# INTRODUCTION AUX RÉSEAUX

*Par Michèle Germain*
*Présidente de l'atelier d'écriture de Forum ATENA*

***Ce livre blanc de la collection « Professeur ATENA » est un document d'initiation et de vulgarisation destiné à ceux qui ne sont pas des professionnels des réseaux et de l'informatique mais qui voudraient acquérir quelques notions.***

## Un livre blanc de Forum ATENA

# SOMMAIRE

# 1. INTRODUCTION

## 1.1. QU'EST-CE QU'UN RÉSEAU ?

…ou plus exactement un réseau de télécommunications.

Un réseau est un ensemble fédérateur constitué d'éléments interconnectés, qui permet à des machines d'échanger des informations.

Les éléments raccordées sont des machines délivrant des informations (serveurs) ou bien des machines qui reçoivent ou émettent des informations (terminaux), telles que ordinateurs et des périphériques, par exemple des terminaux bureautiques (imprimantes, scanners…), des terminaux industriels (lecteurs de codes-barres, capteurs, contacts télécommandés…), des terminaux téléphoniques, etc.

Un réseau peut également être constitué d'un ensemble de réseaux interconnecté, comme c'est le cas d'Internet.

Le réseau est organisé sur une infrastructure de communication filaire ou radio sur laquelle vont circuler divers flux d'information : données informatiques, phonie, vidéo, commandes à distance, acquisition de données par capteurs, etc.

Un réseau est public ou privé, mais appartient à une entité.

## 1.2. TOPOLOGIE DES RÉSEAUX

Sur ce réseau, transite l'information échangée par les équipements raccordés et qui peut être constituée de données informatiques, d'images, de sons, de signaux de télécommandes, etc.

Selon leur dimension, les réseaux sont classés en cinq catégories :

- **WAN** (World Area Network) : Ce sont des réseaux à l'échelle d'une région, d'un pays voire de dimension internationale et souvent publics. C'est par exemple Internet, le réseau téléphonique, etc.
- **MAN** (Metropolitan Area Network) : Ces réseaux sont à l'échelle d'une ville, en général développés par des Collectivités locales ou par des associations de particuliers.
- **LAN** (Local Area Network) : Ce sont les plus nombreux, pour la très grande majorité privés, développés à l'échelle d'une entreprise ou d'un site industriel.
- **PAN** (Personal Area Network) : Ce sont de très petits LAN, à l'échelle résidentielle ou d'une TPE. C'est par exemple le réseau domestique qui raccorde la BOX, les ordinateurs et le téléviseur de la maison. On range aussi dans cette catégorie des réseaux de très faible portée, à la taille de l'individu. C'est par exemple la liaison entre votre téléphone portable et son oreillette.

Un réseau fonctionne très rarement de manière autonome. Il est en général relié à un autre réseau, le cas typique étant le raccordement d'un PAN ou LAN au réseau Internet. La connexion de deux réseaux se fait au moyen d'une **passerelle** (ou **gateway**). Bien sûr, un réseau peut ainsi interopérer avec plusieurs autres réseaux en utilisant autant de passerelles ou en transitant au travers d'un réseau tiers.

## 1.3. LES STANDARDS

Les architectures de réseau et leurs interfaces sont normalisés de façon à garantir l'interopérabilité sur un même réseau d'appareils issus de divers constructeurs.

Il existe un certain nombre d'**organismes de standardisation** chargés de l'élaboration des **standards** (ou **normes**) et de leur évolution. Citons l'IEEE, l'ETSI, l'UIT, etc.

En marge de ces organismes, il existe des **forums** qui rassemblent des industriels et des utilisateurs et qui éditent des **RFC** (Request For Comments) qui après approbation ont valeur de standard. Un forum très présent dans le monde des réseaux est l'IETF.

Certains standards sont produits par des groupes de travail auxquels contribuent plusieurs organismes de standardisation, comme le 3GPP.

## 1.4. QUELQUES DÉFINITIONS

- ***Bit et octet***

Le bit est l'unité élémentaire d'une information, qui peut prendre la valeur 1 ou 0. La numérotation se fait dans un système dit binaire (1='1', 2='10', 3='11', 4='100', etc.).

Par commodité, les bits sont couramment regroupés par 8, définissant ainsi un octet.

Les caractères alphanumériques sont représentés par des patterns de 8 bits (codage ASCII).

- ***Débit***

Il définit les performances d'un réseau, ou une liaison d'un réseau et représente la quantité d'information qu'on peut faire circuler sur ce support. Il s'exprime en bits/seconde (bit/s), dans le cas des réseaux on parlera de Kbits/s (1000) et encore plus souvent de Mbits/s (1 million) et maintenant de Gbits/s (un milliard). Plus le débit est élevé plus une information est transmise rapidement.

Le débit maximal sur une liaison dépend de divers facteurs : performances des équipements terminaux, qualité de la liaison physique (câble de cuivre, fibre optique, radio) et distance entre émetteur et récepteur.

On emploie souvent le terme (en toute rigueur impropre) de **bande passante** pour représenter le débit.

- ***Délai***

C'est le temps qui s'écoule entre le moment où l'émetteur envoie une information sur le réseau et celui où le destinataire la reçoit.

- ***Gigue***

La gigue désigne les variations du délai.

- ***Checksum***

Un code de correction d'erreur calculé par un OU exclusif appliqué aux composants d'un bloc d'information. La checksum est calculée avant l'émission et ajoutée au bloc d'information transmis. Le destinataire effectue le même calcul et vérifie la cohérence de la checksum calculée avec celle jointe au bloc reçu. Si elles sont différentes, c'est que le bloc a été erroné pendant la transmission.

La checksum est un moyen de contrôle très simple dont l'efficacité est limitée. Elle est souvent remplacée par un **CRC** issu d'une opération mathématique plus complexe qu'un OU exclusif.

# 2. CONSTITUTION D'UN RÉSEAU

## 2.1. ARCHITECTURE DES RÉSEAUX

Comme nous l'avons vu ci-dessus, le réseau met en relation des équipements divers, que nous désignons sous le terme générique de **machines**.

Le raccordement peut être **point à point**, une machine donnée n'en raccordant qu'une seule, ou **point à multipoint**, une machine donnée étant raccordée à plusieurs autres.

Pour faire communiquer deux machines, la solution triviale consiste à avoir un lien direct entre elles deux. Mais il est aussi possible de passer par une machine tierce, que l'on appellera **point de transit**, pour faire communiquer deux machines qui n'ont pas de lien direct mais sont toutes deux raccordées à une autre qui va assurer la fonction de transit. Il peut bien sûr y avoir plusieurs transits en cascade entre les deux machines terminales.

La fonction qui permet de définir un chemin entre des machines engagées dans une même transaction s'appelle le **routage**.

### 2.1.1. LA LIAISON POINT À POINT

C'est la forme la plus rudimentaire du réseau qui ne relie que deux machines.

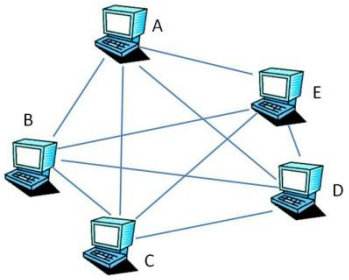
### 2.1.2. LE RÉSEAU MAILLÉ

- ***Maillage total***

Dans cette configuration, une machine, que l'on nommera un **nœud,** est reliée physiquement à chacune des autres.

Cette structure a l'avantage d'être optimisée en termes de temps de transfert. Comme il existe un chemin direct entre deux nœuds, la transmission utilise toujours le plus court chemin entre deux, sans transit, et la fonction de routage est réduite à sa plus simple expression. De plus, une liaison n'étant utilisée que par les deux nœuds qui se trouvent à ses extrémités, celles-ci disposent toujours du débit maximal de la liaison.

Son second avantage est sa fiabilité. Si par malchance un lien est rompu, il existe **toujours** un chemin alternatif en transitant par un nœud tiers. Si par exemple le chemin A-B est rompu, l'information pourra transiter par C et prendre le chemin A-C + C-B. C'est la fonction de routage qui va choisir le chemin alternatif ou **débordement**. Dans ce cas, on perd l'avantage du chemin direct (voir ci-après 'maillage partiel').




***Réseau maillé***

Le gros inconvénient du maillage total est la quantité de fil qu'il faut installer pour raccorder tout ce petit monde et qui devient déraisonnable pour un nombre important de machines. Le nombre de liens se calcule par la formule suivante :

**Nombre de liens = nombre de nœuds x (nombre de nœuds -1)/2**

Ainsi, la configuration ci-dessus, qui comporte 5 nœuds, utilise (5x4)/2 = 10 liens. Si on veut interconnecter 20 nœuds, il faudra 190 liens…

C'est la raison pour laquelle cette structure n'est guère utilisée que lorsqu'il y a un besoin particulièrement fort de fiabilité particulièrement du réseau, digne du Pentagone.

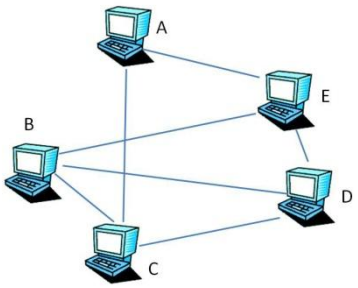
- ***Maillage partiel***

Le câblage étant un gros inconvénient des réseaux maillés, une solution alternative est le maillage partiel. Dans ce modèle, un nombre limité de machines sont raccordées deux à deux. Les autres doivent transiter via des machines raccordées entre elles.

Nous pouvons constater dans le schéma suivant qu'il existe toujours une route pour joindre deux nœuds. Le maillage partiel doit être ainsi fait qu'il existe toujours un moyen de relier deux nœuds, même en cas de perte d'un lien, ceci entraînant au plus des transits supplémentaires.

Dans l'exemple ci-dessous, A et D sont normalement reliés via E. En cas de rupture du lien A-E, A pourra joindre D en passant par C.

Ce modèle est utilisé par des grands réseaux d'infrastructure.




***Réseau à maillage partiel***

Par rapport au maillage total, ce modèle a l'inconvénient d'introduire des points de transit avec deux conséquences :

- Augmentation du délai suite à l'allongement du chemin et au traitement dans les nœuds de transit.
- Partage de la bande passante sur un lien donné par tous les couples de machines qui doivent l'emprunter.

### *2.1.3. LE RÉSEAU SUR SUPPORT UNIQUE*

Ces architectures ont en commun la finalité de réduire le câblage. Au lieu de tirer des fils entre machines, on va ici tirer un fil unique sur lequel vont se raccorder toutes les machines.

L'envers de la médaille est qu'une seule machine peut émettre à la fois, sinon tout se mélangerait. Par conséquent ces structures seront plutôt utilisées pour des structures petites et moyennes, de type PAN ou LAN.

Il résulte de ceci que le débit maximal du réseau est partagé par les différentes machines, contrairement au modèle maillé où chacune des liaisons du maillage dispose de l'intégralité de celui-ci.

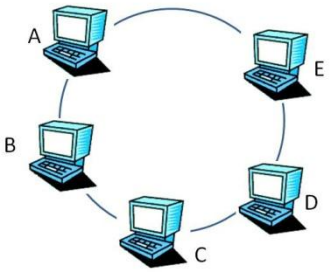
- ***Architecture en anneau***

C'est la forme la plus ancienne de réseau sur support unique, le Token Ring d'IBM, normalisé par l'IEEE sous la référence 802.5.

Toutes les machines sont placées sur une boucle fermée, l'anneau. Les liaisons se font toutes dans le même sens, par exemple celui inverse des aiguilles d'une montre. Ainsi, pour communiquer avec E, A effectue le chemin A-B-C-D-E.

Pour éviter les collisions, un mécanisme de jeton gère les droits d'émission. Par exemple A est possesseur du jeton et émet. Quand il a terminé, il passe le jeton à la machine suivante B qui émet puis repasse le jeton à la suivante C, etc.

L'information est émise sur l'anneau avec l'identification de son destinataire. Chaque machine examine cette information pour savoir si elle est en est destinataire. Seul le ou les destinataires acceptent l'information.




***Token Ring***

Ce modèle n'est plus beaucoup utilisé, au profit des architectures Ethernet.

- ***Architecture Ethernet en bus***

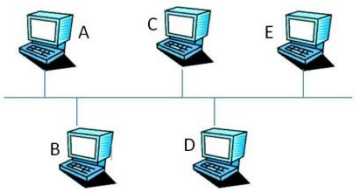
Ce modèle est basé sur le protocole Ethernet, normalisé par l'IEEE sous la référence 802.3.

La première structure de réseau Ethernet est celle sous forme de bus. Le bus, en l'occurrence, est un câble coaxial Ethernet sur lequel viennent se greffer les composants du réseau. Le raccordement utilise des prises vampire qui percent le blindage du câble coaxial pour venir écouter et émettre dans le bus.

Les collisions sont gérées par les machines du réseau elles-mêmes, chacune devant s'assurer avant d'émettre que le bus est libre… comme le piéton regarde à gauche et à droite avant de traverser la rue.

Comme pour l'anneau, l'information est émise sur le bus avec une identification de destinataire et seules les machines concernées l'acceptent.

La technologie en bus n'est aujourd'hui plus utilisée, au profil de la technologie de commutation Ethernet, topologie en étoile.



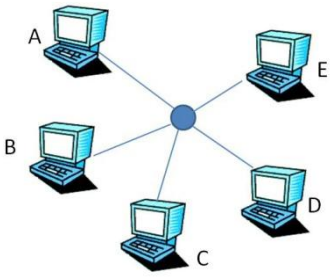

***Réseau Ethernet en bus***

Le câblage sur paires torsadées, proche du câblage téléphonique, supplante maintenant le câblage en bus avec l'architecture Ethernet en étoile.

- ***Architecture Ethernet en étoile***

La transmission Ethernet est limitée par la longueur du câble et l'architecture en bus trouve vite ses limites. Pour palier ceci, l'architecture Ethernet est également présentée en étoile. Toutes les machines sont raccordées à un point central du réseau, que l'on nomme un concentrateur.

Le mécanisme de transmission est le même que pour le bus, avec test anticollision et diffusion sur toutes les branches de l'étoile.




***Réseau Ethernet en étoile***

- ***Architecture Ethernet mixte***

Ce type de réseau combine bus et étoiles, un bus pouvant se trouver au bout d'une branche d'étoile ou une étoile sur un bus.

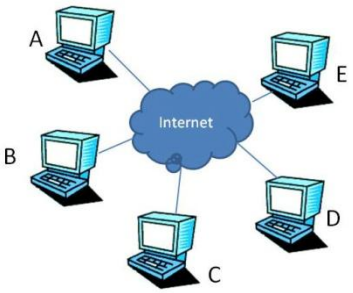
### *2.1.4. LE RÉSEAU PEER-TO-PEER*

Ce type de réseau, dit aussi P2P (ne pas confondre avec les structures point à point, souvent désignées aussi P2P), est un peu atypique, dans le sens où son infrastructure repose sur un autre réseau, Internet ou réseau privé.

On retrouve un peu le modèle du réseau maillé dans lequel les machines sont reliées deux à deux, sauf que dans ce cas, la liaison n'est pas physique mais se fait au travers du réseau partagé.

L'avantage de cette structure est que les liaisons entre nœuds sont pérennes. Les inconvénients sont toutefois multiples, citons : variabilité de la bande passante, difficulté de gestion d'un réseau dont toutes les machines sont décentralisées et enfin, cette forme de réseau est particulièrement vulnérable vis-à-vis des attaques lorsqu'elle est basée sur Internet.

Il faut noter que les architectures de la plupart des réseaux d'accès (mobiles, fixes) ne permettent pas l'échange à proximité des utilisateurs, mais nécessitent la remontée des informations dans le réseau, souvent jusqu'à une plaque régionale, voire nationale, ce qui limite fortement l'intérêt du P2P.




*Réseau Peer to Peer*

## 2.2. L'INFRASTRUCTURE

Le **cœur de réseau** intègre les liaisons entre les machines, en d'autres termes, le support de transmission, et les équipements de routage. On utilise aussi les termes **dorsale**, ou **backbone**.

Nous allons ici nous intéresser aux liaisons.

### *2.2.1. LIAISONS FILAIRES*

Ce sont les plus fréquentes

Les premiers réseaux utilisaient des **câbles coaxiaux**, lourds, peu maniables et chers. Ils se composent d'un conducteur central entouré d'un isolant, lui-même entouré d'une gaine conductrice de blindage et le tout sous gaine protectrice.

*Câble coaxial (photo Wikipedia)*

Le coaxial a peu à peu été remplacé par la **paire torsadée**, blindée ou non blindée, plus économique. Le problème des deux fils est qu'ils induisent de la diaphonie que l'on peut réduire par le torsadage : plus il est serré, plus il est efficace. L'ensemble est mis sous gaine et peut inclure plusieurs paires torsadées deux à deux.

C'est à l'heure actuelle le support le plus utilisé.

*Paire torsadée (photo Wikipedia)*

La **fibre optique** est à présent le « nec plus ultra » en matière de support de transmission. Il s'agit d'un mince fil de verre sur lequel l'information est transmise sous forme optique. Elle présente une très faible atténuation permettant des débits élevés sur de grandes distances. Du fait qu'elle transporte de la lumière et non de l'électricité elle présente une immunité native aux perturbations de nature électromagnétique. Envers de la médaille… elle est encore très chère.

*Fibre optique (photo Wikipedia)*

### 2.2.2. LIAISONS SANS FIL

En marge des réseaux filaires on trouve les réseaux radio sans fil, autonomes ou complémentaires d'un réseau filaire.

Le réseau filaire peut satisfaire des besoins divers, tout d'abord quand il s'agit de raccorder des terminaux sans fil. On a dans ce cas des prolongations radio d'un réseau filaire sous forme de liaisons radio point à point, par exemple pour raccorder une imprimante ou un clavier.

Un autre cas est celui d'un réseau ou sous réseau à part entière qui va accueillir des ordinateurs nomades ou des smartphones. C'est le cas du hot-spot qui offre un service semi-public à des usagers nomades ou celui d'une entreprise ou d'un hôtel qui propose un accès réseau à ses visiteurs.

Un autre cas où l'infrastructure radio se justifie est lorsqu'il y a des difficultés matérielles pour câbler les bâtiments, notamment dans des bâtiments classés.

Un dernier cas est pour couvrir une zone extérieure aux bâtiments, parking, campus, etc.

Il existe différentes techniques de liaisons radio :

- ***Wi-Fi***

Cette technique permet de constituer des LAN autonomes ou en complément d'un réseau filaire sur des distances de quelques centaines de mètres.

- ***WiMAX/LTE***

Ces techniques, de plus longue portée que Wi-Fi, permettent de constituer des réseaux métropolitains.

- ***Bluetooth/Zigbee***

Ces techniques, de très faible portée, sont plutôt utilisées en remplacement du câble pour les oreillettes, les périphériques sans fil, voire en milieu industriel pour passer des signaux là où il est difficile de passer un câble, par exemple dans une automobile.

- ***Les réseaux 3G/4G***

Nous ne faisons que les citer car n'entrent pas directement dans le cadre de ce document. Il s'agit de réseaux de type WAN développés par des opérateurs qui vendent des services de téléphonie et d'accès internet sans fil à leurs clients.

# 3. TRANSMISION DANS LES RÉSEAUX

## 3.1. LE MODÈLE EN COUCHES

### 3.1.1. ENTITÉS TRANSPORTÉES

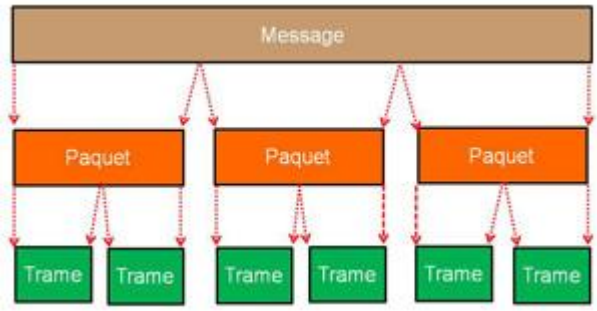
Lorsqu'un ordinateur désire envoyer une information à un autre, il ne va pas tout envoyer en une seule fois, surtout si ce qu'il a à envoyer est gros. Ce serait irréaliste car la liaison serait réservée exclusivement pendant un temps plus ou moins long à une transaction unique et une panne ou une erreur nécessiterait de reprendre toute la transaction dès le début.

Aussi, les mécanismes de transmission de données vont-ils procéder à un découpage de l'information à transporter.

Au départ, on a le **message**. C'est ce qu'on veut transmettre, tout petit ou bien énorme. C'est par exemple un fichier, une image, une vidéo…

Ce message est subdivisé en **paquets** dont le processus d'envoi est supervisé de bout en bout. Contrairement au message qui peut être très gros, le paquet est de taille raisonnable et fixe. Des paquets appartenant à des messages différents pourront s'entrelacer sur une même liaison, permettant ainsi plusieurs transactions simultanées. C'est comme sur le tapis de l'aéroport où vos bagages ne sont pas livrés tous ensemble, mais sont mélangés avec ceux des autres passagers.

Le paquet est lui-même subdivisé en **trames** de longueur fixe dont la supervision se fait entre deux machines en vis à vis (c'est-à-dire liées directement sans transit).




***Découpage d'un message***

### 3.1.2. LE MODÈLE OSI

- ***Les couches***

Ce modèle a été proposé par l'ISO pour interconnecter des ordinateurs et traite entre autres les trois niveaux trame, paquet, message vus ci-dessus.

Il est fondé sur une structure de sept couches ou niveaux :

| | | |
|---|---|---|
| Niveau 7 | **Application** | Accès aux services du réseau (sémantique) |
| Niveau 6 | **Présentation** | Mise en forme des données et de leur structure (syntaxe)<br>Chiffrement |
| Niveau 5 | **Session** | Gestion de sessions de dialogue entre les terminaisons |
| Niveau 4 | **Transport** | Contrôle du transfert des messages de bout en bout<br>Découpage en paquets |
| Niveau 3 | **Réseau** | Acheminement des paquets<br>Découpage en trame<br>Routage/adressage/contrôle de flux |
| Niveau 2 | **Liaison** | Transport des trames<br>Établissement des connexions<br>Détection d'erreurs |
| Niveau 1 | **Physique** | Transfert des information binaires sur le support (média) |

Comme ce n'est pas assez compliqué comme ça, le niveau 2 est lui-même subdivisé en deux niveaux :

| | |
|---|---|
| MAC | Transport des trames entre deux machines en vis à vis |
| LLC | Structure les bits en trames adaptées au support<br>Gère les adresses physiques des cartes réseau (adresses MAC)<br>Indépendante du média |

Nous retrouvons dans ce modèle les notions précédentes :

- le niveau 4 manipule les messages,
- le niveau 3 manipule les paquets,
- le niveau 2 manipule les trames,
- le niveau 1, niveau physique, transporte des bits sur un support filaire ou radio.

- ***Les échanges***

Les échanges entre deux machines sont gérés par un **protocole**.

Une couche ne peut dialoguer qu'avec une couche de même niveau. Une couche reçoit des services de la couche juste inférieure et fournit des services à la couche juste supérieure.

L'émission d'information se fait en descendant les couches une par une. Chaque niveau ajoute un niveau de découpage et d'encapsulation de l'information. L'opération inverse (concaténation, désencapsulation) est faite en réception en remontant les couches.

## 3.2. LES MÉCANISMES DE LA TRANSMISSION DE DONNÉES

### *3.2.1. L'ADRESSAGE*

Lorsque vous envoyez une lettre… ou un email, vous désignez le destinataire par une adresse. C'est la même chose en transmission de données, sauf que dans ce cas nous aurons à gérer diverses adresses.

- ***L'adresse MAC***

C'est l'adresse utilisée au niveau 2 qui sert à envoyer une trame à une machine en vis-à-vis, identifiée par son adresse MAC. En fait l'adresse MAC n'est pas liée à la machine mais à la carte électronique ou autre équipement qui la relie au réseau. Ainsi un ordinateur relié au réseau par Ethernet et par Wi-Fi aura une adresse MAC propre à chacun de ces deux accès.

L'adresse MAC est unique pour un connecteur donné de l'équipement, fixée par le constructeur. C'est comme le numéro de sécurité sociale, unique et défini dès la naissance pour toute la vie.

- ***L'adresse niveau 3***

C'est l'adresse qui va être utilisée pour envoyer des paquets entre deux machines, pas forcément en vis-à-vis, qui sont toutes deux engagées dans une même transaction.

Cette fois, l'adresse est relative à l'utilisateur, l'ordinateur, qui peut appartenir au même réseau que l'émetteur, ou bien à un autre réseau.

Contrairement à l'adresse MAC qui est universelle, l'adresse niveau 3 va dépendre du type du réseau :

- adresse X.25 dans des réseaux de type TRANSPAC,
- adresse IP dans des réseaux de type IP, soit la quasi-totalité des réseaux actuels.

Les adresses IP sont attribuées de manière fixe à un ordinateur ou de manière dynamique dès que la machine se connecte au réseau. Pour assurer l'unicité des adresses sur Internet, le fournisseur d'accès, sous contrôle d'un organisme centralisé, l'ICANN, attribue l'adresse à l'utilisateur final. Des adresses locales sont utilisées lorsque l'adresse Internet doit être partagée dans un réseau. Pour expliquer ceci faisons un petit retour au début des réseaux IP qui étaient alors identifiés par une adresse sur 4 octets (IPv4). Le succès de IP fit que la capacité d'adressage devint rapidement insuffisante pour identifier tous les ordinateurs de la planète. Pour palier cette pénurie, une adresse IP fut alors allouée dynamiquement (au moyen d'un serveur DHCP) à chaque ordinateur, chaque fois qu'il en faisait la demande. Depuis les adresses IP sont passées sur 16 octets (IPv6) afin d'avoir la possibilité d'attribuer de manière fixe une adresse IP à chaque utilisateur qui en aurait le besoin.

- ***Le port***

Cette adresse désigne un application sur une machine. Par exemple, le Port 21 représente traditionnellement l'application FTP de transfert de fichiers.

### 3.2.2. LE ROUTAGE

Lorsque vous partez en vacances, vous prenez une carte routière pour déterminer l'itinéraire, la route, que vous allez emprunter… ou vous laissez votre GPS le faire pour vous. En route, vous pouvez rencontrer des obstacles (route barrée, bouchon…) qui vous contraignent à modifier votre itinéraire.

Il en est de même avec les réseaux.

Le routage détermine le chemin que les paquets vont suivre dans le réseau (voire entre plusieurs réseaux) pour qu'une machine émettrice puisse atteindre une machine destinataire.

Comme sur la route, le réseau n'est pas infaillible. Il peut se produire des ruptures de liens ou des engorgements. Ceci va donner lieu à des routages de débordement qui, selon la nature du réseau, peuvent être prédéfinis (comme les panneaux de déviation placés sur les routes) ou déterminés au coup par coup par auto reconfiguration (comme votre GPS dès que vous vous écartez de l'itinéraire affiché).

On définit ainsi deux types de routages :

- ***Le routage par commutation***

La route entre deux machines est toujours la même (route nominale), décrite dans une table de commutation de la machine de départ.

En cas de panne d'une machine de transit ou d'une liaison, la redéfinition du routage se fait en se référant à cette table.

Ainsi, tout est défini de manière fixe : la route nominale et les routes de débordement.

Tous les paquets prennent obligatoirement la route nominale, les routes de débordement n'étant utilisées qu'en cas de panne ou de congestion. Par conséquent les paquets entre deux machines émettrice et destinataire prennent tous la même route et arrivent dans l'ordre dans lequel ils ont été émis.

- ***Le routage par routeur***

Le routage est construit de manière dynamique par chaque machine traversée, chacune ne connaissant que le premier point de transit vers la machine destinataire.

En cas de panne ou de congestion le routage est autoadaptatif.

Le choix d'un lien pour acheminer un paquet se fait en fonction de différents critères parmi lesquels intervient la charge courante. Ceci permet une répartition de la charge sur l'ensemble du réseau.

Par contre, le choix de la route étant fait lors de l'envoi de chaque paquet, tous les paquets d'un même message peuvent suivre des routes différentes, avec des temps de transfert différents. En final, les paquets peuvent arriver dans un ordre différent de celui dans lequel ils ont été émis. On remédie à ceci en numérotant les paquets, mais il faut attendre de tous les avoir reçus pour reconstituer le message.

- ***Le routage dans Internet***

Internet est constitué de quelque 42 000 sous-réseaux interconnectés – les « Autonomous Systems » ou AS, caractérisés par une administration qui leur est dédiée. Chaque AS indique à ses congénères les AS qui peuvent être atteintes par son intermédiaire. Ce protocole, appelé BGP pour Border Gateway Protocol assure le lien entre les AS. Les flux sont routés au sein d'un AS par un protocole interne. Chaque routeur construit à partir de ces informations des tables de routage dont la taille peut devenir vertigineuse.

Notons que BGP est un des points de faiblesse d'Internet. Les annonces peuvent être erronées par accident ou par malveillance.

### 3.2.3. LA COMMUTATION

La commutation est l'action qui permet d'établir une liaison physique ou virtuelle entre deux machines d'un réseau. Il existe deux grandes familles de commutation :

- ***La commutation de circuits***

Un chemin physique est établi entre l'émetteur et le destinataire pour toute la durée de transmission d'un message (transaction).

Tous les segments du réseau qui constituent la route entre l'émetteur et le destinataire sont réservés à cette transaction et ne peuvent pas être utilisés par d'autres transactions. C'est typiquement le cas du réseau téléphonique dans lequel les lignes nécessaires sont réservées à une communication, pendant toute la durée de celle-ci.

L'avantage de la commutation de circuit est que la totalité de la bande passante est assurée à la transaction.

L'inconvénient est la mise en indisponibilité des ressources vis-à-vis d'autres utilisateurs.

- ***La commutation de paquets***

Un chemin virtuel est attribué à une transaction. Les segments du réseau qui seront utilisés par la transaction sont identifiés mais non réservés. Ils sont alloués uniquement pendant le temps de transfert d'un paquet.

Un même segment de réseau peut être associé simultanément à plusieurs circuits virtuels.

Ceci permet de multiplexer plusieurs transactions sur un même segment de réseau, les paquets relatifs à chacune s'entrelaçant sur la liaison. L'inconvénient est que la bande passante d'un segment est partagée entre les différentes transactions en cours.

- ***Variantes de la commutation de paquets***

Dans certains réseaux, la commutation ne s'opère pas au niveau trame (réseaux Frame Relay) ou cellule, petits blocs de 53 octets (réseaux ATM).

#### *3.2.4. CONTRAINTES SUR LES MESSAGES TRANSPORTÉS*

- ***Données de type informatique***

Il s'agit de fichiers de données. Il est vital qu'aucun élément d'information ne soit perdu en cours de route… Imaginez une lettre dont il manquerait des mots. Si l'esprit humain est dans une certaine mesure capable de combler les vides, il n'en est rien de l'ordinateur et un fichier dont il manque un seul bit est inexploitable.

Pour palier ce risque, plusieurs mécanismes sont mis en place afin de respecter l'intégrité du message :

- introduction de codes de contrôle (CRC) afin de détecter des paquets erronés,
- numérotation des paquets afin de détecter des paquets manquants.

S'il manque un paquet ou si un paquet est erroné, la retransmission est redemandée (mécanisme ARQ) à partir du paquet où a été détectée l'anomalie.

Ceci joue sur les performances puisque le délai de délivrance du message va être allongé par le traitement de contrôle et par les transmissions.

Toutefois, pour ce type d'information, on n'est pas (trop) pressé et mieux vaut recevoir un message un peu plus tard que recevoir un message inexploitable.

Ce mode de transmission est nommé **Best Effort**, en gros, « tu fais pour le mieux… »

- ***Données de type temps-réel***

Il s'agit ici de données de type voix (téléphonie essentiellement) et vidéo.

Ici, il est vital de minimiser le délai de transmission de bout en bout et de stabiliser les variations de ce délai (**gigue**). On a en mémoire les premières communications téléphoniques par satellite géostationnaires sur lesquelles le temps de transmission entre la terre et le satellite induisait des délais insupportables dans la communication.

La stabilisation du délai de transmission permet une réception régulière des paquets afin d'assurer une délivrance fluide du message au destinataire.

Ces contraintes sont prioritaires sur les qualités d'intégrité décrites ci-dessus. Dans le cas de la phonie ou de la vidéo, la perte d'un paquet n'est pas rédhibitoire. Si le nombre de paquets perdu reste raisonnable, ceci sera sans incidence sur la compréhension du message reçu. Par conséquent les mécanismes de contrôle et de répétition du best effort ne sont pas mis en œuvre : si un paquet est inexploitable, on le jette, si un paquet est manquant, tant pis.

Par contre on va mettre d'autres mécanismes afin de garantir les contraintes liées à ce type de données :

- réservation de bande passante,
- priorisation des flux dans les réseaux afin de favoriser les flux temps-réel,
- élimination volontaire de paquets lorsque la liaison atteint un seuil de congestion donné.

Ce mode de transmission est nommé **avec QoS** (Quality of Service), en gros « tu assures la qualité du service coûte que coûte ».

## 3.3. LE MODE CLIENT-SERVEUR

Dans un système d'information, les ordinateurs fonctionnent généralement en mode **client-serveur** au travers d'un réseau.

Ceci veut tout simplement dire qu'un ordinateur « serveur » reçoit des demandes d'autres ordinateurs « clients » et qu'en retour le serveur renvoie aux clients ce qu'ils ont demandé. Exactement comme lorsque vous demandez une limonade à un serveur au café du coin.

Pour corser un peu les choses, disons qu'un même ordinateur peut être à la fois client et serveur. Bien sûr dans ce cas il n'y a pas de réseau entre les deux, mais l'ordinateur supporte deux logiciels respectivement « client » et « serveur » qui communiquent au travers d'un protocole, exactement comme s'ils étaient sur deux ordinateurs différents.

- ***Le serveur***

Un serveur est un ordinateur de grande puissance ou un microordinateur. Il ne dispose pas d'interface homme-machine, excepté pour sa propre administration et pour charger les informations qui seront distribuées aux clients.

Le serveur dispose d'une mémoire de masse sur laquelle il va stocker l'ensemble des informations qu'il est susceptible de délivrer aux clients. Ce volume est le plus souvent très conséquent et cette mémoire est sur disque(s) ou DAT.

Les premiers serveurs faisaient tout au sein du système d'information. L'inconvénient majeur était qu'une panne du serveur entraînait une panne totale du système d'information. Depuis, on préfère avoir serveurs dans un même système d'information, chacun étant dédié à une application ou fonction particulière :

- le serveur d'applications, dédié à une application, ou à plusieurs applications,
- le serveur de fichiers qui centralise un ou plusieurs ensembles d'information, sous forme de fichiers ou sous forme de bases de données,
- le serveur d'impression qui gère les accès les files d'attente des travaux soumis aux imprimantes,
- le serveur Web qui gère les accès aux Intra/extranets et à l'Internet,
- etc.

- ***Le client***

Un client est très rarement un ordinateur de grande puissance. C'est le plus souvent un microordinateur, voire une tablette ou un palm.

Le client traite des applications. Pour cela, il envoie des requêtes aux serveurs pour obtenir les données nécessaires, effectue le traitement puis stocke et/ou présente le résultat.

Il dispose d'une interface homme-machine par laquelle l'utilisateur va saisir les requêtes envoyées au serveur et présenter les résultats. Ce sont typiquement le clavier, l'écran, la souris et l'imprimante.

Il dispose bien sûr d'un disque, mais il peut recevoir des mémoires de masse externes telles que des CD-ROM, des clés USB, etc. pour le transport de données.

L'ordinateur client dispose également de périphériques. Outre les terminaux d'interface homme-machine, il peut également supporter :

- des terminaux industriels : lecteurs de codes-barres ou QR-codes, lecteurs RFID, lecteurs de badges magnétiques, capteurs, senseurs, contacts télécommandés, etc.
- des terminaux téléphoniques : postes téléphoniques, PC équipés d'organes audio,
- etc.

# 4. LES COMPOSANTS D'UN RÉSEAU

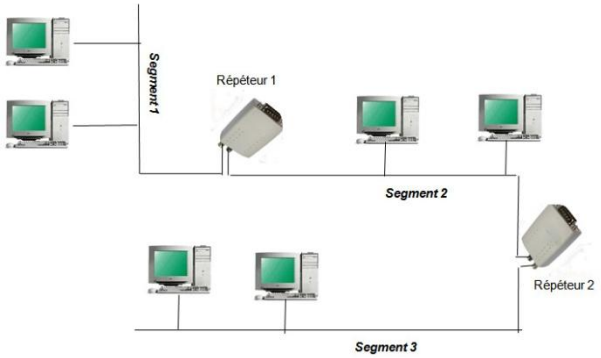
## 4.1. LE RÉPÉTEUR

Le répéteur raccorde deux segments de réseau identiques. Il fonctionne au niveau 1 (couche physique) du modèle OSI.

Par exemple, la longueur maximale d'un bus Ethernet est d'une centaine de mètres. Pour avoir un réseau plus long, on connectera plusieurs brins Ethernet au moyen de répéteurs.

Le répéteur amplifie le signal reçu d'un côté et le retransmet tel quel de l'autre côté. Il est totalement transparent au signal reçu et ne le modifie en rien.

Il peut toutefois effectuer un changement de support physique, pourvu que les deux supportent les mêmes protocoles de couche supérieure. Le répéteur peut ainsi abouter de la paire torsadée et coaxial.




*Configuration de réseau avec répéteur*

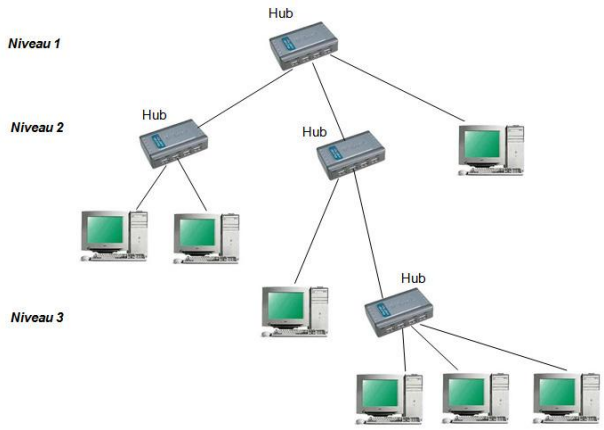
## 4.2. CONCENTRATEUR

Le concentrateur (ou **hub**) est utilisé par les réseaux en étoile pour interconnecter plusieurs machines.

Un signal reçu sur une des branches est transmis sur toutes les autres qui doivent supporter les mêmes protocoles de couches supérieures.

Comme le répéteur, le concentrateur fonctionne au niveau 1 (couche physique) du modèle OSI. Il est transparent aux signaux transportés et n'assure qu'une réamplification du signal.

Il est possible de mixer architectures bus et étoile en mettant une branche de concentrateur sur un bus ou un bus au bout d'une branche d'un concentrateur. Le concentrateurs peuvent aussi se cascader.



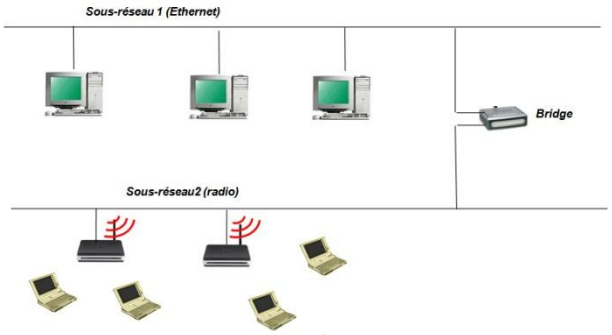

*Configuration de réseau hybride bus et étoile sur concentrateurs*

## 4.3. PONT

Le pont (ou **bridge**) crée un réseau à partir d'un ensemble de sous-réseaux.

Il opère au niveau 2 (couche liaison) du modèle OSI. Il transfère les trames en les mettant au format du sous-réseau suivant. Au passage il filtre les trames en ne laissant passer que celles qui sont destinées au sous-réseau raccordé.

Le pont vérifie le code de contrôle (cheksum) de chaque trame, mais ne fait pas d'autre analyse des trames transportées. En particulier il ne réalise aucune opération de routage.




***Configuration de réseau avec pont***

Le pont est utilisé en premier lieu pour raccorder des sous-réseaux incompatibles au niveau 2 mais compatibles dans les couches supérieures, par exemple raccorder un réseau Ethernet et un réseau Wi-Fi.

Il peut aussi être utilisé pour raccorder des sous-réseaux identiques, par exemple Ethernet, avec le seul but de filtrer les trames qui ne sont pas destinées aux sous-réseaux suivants. Nous avons vu que sur un bus Ethernet, toutes les trames sont émises vers tout le monde. Si on raccorde plusieurs bus Ethernet par des répéteurs, ces toutes les trames sont transmises sur tous les brins Ethernet interconnectés. Si on veut ainsi construire ainsi un grand réseau, le nombre de trames qui circulent sur le bus devient rapidement excessif, engendrant une chute du débit utile pour chaque utilisateur et par là, nuisant à l'efficacité du réseau. Si maintenant on utilise des ponts à la place des répéteurs, le trafic sur un même bus Ethernet reste local et le pont ne laisse passer que les trames destinées aux autres bus.

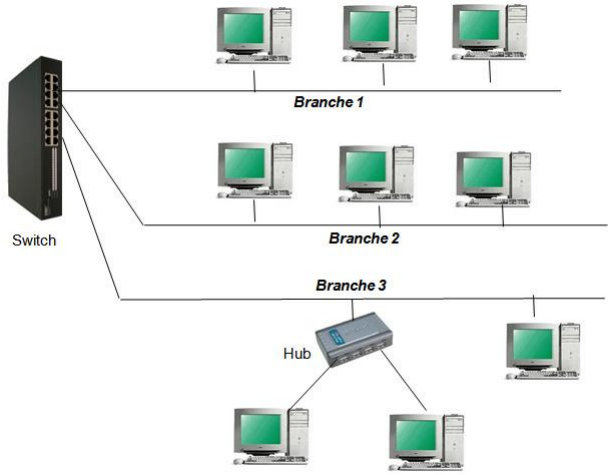
## 4.4. COMMUTATEUR

Le commutateur (ou **switch**) interconnecte des cartes d'interface réseau identifiées par leur adresse MAC.

Le commutateur fonctionne au niveau 2 (couche liaison) du modèle OSI et transmet des trames.

La structure du réseau avec commutateur ressemble à celle du concentrateur avec une différence majeure : une trame n'est transmise que sur la branche à laquelle est raccordé le destinataire et non sur l'ensemble des branches comme le fait le concentrateur.

Le commutateur utilise un routage fixe, défini par une table de routage, comme vu plus haut.



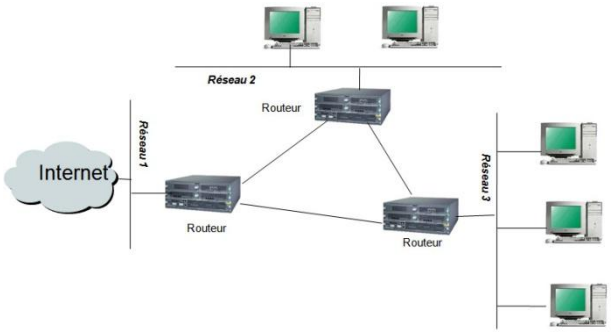

***Configuration de réseau avec commutateur***

## 4.5. ROUTEUR

Le routeur interconnecte des réseaux dans lesquels les utilisateurs ne sont connus que par leur adresse paquet (adresse IPv4 ou IPv6). Il fonctionne au niveau 3 (couche réseau) du modèle OSI.

Le routeur assure l'acheminement des paquets vers le destinataire au travers de machines de transit, chaque paquet comportant l'adresse complète du destinataire.

A l'instar du commutateur, un paquet n'est délivré qu'à son destinataire.




***Interconnection de réseaux par routeurs***

En général, le routeur intègre un pare-feu dont le rôle est de contrôler les flux inter-réseaux.

## 4.6. LA PASSERELLE

La passerelle (ou **gateway**) est utilisée pour interconnecter des réseaux hétérogènes.

Elle opère au niveau 4 en connectant des réseaux incompatibles au niveau 3, par exemple un réseau IP et un réseau X25.

Elle peut aussi opérer à un niveau applicatif, par exemple en interconnectant un téseau de téléphonie sur IP au réseau téléphonique classique.

La configuration est similaire à celle du pont.

# 5. LES PROTOCOLES DE LA TRANSMISSION DE DONNÉES

Nous allons nous limiter aux plus importants dans le monde des réseaux.

## 5.1. PROTOCOLES COUCHES BASSES

On désigne ainsi les protocoles associés aux couches 1 à 3 du modèle OSI.

### 5.1.1. PRINCIPAUX PROTOCOLES

| Protocole | Niveau | Fonction |
|---|---|---|
| V.24 | 1 | Une liaison série pour l'échange d'information entre un ordinateur et un terminal |
| USB | 1 | Un bus de transmission série pour raccorder des périphériques à un ordinateur. Il a supplanté la liaison V.24. |
| xDSL | 1 | Diverses techniques par lesquelles des données haut débit peuvent être transmises sur des lignes téléphoniques avec un débit symétrique (SDSL) ou asymétrique (ADSL) |
| Ethernet | 1 + 2 (MAC) | Un protocole qui définit la couche physique et l'accès au média pour le transport des trames dans des réseaux de type bus ou étoile |
| PPP | 2 | Un protocole qui met en place une liaison point à point entre deux machines. |
| Frame Relay | 2 | Un protocole de commutation de paquets dont l'élément de commutation est la trame. |
| ATM | 2 | Un protocole de commutation de paquets dont l'élément de commutation est la cellule, utilisé en particulier dans les cœurs de réseau téléphoniques. |
| Token Ring | 2 | Un protocole de réseau qui définit la couche physique et le contrôle d'accès au média pour le transport des trames dans des réseaux en anneau. |
| X.25 | 3 | Un protocole pour acheminer des paquets au travers d'un réseau dans un mode connecté. |
| IP | 3 | Un protocole pour acheminer des paquets au travers d'un réseau dans un mode non connecté. |

### 5.1.2. ETHERNET

- ***La famille Ethernet***

La première publication d'Internet remonte à 1973. Par la suite Ethernet a été standardisé par l'IEEE et a fait l'objet de plusieurs éditions :

| Sigle | Standard | Nom | Support | Débit | Portée |
|---|---|---|---|---|---|
| 10 Base-5 | 802.3 | Ethernet bus | Coaxial | 10 Mbits/s | 500 m |
| 10 Base-T | 802.3 | Ethernet standard | Paire torsadée | 10 Mbits/s | 100 m |
| 100 Base-TX | 802.3u | Fast Ethernet | Double paire torsadée | 100 Mbits/s | 100 m |
| 100 Base-T | 802.3u | Fast Ethernet | Fibre | 100 Mbits/s | 2 000 m |
| 1000 Base-LX | 802.3ab | Ethernet Gigabit | Fibre | 1 Gbits/s | 550 m |
| 10G Base-LX4 | 802.3ae | Ethernet 10 Gigabits | Fibre | 10 Gbits/s | 500 m |

- ***Accès au média***

Nous avons vu que le bus ne peut supporter qu'une seule émission à la fois. Ceci est géré par un mécanisme CSMA/CD (Carrier Sense Multiple Access/Collision Detection).

La machine qui souhaite émettre une trame écoute le bus pour savoir s'il est libre. S'il est libre, elle émet, sinon elle attend.

Mais deux machines peuvent avoir la même idée, reconnaître le bus libre en même temps et émettre simultanément. La trame étant reçue par toutes les machines connectées sur le bus, elle l'est en particulier par celle qui l'a émise. La machine émettrice compare ce qu'elle reçoit à ce qu'elle avait émis et

si c'est différent, c'est qu'il y a eu collision avec une machine… qui fait de son côté la même constatation. Avant de réémettre, les deux machines vont compter un délai aléatoire afin d'éviter une nouvelle collision.

### 5.1.3. IP

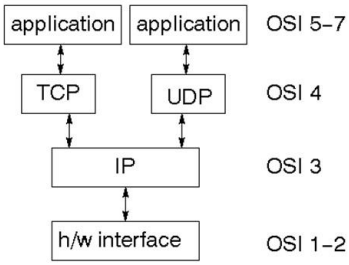
IP (Internet Protocol) est spécifié par la RFC 791 de l'IETF. Il s'appuie très souvent sur Ethernet mais peut supporter d'autres protocoles niveau 2.

Le protocole IP achemine les paquets jusqu'à leur destinataire identifié par une adresse unique. A cet effet, chaque paquet est étiqueté qui contient l'adresse de l'expéditeur, celle du destinataire et d'autres éléments de contrôle. Les contrôles effectués par IP se limitent au contrôle de la checksum.

## 5.2. PROTOCOLES COUCHES HAUTES

Nous n'allons nous intéresser ici qu'au monde IP.

Le modèle OSI a dans ce contexte été fortement simplifié en quatre couches :




| | |
|---|---|
| OSI 5–7 | *La couche application regroupe les couches transport, présentation et application du modèle OSI* |
| OSI 4 | *Niveau transport* |
| OSI 3 | *Niveau réseau* |
| OSI 1–2 | *La couche d'interface matériel (ex. Ethernet) regroupe les couches 1 et 2 du modèle OSI.* |

### 5.2.1. PRINCIPAUX PROTOCOLES

| Protocole | Niveau | IETF | Fonction |
|---|---|---|---|
| UDP | Transport | RFC 768 | Envoi de datagrammes (paquets isolés) |
| TCP | Transport | RFC 793 | Envoi de données en mode paquet |
| RTP/RTCP | Transport | RFC 1889 | Envoi de flux temps réel (phonie, vidéo) |
| DNS | Session | RFC 1034 | Attribution de noms de domaines |
| HTTP | Application | RFC 2616 | Transactions client-serveur sur le Web |
| FTP | Application | RFC 959 | Échange de fichiers |
| POP<br>SMTP | Application | RFC 1939<br>RFC 821 | Deux protocoles utilisés par les applications de messagerie électronique |

### 5.2.2. UDP

UDP est un protocole niveau 4 qui se place au dessus d'IP.

UDP, c'est très simple, on envoie un paquet isolé et on espère qu'il va arriver à bon port. Ce paquet n'est lié en aucune sorte aux autres paquets qui sont envoyés sur la liaison. Il constitue un message à lui seul et on ne l'appelle pas paquet ni message, mais **datagramme**.

Le destinataire du datagramme est une application désignée par une adresse IP et un port.

Rien n'interdit de tronçonner un gros fichier en petits morceaux et d'envoyer chacun de ceux-ci dans un datagramme. Mais certains datagrammes pourront être manquants, erronés et il y a de fortes chances qu'ils arrivent dans le désordre, et ceci sans qu'UDP ait les moyens de s'en apercevoir. C'est donc à l'application de faire elle-même les contrôles d'intégrité nécessaires.

Ce n'est donc pas le moyen idéal pour faire de la transmission de gros fichiers, et c'est pourquoi a été développé TCP.

L'avantage incontestable d'UDP est sa rapidité, due justement à l'absence de contrôles, et UDP va être utilisé pour des transactions rapides et courtes, et surtout, pour la transmission de flux temps-réel, pour lesquels, on l'a vu, la perte d'un paquet n'est pas critique.

### 5.2.3. TCP

TCP est le protocole le plus utilisé en matière de transmission de fichiers.

TCP est également un protocole niveau 4 qui se place impérativement au dessus d'IP. Les deux sont tellement associés qu'on parle communément de **TCP/IP**.

Comme pour UDP, le destinataire est identifié pas son adresse IP + port.

Contrairement à UDP, les transactions TCP sont sécurisées.

Une connexion dans les couches basses est établie pour la durée totale de l'envoi du message et TCP va se charger du contrôle d'intégrité de l'information transmise, au moyen de plusieurs mécanismes.

A l'émission, TCP découpe le message en paquets et les numérote. En réception, TCP remet les paquets dans l'ordre et réassemble le message. Pour cela, il bufferise (stocke) quelques paquets lors de leur réception, afin que s'ils arrivent dans le désordre, il puisse les remettre dans l'ordre.

Les paquets sont envoyés en séquence, selon leur numéro. Cette numérisation est utilisée par le récepteur pour les remettre dans l'ordre, on l'a vu, et de pour détecter les paquets manquants.

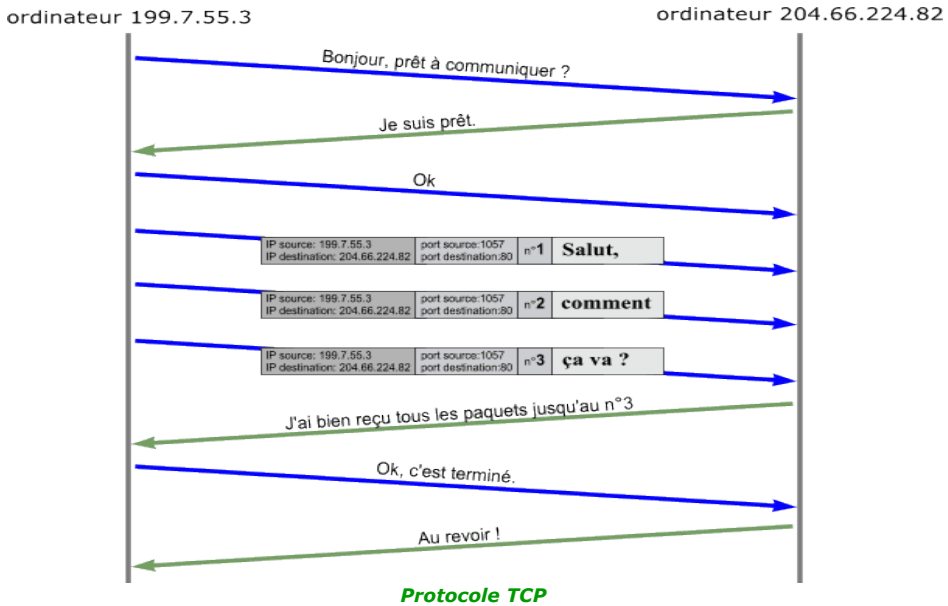
Les paquets sont envoyés également avec un code de contrôle, vérifié par le destinataire, afin de détecter les paquets erronés.

TCP commence par envoyer un certain nombre de paquets, typiquement 8, ce qu'on appelle une **fenêtre d'émission**.

Le destinataire vérifie ces 8 paquets. Il les remet dans l'ordre, vérifie les codes de contrôle et s'assure qu'il ne manque aucun paquet. Si tout est correct, il accuse réception **ACK** des huit paquets auprès de l'émetteur. Dans la négative, il acquitte négativement **NACK** en donnant le numéro du dernier paquet correctement reçu. Les paquets corrects reçus après le paquet erroné ou manquant sont rejetés. L'émetteur reprend alors l'émission, toujours dans une fenêtre de 8 paquets, à partir du paquet erroné ou manquant signalé dans le NACK du destinataire.

La transmission est de ce fait parfaitement sécurisée et le destinataire peut être sûr du message reçu. Par contre, ces mécanismes engendrent un important **overhead**, c'est-à-dire un trafic protocolaire qui grève le débit effectif de la liaison et qui est d'autant plus important qu'il y aura des répétitions.

Le petit exemple ci-dessous illustre les mécanismes de TCP/IP. On voit que la transaction (ici envoi de trois paquets) est précédé de messages d'établissement de connexion et se termine par des messages de fin de connexion.




***Protocole TCP***

### *5.2.4. RTP/RTCP*

Ces deux protocoles, qui sont en général associés, traitent l'envoi de flux temps réel et sont notamment utilisés en téléphonie sur IP.

RTP se place au-dessus d'UDP, et non de TCP trop bavard.

Il se charge du marquage des paquets par un horodatage et bufferise les paquets reçus. Les paquets sont restitués selon un cadencement régulier à leur destinataire.

RTP est associé à RTCP qui assure le contrôle de qualité de la réception. Dans des communications multicast (un vers plusieurs), RTCP contrôle le nombre de participants.

### 5.2.5. DNS

Nous avons vy qu'une adresse IP se présente sous la forme de 4 octets (IPv4) ou de 16 octets (IPv6).

Prenons l'exemple d'une adresse IPv4. Elle va se présenter sous le forme de 4 nombres séparés par des points, par exemple 192.0.65.163[1]. Pas commode de se souvenir de telles adresses, on a déjà bien du mal avec les numéros de téléphone !

Pour simplifier la vie des Internautes, on associe une adresse IP à un nom alphanumérique qu'on appelle **nom de domaine**, par exemple www.forumatena.org. La correspondance est gérée par des serveurs spécialisés, dits serveurs DNS.

Vu le nombre d'adresses IP qui traînent dans la nature, chaque serveur ne gère qu'un nombre limité de noms de domaines et doit s'adresser le cas échéant à d'autres serveurs pour trouver l'information désirée, selon un protocole nommé DNS.

L'attribution des noms de domaine ne se fait pas de manière anarchique, mais sous le contrôle de l'ICANN qui garantit l'unicité de chacun. Ainsi, il n'existe et n'existera dans le monde qu'un seul domaine forumatena.org.

### 5.2.6. HTTP

Bien sûr vous l'avez vu dans la fenêtre d'adresse de votre navigateur http://www.forumatena.org.

HTTP est un protocole client-serveur de niveau application, spécialement développé pour le Web. Il est utilisé par les navigateurs et par les aspirateurs de sites.

Bien que pouvant utiliser tout type de connexion, HTTP s'appuie essentiellement sur TCP/IP.

Sa version sécurisée https, que vous utilisez pour échanger des informations confidentielle, par exemple avec votre banquier, inclut un chiffrement SSL ou TLS.

### 5.2.7. FTP

FTP est également un protocole de niveau application qui s'appuie sur TCP/IP. Il est dédié aux échanges de fichiers binaires ou ASCII.

Il est utilisé pour copier, supprimer et modifier des fichiers sur un ordinateur distant et trouve en grande partie son application pour ma mise à jour de sites web.

### 5.2.8. POP/SMTP

Ces deux protocoles sont utilisés conjointement par les applications de messagerie électronique (email).

Chaque utilisateur de messagerie (par exemple Microsoft Outlook) possède un client messagerie (**MUA** Mail User Agent).

Le MUA émetteur envoie un message au serveur de messagerie (**MTA** Mail Transfer Agent) associé au domaine de messagerie de l 'émetteur par le protocole SMTP (par exemple yahoo.fr).

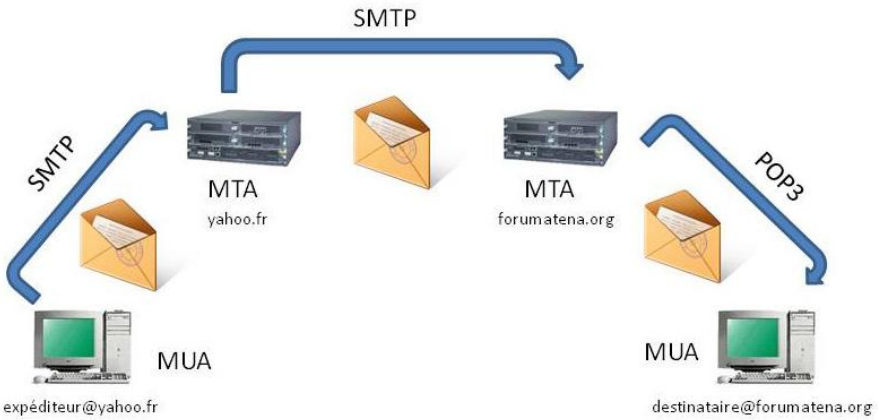
Le MTA émetteur, via Internet, transfère le message aux MTA destinataires par le protocole SMTP (par exemple forumatena.org).

Le destinataire, via son MUA, demande à son MTA les messages reçus au moyen du protocole POP3.

POP3 et SMTP sont tous deux des protocoles de niveau applicatif qui se placent au dessus de TCP/IP.

---

[1] *Ne cherchez pas, c'est une adresse inventée.*




***Fonctionnement d'une messagerie électronique***

# 6. LE RÉSEAU D'ACCÈS

## 6.1. DÉFINITION

Le réseau d'accès, ou encore **boucle locale** est la partie du réseau qui dessert l'utilisateur, particulier ou entreprise.

Celle-ci utilise diverses techniques filaires ou radio. nous allons nous intéresser ici aux techniques filaires.

On trouve tout d'abord le bon vieux **modem** qui, branché sur la prise téléphonique permet de connecter un ordinateur sur internet avec un fabuleux débit de 56 kbits/s.

Les entreprises utiliseront plus volontiers des lignes louées pour se raccorder aux serveurs informatiques distants et à l'Internet.

Du côté des particuliers, le grand vainqueur du moment est **l'ADSL** qui équipe de nombreux particuliers et petites entreprises avec des débits allant jusqu'à 20 Mbits/s. Mais les collectivités commencent à déployer des infrastructures de fibre optique, déjà disponibles dans les grandes agglomérations et qui pourront à terme prendre le relais de l'ADSL pour des débits de l'ordre de 100 Mbits/s.

## 6.2. L'ADSL

### 6.2.1. PRINCIPE

L'ADSL appartient à une familles de techniques DSL (Digital Subscriber Line) basées sur le transport d'informations numériques sur une simple ligne téléphonique.

Quand on considère le fil de cuivre de la ligne téléphonique de l'usager, celui-ci peut potentiellement transmettre des fréquences bien au-delà des 3300 Hz qui bornent le bande téléphonique. D'où l'idée d'utiliser toute cette bonne bande passante, située au-dessus de ce qu'utilise le téléphone pour transmettre des données.

Le A de ADSL signifie qu'il s'agit d'un échange d'informations asymétrique, c'est-à-dire plus lent dans le sens montant (de chez vous vers Internet) que dans le sens descendant (depuis Internet jusque chez vous). Ceci se justifie par le fait que les transactions dans le sens montant sont une requête courte d'un client vers un serveur, tandis que dans le sens descendant, la répons du serveur peut être très volumineuse.

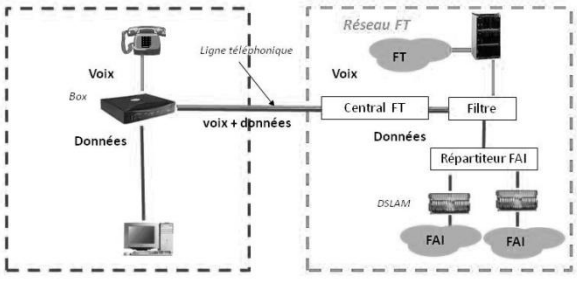
### 6.2.2. LE DÉGROUPAGE

La ligne téléphonique qui dessert l'usager depuis la central téléphonique appartient à France Télécom qui s'en sert pour… le téléphone !

Pour mettre en œuvre une liaison ADSL, il faut que les fournisseurs d'accès Internet puissent accéder à la ligne téléphonique. Ceci est le **dégroupage** issu de l'obligation imposée à France Télécom de louer ses infrastructures à d'autres opérateurs.

Le fournisseur d'accès Internet (FAI) installe au central téléphonique un DSLAM qui le relie ses serveurs informatiques. Bien sûr, plusieurs FAI vont venir installer leurs propres DSLAM au central.

- ***Dégroupage partiel***




***Configuration de dégroupage partiel***

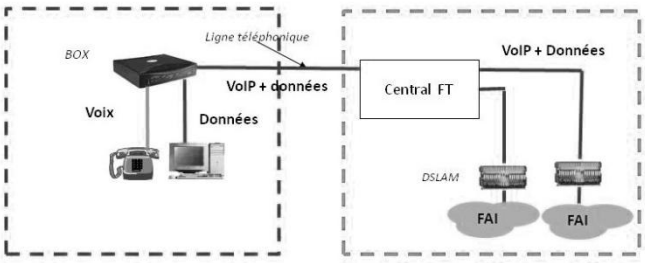
Dans cette configuration, le FAI loue à France Télécom les fréquences hautes de la ligne de l'usager.

France Télécom reste propriétaire et gestionnaire de la ligne et l'usager doit avoir un abonnement téléphonique en bonne et due forme auprès de France Télécom, en plus de l'abonnement Internet qu'il souscrit auprès de son FAI.

La ligne téléphonique supporte le téléphone et les données, simultanément puisque ceci se passe sur des fréquences différentes sur le fil de cuivre.

La Box, installée chez l'usager contient un multiplexeur/démultiplexeur agit comme un filtre en arrivée pour séparer les deux flux et les envoyer respectivement vers le téléphone et vers l'ordinateur. En sens inverse, il concentre les deux flux sur la ligne téléphonique. Une opération identique est effectuée au central.

- ***Le dégroupage total***




***Configuration de dégroupage total***

Ici, le FAI prend entièrement en charge la ligne de l'usager et en assure la gestion. France télécom en reste propriétaire mais la loue intégralement au FAI.

L'usager a un abonnement unique auprès de son FAI et n'a plus besoin d'abonnement France Télécom. Le FAI fournit Internet et le téléphone, mais ici, il n'est plus question du bon vieux téléphone traditionnel, encore utilisé en dégroupage partiel. Le téléphone, dûment numérisé, va se comporter comme un flux de données, la VoIP (voix sur IP). La Box assure la reconversion du flux VoIP en téléphone analogique. Et, cerise sur le gâteau, par le même chemin, le FAI peut également véhiculer la télévision.

# 7. LE RÉSEAU SANS FIL

## 7.1. INTRODUCTION AUX RÉSEAUX SANS FIL

### 7.1.1. POURQUOI UN RÉSEAU SANS FIL ?

Un réseau sans fil est un réseau qui raccorde des machines via une liaison radio, sur une infrastructure qui est elle-même filaire ou radio, voire sans infrastructure du tout.

Si la majorité des réseaux sont filaires, il est des cas où un réseau sans fil s'impose :

- raccordement d'équipements mobiles ou nomades,
- infrastructure radio pour réseaux nomades ou temporaires,
- difficulté de câblage (sites classés),
- desserte extérieure.

On retrouve la topologie des réseaux du § 0.

Les réseau nationaux (WAN) sont des réseaux opérés voix et données (GSM, UMTS…) qui interopèrent avec des LAN privés.

Les réseaux métropolitains (WMAN) sont parfois utilisés pour la desserte d'une ville ou d'un secteur en haut débit (boucle locale radio). Cette application est en diminution, suite à la généralisation de l'ADSL.

Les WLAN sont très répandus, seuls ou en complément d'un LAN filaire. Leur seconde application est le hotspot pour ouvrir un accès Internet dans un lieu public ou semi public.

Il reste les applications de type WPAN pour le raccordement d'équipement sans fil (souris, oreillette…).

### 7.1.2. LES PARTICULARITÉS DE LA RADIO

Si le réseau filaire perdure malgré la contrainte et le coût du câblage, c'est essentiellement pour des raisons de sécurité et de permanence de service.

- ***Premier risque : interception hors de l'entreprise.***

Sur un réseau câblé, on sait où sont les prises et la portée du réseau est facilement maîtrisable à l'intérieur de l'enceinte de l'entreprise. Par contre, la radio diffuse et ne s'arrête pas aux limites artificielles qui constituent le périmètre de l'entreprise. Les ondes radio rayonnent ainsi dans le domaine public, chez le voisin… Même si le réseau est à l'intérieur, les ondes passent par les fenêtres et dans une certaine mesure au travers des murs.

- ***Second risque : trous noirs***

La desserte d'un réseau filaire est exhaustive sur la zone à couvrir par l'installation de prises aux points de desserte souhaités. En radio, il peut se former des *trous noirs* où la réception radio est impossible, par exemple derrière un mur en béton, dans un bâtiment métallique…

L'architecture du réseau doit prendre en compte ces aléas de transmission, et ceci dès sa conception. Ceci implique une étude approfondie d'ingénierie radio avant l'installation. Même si toutes les précautions ont été prises au départ, une modification des bâtiments ou de l'environnement peuvent par la suite générer des trous noirs qui nécessiteront une nouvelle étude d'ingénierie pour une éventuelle modification du réseau.

- ***Troisième risque : sensibilité du réseau à l'environnement.***

Tout ce qui est émis sur un réseau filaire a l'assurance d'être reçu, malgré quelques erreurs de transmission. Un réseau radio lui, est sensible à des perturbations extérieures et non maîtrisables et la probabilité de recevoir un paquet non erroné chute de manière drastique.

Des conditions météorologiques particulières, des parasites électriques, voire le passage d'un camion, et autres sources de perturbations (éclairages néon, fours à micro-ondes, radioamateurs…) risquent de compromettre le bon fonctionnement du réseau radio. Des brouillages peuvent être dus à une émission radioélectrique voisine et peuvent également êtres malveillants.

- ***Quatrième risque : l'intrusion***

Sur un réseau filaire, nous l'avons vu, l'information passe sur des câbles et pas ailleurs, les prises sont connues et contrôlées. L'installation d'une prise par une tierce personne sur un réseau ne passe pas inaperçue.

En radio, des points d'accès réseau peuvent aisément être installés, pourvu qu'ils soient à portée radio d'un des composants du réseau, ouvrant ainsi la porte à des actes malveillants d'intrusion ou d'utilisation frauduleuse du réseau.

Ceci ne doit toutefois pas décourager les utilisateurs et futurs utilisateurs d'un réseau radio, mais montre la nécessité de bien protéger son réseau.

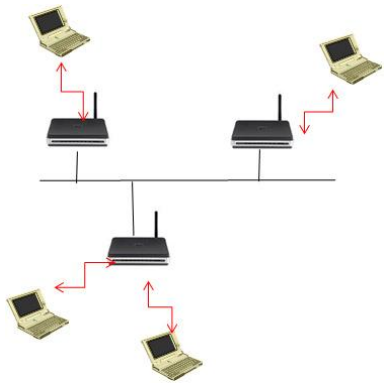
## 7.2. ARCHITECTURE DES RÉSEAUX SANS FIL

### 7.2.1. LE RÉSEAU CELLULAIRE

Un tel réseau, dit aussi **réseau d'infrastructure**, s'appuie sur une infrastructure filaire à laquelle sont raccordés des points d'accès (ou Access Point **AP**) qui rayonnent chacun sur une zone tridimensionnelle donnée nommée **cellule**.

Les équipements terminaux du réseau (ordinateurs, téléphones…) se raccordent par radio à un point d'accès à portée.

Un terminal peut être à portée de radio de plusieurs points d'accès. Il choisit alors celui pour lequel il reçoit le niveau de signal radio le plus élevé.

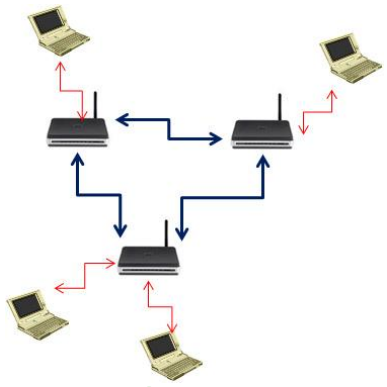


*Réseau cellulaire*

Cette architecture est typique du WLAN, seul ou en complément d'un LAN dont les points d'accès radio utilisent l'infrastructure.

### 7.2.2. LE RÉSEAU MESH

Il ressemble beaucoup au réseau précédent, mais ici, les points d'accès sont reliés par radio entre eux au lieu d'être raccordés sur une infrastructure filaire.



*Réseau mesh*

Cette architecture est assez rare en entreprise. Elle va essentiellement se trouver dans le monde des WMAN.

### 7.2.3. LE RÉSEAU AD-HOC

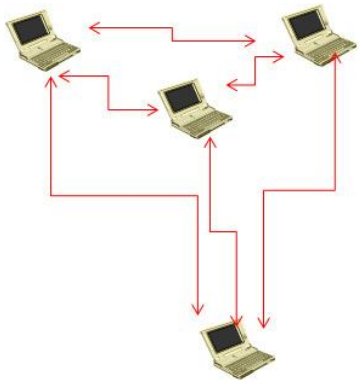
Il s'agit d'un réseau entièrement radio et sans infrastructure.

Toutes les machines du réseau sont reliées à toutes les autres qui sont à portée radio. Chaque machine est donc à la fois point d'accès et terminal.

Ne nécessitant aucune forme d'infrastructure, le réseau ad-hoc est séduisant par sa facilité de déploiement : on allume les machines et le réseau se met tout seul en place.

L'intégrité d'un réseau ad-hoc repose sur le fait que chaque machine doit toujours être à portée d'au moins une autre. Ceci ne peut être garanti quand les machines se déplacent et il y a toujours un risque de rupture de la continuité du réseau. Pour palier ce risque, il est indispensable de mettre en œuvre des mécanismes de supervision du réseau.

La structure ad-hoc est souvent utilisée pour raccorder les machines fixes, par exemple pour faire des réseaux de capteurs.



*Réseau ad-hoc*

Notons que le mode ad-hoc est particulièrement vulnérable quant à l'intrusion de machines externes animées de sentiments plus ou moins avouables. C'est pourquoi il est recommandé de désactiver le mode ad-hoc des ordinateurs quand il n'est pas nécessaire, car source d'attaque d'un réseau filaire par rebond.

## 7.3. PRINCIPAUX STANDARDS RADIO

### *7.3.1. Wi-Fi*

C'est sans doute le plus populaire pour la constitution des WLAN.

Wi-Fi est en fait un label d'interopérabilité et de conformité, attribué aux équipements conformes à un ensemble de normes 802.11 de l'IEEE. Il y a toute une famille de normes 802.11 (cf. <Réf. 2>) désignant soit des évolutions majeures du standard, soit des extensions.

La dernière en date est 802.11n que l'on trouve sur la quasi-totalité des équipements Wi-Fi commercialisés aujourd'hui.

La dernière en date est 802.11n que l'on trouve sur la quasi-totalité des équipements Wi-Fi commercialisés aujourd'hui. Dès 2013, des pré-version de la norme WiFi 802,11ac devraient être disponible sur le marché, qui pourrait être normalisé fin 2013 ou en 2014.

Wi-Fi opère dans les bandes de fréquences libre 2,4 GHz et 5,5 GHz, et est de ce fait utilisable sans redevance de licence et sans autorisation d'émission. Seules doivent être respectées des contraintes sur les niveaux d'émission, contraintes prises en compte par les constructeurs et équipementiers.

La portée maximale d'un réseau Wi-Fi est de l'ordre de la centaine de mètres pour des débits efficaces allant jusqu'à 100 Mbits/s, débit à prendre tout de même avec précaution car toujours dépendant des aléas de la transmission radio. De plus, il ne faut pas perdre de vue que le débit disponible sur le réseau doit être partagé par tous ses utilisateurs, ce qui peut réduire de manière drastique le débit utilisable par une machine lorsque tous les composants du réseau sont en transmission.

### *7.3.2. WiMAX*

A l'instar de Wi-Fi, WiMAX est un label d'interopérabilité et de conformité, applicable aux équipements conformes aux normes 802.16 de l'IEEE.

WiMAX opère dans plusieurs bandes de fréquences 2,5 GHz, 3,5 GHz et 5 GHz. Seule la bande 5 GHz est libre (sans licence), moyennant certaines restrictions. L'utilisation des deux autres est soumise au paiement d'une licence et à une autorisation d'émission.

Les réseaux WiMAX offrent des débits importants sur de longues distances. Il en existe deux grandes versions.

La première (et la plus ancienne), 802.16d couvre 5 à 15 km avec un débit efficace partageable de 40 Mbits/s. Il ne supporte que des terminaux fixes ou nomades.

La seconde, 802.16e introduit la mobilité et supporte des terminaux allant en théorie jusqu'à 60 km/h, en pratique 100-120 km/h. La gestion de la mobilité se fait au détriment du débit qui peut être détérioré, en fonction du bilan radio de la liaison, et au détriment de la portée qui tombe à 3 km.

Les réseaux WiMAX trouvent leur application dans les réseaux métropolitains et pour des flottes mobiles d'entreprise. Ils ont été présentés comme une solution de desserte en haut-débit des rones non éligibles à l'ADSL.

### 7.3.3. LTE

LTE est une technologie radio de 4ème génération pour des transmissions de données haut débit, avec un débit asymétrique, assez proche de WiMAX.

Poussés par le marché des opérateurs de téléphonie mobile, les fournisseurs de produits se tournent vers LTE qui en train de prendre le pas sur WiMAX et de nombreux réseaux WiMAX migrent actuellement vers LTE. On considère que WiMAX représente un marché mondial de moins de 200 million de terminaux, contre déjà plus de 300 pour LTE à fin 2012, avec un potentiel de plus de 6 milliards.

### 7.3.4. BLUETOOTH

Bluetooth est une technologie radio développée par Ericsson puis standardisée par l'IEEE en tant que 802.15.1.

Son principal usage est en point à point en remplacement du câble :

- périphériques informatiques (clavier, souris…),
- téléphones portables (oreillettes),
- liaison ordinateur – PDA ou smartphone,
- industrie (automobile…),
- équipement médical.

Comme Wi-Fi, Bluetooth fonctionne dans la bande 2,4 GHz sans licence.

Bluetooth définit plusieurs portées de 1 mètre à 100 mètres, selon la puissance d'émission. Il peut également proposer divers débits jusqu'à 20 Mbits/s.

### 7.3.5. ZIGBEE

Zigbee est une technologie radio qui s'appuie sur le standard 802.15.4 de l'IEEE. Zigbee est soutenu par un forum d'industriels, nommée la Zigbee alliance.

Comme Bluetooth, Zigbee est essentiellement utilisé en point à point ou pour constituer de très petits réseaux. La ressemblance s'arrête là. Les réseaux Zigbee sont des réseaux dits *ad-hoc*, qui comportent des nœuds qui s'autoconfigurent pour former un réseau maillé dont les liaisons sont radio.

Les composants Zigbee ont une portée et un débit inférieurs à ce que propose Bluetooth, mais en contre partie, fonctionnent à très faible puissance. Ceci donne des composants peu coûteux, très fiables et de très longue autonomie qui peuvent fonctionner une année entière, voire davantage, avec une simple pile.

Zigbee est essentiellement utilisé en milieu industriel, médical et dans les systèmes embarqués pour constituer des réseaux de capteurs et de télécommandes.

# 8. GLOSSAIRE

La plupart des définitions qui suivent sont extraites du *Lexique des TIC* de Forum Atena <Réf. 1>.

| | |
|---|---|
| Adresse IP | Une adresse associée à une machine extrémité d'une liaison IP. |
| Adresse MAC | Une adresse utilisée par les réseaux Ethernet, associée de manière fixe et unique à tout équipement de raccordement réseau. |
| ADSL | *Asymmetric Digital Subscriber Line* – Une technique voix et données qui définit des débits de données asymétriques. |
| ARQ | *Automatic Repeat reQuest* – Une fonction qui permet de redemander la retransmission d'une trame ou d'un paquet si une erreur de transmission est rencontrée. |
| ASCII | *American Standard Code for Information Interexchange* – Une technique de codage des caractères alphanumériques sur 7 bits, étendu aux caractères spéciaux par codage sur un octet. |
| BGP | *Border Gateway Protocol* – Un protocole qui effectue la fonction de routage netre les différents sous-réseaux qui constituent le réseau Internet. |
| CRC | *Cyclic Redundancy Code* – Un code de correction d'erreurs déduit d'un algorithme appliqué à un bloc d'information. |
| CSMA/CD | *Carrier Sense Multiple Access/Collision Detection* – Une méthode d'accès au média utilisée par les réseaux Ethernet. |
| Délai | Le temps écoulé entre l'émission d'une trame et sa réception. |
| DSN | *Domain Name Server* – Un système de serveurs qui associe des noms de domaines à des adresses IP. |
| DHCP | *Dynamic Host Control Protocol* – Un protocole qui permet d'associer dynamiquement une adresse IP à une machine. |
| Ethernet | Un protocole de l'IEEE qui définit la couche physique et l'accès au média pour le transport des trames dans des réseaux de type bus ou étoile. |
| ETSI | *European Telecommunication Standards Institute* – Un organisme de standardisation européen. |
| FTP | *File Transfer Protocol* – Un protocole de l'IETF pour échanger des données entre ordinateurs, qui s'appuie sur les protocoles TCP/IP. |
| Gigue | *Jitter* – La variation du délai. |
| HTTP | *HyperText Transfer Protocol* – Un protocole de l'IETF utilisé par les navigateurs qui définit un mode client-serveur sur le Web. |
| IEEE | *Institute of Electrical and Electronics Engineers* – Un organisme de standardisation américain actif dans le domaine des LAN et WLAN. |
| IETF | *Internet Enginnering Task Force* – Un groupe de travail qui produit sous forme de RFC (Request For Comments) les spécifications applicables au monde IP. |
| IP | *Internet Protocol* – Un protocole de l'IETF pour acheminer des paquets au travers d'un réseau. |
| ICANN | *Internet Corporation for Assigned Names and Numbers* – Un organisme américain qui gère les adresses IP et les noms de domaines |
| ISO | *International Standards Organisation* – Un organisme international qui produit les standards (normes ISO) applicables dans les domaines industriels et commerciaux. |
| ITU | *International Telecommunication Union* (UIT) en français) – Un organisme de standardisation international, rattaché aux Nations Unies, chargé de la standardisation, de la répartition du spectre radio et de l'organisation de l'interopérabilité des réseaux. |
| LAN | *Local Area Network* – Un réseau privé à l'échelle d'une entreprise ou d'un campus. |
| LLC | *Low Layer Control* - Une sous-couche de la couche liaison du modèle OSI qui assure le transfert des trames entre deux machines consécutives. |
| LTE | *Long Term Evolution* – Une technologie radio dite de 4$^{ème}$ génaration pour la desserte radio haut-débit. |
| MAC | *Media Access Protocol* – Une sous-couche de la couche liaison du modèle OSI qui assure le contrôle d'accès au média. |
| MTU | *Mail Transfer Agent* – Un logiciel serveur pour des applications de messagerie. |
| MUA | *Mail User Agent* – Un logiciel client pour des services de messagerie électronique. |

| | |
|---|---|
| OSI | *Open Systems Interconnection* (ISO en français, à ne pas confondre avec l'organisme) – Un modèle de communication en entre ordinateurs, défini par l'ISO. |
| PAN | *Personal Area Network* – Un réseau à l'échelle SoHo, domotique ou de la personne. |
| POP | *Post Office Protocol* – Un protocole de l'IETF point à point entre l'utilisateur et son serveur de messagerie pour récupérer les messages électroniques entrants. La version 3 (POP3) est actuellement utilisée par les messageries. |
| PPP | *Point-to-Point Protocol* – Un protocole qui met en place une liaison point à point entre deux machines. |
| QoS | *Quality of Service* – Une fonction qui définit et contrôle le bon fonctionnement d'un réseau, souvent employée pour garantir l'acheminement correct de flux temps-réel. |
| RTCP | *Real time Transport Control Protocol* – Un protocole de l'IETF complémentaire de RTP qui contrôle la qualité des transmissions temps réel. |
| RTP | *Real Time Protocol* – Un protocole de l'IETF qui se place au-dessus d'UDP pour compenser la gigue et le déséquencement des paquets sur des transactions de type temps-réel. |
| SMTP | *Simple Mail Transfer Protocol* – Un protocole de l'IETF entre l'utilisateur et son serveur de messagerie ainsi qu'entre serveurs de messagerie pour émettre des messages électroniques. |
| SSL | *Secure Socket Layer* – Une méthode de chiffrement développée en collaboration avec les grands groupes de cartes bancaires, progressivement abandonné au profit de TLS. |
| TCP | *Transmission Control Protocol* – Un protocole de l'IETF qui se place au-dessus d'IP pour gérer des transmissions connectées de manière fiable. |
| TLS | *Transport Layer Security* – Une évolution de SSL qui en corrige des failles de sécurité. |
| TRANSPAC | Un réseau de transmission de données développé par France Telecom à la fin des années 1970 et progressivement abandonné au profit d'Internet. Il supportait en autres le service Minitel. |
| UDP | *User Datagram Protocol* – Un protocole de l'IETF qui se place au-dessus d'IP pour gérer la transmission de datagrammes sans connexion et sans garantie du succès de la transaction. |
| USB | *Universal Serial Bus* – Un bus de transmission série pour raccorder des périphériques à un ordinateur. |
| WAN | *Wide Area Network* – Un réseau à l'échelle international ou nationale. |
| WLAN | *Wireless LAN* – Un réseau de type LAN sur une infrastructure sans fil. |
| X.25 | Un protocole de l'ITU pour acheminer des paquets au travers d'un réseau. |

# 9. BIBLIOGRAPHIE


<Réf. 1> Lexique des TIC *Edition Forum ATENA*

<Réf. 2> 802.11 dans tous ses états (Michèle Germain) *Livre blanc Forum Atena*

<Réf. 3> WiMAX à l'usage des communications haut débit *Edition Forum ATENA*

# 10. A PROPOS DE L'AUTEUR

**Michèle Germain** est ingénieur de l'Institut Supérieur d'Électronique de Paris.

Pour Matra Communication et EADS elle a participé à de grands projets de téléphonie et de radiocommunications (Matracom 6500, Radiocom 2000, réseaux PMR…).

Elle anime l'atelier d'écriture de Forum ATENA et elle a participé comme co-auteur et coordinatrice à la production de plusieurs des ouvrages de la Collection ATENA.

A l'ISEP, elle enseigne les techniques de radiocommunications professionnelles PMR.

Elle est auteur des livres « Informatique et numérique à l'usage des Seniors » et « Du téléphone au smartphone » (Éditions du puits fleuri).