeur est relié à cinq sous-réseaux et possède un lien point à point vers un autre routeur, combien d'interfaces sont activées ?

a) 2 b) 5 c) 6

Q6.11 Lors de la fragmentation IP, un datagramme de 128 octets est transmis avec une valeur d'offset de 1000. Quelle sera la valeur d'offset du fragment suivant ?

a) 12 b) 1128 c) 1016

Q6.12 Quels champs de l'en-tête IPv4 sont susceptibles d'être modifiés par les routeurs sur le chemin ?

a) TTL b) Drapeaux c) Version d) *Checksum*

Q6.13 Lesquelles de ces trames possèdent nécessairement une adresse physique destination de diffusion ?

a) Requête d'écho ICMP b) Requête ARP c) Requête DHCP

Q6.14 Lorsque tous les bits hôte sont associés à la valeur 1, quel est le type d'adresse ?

a) Hôte b) Réseau c) Sous-réseau d) Diffusion

Q6.15 Un réseau de classe B est découpé en plusieurs sous-réseaux et on obtient un masque final valant 255.255.252.0. En combien de sous-réseaux le réseau de départ a-t-il été découpé ?

a) 32 b) 64 c) 128 d) 256

Q6.16 Un réseau a comme adresse 180.35.128.0/20. Quelle est l'adresse de broadcast ?

a) 180.35.255.255 b) 180.35.143.255

c) 180.35.128.255 d)180.35.192.255

Q6.17 Un réseau a comme masque 255.255.255.224. Combien de machines peut-il y avoir sur un tel réseau ?

a) 25 b) 128 c) 224 d)30

Q6.18 On découpe un réseau dont le masque est 255.255.224.0 en 16 sous-réseaux. Quel est le nouveau masque ?

a) 255.255.254.0 b) 255.255.255.0

c) 255.255.252.0 d) 255.255.248.0

Q6.19 A envoie à B 4 segments de 1 000 octets chacun : les segments 0, 1000, 2000 et 3000. Le segment 1000 est perdu, et les autres arrivent correctement. Quel acquittement va envoyer B ?

a) 4000 b) 2000 c) 1000 d) 0

Q6.20 A envoie à B un segment de numéro 38 et de taille 4. Alors le numéro d'acquittement dans ce même segment est forcément 42.

a) Vrai b) Faux

Exercices

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

6.1 (*) Comment les protocoles IP et TCP sont-ils identifiés dans une trame Ethernet ?

6.2 (*) Pourquoi parle-t-on de datagramme IP ?

6.3 (**) Une machine faisant partie d'un réseau local est reliée à l'Internet, sa configuration est la suivante :

Adresse IP : 195.18.54.53
Netmask : 255.255.255.224

a) Quelle est l'adresse du réseau local et sa classe ?

b) Quelle est l'adresse du sous-réseau dans lequel se trouve la station ?

c) Combien de sous-réseaux sont utilisables dans ce réseau local ?

d) Combien peut-on déclarer de stations dans chacun des sous-réseaux ?

6.4 L'ICANN vous a affecté une adresse 202.17.69.0 de classe C. Votre réseau privé comporte actuellement cinq sous-réseaux. Chacun d'entre eux dispose d'environ 10 hôtes. Le nombre de sous-réseaux sera doublé l'an prochain. Le nombre d'hôtes de deux des sous-réseaux pourrait atteindre 14.

a) Quel masque de sous-réseau devez-vous choisir ?

b) Quel est le nombre maximum de sous-réseaux autorisés ?

c) Quel est le nombre maximum d'hôtes par sous-réseau autorisé ?

d) Quelle est l'adresse du 3^{e} sous-réseau et des 3 premières machines de ce sous-réseau ?

6.5 (*) Quel est le rôle des numéros de port des protocoles UDP et TCP ?

6.6 (*) Dans l'exemple donné figure 6.19, la station S envoie un datagramme IP avec une valeur initiale du champ TTL égale à 64. Quelle sera la valeur de ce champ dans le datagramme arrivant sur la station D ?

6.7 (***) Les commandes « *Echo Request* » et « *Echo Reply* » du protocole ICMP permettent de tester un réseau IP. La commande utilisateur « ping » suivie d'une adresse IP appelle un programme qui intègre ces deux commandes pour réaliser simplement un test vers la destination.

a) Que mesure cette commande ping ?

b) En retour de la commande ping, un message ICMP de type « durée de vie expirée » est reçu. Que faut-il en déduire ?

c) Si l'on est sûr de l'adresse IP du destinataire mais que le message ICMP de retour indique « destinataire inaccessible », que faut-il conclure ?

d) En général, la commande ping ne génère pas une seule requête d'écho mais plusieurs. Quelle en est la raison ?

6.8 (**) Représenter la table de routage du routeur B de la figure 6.16.

6.9 (***) Le relevé de trames fourni ci-dessous correspond à l'échange d'informations entre les deux machines Student3 et ServerC en utilisant le protocole TCP/IP. Dans ce relevé, les en-têtes de niveau MAC, IP et TCP sont décodés champ par champ. Le contenu du paquet IP est ensuite affiché en hexadécimal.

```
Pkt No. = 2 Time = 09 :27 :24 Length = 60
MAC : Srce = Student3 Dest = ServerC Type = IP
IP : VER/IHL = 45, TOS = 00, Len = 002C, ID = 0400, FLG/FRG = 0000,
TTL = 3C
IP : Prtcl = TCP, Chksm = 6A82, Srce = 192.9.200.50, Dest =
192.9.200.4
TCP : Source Port = 0401, Destination Port = 0019
TCP : Sequence Number = 0000144B, Acknowledgement Number = 904A127E
TCP : TCP Offset / Header Length = 5, Reserved = 000000
TCP : URG = 0, ACK = 1, PSH/EOM = 1, RST = 0, SYN = 0, FIN = 0
TCP : Window = 1400, Checksum = 4ADE, Urgent Pointer = 0000
TCP : Options and Padding = None
0000 : 45 00 00 2C 04 00 00 00 3C 06 6A 82 C0 09 C8 32
0010 : C0 09 C8 04 04 01 00 19 00 00 14 4B 90 4A 12 7E
0020 : 50 18 14 00 4A DE 00 00 85 00 00 00

Pkt No. = 3 Time = 09 :27 :24 Length = 60
MAC : Srce = ServerC Dest = Student3 Type = IP
IP : VER/IHL = 45, TOS = 00, Len = 0028, ID = 019A, FLG/FRG = 0000,
TTL = 40
IP : Prtcl = TCP, Chksm = 68EC, Srce = 192.9.200.4, Dest =
192.9.200.50
TCP : Source Port = 0019, Destination Port = 0401
TCP : Sequence Number = 904A127E, Acknowledgement Number = 0000144F
TCP : TCP Offset / Header Length = 5, Reserved = 000000
TCP : URG = 0, ACK = 1, PSH/EOM = 0, RST = 0, SYN = 0, FIN = 0
TCP : Window = 37FB, Checksum = ABEB, Urgent Pointer = 0000
TCP : Options and Padding = None
0000 : 45 00 00 28 01 9A 00 00 40 06 68 EC C0 09 C8 04
0010 : C0 09 C8 32 00 19 04 01 90 4A 12 7E 00 00 14 4F
0020 : 50 10 37 FB AB EB 00 00 01 31 03 31 32 38
```

a) Combien d'octets comportent les en-têtes IP et TCP du paquet 2 ? Combien reste-t-il d'octets au niveau supérieur ?

b) Indiquer, pour le paquet 2 les adresses IP source et destination en notation classique décimale et en hexadécimal.

c) Les paquets sont-ils fragmentés ?

d) À quoi correspondent les numéros de ports dans les paquets 2 et 3 ?

e) Quel est le numéro de séquence à l'émission envoyé par la station Student3 dans le paquet 2 ? Justifier en conséquence la valeur utilisée dans le paquet 3 pour l'acquittement par la station ServerC.

f) Combien d'octets au niveau supérieur la station Student3 peut-elle recevoir sans acquittement ?

6.10 (**) Déterminer en notation CIDR le bloc d'adresses client et les classes attribuées par un fournisseur Internet à une entreprise ayant besoin de 500 adresses. Le fournisseur possède le bloc suivant : 195.27.16.0 / 20.

6.11 (***) Vous gérez localement un serveur web sur une machine d'adresse privée 192.168.0.110. Toutes les connexions privées/publiques et publiques/privées passent par votre box.

a) Comment devez-vous configurer la fonction NAPT de votre box pour que votre serveur soit joignable de l'extérieur ?

b) Comment ce procédé s'appelle-t-il ?

6.12 (**) Quelle est la différence entre contrôle de congestion et contrôle de flux dans le protocole TCP ?

6.13 (***) Compléter les numéros de séquence et d'acquittement sur le schéma suivant. Pour chaque segment TCP, le rôle est indiqué (SYN pour l'ouverture, DATA pour des données, FIN pour la fermeture). Le numéro entre parenthèses donne le nombre d'octets envoyés.

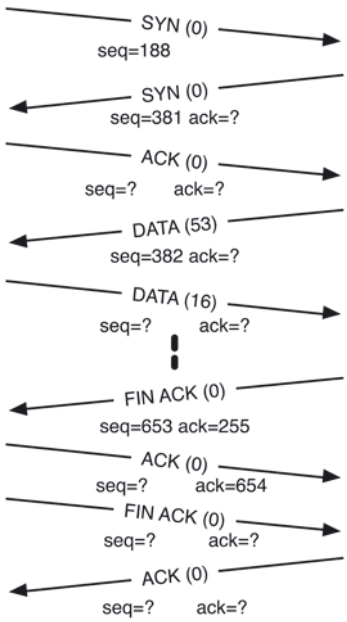


Figure 6.38

Solutions

QCM

Q6.1 : b	**Q6.2** : c	**Q6.3** : d	**Q6.4** : c	**Q6.5** : a-b
Q6.6 : c	**Q6.7** : b	**Q6.8** : d	**Q6.9** : a	**Q6.10** : c
Q6.11 : c	**Q6.12** : a-b-d	**Q6.13** : b-c	**Q6.14** : d	**Q6.15** : b
Q6.16 : b	**Q6.17** : d	**Q6.18** : a	**Q6.19** : c	**Q6.20** : b

Exercices

6.1 Pour une architecture type Ethernet II, le protocole IP est indiqué par la valeur 0800_H dans le champ longueur de l'en-tête MAC.
Le protocole TCP est indiqué par la valeur 06_H dans le champ protocole de l'en-tête IP.

6.2 La notion de datagramme est liée à un mode de transmission sans connexion, ce qui est le cas des paquets IP.

6.3

a) L'adresse du réseau est 195.18.54.0, il s'agit d'une classe C.

b) Un « ET » logique appliqué entre l'adresse IP et le masque permet de trouver l'adresse du sous-réseau : 195.18.54.32. La station est la 21e dans ce sous-réseau (53-32).

c) Le masque comporte 3 bits à 1 sur le 4e octet, ce qui fait $2^3 = 8$ sous-réseaux. Si les deux adresses d'extrémité sont évitées, cela laisse 6 sous-réseaux utilisables.

d) Le masque comporte 5 bits à 0, ce qui permet de numéroter $2^5 = 32$ stations par sous-réseau. Pour chaque sous-réseau, la première adresse (du type 195.18.32.0) est réservée à l'adresse du sous-réseau lui-même et non disponible pour une station ; la dernière adresse (du type 195.18.32.255) est réservée aux diffusions. En fait, seules 30 adresses peuvent être déclarées dans chaque sous-réseau.

6.4

a) Pour 10 sous-réseaux, 4 bits à 1 sont nécessaires
($2^4 = 16 < 10 < 2^3 = 8$) soit un masque de 255.255.255.240.

b) En enlevant les deux adresses d'extrémité, il reste 14 sous-réseaux autorisés.

c) Il reste 4 bits à 0 dans le masque pour adresser $2^4 - 2 = 14$ stations par sous-réseau, ce qui est juste conforme au nombre souhaité.

d) Les sous-réseaux sont numérotés par incréments de 16. Si l'on excepte le premier sous-réseau d'adresse 202.17.69.0, nous aurons comme adresses autorisées : 202.17.69.16 202.17.69.32, 202.17.69.48, 202.17.69.64…

Le troisième sous-réseau a donc comme adresse 202.17.69.48 et les trois premières machines : 202.17.69.49, 202.17.69.50 et 202.17.69.51.

6.5 Le numéro de port est une valeur donnée dans l'en-tête TCP qui identifie l'application (21 pour FTP, 80 pour HTTP…) ou la machine cliente. Les ports systèmes sont prédéfinis et généralement inférieurs à 1 024 (RFC1700). Les ports clients sont affectés à la demande et sont supérieurs à 1 024.

6.6 Le paquet traverse 3 routeurs pour aller de la station S à la station D, le champ TTL sera donc égal à 64 – 3 = 61.

6.7

a) Le temps aller-retour entre un émetteur et un récepteur ou RTT (*Round Trip Time*).

b) Lorsqu'un routeur traitant un datagramme est amené à mettre à jour le champ TTL de l'en-tête IP et que ce champ atteint une valeur zéro, le datagramme doit être détruit. Le routeur peut alors prévenir l'hôte source de cette destruction par ce message.

c) Si, compte tenu des informations contenues dans les tables de routage du routeur, le réseau indiqué dans le champ adresse de destination de l'en-tête IP du datagramme reçu est inaccessible ou inconnu (par exemple, la distance à ce réseau est marquée comme infinie), le routeur pourra émettre un tel message à destination de l'hôte d'origine du datagramme. De plus, dans certains réseaux, le routeur peut être capable de déterminer que l'hôte destinataire n'est pas accessible. Un tel routeur pourra, sur réception d'un datagramme destiné à cet hôte, émettre en retour un tel message ICMP, et détruire le datagramme.

d) Plusieurs datagrammes sont utiles pour tester la réactivité du réseau au niveau du routage et donner un temps moyen. Si seul un datagramme sur quatre est retourné, le réseau n'est pas fiable et la cause peut être trouvée par des *pings* successifs (*ping* en boucle sur la station source, *ping* sur le routeur par défaut…).

6.8

En considérant que les accès distants passent par le routeur A, la table de routage du routeur B peut être établie :

Tableau 6.4

Réseau destination	Masque	Prochain routeur	Interface	Métrique
193.17.52.128	255.255.255.192	193.17.52.131	Ethernet 1	0 (direct)
193.17.52.192	255.255.255.192	193.17.52.193	Ethernet 2	0 (direct)
193.17.52.64	255.255.255.192	193.17.52.129	Ethernet 1	1
193.17.52.0	255.255.255.192	193.17.52.129	Ethernet 1	1
193.48.32.0	255.255.255.0	193.17.52.129	Ethernet 1	1
212.1.23.0	255.255.255.0	193.17.52.194	Ethernet 2	1
0.0.0.0	0.0.0.0	193.48.32.129	Ethernet 1	0

6.9

a) L'analyse nous donne cinq mots de 32 bits pour chacun des en-têtes, soit 20 octets pour IP et 20 octets pour TCP. Il reste 4 octets au niveau supérieur (85 00 00 00).

b) L'analyse nous donne les adresses en décimal : IP source = 192.9.200.50 ; IP destination = 192.9.200.4. Les derniers octets de l'en-tête IP correspondent aux adresses en hexadécimal : C0 09 C8 32 et C0 09 C8 04.

c) Les bits DF et MF sont à 0 (FLG), donc pas de fragmentation.

d) Dans le paquet 2, le numéro de port source correspond à un port client (401_H = 1 025 > 1 024), le port destination 19_H = 25 correspond à une application de messagerie utilisant le protocole SMTP. Dans le paquet 3, les numéros de port sont inversés, ServerC est un serveur SMTP et répond à la requête de Sudent3.

e) Student3 envoie : `Sequence Number = 0000144B`. ServerC répond : `Acknowledgement Number = 0000144F`. ServerC acquitte donc les 4 octets 144B à 144E correspondant à la couche supérieure (octets 85 00 00 00) en envoyant le numéro du prochain octet attendu soit 144F.

f) La fenêtre (TCP: Window) indique que $1\,400_H$ = 5 120 octets peuvent être reçus sans acquittement.

6.10 Le client a besoin de deux classes C (512 adresses). Le fournisseur dispose de 16 classes C, les 4 bits de poids faible du troisième octet permettent de les numéroter. Si l'ISP attribue ses troisième et quatrième classes au client, nous obtenons les adresses :

- Bloc ISP :
  11000011 . 0001 1011 . 00010000 . 00000000 = 195.27.16.0 / 20
- 1re classe C client :
  11000011 . 0001 1011 . 00010010 . 00000000 = 195.27.18.0 / 24
- 2e classe C client :
  11000011 . 0001 1011 . 00010011 . 00000000 = 195.27.19.0 / 24
- Bloc client :
  11000011 . 0001 1011 . 00010010 . 00000000 = 195.27.18.0 / 23

6.11

a) Il est nécessaire de définir une règle de redirection de port sur le NAPT, redirigeant tous les paquets TCP reçus sur son port 80 vers la machine 192.168.0.110.

b) Ce procédé s'appelle redirection de port, *Port Forwarding* ou *Port mapping*.

6.12 Dans TCP, le contrôle de flux est réalisé grâce aux acquittements et à la fenêtre transmise par le récepteur (*window*). C'est donc un contrôle réalisé par rapport au récepteur qui peut demander à l'émetteur de ralentir ou d'interrompre ses émissions.

Le contrôle de congestion est réalisé par la gestion, côté émetteur, d'une fenêtre de congestion (*cwnd*) dont la valeur augmente ou diminue suivant le nombre et la valeur des acquittements reçus. C'est donc un contrôle réalisé par rapport au réseau qui transmet plus ou moins vite les acquittements envoyés.

6.13

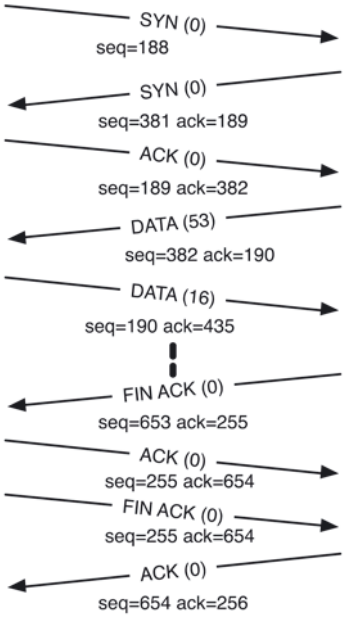


Figure 6.39

7 Les réseaux d'opérateurs

PLAN

OBJECTIFS

- Connaître l'architecture et le fonctionnement des couches basses des principaux réseaux d'opérateurs (RTC, ATM, SDH et SONET).
- Comprendre le rôle de l'architecture MPLS et connaître les mécanismes de commutation utilisés dans MPLS.
- Connaître l'architecture des différentes générations de téléphonie cellulaire (2G, 3G, 4G).
- Comprendre les techniques de multiplexage et d'accès radio utilisées dans la téléphonie cellulaire.

7.1 Caractéristiques des réseaux d'opérateurs

La fonction principale d'un opérateur de télécommunication est le transport des informations des abonnés, d'un point à un autre de son réseau (figure 7.1). Aujourd'hui, on distingue deux types d'opérateurs : les **opérateurs de câblage** (câblo-opérateurs) qui disposent des infrastructures physiques du réseau et les **opérateurs de transport** qui disposent des équipements de communication des données et assurent leur transmission à travers les infrastructures jusqu'aux destinataires.

À ces deux types d'opérateur, il faut ajouter aujourd'hui les **opérateurs de services** de communication définis par l'ARCEP (Autorité de régulation des communications électroniques et des postes) qui sont les prestataires fournissant un accès à un réseau public de communication contre rémunération. C'est donc l'opérateur auprès duquel un abonné contracte un forfait.

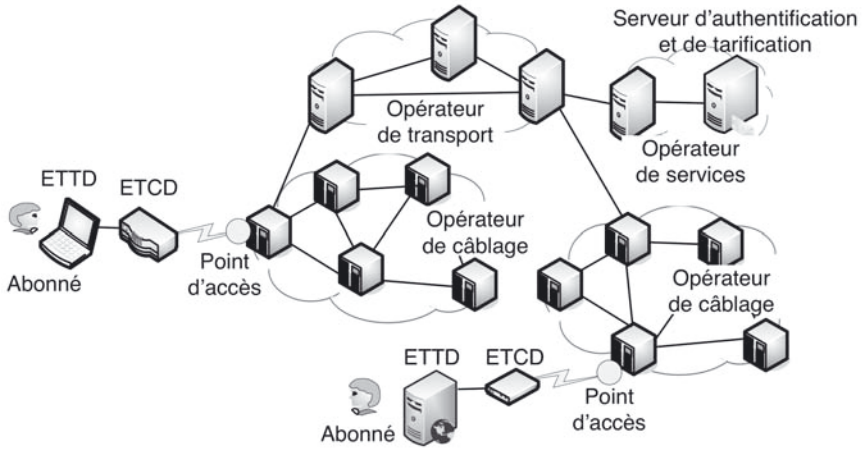


Figure 7.1 – **Réseau d'opérateurs.**

L'infrastructure d'un opérateur de câblage comporte les équipements actifs (commutateurs, multiplexeurs…) et passifs (câbles de transmission ou canaux hertziens).

Leurs capacités de transmission sont caractérisées par :

- les débits ;
- la nature du support utilisé ;
- les modes d'exploitation ;
- des liaisons de type point à point entre les équipements et le réseau ;
- des liaisons commutées ou spécialisées.

Pour les **réseaux commutés**, les liaisons entre éléments sont limitées à la durée des communications. Ils peuvent être de deux types :

- les réseaux commutés non spécialisés, non conçus initialement pour la transmission de données numériques, le réseau téléphonique commuté en est un exemple avec des transmissions par modem ADSL ;
- les réseaux commutés spécialisés comme l'ancien réseau RNIS ou le réseau ATM qui utilise la commutation de cellules pour transporter tout type d'informations (voix, vidéo, données).

Les **lignes spécialisées** (LS), nommées également liaisons louées, sont basées sur des lignes empruntées à l'infrastructure d'un opérateur et mises bout à bout pour constituer un lien permanent entre les extrémités, sur des courtes ou longues distances.

En pratique, la LS est généralement seulement réservée entre le point de raccordement de l'abonné et le point d'accès au réseau de l'opérateur, le transport étant ensuite assuré sur les réseaux ATM ou MPLS des opérateurs de télécommunication qui allouent une partie de leur bande passante disponible pour la LS.

Finalement, le tarif de la LS est fonction du débit et de la distance entre les deux sites à relier ce qui fait qu'aujourd'hui, la plupart des clients choisissent plutôt des

technologies ADSL ou fibre qui peuvent être de plus sécurisées dans le cadre de VPN (voir chapitre 9).

7.2 Le réseau téléphonique commuté

7.2.1 Architecture

Le réseau téléphonique comporte des opérateurs de transport de boucle locale (majoritairement Orange) et d'interconnexion régionale (Orange, SFR, Completel…).

Les opérateurs de boucle locale offrent une interconnexion aux opérateurs d'interconnexion qui le demandent par l'intermédiaire de commutateurs d'interconnexion (figure 7.2).

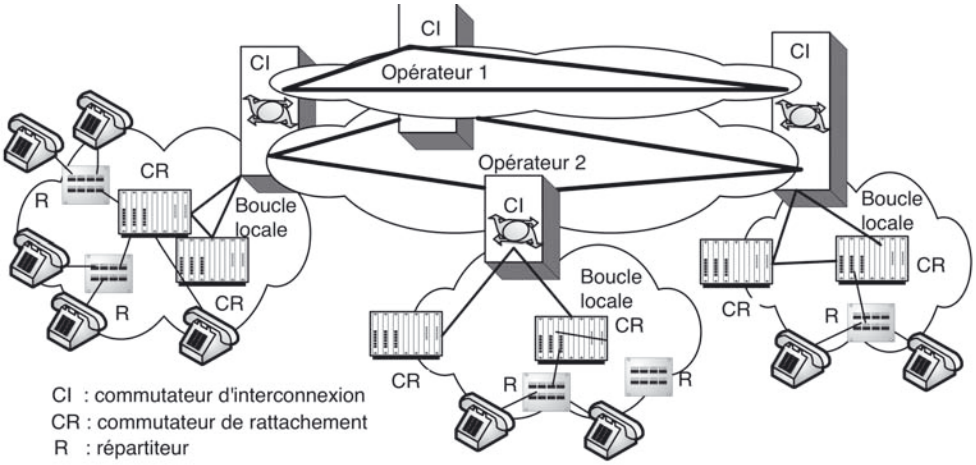


Figure 7.2 – **Architecture du réseau téléphonique commuté.**

À une échelle plus large, chaque opérateur d'interconnexion est structuré en deux niveaux : régional et national. Dans cette architecture, le nombre de liens d'interconnexion nationale est inférieur à celui de l'interconnexion régionale, mais leurs débits sont plus élevés. Au passage du niveau régional au niveau national, les communications doivent être multiplexées.

7.2.2 La boucle locale

Côte utilisateur, dans la mesure où les opérateurs alternatifs (autres que Orange) spécialisés dans l'accès ADSL souhaitent bénéficier, pour des raisons essentiellement commerciales, d'un accès au plus près de l'usager, la boucle locale tend à se rapprocher de l'abonné. Pour ce type d'exploitation, la boucle locale correspond donc à la partie située entre la prise téléphonique de l'abonné final et le central local

(figure 7.3). Plus précisément, le terminal de l'abonné peut être un poste téléphonique, un modem ou une installation complexe (PABX) d'une grande entreprise. De l'autre côté, la boucle locale s'arrête au répartiteur ou sous-répartiteur, armoire qui concentre l'ensemble des lignes d'usagers en paire de cuivre torsadée avant de les renvoyer vers le commutateur de rattachement.

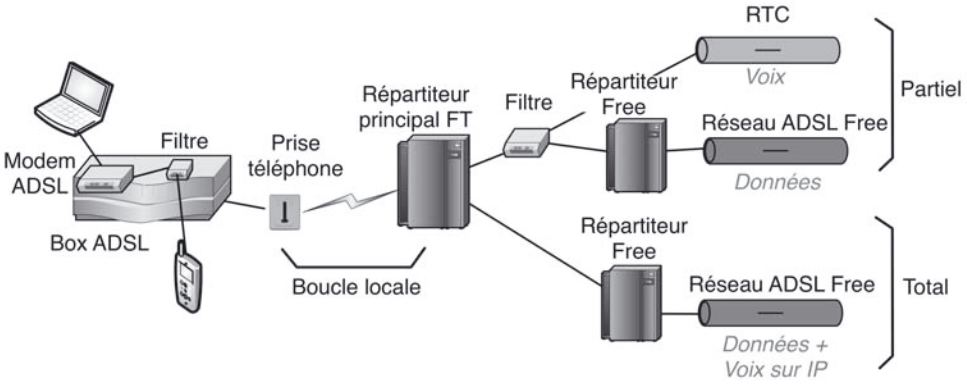


Figure 7.3 – **Dégroupage partiel ou total.**

La boucle locale est une facilité essentielle : un opérateur de télécommunication doit nécessairement y avoir accès pour pouvoir offrir ses services sur le marché de détail. C'est pourquoi Orange doit fournir un accès dégroupé à la boucle locale aux opérateurs alternatifs.

7.2.3 Le dégroupage

Le dégroupage permet aux opérateurs alternatifs de bénéficier d'un accès « direct » à l'utilisateur final. Ils sont en mesure de contrôler de bout en bout le réseau et de fournir ainsi un service différencié de celui de l'opérateur historique. Le dégroupage rend en particulier possible une concurrence réelle dans les offres commerciales d'ADSL et de fait une baisse des tarifs de détail.

Par ailleurs, les opérateurs alternatifs peuvent offrir sur la boucle locale une nouvelle solution de câblage en fibre optique pour des débits plus importants. L'ouverture du marché permet à l'usager de choisir un FAI (Fournisseur d'Accès Internet) différent de l'opérateur qui fournit le câblage mais ce dernier se verra dans ce cas rétribué par le FAI choisi. La pose de la fibre optique représente donc un enjeu financier très important car son exploitation sera rétribuée de nombreuses années quel que soit le FAI qui délivre au final la connexion à l'abonné.

La figure 7.3 montre les deux organisations possibles :

- dans le **dégroupage partiel**, un filtre permet d'orienter les fréquences basses (voix) vers le réseau téléphonique de FT, et les fréquences hautes (données) vers le réseau de l'opérateur alternatif fournissant la connexion ADSL ;

- dans le **dégroupage total**, l'opérateur alternatif dispose de la totalité de la bande de fréquence de la paire de cuivre. Seule la bande haute est utilisée pour les données avec une solution de téléphonie sur IP.

7.3 Le réseau ATM

7.3.1 Principe

L'ATM (*Asynchronous Transfer Mode*) est une technique de transmission commutée faisant appel à des paquets courts de tailles fixes appelés cellules. Dans les commutateurs, le traitement de ces cellules est limité à l'analyse de l'en-tête pour permettre leur acheminement.

L'ATM combine les avantages de la commutation rapide de paquets et du multiplexage temporel asynchrone :

- la station source et le réseau ne sont pas liés par la nécessité d'émettre ou de recevoir une quantité d'information en synchronisme avec une trame de durée fixe ;
- la commutation est indépendante de la nature des informations véhiculées (voix, données, images) et un débit minimum peut être garanti ;
- la cellule a une taille fixe, ce qui permet de concevoir des commutateurs relativement simples et performants ;
- la cellule a une taille courte (53 octets), ce qui permet l'adaptation à différents types de trafics avec une gigue réduite (variation des intervalles de temps entre cellules).

De base ATM est orienté connexion. Les connexions sont établies pour toute la durée des échanges par l'allocation d'un chemin virtuel (voix virtuelle ou conduit virtuel).

Les fonctions de contrôle de flux ou de traitement des erreurs ne sont pas effectuées dans le réseau ATM, mais laissées à la charge des applications utilisatrices ou des équipements d'accès.

Ces caractéristiques permettent à l'ATM de répondre aux contraintes de trafics aussi différents que la voix, la vidéo numérique ou les données. Ce mode de transfert universel rend possible l'intégration de tous types de services sur un accès unique au réseau. D'abord conçu et sélectionné par l'UIT-T pour être la solution technique des réseaux publics large bande (à la place des réseaux Transpac et RNIS en France), l'ATM était également prévu pour être utilisé sur les LAN. Cependant sa complexité et son manque d'interopérabilité avec les réseaux IP ont freiné son implantation au profit de techniques plus universelles comme MPLS. Aujourd'hui, ATM subsiste essentiellement dans les réseaux de collecte des liaisons ADSL.

7.3.2 Architecture

La commutation de cellules d'ATM est basée sur un modèle en trois couches (figure 7.4) :

- la couche **AAL** (*ATM Adaptation Layer*) adapte les flux d'information à la structure des cellules et fait le lien avec les couches applicatives ;
- la couche **ATM** assure la commutation et le multiplexage des cellules ;

- la couche **Physique** ou **PMD** (*Physical Medium Dependent*) assure l'adaptation au support utilisé avec un codage suivant le débit utilisé (155 et 622 Mbit/s).

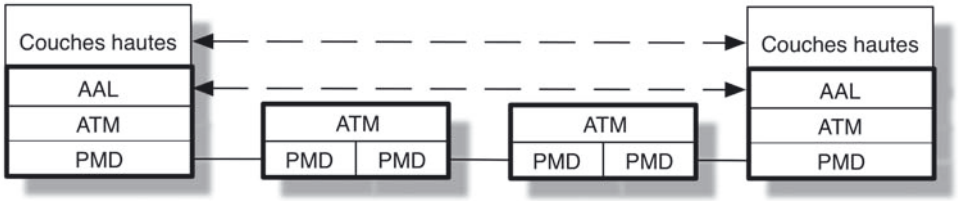


Figure 7.4 – **Couches ATM.**

7.3.3 La couche ATM

Cette couche a pour rôle de convertir les flux de données en cellules et de gérer la commutation et le multiplexage de celles-ci. Le trafic utile (voix, vidéo, images et données) est encapsulé dans les cellules de 53 octets pour être véhiculé sur le réseau.

a) Structure des cellules

La cellule a une longueur de 53 octets et contient deux champs principaux (figure 7.5) :

- l'en-tête sur 5 octets dont le rôle principal est d'identifier les cellules appartenant à une même connexion et d'en permettre l'acheminement ;
- le champ de données sur 48 octets correspondant à la charge utile.

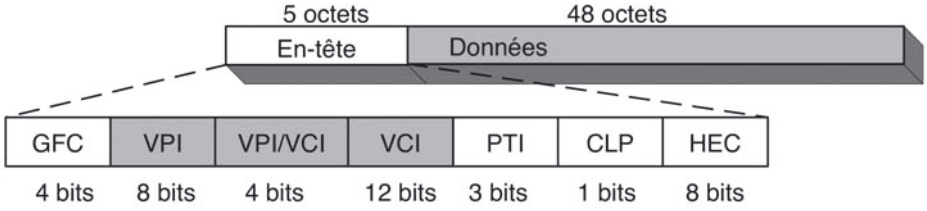


Figure 7.5 – **Structure des cellules ATM.**

L'en-tête comporte les champs suivants :

- un champ de contrôle de flux (GFC, *Generic Flow Control*) dont la définition n'est pas arrêtée ;
- trois octets sont utilisés pour l'identificateur logique (VPI, *Virtual Path Identifier* et VCI, *Virtual Channel Identifier*) ;
- trois bits sont consacrés à la définition du type de la charge utile (PTI, *Payload Type Identification*) et permettent de définir s'il s'agit d'informations utilisateur (indication de congestion, données de type 0 ou 1) ou de messages de service du réseau (maintenance, gestion des ressources du réseau) ;

- un bit de référence à l'écartement (CLP, *Cell Less Priority*) mis à 1 dans les cellules transportant des données de moindre importance pouvant être rejetées en cas de congestion du réseau ;
- un octet pour la détection des erreurs et la correction des erreurs simples portant sur l'en-tête (HEC, *Header Error Check*) et gérée par la couche physique.

b) Fonctions de la couche ATM

La couche ATM assure quatre fonctions essentielles :

- la commutation consistant en un traitement sur l'en-tête de la cellule (champs VPI et VCI). Ces champs sont soit insérés soit extraits et traduits afin d'aiguiller correctement la cellule ;
- le multiplexage-démultiplexage des cellules consistant principalement en une gestion de files d'attente ;
- l'extraction ou l'ajout de l'en-tête devant le champ d'information avant de le transmettre à la couche d'adaptation AAL ou à la couche physique ;
- un mécanisme de contrôle de flux peut être implémenté par l'intermédiaire du champ GFC, pour l'interface utilisateur-réseau.

La figure 7.6 montre un exemple de multiplexage temporel asynchrone des flux. Les cellules correspondant à des applications plus ou moins prioritaires (voix, vidéo, données) sont transmises au rythme du débit engendré par l'application. L'échange avec le réseau est donc **asynchrone** et la station source seule gère son débit en fonction des paramètres définis en début de communication (*bandwith on demand*) autorisant la Qualité de Service (*Quality of Service*) de la transmission de bout en bout.

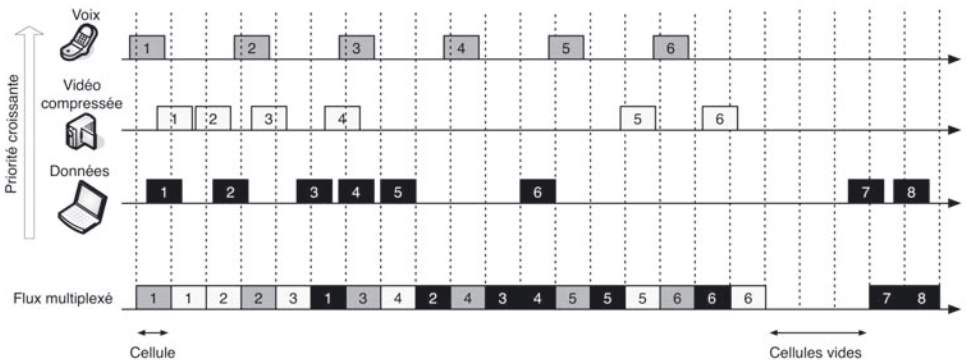


Figure 7.6 – Multiplexage temporel asynchrone des flux.

c) Routage des cellules

Les informations sont transportées par des circuits virtuels (VC, *Virtual Channel*), regroupées dans des chemins virtuels (VP, *Virtual Path*). Les chemins virtuels représentent des conduits reliant des commutateurs dans un réseau maillé (figure 7.7).

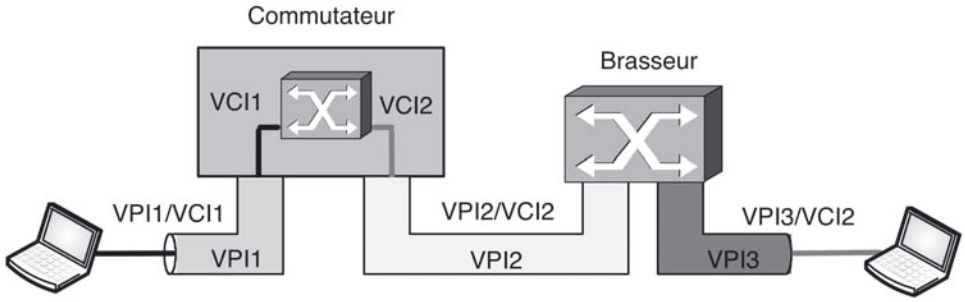


Figure 7.7 – **Notion de chemin et de circuit virtuel.**

Le **commutateur** est l'élément de base permettant d'orienter correctement les cellules dans le réseau. Il agit en fonction des valeurs des indicateurs VPI et VCI contenus dans les cellules et à l'aide de tables de commutation, afin de modifier en conséquence l'en-tête de la cellule et de mettre en correspondance un port d'entrée avec un port de sortie. À l'entrée du réseau, les commutateurs agissent sur la paire VPI/VCI. D'autres commutateurs, au cœur du réseau, limitent leurs tables en ne commutant que les VP : ce sont des **brasseurs**.

7.4 Les liaisons SDH et SONET

La hiérarchie (*Synchronous Digital Hierarchy*) normalisée par l'UIT-T et son équivalent américain SONET (*Synchronous Optical Network*) sont utilisés par les opérateurs de télécommunication dans les réseaux haut débit comme ATM pour fournir une structure de trame et transporter des cellules ATM ou des paquets IP sur des transmissions séries point à point généralement en fibre optique.

La technologie SDH conçue au départ pour des communications en mode circuit, telles les communications téléphoniques, est aujourd'hui fortement concurrencée par Ethernet (voir paragraphe 7.5), architecture conçue à l'origine pour le transport de paquets IP, majoritaires aujourd'hui sur l'ensemble des services.

Suivant le type de trame utilisée, SDH permet des débits hiérarchisés de quelques centaines de mégabits par seconde à plusieurs gigabits par seconde (tableau 7.1).

Tableau 7.1 – **Débits hiérarchisés du protocole SDH.**

Trame SDH	STM-1	STM-4	STM-16	STM-64	STM-128	STM-256
Débit	155,52 Mbit/s	622,08 Mbit/s	2,5 Gbit/s	10 Gbit/s	20 Gbit/s	40 Gbit/s

Les données sont transportées dans des trames synchrones (*Synchronous Transport Module*) et « empaquetées » dans des conteneurs virtuels (*Virtual Container*)

qui englobent les données d'un même paquet réparties sur plusieurs trames. Les trames sont émises toutes les 125 µs.

La trame de base STM-1 comporte 9 × 270 octets (9 rangées de 270 octets). Chaque rangée contient une partie en-tête et une partie données (figure 7.8) :

- **TOH** (*Transport OverHead*) : en-tête de transport sur 9 octets (par rangée), contient des fanions, des informations d'erreur de trames, et la valeur du décalage du paquet de données ;
- **POH** (*Path OverHead*) : en-tête de routage sur 1 octet, contient un identificateur de chemin (adressage au format E.164) contrôlé par une information d'erreur ;
- **Champ des données** : plage de 9 × 261 octets dans laquelle sont placés les paquets de données (*Synchronous Payload Envelope*). Pour pouvoir adapter en temps et en longueur le format des paquets de données aux réseaux et aux protocoles de niveaux supérieurs, un décalage dont la valeur se trouve dans l'en-tête de transport TOH est introduit.

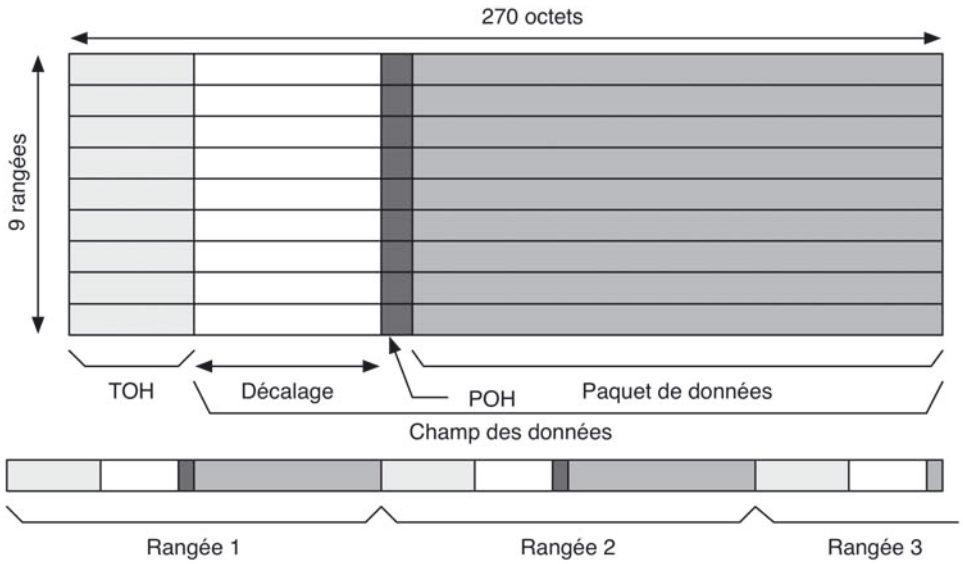


Figure 7.8 – **Structure d'une trame STM-1 et ordre de transmission.**

La figure 7.9 montre comment des cellules ATM de 53 octets et des paquets IP de 500 octets peuvent être transportés. Le décalage du champ TOH donne la position de la première cellule ou paquet dans le champ de données. Suivant le flux et le débit souhaité, plusieurs cellules ou paquets peuvent ainsi se succéder.

L'organisation hiérarchique de SDH permet de multiplier les débits en construisant par exemple une trame STM-4 par « concaténation » de quatre trames STM-1 (figure 7.10). Cette méthode permet :

- de réduire le nombre de liaisons physiques en fibre optique sur un réseau en utilisant des liens d'interconnexion haut débit ;

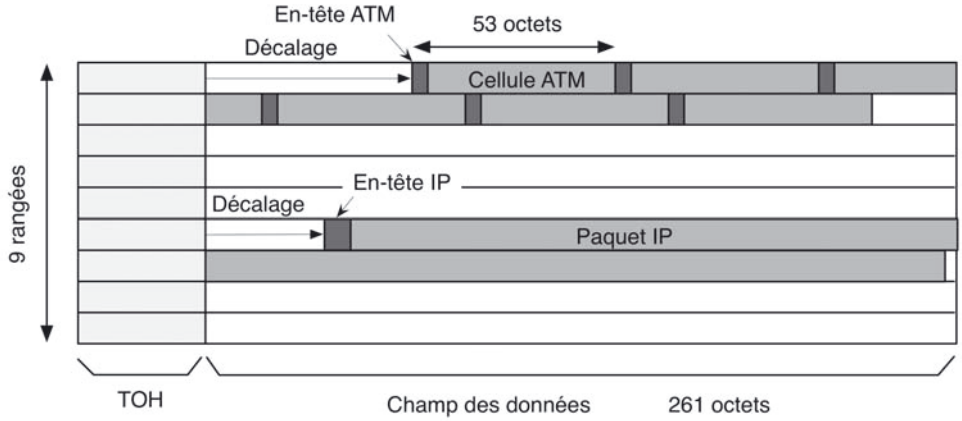


Figure 7.9 – **Exemple de transport de cellules et de paquets dans une trame STM-1.**

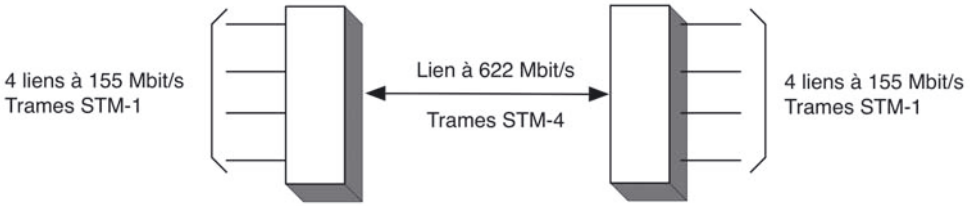


Figure 7.10 – **Hiérarchisation des débits sur les liens d'interconnexion.**

- de transporter plusieurs types de données suivant différents protocoles dans une même trame (IP, ATM, relais de trame, voir chapitres 7 et 8).

7.5 Ethernet classe opérateur

L'objectif de l'Ethernet classe opérateur, ou *Ethernet Carrier Grade*, est d'étendre la technologie Ethernet, prépondérante dans les LAN, à la boucle locale et au cœur du réseau d'opérateur. Cette extension permet de conserver la même structure de trame et d'éviter les fragmentations, les encapsulations et décapsulations successives tout en assurant un débit important, jusqu'à 100 Gbit/s.

La norme initiale doit cependant subir des améliorations pour répondre aux besoins des opérateurs parmi lesquelles :

- le facteur d'échelle : alors qu'Ethernet a été conçu pour des réseaux locaux supportant un nombre limité de machines, les FAI raccordent des milliers d'abonnés et doivent disposer d'un espace d'adressage suffisant ;
- la disponibilité de la ligne : elle doit être équivalente à celle des réseaux de télécommunications. La disponibilité du RTC par exemple est égale à 99,999 %. Il est donc nécessaire d'introduire des procédures de contrôle et de maintenance du réseau et de rétablissement en cas de panne ;

- la qualité de service : certains services comme la téléphonie ont des exigences fortes, notamment en termes de délai moyen garanti. L'Ethernet classe opérateur doit donc rajouter des fonctionnalités pour assurer cette QoS (*Quality of Service*).

Les solutions utilisées actuellement reprennent des principes connus : la création d'un chemin avant l'émission des trames et la réservation des ressources pour garantir la QoS. Elles permettent des connexions point à point de type EVPL (*Ethernet Virtual Private Line*) et multipoint de type VPLS (*Virtual Private LAN Service*).

La figure 7.11 représente une interconnexion de sites locaux Ethernet à l'aide d'un service Ethernet classe opérateur de type multipoint VPLS s'appuyant sur un réseau MPLS (voir paragraphe suivant). La structure de trame reste Ethernet de bout en bout.

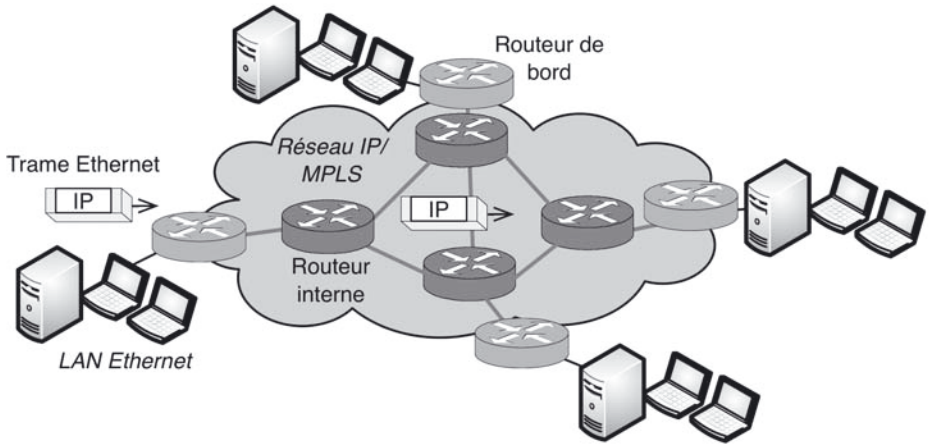


Figure 7.11 – Connexion Ethernet Carrier Grade multipoint.

7.6 L'architecture MPLS

7.6.1 Principe

MPLS (*Multiprotocol Label Switching*) est une architecture normalisée par l'IETF (*Internet Ingineering Task Force*) permettant d'intégrer et d'homogénéiser les différents protocoles de routage et de commutation existant à différents niveaux (Ethernet, IP, ATM…) dans les réseaux d'opérateurs. L'objectif principal étant d'améliorer les délais, et donc la qualité de service dans les équipements intermédiaires en pratiquant une commutation rapide (*switching*) multiniveau basée sur l'identification des étiquettes (*label*) portées par les trames ou les paquets.

MPLS présente les caractéristiques suivantes :

- indépendance des protocoles des couches 2 et 3 ;
- support des couches de niveau 2 des réseaux IP, ATM, Ethernet et Frame Relay ;

- interaction avec les protocoles de réservation et de routage existant (RSVP, OSPF) ;
- possibilité d'association des profils de trafic spécifiques (FEC, *Forward Equivalence Class*) à des labels.

Dans MPLS, la transmission de données se fait sur des chemins à commutation de label ou **LSP** (*Label Switched Path*). Les LSP correspondent à une séquence de labels à chaque nœud (équipement) du chemin allant de la source à la destination. Les labels, qui sont des identifiants spécifiques au protocole des couches basses (adresses MAC Ethernet, champs VPI/VCI des cellules ATM…), sont distribués suivant le protocole **LDP** (*Label Distribution Protocol*).

Chaque paquet de données encapsule et transporte les labels pendant leur acheminement. Dans la mesure où les labels de longueur fixe sont insérés au tout début de la trame ou de la cellule, la commutation haut débit est possible.

Les nœuds sont chargés de lire les labels et de commuter les trames ou les cellules suivant la valeur de ces labels et des tables de commutation établies au préalable sur le LSP (voir exemple de la figure 7.12). Ces nœuds, suivant leur localisation sur le réseau, sont du type :

- **LSR** (*Label Switch Router*) pour un équipement de type routeur ou commutateur situé au cœur d'un réseau MPLS et se limitant à la lecture de labels et à la commutation (les adresses IP ne sont pas lues par les LSR une fois le chemin tracé) ;
- **LER** (*Label Edge Routers*) pour un routeur/commutateur à l'extrémité du réseau d'accès ou du réseau MPLS pouvant supporter plusieurs ports connectés à des réseaux différents (ATM ou Ethernet). Les LER jouent un rôle important dans l'assignation et la suppression des labels pour les paquets entrants ou sortants.

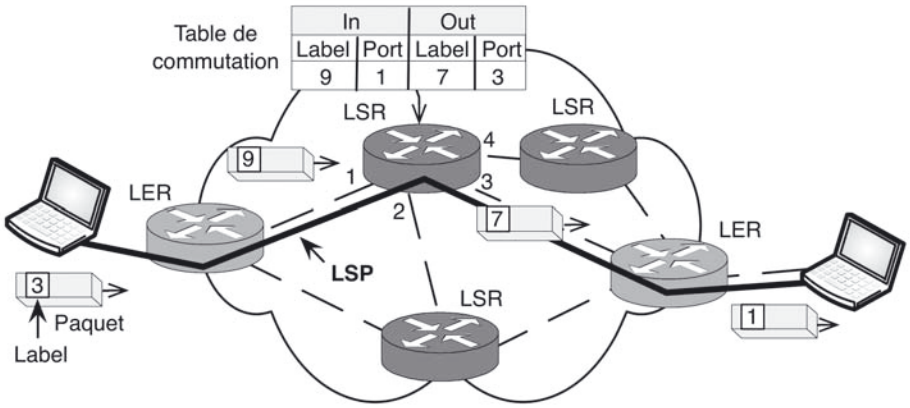


Figure 7.12 – **Nœuds et chemin MPLS.**

7.6.2 Label et classes MPLS

Un **label**, dans sa forme la plus simple, identifie le chemin que le paquet doit suivre. Le label est encapsulé et transporté dans l'en-tête du paquet. Une fois qu'un

paquet est labellisé, le reste de son voyage est basé sur la commutation de labels. Le routeur qui reçoit le paquet analyse son label et cherche l'entrée correspondante dans sa table de commutation pour déterminer l'interface de sortie et le nouveau label affecté au paquet. Les valeurs du label ont donc une portée locale et peuvent être liées à une architecture particulière pour déterminer directement un chemin virtuel (de type VCI/VPI pour ATM par exemple). Le format générique d'un label est illustré par la figure 7.13. Il est situé entre les couches 2 et 3 ou directement dans l'entête de la couche 2 (adresses MAC pour Ethernet, VCI/VPI dans ATM…).

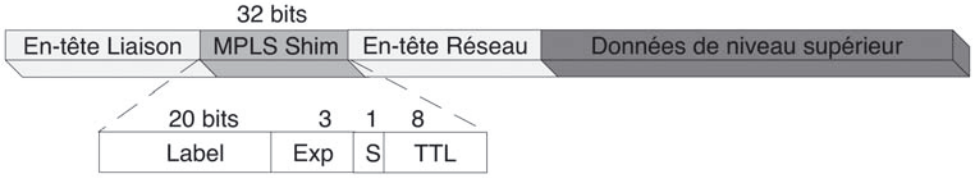


Figure 7.13 – Format de base des labels MPLS.

À côté de la valeur du label, différents champs sont prévus pour rajouter des fonctionnalités :

- le champ expérimental n'est pas normalisé et peut être utilisé pour gérer la QoS, par exemple en lui associant une priorité dans la file d'attente d'un routeur ;
- le bit « Stack » prend la valeur 1 lorsque le label se trouve au sommet de la pile dans une interconnexion de réseaux avec plusieurs niveaux de labels (hiérarchie VPI/VCI d'un réseau ATM par exemple) ;
- le champ TTL (*Time to Live*), comme pour IP, permet de prévenir les bouclages.

Une classe d'équivalence ou **FEC** (*Forwarding Equivalence Class*) correspond à un groupe de paquets qui ont en commun les mêmes besoins, en termes de préfixes d'adresses ou de QoS. Contrairement aux autres modèles, dans MPLS un paquet est assigné à une FEC une seule fois, lors de son entrée sur le réseau. Chaque LSR se construit une table **LIB** (*Label Information Base*) pour savoir comment un paquet doit être transmis. Les labels sont donc associés à une FEC suivant une logique ou une politique basée sur différents critères : QoS, même préfixe d'adresse source ou destination, paquets d'une même application, appartenance à un VPN (*Virtual Private Network*).

7.6.3 Chemins MPLS

Dans l'exemple de la figure 7.14, la FEC correspond au préfixe d'adresses de destinations 18.1. À l'entrée sur le réseau MPLS, le routeur de bord LER inclut le label correspondant à cette FEC pour le paquet entrant suivant sa table de commutation LIB. Les routeurs centraux LSR ont ensuite pour rôle d'échanger le label toujours suivant la FEC et de commuter le paquet. Le routeur de bord LER sortant assure le retrait du label et le routage du paquet vers la destination. Le chemin LSP tracé correspond, dans l'exemple, à la suite des labels 9-7-1.

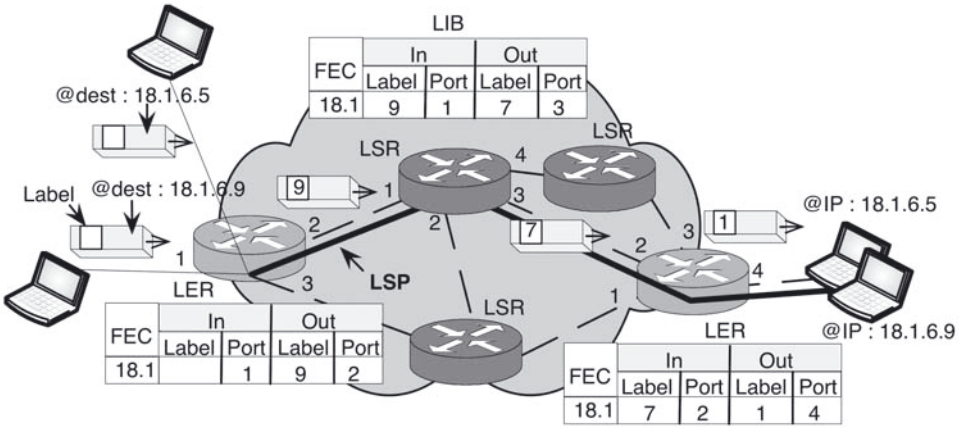


Figure 7.14 – Exemple de commutation MPLS.

Les routeurs de bord LER sont donc obligés de remonter jusqu'au niveau réseau pour analyser les adresses IP et positionner les labels en conséquence. Les routeurs centraux LSR, lorsque les tables ont été positionnées par une signalisation préalable (protocole LPD ou protocole de routage), jouent un simple rôle de commutateur de label (les LSR peuvent être de simples commutateurs ATM). Le processus de tracé du chemin nécessite donc deux niveaux de protocoles :

- un protocole de routage tel OSPF ou BGP chargé de la diffusion des routes et de l'établissement des tables de routages ;
- un protocole de distribution de label tel LDP permettant la mise en place des tables de commutation à partir des tables de routage et des FEC.

7.7 Les réseaux cellulaires

7.7.1 Généralités

Les réseaux cellulaires sont des réseaux d'opérateur organisés en cellules pour offrir à l'abonné une connectivité sans fil vers un réseau téléphonique ou vers l'Internet à partir de son téléphone mobile ou de son smartphone.

Une cellule correspond à une zone géographique, plus ou moins grande selon la densité d'usagers et le relief, dans laquelle une bande de fréquence est allouée et partagée par l'ensemble des utilisateurs connectés. Cette organisation permet d'optimiser le partage des ressources radio et la réutilisation des fréquences. Les cellules sont des zones théoriquement circulaires qui se chevauchent. Pour simplifier, on les représente sous forme d'hexagones. Au centre de chaque cellule, se trouve une antenne-relais (figure 7.15).

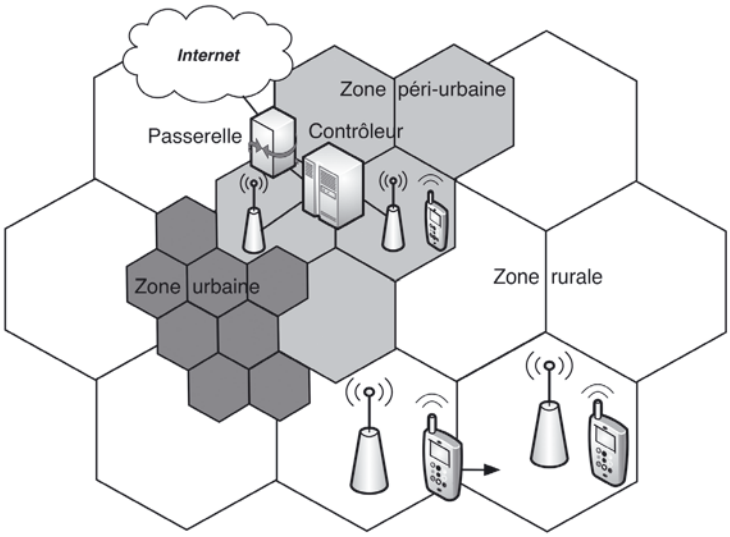


Figure 7.15 – **Organisation du réseau cellulaire.**

Ces réseaux, souvent nommés réseaux de mobiles, sont conçus pour assurer une connectivité ininterrompue lorsque l'abonné se déplace d'une cellule à l'autre (procédure du *hand-over*).

Depuis leurs premiers déploiements dans les années 1990, ces réseaux ont fortement évolué, notamment en termes de débit. Les applications ne sont donc plus limitées à la téléphonie mais couvrent tous les domaines présents dans les réseaux fixes (données, multimédia, TV…). La figure 7.16 présente les générations successives de réseaux cellulaires avec les débits maximums et les appellations correspondant aux différentes normes.

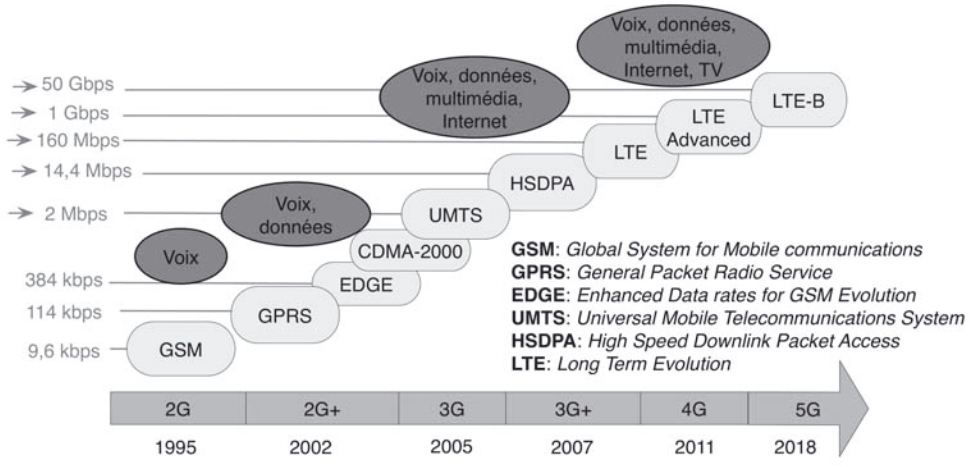


Figure 7.16 – **Générations de réseaux cellulaires.**

7.7.2 Le réseau GSM

a) Architecture

L'architecture d'un réseau GSM de base peut être divisée en deux sous-systèmes (figure 7.17) :

- le sous-système radio ou **BSS** (*Base Station Subsystem*) qui gère la transmission radio. Il est constitué du mobile de l'abonné ou **MS** (*Mobile System*), de la station de base ou **BTS** (*Base Transceiver Station*) qui inclut l'antenne-relais et du contrôleur de station de base ou **BSC** (*Base Station Controller*) ;
- le sous-système réseau ou **NSS** (*Network SubSystem*) qui prend en charge toutes les fonctions de contrôle et d'analyse des informations contenues dans des bases de données nécessaires à l'établissement des connexions (authentification de l'abonné, itinérance, chiffrement…). Le NSS comprend le **MSC** (*Mobile Switching Center*) et les bases de données en liaison (VLR, HLR…).

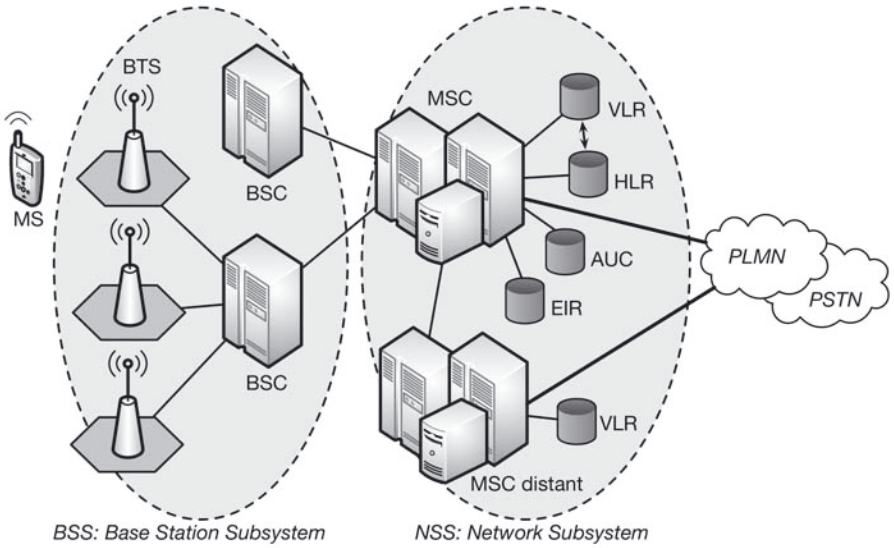


Figure 7.17 – Architecture du réseau GSM.

La **MS** qui intègre le système d'émission/réception radio de l'abonné comporte également une carte à puce qui permet de rendre indépendant l'abonnement du terminal physique. Cette carte SIM (*Subscriber Identity Module*) possède en mémoire (figure 7.18) :

- les caractéristiques de l'abonnement ;
- le **MSISDN** (*Mobile Station International ISDN Number*) : numéro international de l'abonné suivant le plan de numérotation E.164. C'est par ce numéro qu'il peut appeler ou être appelé ;

- le **IMSI** (*International Mobile Subscriber Identity*) qui est l'identité permanente du mobile auprès du réseau. Elle n'est pas connue par l'utilisateur ;
- le **TMSI** (*Temporary Mobile Subscriber Identity*) qui est l'identité temporaire du mobile auprès du MSC ;
- les algorithmes de chiffrement.

Le mobile comporte également :

- le **MSRN** (*Mobile Station Roaming Number*), numéro temporaire au même format que le MSISDN qui remplace ce dernier en cas d'itinérance (*roaming*) ;
- l'**IMEI** (*International Mobile Equipment Identity*), identité propre au terminal allouée lors de sa fabrication.

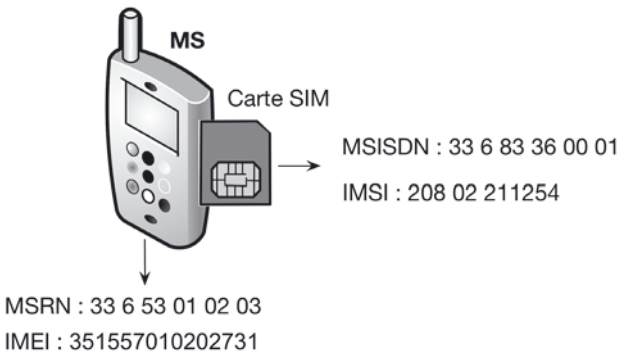


Figure 7.18 – Numéros et identités GSM.

La **BTS** (*Base Transceiver Station*) est la station de base d'émission et de réception. Elle assure la couverture radio d'une cellule (rayon de 200 m à ~30 km) et prend en charge les opérations de modulation/démodulation, de correction des erreurs, de cryptage des communications et de mesure de la qualité et de la puissance de réception.

Le **BSC** (*Base Station Controller*) pilote un ensemble de stations de base (typiquement ~60) et réalise l'aiguillage vers le BTS destinataire. Il gère donc les ressources radio (affectation des fréquences, contrôle de puissance…), les appels (établissement, supervision, libération des communications…) et les transferts intercellulaires (*handover*).

Le **MSC** (*Mobile Switching Center*) est un commutateur numérique en mode circuit qui oriente les signaux vers les BSC. Il établit la communication en s'appuyant sur les bases de données qui lui sont reliées et assure l'interconnexion avec les autres réseaux cellulaires (PLMN, *Public Land Mobile Network*) et les réseaux téléphoniques fixes (PSTN, *Public Switched Telephone Network*).

Les bases de données reliées au MSC ont différents rôles :

- le **HLR** (*Home Location Register*) est unique au réseau et contient les informations relatives aux abonnés : données statiques (IMSI, MSISDN, type d'abonnement…) et données dynamiques (localisation, état du terminal…) ;
- le **VLR** (*Visitor Location Register*) est une base de données locale (un VLR par commutateur MSC) qui contient les informations relatives aux abonnés présents

dans la zone associée (il est donc mis à jour à chaque changement de cellule d'un abonné). Le VLR échange en permanence des informations avec le HLR et contient en plus de ce dernier l'identité temporaire (TMSI) et la localisation de l'abonné ;

- l'**AUC** (*AUthentification Center*) assure l'authentification des abonnés et gère les fonctions de chiffrement grâce aux clés de cryptage contenues dans la carte SIM ;
- l'**EIR** (*Equipment Identity Register*) empêche l'accès au réseau aux terminaux non autorisés (terminaux volés) grâce au IMEI. À chaque appel, le MSC contacte le EIR et vérifie la validité du IMEI.

b) L'accès radio

L'accès radio pour la technologie de base GSM s'appuie sur une combinaison de multiplexage FDMA et TDMA (multiplexage F-TDMA) dans la bande des 890-960 MHz. Un ensemble de 124 canaux de 200 kHz, partagés par les différents opérateurs, est alloué pour les bandes montantes et descendantes (figure 7.19). Sur chaque canal, une trame périodique TDMA de 8 slots temporels est réservée. Le débit total sur la trame est de 270 kbit/s grâce à une modulation non linéaire GMSK (*Gaussian Minimum Shift Keying*).

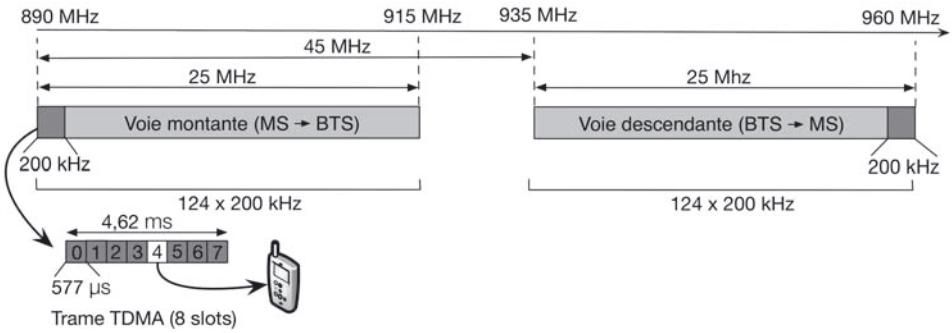


Figure 7.19 – Multiplexages du canal physique GSM.

Le débit pour chaque mobile peut varier suivant le nombre de slots temporels attribués. Dans l'exemple de la figure 7.19, seul le slot 4 de la trame située dans le premier canal montant est attribué à l'abonné et le débit en voie montante est de 270 kbit/s / 8 = 33,75 kbit/s.

Le paquet ou *burst* transmis pendant un slot est organisé en différents champs (figure 7.20) :

- 3 bits de tête et de queue pour ajuster la puissance ;
- les données codées sur 2 × 57 = 114 bits ;
- une séquence d'apprentissage pour permettre au récepteur de se synchroniser ;
- un délai de garde pour régler l'alignement temporel.

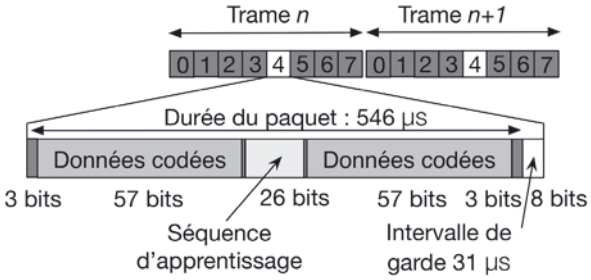


Figure 7.20 – **Organisation du paquet de données.**

Finalement, dans la transmission téléphonique cellulaire de base, chaque trame analogique de parole d'une durée de 20 ms est numérisée sur 260 bits qui deviennent 456 bits après un codage limitant les risques d'erreurs. Ces 456 bits sont repartis dans 8 demi-paquets de 57 bits et chaque demi-paquet est inséré dans le slot périodique réservé de 8 trames TDMA successives (figure 7.21). Cet étalement sur 8 trames alors que 4 trames pourraient suffire ($2 \times 4 \times 57 = 456$) permet une meilleure protection contre les erreurs de transmission qui se produisent souvent par trame.

Les blocs de 57 bits libres dans les 8 trames, pour le même slot réservé et donc le même abonné, sont remplis avec les données de la trame de parole précédente ou suivante (entrelacement).

Les trames TDMA sont ensuite chiffrées avant modulation et transmission sur le canal physique.

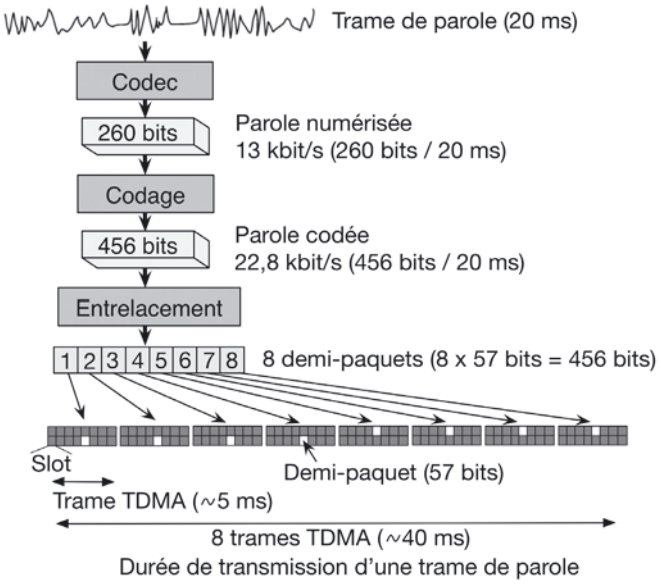


Figure 7.21 – **Chaîne de traitement et de transmission d'un échantillon de parole.**

c) *Handover* et *roaming*

Le *handover* désigne le processus qui permet de basculer une communication en cours d'un canal physique à un autre sans que la communication ne soit interrompue. Un *handover* peut se produire pour différentes raisons (figure 7.22) :

- allocation intracellulaire (changement de slot TDMA) ;
- intercellulaire (changement de cellule sur le même BSC) ;
- intra-MSC (changement de cellule sur un BSC différent mais dans le même MSC) ;
- inter-MSC (changement de cellule sur un MSC différent) ;
- inter-réseau (changement de réseau, par exemple entre GSM et UMTS).

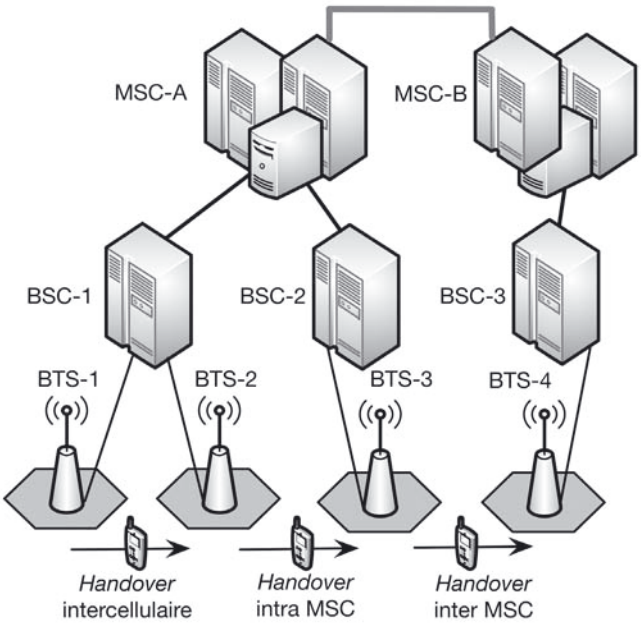


Figure 7.22 – Différents types de handover.

Lors de la procédure de *handover*, le terminal procède en trois phases :

- il détecte et mesure la puissance des fréquences porteuses des cellules voisines ;
- il se déclare auprès de la cellule fournissant la porteuse la plus forte ;
- il demande au réseau le basculement de cellule.

Dans la réalité, le mécanisme est compliqué par le fait :

- que la croissance/décroissance de puissance des porteuses n'est pas linéaire ;
- que le terminal peut se trouver dans le champ de nombreuses cellules (comme en zone urbaine).

Dans les réseaux UMTS, le basculement se fait sur la même fréquence porteuse, contrairement aux technologies précédentes.

L'itinérance ou *roaming* diffère du *handover* dans la mesure où il y a changement d'opérateur. Le *roaming* désigne donc la possibilité pour un abonné d'un opérateur d'utiliser les services d'un autre opérateur lors d'un déplacement, notamment dans un pays étranger. Ce mécanisme utilise les informations contenues dans les HLR et VLR sur la zone où est localisé l'abonné.

7.7.3 La 3G et l'UMTS

a) Objectifs

La technologie GSM proposée à la base dans la deuxième génération possède un débit de transmission limité à 9 kbit/s, suffisant pour la téléphonie mobile pour laquelle elle était prévue au départ, mais insuffisant pour transporter des données. Les évolutions successives de la 2G ont fait évoluer ce débit et ont rajouté d'autres services comme la facturation au volume de données (et pas seulement selon le temps de connexion), l'accès simplifié aux réseaux en mode paquet et un débit adaptatif en fonction du besoin (allocation dynamique de canal).

Les débits proposés par les technologies **GPRS** (114 kbit/s) et **EDGE** (384 kbit/s), basées sur le GSM et son architecture, sont restés cependant insuffisants pour supporter avec succès les applications de l'Internet.

Les objectifs de la troisième génération qui a suivi sont donc multiples :

- transport de données de type voix et données à haut débit sur la même connexion ;
- coexistence avec les réseaux 2G, en particulier le GSM ;
- un réseau cœur IP ;
- extension du plan de fréquences pour faire face à la saturation des zones denses du GSM ;
- introduction de classes de services différenciées ;
- possibilité de *roaming* au niveau mondial, et donc compatibilité entre tous les réseaux.

La technologie retenue en Europe pour la 3G est l'**UMTS** (*Universal Mobile Telecommunication System*). Elle présente les caractéristiques suivantes :

- les tailles de cellule ne sont plus limitées à 0,2-30 km ;
- les bandes de fréquence sont centrées sur 2 GHz et non plus sur 900 MHz ;
- un multiplexage par code à large bande : **W-CDMA** (*Wideband Code Division Multiple Access*) ;
- des débits théoriques suivant la taille de la cellule et la mobilité :
  - ◇ 144 kbit/s pour une utilisation mobile rapide (voiture, train) en zone rurale,
  - ◇ 384 kbit/s pour une utilisation piétonne en zone urbaine,
  - ◇ 2 Mbit/s pour une utilisation fixe en zone urbaine.

b) Architecture

La figure 7.23 présente l'architecture du réseau UMTS avec la partie radio **UTRAN** (UMTS *Terrestrial Radio Access Network*) et le cœur du réseau (*Core Network*).

Le mobile nommé **UE** (*User Equipment*) est connecté *via* une liaison à 2 Mbit/s à la station de base nommée **Node B** qui dessert une cellule. Les Node B sont contrôlés par une **RNC** (*Radio Network Controller*), équivalent du BSC pour le GSM.

Les données en mode circuit pour la téléphonie sont transmises vers le réseau GSM. Les données en mode paquet sont envoyées vers un équipement spécifique (souvent colocalisé avec le MSC) : le **SGSN** (*Serving GPRS Support Node*) qui connecte les différents RNC et qui est chargé d'enregistrer les usagers d'une zone géographique dans une zone de routage. La liaison vers les réseaux à commutation de paquet extérieurs tels Internet est ensuite réalisée par une passerelle **GGSN** (*Gateway GPRS Support Node*). Les services de transmission par paquet du réseau GPRS sont donc en partie réutilisés.

Les bases de données contenant les informations d'abonnés (HLR, VLR, EIR et AUC) sont partagées entre les deux réseaux.

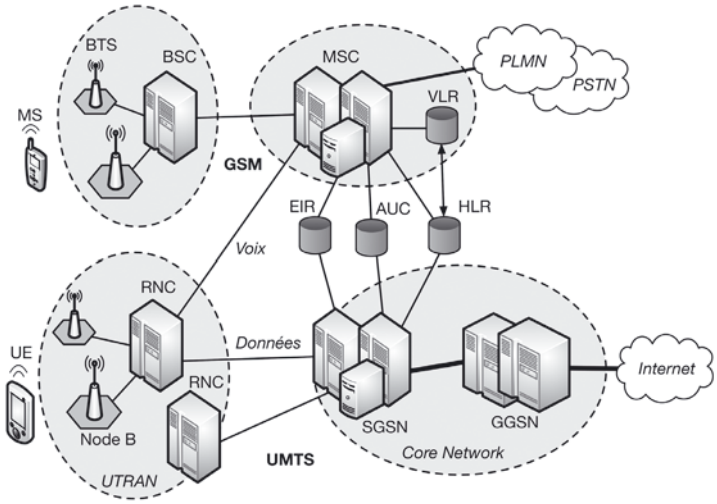


Figure 7.23 – Architecture du réseau UMTS.

c) Protocoles de transmission

Les protocoles de transmission sont regroupés dans les couches 1 et 2 de l'architecture OSI comme le montre la figure 7.24

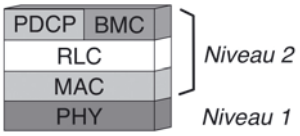


Figure 7.24 – Pile protocolaire de l'UMTS.

Le protocole **BMC** (*Broadcast/Multicast Control Protocol*) est chargé de la gestion de la transmission. Il assure :

- le stockage des messages d'émission cellulaires ;
- le contrôle du trafic et des requêtes radio ;

- la transmission de messages BMC ;
- la livraison des messages vers les couches supérieures.

Le protocole **PDCP** (*Packet Data Convergence Protocol*) est responsable de la transmission des données. Il assure :

- la compression/décompression des paquets IP ;
- la gestion de la numérisation des paquets transmis par le protocole radio RLC.

Le protocole **RLC** (*Radio Link Control*) assure :

- la fragmentation/ré-assemblage des paquets et la retransmission sur erreur (il peut être utilisé conjointement avec les fonctions similaires des protocoles d'autres niveaux, telles que la retransmission TCP au niveau transport ou MAC au niveau liaison) ;
- la gestion des trois modes de transmission :
  - ◇ mode transparent (sans numérotation des messages) pour la voix et la vidéo ;
  - ◇ mode non acquitté (numérotation sans acquittement) pour la voix sur IP ;
  - ◇ mode acquitté (numérotation et acquittement) pour Internet et les messageries.

d) L'accès radio

Les bandes de fréquence allouées pour l'UMTS sont réparties suivant le type de division réalisé entre les voies montantes (UL, *UpLink*) et descendantes (DL, *DownLink*) : division fréquentielle **FDD** (*Frequency Division Duplex*) ou temporelle **TDD** (*Time Division Duplex*), voir figure 7.25.

En France, l'ART a attribué trois porteuses FDD à chaque opérateur ayant acquis une licence 3G. Le FDD est bien adapté aux trafics symétriques et à des environnements extérieurs avec une forte mobilité. Il est donc plutôt réservé au transport de la parole. La technique d'accès multiples utilisée est le W-CDMA (*Wideband Code Division Multiple Access*).

Chaque licence 3G comprend également une porteuse TDD. La division TDD est bien adaptée aux trafics asymétriques et à des environnements intérieurs avec une mobilité restreinte, donc plutôt pour des services orientés multimédias. La technique d'accès multiples utilisée est le TD-CDMA (*Time Division* CDMA).

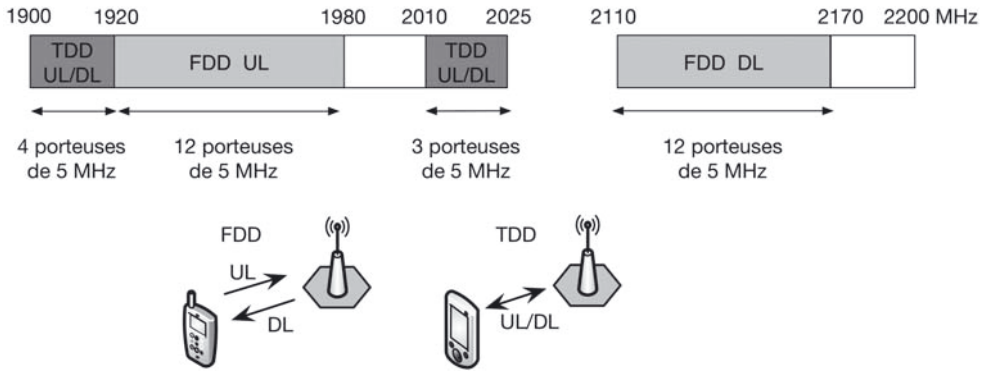


Figure 7.25 – Bandes de fréquence UMTS.

La chaîne de transmission radio simplifiée comporte quatre blocs fonctionnels (figure 7.26) :

- le codage consiste à ajouter de la redondance au train binaire à émettre pour limiter les risques d'erreur ;
- l'entrelacement, comme pour le GSM, consiste à réarranger les paquets de données et à les répartir sur plusieurs trames pour une meilleure protection contre les erreurs de transmission ;
- l'étalement de spectre est effectué par multiplexage CDMA, voir ci-dessous ;
- la modulation est de type QPSK pour la voie descendante et BPSK pour la voie montante.

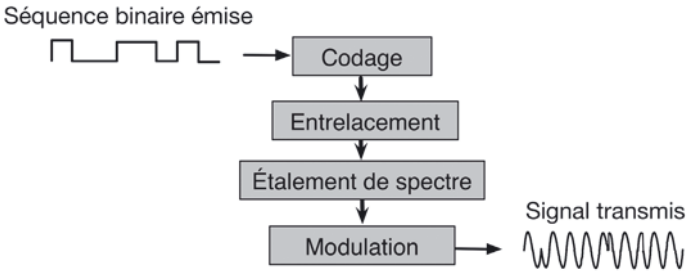


Figure 7.26 – Chaîne simplifiée de transmission radio UMTS.

La technique d'accès multiples pour partager les ressources entre les utilisateurs est de type **CDMA** (*Code Division Multiple Access*). Le principe est de partager une même porteuse en appliquant sur les données de chaque utilisateur un codage différent. Ce codage revient à effectuer un étalement de spectre selon la méthode de répartition par séquence directe (*Direct Sequence*).

Pour un utilisateur donné, une multiplication (OU exclusif) est réalisée entre chaque symbole à transmettre et un code pseudo-aléatoire PN (*Pseudo random Noise code*) propre à cet utilisateur (figure 7.27). Après codage, la séquence constituée des éléments codés (*chips*) est unique pour cet utilisateur et peut être multiplexée sur la même porteuse avec les séquences des autres utilisateurs.

La longueur L du code est appelée facteur d'étalement SF (*Spreading Factor*). Si le débit des symboles est D_s, le débit des éléments codés (*chips*) D_c s'écrit :

$$D_c = D_s \times L$$

L'information résultante est donc étalée sur une bande de fréquence plus large, typiquement 5 MHz contre 200 kHz pour le GSM. L'intérêt de l'étalement étant d'obtenir une meilleure diversité fréquentielle et une sensibilité moindre aux bruits.

À la réception, le signal large bande est multiplié par le même code, ce qui permet de retrouver les données de l'utilisateur au débit initial.

Les codes choisis pour chaque utilisateur doivent présenter une très faible corrélation, ce qui est le cas des codes orthogonaux dits codes OVSF (*Orthogonal Variable*

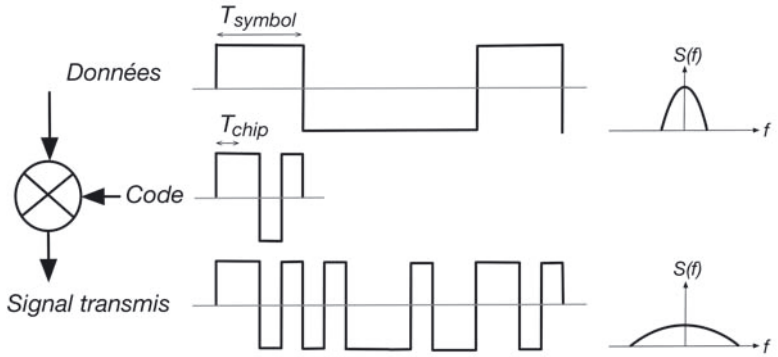


Figure 7.27 – **Principe du codage CDMA.**

Spreading Factor). De plus, ces codes peuvent être de longueur variable, ce qui permet d'avoir plusieurs débits possibles.

e) Évolutions

La technologie **HSDPA** (*High Speed Downlink Packet Access*) considérée comme une évolution de la 3G (3G+ ou 3,5G) permet d'atteindre des débits théoriques jusqu'à 14,4 Mbits/s sur la voie descendante. Contrairement à l'UMTS, HSDPA fait transiter les flux descendants par paquet, en s'appuyant directement sur les mécanismes de la couche IP.

Pour atteindre ces performances, HSDPA exploite essentiellement deux mécanismes supplémentaires :

- un mécanisme de retransmission hybride HARQ (*Hybrid Automatic Repeat Request*) qui permet de limiter et de corriger les erreurs de transmission en agissant sur les couches physique et liaison pour demander rapidement une retransmission ;
- une adaptation dynamique de la modulation et du codage AMC (*Adaptative Modulation and Coding*) en fonction des conditions radio.

7.7.4 La 4G et le LTE

a) Caractéristiques

La technologie **LTE** (*Long Term Evolution*) est utilisée dans la dernière évolution de la 3G, la 3,9G, proche de la 4G avec laquelle elle est souvent confondue. La version évoluée du LTE, le LTE Advanced, est considérée comme une technologie de 4G à part entière.

Le LTE utilise en France plusieurs bandes de fréquences allant de 790 MHz à 2,7 GHz et permettant d'atteindre un débit théorique de 160 Mbit/s en liaison descendante. Les bandes dédiées au LTE sont la bande des 800 MHz et la bande des 2,6 GHz avec des canaux élémentaires de 2 MHz pour la première et des canaux de 5 MHz pour la deuxième. La bande des 1 800 MHZ également utilisée est partagée

avec le GSM. Ces bandes sont partagées par les différents opérateurs. La répartition pour les canaux montant (UL) et descendant (DL) est du type FDD (figure 7.28). Le LTE Advanced offre un débit descendant pouvant atteindre 1 Gbit/s sur les mêmes fréquences mais avec des canaux plus larges.

L'architecture du réseau LTE est proche de celle du réseau UMTS, les principales différences se situent sur les couches physique et liaison :

- multiplexage OFDMA (voir ci-dessous) pour la liaison descendante et SC-FDMA (*Single Carrier FDMA*) pour la liaison montante ;
- utilisation d'antennes multiples MIMO (*Mutiple-Input Multiple-Output*) ;
- codes correcteurs d'erreurs de type « Turbo Code » associés à des algorithmes de retransmission rapides ;
- modulations de type QPSK, 16QAM et 64QAM ;
- temps de latence (RTT) proches de 10 ms (contre 70 à 200 ms en UMTS).

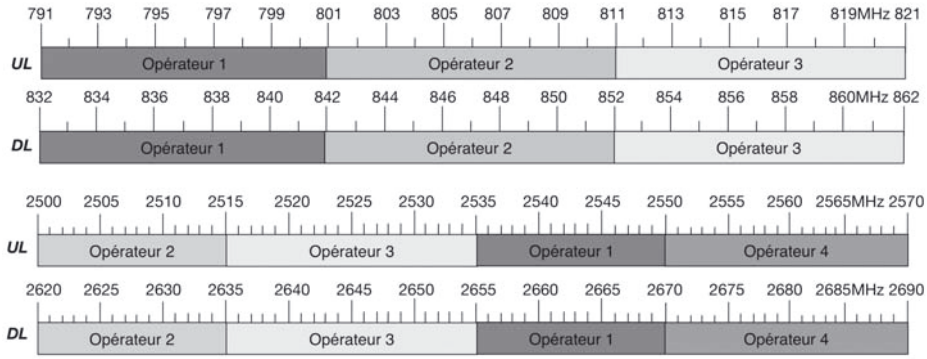


Figure 7.28 – Bandes de fréquence LTE.

b) OFDMA

Le multiplexage OFDMA (*Orthogonal Frequency Division Multiple Access*) rajoute à l'OFDM (voir chapitre 3) un accès multiple pour une exploitation multi-utilisateurs (figure 7.29) :

- la bande est découpée en *N* groupes (*groups*) de P sous-porteuses (*subcarriers*) ;
- un sous-canal (*subchannel*) est un ensemble de sous-porteuses prises dans chaque groupe ;
- un utilisateur se voit attribuer un sous-canal ou plusieurs sous-canaux par intervalle de temps.

Dans le multiplexage OFDM, la totalité des sous-porteuses est attribuée successivement à chaque utilisateur, pour chaque slot de temps dans le cadre d'un multiplexage temporel (figure 7.29). Dans l'OFDMA, un utilisateur peut obtenir, pour chaque slot de temps et de manière dynamique, un nombre variable de sous-canaux en fonction de ses besoins en débit. Le fait que ces sous-canaux soient constitués de

sous-porteuses prises sur l'ensemble de la bande passante permet une meilleure répartition fréquentielle et donc une meilleure immunité face aux interférences.

L'OFDMA peut être donc vu comme une combinaison des multiplexages FDMA (fréquence) et TDMA (temps).

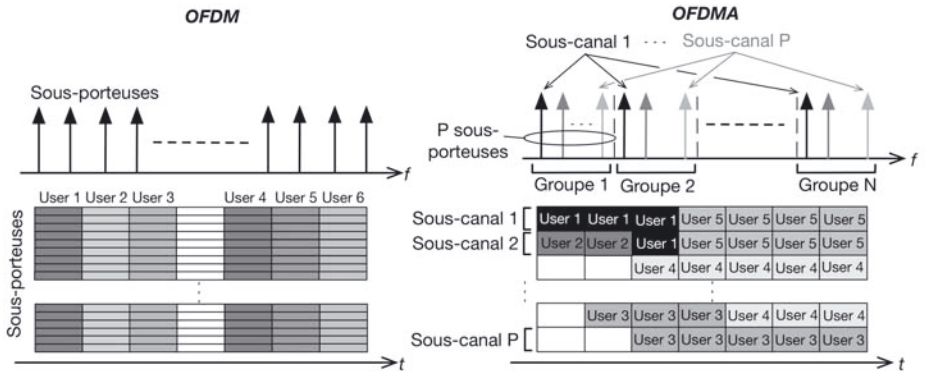


Figure 7.29 – **Principe du multiplexage OFDMA.**

Résumé

- Un réseau de télécommunications est constitué d'un **réseau physique** installé et géré par l'opérateur de câblage et des **services de transport** des informations de l'opérateur de transport.
- Les réseaux d'opérateurs sont des réseaux **commutés** ou des réseaux de **lignes louées**.
- Le **RTC** utilise la commutation de circuit. Il est organisé en **boucle locale** et réseau d'interconnexion. La boucle locale est la partie du réseau entre l'usager et son commutateur de rattachement ou son répartiteur.
- **ATM** est une technique de transmission commutée utilisée dans les réseaux large bande ainsi que sur la boucle locale. Les messages sont découpés en **cellules** de 53 octets, transmises dans des chemins virtuels reliant les commutateurs. Les paramètres définis à l'établissement de la connexion autorisent la Qualité de Service (QoS) de bout en bout.
- La technologie **SDH** (ou SONET aux États-Unis) est utilisée dans les réseaux haut débit comme ATM pour fournir une structure de trame et transporter des cellules ATM ou des paquets IP sur des transmissions séries point à point généralement en fibre optique.
- L'architecture **MPLS** offre une solution pour intégrer plusieurs protocoles de routage et de commutation dans les mêmes équipements intermédiaires, nommés **LSR**, des réseaux d'opérateurs. Un chemin est d'abord tracé grâce à un protocole de routage de niveau 3, les LSR jouent alors le rôle de routeurs. Une

fois le chemin tracé, les LSR fonctionnent comme des commutateurs. Ils lisent les étiquettes (labels) portés dans les en-têtes de paquets et commutent suivant la table de commutation établie lors du tracé du chemin. Les avantages principaux sont l'adaptation à différents protocoles de niveau 2 (ATM, Ethernet…) et la rapidité des commutations lorsque le chemin est établi.

- Les **réseaux cellulaires** proposés au départ pour fournir la téléphonie mobile sans fil aux usagers ont largement évolué pour proposer tous les services de données présents dans l'Internet. Les débits proposés par les générations successives (2G, 2G+, 3G, 3G+, 3,9G, 4G) et les technologies associées (GSM, GPRS, UMTS, HSDPA, LTE) sont passés d'une dizaine de kbit/s et près de 1 Gbit/s en une vingtaine d'années.
- Les améliorations principales se situent au niveau des techniques de codage, de multiplexage et de modulation. Les réseaux de la 4G combinent ainsi le multiplexage OFDMA, l'utilisation d'antennes multiples (MIMO) et des modulations complexes du type 64QAM.

Exercices corrigés

QCM

Q7.1 En cas de dégroupage partiel, quel opérateur gère la partie téléphonie ?

a) Orange b) L'opérateur alternatif

c) L'opérateur de transport

Q7.2 Quelles couches ATM trouve-t-on dans les équipements du réseau ?

a) PMD b) ATM c) AAL

Q7.3 Quelle est la taille des cellules ATM ?

a) 24 octets b) 48 octets c) 53 octets d) 64 octets

Q7.4 À quelles couches OSI correspond la technologie SDH ?

a) Physique b) Liaison c) Transport d) Réseau

Q7.5 À quel(s) niveau(x) intervient l'Ethernet Carrier Grade ?

a) LAN b) Boucle locale c) WAN

Q7.6 Dans un réseau MPLS, un label peut correspondre à :

Une adresse MAC b) Une adresse IP c) Un couple VPI/VCI

Q7.7 Quel équipement est chargé de poser les labels à l'entrée d'un réseau MPLS ?

a) Le LSR b) Le LER

c) Le commutateur ATM d) Le routeur BGP

Q7.8 Pour des flux importants, comment les données sont-elles relayées dans les équipements MPLS ?

a) Routage b) Translation c) Commutation

Q7.9 Dans les réseaux cellulaires, le *handover* désigne un déplacement entre ?

a) Réseaux b) Opérateurs c) Pays d) Cellules

Q7.10 La technologie UMTS permet des débits maximums de quel ordre ?

a) 100 kbit/s b) 1 Mbit/s c) 10 Mbit/s d) 100 Mbit/s

Q7.11 Dans le réseau GSM, à quel type d'équipement correspond la BSC ?

a) L'antenne b) Le mobile

c) Le contrôleur d) Le commutateur

Q7.12 Quel(s) multiplexage(s) est(sont) utilisé(s) dans le réseau UMTS ?

a) CDMA b) TDMA c) FDMA d) OFDMA

Q7.13 Quel(s) multiplexage(s) est(sont) utilisé(s) dans le réseau LTE ?

a) CDMA b) TDMA c) FDMA d) OFDMA

Q7.14 Dans la technologie UMTS et LTE, quels sont les types de répartition pour les voies montantes et descendantes ?

a) Temporelle b) Fréquentielle c) Code orthogonaux

Exercices

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

7.1 (*) Quels équipements sont nécessaires pour faire dégrouper sa ligne ?

7.2 (*) Si la ligne est dégroupée, doit-on continuer à payer un abonnement à Orange ?

7.3 (**) À quoi correspond la boucle locale ? Pourquoi son remplacement est-il stratégique ?

7.4 (**) Quelles sont les fréquences utilisées par des communications de type voix et ADSL sur le RTC ? Pourquoi les distances sont-elles un problème pour des transmissions ADSL et pas pour la voix ?

7.5 (*) Quelle est la taille d'une cellule ATM ? Justifier le fait que la taille soit si petite.

7.6 (***) Soit le réseau MPLS décrit sur la figure ci-dessous. Il comporte 6 nœuds. On suppose que le nœud C est connecté à un réseau de préfixe d'adresse 47.3 et le nœud F à un réseau de préfixe 47.1.

a) Indiquer le rôle de chacun des nœuds.

b) Déterminer le nombre de FEC pour ce réseau.

c) Expliquer comment s'effectue la mise en place d'un LSP pour joindre le réseau de préfixe 47.3.

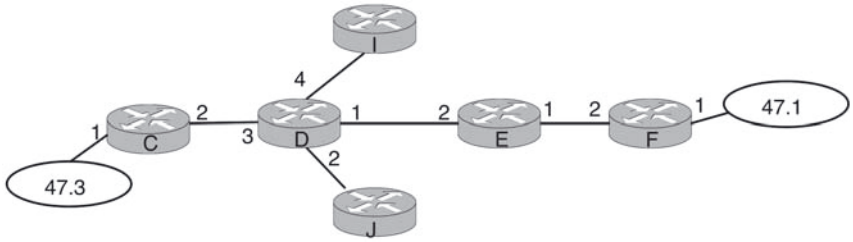


Figure 7.30

7.7 (**)

a) Quelles sont les améliorations principales de la 3G par rapport à la 2G et comment ces améliorations sont-elles rendues possibles ?

b) Même question pour la 4G par rapport à la 3G.

7.8 (***) Une trame LTE dure 10 ms. Elle est découpée en 10 sous-trames de 1 ms. Chaque sous-trame est divisée en deux slots de 0,5 ms. Sept symboles sont transmis dans un slot et un slot correspond à 12 sous-porteuses OFDMA.

a) Quel est le débit de symbole pour un bloc ?

b) Quel est le débit binaire par bloc si une modulation 64QAM est utilisée pour chaque sous-porteuse ?

c) La figure 7.28 donne les bandes attribuées aux opérateurs français pour le LTE. Quels sont les débits maximums possibles dans la bande des 2,6 GHz (débits descendants) pour les différents opérateurs si 25 blocs peuvent être exploités par bande de 5 Mhz ?

d) Quel est finalement le débit que peut obtenir un abonné ?

Solutions

QCM

Q7.1 : a	**Q7.2** : a-b	**Q7.3** : c	**Q7.4** : a-b	**Q7.5** : b-c
Q7.6 : a-c	**Q7.7** : b	**Q7.8** : c	**Q7.9** : a-d	**Q7.10** : b
Q7.11 : c	**Q7.12** : a	**Q7.13** : d	**Q7.14** : a-b	

Exercices

7.1 Les équipements dépendent du service offert par l'opérateur, et non du fait que la ligne soit dégroupée ou non. Par exemple, si une ligne est dégroupée pour un

service ADSL, il faut un modem ADSL et un filtre, si la fonction téléphonique est conservée.

7.2 Tant que la boucle locale est utilisée, Orange est rémunérée pour son entretien. Si la ligne est partiellement dégroupée, cet entretien est payé directement à Orange dans le cadre de l'abonnement de base. Si elle est totalement dégroupée, c'est le nouvel opérateur qui rémunère Orange pour cet entretien.

7.3 La boucle locale est la partie de la ligne téléphonique (paires de cuivre) allant du répartiteur de l'opérateur téléphonique jusqu'à la prise téléphonique de l'abonné. Physiquement, il s'agit de tous les câbles urbains que l'on peut voir dans les rues, des câbles souterrains et même de la paire de fils arrivant chez l'usager.

Son remplacement est stratégique car l'opérateur qui remplacera les équipements actuels en paire de cuivre par de la fibre optique sera rétribué pendant de longues années même s'il n'exploite pas lui-même l'accès.

7.4 La bande passante du RTC, au départ destiné uniquement à la voix, est de 300-3 400 Hz. Pour faire passer des hauts débits (1-20 Mbit/s), ADSL utilise des fréquences beaucoup plus élevées, de l'ordre du mégahertz avec des techniques de modulation évoluées.

Les fréquences élevées sont beaucoup plus sensibles au bruit et aux interférences sur les paires torsadées du RTC.

7.5 La cellule ATM a une taille de 53 octets dont 5 octets d'en-tête. Cette taille est adaptée à la transmission de tout type de données.

7.6

a) Les nœuds C, F, I et J sont situés aux extrémités, ce sont donc des LER. D et E sont des LSR.

b) Deux FEC sont nécessaires pour les deux préfixes d'adresse.

c) Un chemin virtuel est d'abord tracé du routeur F vers le routeur C à partir des adresses de destination 47.3 qui forment une FEC. Les tables de commutation de D et E sont remplies lors de la formation du chemin. Les labels correspondant à la FEC 47.3 sont ensuite posés par le commutateur de bord F sur les paquets venant du réseau 47.1. Ces derniers sont commutés au niveau 2 sur D et E en fonction des labels et des tables pour atteindre le réseau 47.3.

7.7

a) L'amélioration principale est bien sûr le débit qui passe de 100 kbit/s à 2 Mbit/s. On peut citer également : un même réseau d'accès pour la voix et les données, un réseau cœur en IP et un *roaming* à l'échelle mondiale. Ces améliorations s'appuient sur des bandes de fréquence plus élevées, un codage CDMA plus performant et des tailles de cellules plus adaptées.

b) Le débit maximum en 4G passe à 160 Mbit/s (1 Gbit/s en LTE *advanced*). Les bandes de fréquences sont également plus larges et sur des fréquences plus importantes. Le

multiplexage OFDMA, l'utilisation du MIMO et des modulations d'ordre élevé, entre autres, permettent ce gain important en débit.

7.8

a) 7 symboles sont transmis pour 12 sous-porteuses, soit 84 symboles par slot. Un slot dure 0,5 ms, le débit de symbole pour un bloc est donc :

$D_s = 84/0{,}5 \text{ ms} = 168 \text{ ksymboles/s}$

b) Dans une modulation 64QAM, 6 bits sont transmis par symbole ($2^6 = 64$), le débit binaire par bloc est donc :

$D_b = 6\ D_s = 1{,}008 \text{ Mbit/s}$

c) Pour les opérateurs 1 et 2, la bande allouée a une largeur de 15 Mhz, ce qui correspond à 75 blocs (3 × 25) donc 75 blocs. Le débit maximum est donc :

$D_{b\ max} = 75 \times 1{,}008 = 75{,}6 \text{ Mbit/s}$

Les opérateurs 3 et 4 disposent de 100 blocs d'où :

$D_{b\ max} = 100 \times 1{,}008 = 100{,}8 \text{ Mbit/s}$

d) Un abonné de l'opérateur 3 qui disposerait de la totalité des slots dans sa cellule pourrait obtenir, en utilisant seulement la bande des 2,6 GHz, un débit de 100 Mbit/s.

LE RÉSEAU INTERNET 8

PLAN

OBJECTIFS

- ➤ Connaître l'organisation d'Internet, de la périphérie au réseau cœur en passant par le réseau d'accès et ses technologies (ADSL, fibre, accès sans fil).
- ➤ Étudier les principaux services présents sur Internet (DNS, web, mail, FTP, voix et vidéo sur IP).
- ➤ Étudier les protocoles associés à la connexion et aux services.

8.1 PRÉSENTATION

Internet est un ensemble de réseaux interconnectés utilisant tous les mêmes protocoles de routage et de transport TCP/IP. Internet permet d'accéder à des services dont les plus utilisés sont la messagerie (l'e-mail), le transfert de fichier (FTP ou *peer to peer*), les serveurs d'informations en ligne (web) et le streaming ou la VoD (*Video On Demand*).

Dans l'organisation d'Internet, on distingue (figure 8.1) :

- les opérateurs (opérateur de câblage et de transport) ;
- les fournisseurs d'accès Internet (FAI) ;
- les services et les protocoles associés ;
- les outils.

8.2 LES OPÉRATEURS

Les opérateurs de transport qui fournissent à différents niveaux des services pour l'Internet sont appelés de manière générique ISP (*Internet Service Provider*).

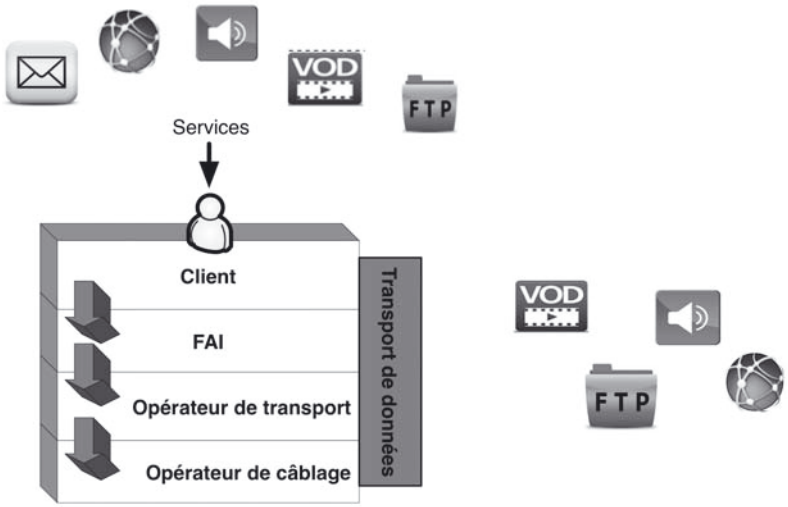


Figure 8.1 – Les acteurs d'Internet.

Ils disposent de leur propre réseau et sont organisés de manière hiérarchique (figure 8.2).

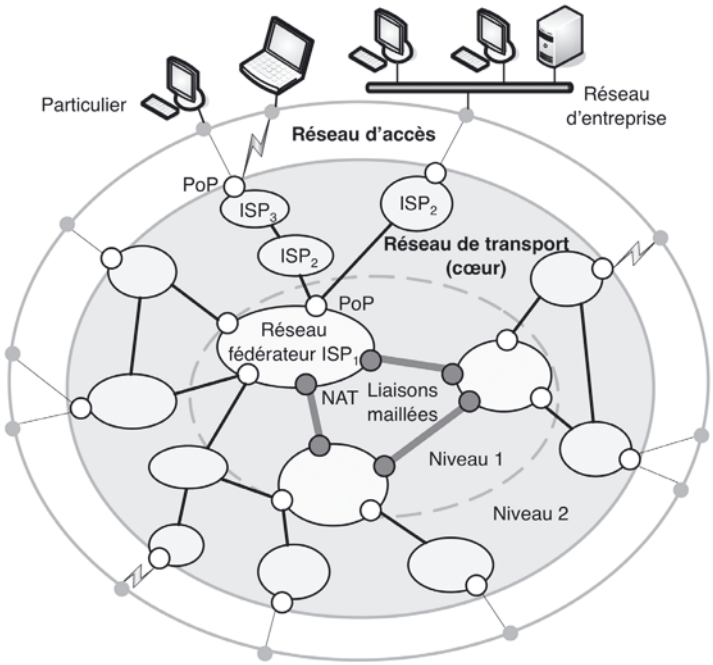


Figure 8.2 – Hiérarchie des opérateurs Internet.

Les réseaux fédérateurs, *backbone* ISP ou **ISP de niveau 1**, sont situés au cœur de l'Internet. Leur couverture est internationale et ils sont reliés directement entre eux par des NAP (*Network Access Point*). Les débits sur les liaisons vont jusqu'à 10 Gbit/s. Exemples aux États-Unis : UUNet, SPRINT, AT&T, QWEST, GEANT.

Les **ISP de niveau 2 ou 3** sont situés à la frontière du réseau d'accès. Ils ont une couverture nationale ou régionale et sont clients des ISP1 auxquels ils sont connectés au niveau des PoP (*Point of Presence*). Certains ISP2 sont également ISP1 et les liaisons sont possibles entre ISP2. Les débits sur les liaisons sont de l'ordre du gigabit par seconde (Gbit/s). Ces ISP de niveau 2 ou 3 sont donc fournisseurs d'accès (FAI) aux entreprises et aux particuliers. Exemples en France : Orange, Free, Bouygues, SFR et Numéricable pour les particuliers ou les entreprises et Renater pour l'enseignement et la recherche.

Au niveau régional et pour éviter de passer systématiquement par le cœur du réseau et les ISP1, les ISP2 ou les ISP3 peuvent échanger du trafic Internet entre leurs réseaux par l'intermédiaire de GIX (*Groupment Internet eXchange*). Un GIX est donc une infrastructure physique qui relie ces réseaux, qui peuvent correspondre à des AS (*Autonomous System*, voir chapitre 6), grâce à des accords mutuels dits de « *peering* »

À titre d'exemple, la figure 8.3 montre l'architecture nationale du réseau de l'opérateur Renater (Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche). Cette architecture appelle deux remarques :

- le réseau national est conçu en boucle pour pouvoir assurer un trafic entre les principales villes universitaires même en cas de rupture d'un des liens ;

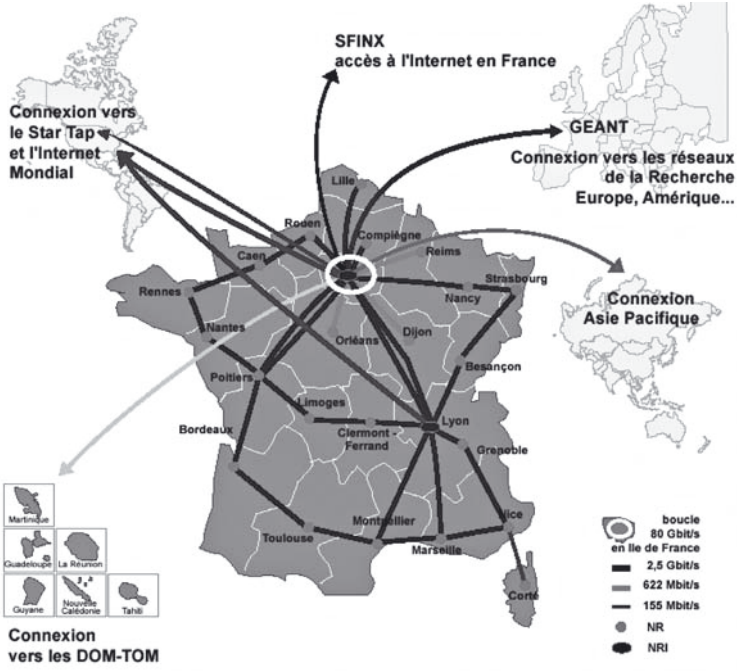


Figure 8.3 – Architecture du réseau Renater.

- tout le trafic international vers les autres réseaux de recherche ou le reste de l'Internet passe par Paris et Lyon. Les équipements de ces deux nœuds internationaux doivent être dimensionnés en conséquence et fiabilisés pour assurer le service de transport des données en tenant compte des pannes possibles.

8.3 Les FAI

Les FAI ou ISP de niveau 3 sont connectés à l'Internet par l'intermédiaire des opérateurs de transport et fournissent :

- des adresses IP aux particuliers ou PME/PMI qui ne peuvent obtenir d'adresse directement auprès de l'ICANN (les adresses ne peuvent être attribuées que par blocs d'adresses, voir chapitre 6) ;
- des services tels que la messagerie, le stockage de fichier ou l'hébergement de pages web ;
- des services de connexion utilisant les réseaux d'opérateurs de télécommunication.

Certains FAI s'intéressent plus au marché des particuliers (Free, Orange…) d'autres à celui des entreprises comme Completel. Certains FAI sont également opérateurs Internet, comme Orange ou Free. Ces FAI maîtrisent le rapport nombre de clients/capacité du réseau.

8.3.1 La gestion des adresses

Le FAI obtient une ou plusieurs classes d'adresse auprès d'un organisme agréé (ICANN). Il gère ces adresses vis-à-vis de ses clients à partir de deux principes :

- un client veut être accessible directement par Internet : le prestataire lui attribuera l'une de ses adresses IP (une adresse IP fixe). Dans ce cas, le client peut être connecté en permanence (connexion type « *full Internet* ») pour héberger, par exemple un serveur web ;
- un client veut accéder à Internet le temps de la consultation d'un serveur (connexion temporaire à la demande type « *dial up* ») : le prestataire « prête » l'une de ses adresses au client, le temps de la consultation. Il utilise pour cela un serveur dynamique d'adresses de type DHCP (voir chapitre 6).

Le prestataire devra donc répartir les N adresses dont il dispose en N1 adresses pour N1 clients du premier type, et N-N1 adresses pour plus de N-N1 clients du deuxième type dont N-N1 maximum connectés simultanément.

8.3.2 Les équipements

Les équipements du FAI sont (figure 8.4) :

- des modems ADSL ou câble, un serveur de connexions pour gérer les accès de ses clients et des équipements pour assurer la sécurité (serveur d'authentification, firewall…) ;
- des routeurs et des équipements de raccordement haut débit de type LS (liaison spécialisée) côté réseau d'opérateurs ;
- différents serveurs pour gérer les services (DNS, DHCP, Web, messagerie…).

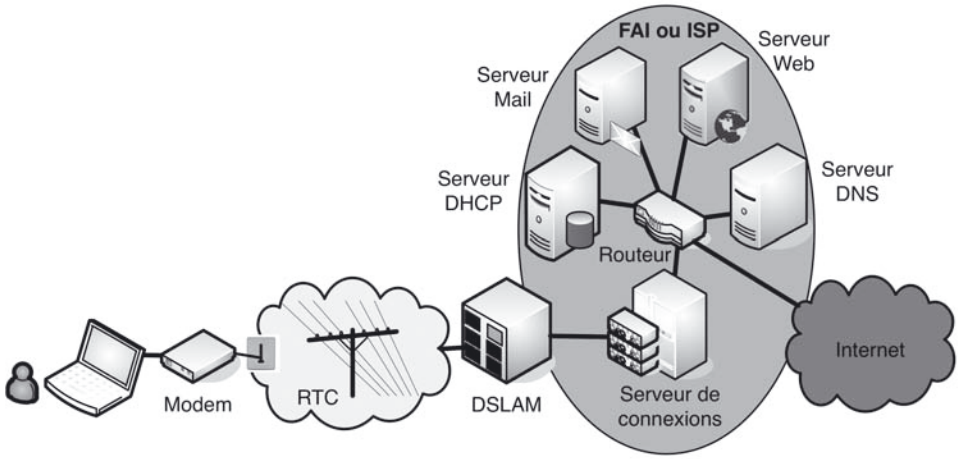


Figure 8.4 – **Équipements d'un FAI.**

8.4 La connexion

Les équipements terminaux situés à la périphérie d'Internet (PC, serveurs, smartphones…) sont reliés au reste de l'Internet par l'intermédiaire du réseau d'accès encore appelé réseau de distribution ou boucle locale. Cette dernière correspond donc à la desserte de l'utilisateur : les derniers mètres ou kilomètres avant d'atteindre le poste client. Différents supports existent pour la réaliser :

- modems xDSL et accès par le RTC en paires métalliques ;
- réseaux câblés (CATV : câble TV et HFC : *Hybrid Fiber/Coaxial*) ;
- fibre optique (FITL : *Fibber In The Loop*) ;
- accès hertziens (WLL : *Wireless Local Loop*) ;
- accès par réseaux cellulaires (3G/UMTS, 3G+, 4G).

8.4.1 L'accès ADSL

Les modems xDSL permettent d'utiliser les paires métalliques du réseau téléphonique pour réaliser une boucle locale haut débit (voir paragraphe 3.4). Le débit dépend fortement de la qualité du câble et de la distance jusqu'au répartiteur. Pour les modems ADSL, le débit descendant peut aller jusqu'à 20 Mbit/s pour des distances inférieures au km (ADSL2+).

8.4.2 L'accès par le câble

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

même câble. La technologie du réseau local à large bande permet de faire coexister ces différents services simultanément.

Le réseau de transport en fibre optique distribue à partir d'une tête de réseau les données ainsi que les signaux TV en numérique jusqu'à un centre local de distribution qui regroupe plusieurs habitations ou immeubles (figure 8.5). Les signaux sont ensuite transportés sur un câble coaxial type TV (CATV) vers chacun des foyers et la connexion est réalisée par un boîtier de raccordement, généralement appelé modem-câble. Ce dernier est spécifiquement dédié aux réseaux de type HFC (*Hybrid Fiber Optic and Coaxial*) qui est une norme pour les réseaux câblés autorisant un flux bidirectionnel. Les débits pour l'Internet peuvent atteindre 100 Mbit/s suivant la qualité des équipements et des liaisons.

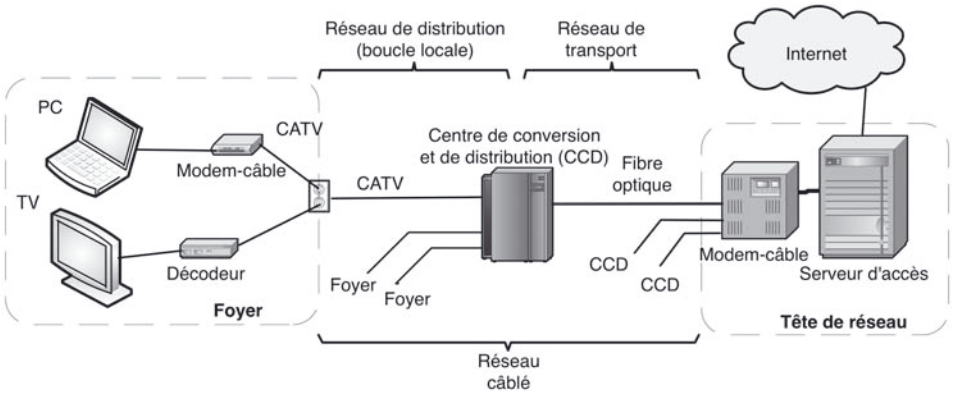


Figure 8.5 – Architecture d'une connexion par câble.

8.4.3 La fibre optique

Cette solution implique de recâbler entièrement le réseau de distribution. Deux stratégies de déploiement sont actuellement en concurrence : PON et FTTH.

Dans le premier cas, la boucle locale optique présente une topologie en arbre passif (PON, *Passive Optical Network*) avec différentes longueurs d'onde pour chaque terminaison (figure 8.6). Il s'agit donc d'une ligne partiellement partagée avec l'avantage d'une infrastructure de câblage plus légère puisqu'elle dessert plusieurs abonnés.

Dans la technologie FTTH (*Fiber To The Home*), la fibre est câblée jusqu'à l'abonné, ce qui permet en théorie un débit plus élevé mais est plus coûteux en câblage.

Dans les deux cas, les débits peuvent être supérieurs à 100 Mbit/s. En France, la technologie PON est déployée par Orange qui possède déjà un réseau important. Elle est très fortement concurrencée par l'opérateur alternatif Free qui a fait le choix de la FTTH.

D'autres solutions intermédiaires existent, notamment la technologie FTTB (*Fiber To The Building*) proposée par SFR-Numéricable pour laquelle le câblage en fibre est réalisé jusqu'à un répartiteur dans l'immeuble, la dernière liaison jusqu'à l'abonné étant assurée en CATV.

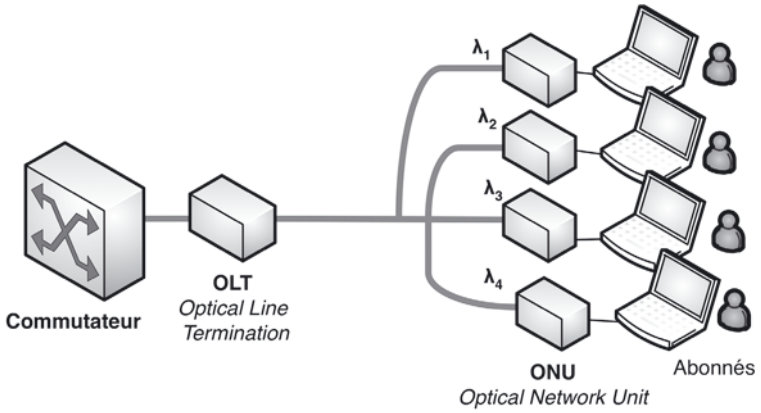


Figure 8.6 – **Technologie PON.**

8.4.4 L'accès sans fil

L'utilisation des technologies sans fil est une solution en devenir pour la boucle locale. Deux orientations sont envisagées suivant la mobilité du client.

L'abonné se déplace d'une cellule à une autre sans interruption de la communication (*handover*). Dans ce cas, le terminal est un smartphone ou une tablette et les technologies de la téléphonie cellulaire (UMTS, HSDPA, LTE) sont adaptées aux hauts débits nécessaires dans les connexions Internet (voir paragraphe 7.7). Pour des raisons essentiellement commerciales, l'accès cellulaire est réservé aux smartphones équipés d'une carte SIM pour l'authentification. L'accès à partir d'un PC est possible à l'aide d'une clé USB intégrant une interface radio-cellulaire et une carte SIM par exemple, mais dans ce cas un nouvel abonnement est nécessaire.

En cas de faible mobilité du client, les technologies des réseaux locaux sans fil et leurs extensions peuvent être utilisées : IEEE 802.11 (WiFi) et IEEE 802.16 (WiMax).

Pour une connexion en WiFi (voir paragraphe 5.8), l'abonné est raccordé à l'extérieur par l'intermédiaire d'un point de concentration fourni par un opérateur (HotSpot SFR, Free…).

Le standard 802.16 (WiMAX, *Worldwide Interoperability for Microwave Access*) permet de son côté d'émettre et de recevoir des données dans les bandes de fréquences radio de 2 à 66 GHz avec un débit maximum théorique de 70 Mbps sur une portée de 50 km (voir paragraphe 3.6). Cette technologie est souvent considérée comme un « ADSL sans fil » et peut être une solution dans des zones rurales où les abonnés sont situés loin des répartiteurs mais son exploitation commerciale reste difficile.

8.5 Les services

8.5.1 Le nommage DNS

a) Principe

Pour simplifier l'identification des machines, un service de résolution permettant d'utiliser des noms symboliques à la place des adresses IP est utilisé localement ou à l'échelle mondiale. Rappelons que, pour circuler sur Internet, un paquet IP doit contenir l'adresse IP de destination et non le nom associé. Lorsque nous saisissons par exemple sur la barre d'adresse d'un navigateur le nom d'un serveur web, il faut donc interroger ce service de résolution pour récupérer l'adresse IP qui correspond au nom symbolique saisi.

À l'échelle mondiale, la méthode consiste à centraliser la gestion des noms sur des machines spécifiques (les serveurs de noms) à l'aide d'un service permettant une organisation hiérarchisée : le **DNS** (*Domain Name Service*). Ce service de nom de domaine travaille suivant une organisation arborescente en divisant le réseau global en un ensemble de domaines primaires, secondaires…

L'autorité de nommage de l'Internet est l'ICANN (*Internet Corporation for Assigned Names and Numbers*). Chaque zone a son responsable de nommage ; en France, c'est l'AFNIC (Association française pour le nommage Internet en coopération). Cet organisme gère donc une base de données relative à la zone *.fr* et c'est ainsi pour tous les autres organismes.

La figure 8.7 présente un extrait de ce nommage hiérarchique. Dans cette structure arborescente sont définis les domaines de premier niveau (appelés TLD, *Top Level Domains*), rattachés au nœud racine représenté par un point. Sont définis ensuite les domaines de deuxième niveau (SLD), de troisième niveau…

Les TLD génériques (gTLD) sont définis au même niveau de l'arborescence que les TLD correspondant à un pays (ccTLD pour *country code*TLD), ce qui peut poser problème lorsque l'on veut définir une activité commerciale en France par exemple.

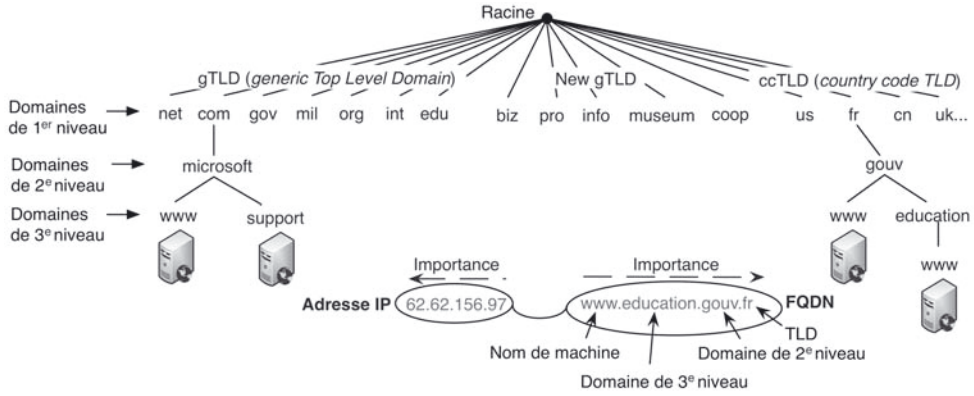


Figure 8.7 – Organisation arborescente du nommage DNS.

Il serait plus judicieux dans ce cas d'utiliser un nom du type *entreprise.com.fr*, le gTLD *com* serait alors passé au deuxième niveau et le nom de l'entreprise au troisième niveau.

Un nom complet d'hôte ou FQDN (*Fully Qualified Domaine Name*) est constitué des domaines successifs séparés par un point. Contrairement aux adresses IP pour lesquelles l'identifiant de la machine est situé sur la partie droite, les noms DNS présentent le nom de la machine à gauche suivi des noms de domaines d'importance croissante (figure 8.7).

b) Résolution DNS

En haut de l'arborescence, il y a officiellement 13 serveurs de noms racine (de a.root-servers.net à m.root-servers.net) qui connaissent les serveurs de nom de premier niveau (.com, .fr…). Ces serveurs sont dupliqués et répartis dans le monde (plus de 300 serveurs physiques).

Pour les niveaux suivants, chaque serveur de noms gère une ou plusieurs zones du réseau. Chacune des zones possède au moins un serveur de noms ayant la connaissance complète des adresses des machines de la zone. Chaque serveur de noms connaît également l'adresse d'au moins un autre serveur de noms de la zone supérieure.

Côté client, chaque machine possède au moins l'adresse d'un serveur DNS (serveur primaire) et éventuellement l'adresse d'un second (serveur secondaire) en cas de panne du premier. Lorsqu'une application (navigateur, client FTP, client mail…) a besoin de résoudre un nom symbolique en une adresse réseau, elle envoie une requête au résolveur local (processus sur la machine client) qui la transmet au serveur de noms de la zone locale, c'est-à-dire le serveur primaire déclaré (voir exemple de la figure 8.8). Si le nom est local (phases 1-2-3 de la figure 8.8) ou si la correspondance est déjà mémorisée dans sa mémoire cache (phases a-b-c de la figure 8.8), le serveur primaire qui fait autorité sur la zone renvoie directement l'adresse IP demandée.

Si le nom ne peut être résolu localement (zone distante ou nom absent du cache), le serveur primaire transmet à un serveur distant ayant autorité sur le domaine de

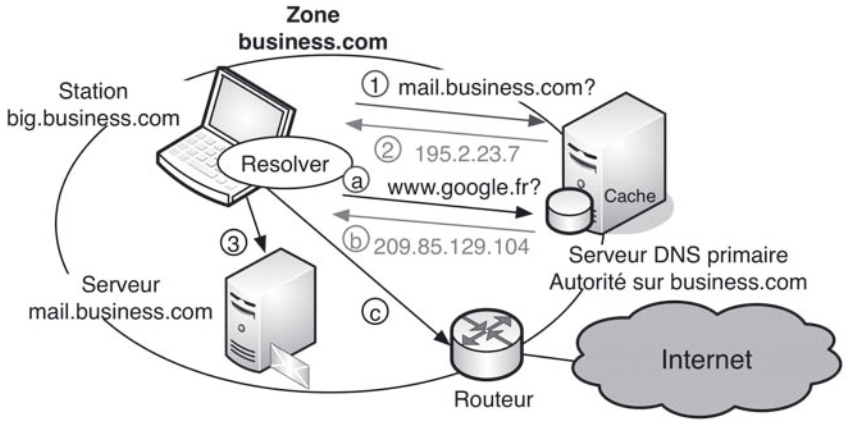


Figure 8.8 – Exemple de résolution DNS locale.

premier niveau concerné (figure 8.9). Le serveur choisi qui a la connaissance complète des adresses des machines de sa zone relaie la requête vers le serveur DNS de deuxième niveau. La requête est ensuite relayée jusqu'à atteindre le serveur DNS ayant autorité sur la zone demandée. L'adresse IP de la machine est alors renvoyée. Si le serveur primaire ne connaît pas l'adresse du serveur ayant autorité sur le domaine de premier niveau, il doit au préalable interroger un serveur racine. Les serveurs racine connaissent au moins les serveurs de noms pouvant résoudre le premier niveau (.fr, .com, .net…). Si les serveurs racine ne sont pas opérationnels, plus de communications sur l'Internet !

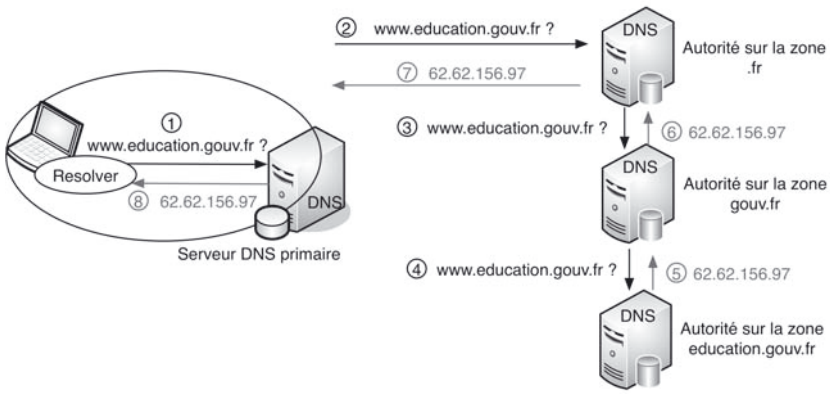


Figure 8.9 – Exemple de résolution DNS récursive.

Le protocole DNS autorise également l'usage de recherches itératives. Lorsqu'un serveur DNS n'est pas en mesure de relayer la requête de manière récursive, il transmet au serveur primaire l'adresse du prochain serveur. Dans l'exemple décrit figure 8.10, les deux premières requêtes sont de type itératif : c'est le serveur primaire qui est chargé de répéter les requêtes lorsqu'il a connaissance de l'adresse du serveur suivant. Dans la plupart des cas, le serveur de nom de premier niveau, fortement sollicité, ne relaye pas les requêtes de manière récursive. Seule la requête vers le serveur de nom de premier niveau est itérative, les autres sont récursives (cas de la figure 8.10). Les serveurs racine également ne sont jamais récursifs. Les DNS proposés par les FAI sont toujours récursifs : ils savent répondre à n'importe quelle requête et ils font généralement autorité pour le domaine du FAI.

c) Enregistrements DNS

La base de données des serveurs de noms est constituée « d'enregistrements de ressources » ou « *Ressource Records* » (RR). Il était prévu initialement que ces enregistrements soient répartis en différentes classes suivant le réseau utilisé. Finalement, la seule classe d'enregistrement utilisée est la classe Internet (IN). À chaque nom de domaine est donc associé un enregistrement RR. Il existe plusieurs types de RR (voir exemple figure 8.11) :

- A : *Address*, correspondance entre le nom et l'adresse IP (le plus usuel) ;
- NS : *Name Server*, serveur(s) de nom pour ce domaine ;

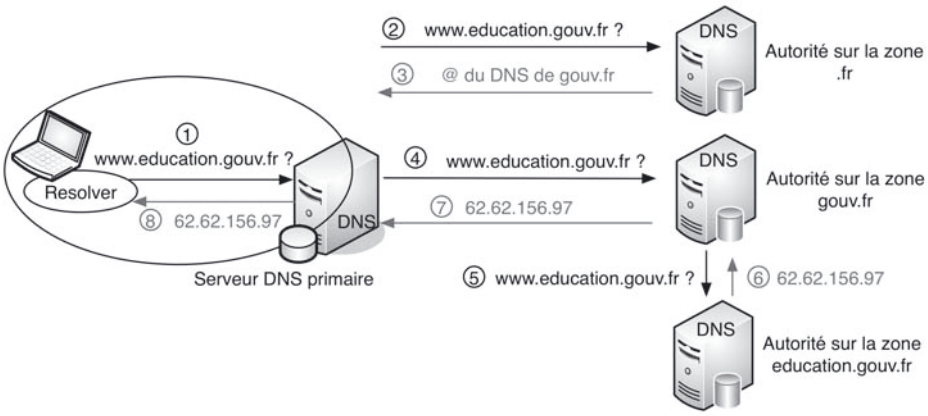


Figure 8.10 – Exemple de résolution DNS itérative et récursive.

- CNAME : *Canonical NAME*, nom d'origine (des alias peuvent exister) ;
- SOA : *Start Of Authority*, serveur(s) faisant autorité sur la zone ;
- PTR : *PoinTeR*, correspondance entre l'adresse IP et le nom (résolution inverse) ;
- MX : *Mail eXchange*, indique le serveur de messagerie.

FQDN (nom de domaine)	TTL	Type	Classe	Rdata
www.education.gouv.fr	3600	A	IN	62.62.156.97

Figure 8.11 – Exemple de RR.

Pour transporter les enregistrements stockés sur les serveurs DNS, le protocole associé utilise le même format de message pour les demandes et les réponses (figure 8.12).

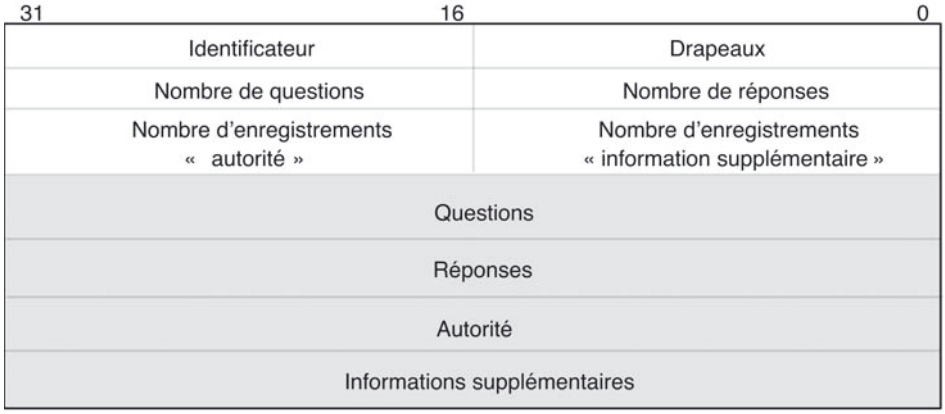


Figure 8.12 – Format général des messages DNS.

- le champ « identificateur » est une valeur donnée par le client et renvoyée par le serveur qui permet de faire correspondre les réponses aux demandes ;
- les drapeaux (*flags*) donnent des indications supplémentaires sur le message (demande ou réponse, demande standard ou inverse, erreur de nom, récursivité disponible…) ;
- les 4 valeurs suivantes de 16 bits précisent le nombre d'enregistrements RR dans les 4 champs de longueur variable qui terminent le message ;
- les champs « questions » et « réponses » précisent le type et le contenu de la demande ou de la réponse (résolution IP, nom demandé, adresse retournée…) ;
- les champs « autorité » et « informations supplémentaires » donnent éventuellement dans une réponse des indications sur les serveurs DNS ayant participé à la résolution.

Les figures 8.13 et 8.14 montrent un exemple de dialogue DNS relevé à l'aide d'un analyseur de protocoles. Les messages DNS sont encapsulés dans des segments UDP dans la mesure où la fiabilité sur une connexion établie n'est pas nécessaire : une requête ayant échoué peut être retentée aussitôt. Le port UDP associé porte le numéro 53. Pour la demande, seul le champ « question » (*Queries*) comporte un enregistrement, il contient le nom correspondant à l'adresse IP demandée pour un RR de type A. Le message de réponse comporte les quatre champs avec un enregistrement pour le champ « question » et deux enregistrements pour chacun des trois autres champs. L'adresse IP demandée est donnée dans le deuxième enregistrement de réponse (*Answers*). La première réponse donne le nom canonique (RR de type CNAME) même si celui-ci n'était pas demandé. Nous remarquons que www.education.gouv.fr est un alias et que le nom canonique, « le vrai nom », est très différent. Les deux derniers champs donnent respectivement les noms des serveurs faisant autorité sur la zone concernée (RR de type NS) et les adresses IP de ces serveurs (RR de type A). Les RFC 1034, 1035 et les amendements qui ont suivi (RFC 2181) décrivent complètement l'organisation des domaines et le protocole associé.

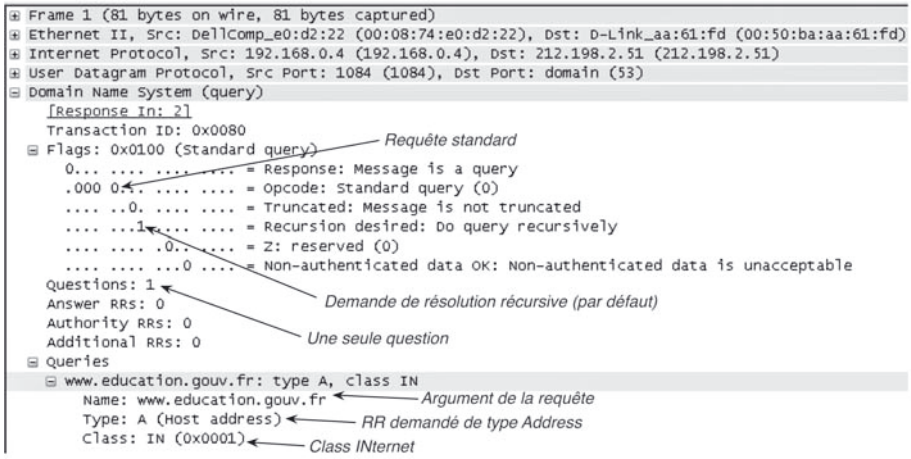


Figure 8.13 – Exemple de message de demande de résolution DNS.

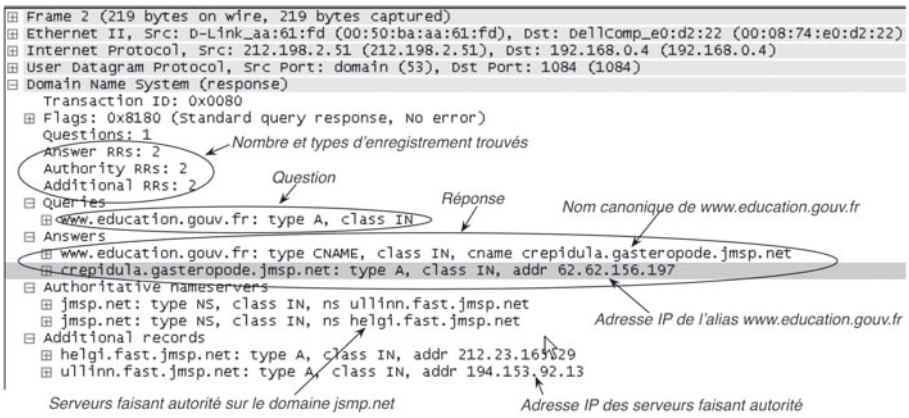


Figure 8.14 – Exemple de message de réponse DNS.

8.5.2 Service web

Le service web permet d'accéder à des documents au format HTML (*Hyper Text Markup Language*) en utilisant pour la connexion et les échanges le protocole **HTTP** (*Hyper Text Transfer Protocol*) qui est un protocole de communication entre le navigateur du client et les serveurs web, basé sur le principe des liens hypertextes (voir § 8.6.2). Ces liens qui apparaissent dans le navigateur sous forme de mots ou d'images surlignés ou de couleur différente contiennent la localisation de la ressource à laquelle le navigateur va se connecter en cas d'activation.

L'**URL** (*Uniform Ressource Locator*) est le nom donné à la localisation de la ressource (« l'adresse web ») correspondant à l'hyperlien. L'URL comporte au minimum le nom de la machine qui contient la ressource (serveur http, serveur ftp, répertoire local…) et éventuellement le chemin d'accès à la ressource et le nom de celle-ci. La syntaxe générale est la suivante (les parties entre crochets sont optionnelles) :

```
protocol://[user:password@]host[:port][/path][/document]
```

- `user` : nom d'utilisateur utilisé par certains protocoles (FTP…)
- `password` : mot de passe pour user
- `host` : nom complet d'hôte FQDN (www.education.gouv.fr)
- `port` : identifie la connexion sur le serveur suivant le protocole (80 pour HTTP)
- `path` : chemin pour accéder à la ressource (/répertoire/sous-répertoire)
- `document` : nom du fichier ressource (index.html, video.mpeg…)

Exemple d'URL :

http://www.babaorum.armor.fr
ftp://ftp.laudanum.fr
http://server/directory/file.htm
file :///c :/temp/fichier.txt
mailto:asterix@babaorum.fr

8.5.3 Service de messagerie

Plus connu sous le nom d'e-mail (*electronic mail* ou courrier électronique), ce service permet d'échanger des messages et des fichiers (figure 8.15). Il nécessite :

- pour l'expéditeur et le destinataire, un client de messagerie et un logiciel client ou MUA (*Mail User Agent*, ex. : *Outlook, Thunderbird*…) ;
- un serveur de messagerie expéditeur et un logiciel serveur pour le transfert ou MTA (*Mail Transfert Agent,* ex. : *Sendmail, Postfix, Exchange*…) ;
- un serveur de messagerie destinataire intégrant une boîte aux lettres (BAL) pour chaque client, un MTA pour le transfert entre serveurs et un logiciel serveur pour la délivrance des messages ou MDA (*Mail Delivery Agent,* ex. : *Sendmail, Postfix, Exchange*…) ;
- des protocoles d'échange (SMTP, POP3, IMAP…).

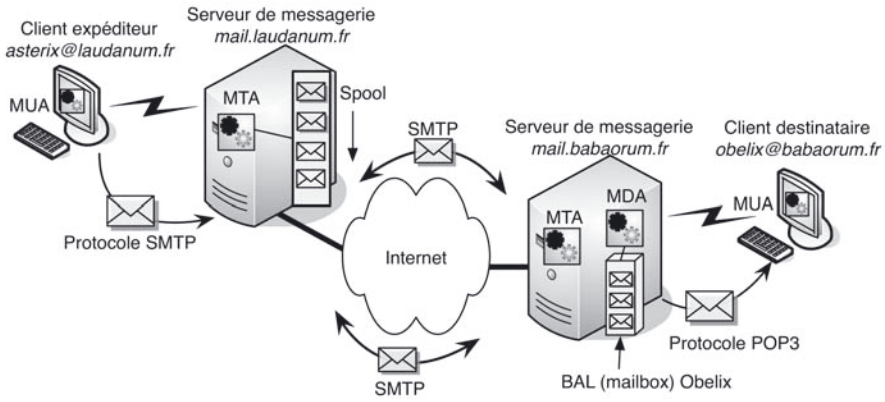


Figure 8.15 – Service e-mail simple.

Un message est envoyé à l'aide du logiciel MUA situé sur le client expéditeur. Il est reçu par l'intermédiaire du MTA sur le serveur local du client et stocké dans une file d'attente (*spool*) avec tous les autres messages des autres expéditeurs du domaine. Le MTA du serveur d'expédition transfère ensuite le message stocké vers le serveur de messagerie correspondant au domaine du destinataire. La file d'attente du serveur expéditeur est ainsi traitée avec une politique du type FIFO (*First In First Out*), le temps d'attente pour un message donné est donc fonction du volume de messages qui transitent sur le serveur de messagerie du domaine.

Le MTA destinataire vérifie ensuite que le destinataire de l'e-mail existe bien pour le nom de domaine qu'il a en charge. Il s'appuie pour cela sur une base de données contenant tous les comptes mail existant. Si le destinataire n'existe pas, le MTA renvoie un message d'erreur à l'émetteur du mail.

Si l'adresse de destination est reconnue dans le domaine, le message atterrit finalement dans la boîte aux lettres du destinataire en attente de lecture grâce au MDA du serveur de destination (figure 8.15). Le message peut rester stocké sur le serveur

et être lu à distance (fonctionnement en mode *online*) ou être déplacé vers la station du client et effacé du serveur (mode *offline*).

Pour le courrier sortant, c'est-à-dire pour expédier un message de MUA vers MTA ou pour échanger les messages entre deux serveurs de messagerie (MTA vers MTA), le protocole SMTP (*Simple Mail Transfer Protocol*) est utilisé, voir § 8.6.3.

Pour le courrier entrant, c'est-à-dire pour récupérer et lire leur courrier (MDA vers MUA), les stations utilisent soit le protocole POP (*Post Office Protocol),* voir § 8.6.4, qui est orienté vers un fonctionnement en mode *offline* et permet notamment de vérifier l'identité du client voulant lire le courrier d'une boîte aux lettres, soit le protocole IMAP (*Internet Mail Access Protocol*) destiné à la lecture interactive des messages *via* une interface web, voir § 8.6.5.

Les serveurs **webmail** offrent le même service d'e-mail et permettent aux utilisateurs d'accéder à leurs boîtes à lettres à partir de n'importe quel navigateur Internet. Le cœur du serveur webmail est un module logiciel d'interfaçage entre les serveurs SMTP/IMAP et le navigateur du client. Ce logiciel, souvent écrit en PHP, code les messages en HTML et JavaScript, afin de les rendre compatibles avec les langages interprétés par les navigateurs. La figure 8.16 montre le principe de fonctionnement d'un module webmail.

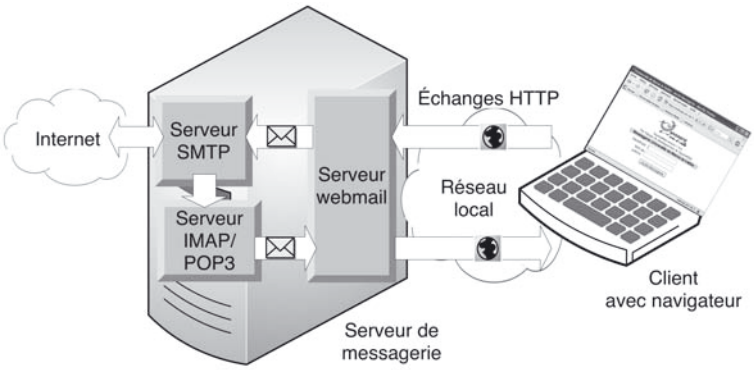


Figure 8.16 – Principe d'un serveur webmail.

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

Les **listes de diffusion** (*mailing lists*) permettent d'envoyer un même courrier à plusieurs personnes en utilisant une adresse commune de liste. Les destinataires doivent être abonnés à la liste, celle-ci est gérée par un serveur de liste qui comprend les commandes d'abonnement, de désabonnement, de consultation d'archives…

Les **forums** permettent également de regrouper des abonnés intéressés par un même sujet. Contrairement aux listes de diffusion pour lesquelles un seul courrier est envoyé vers plusieurs destinataires, les messages des forums sont stockés sur un serveur et consultés ou enrichis lorsque l'utilisateur le souhaite. Les discussions sont donc archivées, ce qui permet une communication asynchrone, à la différence de la messagerie instantanée. La plupart des forums sont aujourd'hui à base d'interface web.

Les espaces de **messagerie instantanée** ou ***chat*** sont des sortes de forum où chaque utilisateur peut dialoguer à tout moment avec tous les contacts qu'il a référencés au préalable, si ceux-ci sont en ligne. Les utilisateurs peuvent se connecter ou se déconnecter à loisir, discuter à plusieurs, s'échanger des fichiers… L'avantage principal est la grande simplicité d'utilisation : il suffit d'un compte e-mail. L'un des inconvénients est la difficulté de gérer les interventions multiples et inappropriées lorsque la liste de contacts est grande. Les dernières versions intègrent des fonctionnalités étendues comme la vidéoconférence et la téléphonie.

8.5.4 Service de transfert de fichiers

a) FTP client/serveur

Ce service permet à un client de télécharger des fichiers depuis ou vers un serveur de fichiers. Il est plutôt réservé aux transferts de fichiers volumineux qui ne peuvent être transmis simplement sous forme de pièce jointe à un courrier électronique (les serveurs SMTP refusent généralement les fichiers attachés d'une taille supérieure à quelques dizaines de Mo). La connexion et le dialogue entre la station du client et le serveur utilisent le protocole FTP (*File Transfer Protocol*), voir § 8.6.6.

Après établissement de la connexion, le serveur demande une authentification au client (nom et mot de passe). Si l'authentification réussit, le client peut commander le téléchargement dans un sens ou dans l'autre de fichiers ou de répertoires.

Les logiciels sur la station du client disposent des commandes permettant de se déplacer dans l'arborescence du serveur, de définir le type des données transférées (binaire ou ASCII) et de télécharger un fichier.

b) Transfert *peer to peer*

Les logiciels de transfert « *Peer to Peer* » ou **P2P** (d'égal à égal) n'utilisent pas de serveur unique et centralisé. Lorsqu'un client veut télécharger un fichier donné, il commence par interroger un annuaire de localisation de contenu situé sur une ou plusieurs machines. Cet annuaire lui permet de localiser les utilisateurs, les *Peers*, possédant la totalité ou une partie du fichier. Le client se connecte et le téléchargement est effectué à partir de sources multiples décentralisées : les blocs du fichier sont téléchargés simultanément ou séquentiellement à partir des différents clients identifiés (figure 8.17). Le client fait alors partie du réseau, il devient à son tour un *Peer* et peut mettre à disposition des autres les fichiers présents sur sa machine ainsi que les blocs du fichier en cours de téléchargement, multipliant ainsi les sources.

Le logiciel utilisé est donc un programme complet, capable de se connecter aux annuaires, d'identifier les clients possédant la ressource, d'effectuer les téléchargements à différents débits et avec un contrôle d'erreur et au final de reconstituer le fichier dans son intégralité à partir des différents blocs téléchargés.

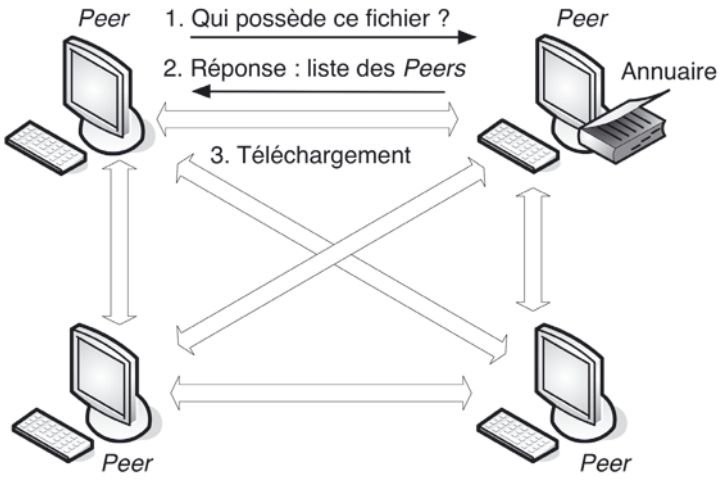


Figure 8.17 – Principe des transferts P2P.

L'intérêt principal de ce type de transfert est le temps réduit de téléchargement obtenu en multipliant les sources par rapport à une application avec un seul serveur devant servir successivement tous les clients. La difficulté du système réside dans l'indexation des fichiers : « *qui possède à un instant donné quelle partie du fichier ?* » et dans la recherche d'un équilibre sur le réseau et d'une équité entre les *Peers* : « *un client qui ne partage rien doit-il télécharger aussi rapidement qu'un autre ?* ».

Dans les applications P2P, les annuaires peuvent être :

- centralisés sur des serveurs (*Napster*) ;
- partiellement décentralisés sur les postes (*Kazaa, Emule, edonkey*) ;
- décentralisés (*Gnutella, BitTorrent*).

8.5.5 Voix et vidéo sur IP

a) Voix sur IP

La voix sur réseau IP ou **VoIP** (*Voice over Internet Protocol*) est une technique qui permet de communiquer par la voix *via* l'Internet ou tout autre réseau acceptant le protocole TCP/IP. Cette technologie est notamment utilisée pour supporter le service de téléphonie IP (**ToIP**, *Telephony over Internet Protocol*). Toutes les solutions de téléphonie sur IP commencent par convertir la voix en paquets de données numériques. Les paquets de voix sont ensuite transmis sur Internet de la même manière que les autres types de trafic (web, mail, FTP…).

La voix est une information bien particulière qui nécessite une certaine qualité de service. En ce qui concerne le débit, pour numériser et transporter la voix avec une qualité standard, il faut disposer d'un canal de 64 kbit/s (8 000 échantillons/s codés sur 8 bits).

La qualité de service est également liée au délai de transmission ou temps de latence. Ce délai comprend le codage, le passage en file d'attente d'émission, la propagation dans le réseau, le traitement en file d'attente à la réception et le décodage. D'après la norme ITU G114, ce temps de latence doit être inférieur à 300 ms pour une qualité acceptable.

Le phénomène d'écho est également important (il est souvent perçu en téléphonie cellulaire). C'est le délai entre l'émission du signal et la réception de ce même signal en réverbération. Celle-ci est causée par les composants électroniques des parties analogiques. Un écho inférieur à 50 ms n'est pas perceptible. Plus il est décalé dans le temps, plus il est insupportable.

Parmi les avantages de la ToIP, nous pouvons citer :

- la réduction des coûts de communication (les ressources sont partagées avec d'autres applications) ;
- un seul réseau à maintenir en service (par exemple dans le cas d'une offre « *triple play* » pour un particulier) ;
- les options pointues et gratuites (transfert, messagerie…).

Les terminaux utilisés sont la plupart du temps des téléphones connectés à des boîtiers chargés de convertir la voix analogique en paquet IP (type Box ADSL). Dans un contexte d'entreprise, il peut s'agir de téléphones directement connectés au réseau IP (*IP Phone*) vers un commutateur du type PBX numérique (figure 8.18). Une autre solution est l'utilisation, à partir d'un PC, d'un logiciel de téléphonie sur IP (*soft phone),* type *Skype.*

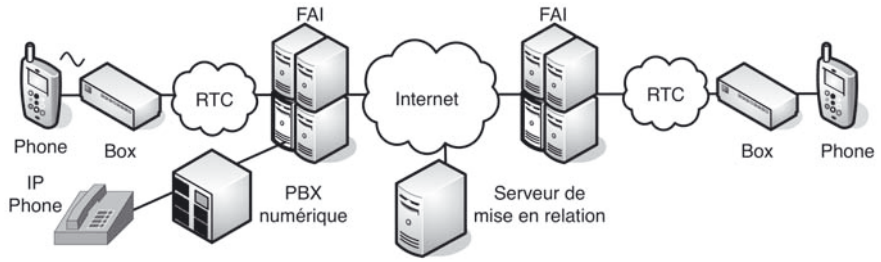


Figure 8.18 – ToIP avec téléphone analogique ou IP Phone.

b) Vidéo sur IP

La **vidéo sur IP** permet également le développement d'autres services audiovisuels de plus en plus présents sur Internet tels que la vidéo à la demande (VoD), la vidéoconférence ou encore la TV numérique.

Les services de vidéo à la demande utilisent des serveurs de téléchargement de vidéo ou des serveurs de streaming lorsque le flux vidéo est transmis en continu, sans stockage préalable. Dans ce dernier cas, le client commence par tester les performances de la ligne. En fonction du débit mesuré, il précisera dans une première requête la version du fichier vidéo, la qualité étant inversement proportionnelle à la taille. Toujours en fonction du débit mesuré, un tampon permettant de stocker temporairement une partie de la vidéo est créé. Ce tampon permettra d'assurer une lecture continue en cas de baisse ponctuelle du débit sur le réseau (figure 8.19).

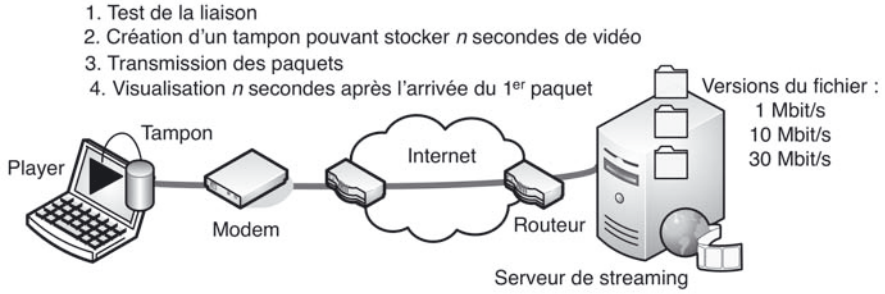


Figure 8.19 – Principe du Streaming.

Dans le cas de la vidéoconférence où les communications sont interactives, les délais de transmission doivent être limités et les débits de transmission doivent s'adapter à ceux des réseaux empruntés (ADSL, réseaux câblés, liaisons spécialisées…).

Notons que pour ces différents services de téléphonie ou de vidéo, Internet n'est pas approprié au transport des informations « temps réel », c'est-à-dire pour lesquelles un délai minimum entre l'émission et la réception doit être respecté. Des protocoles de transport adaptés comme RTP et RTCP devront donc assurer les exigences temporelles que demandent ces applications multimédias (voir § 8.6.7).

8.6 Les protocoles

8.6.1 PPP

Dans le cadre d'une connexion point à point par modem à l'Internet, il est nécessaire d'utiliser une procédure capable de transporter les datagrammes IP sur une liaison série. Le premier protocole conçu dans ce but est SLIP (*Serial Line Internet Protocol*) ; **PPP** (*Point to Point Protocol*) ajoute l'authentification et la détection d'erreurs en liaison avec d'autres protocoles de contrôle.

Par extension, PPP a été implémenté sur des couches liaison ou réseau comme Ethernet (*PPP over Ethernet*) ou ATM (*PPP over ATM*). Quel que soit le support utilisé « en dessous » (Ethernet, ATM…), une liaison PPP transportera les mêmes données « au-dessus » (figure 8.20) : un paquet IP, qui lui-même encapsulera un segment TCP ou UDP, qui lui-même intégrera des messages HTTP, SMTP, POP3, FTP…

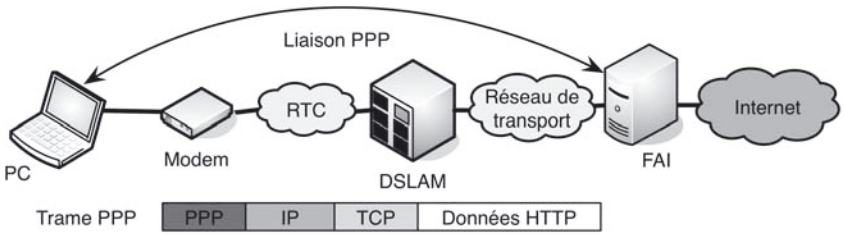


Figure 8.20 – Liaison PPP et trame PPP.

Pour une connexion de type ADSL, des protocoles supplémentaires seront nécessaires pour adapter PPP au réseau traversé (figure 8.21) :

- PPPoE (*PPP over Ethernet*) permet d'adapter PPP pour le réseau local Ethernet du client ou de son FAI ;
- PPPoA (*PPP over ATM*) pour adapter PPP au réseau de transport ATM (*Asynchronous Transfert Mode*) ;
- PPTP (*Point to Point Tunneling Protocol*) pour créer un tunnel VPN (*Virtual Private Network*) sécurisé entre deux clients distants (voir chapitre 9 sur la sécurité).

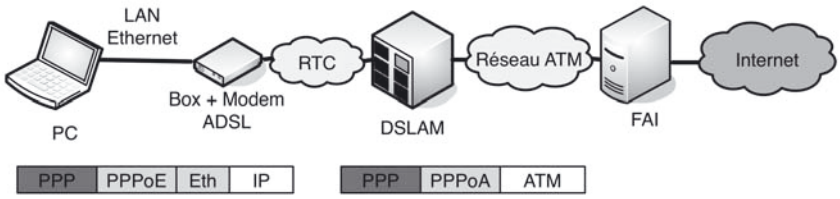


Figure 8.21 – Différentes encapsulations PPP.

Le protocole PPP fonctionne en plusieurs étapes : après contrôle de la liaison (activation de la ligne, test et négociation des options) et authentification de l'abonné, les paquets IP sont découpés et encapsulés dans des trames au format PPP. Pour réaliser ces différentes étapes, PPP apporte quatre éléments :

- une méthode pour encapsuler les datagrammes IP, donc pour délimiter de façon non ambiguë la fin d'une trame et le début de la suivante ;
- un protocole de contrôle de liaison (LCP, *Link Control Protocol*) qui active la ligne, la teste, négocie les options et la désactive ;
- un protocole d'authentification, généralement CHAP (*Challenge Handshake Authentication Protocol*), voir § 9.5 ;
- la possibilité de négocier les options de la couche réseau indépendamment du protocole associé ; la méthode choisie consiste à avoir un protocole intermédiaire de contrôle de réseau (NCP, *Network Control Protocol*) différent pour chaque couche réseau supportée.

8.6.2 HTTP

a) Principe

Lorsque le navigateur du client veut accéder à une ressource vers un serveur, l'adresse IP correspondant au nom indiqué dans l'URL est récupérée grâce au protocole DNS. Une connexion TCP vers le serveur est ensuite établie sur le port 80 par défaut. Pour utiliser un port non standard, il faut le préciser dans l'URL (ex. : http://www.babaorum.armor.fr:1224). Une fois la connexion TCP établie, le navigateur envoie sa demande de ressource par l'intermédiaire du protocole HTTP. La requête contient la méthode à utiliser pour récupérer la ressource (GET par exemple), l'URL de la ressource demandée et la version du protocole HTTP invoqué (figure 8.22). Le protocole HTTP communique ses informations au format texte afin de ne pas être gêné par les différences d'implémentation des jeux de caractères d'une plate-forme à l'autre.

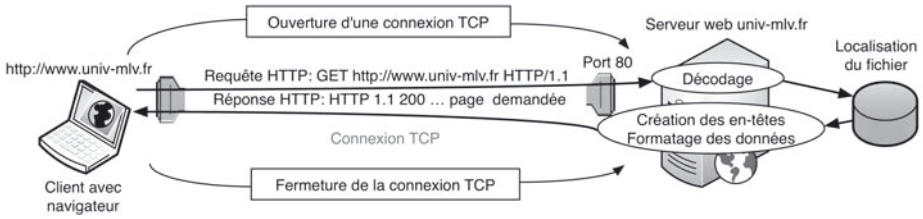


Figure 8.22 – Ouverture d'une connexion TCP et requête HTTP.

Dans les premières versions du protocole HTTP (jusqu'à la version 1.0), la connexion TCP n'était pas persistante, cela signifiait qu'à chaque nouvelle demande de ressource, même si celle-ci se trouvait sur le même serveur, la connexion précédente était fermée et une nouvelle connexion devait être établie. À partir de la version 1.1, si le serveur l'autorise, les connexions sont persistantes par défaut. Cela permet d'enchaîner les requêtes au sein d'une même connexion entre le client et le serveur (*pipeline*), de limiter ainsi les délais de latence dus aux ouvertures multiples de connexion et de permettre de reporter des erreurs HTTP sans pénaliser le client par une fermeture de la connexion.

Par ailleurs, lorsque la ressource demandée contient des éléments dynamiques (résultat de calcul, animations…), d'autres outils seront utilisés : des langages spécifiques côté serveur (PHP, ASP…) ou côté client (applets Java, JavaScript…) et des logiciels capables d'afficher ces éléments dynamiques en liaison avec le navigateur utilisé sur le client (animations Flash, audio ou vidéo Real Player…).

b) Requêtes et réponse HTTP

Quelle que soit la méthode invoquée, la syntaxe d'une requête HTTP a le même format de base composé de trois parties :

```
Méthode URL Version
En-tête : valeur
En-tête : valeur
…
Corps de la requête
```

La première ligne correspond à la requête et comprend trois éléments séparés par un espace : la méthode (GET, HEAD, POST…), l'URL et la version du protocole utilisée par le client (actuellement *HTTP/1.1*).

Les différents en-têtes HTTP sont un ensemble de lignes facultatives qui permettent de donner des informations supplémentaires sur la requête et/ou le client (navigateur, OS…). Pour HTTP 1.1, l'URL est passé dans le champ d'en-tête « *Host* » qui devient obligatoire.

Le corps de la requête contient les données HTTP ; c'est un ensemble de lignes optionnelles devant être séparé des lignes précédentes par une ligne vide et utilisé par exemple pour un envoi de données par la méthode POST lors de l'utilisation de formulaires.

La figure 8.23 représente une trame relevée au moment d'une requête HTTP de type GET. L'analyse au niveau 7 montre la méthode utilisée, (*Host*) et un certain nombre de paramètres supplémentaires dans l'en-tête.

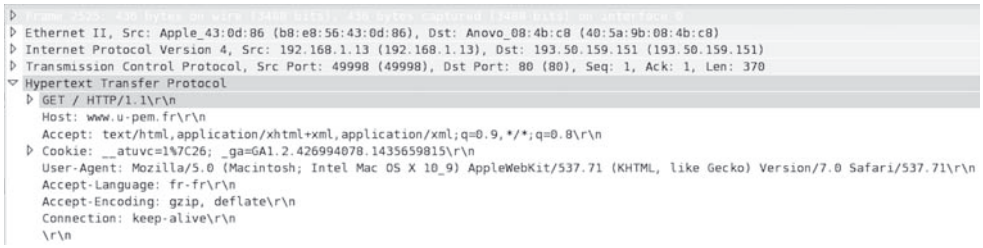


Figure 8.23 – Exemple de requête HTTP.

La réponse est également constituée de trois parties :

```
Version Code de réponse
En-tête : valeur
En-tête : valeur
…
Corps de la réponse
```

Dans la première ligne, le code de réponse suivi d'une chaîne de caractères décrit le résultat. Un code commençant par 2 indique le bon déroulement de la transaction (200 *OK* pour un acquittement, 204 *NO RESPONSE* lorsqu'il n'y a pas d'information à renvoyer…). Un code commençant par 3 signifie une redirection : la ressource n'est plus à l'emplacement demandé, ce qui est fréquent sur Internet (310 *MOVED* lorsque les données demandées ont été transférées à une nouvelle adresse…). Un code commençant par 4 signifie une erreur due au client. La plus fréquente est l'erreur 404 *NOT FOUND* ; elle signifie que la ressource recherchée a changé d'adresse ou de nom, ou bien qu'elle a été supprimée. Enfin un code commençant par 5 indique une erreur due au serveur, ce qui est plus rare (503 *SERVICE UNAVAILABLE* indique que le serveur est pour l'instant incapable de répondre, le client doit réessayer plus tard).

Comme pour la requête, les champs d'en-tête HTTP forment un ensemble de lignes facultatives permettant de donner des informations supplémentaires sur la réponse (type du serveur, version du codage MIME…)

La dernière partie correspond au corps de la réponse et contient les données HTTP, la page web demandée, généralement au format HTML.

La figure 8.24 représente une trame relevée au moment d'une réponse HTTP. De nombreuses options dans l'en-tête permettent de savoir notamment si la page a été récemment modifiée ou le type de contenu (texte, image, vidéo…). Les données ne sont pas représentées sur cette capture.

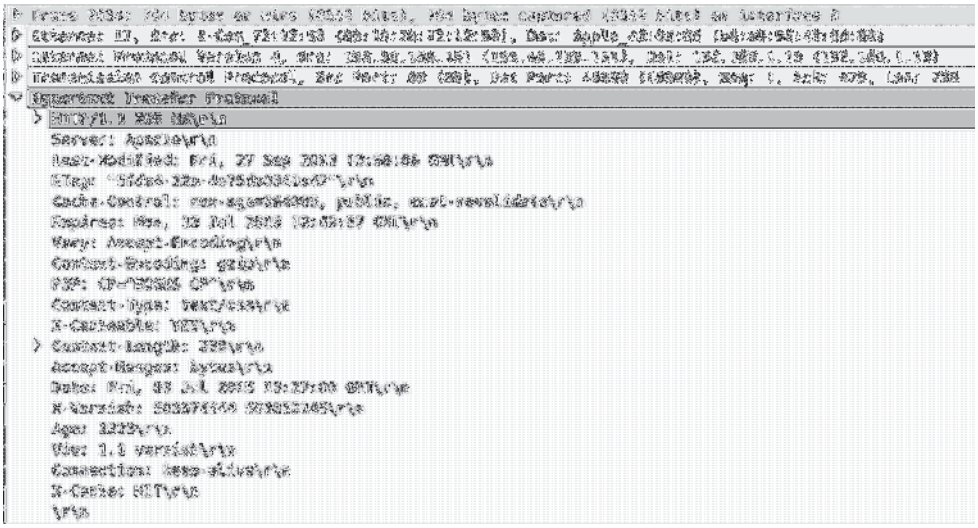


Figure 8.24 – **Exemple de réponse HTTP.**

8.6.3 SMTP

SMTP (*Simple Mail Transport Protocol*) est le protocole courant de gestion du courrier électronique sur Internet. Il est complètement décrit dans la RFC 2821. C'est un protocole point à point dans la mesure où il met en communication deux serveurs de messagerie : celui de la personne qui envoie un courrier et celui de la personne qui le reçoit. Initialement, ce protocole simple était destiné au transfert de messages pour des machines connectées en permanence (fonctionnement *on-line*). Les serveurs SMTP sont chargés du stockage dans une file d'attente et du transport du courrier, ils doivent acheminer régulièrement les messages stockés vers les destinations mentionnées dans les champs adresse (figure 8.15).

Dans la mesure où SMTP est conçu au départ pour des systèmes reliés en permanence, un utilisateur connecté de façon intermittente (*Dial-up*) *via* le RTC utilisera SMTP pour expédier son courrier sur son serveur de messagerie (courrier sortant), et un protocole tel POP3 ou IMAP pour lire les courriers qui l'attendent sur le serveur (courrier entrant).

Le protocole SMTP spécifie :

- le format des adresses des utilisateurs suivant une notation Internet classique faisant figurer le nom de l'utilisateur suivi du nom de domaine (asterix@babaorum.fr) ;
- les champs des en-têtes de courrier (*from*, *to, cc, bcc*…) ;
- les possibilités d'envoi groupé :
- la gestion des heures ;
- le codage utilisé pour le message et les fichiers joints :
  - ◇ texte pur codé en ASCII 7 (RFC 822) ou 8 bits pour une prise en compte des caractères accentués ;
  - ◇ standard MIME (*Multipurpose Internet Mail Extension*) pour du texte formaté, des images ou du son.

Le protocole SMTP n'est pas sécurisé, il n'y a pas d'authentification des correspondants ni de chiffrement des données. Il faut ajouter par exemple un protocole de niveau transport comme SSL pour assurer cette sécurité (voir chapitre 9).

Une fois formatés, les messages sont envoyés en utilisant les commandes SMTP :

- commandes d'envoi constituées de quatre lettres ;
- commandes de réponse du serveur constituées d'un code sur trois chiffres suivi d'un message texte (un premier chiffre à 1, 2 ou 3 signifie une réussite ; une valeur 4 ou 5 un échec).

La figure 8.25 donne un exemple d'échange SMTP avec les trois phases classiques de dialogue :

- établissement de la connexion au niveau SMTP et identification de la source et de la destination ;
- envoi du message avec les différents en-têtes RFC 822 et RFC 1521 ;
- libération de la connexion.

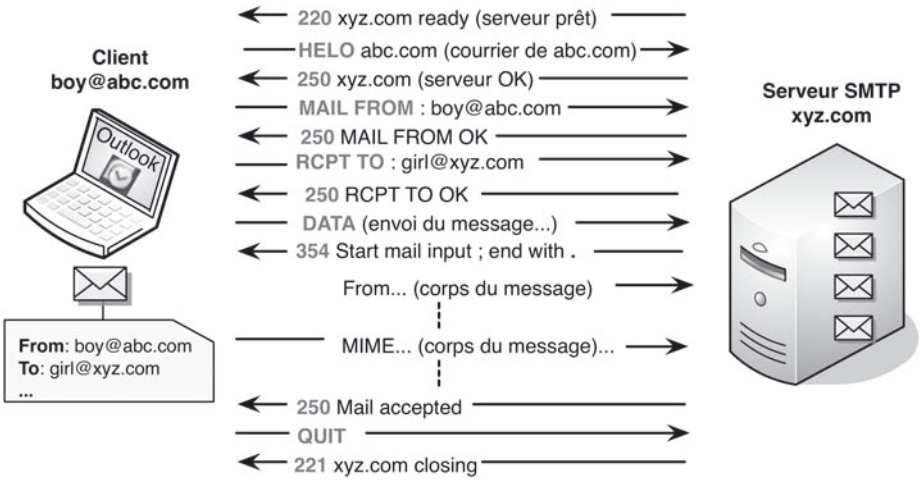


Figure 8.25 – **Exemple de dialogue SMTP.**

La figure 8.26 montre une analyse SMTP au moment où le message est transmis au serveur avec les différents en-têtes et le corps du message (DATA) suivant les formats RFC 822 et RFC 1521. Dans l'exemple, le message est de type texte, sans fichier attaché. Le sous-type « *plain* » indique qu'il s'agit de texte brut, sans formatage HTML ou autre.

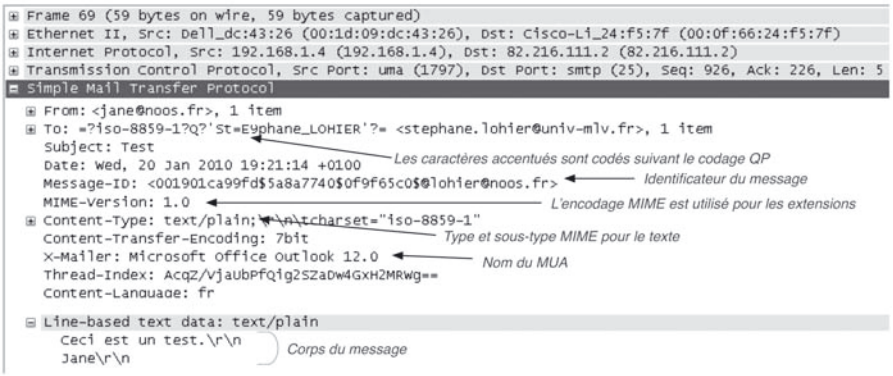


Figure 8.26 – Le client transmet le message.

8.6.4 POP3

Après vérification de l'adresse de destination et transfert par le MDA du message de la file d'attente vers la BAL concernée (figure 8.15), le client de messagerie ou MUA peut venir relever son courrier en utilisant le protocole POP3 (*Post Office Protocol version 3*). Ce dernier est complètement décrit dans la RFC 1939. Le protocole POP qui, comme son nom l'indique, a été conçu pour récupérer le courrier sur une machine distante pour un utilisateur non connecté en permanence, gère :

- l'authentification, c'est-à-dire la vérification du nom et du mot de passe ;
- la réception, suite à une requête, des courriers et fichiers attachés à partir du serveur de messagerie ;
- la réception de messages d'erreur ou d'acquittement.

L'envoi de messages n'est pas supporté par le protocole POP3 de base. Il n'est pas sécurisé au niveau de l'authentification et du transfert des messages. Comme pour SMTP, un autre protocole comme SSL doit être utilisé pour sécuriser la phase d'authentification et chiffrer les données.

Les commandes POP3 (RFC 1939) reprennent la syntaxe sur quatre lettres de SMTP. Les réponses du serveur, transmises sous forme d'une chaîne de caractères, sont de deux types : +OK et –ERR suivi d'un texte.

La figure 8.27 montre un exemple d'échange POP3. La première trame correspond à la réponse (+OK) à une demande de connexion TCP au serveur POP3, le protocole POP3 utilise le port TCP 110 par défaut. Le client POP3 s'identifie ensuite au serveur, ce dernier demande un mot de passe au client qui le lui transmet sous forme non cryptée sur le réseau. Après acceptation, le client peut relever le courrier

choisi à l'aide de la commande RETR. Il faut noter que les messages lus ne sont pas effacés par défaut du serveur : c'est le logiciel client de messagerie qui doit être configuré pour laisser ou effacer grâce à la commande DELE les messages relevés.

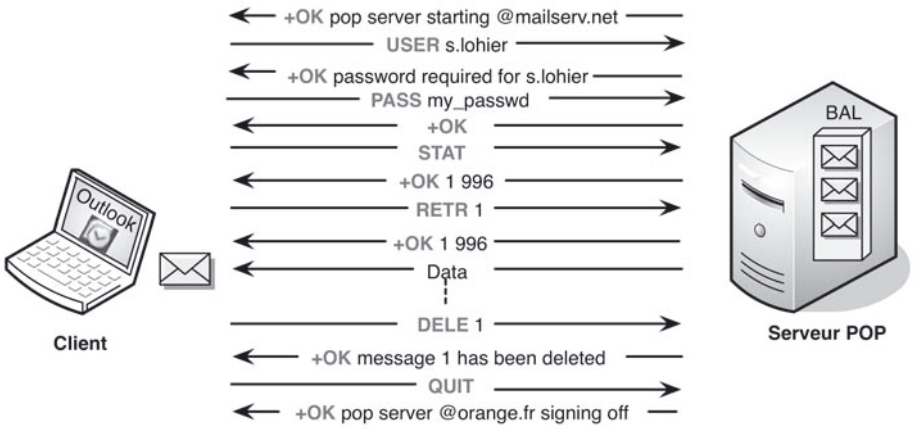


Figure 8.27 – **Exemple de dialogue POP3.**

La figure 8.28 montre un exemple d'analyse POP3 lors d'une capture de trames. Il s'agit de la phase de lecture du courrier, après authentification et sélection du message. Les premiers en-têtes permettent de connaître la succession des serveurs de messagerie traversés, plusieurs champs « *received* » peuvent figurer lors de relais successifs. Les dates correspondant aux différents serveurs permettent de connaître le délai d'acheminement du message qui dépend bien entendu de l'instant choisi par le destinataire pour aller relever son courrier. On retrouve ensuite les en-têtes ajoutés par le serveur d'expédition et le corps du message.

8.6.5 IMAP

Contrairement au protocole POP, le protocole **IMAP** (*Internet Mail Access Protocol*), RFC 3501, est conçu essentiellement pour lire le courrier « en ligne ». Il permet également la manipulation à distance sur les messages. Parmi les principales fonctionnalités d'IMAP, on peut noter :

- lecture des objets des messages seulement (sans le corps) ;
- lecture des messages en les laissant sur le serveur ;
- effacement des messages sans les avoir lus ;
- marquage des messages sur le serveur (non lus, récents…) ;
- création de dossiers sur le serveur ;
- déplacement de messages sur le serveur d'un dossier à l'autre.

De par sa nature interactive, le protocole IMAP est très souvent utilisé par l'intermédiaire d'un webmail.

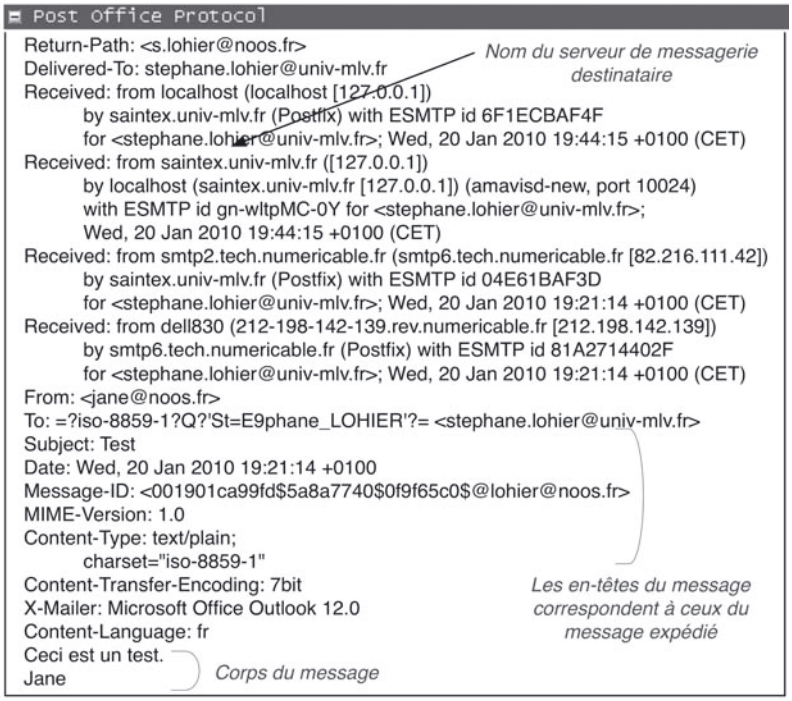


Figure 8.28 – Exemple d'analyse POP3.

Parmi ses avantages, nous pouvons noter une gestion simplifiée de la messagerie en cas de mobilité de l'utilisateur (gestion des dossiers et des messages sur le serveur) et la facilité de changer de client de messagerie (aucun message à transférer). IMAP présente cependant quelques inconvénients comme la nécessité de gérer son espace disque du serveur et une certaine lenteur due à l'aspect interactif.

La figure 8.29 montre un exemple d'enchaînement des différentes phases d'authentification et de transfert. Le protocole IMAP4 utilise le port TCP 143 par défaut pour ouvrir la connexion. Après authentification, le client sélectionne la boîte de réception (INBOX). Le serveur répond en envoyant des informations sur le contenu de la boîte sélectionnée :

- la liste des indicateurs (*FLAGS*) possibles sur les messages (message lu, réponse envoyée, message marqué…) ;
- le nombre de messages dans la boîte (*6 EXIST*) ;
- le nombre de messages récents (*1 RECENT*)…

Le client demande ensuite la lecture des indicateurs pour tous les messages : *FETCH 1 :* (FLAGS).* La commande est précédée de « *UID* » pour demander l'utilisation d'un index simple plutôt qu'un numéro de séquence. Le client demande finalement la lecture complète du message 6 (FETCH 6).

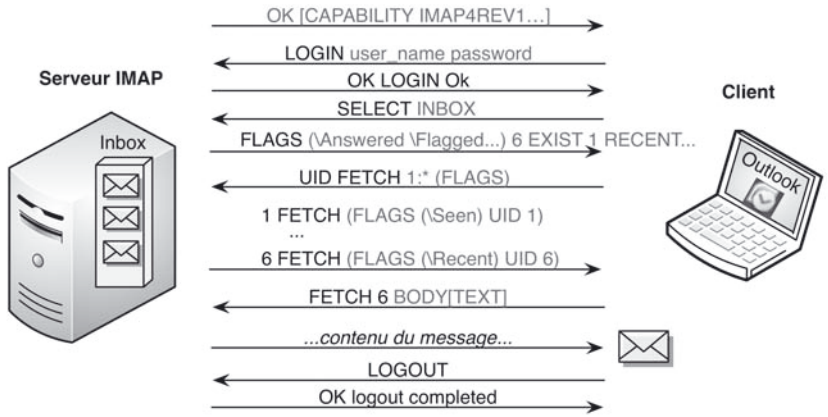


Figure 8.29 – **Exemple de dialogue IMAP.**

8.6.6 FTP

Le protocole **FTP** (*File Transfer Protocol*) permet le transfert de fichiers et de répertoires entre un serveur et un client sur un réseau IP. Sa particularité est de fonctionner avec deux canaux TCP (figure 8.30) :

- le port TCP 21 est toujours utilisé pour le canal de commande ;
- le port TCP 20 par défaut est utilisé pour le canal de données.

Le premier canal permet l'envoi de commandes vers le serveur ou de messages d'erreur vers le client, y compris pendant le transfert de fichier, ce qui autorise par exemple une interruption en cas de blocs de fichier corrompus avant la fin de la transmission.

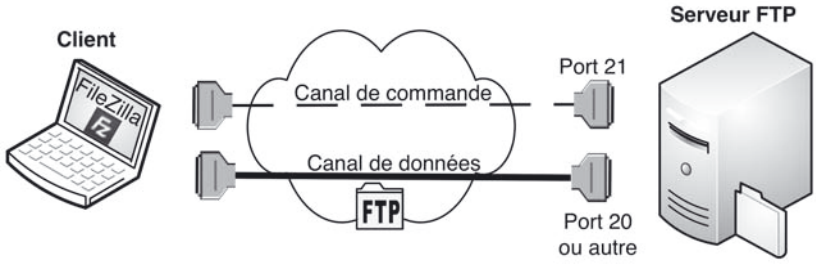


Figure 8.30 – **Organisation d'une connexion FTP.**

L'authentification qui suit la connexion peut être réalisée de deux façons :

- en anonyme pour un accès limité aux répertoires publics ;
- en non anonyme pour un accès associé à des permissions sur des fichiers ou des répertoires particuliers.

Suite à l'authentification, les commandes de l'utilisateur (user, password, dir, get…) utilisées sur le logiciel client sont traduites en commandes internes FTP

(USER, PASS, LIST, RETR…), suivies éventuellement d'arguments (nom d'utilisateur, nom de répertoire) ou de données correspondant au fichier transféré. Les réponses du serveur sont transmises sous forme de codes de retour à trois chiffres éventuellement suivis d'un message ASCII.

L'ensemble de ces commandes et des codes de réponse est donné dans la RFC 454. La figure 8.31 présente un exemple d'enchaînement de commandes et de réponses FTP. Les lignes grisées sont rajoutées par le logiciel client pour donner des indications sur l'état du dialogue en cours. Après la phase d'authentification, le logiciel client envoie une commande *PWD* pour connaître le répertoire en cours et son contenu. À partir de ce répertoire de base, il est possible de se déplacer (*CWD*). Avant de lancer un téléchargement par la commande *RETR* (ou *STOR* dans l'autre sens), il est nécessaire de préciser par la commande *TYPE* que le téléchargement se fera en mode binaire (le mode ASCII est réservé aux fichiers texte) et de demander par la commande *PASV* l'ouverture en mode passif du canal des données. Dans l'exemple, le serveur répond à la commande *PASV* avec les 6 valeurs 192,168,1,3,4,1, ce qui signifie que le client peut ouvrir une connexion TCP vers le serveur d'adresse IP **192.168.1.3** et sur le port **4** × 256 + **1** = 1 025. Le serveur propose donc pour éviter les écoutes clandestines un port différent du port standard 20.

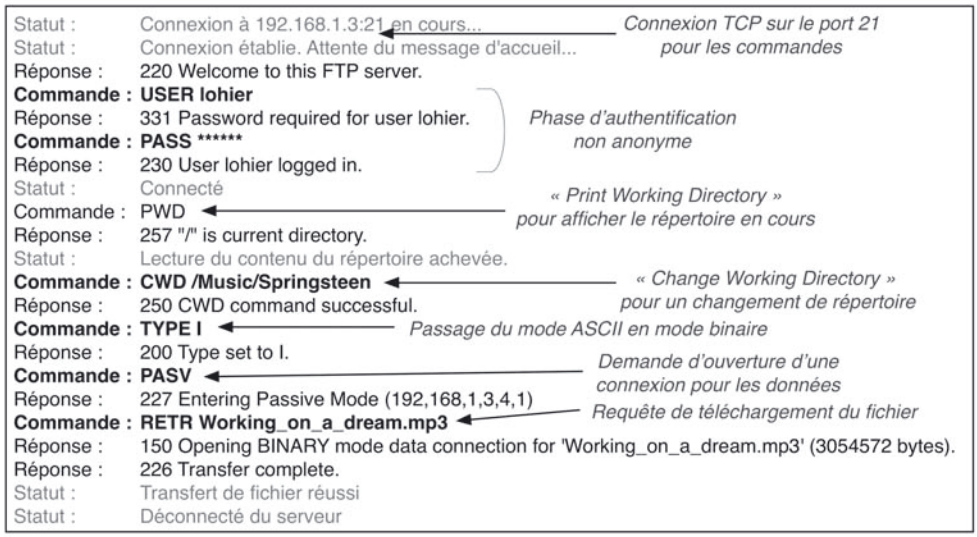


Figure 8.31 – Exemple de dialogue FTP.

8.6.7 RTP et RTSP

Il est nécessaire pour transporter des flux multimédias comme la voix ou la vidéo d'utiliser des protocoles spécifiques de niveau transport qui vont apporter des garanties temporelles. Deux protocoles sont ainsi utilisés au-dessus de la couche UDP (figure 8.32).

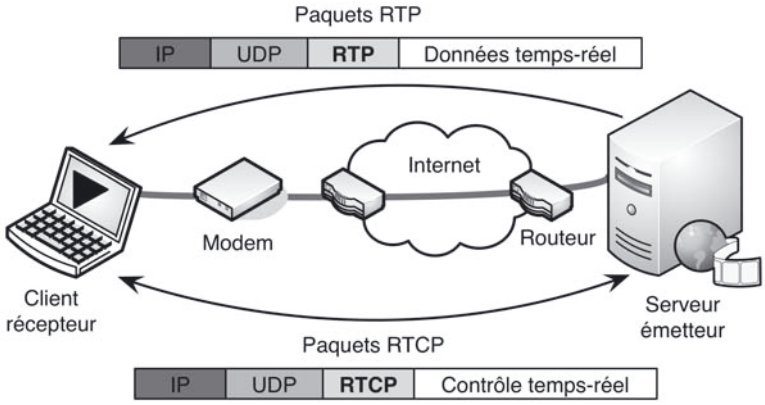


Figure 8.32 – **Protocoles « temps réel ».**

RTP (*Real Time Transport Protocol*), RFC 3550 a pour rôle de fournir un moyen uniforme pour transmettre, quelle que soit la qualité du réseau IP sous-jacent, des données multimédia soumises à des contraintes de temps réel. Ses principales fonctionnalités sont :

- identifier le type de l'information transportée ;
- ajouter des numéros de séquence et des marqueurs temporels (*timestamps*) sur les données transportées ;
- contrôler l'arrivée à destination des paquets et analyser les marqueurs temporels.

De plus, les informations RTP peuvent être transportées dans des paquets multicast afin d'acheminer des conversations vers des destinataires multiples.

Le protocole **RTCP** (*Real time Transport Control Protocol*), RFC 3550, fonctionne avec RTP et permet de contrôler des flots de données qui ont des propriétés temps-réel. Il est basé sur des transmissions périodiques de paquets de contrôle par tous les participants de la session pour fournir un retour (*feedback*) à RTP. Ces deux protocoles liés utilisent deux ports UDP successifs : RTP utilise le port pair et RTCP le port impair immédiatement supérieur.

8.6.8 SIP et RTSP

Au niveau applicatif, les différents protocoles normalisés sont les suivants :

- le protocole de signalisation **H323** se base sur les travaux de la série H.320 sur la visioconférence. C'est une norme stabilisée mais ancienne et pas toujours adaptée aux nouveaux services sur IP ;
- le protocole **SIP** (*Session Initiation Protocol*), prévu au départ pour l'ouverture/fermeture de session multimédia, est natif du monde Internet et est un concurrent direct de l'H323. Il suscite actuellement un très grand intérêt dans la communauté Internet et principalement pour la téléphonie ;

- le protocole **RTSP** (*Real-Time Streaming Protocol*) pour initier et commander à distance des flux multimédia stockés sur un serveur de *streaming* à travers un réseau IP.

a) SIP

SIP (RFC 3261) est un protocole de signalisation (ouverture, gestion, libération des sessions audio et vidéoconférence) appartenant à la couche application du modèle OSI. Ses données sont encapsulées dans des segments UDP. Précisons que SIP ne transporte pas les échantillons de voix, c'est généralement le rôle de RTP.

Pour ouvrir une session, un utilisateur émet une invitation transportant un descripteur de session permettant de vérifier la compatibilité des médias. SIP permet de relier des stations mobiles en transmettant ou en redirigeant les requêtes vers la position courante de la station appelée. Il possède l'avantage de ne pas être attaché à un médium particulier et est censé être indépendant du protocole de transport des couches basses. Parmi les fonctionnalités proposées, on peut noter :

- la localisation du terminal correspondant ;
- l'analyse du profil et des ressources du destinataire ;
- la négociation du type de média (voix, vidéo, données…) et des paramètres de communication ;
- la disponibilité du correspondant : détermine si le poste appelé souhaite communiquer et autorise l'appelant à le contacter ;
- l'établissement et le suivi de l'appel : avertit les parties appelant et appelé de la demande d'ouverture de session, gère le transfert et la fermeture des appels ;
- la gestion de fonctions évoluées : cryptage, retour d'erreurs…

D'un point de vue protocolaire, SIP utilise des requêtes et des réponses du même type que HTTP. La figure 8.33 montre un exemple d'établissement d'une communication SIP avec les différentes phases :

- l'UA (*User Agent*) de l'appelant tente d'établir une session VoIP avec un correspondant en passant par son Proxy SIP qui est un serveur intermédiaire entre deux UA qui ne connaissent pas leurs adresses IP respectives ;
- le Proxy interroge un *Registar* qui possède dans sa base de données la correspondance URL/adresse IP ;
- le Proxy peut alors relayer l'invitation vers le destinataire dont il connaît l'adresse IP ;
- après une demande de connexion et une réponse positive, la session VoIP est établie, les données peuvent être échangées *via* le protocole de transport RTP sans transiter par le Proxy intermédiaire ;
- la session est fermée à l'initiative de l'appelé.

b) RTSP

RTSP est un protocole de niveau applicatif prévu pour fonctionner sur des protocoles tels que RTP et RTCP. Son rôle principal est d'initier et de commander à distance des flux multimédia stockés sur un serveur de *streaming*. Il offre des fonctionnalités

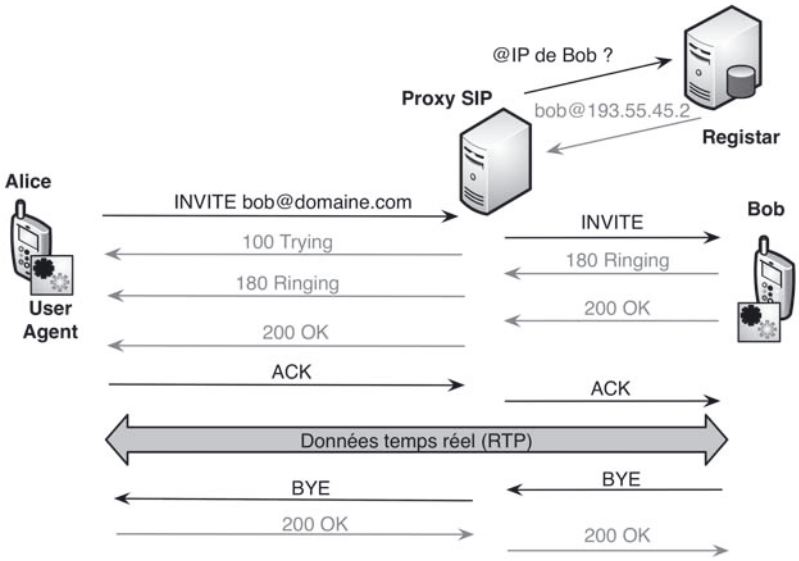


Figure 8.33 – Exemple de fonctionnement de SIP.

comme l'arrêt, l'avance rapide, la recherche avancée pour des flux vidéo et audio. Les flux peuvent provenir soit de vidéos stockées, soit d'une source temps réel (caméra, micro). Les données multimédias sont transmises séparément en utilisant le plus souvent RTP.

RTSP est similaire au niveau de la syntaxe et des fonctionnalités à HTTP, chaque présentation et chaque flux média est identifié par un URL. Une présentation peut contenir plus d'un flux média. Le fichier de description de la présentation (*meta file*) qui est adressé par un navigateur (figure 8.34) contient les codages, le langage et d'autres paramètres qui permettent au client de choisir la combinaison la plus adéquate de médias.

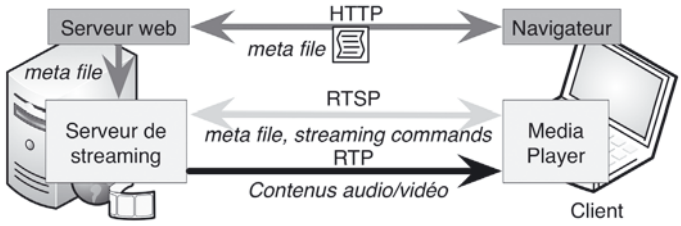


Figure 8.34 – Rôle du protocole RTSP.

Résumé

- Internet est un réseau de réseaux et de services utilisant le protocole **TCP/IP**. Il fait intervenir des opérateurs de **câblage**, des opérateurs de **transport** et des **FAI** (Fournisseurs d'Accès Internet).
- Les réseaux fédérateurs, ou **ISP de niveau 1**, sont au cœur de l'Internet et ont une couverture internationale. Ils relient les **ISP de niveau 2 et 3,** ou FAI, qui sont à la frontière du réseau d'accès et ont pour vocation de connecter les entreprises ou les particuliers.
- Les **FAI** fournissent à leurs clients des connexions sur le réseau Internet et des adresses IP fixes ou dynamiques attribuées par un serveur DHCP le temps de la connexion sur Internet. Les FAI gèrent pour leurs clients un serveur de **messagerie,** le **stockage** de fichiers et l'hébergement de pages **web**.
- Les services les plus courants sur Internet sont la **messagerie** (e-mail), le **transfert de fichiers** (FTP) et les **serveurs d'informations** en ligne (serveurs web). On trouve également des services de **voix sur IP** et de visioconférence.
- Le **service DNS** est chargé d'identifier et de localiser par leurs **adresses IP** les postes et les serveurs accessibles sur Internet à partir de **noms symboliques**. Le nommage des machines fait appel à des **noms de domaines** hiérarchisés suivant une organisation arborescente.
- Le **protocole PPP** (*Point to Point Protocol*) est utilisé pour le dialogue TCP/IP entre un client et un prestataire à travers un réseau d'opérateurs de télécommunications, par encapsulation des paquets IP.
- Les **serveurs web** donnent accès à des fichiers de tous types (texte, image, son, vidéo) grâce à des hyperliens. Ces ressources sont pointées par des **URL** (*Uniform Ressource Locator*). Le client doit disposer d'un navigateur.
- Le **protocole HTTP** (*HyperText Transmission Protocol*) est utilisé dans le dialogue entre les navigateurs et les serveurs web. Le dialogue HTTP est de type requête/réponse. La méthode **GET** permet de demander une ressource pointée par son URL. Le serveur renvoie en retour le fichier demandé ou un code d'erreur.
- Un service de **messagerie** s'appuie sur des serveurs gérant des BAL (boîtes à lettres) où sont stockés les messages en attente d'être lus.
- Le client envoie un courrier au serveur de sa zone grâce au protocole de courrier sortant **SMTP** (*Simple Mail Transport Protocol*). SMTP est également utilisé pour le transfert de messages entre serveurs de messagerie.
- Pour le courrier entrant, les serveurs se répartissent entre **serveurs POP3** nécessitant l'installation sur le poste client d'un « client de messagerie » et **serveurs Webmail** s'appuyant sur le **protocole IMAP** et accessibles à partir d'un navigateur.

- Pour le courrier entrant, les serveurs se répartissent entre **serveurs POP3** nécessitant l'installation sur le poste client d'un « client de messagerie » et **serveurs Webmail** s'appuyant sur le **protocole IMAP** et accessibles à partir d'un navigateur.
- **POP3** (*Post Office Protocol*) permet à un client non connecté en permanence d'aller chercher ses messages sur le serveur après identification (nom et mot de passe). **IMAP4** (*Interactive Mail Access Protocol*) propose au client un jeu de commandes interactives plus complet que celui de POP3.
- Les services de **transfert de fichiers** nécessitent des serveurs et des clients faisant appel au protocole **FTP** (*File Transfer Protocol*). Les clients sont identifiés (compte utilisateur et mot de passe), peuvent se déplacer dans l'arborescence du serveur et télécharger des fichiers. Le transfert de fichiers en ***« peer to peer »***, sans passer par un serveur, est utilisé pour partager des ressources entre particuliers en multipliant le nombre de sources potentielles.
- Les services de **voix et de vidéo sur IP** sont de plus en plus utilisés sur Internet. Ils offrent l'avantage de s'intégrer avec d'autres flux sur un réseau?IP plutôt que d'utiliser des infrastructures particulières (réseau téléphonique ou vidéo distinct). La difficulté est de respecter des **contraintes de temps** sur un réseau IP non prévu à la base pour ces applications.
- Les deux principaux protocoles utilisés au niveau du transport sont **RTP** (*Real-time Transport Protocol*) pour la transmission des données et **RTCP** (*Real-time Transport Control Protocol*) pour le contrôle des paramètres de transmission.
- Un niveau applicatif, le protocole SIP (***Session Initiation Protocol***), permet de gérer l'ouverture et la fermeture de sessions **VoIP** entre terminaux. **RTSP** (*Real-Time Streaming Protocol*) est utilisé pour initier et commander à distance des flux **vidéo** stockés sur un serveur de *streaming* à travers un réseau IP.

Exercices corrigés

QCM

Q8.1 L'opérateur de transport fournit un service direct :

a) À l'opérateur de câblage b) Au FAI c) À l'internaute

Q8.2 Parmi les critères suivants, lesquels sont susceptibles de ralentir une navigation sur Internet ?

a) Le serveur web saturé.

b) La surcharge due aux en-têtes de protocoles.

c) Le contrôle de flux.

d) La qualité de la ligne.

Q8.3 La liaison entre le client et le FAI est de type :

a) Point-multipoint b) Point à point

c) Multipoint-multipoint

Q8.4 À quoi correspond la boucle locale ?

a) À la portion entre le répartiteur et le DSLAM.

b) À la portion entre le répartiteur et les équipements du FAI.

c) À la portion entre l'abonné et son répartiteur.

d) À la portion entre l'abonné et l'autocommutateur de raccordement.

Q8.5 Dans une connexion par câble, quelle technique est utilisée pour transporter simultanément des données et de la TV ?

a) Le multiplexage temporel

b) Le multiplexage fréquentiel

c) La compression

Q8.6 Lorsque vous vous connectez sur Internet de chez vous *via* un modem :

a) Vous utilisez votre propre adresse IP locale que vous avez configurée dans les paramètres TCP/IP.

b) Le FAI vous assigne une adresse IP que, seul à ce moment, vous pouvez utiliser.

c) On vous assigne une adresse IP qui peut être également attribuée au même moment à une autre personne, mais obligatoirement chez un autre FAI.

Q8.7 À quelle couche du modèle OSI le protocole PPP est-il associé ?

a) Transport b) Session c) Réseau d) Liaison

Q8.8 Les serveurs DNS permettent :

a) D'associer à un nom de domaine une adresse IP.

b) D'associer à un nom machine une adresse IP.

c) À un internaute d'utiliser directement les adresses IP.

d) De garder en mémoire les pages fréquemment consultées.

Q8.9 Dans une résolution DNS récursive :

a) Le serveur DNS primaire connaît au moins l'adresse d'un serveur racine ou de premier niveau.

b) Chaque serveur DNS interrogé renvoie au DNS primaire l'adresse du serveur suivant.

c) Le serveur DNS primaire relaie toutes les requêtes.

d) L'adresse IP est renvoyée directement au DNS primaire.

Q8.10 HTML est :

a) Un protocole pour accéder à des serveurs web.

b) Un langage de description de page web.

c) Un langage de programmation.

d) Un langage intégrant des balises et des hyperliens.

Q8.11 Pour envoyer un message, il est nécessaire :

a) De disposer d'une BAL sur le serveur auquel se connecte le poste.

b) De disposer d'une BAL sur le serveur du destinataire.

c) Il n'est pas nécessaire de disposer d'une BAL.

Q8.12 Quels sont les protocoles utilisés lorsque vous relevez votre courrier par l'intermédiaire d'un webmail ?

a) HTTP b) IMAP c) POP3 d) SMTP

Q8.13 Lors d'un transfert de fichier en « *peer to peer* »

a) L'intégralité du fichier est stockée sur un serveur.

b) Les fichiers sont découpés en blocs.

c) Les clients doivent se connecter en non anonyme.

Q8.14 La téléphonie sur IP permet :

a) De téléphoner en utilisant son PC équipé d'un casque et d'une micro.

b) De téléphoner en utilisant son téléphone classique.

c) D'inclure les frais de communication dans son abonnement Internet.

d) De naviguer et de téléphoner simultanément.

Q8.15 Dans une application de streaming :

a) Les fichiers vidéo sont d'abord stockés sur le PC.

b) La qualité de la connexion entre le client et le serveur n'a aucune influence sur la qualité de la diffusion.

c) Des protocoles spécifiques « temps réel » sont utilisés.

Q8.16 Le protocole RTP :

a) Est utilisé pour gérer les contraintes de temps des applications multimédia.

b) Est utilisé pour transporter les flux multimédias.

c) Offre des fonctionnalités comme l'arrêt, l'avance rapide, la recherche avancée pour des flux vidéo et audio.

d) Fonctionne avec le protocole RTCP.

Exercices

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

8.1 (*) Quelle est la différence entre une liste de diffusion et une lettre d'information (*newsletter*) ?

8.2 (**) Imaginez qu'un étudiant de l'université de Paris 6 vienne d'écrire un nouveau programme qu'il souhaite rendre accessible par FTP. Il place le programme dans le répertoire *ftp/pub/maitrise/newprog.c.* Quelle sera l'URL permettant d'atteindre ce programme ?

8.3 Quels sont les avantages et les inconvénients du webmail ?

8.4 (*) Existe-t-il un rapport entre les classes d'adresse IP et les noms de domaine DNS ?

8.5 (**) Pourquoi ne peut-on pas transporter directement des datagrammes IP sur une liaison série ?

8.6 (*) Vous disposez d'une connexion Internet en *Dial-up* et votre FAI vous fournit un service complet de messagerie. Où sont stockés physiquement vos messages ? Pouvez-vous les récupérer en cas de panne de votre PC ?

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

8.8 (***) Quelle méthode HTTP est utilisée pour :

a) Demander un document texte *via* le web ?

b) Lancer une recherche sur un moteur de recherche ?

c) Vérifier l'existence d'un document ?

d) S'enregistrer sur un site *via* un formulaire pour recevoir une lettre périodique d'information ?

8.9 (***) La trame suivante a été relevée lors de la connexion sur un serveur web :

```
+ FRAME : Base frame properties
+ ETHERNET : ETYPE = 0x0800 : Protocol = IP : DOD Internet
Protocol
+ IP : ID = 0x8C11 ; Proto = TCP ; Len : 1496
+ TCP : .A….., len : 1456, seq : 23624030-23625485, ack :
8810360, win : 8385, src : 80 dst : 1125
HTTP : Response (to client using port 1125)
HTTP : Protocol Version = HTTP/1.0
HTTP : Status Code = OK
HTTP : Reason = OK
HTTP : Undocumented Header = Via : 1.0 PROXYA
HTTP : Undocumented Header Fieldname = Via
HTTP : Undocumented Header Value = 1.0 PROXYA
HTTP : Content-Type = text/html
HTTP : Date = Thu, 20 Jan 2010 09 :27 :08 GMT
HTTP : Server = Apache/1.3.9 (Unix)
HTTP : Data : Number of data bytes remaining = 1329 (0x0531)
```

a) Justifier les valeurs des différents champs longueur pour les différentes couches.

b) À quoi correspondent les valeurs des ports source et destination ?

c) Commenter les différents champs de l'en-tête HTTP et leurs contenus.

8.10 (**) Pour relever son courrier, quelles sont les principales différences entre :

a) Un accès direct par SMTP ?

b) Un accès par POP3 ?

c) Un accès par IMAP ?

8.11 (*) Pourquoi utiliser la téléphonie sur IP plutôt que la téléphonie classique ?

8.12 (**) On s'intéresse à une application de diffusion vidéo de type « temps réel » (*streaming*).

a) Quelle est selon vous la contrainte la plus forte en termes de QoS ? Justifiez votre réponse.

b) Pourquoi l'adressage multicast est-il utilisé en streaming ?

c) Quels sont les trois principaux protocoles utilisés dans le streaming ? Décrire en une phrase le rôle de chacun en précisant la couche concernée.

Solutions

QCM

Q8.1 : b **Q8.2** : a-b-c-d **Q8.3** : b **Q8.4** : c **Q8.5** : b
Q8.6 : b **Q8.7** : d **Q8.8** : b **Q8.9** : a **Q8.10** : b-d
Q8.11 : c **Q8.12** : a-b **Q8.13** : b **Q8.14** : a-b-c-d
Q8.15 : c **Q8.16** : a-b-d

Exercices

8.1 Dans le premier cas, tous les abonnés peuvent envoyer un message alors que dans le deuxième cas, c'est une lettre électronique envoyée périodiquement à tous les abonnés. Ceux-ci sont passifs dans la mesure où ils n'envoient pas de messages.

8.2

```
ftp://ftp.paris6.fr/maitrise/newprog.c
```

8.3 Avantages du webmail : pas de logiciel client à configurer, courrier consultable depuis n'importe quel navigateur. Inconvénients : lenteur, dépendance de l'interface et des capacités du webmail, personnalisation difficile.

8.4 Il n'y a pas de lien direct entre les classes d'adresse IP et les noms de domaine DNS. Suivant l'importance des réseaux, un domaine peut correspondre à plusieurs classes et inversement.

8.5 Une couche liaison telle PPP est nécessaire pour au moins deux raisons : délimiter le début et la fin d'une trame à l'aide de codes spécifiques (il n'y a pas de moyen de distinguer la fin d'un datagramme du début du suivant) ; activer la ligne et négocier les options (notamment la taille des paquets).

8.6 Les messages qui vous sont destinés sont stockés au départ dans la BAL de votre serveur de messagerie. Lorsque vous les téléchargez, ils sont copiés par votre logiciel client de messagerie sur votre disque dur. Suivant l'option choisie, vous pouvez alors les effacer du serveur. Si vous avez choisi de les conserver, il vous restera une copie en cas de panne de votre PC.

8.7 Une connexion anonyme sur un serveur FTP permet de ne pas avoir à gérer un compte et un mot de passe. Mais dans la mesure où il n'y a pas d'authentification réelle, c'est un point d'entrée dans le système. Une connexion non anonyme permet donc de sécuriser les accès et d'attribuer des droits sur certains répertoires (lecture, écriture…).

8.8

a) La méthode GET permet de récupérer le contenu identifié par l'URL ; il peut s'agir d'un document HTML, mais aussi d'une page générée dynamiquement par un processus sur le serveur.

b) C'est encore la méthode GET avec le champ « Request URL » correspondant à la recherche.

c) La méthode HEAD permet de demander des renseignements sur la ressource. Cette méthode sert à tester, par exemple, la validité des liens sans télécharger le corps du document ; seul l'en-tête HTTP correspondant à la requête est retourné.

d) La méthode POST permet de demander au serveur de réaliser une action dont le résultat ne pourrait pas être stocké sous un nom d'URL. Par exemple : poster un message dans les forums ou les listes de diffusion ou envoyer les données correspondant à une réponse à un formulaire en ligne. L'utilisation de POST permet de masquer les informations transmises (car non visibles dans l'URL) et est obligatoire pour des informations longues (dont la taille serait supérieure à celle de la longueur maximale d'une URL).

8.9

a) 1 329 octets de données HTTP + 127 octets d'en-tête HTTP = 1 456 octets.
1 456 octets HTTP + 20 octets d'en-tête TCP + 20 octets d'en-tête IP = 1 496 octets.

b) Le port source est égal à 80, il correspond au protocole HTTP, le port destination 1125 est un port client. Il s'agit donc d'une réponse d'un serveur web à un client.

c) L'en-tête HTTP nous donne successivement : la version (http 1.0), le code de réponse (OK), le nom du proxy (PROXYA), le type de contenu (text /html), la date et l'heure, le type du serveur web (Apache).

8.10

a) SMTP n'est pas prévu pour le courrier entrant lorsque les machines ne sont pas connectées en permanence. Il ne gère pas l'authentification.

b) Avec POP3, il est nécessaire de télécharger l'intégralité des courriers. Il n'est pas possible d'ajouter d'autres boîtes aux lettres.

c) Avec IMAP, il n'est pas nécessaire de paramétrer un client. Il est possible de créer des boîtes, de ne consulter que les en-têtes des messages et de laisser sur le serveur les courriers spammés ou infectés.

8.11 L'intérêt est de n'utiliser qu'un seul réseau IP pour toutes les applications (téléphonie, Internet, TV). La numérisation offre de plus d'autres possibilités : compression, stockage…

8.12

a) La contrainte de temps est la plus importante en streaming. Les variations de délai sont mal tolérées en raison de la nature continue du flux.

b) Le multicast permet d'utiliser la même adresse lorsque le même flux doit être envoyé à plusieurs personnes en même temps.

c) RTP au niveau transport pour transmettre les flux temps réel audio et vidéo.

RTCP au niveau transport, en liaison avec RTP, pour contrôler la diffusion des flux temps réel audio et vidéo.

RTSP au niveau application pour contrôler la distribution des flux multimédia sur le réseau IP (allocation des ressources, demande de transmission des flux, pause…).

LA SÉCURITÉ DANS LES RÉSEAUX

9

PLAN

OBJECTIFS

- Connaître les principales techniques d'attaque par intrusion ou déni de service.
- Connaître les mécanismes de défense matérielle (*firewall*, DMZ, VPN…) et logicielle (chiffrement, authentification, certificats…).
- Étudier les principaux protocoles associés aux VPN, à l'authentification et au chiffrement des informations.

9.1 POURQUOI SÉCURISER ?

Les attaques visant à pirater un système en réseau dans le but de récupérer des informations sensibles ou d'altérer les services existent à tous les niveaux. Les points d'entrée les plus vulnérables sont les navigateurs (lien malveillant) et les clients de messagerie (faux lien intégré et pièces jointes). Les services récents sont également concernés : les nouvelles menaces impliquent les blogs, le partage des fichiers multimédia et les sites des réseaux sociaux.

Quelle que soit leur place ou leur rôle dans une architecture de réseau local ou sur Internet, les systèmes (serveurs, PC, routeurs, systèmes de stockage…) sont donc tous vulnérables à un certain niveau :

- émergence en permanence de nouveaux usages et de nouvelles technologies, et donc de nouvelles vulnérabilités (réseaux sociaux, *peer to peer*, messagerie instantanée, réseaux sans fil, *smartphone* connectés en WiFi ou en 3G, téléphonie sur IP, stockage sur clé USB…) ;
- les politiques de sécurité sont complexes car elles doivent opérer simultanément sur tous les éléments d'une architecture réseau et pour différents types d'utilisateurs

(*firewall* sur les routeurs d'accès et sur les serveurs d'extrémité, cryptage de certains fichiers, droits accrus pour les administrateurs sur certaines ressources…) ;

- les politiques de sécurité mises en place sont basées sur des jugements humains qui doivent de plus être révisés en permanence pour s'adapter aux nouvelles attaques ;
- la sécurisation est coûteuse en moyens, en temps et surtout en ressources humaines.

Pour limiter ces vulnérabilités (quelles que soient les solutions, un système reste toujours vulnérable), la sécurité informatique vise généralement trois objectifs principaux :

- l'**intégrité** consiste à garantir que les données n'ont pas été altérées sur la machine ou durant la communication (sécurité du support et sécurité du transport) ;
- la **confidentialité** consiste à assurer que seules les personnes autorisées ont accès aux ressources ;
- la **disponibilité** consiste à garantir à tout moment l'accès à un service ou à des ressources.

Un quatrième objectif peut être rajouté, il s'agit de la non-répudiation qui permet de garantir qu'aucun des correspondants ne pourra nier la transaction. Précisons que l'authentification est un des moyens qui permet de garantir la confidentialité.

La figure 9.1 présente les trois objectifs visant à protéger l'information centrale et les différents moyens pour y parvenir compte tenu des menaces situées à la périphérie. Les paragraphes suivants présentent dans le détail les attaques ainsi que les méthodes matérielles et logicielles (les deux étant complémentaires) pouvant être mises en œuvre pour protéger l'information dans les systèmes informatiques en réseau.

9.2 Les attaques

Les attaques peuvent être classées en deux grandes catégories : les techniques d'intrusion dont l'objectif principal est de s'introduire sur un réseau pour découvrir ou modifier des données et les dénis de service qui ont pour but d'empêcher une application ou un service de fonctionner normalement. Cette deuxième catégorie agit donc sur la disponibilité de l'information tandis que la première concerne essentiellement la confidentialité et l'intégrité. Une autre classification existe : elle distingue les attaques passives basées sur l'écoute et l'interception qui concernent seulement la confidentialité et les attaques actives qui altèrent également les données ou les services et concernent donc la disponibilité et l'intégrité.

9.2.1 Techniques d'intrusion

Ces techniques peuvent être classées suivant le niveau d'intervention :

1. les accès physiques vont du vol de disque dur ou de portable à l'écoute du trafic sur le réseau (*sniffing*) ;

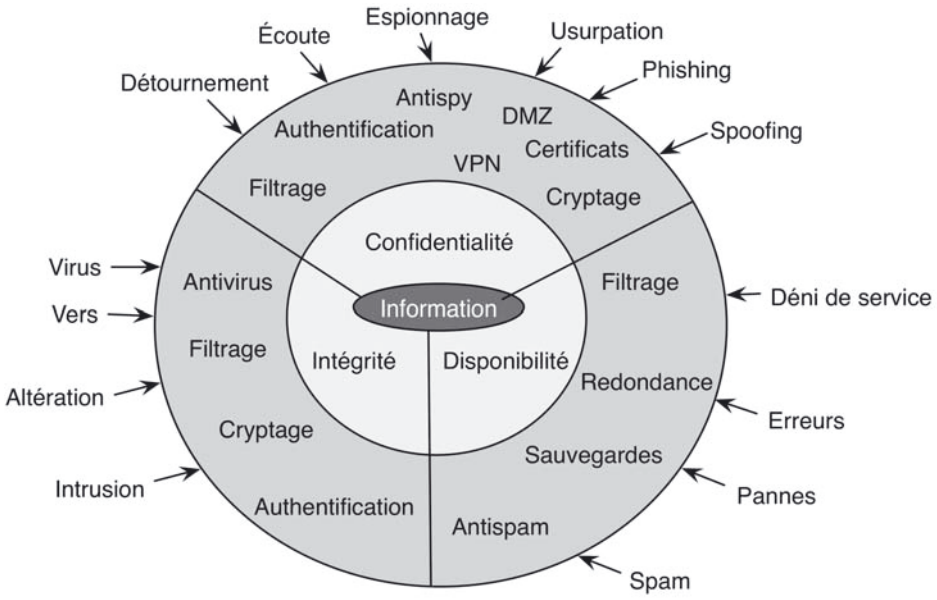


Figure 9.1 – Objectifs, moyens et attaques.

2. l'ingénierie sociale (*social engineering*) permet de retrouver ou de récupérer directement des couples identifiant/mot de passe en envoyant par exemple des messages falsifiés (*phishing*) ;
3. l'interception de communications permet l'usurpation d'identité, le vol de session (*session hijacking*), le détournement ou l'altération de messages (*spoofing*) ;
4. les intrusions sur le réseau comprennent le balayage de ports (*port scan*), l'élévation de privilèges (passage du mode utilisateur au mode administrateur) et surtout les logiciels malveillants ou *malwares* (virus, vers et chevaux de Troie).

Les principales attaques de ce type sont détaillées dans les paragraphes suivants.

a) Le sniffing

Sur la plupart des réseaux, les trames sont diffusées sur tout le support (câble Ethernet, transmission radio WiFi…). En fonctionnement normal, seul le destinataire reconnaît son adresse (adresse MAC destination sur un réseau Ethernet) et lit le message. La carte Ethernet ou WiFi d'un PC peut être reprogrammée pour lire tous les messages qui traversent le réseau (*promiscious mode*). La limite dans ce cas est le dispositif d'interconnexion utilisé sur le LAN ou le segment de LAN (*hub*, *switch*, AP WiFi, routeur…). Les *hackers* utilisent des « *sniffers* » ou analyseurs réseau qui scannent tous les messages qui circulent sur le réseau et recherchent ainsi des identités et des mots de passe.

b) Le « craquage » de mot de passe

Le *hacker* utilise un dictionnaire de mots et de noms propres construit à partir d'informations personnelles et privées qui ont été collectées (*social engineering*). Ces chaînes de caractère sont essayées une à une à l'aide de programmes spécifiques qui peuvent tester des milliers de mots de passe à la seconde. Ce type d'attaque est souvent nommé attaque par force brute car le mot de passe est deviné grâce à des milliers d'essais successifs à partir d'un dictionnaire, et non pas retrouvé à l'aide d'un programme capable de décrypter une chaîne de caractères.

c) Le phishing

Ce néologisme anglais provient de la contraction de *fishing* (pêcher) et de *phreaking* (pirater le réseau téléphonique). Il s'agit de conduire des internautes à divulguer des informations confidentielles, notamment bancaires, en usant d'un hameçon fait de mensonge et de contrefaçon électronique (identité visuelle d'un site connu, en-têtes, logo…). Le cas le plus classique est celui d'un mail usurpant l'identité de votre banque et contenant un lien vers un faux site où l'on vous demandera de confirmer votre numéro de carte bleue par exemple.

d) Le spoofing (to spoof : « faire passer pour, usurper »)

Les falsifications peuvent intervenir sur tous types de serveur, en particulier sur les serveurs DNS et web.

Le **DNS *spoofing*** : le pirate utilise les faiblesses du protocole DNS et de son implémentation sur les serveurs de noms de domaine pour rediriger des internautes vers des sites falsifiés. Le but du pirate est donc de faire correspondre l'adresse IP d'une machine qu'il contrôle à l'URL réel d'une machine publique.

Le **web *spoofing*** est une version élaborée de l'IP *spoofing* : il s'agit de remplacer un site par une version pirate du même site. Cette technique est notamment utilisée dans la dernière étape du *phishing*. La falsification se déroule en plusieurs temps :

- amener la victime à entrer dans le faux site web (grâce à l'utilisation du DNS *spoofing* par exemple) ;
- intercepter les requêtes HTTP ;
- récupérer les vraies pages web et modifier ces pages ;
- envoyer de fausses pages à la victime.

e) Les malwares

Le terme « virus » est souvent employé abusivement pour désigner toutes sortes de logiciels malveillants (les virus ont été historiquement les premiers *malwares*).

Un **virus** est un programme qui se propage à l'aide d'autres programmes ou de fichiers. Il est souvent simple et facile à détecter à partir de son code (signature) mais néanmoins efficace lorsqu'il se propage plus rapidement que la mise à jour des anti-virus. Un virus passe le plus souvent par la messagerie et est activé par la sélection d'un lien sur le message ou l'ouverture d'un fichier attaché. Les conséquences de l'exécution du virus peuvent aller de la simple modification des paramètres d'une

application (page par défaut du navigateur) ou de la base de registre du système (exécution automatique d'un programme commercial à chaque démarrage) à l'effacement de données ou de fichiers essentiels au système d'exploitation.

Un **ver** (*worm*) est un programme plus sophistiqué capable de se propager et de s'auto-reproduire sans l'utilisation d'un programme quelconque (d'un vecteur) ni d'une action par une personne. La particularité des vers ne réside pas forcément dans leur capacité immédiate de nuire mais dans leur facilité pour se propager grâce par exemple aux listes de contacts présentes sur les PC ou les *smartphones*.

Un **cheval de Troie** (*troyan*) est un programme caché dans un autre programme qui s'exécute au démarrage du programme « hôte ». Il permet donc de s'introduire sur le système à l'insu de la victime (ouverture d'une « porte dérobée » ou *backdoor*) ; le cheval de Troie devient alors autonome et peut agir comme un virus en infectant des données ou des programmes.

9.2.2 Déni de service

Ce type d'attaque nommé en anglais *Denial of Service* ou **DoS** empêche par saturation un service de fonctionner correctement sur une machine.

a) SYN Flood

Cette attaque consiste à inonder (*flooding*) la cible à l'aide de demandes successives d'ouverture de connexion TCP. Lors d'une ouverture normale (figure 9.2 a) :

- le premier segment TCP est transmis par le client avec le bit SYN à 1 pour demander l'ouverture ;
- le serveur répond avec dans son segment TCP les bits SYN et ACK à 1 ;
- le client demandeur conclut la phase avec le bit ACK à 1.

Les abus interviennent au moment où le serveur a renvoyé un accusé de réception (SYN ACK) au client mais n'a pas reçu le « ACK » du client. C'est alors une connexion semi-ouverte et l'agresseur peut saturer la structure de données du serveur victime en créant un maximum de connexions partiellement ouvertes. Le client autorisé ne pourra alors plus ouvrir de connexion (figure 9.2 b).

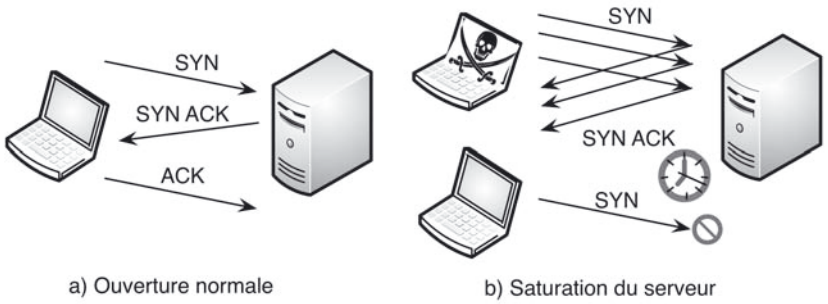


Figure 9.2 – Principe du SYN Flood.

b) DDOS

Le déni de service distribué ou DDOS (*Distributed Denial Of Service*) a les mêmes effets que le DOS traditionnel excepté que ce n'est plus une seule machine qui attaque les autres mais une multitude de machines nommées zombies contrôlées par un maître unique. L'attaque se déroule en plusieurs étapes (figure 9.3) :

- recherche sur Internet d'un maximum de machines vulnérables qui deviendront des complices involontaires, des « zombies ». Les réseaux de zombies (*botnet* en anglais) ainsi formés sont une ressource précieuse pour les *hackers* ;
- installation sur ces machines de programmes dormants (*daemons*) et suppression des traces éventuelles (*logs*). Les *daemons* sont basés sur les attaques DOS classiques (paquets UDP multiples, SYN Flood, *buffer overflow*…) ;
- activation du dispositif à l'heure et au jour programmé.

Parmi les attaques DDOS très populaires, on connaît l'attaque sur les sites Yahoo, CNN, Amen et eBay qui ont subi une inondation de leur réseau.

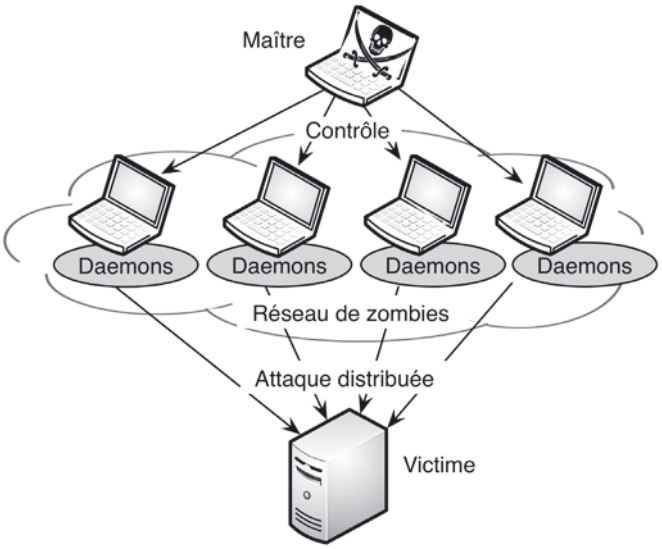


Figure 9.3 – Principe du DDOS.

9.3 Les défenses matérielles

Les défenses matérielles interviennent au niveau de l'architecture du réseau, directement sur le support sur lequel est stockée l'information à protéger (protection d'une base de données centralisée sur le disque dur d'un serveur par exemple), sur les

médias servant à transporter cette information (sécurisation du réseau WiFi) et sur les équipements intermédiaires traversés lors du transport (utilisation d'un *firewall* installé sur le routeur d'accès).

9.3.1. Les *firewalls*

Le *firewall* ou pare-feu est chargé de filtrer les accès entre l'Internet et le réseau local ou entre deux réseaux locaux (figure 9.4). La localisation du *firewall* (avant ou après le routeur, avant ou après le NAT) est stratégique. Le *firewall*, qui est souvent un routeur possédant des fonctionnalités de filtrage, possède autant d'interfaces que de réseaux connectés. Suivant la politique de sécurité, le filtrage est appliqué différemment pour chacune des interfaces d'entrée et de sortie : blocage des adresses IP privées entrantes, autorisation des accès entrants vers le serveur d'identification ou le serveur web institutionnel, blocage des accès entrants vers l'Intranet… Les machines d'extrémité possèdent également un *firewall* mais celui-ci est logiciel (pare-feu *Windows* ou *iptables* sous Linux par exemple) et sert à protéger les machines du trafic entrant si le *firewall* à l'entrée du LAN n'a pas été suffisamment sélectif.

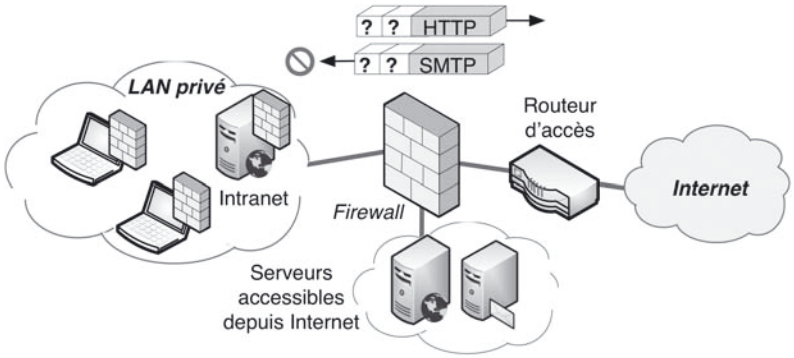


Figure 9.4 – Rôle et situation du *firewall*.

Pour chaque trame ou chaque paquet entrant ou sortant sur une interface donnée, les en-têtes correspondant aux différentes couches sont analysés et le filtrage sélectif est appliqué suivant la stratégie de sécurité définie par l'administrateur du réseau (figure 9.4). Le filtrage peut porter sur :

- les adresses MAC source ou destination ;
- les adresses IP source ou destination ;
- les ports TCP ou UDP source ou destination ;
- les *flags* de l'en-tête TCP (SN, ACK…) ;
- le type de message ICMP ;
- le type de message ou le contenu HTTP, SMTP, POP (filtrage applicatif).

Le *firewall* peut également empêcher les connexions entrantes en analysant la valeur du bit ACK de l'en-tête TCP. Lors d'une demande de connexion, le bit ACK

du premier segment TCP est à 0, les bits ACK des segments suivants sont généralement tous à 1. Il suffit donc de bloquer les segments entrants avec le bit ACK à 0, les segments suivants pour cette connexion ne seront pas pris en compte (voir figure 9.5).

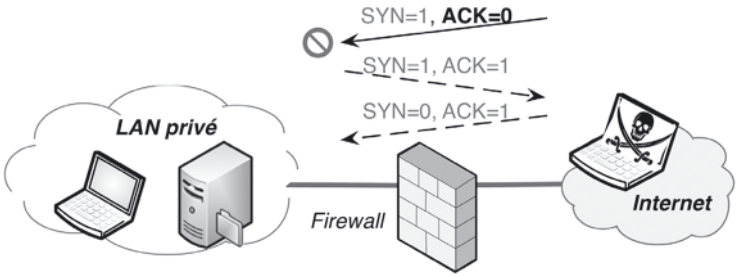


Figure 9.5 – Blocage des connexions entrantes.

La configuration d'un *firewall* passe par l'écriture d'une suite de règles qui décrivent les actions à effectuer (accepter ou refuser le trafic) suivant les informations contenues dans les en-têtes des paquets. Les caractéristiques de chaque paquet sont comparées aux règles, les unes après les autres. La première règle rencontrée qui correspond aux caractéristiques du paquet analysé est appliquée : l'action décrite dans la règle est effectuée. Pour assurer une sécurité maximum, la seule règle présente par défaut doit être celle qui interdit l'accès à tous les paquets entrants et sortants, d'autres règles seront ensuite insérées pour ouvrir les accès souhaités. La stratégie appliquée est donc : « tout ce qui n'est pas explicitement autorisé est interdit ».

Le tableau 9.1 donne un exemple de règles d'un *firewall* muni de deux interfaces : une vers le LAN privé, une autre vers l'extérieur (cas de la figure 9.5). Les règles précisent l'interface, la direction du trafic, les adresses IP (une valeur à 0 autorise toutes les adresses), le protocole de niveau 4, les services (valeurs des ports) et éventuellement le blocage des connexions entrantes (test du bit ACK). La stratégie de sécurité est la suivante :

- la règle A permet à toutes les machines situées sur le réseau local d'adresse 192.168.0.0 d'ouvrir une connexion TCP vers un serveur web (port 80) externe quelconque (adresse 0.0.0.0) ;
- la règle B autorise le serveur web consulté à répondre aux machines locales ;
- émission (règle C) ou réception (règle D) de courrier SMTP (port 25) avec un serveur externe ;
- les paquets entrants depuis des supposés serveurs SMTP ne peuvent passer que si la connexion a été initiée de l'intérieur (règle D) ;
- blocage de tout autre trafic (règle E).

Quelle que soit l'origine du *firewall* utilisé et le système d'exploitation associé, les règles portent plus ou moins sur les mêmes propriétés des paquets entrants ou sortants. Le degré de filtrage peut cependant varier, certains *firewalls* permettent un filtrage applicatif en travaillant sur les contenus des messages et peuvent se baser sur

Tableau 9.1 – **Exemple de règles d'un *firewall*.**

Règle	Direction	@ source	@ dst	Prot.	Port src	Port dst	ACK = 1	Action
A	Sortant	192.168.0.0	0.0.0.0	TCP	> 1023	80		Autorisé
B	Entrant	0.0.0.0	192.168.0.0	TCP	80	>1023	Oui	Autorisé
C	Sortant	192.168.0.0	0.0.0.0	TCP	> 1023	25		Autorisé
D	Entrant	0.0.0.0	192.168.0.0	TCP	25	> 1023	Oui	Autorisé
E	Tous	Tous	Tous	Tous	Tous	Tous		Refusé

les connexions antérieures pour prendre leurs décisions (*firewall statefull*). Les syntaxes pour décrire les règles sont également très variables suivant les constructeurs ou les OS : utilisation d'ACL (*Acces Control List*) pour les routeurs/*firewall* Cisco ; utilisation du programme *iptables* pour les *firewalls* Linux…

9.3.2 Le NAT

Comme indiqué dans le § 6.2, la translation d'adresse ou **NAT** est aussi un dispositif de sécurité complémentaire au filtrage dans la mesure où elle masque les adresses privées qui ne sont par conséquent plus visibles de l'extérieur. Les *firewalls* étant généralement intégrés aux routeurs qui possèdent de plus des fonctionnalités de translation, il est nécessaire pour la compréhension des règles de routage et de filtrage de savoir dans quel ordre sont effectuées ces différentes opérations.

Pour un paquet entrant, la translation concerne l'adresse destination (celle qui est masquée), cette opération est nommée **DNAT** (*Destination* NAT). Il est nécessaire que la translation soit réalisée avant le processus de routage puisque le routeur doit connaître l'adresse interne pour prendre sa décision. Dans l'exemple décrit par la figure 9.6, le paquet entrant est destiné au serveur web interne. L'adresse de destination qui est initialement celle du routeur (193.55.45.254), la seule visible de l'extérieur, est translatée vers celle du serveur web (172.16.0.11) grâce à l'indication du numéro de port 80. Le paquet peut ensuite être routé suivant la table et traité par la première règle du *firewall*, sur l'interface concernée (Eth1).

Pour un paquet sortant, la translation concerne l'adresse source (celle qui doit être masquée) ; cette opération est nommée **SNAT** (*Source* NAT). Dans ce cas, le filtrage est d'abord effectué pour savoir si le paquet est autorisé à sortir. La translation est ensuite réalisée après le processus de routage, en sortie du routeur. Dans l'exemple, le paquet sortant provient du serveur web interne, il est autorisé à sortir par la deuxième règle de filtrage. Après routage, son adresse est translatée vers celle de l'interface de sortie du routeur (Serial1).

9.3.3 Les DMZ

Une zone démilitarisée (ou DMZ, de l'anglais *DeMilitarized Zone*) est une zone de réseau privée ne faisant partie ni du réseau local privé ni de l'Internet (figure 9.7).

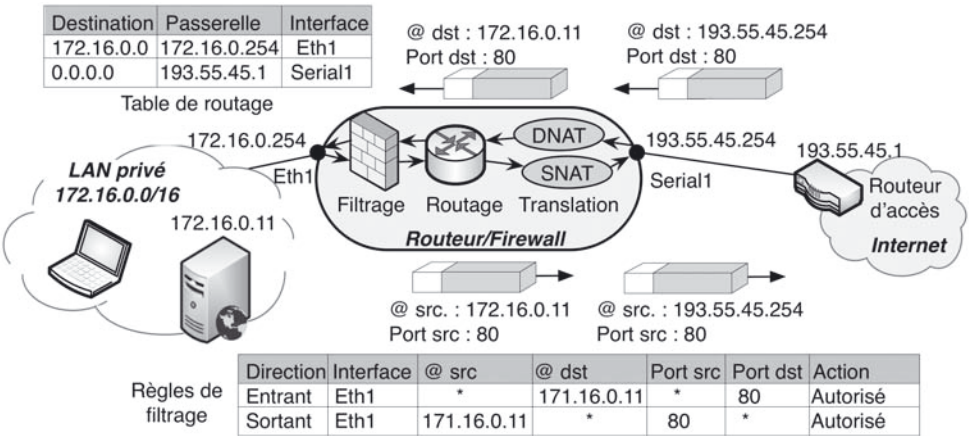


Figure 9.6 – NAT, routage et *firewall*.

À la manière d'une zone franche au-delà de la frontière, la DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire. Comme un réseau privé, elle est isolée par un firewall mais avec des règles de filtrage moins contraignantes.

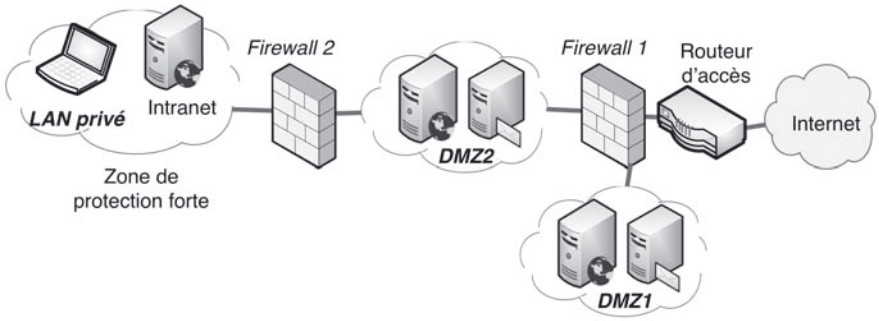


Figure 9.7 – DMZ simple et DMZ en sandwich.

Un niveau supplémentaire de sécurité peut être introduit avec un deuxième *firewall*. Les règles d'accès sur le *firewall* du réseau local privé sont plus restrictives. La DMZ est située entre les deux *firewalls* (DMZ « en sandwich ») avec des règles moins restrictives introduites par le premier *firewall* (DMZ2 sur la figure 9.7).

9.3.4 Les *proxys*

Un système mandataire (*proxy*) repose sur un accès à l'Internet par une machine dédiée : le serveur mandataire ou *proxy server*, qui joue le rôle de mandataire pour les autres machines locales et exécute les requêtes pour le compte de ces dernières (figure 9.8). Un serveur mandataire est configuré pour un ou plusieurs protocoles de

niveau applicatif (HTTP, FTP, SMTP…) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients…).

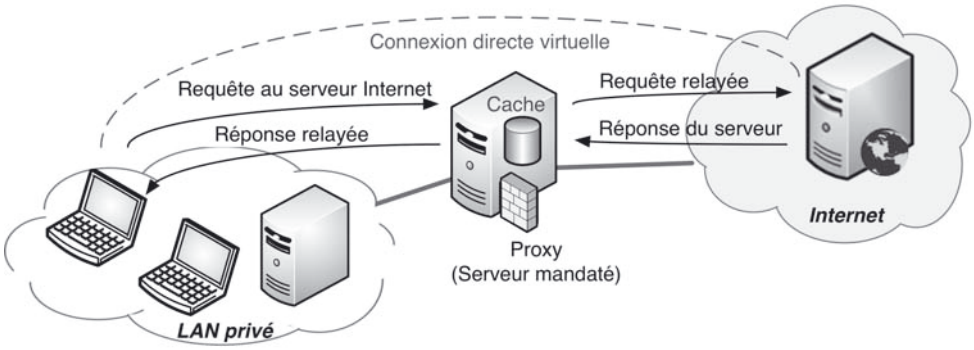


Figure 9.8 – Serveur mandataire.

Les serveurs mandataires configurés pour HTTP permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés (*proxy cache*).

9.3.5 Les VPN

Le réseau privé virtuel (VPN, *Virtual Private Network*) est un élément essentiel dans les architectures modernes de sécurité. Un VPN est constitué d'un ensemble de LAN privés reliés à travers Internet par un « tunnel » sécurisé dans lequel les données sont cryptées. Les postes distants faisant partie du même VPN communiquent de manière sécurisée comme s'ils étaient dans le même espace privé, mais celui-ci est virtuel car il ne correspond pas à une réalité physique. Cette solution permet d'utiliser les ressources de connexion de l'Internet plutôt que de mettre en place, comme par le passé, une liaison spécialisée privée entre deux sites qui peut être très coûteuse si les sites sont fortement éloignés. La principale contrainte du VPN est de sécuriser les transmissions, par nature exposées sur le réseau public Internet.

Ce mécanisme est illustré par la figure 9.9. Les PC des deux LAN et le PC nomade font partie du même VPN. Les communications passent par des passerelles matérielles ou logicielles chargées d'identifier les extrémités du tunnel, de crypter les données et de les encapsuler dans un nouveau paquet en gérant un double adressage privé et public.

Pour mieux comprendre le rôle des passerelles et la gestion des adresses, un exemple de communication à travers un tunnel VPN est donné sur la figure 9.10. Le transfert se déroule en quatre étapes :

- le PC1 (10.1.0.1) envoie un paquet vers le serveur web (10.2.0.2) comme il le ferait si ce dernier était sur le même LAN ;
- le routeur qui joue le rôle de passerelle VPN encrypte le paquet, ajoute l'en-tête VPN et un nouvel en-tête IP avec les adresses publiques et relaie le paquet ;

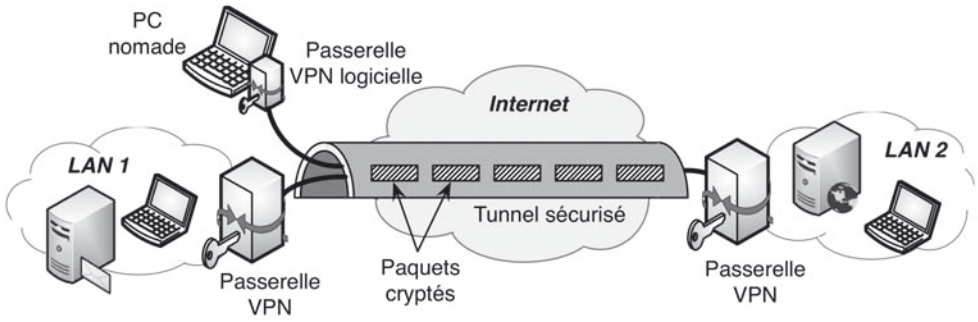


Figure 9.9 – **Principe du VPN.**

- à l'autre extrémité, le routeur/*firewall* reçoit le paquet, confirme l'identité de l'émetteur, confirme que le paquet n'a pas été modifié, décapsule et décrypte le paquet original ;
- le serveur web reçoit le paquet décrypté.

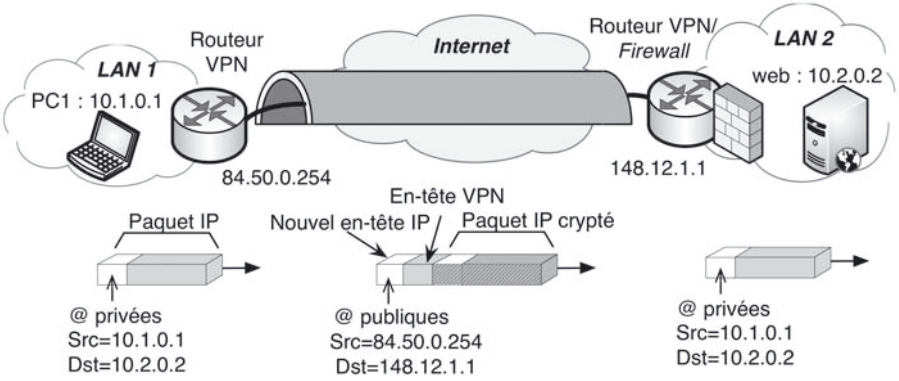


Figure 9.10 – **Exemple de transfert dans un VPN.**

Les protocoles utilisés pour crypter les données, encapsuler le paquet et gérer les authentifications sont décrits dans le § 9.5.

9.4 Les défenses logicielles

Tous les systèmes de défense utilisent des programmes ou des algorithmes pour gérer essentiellement l'authentification, le cryptage des données et la détection de *malwares*. Ces défenses logicielles sont mises en pace sur des architectures matérielles, par exemple l'authentification sur une liaison point à point pour se connecter à son FAI, le cryptage sur un tunnel VPN ou l'antivirus sur les postes de travail. Les paragraphes suivants décrivent les principes de base utilisés dans le cryptage et l'authentification.

9.4.1 Le cryptage

Le but de la cryptographie est de garantir la confidentialité, l'authenticité et l'intégrité des données échangées. Il existe à l'heure actuelle deux grands principes de chiffrement ou cryptage : le cryptage symétrique qui utilise une même clé partagée et le cryptage asymétrique qui utilise deux clés distinctes.

a) Cryptage symétrique

Il est basé sur l'utilisation d'une clé privée (ou algorithme) partagée entre les deux parties communicantes. La même clé sert à crypter et à décrypter les messages (figure 9.11). Ce type de chiffrement est efficace (des longueurs de clés de 64 ou 128 bits sont suffisantes), rapide et peu gourmand en puissance de calcul. La principale difficulté est de trouver un moyen sécurisé pour communiquer la clé aux deux entités.

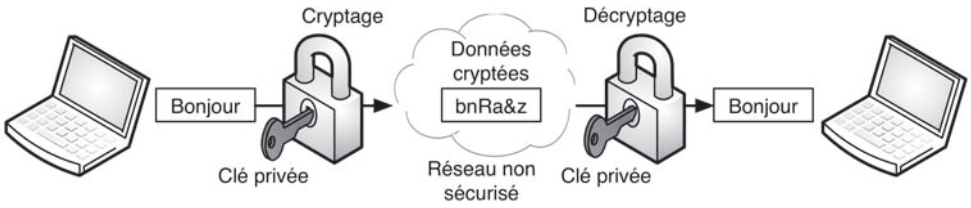


Figure 9.11 – Principe du chiffrement symétrique.

Les algorithmes de chiffrement symétrique les plus utilisés sont :

- DES (*Digital Encryption Standard*) : avec des clés de 64 bits seulement et la puissance de calcul actuelle, sa robustesse est mise en cause ;
- AES (*Advanced Encryption Standard*) : utilise des clés de 128 bits, le plus efficace aujourd'hui compte tenu des faibles ressources de calcul nécessaires.

b) Cryptage asymétrique

Le cryptage asymétrique utilise deux clés différentes pour chaque utilisateur :

- la première est privée et n'est connue que de l'utilisateur qui a généré les clés ;
- la deuxième est publique et peut être transmise sur Internet.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante et qu'il est impossible de déduire la clé privée à partir de la clé publique. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage (figure 9.12). Son principal avantage est qu'il résout en partie le problème du transfert de la clé mais en revanche, il est plus coûteux en termes de temps de calcul et nécessite des tailles de clé plus importantes (couramment 1 024 ou 2 048 bits).

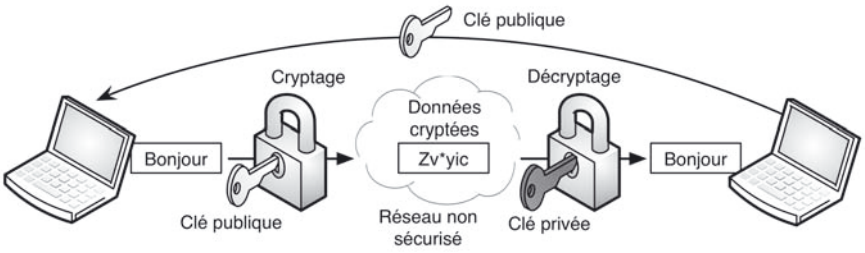


Figure 9.12 – Principe du chiffrement asymétrique.

L'algorithme de chiffrement asymétrique le plus courant est l'algorithme RSA (Rivest, Shamir, Adleman).

L'algorithme ElGamal, du nom de son créateur Taher Elgamal, est un algorithme asymétrique basé sur les logarithmes discrets. Il est également très utilisé pour le chiffrement et la signature.

Le programme complet de cryptographie à clé publique le plus connu est PGP (*Pretty Good Privacy*). Le format OpenPGP est le standard ouvert de cryptographie issu de PGP.

c) Échange de clé

Pour profiter de l'efficacité du chiffrement symétrique, il existe deux méthodes pour résoudre le problème de l'échange de clé symétrique :

- **l'échange de clé RSA** (figure 9.13), nommé ainsi car des clés asymétriques publique et privée utilisant cet algorithme servent à l'échange :
  - ◇ on chiffre le message avec une clé symétrique,
  - ◇ on chiffre la clé symétrique avec la clé publique du destinataire,
  - ◇ on joint la clé symétrique chiffrée au message,
  - ◇ le destinataire déchiffre la clé symétrique avec sa clé privée, puis le message avec la clé symétrique qu'il peut utiliser à son tour pour envoyer des messages chiffrés ;

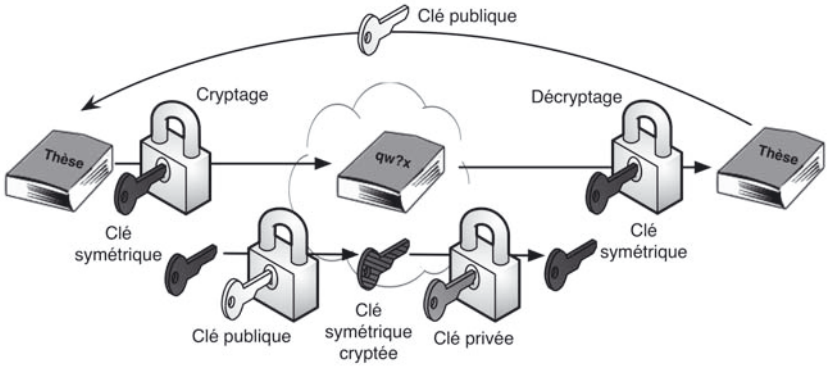


Figure 9.13 – Échange de clés RSA.

- (la principale faiblesse de cette méthode est que la clé symétrique cryptée est transmise sur le réseau et donc susceptible d'être interceptée et déchiffrée) ;
- **l'échange Diffie-Hellman** (notamment utilisé dans le protocole SSH, voir § 9.5) dans lequel la clé symétrique est générée par les deux extrémités sans qu'il ne soit nécessaire de la transmettre ; seules des valeurs calculées à partir d'un nombre aléatoire sont échangées. La figure 9.14 montre le principe de cet échange :
  - ◇ Alice et Bob ont choisi un groupe de nombres et une génératrice g de ce groupe,
  - ◇ Alice choisit un nombre au hasard a, élève g à la puissance a, et transmet g^a à Bob,
  - ◇ Bob fait de même avec le nombre b,
  - ◇ Alice, en élevant le nombre reçu de Bob à la puissance a, obtient g^{ba} et la clé K,
  - ◇ Bob fait le calcul analogue et obtient g^{ab}, et donc la même clé K :

$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$.

Il est très difficile d'inverser l'exponentiation dans un corps fini. Une personne malveillante sur le réseau (*MiM*, *Man in the Middle*) ne peut pas découvrir a et b, donc ne peut pas calculer g^{ab}.

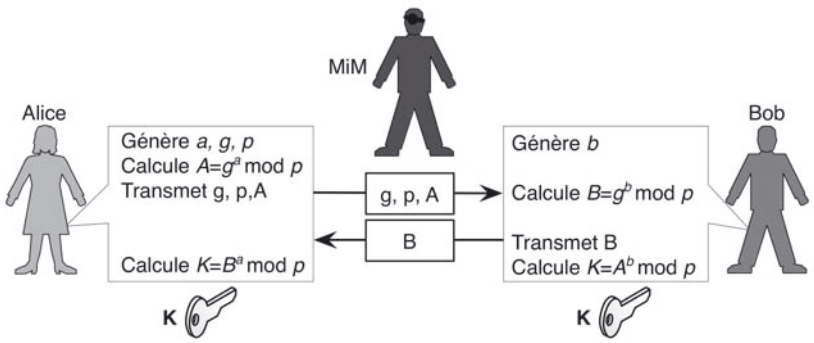


Figure 9.14 – **Principe de l'échange Diffie-Hellman.**

9.4.2 Le *hash*

Un algorithme de hachage est une fonction mathématique qui convertit une chaîne de caractères d'une longueur quelconque en une chaîne de caractères de taille fixe appelée empreinte ou *hash* ou encore *digest*. Cette fonction possède deux propriétés essentielles (figure 9.15) :

- elle est irréversible : il est impossible de retrouver le message lorsqu'on connaît le *hash* ;
- elle est résistante aux collisions : deux messages différents ne produiront jamais (en théorie) le même *hash*.

Ce type de fonction cryptographique est donc conçu de façon qu'une modification même infime du message initial entraîne une modification du *hash*. Si un message

est transmis avec son *hash*, le destinataire peut vérifier son intégrité en recalculant son *hash* et en le comparant avec le *hash* reçu.

Les algorithmes de hachage les plus utilisés sont : MD5 (*Message Digest*) sur 128 bits et SHA-1 (*Secure Hash Algorithm*) sur 160 bits.

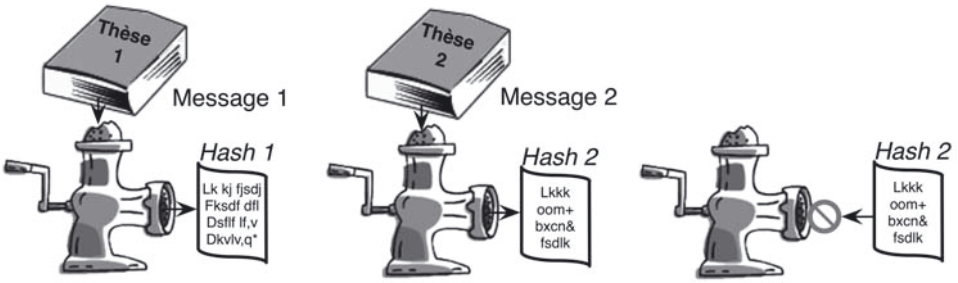


Figure 9.15 – **Propriétés du *hash*.**

9.4.3 La signature

La signature par chiffrement est l'équivalent électronique de la signature physique des documents papiers. Elle garantit l'authenticité de l'expéditeur et l'intégrité du message reçu. Pour signer électroniquement un message, il suffit de le chiffrer avec la clé privée. Le déchiffrement avec la clé publique correspondante prouve que seul le détenteur de la clé privée a pu créer la signature. Il est bien entendu nécessaire que le signataire du message ait transmis au préalable la clé publique au destinataire qui vérifie la signature. Par ailleurs, il n'est pas nécessaire de chiffrer tout un document pour le signer, il suffit de chiffrer son *hash*. Le destinataire pourra calculer à son tour le *hash* avec le même algorithme (le document aura aussi été transmis) et comparer avec le *hash* reçu et déchiffré (figure 9.16). La résistance aux collisions de la fonction de hachage permet de garantir que c'est bien ce document qui a été signé.

L'algorithme DSA (*Digital Signature Algorithm*) proche de RSA est souvent utilisé pour générer une signature.

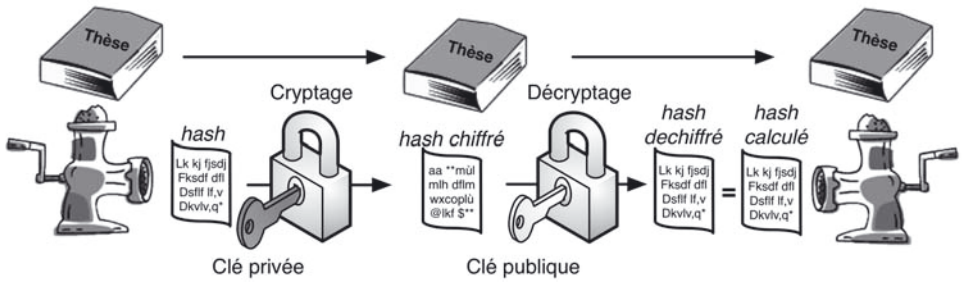


Figure 9.16 – **Signature par le *hash*.**

9.4.4 L'authentification

Une autre méthode pour s'assurer de l'identité de l'expéditeur est d'utiliser un chiffrement symétrique pour chiffrer le *hash.* Dans ce cas, il s'agit d'une authentification et non d'une signature. La clé symétrique utilisée pour vérifier le *hash* permet aussi de le créer. Si cette clé n'est connue que par les deux partenaires, alors elle permet d'authentifier l'expéditeur du message.

Pratiquement, la clé n'est pas utilisée directement pour chiffrer le *hash* mais elle intervient lors du calcul du *hash* (figure 9.17). Un *hash* ainsi généré est appelé un MAC (*Message Authentication Code*). Les algorithmes de hachage classiques sont utilisés : HMAC-SHA et HMAC-MD5.

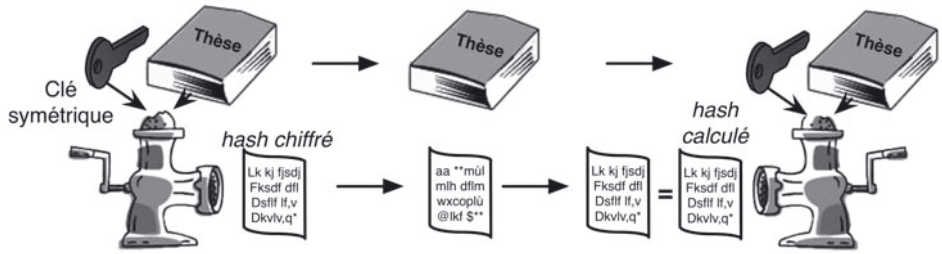


Figure 9.17 – Authentification par le *hash*.

9.4.5 Les certificats

a) Intérêt des certificats

La transmission de clés publiques peut être sujette à l'interception sur le réseau par le « MiM ». Celui-ci peut intercepter la clé publique, transmettre une fausse clé publique à l'expéditeur, déchiffrer avec sa fausse clé privée correspondante les messages envoyés par l'expéditeur et les retransmettre au destinataire après les avoir éventuellement modifiés (figure 9.18).

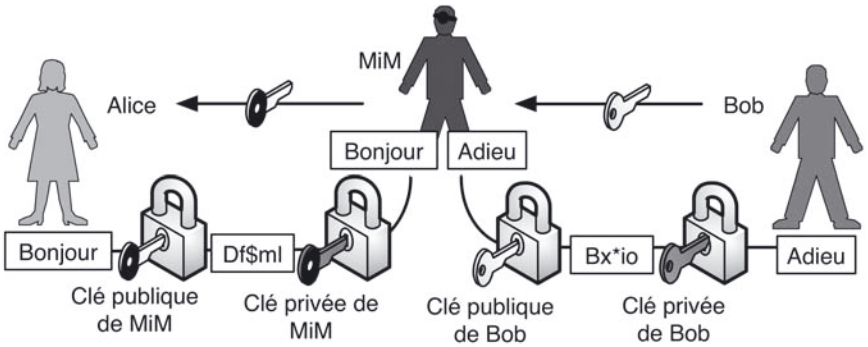


Figure 9.18 – Attaque de type *Man in the Middle*.

Pour garantir l'origine d'une clé publique, l'une des solutions est d'utiliser un certificat fourni en même temps que la clé. Le certificat réalise donc l'association d'une clé publique à une entité (personne, machine…) afin d'en assurer la validité. Il est bien entendu nécessaire que le certificat provienne d'un tiers de confiance. C'est le mécanisme de signature qui est utilisé pour garantir l'identité de ce tiers.

La figure 9.19 illustre ce principe. Bob ne transmet pas directement sa clé publique à Alice. Il la transmet d'abord à Trent (1), le tiers de confiance. Ce dernier dispose lui aussi d'une paire de clés asymétriques, il utilise sa clé privée pour signer le certificat contenant la clé publique de Bob (2) et lui transmet celui-ci (3). Bob peut alors envoyer le certificat signé à Alice (5). Celle-ci, qui a également reçu la clé publique de Trent (4), peut vérifier la signature et être sûre que la clé publique provient bien de Bob. Ce mécanisme de certification n'élimine pas complètement les risques : le MiM peut toujours intercepter le certificat ou la clé publique de Trent mais même s'il intercepte ces deux informations, il ne pourra générer un faux certificat sans la clé privée de Trent.

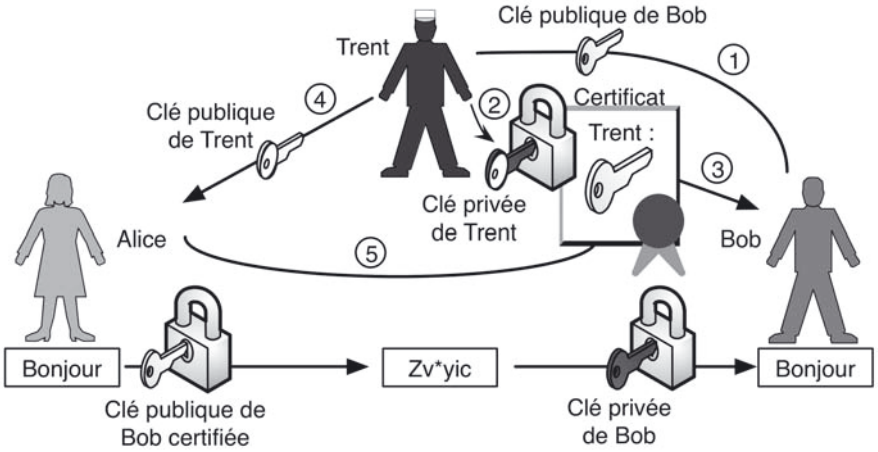


Figure 9.19 – Principe de certification d'une clé publique.

b) Les certificats sur Internet

La génération et la distribution sur Internet des certificats sont organisées autour d'infrastructures à clé publique (PKI, *Public Key Infrastructure*). Une PKI est constituée des éléments suivants (figure 9.20) :

- une autorité d'enregistrement ou RA (*Register Authority*) qui a pour rôle d'authentifier chaque nouveau participant. Ce dernier peut alors générer par son intermédiaire une paire de clés publique/privée ;
- une autorité de certification ou CA (*Certification Authority*) qui crée et signe les certificats avec l'identité du participant, sa clé publique, une date d'expiration et sa propre signature. Elle fournit une copie de sa propre clé publique au participant. Muni de son certificat et de la clé publique de la CA, le nouveau participant

peut communiquer avec tous les autres participants certifiés par la même CA. La RA peut être intégrée à la CA ;

- des annuaires de certificats.

Le cas d'utilisation le plus courant est la connexion à un site bancaire ou marchand à partir de son navigateur. Ce site doit être certifié par une CA. Les clés publiques des principales CA sont donc mémorisées (et éventuellement révoquées) dans les navigateurs et ne nécessitent pas d'installation spécifique de la part des usagers.

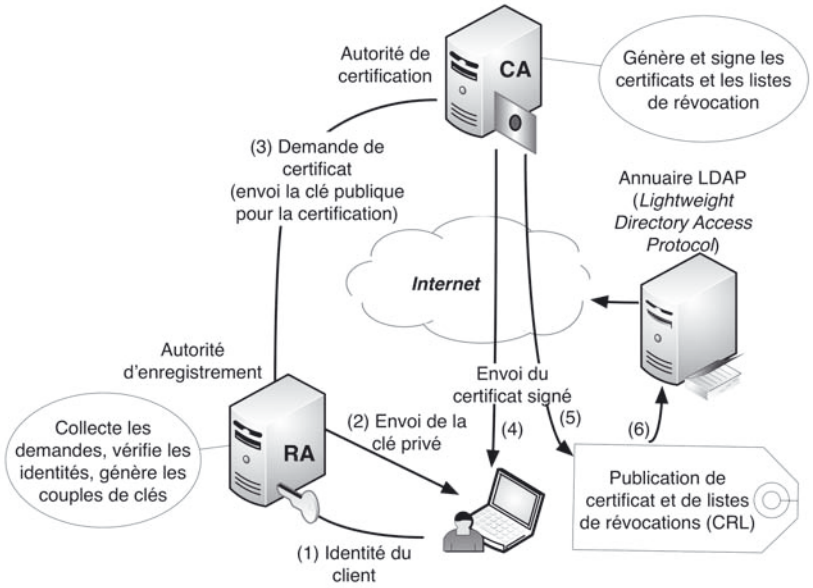


Figure 9.20 – Architecture d'une PKI.

La plupart des certificats couramment utilisés sur Internet sont au format X.509 qui est une norme de cryptographie de l'UIT (Union Internationale des Télécommunications), dédiée aux PKI. Ce fichier transmis par la CA sur l'ordinateur du client contient la clé publique de l'utilisateur et la signature de la CA ainsi que différents champs normalisés qui donnent l'identité de l'émetteur (CA), les dates de validité et les algorithmes de cryptage utilisés pour la clé publique et la signature (figure 9.21).

Précisons que la signature est réalisée par *hash* de tous les champs précédents du certificat et un chiffrement de ce hash par la clé privée de la CA. Tout utilisateur possédant la clé publique de cette CA peut déchiffrer le *hash* et le comparer au calcul de son propre *hash* du certificat.

9.5 Les protocoles de sécurité

Les protocoles qui utilisent les principes de cryptage, d'authentification ou de certification décrits dans le paragraphe précédent permettent de mettre en place des solutions de sécurité pour différentes architectures de réseau et en intervenant à

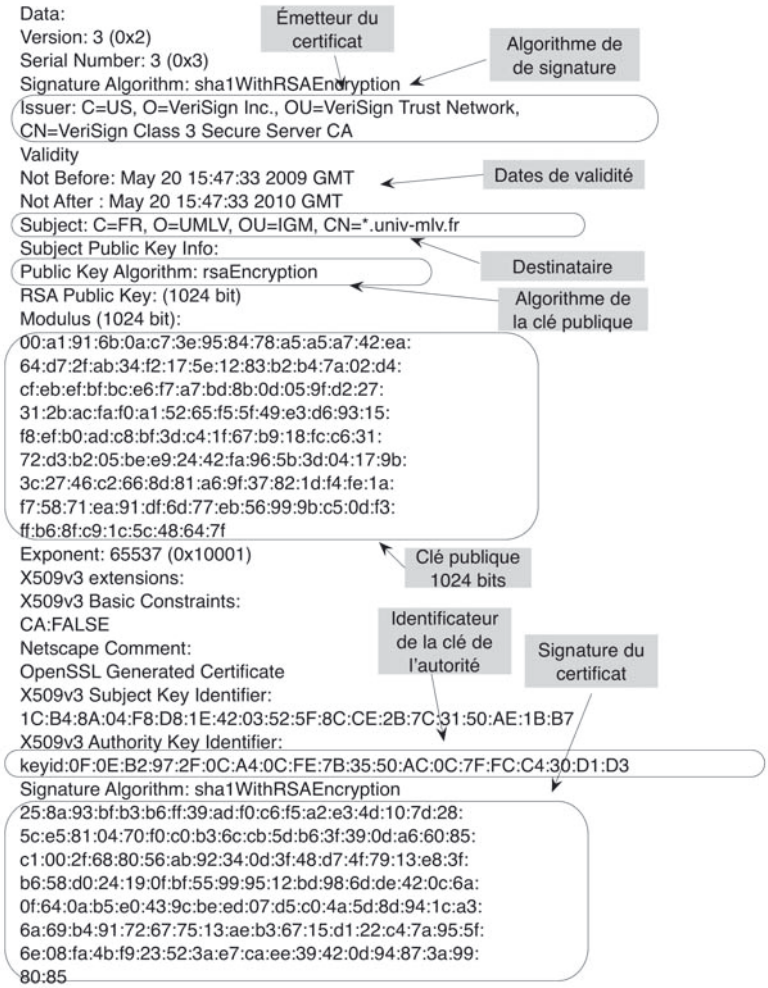


Figure 9.21 – Exemple de certificat X509.

différents niveaux du modèle OSI. Certains protocoles concernent les VPN avec du cryptage aux niveaux 2 ou 3, d'autres sont utilisés pour sécuriser les applications en cryptant toutes les données encapsulées au niveau 7, d'autres encore sont dédiés à l'authentification de l'utilisateur externe lors de l'accès à un réseau privé.

9.5.1 Protocoles pour les tunnels VPN

Au niveau 2, les deux protocoles les plus utilisés pour mettre en place un tunnel VPN sont **PPTP** (*Point to Point Tunneling Protocol* – RFC 2637) proposé au départ par Microsoft et **L2TP** (*Layer 2 Tunneling Protocol* – RFC 2661) normalisé par l'IETF (*Internet Engineering Task Force*) et qui est le résultat de la fusion du protocole L2F (*Layer 2 Forwarding*) de Cisco et de PPTP.

Au niveau 3, **IPSec** (*IP Security* - RFC 2401) défini par l'IETF permet de sécuriser les paquets IP et de créer un tunnel sur la couche réseau.

Aux niveaux supérieurs, **SSL/TLS** (*Secure Socket Layer/Transport Layer Security* – RFC 2246) et **SSH** (*Secure Shell* - RFC 2401) permettent de chiffrer les messages encapsulés dans des segments TCP et donc de créer indirectement des VPN de niveau 7.

a) PPTP

La méthode standard pour accéder à distance à un réseau non sécurisé, par exemple à l'Internet *via* son FAI, est de se connecter par un modem à un serveur d'accès distant ou *Remote Access Server* (RAS) à l'aide du protocole PPP (voir § 8.6).

Dans le cas d'un VPN, le serveur RAS devient une passerelle VPN à laquelle on accède par le protocole PPTP (*Point to Point Tunneling Protocol*). Le rôle de PPTP est donc de chiffrer et d'encapsuler, en les faisant passer par un tunnel crypté, les datagrammes IP dans le cadre d'une connexion point à point (figure 9.22).

Une trame PPTP est constituée :

- du datagramme IP contenant les données utiles et les adresses IP de bout en bout ;
- de l'en-tête PPP nécessaire pour toute connexion point à point ;
- d'un en-tête GRE (*Generic Routing Encapsulation*) qui gère l'encapsulation et permet d'isoler les flux IP privé et public ;
- d'un nouvel en-tête IP contenant les adresses IP source et destination des passerelles VPN (client et serveur VPN).

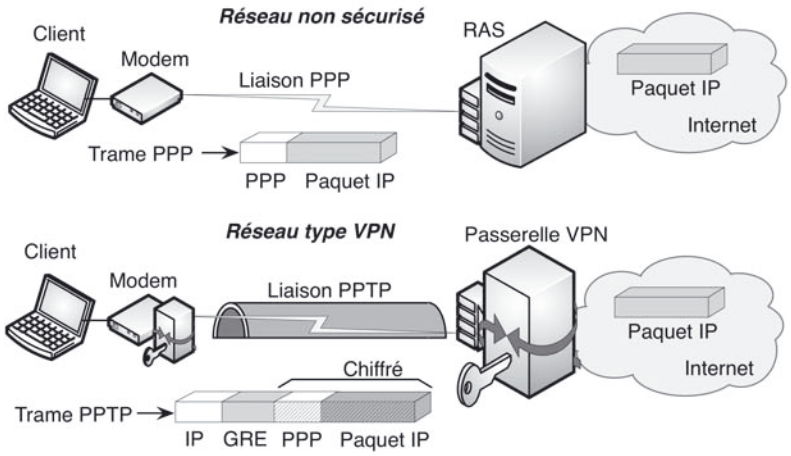


Figure 9.22 – Architectures PPP et PPTP.

Avant d'établir le tunnel GRE, une connexion TCP sur le port 1723 est réalisée. Elle intègre la négociation des paramètres et l'authentification de l'utilisateur.

L'un des points faibles de PPTP est que toute la partie négociation de la connexion n'est pas protégée. Par ailleurs, de nombreuses implémentations de ce protocole,

notamment celles de Microsoft, ont fait l'objet de découvertes de vulnérabilités et d'incapacité à protéger efficacement les mots de passe des utilisateurs. Ce mécanisme offre par conséquent une authentification moins fiable que celle proposée par IPSec.

b) IPSec

Ce protocole, lié à IPV4 et IPV6 et essentiellement employé dans les VPN, assure l'authentification et l'encryptage des paquets IP au travers de l'Internet. Il intervient donc au niveau 3.

IPSec peut être utilisé pour ne faire que de l'authentification : dans ce cas, l'ajout d'un en-tête d'authentification **AH** (*Authentication Header*) permet de vérifier l'authenticité et l'intégrité des paquets (figure 9.23). AH ne spécifie pas d'algorithme de signature particulier mais MD5 et SHA-1 sont les plus utilisés.

Dans la plupart des applications IPSec, l'enveloppe **ESP** (*Encapsulated Security Payload*) qui permet de chiffrer et d'authentifier les paquets est utilisée (figure 9.23).

Le chiffrement ne porte que sur les données encapsulées et le *trailer*. Il ne porte pas sur les champs de l'en-tête et les données d'authentification. L'authentification optionnelle porte sur l'en-tête ESP et tout ce qui suit, mais pas sur l'en-tête IP. ESP ne spécifie pas d'algorithmes de signature ou de chiffrement particuliers, ceux-ci sont décrits séparément. Cependant, la plupart des implémentations supportent les algorithmes de chiffrement DES et les signatures à l'aide des fonctions de hachage MD5 et SHA-1.

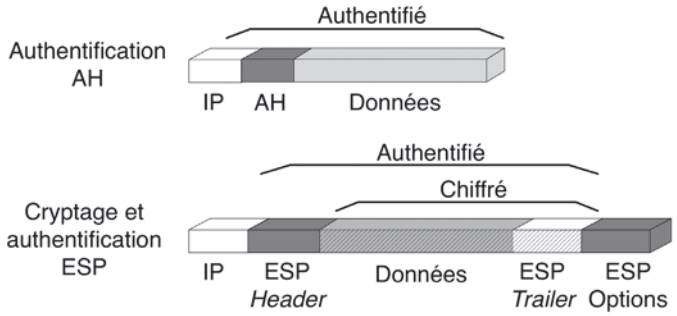


Figure 9.23 – Structure des paquets IPSec de type AH et ESP.

Par ailleurs, deux modes correspondant à deux architectures sont possibles avec IPSec (figure 9.24) :

- le mode **transport** qui ne protège (par authentification AH ou chiffrage ESP) que les données des paquets transmis ;
- le mode **tunnel** dans lequel le paquet entier est protégé (par authentification AH ou chiffrage ESP) en l'encapsulant dans un nouveau paquet IP.

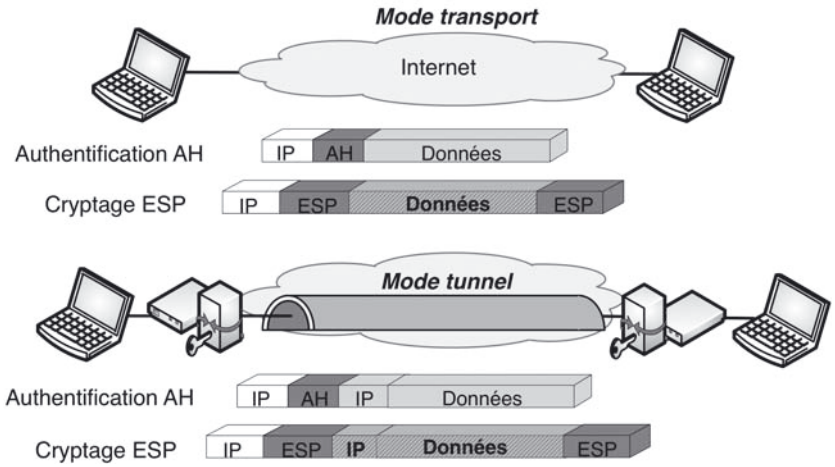


Figure 9.24 – Authentification et cryptage dans les deux modes IPSec.

Sur chaque système susceptible d'utiliser IPSec, une base de données nommée SPD (*Security Policy Database*) doit être présente. Sa forme précise est laissée au choix de l'implémentation ; elle permet de préciser la politique de sécurité à appliquer au système. Une communication protégée entre deux systèmes à l'aide d'IPSec est appelée une SA (*Security Association*). Une SA est une entrée de la SPD, c'est-à-dire un enregistrement contenant des paramètres de communication IPSec : algorithmes, types de clés, durée de validité, identité des partenaires.

Enfin, pour éviter d'avoir à gérer les clés de cryptage et d'authentification manuellement, IPSec intègre un protocole d'échange automatique de clé nommé IKE (*Internet Key Exchange*). Ce protocole utilisé dans la phase d'initialisation est chargé dans un premier temps de négocier une SA (paramètres des clés pour AH ou ESP) et ensuite de procéder à l'échange des clés choisies par l'intermédiaire de certificats X509 par exemple.

9.5.2. Protocoles pour sécuriser les applications

a) SSL/TLS

Le protocole **SSL** (*Secure Socket Layer*) a été proposé au départ par Netscape (jusqu'à la version 2.0) pour permettre des connexions sécurisées sur des serveurs web. La version 3.0 (actuellement la plus répandue) est standardisée par l'IETF.

TLS (*Transport Layer Security*), proposé par l'IETF, est la version 3.1 de SSL. Le protocole TLS est défini dans la RFC 2246 et n'impose pas de méthodes de chiffrement spécifiques.

SSL intervient au-dessus de la couche transport (figure 9.25) et peut être utilisé pour sécuriser pratiquement n'importe quel protocole utilisant TCP/IP (SMTP, POP3, IMAP…) en créant un tunnel dans lequel toutes les données échangées seront

automatiquement chiffrées. Certains protocoles applicatifs ont été spécialement adaptés pour supporter SSL :

- HTTPS (HTTP+SSL) est inclus dans tous les navigateurs et permet par exemple de consulter des comptes bancaires par le web de façon sécurisée ;
- FTPS est une extension de FTP utilisant SSL.

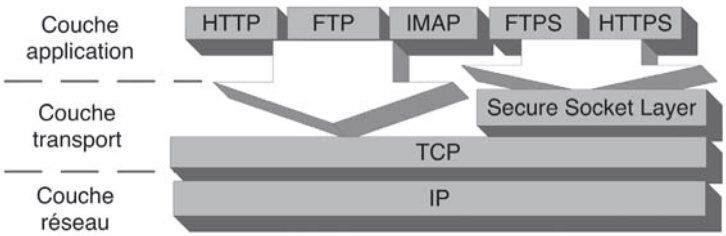


Figure 9.25 – SSL dans le modèle OSI.

Plus précisément, le protocole SSL/TLS utilise un cryptage asymétrique par clé publique/clé privée pour authentifier le serveur (et éventuellement le client) ainsi que pour échanger la clé maîtresse. Celle-ci, connue des deux extrémités, permet un cryptage symétrique efficace des données pendant toute la durée de la session. Les différentes phases permettant l'authentification et la génération de la clé maîtresse et donc la création du tunnel sécurisé sont décrites sur la figure 9.26 :

- après établissement de la connexion TCP sur le port 443, un premier dialogue permet de choisir la version SSL et les types de cryptage qui seront utilisés ;
- au cours de ce dialogue, le serveur envoie au client un certificat X509 qui contient la clé publique du serveur (PK : *Public Key*) signée par une autorité de certification (CA) ; l'usage du certificat n'est pas obligatoire mais est couramment réalisé ;
- le client vérifie le certificat, génère une pré-clé maîtresse PMK (*Primary Master Key*) et calcule la clé maîtresse MK à partir de PMK. Le client se sert de PK pour crypter PMK et transmet PMK cryptée au serveur avec un message indiquant que le chiffrage est effectif côté client (*Change Cipher Spec*) ;
- le serveur reçoit PMK, la décrypte avec sa clé privée, calcule à son tour MK et indique que le chiffrage est effectif (*Change Cipher Spec*) ;
- le tunnel sécurisé est créé, toutes les données applicatives seront cryptées et décryptées avec la clé symétrique MK.

  Pour sécuriser davantage, un certificat peut aussi être installé sur le client.

b) SSH

L'environnement **SSH** (*Secure Shell*) s'adresse aux utilisateurs qui souhaitent accéder de manière sécurisée à des systèmes Linux distants. Ses composants remplacent des programmes peu sécurisés comme *telnet* pour établir à partir d'un terminal une session sur un serveur ou FTP pour les échanges de fichiers. La sécurité est

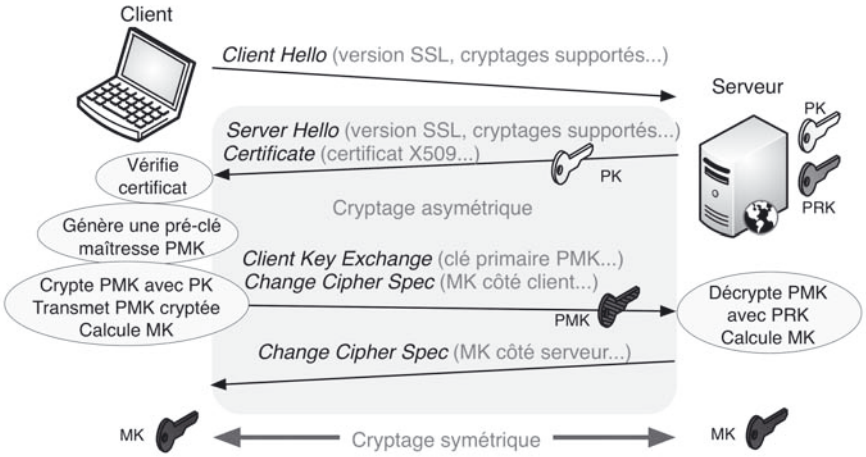


Figure 9.26 – Échange SSL/TLS avec certificat.

garantie par une authentification à l'établissement de chaque connexion et par l'encryptage des données (y compris les mots de passe).

SSH intervient donc au **niveau 7**, la connexion TCP est établie sur le port 22. Une connexion SSH peut également être utilisée pour transporter un autre protocole, par exemple SMTP. Il s'agit alors de la **redirection de port**. Le modèle en couches n'est pas respecté mais le tunnel sécurisé dans lequel les communications sont chiffrées permet, comme pour SSL, d'encapsuler n'importe quel dialogue applicatif.

Deux protocoles de transfert ont été prévus pour fonctionner avec une connexion SSH :

- SCP (*Secure CoPy*), utilisé généralement en mode commande, permet de télécharger des fichiers de manière sécurisée dans un tunnel SSH ;
- SFTP, version SSH de FTP, peut également être utilisé pour les transferts de fichiers. SFTP ne nécessite pas de clients ou de serveur FTP puisque le transfert se fait par le « *shell* ».

Les différentes phases permettant l'authentification et la création de la connexion sécurisée SSH sont décrites à la figure 9.27 (l'échange de clé Diffie-Hellman est détaillé dans le § 9.4.1) :

- dès que la connexion TCP est établie sur le port 22 du serveur, le client et le serveur se mettent d'accord sur la version SSH ;
- suit la phase d'initialisation de SSH qui consiste à mettre en place le tunnel sécurisé : le client et le serveur s'envoient la liste des méthodes supportées pour le chiffrement et l'authentification (messages *Key EXchange Init*) ;
- le client demande un échange de clé de type Diffie-Hellman (*DH GEX Request pour DH Group EXchange Request*) ;
- le serveur choisit deux nombres g et p et les transmet au client (*DH Key Exchange Reply*) ;
- le client génère un nombre aléatoire a, calcule $A = g^a \bmod p$ et transmet A (*DH GEX Init*) ;

- le serveur génère b, calcule $B = g^b \bmod p$ et la clé de session $K = A^b \bmod p$. Le serveur calcule également un *hash* H à partir d'un maximum d'informations partagées avec le client, il signe H avec sa clé privée RSa. Il transmet B, la signature s de H et la clé publique RSA *Host Key* (*DH GEX Reply*) ;
- le client décrypte s avec la clé publique reçue et compare le résultat avec son propre calcul de H. Ce mécanisme évite d'avoir recours à un certificat. Le client qui a ainsi vérifié l'authenticité du serveur peut alors calculer à son tour $K=B^a \bmod p$;
- après confirmation du client (*New Key*), le reste des communications est chiffré grâce à un algorithme de chiffrement symétrique utilisant la clé de session K partagée par le client et le serveur.

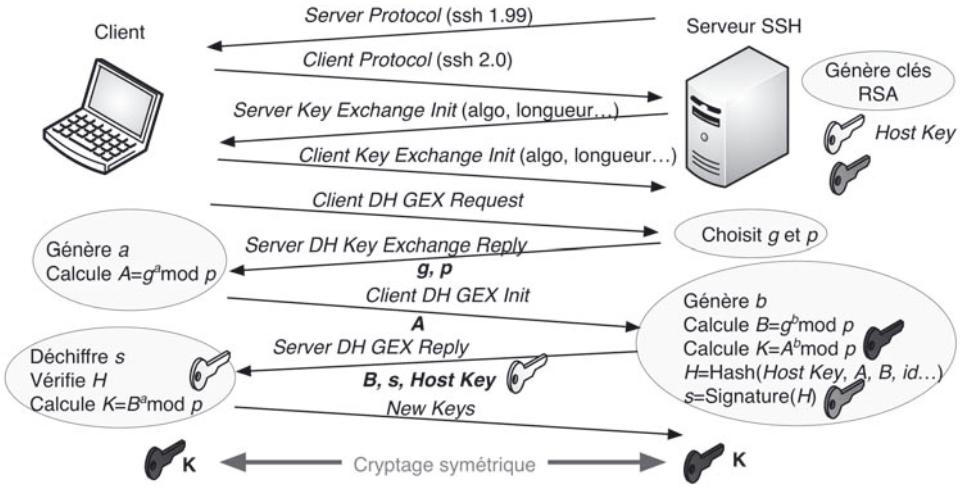


Figure 9.27 – **Échange SSH.**

9.5.3. Protocoles pour l'authentification sur un réseau

Beaucoup de protocoles et leurs variantes existent pour authentifier un utilisateur lorsqu'il cherche à se connecter sur un réseau par une connexion distante ou locale. Dans le cadre d'une connexion distante point à point vers son FAI par exemple, le protocole PPP définit une méthode d'authentification de type CHAP (*Challenge Handshake Authentication Protocol*). Pour une authentification sur un réseau local privé, éventuellement avec une connexion sans fil, le standard IEEE 802.1x et ses nombreuses déclinaisons sont considérés comme les plus sécurisés à l'heure actuelle.

a) CHAP et MS-CHAP

Le protocole **CHAP** est un protocole simple et faiblement sécurisé d'authentification à distance par une liaison PPP, il est défini dans la RFC 1994. L'authentification se déroule en trois temps (figure 9.28) :

- le serveur commence par envoyer un « défi » au client (16 octets aléatoires), ainsi qu'un compteur qu'il incrémente à chaque défi ;

- le client doit alors passer le compteur, son mot de passe et le défi au travers d'un algorithme de hachage MD5 pour délivrer un *hash* sur 16 octets ;
- le *hash* est envoyé au serveur, qui peut alors effectuer le même calcul et vérifier si son résultat concorde avec celui du client.

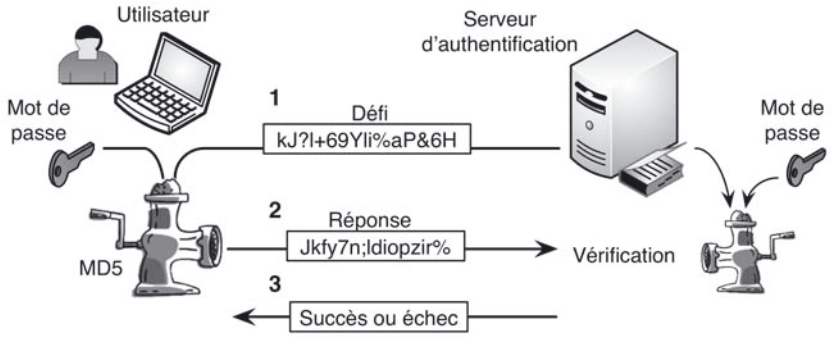


Figure 9.28 – Principe d'une authentification CHAP.

Cet algorithme permet d'éviter que le mot de passe ne soit transféré et évite également qu'un pirate ne répète simplement une authentification réussie qu'il aurait enregistrée auparavant, puisque le défi change à chaque authentification. Il ne permet cependant pas au client de s'assurer de l'identité du serveur. L'autre point faible de CHAP est le stockage en clair des mots de passe dans la base de données des utilisateurs située sur le serveur d'authentification.

Des améliorations de CHAP ont été proposées notamment par Microsoft (MS-CHAP v1 puis MS-CHAP v2) mais ce protocole reste vulnérable face à des attaques hors ligne de type dictionnaire.

b) 802.1x/EAP

Pour compenser les faiblesses de MS-CHAP et pour proposer aux FAI d'autres méthodes d'authentification que par le mot de passe (carte à puce, certificats électroniques…), l'IEEE a proposé en 2001 le standard **802.1x** (RFC 3580). Il permet d'authentifier un utilisateur souhaitant accéder à un réseau distant ou local, filaire ou sans fil, grâce à un serveur d'authentification.

Le standard 802.1x repose sur le protocole **EAP** (*Extensible Authentication Protocol*) défini par l'IETF. Son rôle est de transporter les informations d'authentification des utilisateurs. C'est donc un protocole de transport qui doit être associé à un protocole d'authentification comme MS-CHAP ou TLS par exemple. Il est extensible dans la mesure où d'autres protocoles d'authentification que ceux prévus au départ peuvent être associés.

L'architecture d'EAP est décrite sur la figure 9.29 :

- le client nommé *Supplicant* cherche à établir une connexion, éventuellement sur une liaison WiFi, vers le réseau privé ;

- le contrôleur d'accès (NAS, *Network Access Server* ou *Authenticator*) est chargé d'établir ou non l'accès au réseau pour un client. Le NAS est un simple garde-barrière servant d'intermédiaire entre le client et un serveur d'authentification. Dans le cas d'un réseau sans fil, le point d'accès (AP, *Access Point*) peut jouer le rôle de contrôleur d'accès ;
- le serveur d'authentification (AS, *Authentication Server*) permet de valider l'identité de l'utilisateur, et de lui renvoyer les droits associés en fonction des informations d'identification fournies. L'AS est généralement un serveur RADIUS (*Remote Authentication Dial In User Service*), serveur d'authentification standard défini par les RFC 2865 et 2866.

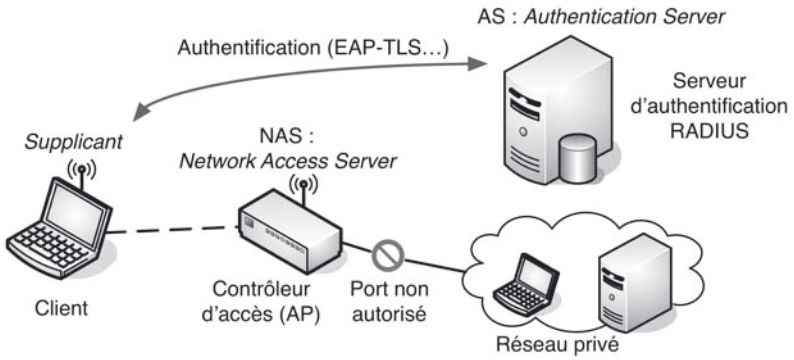


Figure 9.29 – Architecture EAP/802.1x.

AP peut être utilisé sur un réseau WiFi ou dans de multiples contextes. Le fait que le contrôleur d'accès ne soit qu'un intermédiaire entre le client et le serveur est l'un des grands intérêts de l'EAP :

- il n'a pas besoin de comprendre l'échange entre le client et l'AS, seul le résultat transmis par l'AS (succès ou échec de l'authentification) lui indique s'il doit ouvrir ou laisser fermé le port d'accès au réseau ;
- pour une nouvelle méthode d'authentification, seuls les clients et le serveur d'authentification devront être mis à jour.

Le protocole 802.1x définit comment EAP peut être utilisé sur un LAN ou un WLAN grâce au protocole EAPoL (EAP over LAN). EAPoL est utilisé entre le client et le NAS : les messages EAP qui transportent des données d'authentification sont encapsulés dans des paquets EAPoL, eux-mêmes encapsulés dans des trames Ethernet (802.3) ou WiFi (802.11). Entre le NAS et le serveur RADIUS, les messages EAP sont généralement encapsulés dans des paquets RADIUS (figure 9.30).

Les méthodes d'authentification supportées de base par EAP sont les suivantes :

- EAP/MD5 est basée sur le protocole CHAP associé à un algorithme de hachage MD5 ;
- EAP MS-CHAP-v2 est basée sur la dernière version CHAP de Microsoft ;
- EAP/OTP (*One Time Password*) est basée sur l'utilisation unique d'un mot de passe non nécessairement crypté ;

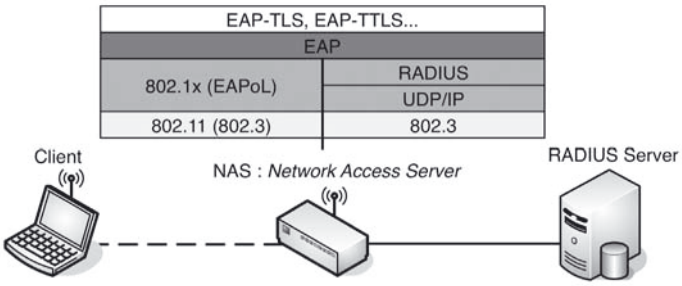


Figure 9.30 – Encapsulations EAP.

- EAP/SIM permet à un utilisateur de s'identifier grâce la carte SIM de son téléphone portable ;
- EAP/TLS utilise le mécanisme d'authentification par certificat proposé par SSL/TLS, le tunnel TLS n'est pas utilisé ;
- EAP/PEAP (*Protected EAP*) utilise une méthode d'authentification, CHAP/MD5 par exemple, à l'intérieur d'un tunnel TLS ;
- EAP/TTLS (*Tuneled TLS*) réalise également une authentification dans un tunnel TLS avec davantage de méthodes d'authentification possibles.

Les plus utilisées sont les deux dernières dans la mesure où elles permettent une authentification du client à l'intérieur d'un tunnel sécurisé.

Résumé

- Pour limiter les vulnérabilités d'un réseau privé et préserver l'information qui est au cœur, la sécurité informatique vise trois objectifs principaux : **l'intégrité**, **la confidentialité** et **la disponibilité**. Les attaques sont généralement classées en deux catégories : les techniques d'**intrusion** (écoute du réseau, ingénierie sociale, détournement ou altération de messages, injection de code malveillant) et les **dénis de service** (inondation d'une machine ou DDOS).
- Les **défenses matérielles** interviennent sur le support stockant l'information, sur les médias servant à transporter cette information et sur les équipements intermédiaires traversés lors du transport. Parmi ces défenses, nous trouvons les ***firewalls*** chargés principalement de filtrer les paquets entrants sur le réseau privé, les **NAT** pour masquer les adresses internes de l'extérieur, les **DMZ** pour isoler une partie du réseau privé, les ***Proxys*** pour centraliser tous les accès vers l'extérieur et les **VPN** qui permettent de réaliser un tunnel sécurisé entre des réseaux privés distants.
- Tous les systèmes de défense utilisent de plus des programmes ou des algorithmes pour gérer l'authentification, le cryptage des données et la détection de *malware*. Les algorithmes de **cryptage symétrique et asymétrique** sont souvent combinés pour offrir les avantages des deux : l'efficacité du chiffrement pour le premier et une solution au problème de l'échange de clés pour le deuxième. Les algorithmes de **hachage** sont utilisés, en association avec le cryptage, pour réaliser des **authentifications** ou des **signatures**.

- Pour garantir la provenance d'une clé publique de cryptage ou pour garantir l'authenticité d'un serveur ou d'un client, un **certificat** délivré par une autorité de certification ou **CA** est souvent utilisé. Sur Internet, la génération et la distribution des certificats sont organisées autour d'infrastructures à clé publique, des **PKI**.
- Les protocoles qui utilisent les principes de cryptage, d'authentification ou de certification permettent de mettre en place des solutions de sécurité pour différentes architectures de réseau et en intervenant à différents niveaux du modèle OSI. Le protocole **PPTP** est utilisé pour gérer des VPN au niveau 2, **IPSec** met en place des VPN au niveau 3 en cryptant les paquets IP. Le protocole **SSL** intervient au niveau 4 pour mettre en place un tunnel qui permettra de sécuriser toutes les applications qui l'emprunteront. SSH qui intervient au niveau 7 permet d'ouvrir une session sécurisée vers un serveur Linux. Les protocoles **CHAP**, **MS-CHAP** et **802.1x/EAP** sont dédiés à l'authentification de l'utilisateur externe lors de l'accès à un réseau privé.

Exercices corrigés

QCM

Q9.1 Quelles attaques sont considérées comme des dénis de service ?

a) Le *spoofing* b) Le *flooding*

c) Les virus d) Le *phishing*

e) Le *spamming*

Q9.2 Le but du DNS *spoofing* est :

a) De falsifier l'adresse IP d'un utilisateur.

b) De rediriger un utilisateur vers un site falsifié.

c) De falsifier un serveur DNS.

Q9.3 Dans une attaque de type DDOS :

a) Une machine maître contrôle d'autres machines qui pourront réaliser une attaque distribuée sur la cible.

b) Une machine maître inonde des machines cibles à l'aide d'applications distribuées.

c) L'objectif est de paralyser la machine cible.

Q9.4 Le rôle d'un *firewall* est :

a) De créer des connexions sécurisées entre les machines internes et externes.

b) D'empêcher l'accès à certaines ressources du réseau interne.

c) De détecter les virus accompagnant les messages.

d) De filtrer les accès entre l'Internet et le réseau local.

Q9.5 Le tableau suivant représente un ensemble de règles de filtrage sur un *firewall*. Quelles affirmations sont vraies :

Règle	Direction	IP source	IP dest.	Protocole	Port source	Port dest.	ACK=1	Action
A	Entrant	Externe	Interne	TCP	>1023	21		Permission
B	Sortant	Interne	Externe	TCP	21	>1023		Permission
C	Sortant	Interne	Externe	TCP	>1023	21		Permission
D	Entrant	Externe	Interne	TCP	21	>1023	Oui	Permission
E	Toutes	Toutes	Toutes	Toute	Toute	Toute		Refus

Figure 9.31

a) Les transferts FTP vers un serveur interne sont toujours autorisés.

b) Les transferts FTP vers un serveur interne sont autorisés seulement si la connexion est initiée de l'extérieur.

c) Les transferts FTP vers un serveur externe sont toujours autorisés.

d) Les transferts FTP vers un serveur externe sont autorisés seulement si la connexion est initiée de l'intérieur.

e) Les transferts de courrier SMTP sont autorisés dans les deux sens.

Q9.6 La translation d'adresse (NAT) permet :

a) D'utiliser davantage d'adresses privées que d'adresses publiques disponibles sur un site.

b) De réaliser le routage des paquets vers le réseau privé.

c) De filtrer les adresses entrantes qui ne correspondent pas à une machine du réseau privé.

d) De masquer les adresses privées au reste de l'Internet.

Q9.7 Le rôle d'un système mandataire (*proxy*) est :

a) De relayer les requêtes des machines locales pour diverses applications sur Internet.

b) De centraliser les accès extérieurs pour sécuriser en un seul point les communications.

c) De filtrer les paquets en fonction de leur numéro de port.

d) D'enregistrer dans un cache les informations ou les fichiers fréquemment consultés.

Q9.8 Concernant les DMZ, quelles affirmations sont vraies ?

a) Une DMZ nécessite un *firewall*.

b) Les serveurs web sont toujours placés à l'extérieur d'une DMZ.

c) Lorsque plusieurs DMZ sont installées, la plus proche du réseau privé est la moins sécurisée.

d) Une DMZ sert de zone intermédiaire entre un réseau local et Internet.

Q9.9 Concernant un VPN, quelles affirmations sont exactes ?

a) Un tunnel sécurisé est créé entre deux sites distants.

b) Des passerelles sont nécessaires pour isoler les réseaux privés du réseau public.

c) Les paquets qui circulent sur Internet sont cryptés.

d) Les utilisateurs doivent crypter tous les messages qu'ils envoient.

Q9.10 En cryptographie, une fonction de *hashage* :

a) Est une fonction qui extrait d'un message long une empreinte courte.

b) Ne permet pas d'extraire la même empreinte à partir de deux messages différents.

c) Permet de chiffrer seulement l'empreinte plutôt que de chiffrer tout le message.

d) Permet de vérifier l'intégrité d'un message transmis.

Q9.11 Que contient un certificat ?

a) Une clé publique.

b) Une identité.

c) Une signature du certificat.

d) Une date d'expiration.

Q9.12 Le protocole SSH permet :

a) La navigation sécurisée sur les serveurs web.

b) Le transfert de fichiers cryptés vers un serveur FTP.

c) L'envoi de messages cryptés *via* un tunnel.

d) Une connexion distante sécurisée sur un serveur à partir d'un terminal.

Exercices

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

9.1 (*) Quels sont les deux grands types d'attaque ? À quels domaines de sécurité (intégrité, confidentialité, disponibilité) se rapportent ces deux types ?

9.2 (*) Quelle est la différence entre virus et vers ? Dans quelle mesure ces derniers sont-ils plus dangereux ?

9.3 (**) La règle A du *firewall* permet aux machines du LAN privé d'accéder à DMZ 2, alors que la règle C devait l'interdire. Comment remédier à cela ?

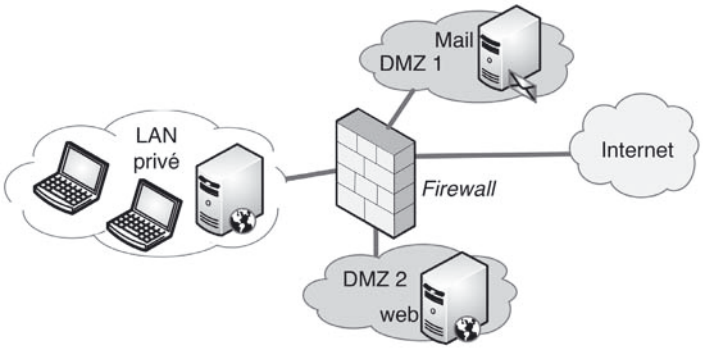


Figure 9.32

Tableau 9.2

Règle	@ src	@ dest.	Protocole	Port source	Port dest.	Action
A	Toutes	DMZ 2	TCP	Tous	80	Autorisé
B	LAN	DMZ 1	TCP	Tous	25	Autorisé
C	LAN	Toutes	TCP	Tous	Tous	Refusé
E	Tous	Tous	Tous	Tous	Tous	Refusé

9.4 (***) Un réseau sécurisé d'entreprise est décrit par la figure :

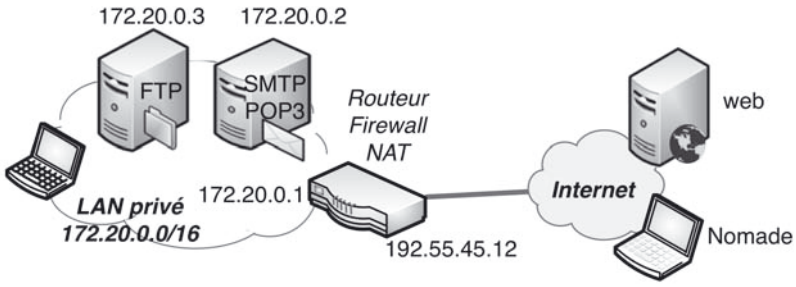


Figure 9.33

a) Écrire le tableau de règles du *firewall* permettant de ne laisser passer que les transferts de messagerie vers le serveur interne (protocoles SMTP et POP3) et de navigation vers l'extérieur (protocole HTTP). Dans ce dernier cas, la connexion devra obligatoirement être initiée de l'intérieur.

b) Le système de translation d'adresse (NAT) intégré au *firewall* utilise une adresse publique pour offrir un accès Internet aux stations et aux serveurs. Expliquer en quoi la translation d'adresse participe à la sécurisation du LAN privé. S'agit-il de DNAT ou de SNAT ?

c) D'après le schéma, quelle est l'adresse destination portée par un paquet entrant à destination du serveur SMTP ? Quelle information permet au routeur/NAT de savoir qu'il doit diriger ce paquet vers le serveur SMTP ?

9.5 (**) Vous utilisez un système de chiffrement asymétrique. Vous venez de perdre votre clé privée, mais vous avez encore la clé publique correspondante.

a) Pouvez-vous encore envoyer des mails de manière confidentielle ? Lire les mails chiffrés que vous recevez ?

b) Pouvez-vous encore signer les mails que vous envoyez ? Vérifier les signatures des mails que vous recevez ?

c) Que devez-vous faire pour de nouveau être capable d'effectuer toutes les opérations citées ?

9.6 (*) Les systèmes d'authentification standards vérifient les mots de passe à l'aide de *hashs* de mots de passe stockés dans des fichiers protégés.

a) Quelle est l'utilité de stocker les *hashs* des mots de passe plutôt que les mots de passe ?

b) Pourquoi doit-on protéger l'accès aux *hashs* des mots de passe ?

9.7 (**) Alice transmet un document à Bob. Ce document n'a pas besoin d'être chiffré mais Alice souhaite être sûre que Bob recevra le bon document et non un document qui pourrait être fourni par l'homme au milieu.

a) Comment Alice doit-elle procéder ? Vous donnerez, en les comparant, les deux solutions avec les deux types de cryptage. Vous préciserez ce qui distingue une signature d'une authentification.

b) Ces deux solutions sont-elles totalement sécurisées contre une attaque de l'homme au milieu ?

9.8 (**) Réseaux privés virtuels

a) Expliquez le concept et le fonctionnement d'un VPN. Vous préciserez en particulier les équipements mis en œuvre, la gestion des adresses IP et comment les messages sont encryptés.

b) Quelles sont les principales différences entre des tunnels VPN utilisant PPTP, IPSec et SSL ?

9.9 (***) Vous désirez avoir accès à distance à la messagerie interne de votre entreprise depuis votre portable. Donnez les avantages et les inconvénients des trois solutions suivantes :

a) Utilisation d'un client IPSec sur le portable pour établir une connexion VPN avec votre réseau interne.

b) Utilisation d'un client de messagerie supportant TLS pour faire du ESMTP et du POP3 sécurisé avec un serveur de messagerie dans la DMZ de votre entreprise.

c) Utilisation d'un navigateur standard pour accéder à une interface web de votre messagerie par HTTPS.

9.10 (**) Dans un paiement par carte bancaire sécurisé par le protocole https,

a) Comment le client est-il averti que la transaction est sécurisée ?

b) Comment le numéro de CB transmis est-il protégé ?

c) Quelle clé de cryptage le client utilise-t-il pour crypter les informations transmises ?

d) Comment le client est-il sûr qu'il dialogue bien avec le serveur choisi ?

e) Comment le serveur est-il sûr qu'il dialogue bien avec un client « légal » ?

Solutions

QCM

Q9.1 : b-c-e **Q9.2** : b-c **Q9.3** : a-c **Q9.4** : b-d **Q9.5** : a-d

Q9.6 : a-d **Q9.7** : a-b-d **Q9.8** : a-d **Q9.9** : a-b-c **Q9.10** : a-b-c-d

Q9.11 : a-b-c-d **Q9.12** : b-d

Exercices

9.1 Les deux grands types d'attaque sont l'intrusion et le déni de service (DoS). L'intrusion menace l'intégrité, la confidentialité et éventuellement la disponibilité dans le cas des vers ou des virus. Les DoS menacent la disponibilité.

9.2 Un virus est un programme qui se propage à l'aide d'un vecteur c'est-à-dire un autre programme. Un ver est un programme autonome. De par son autonomie, un ver aura plus de facilité à se propager.

9.3 Une solution est de passer la règle A en troisième position :

Tableau 9.3

Règle	@ src	@ dest.	Protocole	Port source	Port dest.	Action
B	LAN	DMZ 1	TCP	Tous	25	Autorisé
C	LAN	Toutes	TCP	Tous	Tous	Refusé
A	Toutes	DMZ 2	TCP	Tous	80	Autorisé
E	Tous	Tous	Tous	Tous	Tous	Refusé

La règle B permet aux machines du LAN d'accéder à DMZ 1. La règle C interdit tout autre trafic en provenance du LAN. La règle A n'a plus d'influence sur le trafic du LAN et permet aux machines externes d'accéder à DMZ 2.

9.4

a)

Tableau 9.4

Règle	Direction	@ src.	@ dest.	Prot.	Port src.	Port dest.	Ack=1	Action
A	In	Externe	170.20.0.2	TCP	>1023	25		Permit
B	Out	170.20.0.2	Externe	TCP	25	>1023		Permit
C	In	Externe	170.20.0.2	TCP	>1023	110		Permit
D	Out	170.20.0.2	Externe	TCP	110	>1023		Permit
E	Out	Interne	Externe	TCP	>1023	80		Permit
F	In	Externe	Interne	TCP	80	>1023	Yes	Permit
G	All	All	All	All	All	All	All	Deny

b) Les adresses privées sont masquées par le NAT. Seule l'adresse publique du routeur est visible de l'extérieur, les équipements privés ne peuvent être adressés de l'extérieur. Il s'agit de SNAT car la translation concerne l'adresse source, celle qui est masquée.

c) Tous les paquets entrants portent la même adresse de destination publique : 193.55.45.12. Le numéro de port destination 25 permet au routeur de diriger le paquet entrant vers le serveur SMTP.

9.5

a) Nous pouvons encore envoyer des mails chiffrés puisque nous utilisons pour cela la clé publique du destinataire. Nous pouvons recevoir des mails chiffrés tant que nous n'aurons pas révoqué la clé perdue, mais nous ne serons plus en mesure de les déchiffrer.

b) Nous ne pouvons plus signer des mails car nous utilisons la propre clé privée pour signer. Nous pouvons vérifier les signatures des mails puisque nous utilisons la clé publique de l'expéditeur du mail pour vérifier la signature.

c) Il est avant tout important de révoquer la clé perdue. Ensuite, il faut se procurer un nouveau couple (clé publique, clé privée), soit en s'adressant à une autorité de certification (CA), soit en la générant soi-même (PGP).

9.6

a) Étant donné que les *hashs* sont irréversibles, le vol du fichier des *hashs* ne permet pas en principe de connaître les mots de passe.

b) Bien que les *hashs* soient irréversibles, les mots de passe peuvent être retrouvés en utilisant soit une attaque par dictionnaire, soit une attaque par recherche exhaustive si l'ensemble des mots de passe possibles est trop petit. Cette protection n'est pas nécessaire si les mots de passe sont suffisamment complexes (longueur, combinaison de lettres, de chiffres, majuscules, minuscules, symboles…).

9.7

a) **Cryptage asymétrique :**

◇ Alice génère un couple de clés publique/privé et envoie à Bob, de manière sécurisée (à l'intérieur d'un certificat), une copie de sa clé publique.

◇ Alice envoie le document et un *hash* du document chiffré avec sa clé privée. Le chiffrement du *hash* fait office de signature.

◇ Bob reçoit le document et son *hash* qu'il déchiffre avec la clé publique reçue. Il le compare avec le *hash* qu'il recalcule à partir du document. Il vérifie donc l'identité d'Alice qui seule a pu crypter avec la clé privée correspondante.

Le point délicat est la transmission de la clé publique.

Cryptage symétrique :

◇ Alice utilise la clé symétrique pour le calcul du *hash*.

◇ Le document est transmis avec son *hash*.

◇ Bob qui possède aussi la clé symétrique recalcule le *hash* et le compare avec le *hash* reçu. Ce qui permet l'authentification d'Alice.

◇ Le point délicat est l'échange de clés (RSA, DH).

La signature utilise le cryptage asymétrique, l'authentification le cryptage symétrique. Les deux méthodes permettent d'authentifier le document.

b) Pour une signature, la clé publique peut être interceptée par l'homme au milieu mais sans la clé privée celui-ci ne pourra pas chiffrer un faux document.
Pour une authentification, l'homme au milieu ne pourra pas fournir un faux *hash* sans la clé symétrique.
Les deux solutions sont donc efficaces mais pas totalement sécurisées (il est toujours possible de se procurer ou de retrouver une clé privée ou une clé symétrique). Le cryptage symétrique est plus robuste.

9.8

a) Un VPN est constitué d'un ensemble de LAN privés reliés à travers Internet par un « tunnel » sécurisé dans lequel les données sont cryptées.
Un VPN utilise une passerelle de chaque côté du tunnel pour encapsuler et chiffrer les données. L'en-tête contenant les adresses privées est crypté et un nouvel en-tête avec les adresses publiques est ajouté par la passerelle émettrice. La passerelle réceptrice est chargée de vérifier l'authenticité et l'intégrité des données (généralement grâce à un *hash* sur les autres champs et transmis dans l'en-tête spécifique VPN) puis de décrypter les données pour le réseau privé destination.

b) PPTP intervient au niveau 2, IPSec au niveau 3 et SSL au niveau 4.
PPTP pour une connexion point à point. IPSec pour encapsuler tous les paquets IP. SSL met en place un tunnel entre deux entités mais pas de passerelles pour gérer un double adressage IP et des réseaux privés complets.

9.9

a) Avec la solution IPSec, on obtient un accès complet sécurisé au réseau interne, ce qui est bien plus que ce que l'on recherchait.
Avantage : le serveur de messagerie n'est accessible qu'après une authentification réussie au niveau IPSec. Ceci protège le serveur contre des attaques par des utilisateurs externes à l'entreprise.
Inconvénient : le cryptage IPSec peut être complexe à mettre en œuvre sur les OS pour n'utiliser finalement que la messagerie.
b) Tunnel sécurisé avec TLS.
Avantage : permet de conserver le client habituel SMTP/POP3 pour accéder à sa messagerie (la sécurité est effectuée au niveau du protocole de transport TLS).
Inconvénient : il faut que les clients et les serveurs de messagerie supportent les versions sécurisées des protocoles SMTP et POP3.
c) Navigateur standard avec HTTPS
Avantage : pas d'installation spécifique côté client, tous les navigateurs supportent HTTPS, possibilité de lire ses mails de n'importe quelle machine.
Inconvénient : les messages restent stockés sur le serveur HTTPS et ne sont plus disponibles hors ligne.

9.10

a) L'URL est du type https://... et une icône en forme de cadenas apparaît dans son navigateur.
b) Toutes les informations transmises sont cryptées avec SSL et un chiffrement sur 128 bits.
c) La clé maîtresse (MK) utilisée pour le cryptage est générée à partir d'une clé publique (PK) transmise sur Internet.
d) Le client reçoit du serveur un certificat délivré par une autorité de certification. Le client peut alors vérifier l'authentification du serveur.
e) Le serveur peut également demander un certificat au client.

INDEX

B

C

D

E

F

S

T

U

V

W

X

Z