République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie d'Oran - Mohamed Boudiaf

Faculté de Mathématique et d'Informatique

Département d'Informatique

Polycopié de cours :

Réseaux

2ème Année MI - Licence

Dr. Asmaa BOUGHRARA

2019-2020

Formation : *Licence -LMD*

Semestre : ***4***
Intitulé de l'UE : Fondamentale
Crédits : 5
Coefficients : *3*
Volume Horaire Hebdomadaire : 01h30 (Cours Magistral), 01h30 (TD) et 01h30 (TP)

Connaissances préalables recommandées

Architecture d'un système informatique, Représentations binaires de l'information, Système d'exploitation

Objectifs

Ce cours a pour but d'avoir une vue d'ensemble sur les réseaux d'entreprise, de présenter leur rôle ainsi que les différents équipements qui les composent. Il explique les principes fondamentaux des réseaux, tels que les modes de commutation ou la structuration des protocoles en couches. Il permet de comprendre le fonctionnement des principales techniques utilisées dans les réseaux modernes, sans rentrer dans le détail de chacune d'elles, en introduisant I' Internet comme un exemple de réseau.

Table des matières

Chapitre 1 : Introduction au Réseaux Informatiques

1.1 Définition

Un réseau informatique est un ensemble d'ordinateurs et/ou d'autres types de machine (ex : serveur, imprimante, ...etc) interconnectés, dans le but d'échanger des données numériques.

Deux ordinateurs connectés constituent déjà un réseau.

Le réseau informatique est utilisé pour faciliter la communication entre des personnes distantes et utiliser du matériel important mais distant comme une imprimante ou un serveur de stockage ou même des logiciels.

Remarque Dans un réseau informatique, les ordinateurs et les autres périphériques qui envoient et reçoivent les données sont appelés : **périphériques finaux** ou **machines hôtes.**

1.2 Caractéristiques des réseaux informatiques

Il existe plusieurs types de réseaux informatiques. La classification se fait suivant un critère comme :

1.2.1 Type d'interconnexion

Dans un réseau informatique, les périphériques finaux peuvent être interconnectés par une liaison :

- **filaire** : on parle alors de réseaux filaires ou réseau tout court ;
- **Non filaire** : (*Wireless Network*). Il est basé sur une liaison utilisant un support non câblé (onde radio, laser, ou infrarouge). L'objectif est d'offrir à l'utilisateur une liberté de mobilité tout en restant connecté.

1.2.2 La taille du réseau

En fonction de la localisation, la distance physique et le débit, on distingue différents types de réseaux :

1. *Personnel Area Network* : (PAN) petit réseau de quelques mètres (Max 10 m) Exemple : un cluster. Un ensemble d'unités centrales reliées entre elles pour fonctionner comme un seul ordinateur pour un calcul distribué ;
2. *Local Area Network :* (LAN) développer sur un ou plusieurs bâtiments. Il peut s'étendre de quelques mètres à quelques kilomètres et atteindre jusqu'à 1000 utilisateurs ;

Suivant les services fournis par les périphériques finaux d'un réseau, il est possible de distinguer deux modes de fonctionnement :

- Client/serveur : un périphérique central (appelé serveur) fournit des services à d'autres périphériques du réseau (appelés clients) ;
- Égal à Égal (Peer to Peer) : tous les périphériques ont un rôle similaire (à la fois client et serveur).

3. *Campus Area Network :* (CAN) réunis plusieurs réseaux locaux dans un campus (campus universitaire, base militaire) ;
4. *Metropolitan Area Network* : (Man) interconnecte plusieurs LAN (situés dans une même ville) avec des débits importants ;
5. *Wide Area Network* : (WAN) interconnecte plusieurs LAN à l'échelle d'un pays, ou de la planète entière. Le plus connu des WAN est Internet ;
6. *Global Area Network* : (GAN) c'est un réseau mondial qui relie des satellites.

Remarque

La classification suivant le critère de « la taille de réseaux » s'applique aussi sur les réseaux non filaires : WPAN (Wireless PAN), WLAN, WMAN.

1.2.3 Topologie

Il s'agit des différentes formes que peuvent prendre des réseaux. Il existe deux types de topologie- :

- **topologie physique** : représente l'apparence physique du réseau. Elle indique comment les différents périphériques sont raccordés physiquement (câblage). Il existe plusieurs topologies : bus, étoile (la plus utilisée), maillée (mesh), l'anneau, hybride et en arbre ;
- **topologie logique** : décrit la façon dont les données se déplacent via le réseau soit comment est distribué le droit à parole.

1.2.4 Type de liaison

On distingue deux types :

- ***point à point (Point-To-Point) :*** caractérisée par un canal de communication qui ne relie que deux périphériques (liaison point à point).
- ***multipoint*** : caractérisé par un canal de communication partagé par un ensemble de périphériques. Un périphérique peut utiliser l'un des trois modes de diffusion :

  - *unicasting* : envoi d'un message d'un périphérique source vers un périphérique destination. Cette dernière est identifiée par « une adresse unique » ;
  - *multicasting* (diffusion restreinte) : envoi d'un message à un ensemble restreints de périphériques (groupe de multicast) ;
  - *broadcasting* : envoi d'un message vers toutes les autres périphériques du réseau. L'adresse de destination est appelée : adresse de diffusion.

1.3 Topologies des réseaux

Un réseau informatique est un ensemble de périphériques reliés entre eux grâce à des liaisons et d'autres périphériques intermédiaires permettant d'assurer la bonne circulation des données. La disposition physique du réseau est appelée topologie physique. Il existe plusieurs :

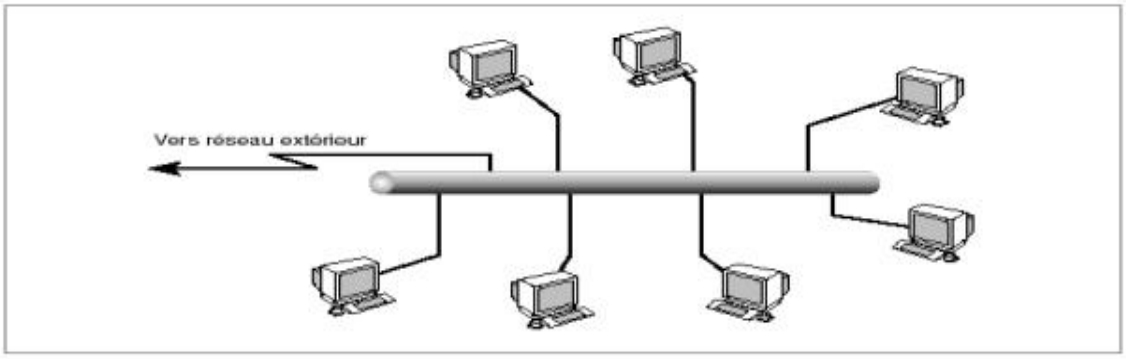
1.3.1 Topologie Point à point

C'est la topologie la plus simple, composée d'une liaison entre deux périphériques. Elle est donc très répandue.

1.3.2 Topologie en bus

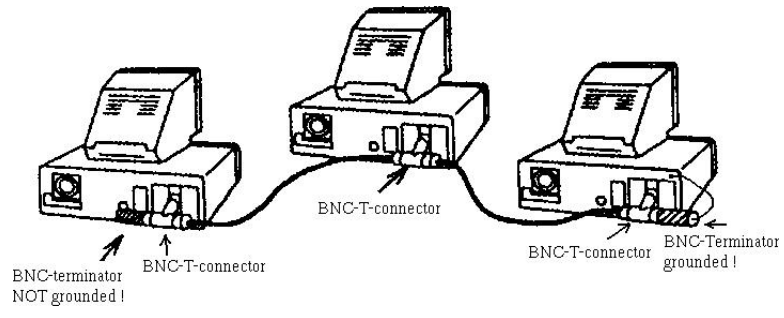
Tous les ordinateurs sont reliés au même câble, chaque extrémité est reliée à une terminaison.
Cette topologie présente l'avantage d'être facile à réaliser, par contre, en cas de rupture du câble ou une panne dans une carte réseau, toutes les communications seront interrompues.

Elle doit répondre au principe : 5-4-3. Soit : 5 segments, 4 répéteurs et 3 segments peuplés.



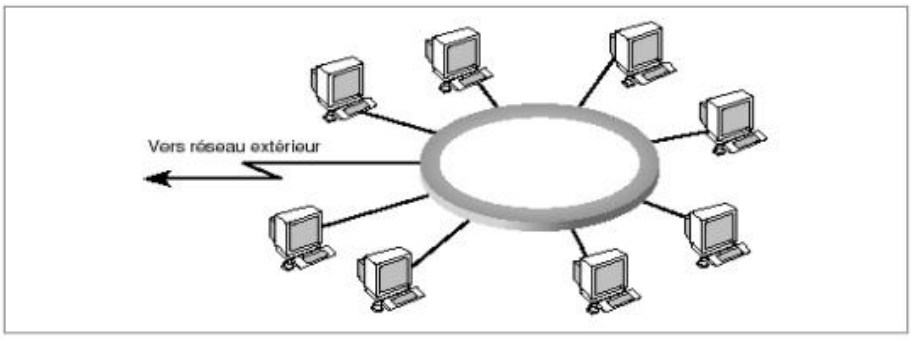
1.3.3 Type 10BASE2

Supporte des transmissions de données à des débits jusqu'à 10 Mbit/s sur câble coaxial d'une longueur de 185 mètres et 30 nœuds maximum par segment. Les connecteurs utilisés sont de types : connecteur BNC en T. La distance minimum entre stations = 0,5 m.



1.3.4 Topologie en Anneau

Les ordinateurs sont reliés à un seul câble en anneau, les signaux transitent dans une seule direction, chaque ordinateur joue le rôle de répéteur, régénérant le signal, ce qui en préserve la puissance.



Avantages

Accès égalitaire de toutes les stations.

Performances régulières même avec un grand nombre de stations.

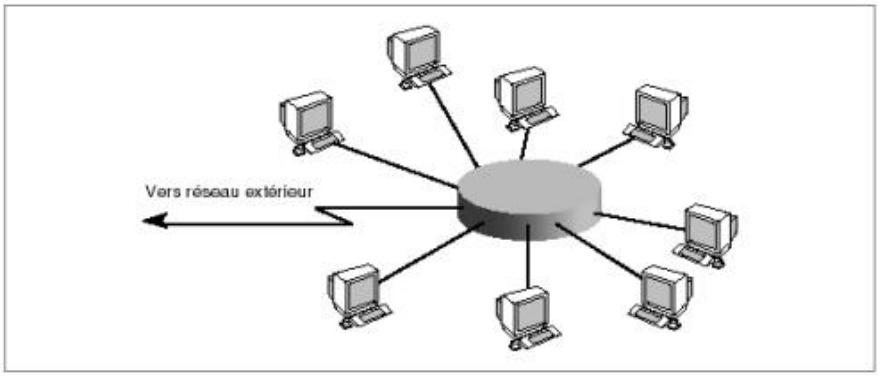
Inconvénients

Une panne d'ordinateur peut affecter le réseau.

1.3.5 Topologie en étoile

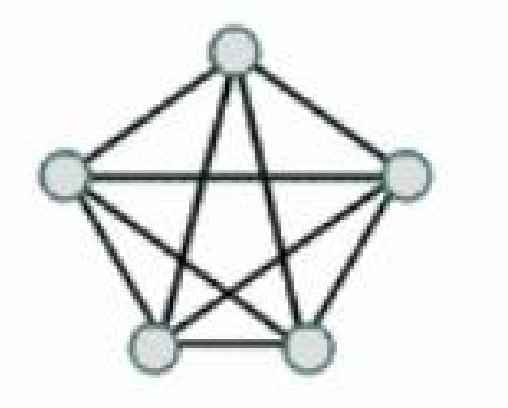
Tous les ordinateurs sont reliés à l'aide d'un câble à un nœud central. La plupart des réseaux locaux fonctionnent sur ce principe, en utilisant un switch comme nœud central.

Le câble employé dans cette topologie est généralement la paire torsadée, aussi appelée 10BASE-T. Une longueur de 100 mètres maximum est tolérée par segment, avec uniquement un nœud par segment. Les connecteurs sont du type RJ45.



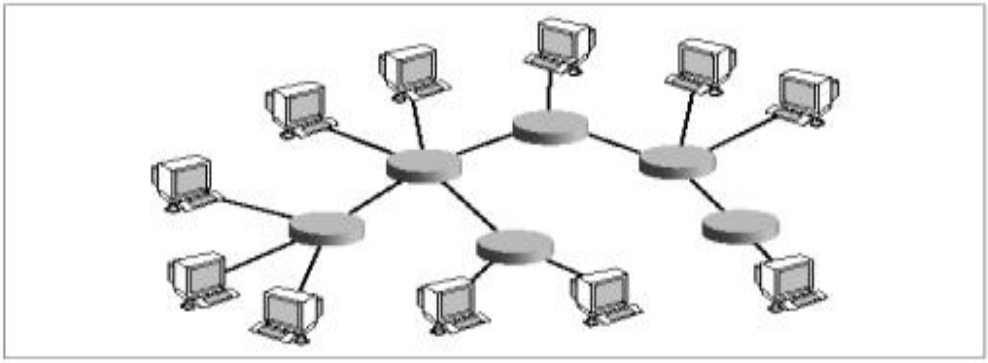
1.3.6 Topologie Maillée *(mesh)*

Chaque ordinateur est connecté aux autres par un câble séparé. Il peut être régulier si l'interconnexion est totale (n(n-1)/2 liaisons, avec n le nombre de machines) ou irrégulier si certaines connexions sont supprimées.



1.3.7 Topologie en arbre

Ou topologie « hiérarchique ». L'organisation est sous forme d'un arbre, avec plusieurs niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur, dans l'arborescence. L'inconvenant est que si un noeud « père » tombe en panne, la moitié du réseau sera paralysée.



1.3.8 Topologie Hub and Spoke

C'est une topologie en étoile mais pour les WAN. Un site central connecte plusieurs sites des filiales.

Remarque :

— Il est possible de trouver plusieurs topologies combinées, on parle alors de **topologie hybride.**

— Les topologies : Point à point, Maillée et Hub and spoke sont des topologies de réseau étendu. Tandis que le reste des topologies, sont pour les LAN.

1.4 Modèle en couche

L'utilisation d'un modèle en couches présente certains avantages :

— il décrit le fonctionnement des protocoles au sein de chacune des couches ;

— favorise le développement d'une technologie ou l'optimisation des fonctionnalités d'une couche, indépendamment des couches supérieures et inférieures.

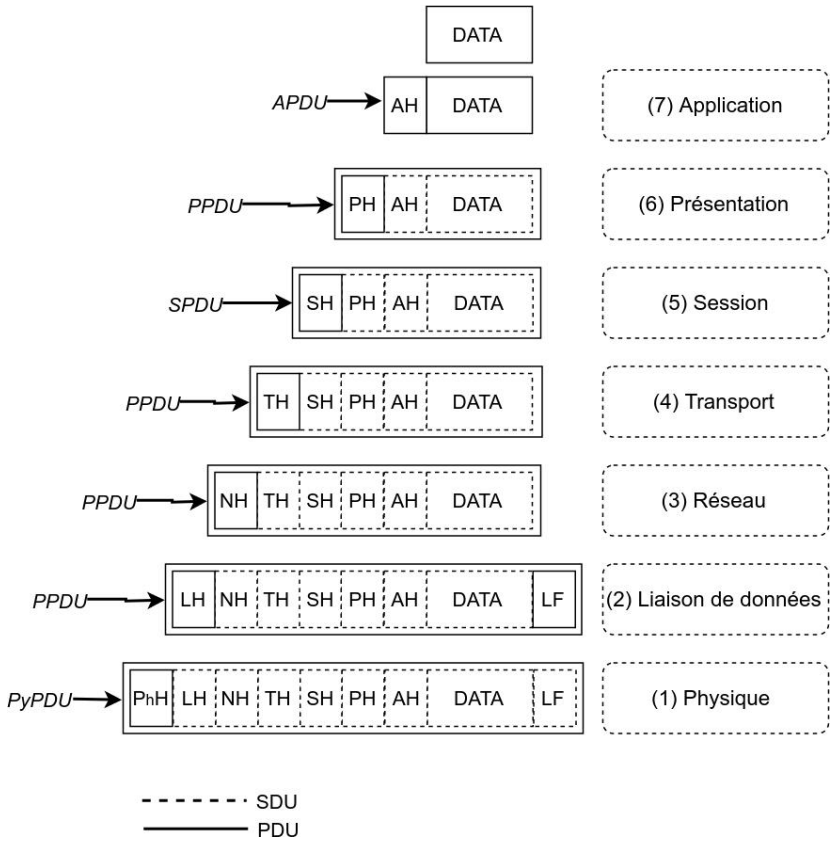
1.4.1 Types de modèles

Dans ces modèles en couche, il existe deux types : *modèle de protocole* et *modèle de référence*. La différence est que :

1. **Un modèle de protocole** correspond à la structure d'une suite de protocoles réellement utilisées dans le réseau de données. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent au niveau de chaque couche pour le transfert de données dans le réseau ***Internet***.
2. **Un modèle de référence** n'est pas destiné à être une spécification d'implémentation. L'objectif de ce modèle est d'aider à obtenir une compréhension plus claire des fonctions et du processus impliqués. Il sert de référence académique (Modèle théorique). Exemple le modèle OSI.

1.5 Description des modèles en couche

Modèle OSI		TCP/IP
7	Application	*Applications Services Internet*
6	Présentation	
5	Session	
4	Transport	*Transport (TCP)*
3	Réseau	*Internet (IP)*
2	Liaison	*Accès au Réseau*
1	Physique	



De manière générale, l'unité de données dans chaque couche s'appelle SDU (Service Data Unit). Le protocole opérationnel dans le niveau ajoute ses informations de contrôle appelé PCI (Protocol Control Information), c'est l'encapsulation.

Cette encapsulation au niveau d'une couche N est la concaténation du SDU et d'un entête (Header) et/ou en queue (Footer).

La forme constituée est appelée PDU (Protocol Data Unit).

Au niveau d'une couche, la PDU possède un nom spécifique : message (au niveau de la couche application), segment, paquet, trame ou bit. Sachant que le bit est la représentation binaire de la trame.

1.5.1 Modèle OSI

Les sept couches peuvent être regroupés en deux blocs, les couches basses (1, 2, 3, 4) qui assurent la transmission et l'acheminement des informations à travers le réseau et les couches hautes (5, 6,7).

1.4.2.1 Couche physique (couche 1) :

Réalise la transmission des éléments binaires constitutifs des trames sur le support suivant les caractéristiques physiques, électriques, optiques et mécaniques définies par des normes (Ethernet, Wifi, RS232…..).

1.4.2.2 Couche liaison (Couche 2) : Dans un réseau commuté, assure un service de transport des trames sur une ligne et dispose de moyens de détection d'erreurs et éventuellement de correction. La couche liaison peut aussi assurer un contrôle de flux au niveau trames. Le protocole associé définit la signification et l'organisation des trames (exemple : HDLC).

1.4.2.3 Couche réseau (couche 3) : assure l'acheminement ou le routage des données groupées en paquets au travers du réseau. D'autres fonctions telles que l'interconnexion de réseaux hétérogènes et le contrôle de congestion peuvent être réalisés dans cette couche.

1.4.2.4 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 est le plus souvent réalisé par cette couche.

1.4.2.5 Couche session (couche 5)

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.

La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

1.4.2.6 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 d'encryptage, de traduction, de compression,….). Par exemple choisir le format d'un entier (16, 32, 64 bits), l'ordre de transmission des bits (poids fort au début ou à la fin), conversion de codes (EBCDIC, ASCII,….).

1.4.2.7 Couche application (couche 7)

Est chargée de l'exécution de l'application et de son dialogue avec la couche 7 du destinataire

1.5.2 Le modèle TCP/IP

Le modèle TCP/IP est le résultat d'une implémentation. La normalisation est venue ensuite. Appeler « pile TCP/IP», car les protocoles TCP et IP ont un rôle majeur dans la mesure ou ils constituent l'implémentation la plus courante.

1.5.2.1 La couche application TCP/IP

Le modèle TCP/ IP a été développé avant le modèle OSI, n'empêche que la couche application TCP/IP comporte le fonctionnement des trois couches supérieures du modèle OSI : les couches application, présentation et session.

Cette couche contient plusieurs protocoles qui fournissent des fonctionnalités spécifiques à plusieurs applications d'utilisateur final : Le protocole DNS (Domain Name Service) HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), protocole Telnet (terminal network), FTP (File Transfer Protocol), ...etc.

1.5.2.2 La couche Transport TCP/IP

Cette couche a les mêmes fonctionnalités que la couche 4 du modèle OSI. Cependant, dans le mode de connexions, ou le modèle OSI propose uniquement la communication orientée connexion, alors que le modèle TCP/IP offre aux applications la possibilité d'utiliser deux modes :

— *Orienté connexion :* avec Transmission Control Protocol (TCP) pour un transport fiable ;

— *Sans connexion :* avec User Datagram Protocol (UDP) pour un transport non fiable.

1.5.2.3 La couche Internet

Cette couche possède le même rôle que la couche 3 du modèle OSI. Avec ce protocole, aucun chemin n'est établi à l'avance : il est dit que le protocole est « non orienté connexion ». Par opposition, au modèle OSI qui propose les deux types de communication au niveau de la couche 3.

1.5.2.4 La couche Accès Réseaux

Cette couche n'est pas spécifiée. Elle regroupe les fonctionnalités de la couche 1 et 2 du modèle OSI. Son implémentation est laissée libre. Elle dépend de la technologie utilisée sur le réseau local. Par exemple : Ethernet, qui est beaucoup utilisé dans les LAN.

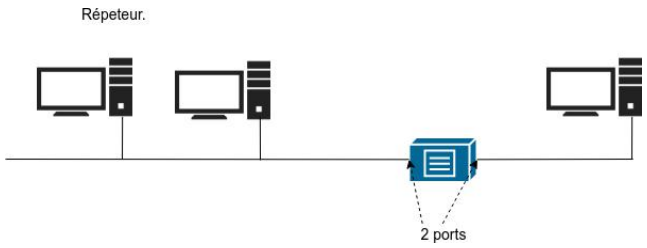
Les spécifications de cette couche ne sont pas visibles aux yeux de l'utilisateur. Dans la mesure, ou ces tâches sont réalisées par le système d'exploitation et les drivers permettant la connexion réseau.

Chaque protocole de cette couche possède une syntaxe pour la trame. Exemples de protocoles de la couche de liaison de données : Ethernet, Wireless Ethernet, SLIP, Token Ring, HDLC, PPP et ATM.

1.6 Les composants d'un système de transmission

1.6.1 Répéteur

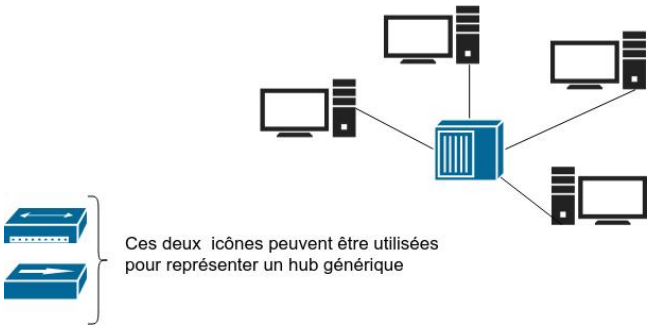
C'est un composant électronique simple non intelligent. Il permet d'augmenter la taille du réseau en amplifiant le signal.



1.6.2 Concentrateur (*Hub*)

C'est un dispositif électronique possédant 4 à 32 ports, permettant ainsi de relier plusieurs machines. Ce matériel n'est pas intelligent dans la mesure où il renvoie sur tous les ports les données qu'il reçoit. Ainsi, il réduit le débit en le répartissant entre les différents périphériques connectés à lui. Ce qui augmente la probabilité d'apparition de **collision**.

Le hub est considéré comme un répéteur multiport.



1.6.3 Pont (*Bridge*)

C'est un équipement qui relie deux réseaux (segments de réseaux) de même type (utilisant les mêmes protocoles) ou de technologies différentes. C'est un dispositif intelligent car il peut analyser l'adresse MAC de chaque trame pour ne laisser passer que celles qui sont adressées à l'autre réseau.

Quand une trame arrive au niveau du pont, ce dernier vérifie avec sa table de correspondance l'adresse de l'émetteur et du récepteur.

- S'il ne connaît pas l'émetteur alors il enregistre son adresse dans la table avec le N° de segment (Numéro de port) auquel il appartient ;
- S'il ne connaît pas le destinataire, il envoie, par défaut, la trame à l'autre segment ;
- Si l'émetteur et le destinataire sont situés du même côté, le pont ne fait rien, sinon il transmet la trame sur l'autre réseau.

Avec ce mécanisme de filtrage, un pont sépare le domaine de collision en deux.

1.6.4 Commutateur (*Switch*)

Un commutateur (un switch) est un pont qui possède plusieurs ports, Il est capable aussi d'orienter la trame vers la ligne de sortie correspondante au destinataire, contrairement au hub qui le fait transiter vers toutes les sorties.

Le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité. Les stations connectées au switch bénéficient de la totalité du débit du réseau.

1.6.5 Routeur

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter, il va ainsi déterminer la prochaine machine à laquelle les données vont être acheminées de manière à ce que le chemin choisi soit le meilleur. Pour y parvenir, les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée. Il existe de nombreux protocoles dédiés à cette tâche.

La passerelle :

Une passerelle (en anglais « gateway ») est un système matériel et logiciel permettant de faire la liaison entre deux réseaux, afin de faire l'interface entre des protocoles réseaux différents. Ce système offre en fait une interface entre deux réseaux hétérogènes.

Le B-Routeur :

Un B-Routeur (en anglais b-routeur, pour bridge-routeur) est un élément hybride associant les fonctionnalités d'un routeur et celles d'un pont. Ainsi, ce type de matériel permet de transférer d'un réseau à un autre les protocoles non routables et de router les autres. Plus exactement, le B-routeur agit en priorité comme un pont et route les paquets si cela n'est pas possible.

1.6.6 Pare-feu (*Firewall*)

C'est un dispositif matériel et/ou logiciel permettant de protéger un ordinateur ou tout le réseau des intrusions provenant d'un réseau externe (notamment internet). Il permet de filtrer les données suivant une politique de sécurité. Il existe plusieurs types de filtrage : filtrage simple (couche internet), filtrage dynamique (couche transport) et filtrage applicatif (couche application).

1.6.7 Modem

Pour **mod**ulateur-**dém**odulateur, il s'agit d'un périphérique servant à communiquer avec des utilisateurs distants par l'intermédiaire d'un réseau téléphonique.

Le réseau internet n'est capable de véhiculer que des données numériques (des zéros et des uns) et le réseau téléphonique n'est capable de transporter que du signale. Le modem permet, ainsi, de convertir un signal numérique en signal analogique et vice-versa.

Ainsi, un périphérique final peut communiquer sur Internet par l'intermédiaire du réseau téléphonique grâce au modem.

Le modem est un exemple d'un **ETCD (Equipement Terminal de circuit de données)**

1.6.8 Point d'accès

Il s'agit d'un dispositif qui permet aux périphériques sans fil de se connecter à un réseau câblé ou au réseau internet (voir chapitre 1 section 1.2.3, « mode infrastructure »).

1.6.9 Pont sans fil (*Wireless Bridge*)

Il est utilisé pour la transmission sur les réseaux locaux étendus. Il permet de joindre deux réseaux locaux distants (allant de 5000 mètres à 40 kilomètres) sans avoir recours à des câbles (liaison sans fil) et de relier ainsi plusieurs sites éloignés. Ce type d'équipement est coûteux.

Chapitre 2 : Couche Physique

Introduction

La couche physique est responsable de la transmission de la donnée convertie en signal sur le support de transmission.

2.1 Terminologie de Réseaux

La donnée binaire est véhiculée sur le support de transmission sous forme de signal ondulatoire résultant de la propagation d'un phénomène vibratoire. Trois types d'ondes existent :

- ondes électriques (câbles, fils, ...),
- ondes radio (faisceau hertzien, satellite),
- ondes lumineuses (fibres optiques, infrarouge).

Le signal peut être sous forme de carrée « signal numérique » ou sous forme sinusoïdale « signal analogique ».

Ainsi, on trouve deux types de transmission :

- transmission en bande base : pour le signal numérique
- transmission en large bande : pour le signal analogique.

2.2 Les modes de transmission :

a. Le mode Simplex :

La transmission ne s'effectue que dans un seul sens, utilisée surtout dans le domaine de la télévision et de la radio.

b. Le mode Semi-Duplex :

Chaque système fonctionne alternativement comme émetteur et comme récepteur. La transmission peut se faire dans les deux sens, mais jamais simultanément (Talkie-walkie).

c. Le mode Duplex-Intégral

Dans une telle application, il doit y avoir une liaison qui permette la transmission de deux canaux simultanés, cela peut se faire sur des voies distinctes (4 fils), soit sur la même voie (Liaison 2 fils avec multiplexage, téléphone par exemple).

2.3 Caractéristiques du support de transmission

1. Rapidité de Modulation et valence

IL y a une synchronisation du signal émis sur une horloge lorsqu'un élément binaire est transmis. La vitesse de l'horloge donne le débit de la ligne en bauds, c'est-à-dire le nombre de tops d'horloge par seconde (rapidité de modulation) par contre le débit binaire (noté D) est le nombre de bits émis par seconde.

Un signal a une valence de n si le nombre de niveaux transportés dans un intervalle de temps élémentaire est de $\mathbf{2^n}$.

La capacité de la ligne en nombre de bits par seconde vaut n multiplié par la vitesse en baud.

$$\mathbf{D = R * n}$$

Exemple : Une ligne d'une vitesse de 50 bauds avec une valence de 2 a une capacité de 100 b/s.

2 Largeur de bande et bande passante :

La largeur de bande est la zone de fréquence utilisée par un signal. Cette largeur de bande dépend de la façon dont le signal a été émis et de la qualité technique de la voie de transmission qui ne laisse passer que certaines fréquences nommées bande passante.

Exemple : Le réseau téléphonique commuté classique assure une transmission jugée correcte des fréquences comprises entre 300 et 3400 HZ, soit une bande passante de 3100 Hz.

Remarque : La bande passante limite la rapidité de modulation d'après le théorème de Nyquist qui a démontré que le nombre d'impulsions par unité de temps est deux fois la bande passante.

$$\mathbf{R= 2 * W}$$

R : rapidité de modulation
W : Bande passante

3.3 Vitesse de propagation

Selon les caractéristiques des matériaux traversés, le signal se propage différemment. La vitesse de propagation est indiqué en pourcentage de la vitesse de la lumière dans. Le vide soit 300000 Km/s. La vitesse de propagation varie couramment entre 6% et 85% .

3.4 Temps de propagation (T_p) :

Le temps de propagation (Tp) est le temps nécessaire à un signal pour parcourir un support d'un point à un autre.

Exemple : 5µs/Km pour un réseau Ethernet

Remarque : Le temps de propagation est généralement négligeable.

3.5 Temps de transmission (T_t)

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

Délai $_{transmission}$ = quantité information / débit

3.6 Délai d'acheminement (temps de traversée)

Il est égal au temps total mis par un message pour parvenir d'un point à un autre, c'est donc la somme des temps Tp et Tt

$$Da = Tp + Tt$$

Exemple :

Pour un message de 100 bits transmis à 2400 bit/s sur une paire torsadée d'une longueur de 100 Km avec un temps de propagation de 10µs/Km, on obtient :

Tt=100/2400=42ms

Tp= 10*100=1000 µs = 1ms

3.7 Débits nominal et utile

– Le débit nominal d'un réseau est la quantité théorique maximale d'information pouvant être transmise par unité de temps.

– Le débit utile est la quantité d'information effectivement transmise par unité de temps.

3.8 Taux d'utilisation :

Le taux d'utilisation du réseau est donc le rapport du débit utile au débit nominal :

Taux d'utilisation = Débit utile / Débit nominal

Le taux d'utilisation est inférieur à 100%. Ceci est dû entre autres aux pertes sur la voie de communication et à l'intervalle de temps laissé entre l'envoi de deux messages.

4. Les différentes méthodes de transmission :

L'information binaire peut être transportée de différentes façons sur les voies de transmission.

La question à poser : Comment un émetteur peut-il coder puis envoyer un signal pour que le récepteur le reconnaisse comme un 1 ou 0.

4.1 La transmission en bande de base

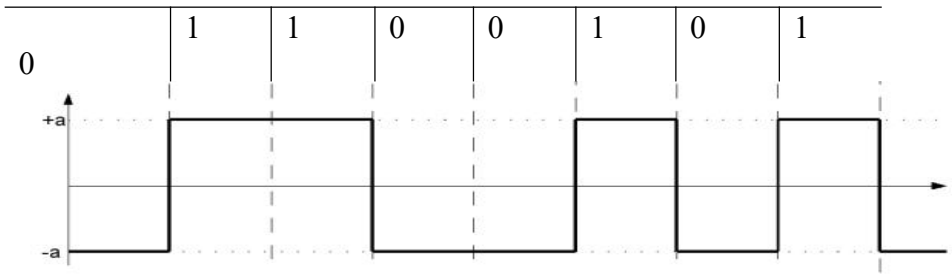
Elle consiste à transmettre l'information sous forme numérique (digitale), l'inconvénient de cette méthode est l'atténuation du signal sur une grande distance. C'est la méthode de transmission la plus utilisée dans les réseaux locaux. Plusieurs codages existent pour ce mode de transmission.

4.1.1 Le codage NRZ

Utilise une tension positive pour représenter un 1 binaire et une tension négative pour représenter un 0 binaire.

Il est généralement utilisé pour des connexions sur de petites distances comme entre un ordinateur et un modem externe, liaison Série : RS-232.

Exemple : 01100101



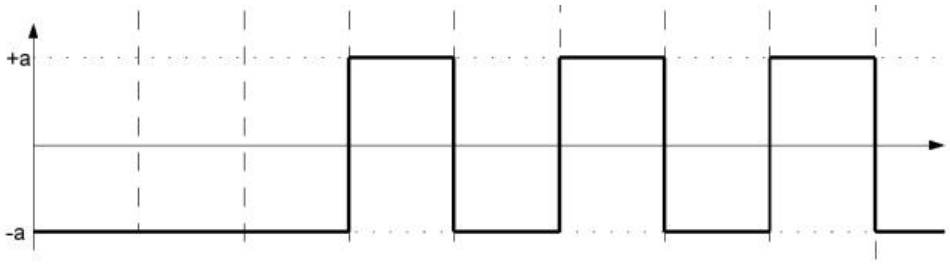
4.1.2 Le codage NRZI :

Le codage NRZI code les bits suivants la présence ou l'absence de changement de tension. Une variation du signal d'une tension haute à une tension basse ou inversement correspond à un binaire et l'absence de variation correspond à un 0 binaire.

Ici, le signal est codé suivant les règles suivantes :

- bit de donnée à 0 -> la tension reste constante à chaque période
- bit de donnée à 1 -> la tension s'inverse à chaque période

Exemple : 00011111



Il est utilisé pour des connexions USB

4.1.3 Le codage Manchester :

Une solution permettant de décaler le spectre du signal vers les fréquences plus élevées consiste à coder les états de base par des transitions et non par des niveaux. C'est la solution adoptée par le codage Manchester, encore appelé codage biphase.

Avec ce code, c'est le point ou le signal change qui représente la valeur du bit transmis. Cela se traduit par les règles suivantes :

- bit de donnée à 0 -> un front montant (Transition de bas en haut)
- bit de donnée à 1 -> un front descendant (Transition de haut en bas)

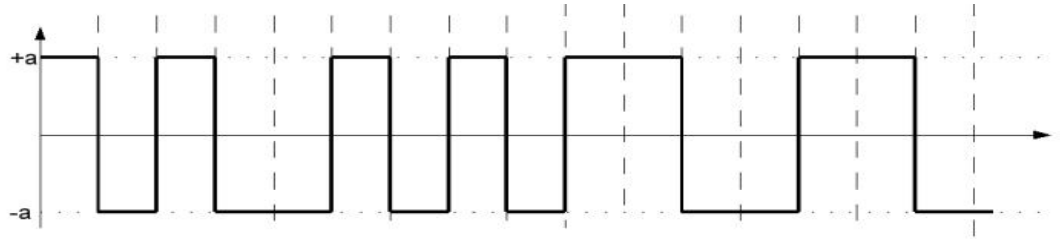
Ce codage est utilisé dans les réseaux Ethernet.

Caractéristiques de ce codage :

- Bonne résistance au bruit (2 niveaux)
- Bonne adaptation aux supports à bande passante large
- Beaucoup de transitions, donc facilité de synchronisation d'horloge

Le principal inconvénient de ce code réside dans la grande largeur de son spectre, ce qui le confine aux supports à large bande comme les câbles coaxiaux

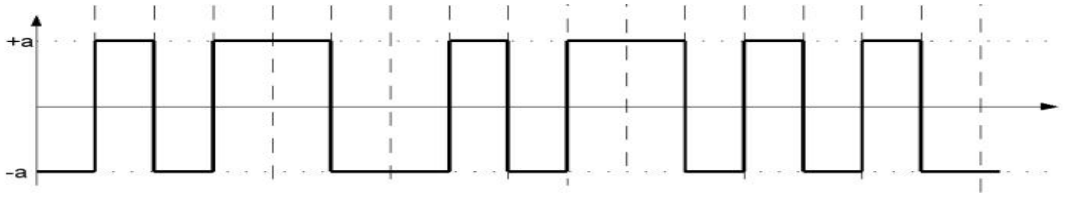
Exemple : 11000101



4.1.4 Le codage Manchester Différentiel

Il y a changement de tension au début de la transmission d'un 0 et pas au début d'un 1.

Exemple : 00110100



Il est utilisé pour des réseaux Token Ring

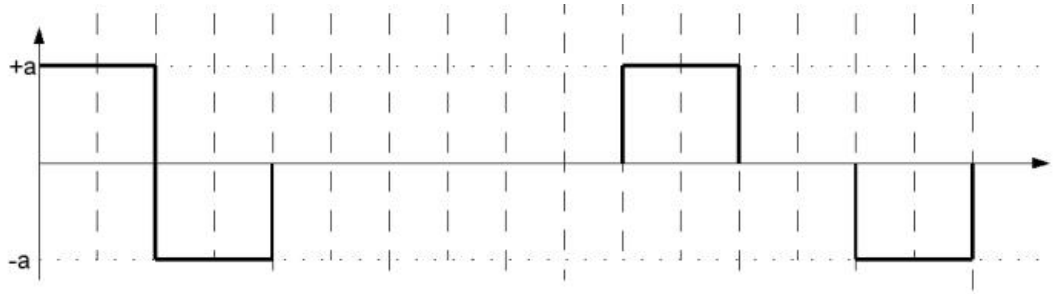
4.1.5 Le codage bipolaire

Le codage bipolaire simple est un codage sur trois niveaux. Il propose trois états de grandeur transportée sur le support physique :

La valeur 0 lorsque le bit est à 0

Alternativement v est –v lorsque le bit est à 1.

Exemple : 11000101

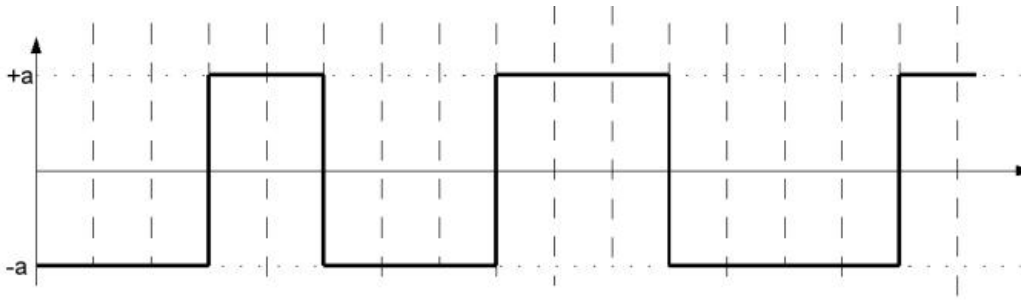


4.1.6 Le codage Miller (Delay)

Le code de Miller s'obtient à partir du codage Manchester dans lequel on supprime une transition sur deux. En d'autres termes, les règles d'encodages prennent la forme suivante :

- Si le bit de donnée vaut 1, alors on insère une transition au milieu de l'intervalle significatif
- Si le bit de donnée vaut 0, alors pas de transition au milieu de l'intervalle significatif, mais si le bit suivant vaut 0, alors on place une transition à la fin de l'intervalle significatif

Exemple : 01100101



Les caractéristiques de ce code sont les suivantes :

- Permet des débits élevés sur support à bande passante limitée
- Une puissance non nulle est transmise pour la fréquence nulle, ce qui peut introduire des distorsions

Le principal inconvénient de ce code tient en une moins grande immunité vis-à-vis du bruit que les codes précédents.

4.2 La transmission en large bande ou modulation

Signalisation

Dans une transmission, la communication peut être en analogique ou en numérique. Le terme analogique désigne les informations qui se présentent sous forme continue. Le terme numérique désigne des informations qui se présentent sous forme discrète (des états discrets).

Le processus par lequel un ordinateur interagit avec le support de transmission du réseau et envoie un signal sur ce support s'appelle signalisation.

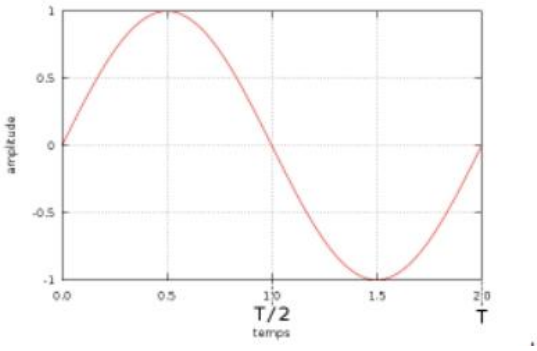
A) Les signaux utilisés

Les signaux digitaux sont difficiles à transmettre sur des longues distances, les signaux analogiques seront alors utilisés.

Le signal analogique le plus élémentaire est l'onde sinusoïdale dont l'équation est :

$$a(t)= A . \sin(w.t+\phi)$$

- **a(t)** : L'amplitude à l'instant t
- **A** : l'amplitude maximale
- **W** : pulsation=2.π.F (F exprime la fréquence en hertz) nombre de périodes par seconde.
- **T** : temps en seconde
- **ϕ** :Phase (décalage de l'onde par rapport à l'origine)



L'onde sinusoïdale

A, F et ϕ sont les trois caractéristiques fondamentales d'une onde sinusoïdale.

B) Déformation des signaux et caractéristiques des médias

Les signaux sont souvent soumis à des phénomènes qui les altèrent et qui sont liés à la nature du support qui sert pour la transmission ie le média (paire torsadée, câble coaxial, fibre optique,…).

Parmi ces phénomènes nous citons :

B.1) Affaiblissement ou Atténuation :

Le signal émis est reçu avec une moindre importance (affaiblissement). Les lignes de transmission doivent répondre à certaines caractéristiques quant à l'affaiblissement qu'elles apportent aux signaux. L'atténuation s'exprime en Db par unité de temps, elle traduit l'énergie perdue par le signal au cours de sa propagation. Elle dépend de l'impédance du câble et de la fréquence des signaux.

$$A = 10 \log(P1/P2)$$

- P1 : Puissance du signal en entrée.
- P2 : puissance du signal en sortie.

Les supports sont jugés selon qu'ils offrent ou nom une faible atténuation.

B.2) Distorsions :

Deux types de distorsions :

1) ***Distorsions d'amplitude*** **:** Qui amplifient ou diminuent l'amplitude normale du signal à un instant t.
2) ***Distorsions de phase*** **:** Qui provoquent un déphasage de l'onde par rapport à la porteuse.

B.3) Bruits – Diaphonie – Paradiaphonie

Bruits

Lors de la transmission, des perturbations de la ligne physique peuvent se produire. On parle alors de bruit.

Le bruit est un processus aléatoire, décrit par une fonction b(t), si s(t) est le signal transmis, le signal parvenant au récepteur s'écrit s(t)+b(t). Le rapport signal/bruit est une caractéristique du canal. On l'estime par une valeur moyenne sur un intervalle de temps exprimé en Décibel (db), il s'écrit s/b.

La capacité maximale d'un canal qui est soumis à un bruit est donnée par le théorème de Shannon, selon la formule suivante :

$$C = W \log_2(1 + S/b)$$

- C : la capacité Maximale en bit par seconde.
- W : bande passante en HZ

Exemple : sur une ligne de téléphone dont la bande passante est de 3200 Hz pour un rapport signal/bruit=10 db on peut atteindre 10 kbits/s.

Remarque

Deux types de bruits existent :

- Le bruit blanc : dû à l'agitation thermique dans les conducteurs.
- Le bruit impulsif : dû aux signaux parasites extérieurs.

La diaphonie

C'est un phénomène dû au couplage inductif des paires proches, qui limite l'utilisation de la paire torsadée à des distances relativement faibles.

La paradiaphonie

Indique l'atténuation du signal transmis sur une paire, en fonction du signal transmis sur une paire voisine. Elle s'exprime en db.

Modulation

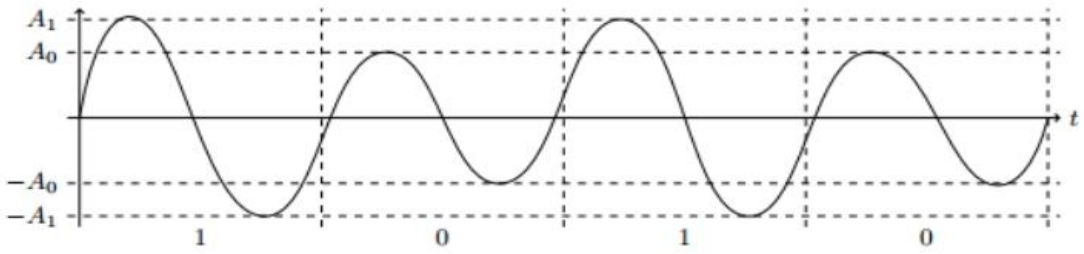
Les recherches en transmission de signaux ont montré qu'un signal oscillant continuellement se propageait mieux qu'un autre signal.

La plupart des systèmes de communication longue distance envoient un signal qui oscille en permanence, les ondes sont généralement sinusoïdales pour envoyer des données par-dessus le signal contenu, l'émetteur modifie légèrement la porteuse de manière à refléter les informations.

Ce type de modification de la porteuse s'appelle modulation. Plusieurs types de modulations existent :

4.2.1 La modulation d'amplitude

Dans ce type de transmission, le signal modulé s'obtient en associant à une information logique 1 une amplitude donnée (exemple : amplitude élevée) et une autre amplitude à un 0 logique (exple : amplitude basse)

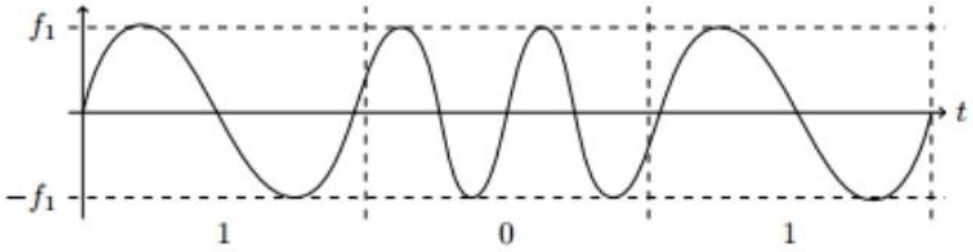


Données représentées par une modulation d'amplitude

4.2.2 La modulation de fréquence :

Cette méthode consiste à modifier la fréquence de la porteuse pour représenter les données.

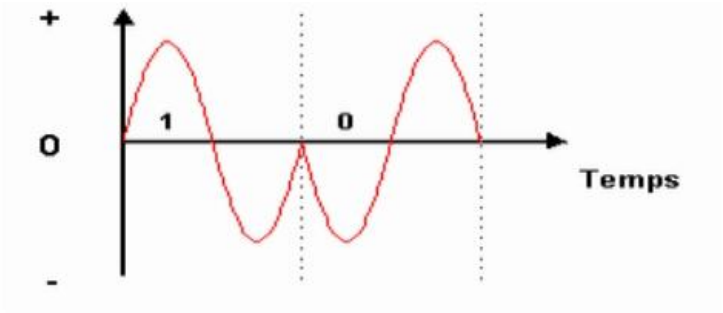
Par exemple : une hausse de la fréquence peut représenter un 1 binaire et une diminution de la fréquence un 0 binaire.



Données représentées par une modulation de fréquence

4.2.3 La modulation de phase

Dans ce type de transmission, le signal modulé s'obtient en générant un déphasage représentatif des 0 et 1 logique à transmettre. Ainsi il est possible d'adjoindre au 1 logique un déphasage de Pi et au 0 logique un déphasage nul par rapport à l'onde porteuse de référence



Données représentées par une modulation de phase

Modulation à 4 niveaux de phase

Exemple :

–Phase de 0° pour 01

–Phase de 90° pour 00

–Phase de 180° pour 10

–Phase de 270° pour 11

La modulation de phase est la plus employée dans les modems

5. Le multiplexage

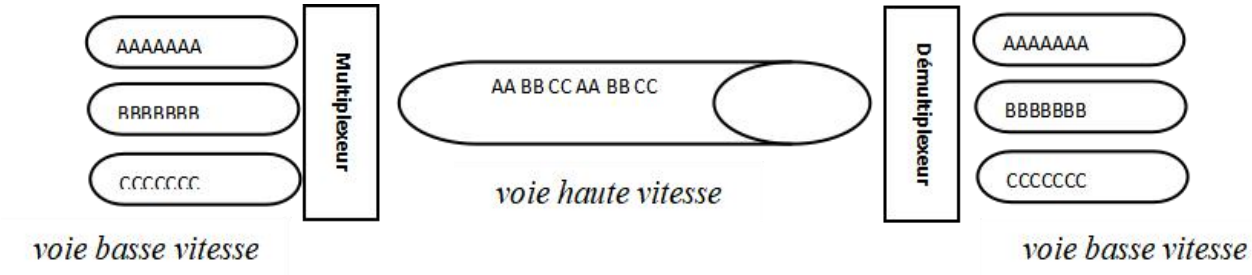
Le multiplexage consiste à faire transiter sur une seule et même ligne de liaison, dite voie haute vitesse, des communications (dite voie basse vitesse) appartenant à plusieurs paires d'équipements émetteurs ou/et récepteurs. → Partage de la bande passante du canal

Plusieurs techniques sont possibles :

5.1 Multiplexage temporel TDMA (Time Division Multiplexing Access)

Ou *MRT (Multiplexage à répartition dans le temps)*

Les différentes voie basse vitesse partagent l'utilisation de la voie haute vitesse en l'attribuant successivement un intervalle de temps (IT), intervalle pendant chacune d'elle envoie.

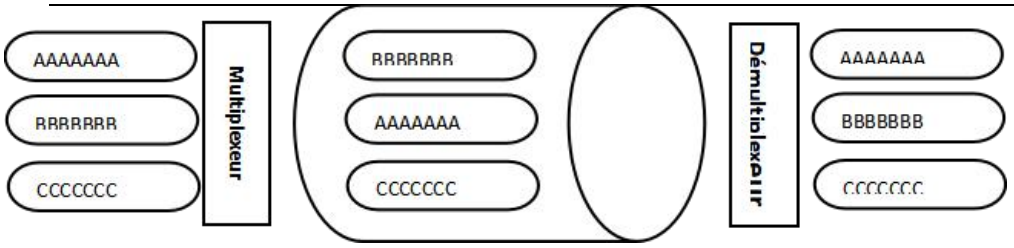


Le multiplexage temporel permet une meilleure utilisation de la bande passante. Sauf que s'il y a des données qui sont prêtes sur une voie, mais ce n'est pas leur tour, il faudra ainsi mémoriser ces données en attendant leur tour.

5.2 Multiplexage fréquentiel FDM (Frequency Division Multiplexing)

Ou multiplexage par répartition de fréquence (MRF)

Il consiste à découpe la bande passante (large) en plusieurs sous bande (étroite) et affecter à chaque voie de transmission (voie basse vitesse) une bande passante particulière en s'assurant qu'aucune bande passante de voie basse vitesse ne se chevauche.



L'ADSL (Asynchronous Digital Subscriber Line) est un bon exemple de l'utilisation de FDM.

Sachant qu'une ligne téléphonique possède une bande passante d'environ 1 Mhz dans laquelle seule, une largeur de bande de 4 Khz est utilisée pour les communications téléphoniques. Il reste donc une bande passante importante disponible pour un autre usage.

5.3 Le multiplexage en longueur d'onde (WDM)

Le FDM est utilisé dans les transmissions de type analogiques et dans le cas de supports à large bande passante (ex. hertzien, satellite). Dans le cadre des réseaux de fibres optiques, le Multiplexage en Longueur d'Onde ou WDM (Wavelength DivisionMultiplexing) est utilisée.

2.4 Supports guidés et non-guidés

Les périphériques réseaux (finaux et intermédiaires) sont reliés par des supports de transmission. La représentation des bits (type de signal) dépend du type de support.

Pour un support à câble de cuivre, les signaux sont des variations d'impulsions électriques. Pour la fibre optique, les signaux sont des variations lumineuses. Pour les supports sans fil, les signaux sont des variations de transmissions radio :

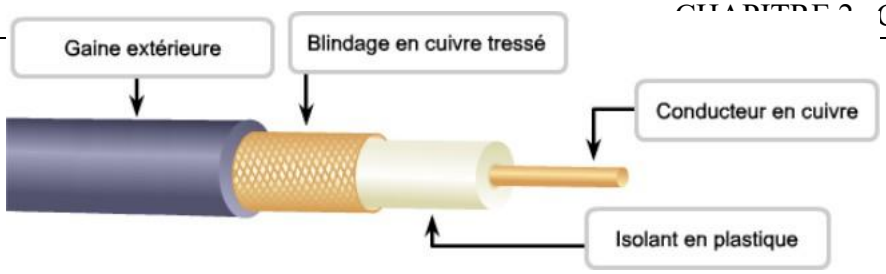
2.4.1 Supports guidés

2.4.1.1 Câble cuivré

1) Le câble coaxial

Il était longtemps le câble le plus utilisé car il est peu coûteux et facilement manipulable. Il est composé de

- **La gaine :** généralement en caoutchouc. Elle protège le câble de l'environnement extérieur ;
- **Le blindage :** il s'agit d'une tresse métallique. Elle permet de protéger les données transmises des parasites (bruit) ;
- **L'isolant :** à base d'un matériau diélectrique. Elle empêche tout contact avec le blindage, provoquand des courts-circuits ;
- **L'âme :** c'est le fil conducteur. Il peut être un seul brin en cuivre ou plusieurs brins torsadés.



Il existe deux types de câbles coaxiaux :

1. **Le 10Base2** : (**10** MBps sur **2**00 yards) c'est un câble coaxial fin de diamètre 6 mm aussi appelé *Thinnet* ou *CheaperNet*. Il permet de transporter, sans affaiblissement, des signaux sur une distance atteignant 185 mètres.
2. **Le 10Base5** : (**10** MBps sur **5**00 m) c'est un câble coaxial épais blindé de plus gros diamètre : 12 mm (en raison de l'épaisseur de son âme). Aussi appelé *Thicknet*, *Thick Ethernet* ou *yellow Cable*. Il permet de transmettre, sans affaiblissement, des signaux sur une distance atteignant 500 mètres avec une bande passante égale à 10 Mbps.

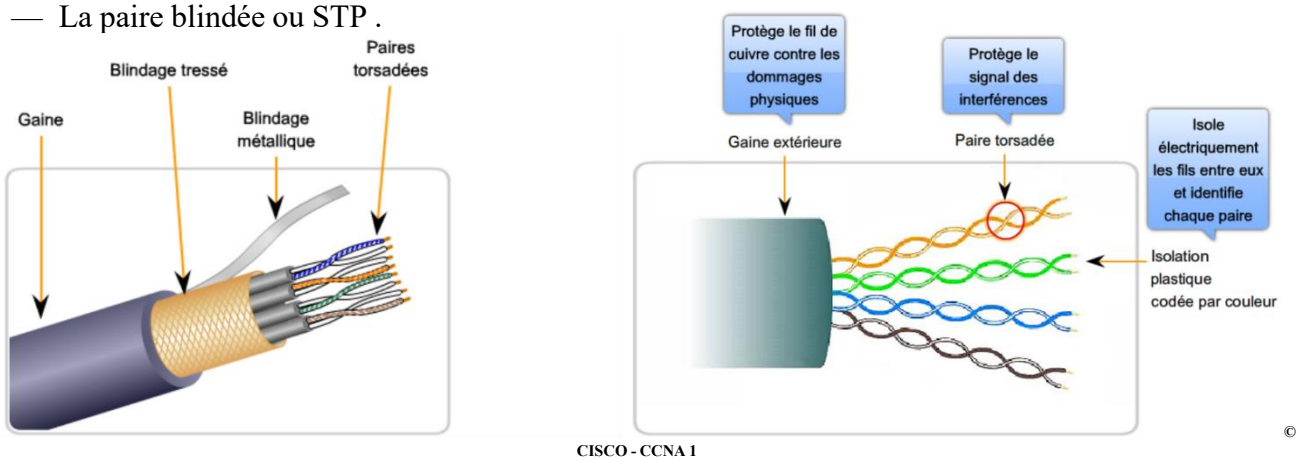
Le câble coaxial est d'une qualité de transmission et débits meilleurs que les paires torsadées et peut-être utilisé en point à point ou en diffusion. Cependant, il est un peu plus cher.

2) Le câble à paire torsadée

En anglais *Twisted-pair cable* est constitué de plusieurs paires torsadées regroupées et recouvertes d'isolants. La torsion a pour objectif de supprimer les bruits (interférences électriques) dus aux paires de file. La paire torsadée répond aux spécifications de la norme « 10 base T » (**10** MBps sur 100 m). Elle est adaptée à la mise en réseau local. Il existe plusieurs types de paires torsadées :

— La paire non blindée ou UTP ;

— La paire blindée ou STP .



<u>UTP (*Unshielded Twisted-Pair*)</u>

Utilisé à l'origine pour les lignes téléphoniques, actuellement il est très utilisé pour les réseaux locaux.

La norme « Commercial Building Wiring Standard 568 » de l'EIA/TIA (*Electronic Industries Association / Telecommunication Industries Association*) classe les câbles UTP en 5 catégories :

1. ***Catégorie 1 :*** Câble téléphonique traditionnel (signal analogique) ;
2. ***Catégorie 2 :*** composé de 4 paires torsadées. Il offre une bande passante égale à 4 Mbit/s ;
3. ***Catégorie 3 :*** composé de 4 paires torsadées et de 3 torsions par pied avec un débit de 10 Mbit/s maximum ;
4. ***Catégorie 4 :*** composé de 4 paires torsadées avec un débit de 16 Mbit/s maximum ;
5. ***Catégorie 5 :*** composé de 4 paires torsadées avec un débit de 100 Mbit/s maximum ;

En raison de son faible blindage, ce type de câble est sensible aux interférences.

STP (*Shielded Twisted-Pair*)

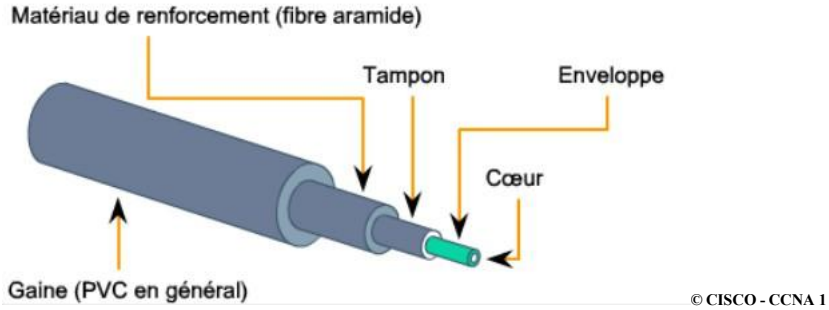
En plus de la gaine extérieure et les paires torsadées, ce type de câble possède une enveloppe de protection entre les paires et une autre autour des paires. Le câble STP offre une meilleure protection contre les interférences et une transmission plus rapide et sur une plus longue distance.

2.4.1.2 Fibre optique

La fibre optique est la technologie la plus récente en matière d'accès à Internet. Elle permet le transfert des données à grande vitesse via la lumière (les bits sont codés sur la fibre comme impulsions lumineuses). Ainsi, le support est à l'abri des interférences électromagnétiques. Le signal lumineux codé par une variation d'intensité est capable de transmettre une grande quantité d'informations.

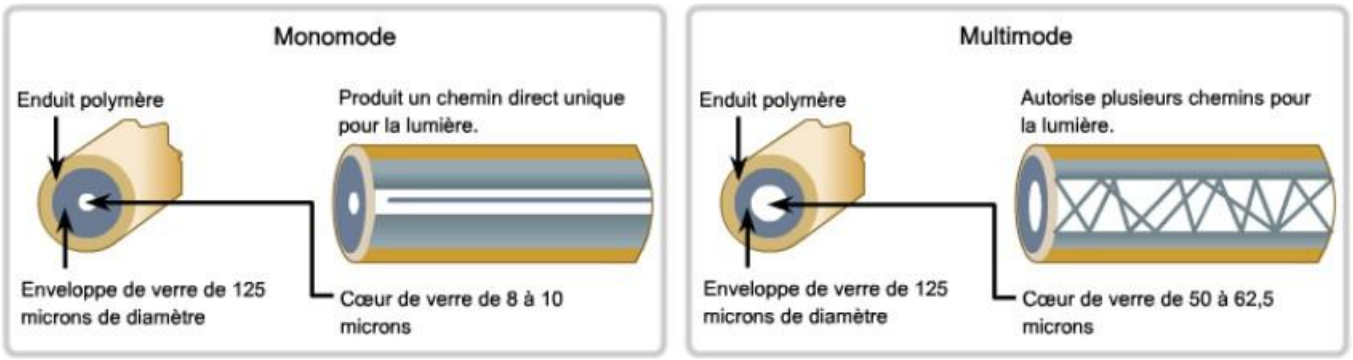
Les différentes couches de la fibre optique sont les suivantes :

1. ***Le cœur*** : des fils de verre pur ou en plastique de la taille d'un cheveu (250 micromètre). Elle est conçue grâce à un composé chimique appelé **silice.**
2. ***La gaine optique*** : elle fonctionne comme un miroir pour refléter les impulsions lumineuses qui se propagent dans le cœur pour les contenir dans le cœur de la fibre selon un phénomène appelé *réflexion totale interne*.
3. ***La protection :*** il s'agit généralement d'une gaine en PVC (un matériau plastique) qui protège le cœur et la gaine optique.



Il existe deux types de fibre optique :

1. **La fibre optique monomode :** (SMF, pour Single Mode Fiber), le cœur est très fin et n'admet qu'un mode de propagation (un seul rayon lumineu), direct dans l'axe de la fibre. La fibre monomode utilise des diodes au laser et a une grande puissance d'émission (' 100GHz/km). Les fibres monomodes sont de ce fait adaptées pour les lignes intercontinentales (câbles sous-marin).
2. **La fibre optique multimode :** (MMF, pour Multi Mode Fiber), permet de transporter plusieurs trajets lumineux. Des émetteurs à DEL produisent ces chemins lumineux. La lumière traverse la fibre selon différents angles. La traversée de la fibre prenne ainsi plus de temps. La longueur de la fibre peut générer des impulsions troubles à l'arrivée à l'extrémité réceptrice, appelé *distorsion modale.* Ainsi, la fibre optique multimode est utilisée uniquement pour des bas débits ou de courtes distances.



CISCO - CCNA 1

Le déploiement de la fibre nécessite :

— la création d'un nouveau réseau totalement indépendant ;
— un coût plus élevé par rapport au support en cuivre pour la même distance (mais pour une capacité supérieure) ;
— des compétences (il existe des formations certifiées) et matériel différents pour le raccordement ;
— une utilisation plus délicate que les supports en cuivre.

2.4.2 Supports non guidés

Les supports sans fil transportent des signaux électromagnétiques à des fréquences radio.

Quand les dispositifs de transmission appartiennent à une entreprise on parle de «**réseaux locaux**» ou de «**réseaux locaux étendus**», quand ils appartiennent à une entreprise de télécommunication ou à un service public, on parle d'« **informatique mobile** ».

Il existe plusieurs techniques de transmission, suivant la couverture géographique :

1. **Infrarouge**
   Utilise un faisceau de lumière infrarouge qui offre un débit égale à 10 Mb/s mais avec une faible portée (30 mètres). Il existe plusieurs types d'infrarouge : Infrarouge en visibilité directe, Infrarouge avec rebondissement, Réseau avec réflecteur, ...etc.
2. **Laser**
   Similaire à la technologie infrarouge dans le sens ou elle requiert un champ de visibilité directe.
3. **Radio :**
   Des ondes radio sont utilisées pour transporter les données. Suivant le nombre de fréquences, on trouve :
   — *à bande étroite :* (narrow band) consiste à utiliser une seule fréquence radio pour la transmission et elle doit être aussi petite que possible afin de limiter les interférences avec

les bandes adjacentes.

— *à spectre étalé :* les signaux sont transmis sur une plage de fréquences. Les cartes réseaux sont réglées pour une durée prédéterminée sur un des canaux, puis passent sur un autre canal. C'est ce qu'on appelle « des sauts de fréquence ».

Les interfaces de connexion normalisées

Pour chaque type de support filaire, il existe un modèle de **jonction** avec la carte réseau, appelée **Connecteur**. Ainsi nous trouvons :

— BNC pour le câble coaxial ;

— RJ45 pour la paire torsadée ;

— SC, ST, LC, MIC pour fibre optique.

Les connecteurs RJ11 – RJ45

Les câbles à paires torsadées blindées (STP) ou non blindées (UTP) se branchent à l'aide d'un connecteur RJ-45. Ce dernier comporte 8 broches ou 8 conducteurs.

L'ordre des codes de couleurs des fils dans une broche du connecteur sont décrits dans la norme TIA/EIA 568, il existe deux normes : T568A et T568B.

Suivant le type de connecteur utilisé, on trouve deux types de câble à paire torsadée :

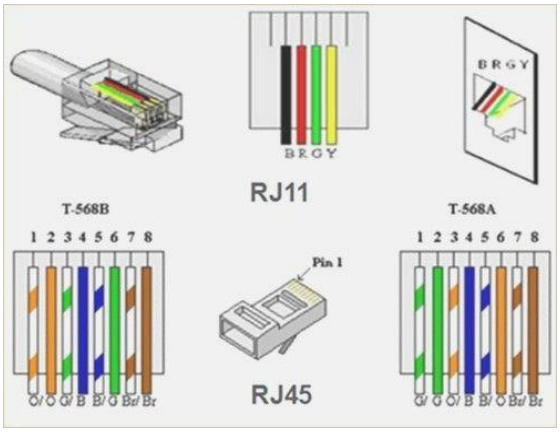
1. ***Câble Ethernet droit :*** (T568A dans les deux extrémités ou T568B dans les deux extrémités), il est utilisé pour connecter une machine hôte ou un routeur à un commutateur ou à un concentrateur.

2. ***Câble Ethernet croisé :*** (T568A dans une extrémité et T568B dans l'autre) câble peu utilisé permettant de relier des périphériques similaires. Par exemple, pour connecter un commutateur à un commutateur, une machine hôte à une autre machine hôte ou même une machine hôte à un routeur.

Remarque :

— De nos jours, la question du choix du type de câble à paire torsadée ne se pose plus, car les équipements réseau moderne sont capables de faire du MDI/MDI-X, c'est-à-dire du (dé) croisement automatique selon le type de câble utilisé.

— Il existe un troisième câble : **Câble console**. C'est câble propriétaire Cisco permettant d'établir une connexion avec un routeur ou un port de console de commutateur. L'objectif est de pouvoir configurer le routeur ou le switch en utilisant l'interface en ligne de commande de l'ordinateur.

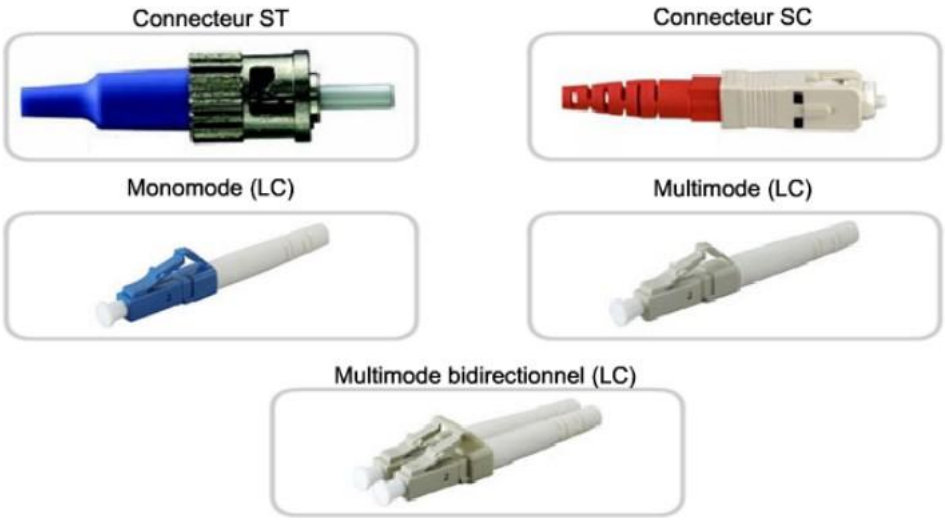


— Il existe un autre connecteur similaire au RJ-45 c'est le RJ-11. Il est utilisé dans la téléphonie. Il se compose de six broches mais il n'y a que 4 qui sont utilisés.

Les connecteurs SC, ST, LS, MIC

Les connecteurs fibre optique réseau ou connecteur optique les plus répandus sont les suivants :

1. **Connecteur ST** (Straight-Tip) : connecteur rond couramment utilisé avec la fibre monomode ;
2. **Connecteur SC** (Subscriber Connector) : appelé aussi connecteur carré ou connecteur standard. Il fait appel à un mécanisme de clipsage permettant de vérifier l'insertion. Il est utilisé avec la fibre optique multimode et monomode.
3. **Connecteur LC** (Lucent Connector) : parfois appelé petit connecteur ou connecteur local, il est de plus en plus répandu en raison de sa petite taille. Il est utilisé avec la fibre monomode et la fibre multimode.
4. **Connecteur MIC** (Media Interface Connector) : utilisé dans les réseaux métropolitains.



Dans la mesure ou la lumière circule que dans une seule direction, deux fibres sont nécessaires pour prendre en charge le fonctionnement bidirectionnel simultané. Elles sont raccordées par une paire de connecteurs monovoies ou un connecteur bidirectionnel.

2.5 La Numérisation

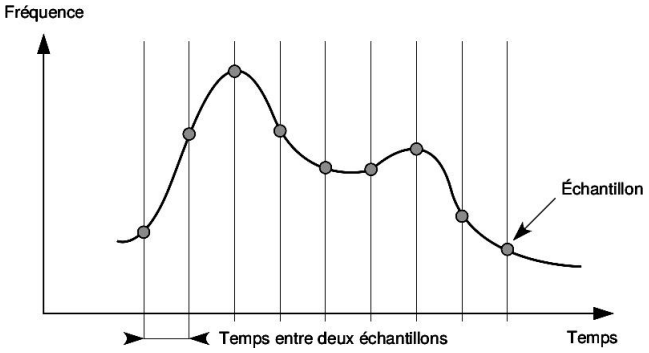
Elle consiste à transformer un signal analogique qui contient une quantité infinie d'amplitudes en un signal numérique contenant lui une quantité finie de valeurs.

La numérisation passe par deux étapes majeures : l'échantillonnage et la quantification

2.5.1 L'échantillonnage

Il consiste à choisir des points, ou ***échantillons***, du signal analogique. Il est important de fixer la vitesse à laquelle seront prélevés ces échantillons (la fréquence d'échantillonnage).

Plus la bande passante est grande, plus il faut prendre d'échantillons par seconde.



[2]

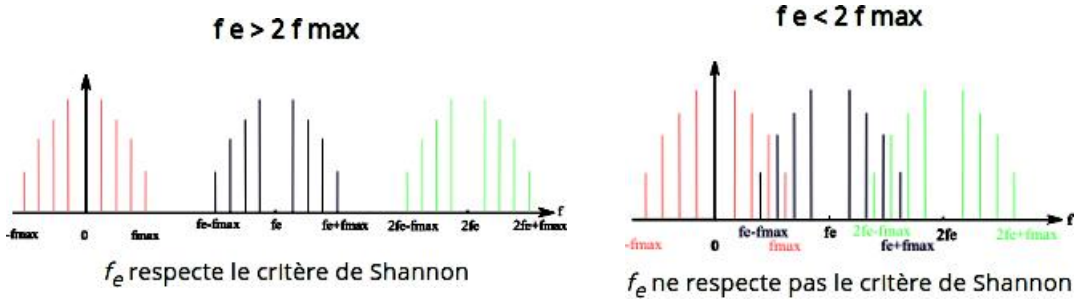
Le ***théorème de Shannon (Théorème d'échantillonnage)*** permet de connaître la fréquence d'échantillonnage à choisir pour un signal donné :

Pour un signal qui se propage dans un milieu de bande passante B, la fréquence d'échantillonnage doit être au moins le double de B :

$$f_e > 2 * B \tag{2.6.1}$$

Sinon des fréquences parasites apparaissent. Ce phénomène s'appelle le ***repliement spectral*** ou ***Aliasing***.

Exemple : Pour un signal avec une largeur de bande passante égale à 5 000 Hz, il faut échantillonner au moins 10 000 fois par seconde

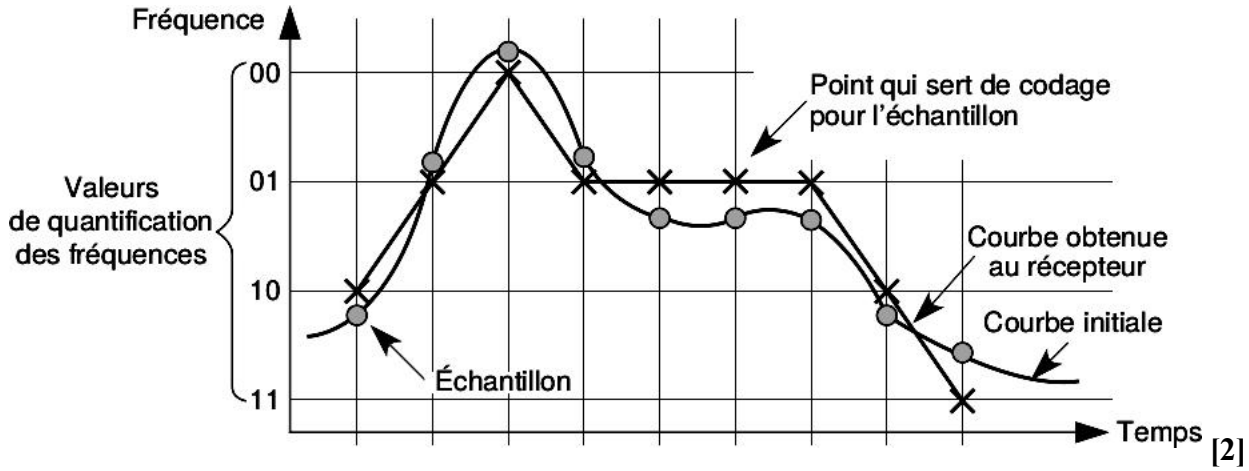


ttp ://culturesciencesphysique.ens-lyon.fr

2.5.2 la quantification

Elle consiste à représenter un échantillon par une valeur numérique au moyen d'une loi de correspondance (ex : la **loi A** en Europe et la **loi Mu** en Amérique du Nord).

La loi de correspondance doit être choisie de telle sorte que la valeur des signaux ait le plus de signification possible.



[2]

La précision, liée au nombre de bits dépend du convertisseur utilisé.

Le passage dans le numérique s'accompagne d'une perte d'information puisque du signal analogique n'est conservé que des échantillons. Ainsi, il est important de prendre un nombre d'échantillons optimal avec une cadence acceptable pour reconstruire au mieux le signal de départ tout en gardant un signal qui ne soit pas trop volumineux.

Chapitre 3 : Couche Liaison de Données

Introduction

La couche liaison de données permet la connexion entre les couches supérieures intelligentes et la couche physique. Elle est responsable du transfert des trames entre les périphériques adjacents.

Il existe des termes spécifiques à cette couche :

— **Nœud** : les périphériques réseaux connectés à un support commun.

— **Support** : le matériel qui transporte les signaux de données, tels que les câbles en cuivre, ...etc.

— **Segment de réseau ou Réseau physique** : qui diffère d'un réseau logique. Ce dernier est défini dans la couche réseau suivant le plan d'adressage. Les réseaux physiques représentent l'interconnexion des périphériques sur un support commun.

3.1 Services de la couche LDD

La couche liaison de données fournit un service de liaison entre deux hôtes. Les services fournis sont :

1) Tramage : Construction de la trame ;
2) Accès à la liaison : un protocole d'accès au média (support) la sous-couche MAC (Medium Access Control) décrit les règles selon lesquelles la trame doit être émise sur la liaison ;
3) Transfert fiable : ce protocole garantit un transfert sans erreur ;
4) Contrôle de flux : régler le débit pour que l'un des interlocuteurs ne soit déposé par le flux ;
5) Détection d'erreurs et éventuellement correction d'erreurs.

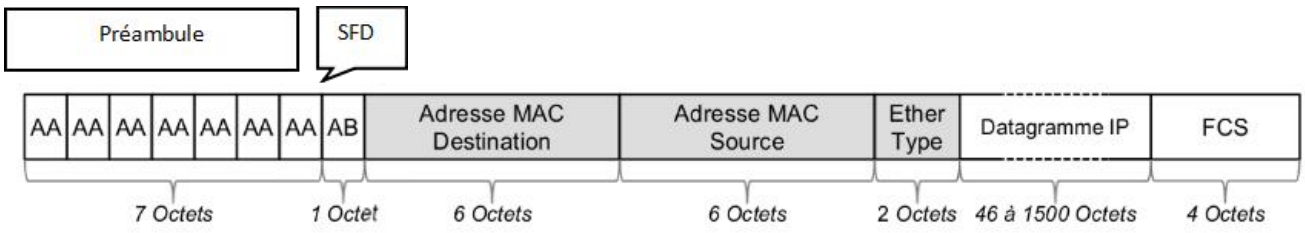
La couche liaison des données est constituée de deux sous-couches ;

- Sous-couche MAC (Medium Access Control)
- Sous-couche LLC (Logical Link Control)

3.2 Les trames

- Une trame est une suite de bits dont on connaît le début et la fin.
- Selon le protocole, elle peut être de taille fixe ou variable : Trame ATM -> 53 Octets

1) Trame Ethernet II



Préambule : (7 octets) Permet la synchronisation des horloges de transmission. Il s'agit d'une suite de 1 et de 0 soit 7 octets à la valeur AA = 10101010

SFD : (1 octets) "Starting Frame Delimiter". Il s'agit d'un octet à la valeur AB = 10101011. Il doit être reçu en entier pour valider le début de la trame.

Adresse MAC du destinataire et émetteur : (6 octets) contiennent les adresses physiques de la carte physique de chaque hôte.

EtherType (Type de protocole) : (2 octets)

EtherType	**Protocole**
0x0800	IPv4
0x0806	ARP
0x809B	AppleTalk
0x8035	RARP
0x86DD	IPv6

FCS : (4 octets) Frame Check Sequence. Ensemble d'octets permettant de vérifier que la réception s'est effectuée sans erreur.

2) Trame HDLC

Fanion	Adresses	Commande	Données	FCS	Fanion
8 bits	8 bits	8 bits	Taille variable	16 bits	8 bits

Fanion « ou flag » : indique les bordures de la trame (début et fin). Il est représenté par 01111110.
Que faire si la données contiennent la même séquence de bits (donnée = ...01111110...) ?
Solution : ajouter un 0 (appeler *bit de transparence*) après chaque 11111 (5 un consécutifs au niveau de l'émetteur).

Exemple
Message à envoyer : 011111011111011111111
Message envoyé : 011111 **0**011111 **0**1011111 **0**111
Le récepteur doit enlever un 0 après chaque suite : 11111

Adresse : identifie la station secondaire dans le cas d'une liaison multipoint. Dans une commande il représente la station destinataire. Dans une réponse il représente la station émettrice

Commande : indique le type de la trame. Il y a 3 formats de trame :

1. *Trames I (Information):* trames de données

1er bit	2ème	3ème	4ème	5ème	6ème	7ème	8ème
0	**N(S)**			**P/F**	**N(R)**		

N(S) : numéro de la trame envoyée.
N(R) : numéro trame I attendue.
P/F (Poll/Final) : P pour commandes, F pour réponses.

2. *Trames S (Supervision):* trames de supervision de l'échange

1er bit	2ème	3 ème	4 ème	5 ème	6 ème	7 ème	8 ème
1	**0**	*S*	*S*	**P/F**	**N(R)**		

4 types de trames de supervision :

- RR ("Received & Ready") - 00 : acquittement

Confirme la réception des trames de données de nº < N(R)

Demande la transmission des trames suivantes

- RNR ("Received & Not Ready") - 10 : contrôle de flux

Confirme la réception des trames de données de nº < N(R)

Interdit la transmission des trames suivantes

- REJ ("Reject") - 01 : protection contre les erreurs

Confirme la réception des trames de données de nº < N(R)

Demande la retransmission des trames de nº >= N(R)

- SREJ ("Selective Reject") - 11 : protection contre les erreurs

Confirme la réception des trames de données de nº < N(R)

Demande la retransmission de la trame de nº = N(R)

3. *Trames U (Unnumbered):* trames non numérotées. Initialisation et libération de la liaison de données

1er bit	2ème	3 ème	4 ème	5 ème	6 ème	7 ème	8 ème
1	**1**	*M*	*M*	**P/F**	*M*	*M*	*M*

Ces trames transportent des commandes ou des réponses de la gestion de la liaison (établissement, rupture, choix d'un mode de réponse…).

- Commandes

- SABM (Set Asynchronous Balanced Mode) [1 1 1 1 P 1 0 0] : demande de connexion
- SABME : Identique à SABM, mais mode étendu (numéroté en modulo 128).
- DISC (Disconnect) [1 1 0 0 P 0 1 0] : libération de connexion

- Réponses

- UA (Unnumbered Acknowledgement) [1 1 0 0 F 1 1 0] : acquittement de trame non-numérotée
- FRMR = FRaMe Reject [1 1 1 0 F 1 0 1] : rejet de trame
- DM = Disconnect Mode [1 1 1 1 F 0 0 0] : le terminal est déconnecté

FCS (Frame Check Sequence) permet la détection d'erreurs

3.3 Détection d'Erreurs

A l'heure actuelle, les données sont constamment en circulation, il est donc nécessaire d'assurer une transmission convenable et sans erreurs des informations. Ainsi, la complexité des réseaux modernes est due en grande partie à des techniques servant à détecter et à corriger les erreurs de transmission.

Technique des codes cycliques

Dans cette technique, l'information redondante est une clé qui s'appelle le CRC (Cyclic Redundancy Check). Elle est déterminée par une opération mathématique complexe appliquée au bloc de données à transmettre et est transmise avec celui-ci.

Données : Suite de bits quelconque	Clé ou CRC ou FCS
Bloc ou trame à transmettre	

Cette méthode considère le bloc à transmettre de N bits comme un polynôme de degré N-1, qu'on va appeler P(x).

Ce polynôme sera divisé par un autre polynôme, dit polynôme générateur G(x) selon les règles de l'arithmétique booléenne ou arithmétique modulo 2.

Le reste de cette division constitue le CRC parfois aussi appelé FCS (Frame Check Sequence). Ce CRC sera transmis à la suite du bloc de données.

En réception, le destinataire effectue la même opération sur le bloc reçu, le CRC obtenu sera comparé au CRC émis, si les valeurs différent une erreur sera signalée.

La réalité diffère un peu de ce qu'on dit en théorie, et les deux procédures de codage et de décodage sont les suivantes :

Procédure de codage :

1. A toute séquence de n bits, on associe un polynôme à n termes donc de degré n-1.

Exemple : 1001001 → $1.x^6+0.x^5+0.x^4+1.x^3+0.x^2+0.x^1+1.x^0$ → $x^6 + x^3 + 1$

2. La source et le destinataire choisissent un même polynôme générateur G(x) qui sera utilisé pour générer les bits de contrôle.
3. La séquence envoyée doit être un multiple de G(x)
4. On calcule le polynôme $P'(x) = P(x)* X^k$ ou k est le degré de G(x) → ceci équivaut à ajouter k zéros à la fin du message initial.
5. On divise P'(x) par G(x) → P'(x)=Q(x)*G(x) +R(x)
6. P'(x)-R(x)=P'(x)+R(x) = Q(x)*G(x)
7. P'(x) +R(x) = T(x) représente le nouveau message à envoyer. C'est un multiple de G(x) .

Remarque :

- La soustraction et l'addition sont la même opération en arithmétique booléenne (modulo2). Il n y a pas de retenue dans l'addition ni dans la soustraction. Faire une addition ou une soustraction équivaut à effectuer un ou exclusif entre les opérandes. Les divisions sont effectuées de la même manière qu'en binaire sauf que la soustraction est faite modulo 2.
- Cette dernière opération revient à ajouter les r bits de R(x) à la fin de P'(x).

Exemple :

On désire protéger le message 101101 par une clé calculée du polynôme générateur 1011.
Au message 101101, on fait correspondre le polynôme suivant :
$P(x)= x^5+x^3+x^2+1$
$G(x)= x^3+x+1$
$P'(x)= (x^5+x^3+x^2+1)*x^3 = (x^8+x^6+x^5+x^3) = 101101000$
On effectue la division des polynômes P'(x) et G(x)

$x^8+x^6+x^5+x^3$	x^3+x+1
$x^8+x^6+x^5$	
x^3	x^5+1
x^3+x+1	
$x+1$	

Q(x)=100001

R(x)=011

On peut effectuer la division binaire modulo 2

101101000	1011
1011	100001
01000	
1011	
0011	

R(x)=011

T(x) = P'(x)+R(x) → 101101000
+ 011

= 101101011

Le message à envoyer est T(x)= 101101011

Procédure de décodage :

1. Soit M(x) le message reçu.
2. On divise M(x) par G(x)
   - Si le reste de division est non nul alors détection d'une erreur
   - Si le reste de division est nul il y a une forte probabilité que la transmission soit correcte.

Exemple :

101101011	1011
1011	100001
000001011	
1011	
0000	

Le reste de division est égale à zéro, le message a été correctement transmis.

Exemples de polynômes générateurs :
Les principaux polynômes générateurs utilisés sont :

1) $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{10}+x^8+x^7+x^5+x^4+x^2+1$ → Comité IEEE 802 utilisé dans les réseaux locaux
2) $x^{16}+x^{12}+x^5+1$ → CCITT 41 utilisé dans HDLC

3.4 Les méthodes d'accès :

1) La contention

CSMA (carier sense multiple access) : Dans les réseaux avec un support partagé, il est nécessaire d'avoir un protocole apte à décider quelle station a le droit d'émettre, sinon une collision des différents signaux émis est inévitable. Une solution existe, elle s'appuie sur une technique d'écoute de la porteuse, c'est à dire que la station qui veut émettre écoute le canal avant, s'il elle ne détecte aucun signal sur la ligne elle envoie ses données sinon elle diffère son émission à une date ultérieure. Trois variantes existent :

1. **CSMA/CD** (carrier sense multiple access with collision detection) : Il s'agit de la même méthode d'écoute avec la détection des collisions, c'est à dire que la station émettrice continue à écouter le canal pendant la transmission, s'il se produit une collision, elle interrompt sa transmission et envoie aux autres stations des signaux spéciaux pour les prévenir de la collision. Elle tente par la suite de réémettre après un temps aléatoire.
   Les coupleurs émetteurs détectent une collision en comparant le signal émis avec celui qui passe sur la ligne, i.e. par détection d'interférences. Cette méthode nécessite des techniques de codage performantes pour permettre de reconnaître la superposition de signaux tel que le codage Manchester.

2. CSMA/CA (Carrier Sens multiple access with collision avoidance) : **Il s'agit de la même méthode d'écoute du canal qui consiste à éviter les collisions au lieu de les détecter.**

Quand la détection de la collision n'est pas possible, on utilise cet algorithme qui consiste à émettre si le canal est vide, et d'attendre si le canal est occupé un temps de durée différente pour permettre au récepteur d'envoyer un acquittement à l'émetteur, ceci permet d'éviter les collisions.

3. **CSMA/CR (Carrier Sens multiple access with contention resolution) : Techniques** d'accès des réseaux partagés reprenant la partie CSMA des réseaux ETHERNET mais évitant les collisions par une gestion des priorités.

2) La méthode du jeton :

Consiste à donner la possibilité aux machines de transmettre par tour de rôle. Un nœud n'a le droit d'émettre que s'il a en sa possession un jeton qui peut être une suite de bits ou un bit.
Le jeton fait le tour des nœuds pour revenir au même nœud. On dit que cette méthode est déterministe car le temps d'attente est limité.

-

Chapitre 4 : Couche Réseau

Introduction

Les services de la couche réseau permettent de transférer un paquet d'un réseau à un autre. Le rôle de la couche réseau se résume dans :

1. ***Encapsulation*** : la couche réseau ajoute des informations de contrôle au PDU provenant de la couche supérieure pour constituer ce qu'on appelle un paquet. L'encapsulation au niveau de l'émetteur est suivie d'une ***Dés-encapsulation*** au niveau du récepteur.
2. ***Adressage*** : en plus de l'adresse physique qui identifie le périphérique dans son sous-réseau, il est aussi identifié d'un réseau à un autre grâce à l'adresse IP. Cette dernière est une des informations ajoutées dans l'en-tête du paquet.
3. ***Routage*** : ce service permet de trouver une route d'un réseau à un autre pour le paquet pour qu'il soit acheminé à destination. Le routage est réalisé par le Routeur.
4. ***Fragmentation*** : chaque type de réseau possède un MTU (la taille maximale d'un paquet) propre à lui. Si la taille d'un paquet est plus grande que la valeur du MTU du réseau qu'il doit traverser, le routeur doit le fragmenter.

Il existe plusieurs protocoles de couche réseau :

- Le protocole IP version 4 (IPv4)
- Le protocole IP version 6 (IPv6)
- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

4.1 Adressage IPv4

Les classes d'adresses IP

L'adresse IP (Internet Protocol) se présente comme une suite de quatre nombres décimaux séparés par un point. Cette notation est dite décimale pointée. En binaire, les adresses IP sont codées sur 32 bits, groupés en 4 ensemble de 8 bits.

Exemple :

125.0.0.1

correspond à quatre octets binaires

01111101.00000000.00000000.00000001

Chaque adresse IP est composée de deux parties :

1. Une partie d'adresse réseau
2. Une partie d'adresse de la machine dans le réseau.

Cinq classes d'adresses ont été définies : Les classes A, B, C, D, E.

La classe A :

0------- . -------- .-------- .--------
@réseau (8bits) @ machine (24 bits)

Les adresses de cette classe commencent par 0 et s'étendent de 1.0.0.1 à 126.255.255.254. Elles permettent d'adresser 126 réseaux (2^7-2) et (2^4-2= 16 777 214) machines.

Remarque :

- Pour l'adresse réseau l'adresse 0 est interdite et l'adresse 127 est réservée.
- Pour l'adresse machine 0.0.0 est 255.255.255 ne sont pas utilisés

La classe B:

10------ . -------- . -------- .--------
@réseau (16 bits) @ machine (16 bits)

Les adresses de cette classe commencent par 10 et s'étendent de 128.0.0.1 à 191.255.255.254. Elles permettent d'adresser 2^{14} réseaux et (2^{16}-2= 65 534) machines.

La classe C :

110----- . -------- . -------- . --------
@réseau (21 bits) @ machine (8 bits)

Les adresses de cette classe commencent par 110 et s'étendent de 192.0.0.1 à 223.255.255.254. Elles permettent d'adresser 2^{21} réseaux et (2^8-2= 254) machines.

La classe D :

1110 Identificateur de groupe

Les adresses de cette classe commencent par 1110 et s'étendent de 224.0.0.0 à 239.255.255.255. Elles sont utilisées pour le diffusion (multicast) vers des machines d'un même groupe. Par exemple, un ensemble de routeurs pour la diffusion des tables de routage.

La classe E :

11110 Réservé pour un usage futur

Les adresses de cette classe commencent par 11110 et sont réservées aux expérimentations.

Les adresses spéciales

Certaines adresses particulières sont définies par convention :

- L'adresse 127.0.0.1 est dite adresse de rebouclage (loopback host), adresse de test de soi-même, elle est utilisée lors de test de la machine ou de programmes applicatifs.

- Aucune adresse entre 127.0.0.0 et 127.255.255 ne peut être utilisée.

- Les adresses ne peuvent pas théoriquement contenir uniquement des 0 ou uniquement des 1. Toutefois 0.0.0.0 est l'adresse d'une machine qui ne connaît pas son adresse avant de faire une demande d'attribution d'adresse IP.

- Tous les bits de la partie machine à 0 correspond à l'adresse réseau

- Tous les bits de la partie machine à 1 correspond à l'adresse de diffusion (broadcast) qui désigne tous les nœuds du réseau.

Le masque de réseau

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse. On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque réseau.

Classe	Masque réseau
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Sous-adressage (subnetting)

Lorsque trop de machines sont sur le même réseau, le trafic augmente, entraînant un nombre important de collisions ce qui a pour conséquence de diminuer l'efficacité du réseau. Une solution consiste à diviser ce réseau en sous-réseaux. Pour cela, le même préfixe de réseau doit être partagé entre plusieurs petits réseaux physiques distincts. On utilise quelques bits de la partie hôte pour représenter les sous-réseaux, ils sont en fait ralliés à la partie réseau de l'adresse.
De ce fait, Le masque de sous-réseau change.

Exemple :

Soit l'adresse suivante : 194.57.85.40

- C'est une adresse de classe C, son masque de réseau est 255.255.255.0
- L'adresse réseau est 194.57.85.0

On veut **diviser ce réseau en quatre sous-réseaux** différents :

On a besoin de deux bits supplémentaires pris de la partie hôte. Le nouveau masque de sous-réseau est:

11111111.11111111.11111111.11000000

ce qui est équivalent à

255.255.255.192

Chaque sous-réseau pourrait contenir 2^6-2=62 machines

Les adresses des sous réseaux sont :

- 11000010.00111001.01010101.00000000
- 11000010.00111001.01010101.01000000
- 11000010.00111001.01010101.10000000
- 11000010.00111001.01010101.11000000

La plage d'adresses du 2eme S/R

- FM : 11000010.00111001.01010101.01000001
- LM : 11000010.00111001.01010101.01111110

Les adresses de diffusion des 4 sous-réseaux sont :

- 11000010.00111001.01010101.00111111
- 11000010.00111001.01010101.01111111
- 11000010.00111001.01010101.10111111
- 11000010.00111001.01010101.11111111

4.2 Protocole IP : IPV4, IPV6

Le protocole IP est le service de couche réseau mis en œuvre par la suite de protocoles TCP/IP.

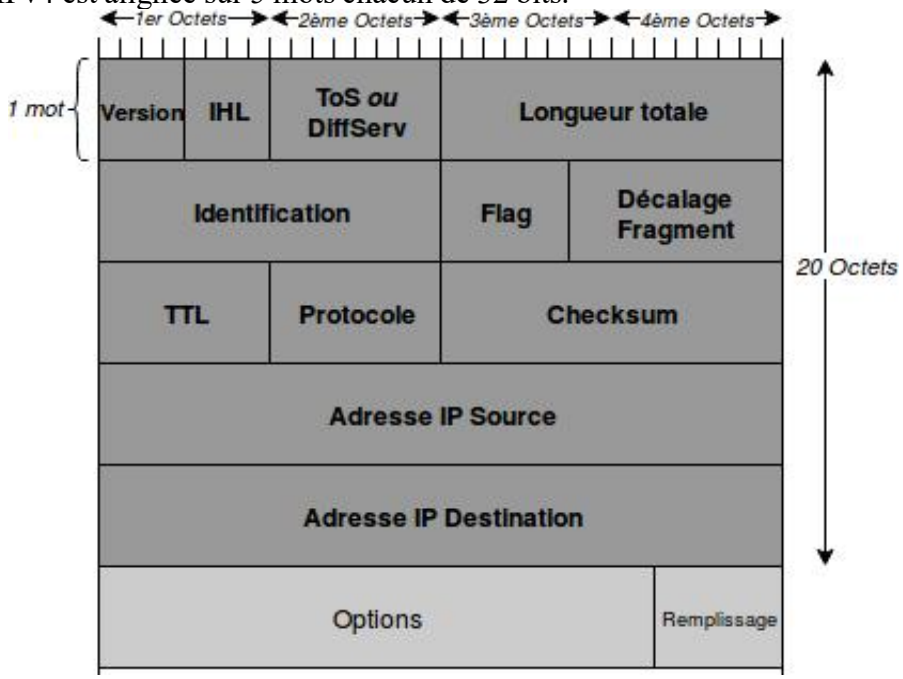
Les principales caractéristiques du protocole IP sont les suivantes :

- **Sans connexion** – aucune connexion avec la destination n'est établie avant d'envoyer des paquets de données.
- **Acheminement au mieux (peu fiable)** – la livraison des paquets n'est pas garantie.
- **Indépendant du support** – le fonctionnement est indépendant du support transportant les données.

4.2.1 En-tête IPv4

Ce qui nous intéresse dans le paquet IPv4 c'est d'étudier l'en-tête. Dans la mesure où la partie données du paquet (PDU de couche transport) n'est pas modifiée par le protocole de la couche réseau.

L'en-tête IPv4 est alignée sur 5 mots chacun de 32 bits.

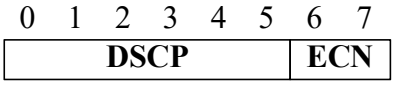


- **Version :** indique la version du protocole (toujours égal à 4 pour IPv4)

➢ **Longueur de l'en-tête IPv4** "**IHL"** (nécessaire en raison de la présence possible d'options) Elle indique le nombre de mots de 32 bits contenus dans l'en-tête. Cette valeur varie en fonction des champs d'options et de remplissage. La valeur minimale de ce champ est 5 (c.-à-d., 5 x 32 = 160 bits = 20 octets) et la valeur maximale 15 (c.-à-d., 15 x 32 = 480 bits = 60 octets).

➢ **Type de Service (ToS) :** permet de marquer un paquet comme étant plus important.

➢ **Type de Service** (ToS) : le champ TOS est actuellement remplacé par la norme **DiffServ** (*Dif- ferentiated Services*) pour une meilleure gestion de la qualité de service. Toujours une taille de 8 bits, il est composé de deux champs :



1. **DSCP** (*Differentiated Service Code Point*) : définit la priorité du paquet ;
2. **ECN** (*Explicit Congestion Notification*) : utilisés comme bits de notification de congestion pour éviter l'abondant des paquets au moment de l'encombrement du réseau.

➢ **Longueur totale du paquet IPv4**(**TPL) :** Parfois appelé longueur de paquet, y compris l'en-tête et les données, en octets. Sa valeur minimale est de 20 octets (un en-tête de 20 octets + 0 octet de données) et sa valeur maximale est de 65 535 octets. . Si un datagramme devant traverser un réseau est de taille supérieure à ce que le réseau peut transmettre (c.-à-d. au Maximum Transfer Unit ou MTU du réseau), il doit être fragmenté par le routeur ou la station l'injectant dans le réseau.

➢ **Identification** (**Fragment ID) :** Identifier un fragment de paquet pour de le reconstituer plus tard. Utilisé lorsqu'un paquet est fragmenté.

➢ **Drapeau (FLAG) :** Marqueurs permettant d'indiquer si un paquet peut/doit ou ne peut pas être fragmenté.

• **bit 0** : bit inutilisé et à 0.

• **bit Don't Fragment** : si positionné à 1, indique que ce datagramme ne doit pas être fragmenté. Dans ce cas, un routeur qui n'a d'autre choix que le fragmenter va le détruire et enverra un message *ICMP de compte rendu de destination inaccessible*.

• **bit More** : si positionné à 1, indique que le datagramme n'est qu'une partie (fragment) du datagramme d'origine et que ce n'est pas le dernier fragment. Si à 0, indique que le datagramme est le dernier fragment du datagramme d'origine. On reconnaît un datagramme non fragmenté lorsque le bit More est à 0 et que le Déplacement est aussi à 0.

- **Décalage Fragment (Fragment Offset) :** Indique la position du fragment au sein du paquet original. En multipliant sa valeur par 8, on obtient la position dans le datagramme d'origine du premier octet de données de ce datagramme.

- **Durée de Vie (TTL : Time To Live) :** représente le nombre d'intermédiaire (routeurs) par lesquels le paquet peut encore passer avant d'être détruit. Il s'agit d'un mécanisme permettant d'éviter qu'un paquet ne tourne indéfiniment dans un réseau suite à un problème de routage. On peut comparer cela à une date de péremption.

Valeur fixant la durée de vie en secondes du datagramme. Le but est d'éliminer un datagramme qui ne serait pas arrivé à destination dans le délai imparti, ou d'éliminer les fragments d'un datagramme lorsqu'il ne peut être reconstitué (fragment perdu ou trop retardé). En pratique, tout routeur devant transmettre le datagramme va décrémenter sa durée de vie d'au moins 1. Il en résulte que le TTL est une limite du nombre de routeurs pouvant être traversés jusqu'à la destination. Généralement appelée "Nombre de sauts"

- **Protocole :** Contient une valeur numérique qui identifie la nature du contenu du paquet.

  Quelques protocoles reconnus par IP (en décimal) :

  0 : IP

  1 : ICMP

  6 : TCP

  17 : UDP

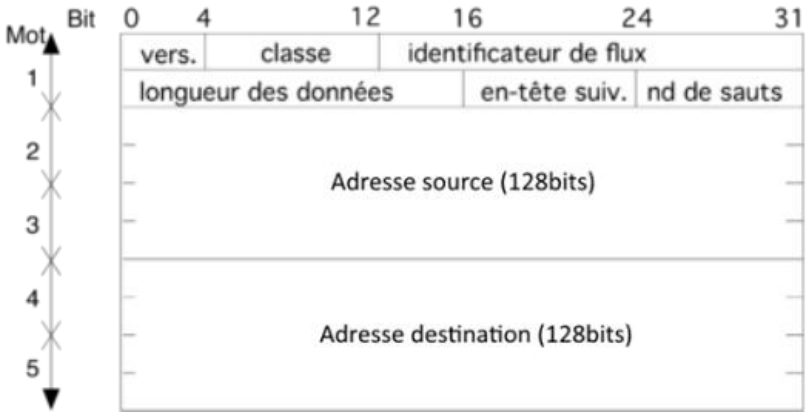
- **Somme de contrôle (Checksum):** calculée sur l'en-tête du paquet IPv4. Permet de contrôler l'intégrité de l'entête (mais pas des données) et donc de le détruire s'il avait été altéré.

- **Source IP :** Adresse IPv4 de la machine qui a émis le paquet.

- **Destination IP :** Adresse IPv4 de la machine à laquelle est destiné le paquet.

- **Options :** Permet d'ajouter différentes informations optionnelles. En cas de fragmentation, certaines options sont copiées dans tous les datagrammes (comme le routage à la source),

4.2.2 En-tête IPv6



- **Version** – (4 bits) : Numéro de version du protocole Internet = 6.
- **Classe** – (8 bits) : Champ de classe de trafic.
- **Indicateur de flux** – (20 bits).
- **Longueur des données**– (16 bits) : représente le reste du paquet qui suit l'en-tête IPv6 (en octets).
- **En-tête suivante**– (8 bits): Identifie le type d'en-tête qui suit immédiatement l'en-tête IPv6.
- **Nombre de sauts** - (8 bits): Décrémentation de 1 par nœud transférant le paquet. Si la valeur du champ est définie sur zéro, le paquet est abandonné.

4.3 Fragmentation

Chaque paquet est transmis à la couche inférieure pour être encapsulé dans une trame. Bien que la longueur maximale d'un datagramme Ipv4 soit 65535 octet, il ne doive pas dépasser la taille max du champ Data de la trame.

Cette limite est appelée **MTU** (unité de transmission maximale). La couche réseau est informée de la valeur de la MTU grâce à la couche inférieure.

Il existe différentes technologies réseau, chacune possède sa propre MTU :

Type de réseau	MTU (en octets)
Arpanet	1000
PPPoE	1492
Ethernet [2]	1500
Wi-Fi	2300
Token Ring	4464
FDDI	4470
ATM Cisco	4470
ATM	9180

Si la taille du paquet IP est plus grande que la valeur du MTU du réseau qu'il doit traverser, la machine émettrice ou le routeur [3] doit le fragmenter en un certain nombre de fragments transportés par autant de trames sur le support physique. C'est **la fragmentation du paquet** ou **fragmentation IP**. Le destinataire final reconstitue le paquet initial grâce au service de la couche réseau.

Au niveau du routage, il est possible que chaque fragment emprunté un chemin différent. Si un seul des fragments est perdu, le paquet est considéré comme perdu

4.4 Routage

Un paquet peut passer par de nombreux périphériques intermédiaires avant d'atteindre l'hôte de destination. Chaque route que le paquet emprunte pour atteindre l'hôte de destination est appelée un saut.

Le routage est une tâche de la couche réseau (couche 3 du modèle OSI) qui permet de décider sur quelle

interface du routeur un paquet doit être émis.

La couche réseau fonctionnant en mode non connecté, cette tâche doit être répétée pour chaque paquet entrant, d'où la nécessité d'une prise de décision rapide.

Une table maintenue par chaque routeur d'un réseau, la ***table de routage***, permet d'établir une correspondance entre le réseau de destination (auquel appartient le destinataire du paquet), et l'adresse du prochain routeur (prochain saut) permettant d'atteindre la destination finale. Il existe 3 types de de routes :

- Route par défaut : définit par l'adresse 0.0.0.0, elle permet d'acheminer un paquet dont la destination ne correspond à aucune autre route de la table de routage

- Routes vers les réseaux directement connectés,

- Routes vers les réseaux distants : Les réseaux distants sont ajoutés à la table de routage grâce à la configuration de routes statiques ou à l'activation d'un protocole de routage dynamique.

Remarque :

Si l'adresse IP de destination du paquet n'appartient ni à un réseau connecté ni à un réseau distant, et que le routeur ne possède pas de route par défaut, le paquet est abandonné. Le routeur envoie un message ICMP de destination inaccessible à l'adresse IP source du paquet.

1) Réseau directement connecté

Avant la configuration de routage statique ou dynamique sur un routeur, celui-ci ne connaît que les réseaux qui lui sont directement connectés. Ceux-ci sont donc les seuls réseaux affichés dans la table de routage tant que le routage statique ou dynamique n'est pas configuré. Les réseaux directement connectés sont d'une importance capitale pour les décisions de routage. Les routes statiques et dynamiques ne peuvent pas exister dans la table de routage si le routeur n'a pas de réseaux directement connectés.

2) Routage Statique

- Ne dépends pas de l'état du réseau
- Le choix de la route est défini une fois pour toute et ne change pas
- Les tables sont configurées manuellement
- Simple mais il n'est pas adapté à la défaillance d'un lien
- Adapté aux petits réseaux
- Assure le séquencement des paquets
- l'administrateur doit faire les mises à jour en cas de changement de la topologie du réseau
- réduction de la charge du système, car aucune mise à jour de routage n'est envoyée

3) Routage Dynamique

- Le chemain emprunté est en fonction de l'état de routage.
- Les tables de routage sont régulièrement mise à jour
- Plus complexe
- Surcharge de réseau à cause de l'échange d'information

- Permet de choisir la route optimale

Il existe deux grandes familles d'algorithme de routage dynamiques :

- Le routage à vecteur de distance (Distance Vector)
- Le routage à états de lien (Link State)

3.1) Routage à vecteur de distance

- Les routes sont exprimées sous forme de vecteur
- Chaque routeur envoie une mise à jour de sa table dans son intégralité régulièrement
- Utilise l'algorithme de BELLMAN-FORD pour calculer le chemin optimal vers une route

On trouve plusieurs types de protocoles :

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)

3.2) Routage à états de lien

- Chaque routeur reçoit plus d'information (par rapport aux algorithmes à vecteur de distance) → Il possède une vue générale du réseau
- Les mises à jour ne sont envoyées que lorsqu'une route est modifiée
- Utilise l'algorithme de DIJKSTRA pour calculer le chemin optimal vers une route

On trouve plusieurs types de protocoles :

- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System-to-Intermediate System)
- BGP (Border Gateway Protocol)

	Protocoles à vecteur de destance		**Protocoles à état de lien**	
Par classe	RIPv1	IGRP		
Sans classe	RIPv2	EIGRP	OSPFv2	IS-IS
IPv6	RIPng	EIGRP pour IPv6	OSPFv3	IS-ISpour IPv6

4) Les différentes métriques :

Il existe plusieurs métriques utilisée par les protocoles de routage comme : *nombre de sauts , bande passante, délai, fiabilité , MTU.*

4.5 Le protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet transmettre des informations relatives à des routeurs ou des machines hôtes. Il ne corrige pas les erreurs mais fait part de ces erreurs aux protocoles des couches voisines.

En-tête ICMP

Type *(8 bits)*	Code *(8 bits)*	Checksum *(16 bits)*	Option *(taille variable)*

Type	Code	Message	Signification du message
8	0	Demande d'ECHO	Ce message est utilisé lorsqu'on utilise la commande PING. Cette commande, permettant de tester le réseau, envoie un datagramme à un destinataire et lui demande de le restituer
0	0	Réponse d'ECHO (echo-reply)	Réponse au message de type 8
3	0	Destinataire inaccessible	Le réseau n'est pas accessible
3	1	Destinataire inaccessible	La machine n'est pas accessible
3	4	Destinataire inaccessible	Fragmentation nécessaire mais impossible à cause du drapeau (flag) DF
11	0	Temps dépassé	Ce message est envoyé lorsque le temps de vie d'un datagramme est dépassé.

4.6 Le protocole ARP (Protocole de Résolution d'Adresse)

Quand un équipement a besoin de connaître l'adresse Ethernet d'un autre équipement, elle envoie une requête ARP qui est encapsulée dans une trame Ethernet de diffusion, en précisant l'adresse IP de la machine destinataire. Toute les machines sur le réseau prélèvent la trame, reconnaissent un paquet ARP et seule la machine ayant l'adresse IP demandée répondra à la requête.

Les adresses Ethernet et IP de la source étant incluse dans la requête, toutes les stations enrregistrent cette correspondance dans leurs chache ARP ou table ARP.

Si la réponse ne parvient pas dans un délai imparti alors **Time-Out** et réexpédition de la requête.

4.7 Le protocole RARP

L'adresse Ethernet est une adresse physique est une adresse inscrite matériellement sur la carte réseau. Par contre, l'adresse IP est une adresse se trouvant sur disque.

RARP (*Reverse Address Resolution Protocol*) est un protocole permettant à un équipement sans disque (Terminal X, station sans disque) d'obtenir son adresse IP en communiquant son adresse Ethernet à un serveur RARP.

Ne pas confondre avec DHCP !!!

Chapitre 5 : Couche Transport

Introduction

La couche transport est responsable du transfert des données entre l'application de l'émetteur et celle du récepteur.

5.1 Services de la couche transport

Cette couche a pour rôle de :

1. **Identifier chaque application** : un hôte peut exécuter plusieurs applications et/ou services [1]. La couche transport donne un identificateur à chaque application et service qui sera ajouté à chaque donné au moment de l'encapsulation. Cet identificateur est appelé **numéro de port**.
2. **Découper les données** : le matériel réseau ne gère que des paquets d'une certaine taille. Cependant, la donnée provenant de la couche application (modèle TCP/IP) peut dépasser cette taille. Pour cela, la couche transport le découpe en plusieurs blocs avant de les envoyer à la couche Ré- seau ou Internet du modèle TCP/IP. De plus, si un bloc est perdu, ce n'est pas la donnée dans sa totalité qui sera perdue. Par la suite chaque bloc est encapsulé avec un deuxième identifiant utile à la réorganisation et réassemblage des blocs au niveau du récepteur.

Multiplexage de conversations

C'est le fait que plusieurs communications différentes, provenant de nombreuses applications, soient imbriquées sur le même réseau. Ceci est grâce à la segmentation des données et l'identification de chaque bloc. Sans la segmentation, une seule application pourrait recevoir des données à la fois.

Mode d'acheminement

La suite de protocoles TCP/IP propose deux protocoles de couche transport : **TCP** (Transmission Control Protocol) et **UDP** (User Datagram Protocol).

Le choix entre ces deux protocoles est suivant l'importance accordée à la fiabilité ou à la charge imposée au réseau.

1. Application : programme qui permet à l'utilisateur de communiquer sur le réseau (ex : navigateur web). Service : programme qui s'exécute en arrière-plan. Il aide une application (ex : transfert de fichiers)

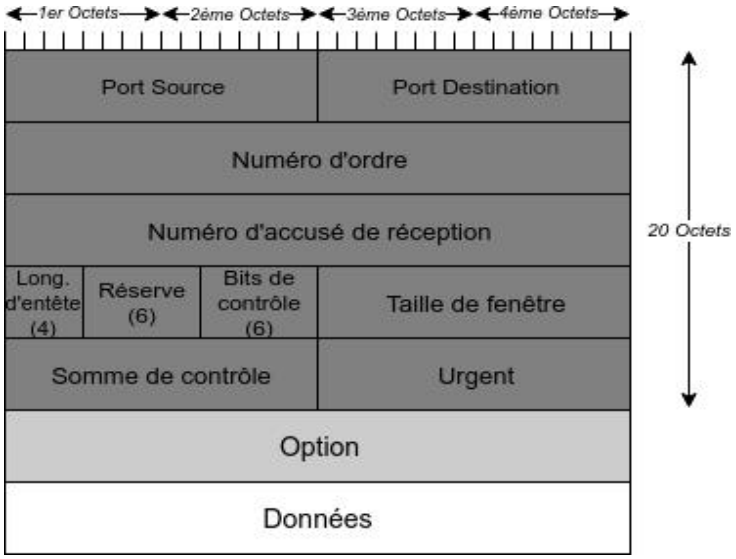
5.2 TCP (Transmission Control Protocol)

Le protocole TCP est un protocole de transport fiable.
Il permet :

- Orienté connexion : création d'une session entre la source et la destination
- Acheminement fiable : retransmission des données perdues ou endommagées
- Reconstitution ordonnée des données : numérotation et séquencement des segments
- Contrôle de flux : régulation de la quantité de données transmises
- Protocole avec état : garde une trace de la session

5.2.1 En-tête TCP

La taille de l'en-tête TCP est de 20 octets, elle comprend :



— **Numéro de port** : c'est un identifiant unique utiliser pour différencier les segments de chaque application. Le numéro de port source est associé à l'application de l'émetteur et le numéro de port de destination à celle du destinataire.

— **Un numéro d'ordre (SEQ)** : pour identifier la position de chaque segment dans le message d'origine. Lors de l'établissement de la session, ce champ contient un numéro d'ordre initial (ISN) non null est difficilement prévisible. Lors de la transmission des données pendant la session, le numéro est incrémenté du nombre d'octets ayant été transmis. Il est ainsi possible d'identifier les segments manquants.

— **Un numéro d'accusé de réception (ACK)** : indique les données qui ont été reçues.

— **Longueur d'en-tête** ou **OFFSET** : le nombre de mots de 4 octets qui composent l'entête.

— **Réservé** : réservé pour un futur usage.

— **Bits de contrôle** ou **code** ou **flags** : comprennent un code sur 6 bits indiquant la fonction du segment (la nature du segment) :

  — bit 0 → URG (urgent pointer) : si ce drapeau est à 1, le segment transporte des données urgentes dont la place est indiquée par le champ Pointeur d'urgence (voir ci-après).

- bit 1 → ACK (Acknowledgement) : le segment transporte un accusé de réception.
- bit 2 → PSH (Push) : le segment devra être délivré immédiatement. Le récepteur ne doit pas attendre que son tampon de réception soit plein pour délivrer les données à l'application.
- bit 3 → RST (Reset) : réinitialisation de la connexion.
- bit 4 → SYN (Synchronize) : indiquer qu'il s'agit de l'ouverture de connexion. Le champ « sequence number » contient la valeur de début de la connexion.
- bit 5 → FIN (Final) : terminer l'émission des segments.

— **La taille de fenêtre** : c'est la taille du buffer de réception. Elle indique le nombre de segments qui peuvent être acceptés en réception avant l'envoi d'un ACK. La fiabilité impose la surcharge des ressources du réseau en raison des accusés de réception, de suivi et de retransmission. Pour cela, un ACK n'est pas envoyé pour chaque segment envoyé mais pour un ensemble de segment.

— **La somme de contrôle** : utilisée pour le contrôle des erreurs sur l'en-tête et les données de segment.

— **Urgent** : ce champ est valide lorsque le bit URG est activé. Indique le rang à partir duquel le segment est une donnée urgente.

— **Options** : (taille variable), sa présence est détectée lorsque l'offset est supérieur à 5. On trouve dans ce champ :

- *MSS* : au moment de l'établissement d'une connexion, chaque partie annonce sa taille de MSS (ex : Ethernet MSS = 1 460 octets, tel que $MSS = MTU - entêtes\ IP - entête\ couche\ transport$). Sa valeur n'est pas négociable.
- *Timestamp* (estampille temporelle) : permet de calculer la durée qu'un segment prend aller et retour (RTT, Round Trip Time).
- *Wscale* (Window Scale ou facteur d'échelle) : pour augmenter la taille de la fenêtre au-delà des 16 bit du champ Fenêtre normal. Si la valeur proposée est n, alors la taille maximale de la fenêtre est de $65535 * 2^n$.

—

5.2.2 Communication TCP

Le TCP est un **protocole avec état.** Il garde une trace de la session où le récepteur suit les informations envoyées et sait quelles informations ont été reçues.

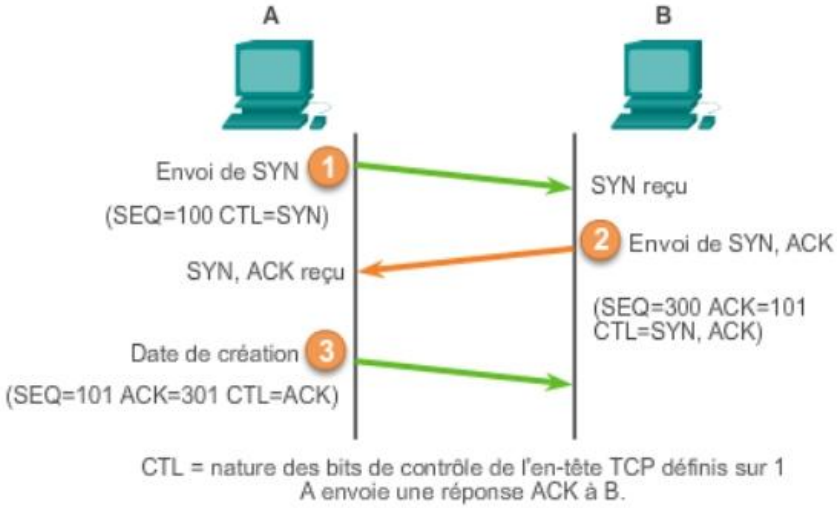
La session avec état est orientée connexion. Elle commence par l'établissement d'une session, suivis de l'envoi des segments et la réception des ACK et se termine par la fermeture de la session.

5.2.2.1 Établissement d'une session

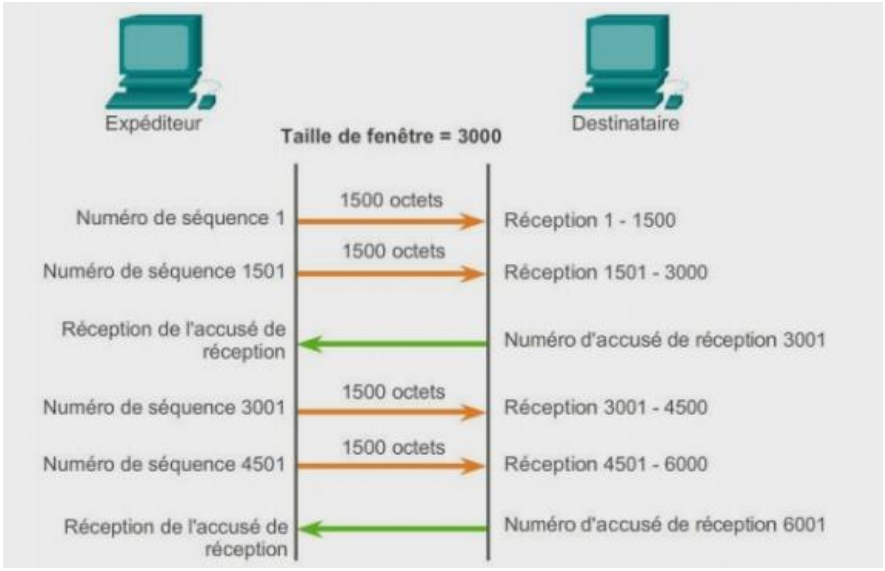
Connexion - envoie de segments - Déconnexion

Connexion en trois étapes

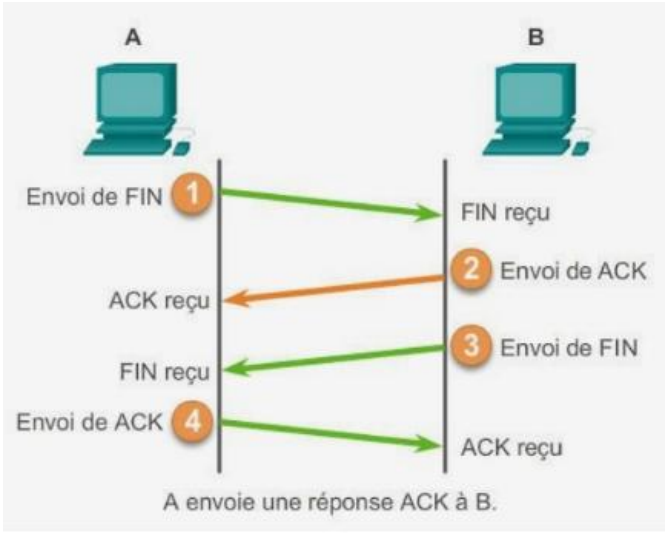
Étape 1 : Le client demande l'établissement d'une session de communication client-serveur avec le serveur.
Étape 2 : Le serveur accuse réception de la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client
Étape 3 : Le client accuse réception de la session de communication serveur-client.



Envoie de segments



Déconnexion



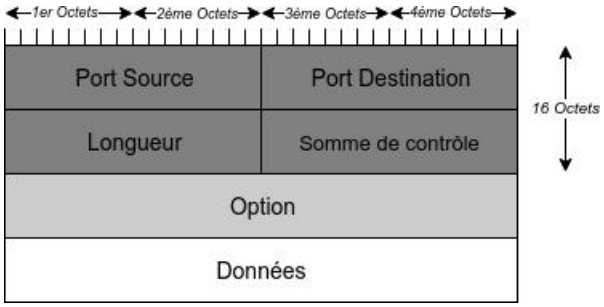
5.3 UDP (User Datagram Protocol)

Le protocole UDP [4] fournit uniquement les fonctions d'acheminement de base entre les applications appropriées :

- Sans négociation préalable
- Sans garantie de remise
- Sans reconstitution ordonnée des données
- Sans contrôle de flux
- Protocole sans état

5.3.1 En-tête UDP

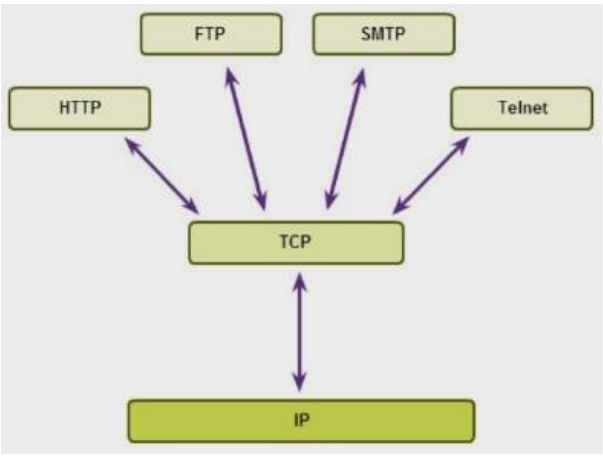
En supprimant le service avec connexion, la fiabilité et contrôle du flux, l'entête UDP est de taille de 8 octets :

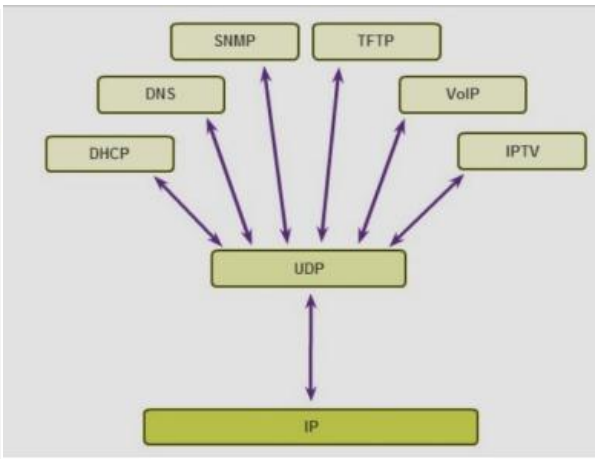


Longueur : la longueur totale du datagramme UDP, exprimée en octets, en-tête comprise. La longueur maximale est de 65 515 octets.

TCP OU UDP

- Compromis entre l'importance accordée à la fiabilité et la charge imposée au réseau
- Les développeurs d'applications choisissent le protocole de transport en fonction des besoins





5.4 Numéros de port

L'*Internet Assigned Numbers Authority* (IANA) attribue les numéros de port. Il existe 3 catégories de numéros de port :

1. **Ports réservés** $[0 - 1023]$: sont des ports connus ou réservés (*well known ports*). Ils sont affectés aux processus système ou aux programmes exécutés par les serveurs ;
2. **Ports inscrits** ou **enregistrés** $[1024 - 49151]$: ils sont attribués par l'IANA pour le service spécifique à la suite d'une demande d'un d'utilisateur ou d'une entreprise de développement d'applications ;
3. **Ports privés** ou **dynamiques** $[49152 - 65535]$: ne sont pas enregistrés auprès de l'IANA. Ils sont utilisés pour des applications privées ou pour des besoins temporaires. Ils sont affectés de façon dynamique à des applications clientes lorsqu'une connexion à un service est initiée par un client. Certains services de partage de fichiers peer-to-peer utilisent ces ports.

À savoir que les numéros de port des applications clients sont attribués, de façon plus ou moins aléatoire, par le système d'exploitation de la machine hôte.

Chapitre 6 : Couche Application

Introduction

Les applications réseaux représentent l'interface entre l'utilisateur et le réseau. Ainsi, la couche supérieure comprend des protocoles permettant de les gérer.

Sachant que la couche application TCP/IP regroupe les fonctionnalités des trois couches supérieures du modèle OSI, ce chapitre décrit les protocoles majeurs de la couche application TCP/IP à savoir :

6.1 SMTP, POP, IMAP

L'e-mail est une méthode de stockage et de transfert des messages électroniques à travers un réseau. Les messages sont stockés dans des **serveurs de messagerie** qui prennent en charge de nombreux comptes client différents.

Un client de messagerie ne communique pas directement avec un autre client lors de l'envoi des e-mails. Les deux clients dépendent du serveur de messagerie pour transporter les messages même s'ils appartiennent au même domaine.

Pour que la messagerie fonctionne, trois protocoles sont nécessaires :

— **SMTP** (Simple Mail Transfer Protocol) : utilisé pour envoyer un message d'un client à un serveur ou d'un serveur à un autre.

— **POP** (Post Office Protocol) : utilisé pour que le client puisse récupérer l'e-mail.

— **IMAP** (Internet Message Access Protocol) : utilisé aussi pour que le client puisse récupérer l'e-mail.

Les différents éléments du dialogue sont :

- MUA (Mail User Agent) : Programme qui permet d'envoyer ou de recevoir du courrier (Incredimail, Outlook…).

- Le MTA (Mail Transport Agent) : Programme qui permet d'acheminer le courrier d'un serveur à l'autre.

- Le MDA (Mail Delevery Agent) : Logiciel qui stocke le courrier en attendant que le MUA vienne le relever.

Principe de fonctionnement :

1-Le client de messagerie A (MUA) envoie le courrier (grâce au protocole SMTP) au MTA de son serveur de courrier sortant.

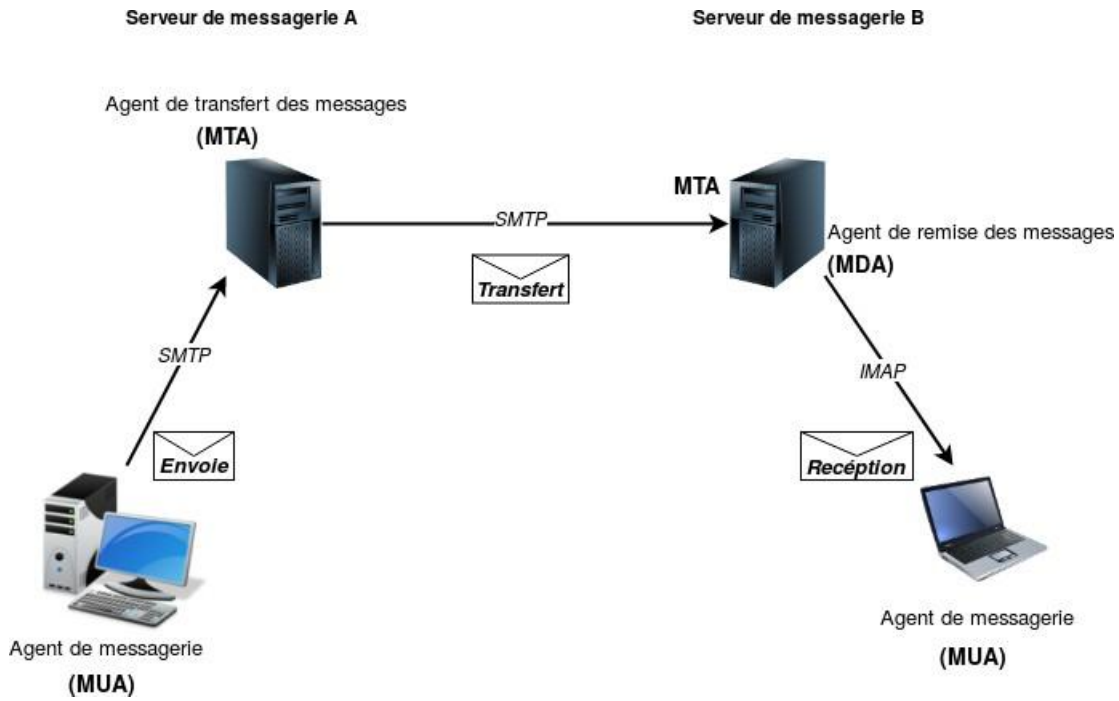
2- Le serveur de courrier entrant consulte un serveur DNS pour savoir à quel serveur SMTP envoyer le courrier (en utilisant le nom de domaine de l'adresse mail du courrier). Le DNS renvoie un enregistrement de type MX du nom de domaine demandé (cf. chapitre précédent sur les DNS).

3- Le MTA du serveur de courrier entrant, transfert le courrier au MTA du serveur SMTP de destination (grâce au protocole SMTP).

4- Le MTA transfert le courrier au MDA du serveur de courrier entrant du destinataire (grâce protocole LMTP)

5- Le serveur de courrier entrant stocke le courrier.

- Le client de messagerie B (MUA) relève le courrier sur son serveur de courrier entrant (grâce au protocole POP ou IMAP).



6.2 HTTP

C'est le protocole le plus utilisé sur internet. Il permet à un navigateur d'obtenir des pages Web. Le navigateur Web est une **application cliente** qui accède aux ressources stockées sur un **serveur Web.** Lorsqu'une adresse Web ou URL est saisie dans un navigateur Web, le client HTTP établit une connexion avec le serveur HTTP pour demander les ressources voulues. Le serveur Web s'exécute en tant que service en tâche de fond et retourne les ressources. Le navigateur les reçois et interprète les données pour les présenter à l'utilisateur.

Les données reçues peuvent être de différents types : données en texte clair ou HTML (*HyperText*

Markup Language), plug-in (données nécessitant un autre service ou programme), ...etc. Pour aider le navigateur à déterminer le type de fichier qu'il reçoit, le serveur indique le type de donnée que contient le fichier.

6.2.1 Requête HTTP

Une requête HTTP comprend 3 parties :

1. Une ligne de commande (obligatoire) qui contient trois informations (écrites à la suite l'une de l'autre) :

   (a) **La méthode** : qui peut être soit de type :

   — ***GET*** : c'est une requête cliente pour demander des pages HTML. La réponse du serveur peut être le fichier HTML demandé, un message d'erreur ou autres informations telles que « l'emplacement du fichier demandé a changé ».

   — ***HEAD*** : demander que des informations sur la ressource, sans demander la ressource elle-même.

   — ***POST*** : envoyer des données saisies dans un formulaire intégré à une page Web au serveur Web.

   — ***PUT*** : télécharge des données (un fichier ou une image) vers le serveur Web (upload).

   (b) **L'URL** : pour identifier la ressource.

   (c) **La version du protocole HTTP** utilisé : HTTP/1.0 ou HTTP/1.1. Depuis 2014, c'est le HTTP/2

2. Une liste d'entêtes avec leurs valeurs (facultative) : donner des informations sur le client. Chaque ligne de la liste est constituée du nom de l'entête séparé de sa valeur par 2 points.

3. Le corps de la requête (facultatif) : Il doit être séparé du reste de la requête par une ligne vide. Il contient les données à fournir au programme du serveur.

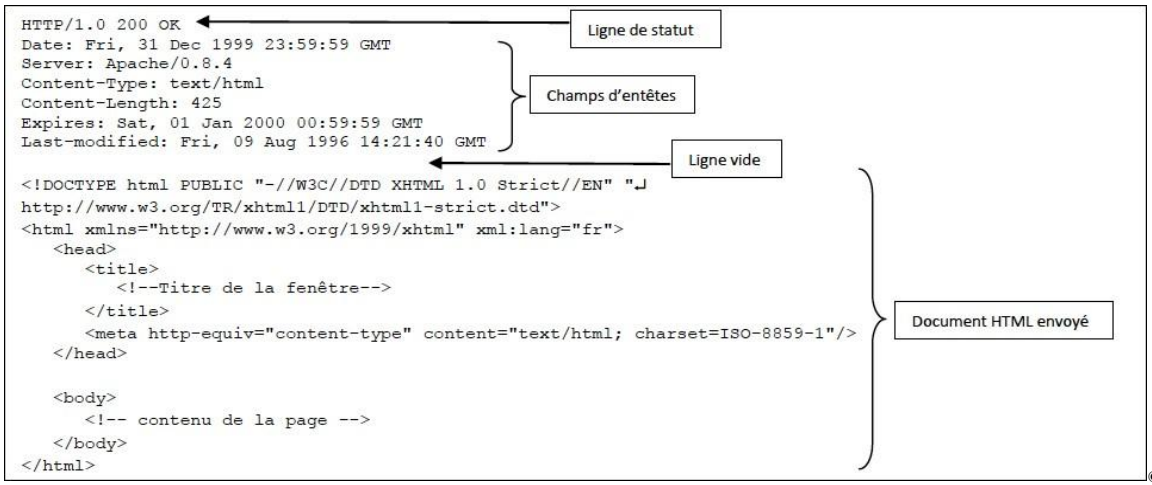
6.2.2 Réponse HTTP

Une réponse HTTP comprend 3 parties :

1. **Une ligne de statut** (obligatoire) : contient des informations comme la version du protocole HTTP utilisé ;

2. **Une liste d'entêtes avec leurs valeurs** (facultative) : permet de donner des informations supplémentaires sur la réponse ;

3. **Le corps de la requête** (facultatif) : il doit être séparé du reste de la requête par une ligne vide. Il contient le document demandé par le client.



©www.supinfo.com

6.3 FTP

FTP est un protocole client/serveur qui permet de transférer des fichiers entre 2 machines distantes. Un client FTP peut être une application ou un service, et le serveur peut exécuter un démon FTP appelé **FTPd**.

Le protocole impose deux connexions (ou canaux) établies entre le client et le serveur : une connexion pour les commandes (ou contrôle) et les réponses et une autre pour le transfert des fichiers.

1. **Le canal de contrôle :** L'élément de commande au niveau de chaque entité est appelé **PI** (Protocol Interpreter ou Interpréteur de protocole). Il y a un PI côté client (USER-PI) et un PI côté serveur (SERVER-PI).

   Le USER-PI est chargé d'initier la connexion avec le serveur FTP sur le port TCP 21, d'envoyer les commandes FTP et de recevoir les réponses du SERVER-PI.

   Le SERVER-PI est chargé d'écouter les commandes provenant d'un USER-PI sur le canal de contrôle, d'établir la connexion pour le canal de contrôle, de recevoir sur celui-ci les commandes FTP de l'USER-PI et d'y répondre.

2. **Un canal des données**. le client initie aussi la seconde connexion au serveur via le port TCP

   20. Cette connexion est réservée uniquement pour le transfert des fichiers et est crée à chaque transfert de fichiers. Ce dernier peut s'effectuer dans les deux directions. Le client peut télécharger (extraire) des données à partir du serveur ou télécharger (stocker) des données vers le serveur.

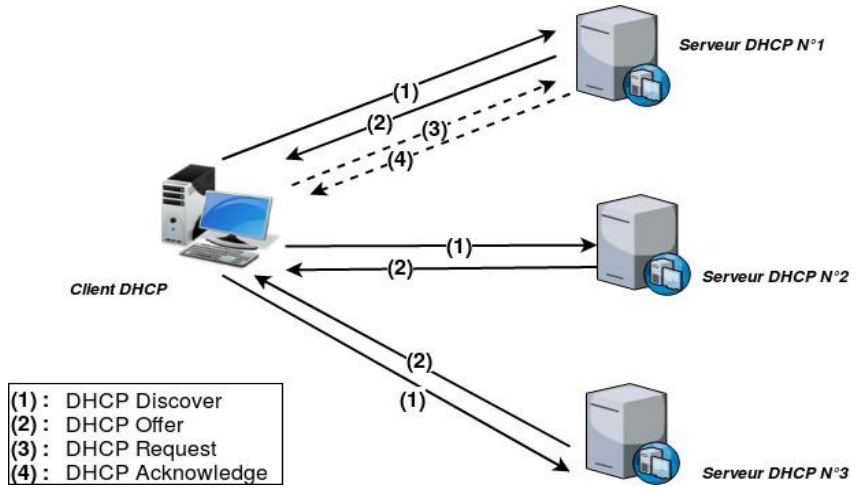
   L'élément du dialogue est **DTP** (Data Server Protocole ou Processus de transfert de données). Il y a un DTP côté client (USER-DTP) et un DTP côté serveur (SERVER-DTP).

Remarque Il existe un autre protocole de transfert de fichier appelé **TFTP** (***Trivial File Transfer Protocol***). Ce protocole est utilisé pour le transfert actif de fichiers sans connexion.

6.4 DHCP

Afin de pouvoir communiquer sur un réseau, un périphérique a besoin d'informations (adresse IP, masque, adresse d'un serveur DNS, adresse d'une passerelle..). Il serait possible de configurer manuellement chaque périphérique, mais cela serait fastidieux, sujet à erreur et surtout très rigide. Le protocole DHCP nous permet d'automatiser tout cela.Ce protocole utilise le port UDP 67 côtés serveur et 68 côtés client.

Le serveur DHCP doit garantir que toutes les adresses IP soient uniques. L'obtention d'une adresse IP dynamique s'effectue en quatre étapes :



(**DHCPNAK**). Le client doit recommencer le processus de sélection.

6.5 DNS

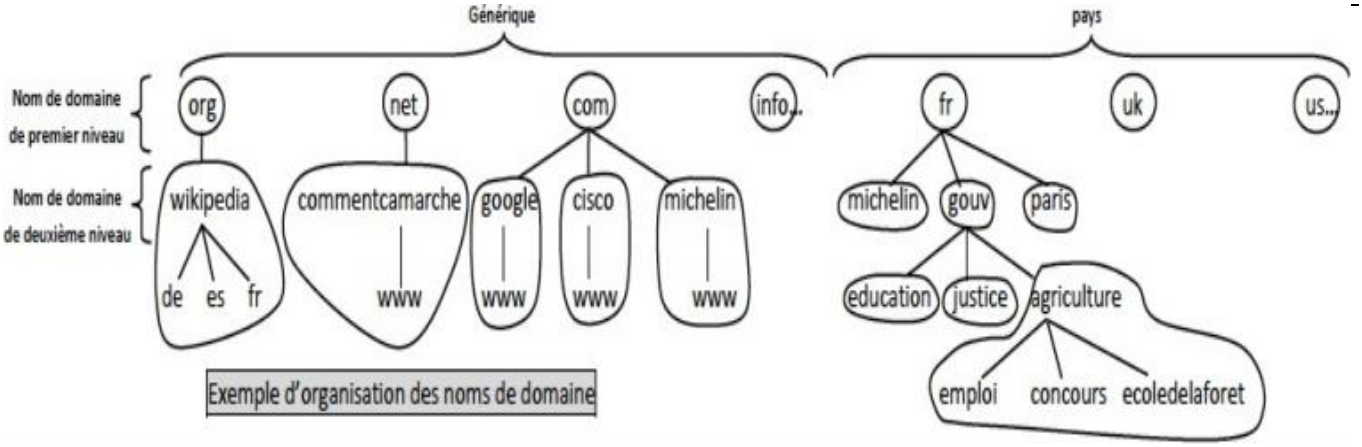
Sur les réseaux, les périphériques sont identifiés à l'aide d'un adresse numérique (combinaison de 4 série de 3 chiffre pour IP V4, ex : 199.156.23.25). Or, ces adresses numériques sont difficiles à mémoriser, on préfère donner un nom à un périphérique.

Le protocole DNS permet de connaitre l'adresse logique qui se cache derrière un nom de périphérique.

Notion de domaine :

- Un domaine est un ensemble de périphériques reliés à internet ayant des caractéristiques en commun.
- Les domaines sont organisés de façon hiérarchique sous forme d'arbres (un domaine peut être décomposé en plusieurs autres domaines qui à leur tour peuvent à nouveau être décomposés en plusieurs autres domaines…).
- Le nom d'un domaine se représente en écrivant (successivement, dans l'ordre et séparé d'un point), tous les noms des domaines se situant entre lui et le domaine de plus haut niveau.

Exemple : www.education .gouv.fr



Serveurs de nom

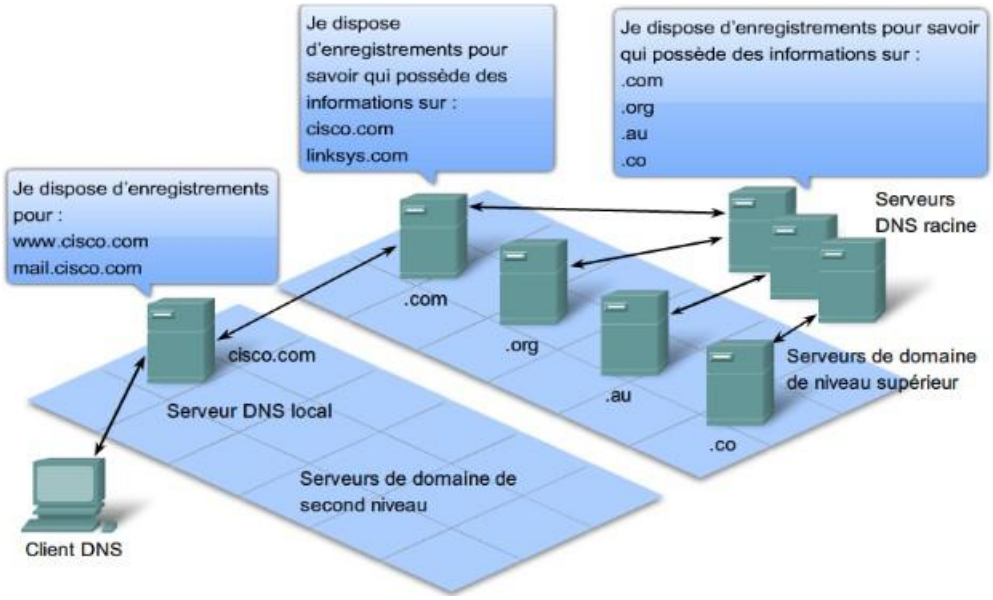
Les serveurs de nom (DNS) sont les périphériques qui permettent d'effectuer des résolutions de noms de domaine (c'est à dire associer une adresse IP à un nom de domaine).

Lorsqu'un périphérique souhaite connaitre l'adresse IP correspondant à un nom de domaine, il doit en faire la demande (requête DNS) au serveur DNS local défini dans sa configuration.

Il existe 3 types de serveur DNS :

- Les serveurs (de zone) primaires : il y en a un seul par zone. Ils tiennent à jour un fichier qui établit les correspondances entre les noms de domaine de leur zone et les adresses IP. Ils font autorité sur leur zone car ils sont obligatoirement à jour.
- Les serveurs (de zone) secondaires : Il peut y en avoir plusieurs par zone. Ils tiennent leurs informations du serveur primaire de leur zone avec lequel il font des mises à jour régulières.
- Les serveurs caches : Ils ne sont pas liés à une zone en particulier. Leurs informations sont issues de requêtes qu'ils ont effectuées auprès d'autres serveurs DNS.

Remarque : Un serveur primaire ou secondaire peut aussi remplir un rôle de serveur cache.



Le service DNS se base sur une architecture client/serveur. Le client DNS est nommé **résolveur DNS**, et le serveur qui effectue la résolution des noms est appelé **named** (**name daemon**). Pas un seul

serveur mais un ensemble distribué de serveurs existent :

Il existe deux types de requêtes effectuées par le client :

— **Une requête récursive** : lorsqu'un serveur DNS reçoit une requête récursive, le processus de démon de nom du serveur examine d'abord ses propres enregistrements pour voir s'il peut résoudre le nom. S'il ne peut pas résoudre le nom à l'aide de ses enregistrements stockés, il contacte d'autres serveurs, au nom du résolveur, pour résoudre le nom. La requête peut être transmise à plusieurs serveurs, ce qui peut nécessiter un délai supplémentaire et consommer de la bande passante. Lorsqu'une correspondance est trouvée et retournée au serveur demandeur d'origine, le serveur stocke temporairement dans le cache l'adresse numérique correspondant au nom.

— **Une requête itérative** : le serveur renvoie la réponse dont il dispose sans contacter d'autres serveurs DNS. Si il n'a pas de réponse, il répond avec l'adresse d'un autre serveur résolveur. Le client peut utiliser l'adresse suggérée ou peut l'ignorer et de travailler sur une liste de serveurs DNS qu'il a dans une base de données.

Le service client DNS stocke en mémoire les noms déjà résolus. Sous Windows, la commande **ipconfig /displaydns** permet d'afficher le contenu du cache DNS d'une machine hôte.

L'utilitaire **nslookup** permet de consulter le serveur DNS par défaut de la machine hôte.

Références

[1] Rémy H. : *Concepts de base des réseaux sans fil.*

Disponible sur : https ://zigbee.readthedocs.io/fr/latest/resans-fil.html. 2013.

[2] Servin, C., & Arnaud, J : *Réseaux et télécoms : cours et exercices corrigés*. Publisher-Dunod. 2003.

[3] Pujolle, G. : *Initiation aux réseaux : Cours et exercices*. Éditions Eyrolles. 2001.

— RFCs : https ://www.ietf.org/standards/rfcs/.

— Bron, A. : *Services et Réseaux v5.0*. Publisher-Alain Bron. 2016.

— *Notions de base DHCP*. https ://support.microsoft.com/fr-dz/help/169289/dhcp-dynamic-hostconfiguration-protocol-basics.

— Pujolle, G. : *Cours réseaux et télécoms : avec exercices corrigés*. Éditions Eyrolles. 2004.

— Pujolle, G. *Les réseaux.* Éditions Eyrolles. 2014.

— Certification CISCO CCNA : Routing and Switching - CCNA 1 Introduction aux réseaux V6.0.

— Andrew S. Tanenbaum : *Réseaux (Exercices et corrigés)Avec plus de 400 exercices.* Édition Pearson (4eme édition). 2004.