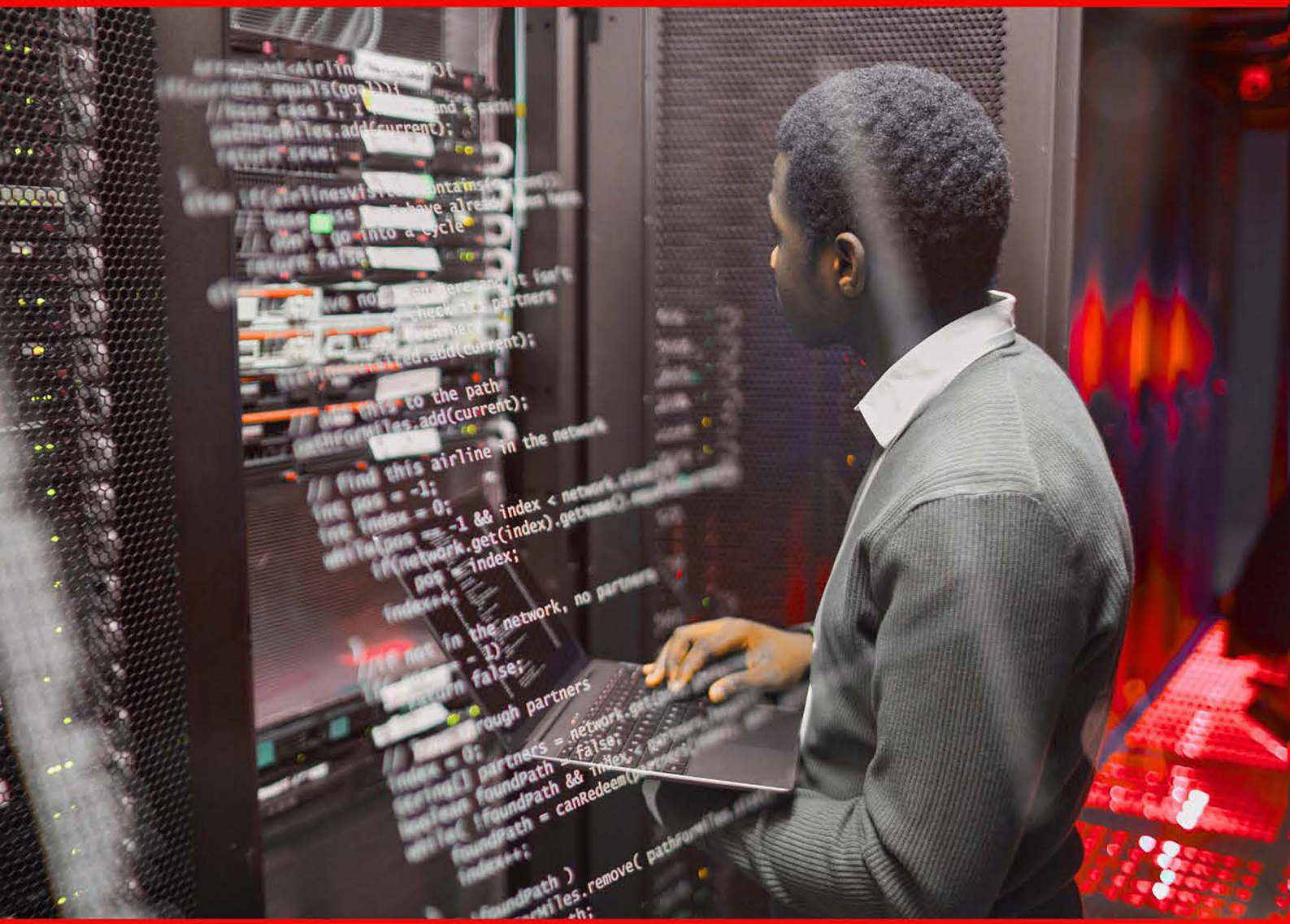
Réseau En Clair

Comprendre les bases du réseau pour bien démarrer en CCNA

Ressource indépendante – non affiliée à Cisco

Notions de base en réseautique

CCNA 1 Companion Guide



Support d'apprentissage indépendant couvrant les notions fondamentales du CCNA 1

SOMMAIRE

Module 1

Présentation des réseaux

Éléments requis pour une connexion à Internet :

Pour se connecter à Internet, il faut avoir : une connexion physique, une connexion logique et plusieurs applications.

Connexion physique : relier l'interface réseau d'un PC (une carte NIC ou modem) à un réseau. → Transfert des signaux.

Connexion logique : utiliser des protocoles (ensemble des règles) pour permettre la communication et la transmission des données entre les unités réseaux. → Généralement la suite des protocoles TCP/IP.

Applications : programmes servant à interpréter les données et les afficher sous une forme compréhensible.

Notions de base sur les PC :

Les petits composants :

- *Transistor* : dispositif qui amplifie un signal ou qui ouvre et ferme un circuit.
- *Circuit intégré* : dispositif constitué d'un matériau semi-conducteur, qui contient de nombreux transistors et remplit une fonction précise.
- *Résistance* : composant électrique qui limite ou régule le flux de courant électrique dans un circuit électronique
- *Condensateur* : composant électronique qui emmagasine de l'énergie sous forme de champ électrostatique
- *Connecteur* : partie d'un câble qui se branche sur un port ou une interface
- *Diode électroluminescente* (LED) : dispositif semi-conducteur qui émet de la lumière lorsqu'un courant le traverse

Sous-systèmes :

- *Cartes de circuits imprimés*
- *Lecteurs* : de CD, de disquette.
- *Disque dur*.
- *Processeur* & microprocesseur.
- *Carte mère*.
- *Mémoires* : RAM & ROM
- *Emplacements d'extension* : ISA, PCI, AGP …
- *Bus*.
- *Alimentation*.
- *Boitier*.

Composants de fond de panier :

- *Les cartes d'extension* (carte NIC, carte graphique, carte son …)
- *Les ports* de la carte mère (parallèle, série, USB, Firewire …)
- *Cordons d'alimentation*.

Carte réseau :

La carte réseau (adaptateur réseau) est une carte de circuits imprimés insérés dans un emplacement de la carte mère.

- Le bus PCI ou ISA (ou intégré) : sur un ordinateur de bureau.
- Le bus PCMCIA : sur les ordinateurs portables.

On peut également utiliser des cartes réseaux externes (via le port USB).

La carte communique avec le réseau via une connexion série et avec l'ordinateur par le bus interne (connexion parallèle).

La carte utilise une demande d'interruption (IRQ), une adresse d'entrée/sortie (E/S) et de l'espace en mémoire haute pour communiquer avec le système d'exploitation.

Les critères pour choisir une carte réseau :

- Protocoles : Ethernet, Token Ring ou FDDI.
- Types de média : paire torsadée, coaxial ou fibre optique.
- Type de bus système : PCI ou ISA.

Installation d'une carte réseau et d'un modem :

Le modem (modulateur-démodulateur) est un équipement nécessaire pour relier l'ordinateur à une ligne téléphonique. Il convertit les signaux numériques de l'ordinateur en signaux analogiques compatibles avec une ligne téléphonique standard et vice versa.

Il existe des modems internes et autres externes.

Quand installer une carte réseau ?

- Installation sur un PC qui n'en est pas déjà.
- Remplacement d'une carte endommagée.
- Mise à niveau d'une carte réseau pour augmenter la vitesse.
- Installation d'une carte de type différent, par exemple sans fil.
- Ajout d'une carte secondaire ou de secours.

L'évolution des technologies de connectivité :

Les modems sont apparus au début des années 1960, ils servaient à connecter des terminaux passifs à un ordinateur central. (vitesse de 300 bits/s).

Dans les années 1970, le prix des PC est devenu plus adorable et les systèmes BBS (Bulletin Board System) sont apparus.

Dans les années 1990, le débit des modems est passé à 9 600 bits/s jusqu'à atteint 56 Kbits/s.

En 1998, Les services à haut débit (DSL) sont utilisés dans les environnements d'entreprise.

Test de connectivité avec la commande ping :

La commande Ping lance un utilitaire qui vérifie l'existence d'une adresse IP et son accessibilité en utilisant des paquets ICMP (*Internet Control Message Protocol*).

La réponse renvoyée indique le taux de réussite et le temps de parcours aller-retour entre les équipements source et de destination.

Processus :

- Ping de l'@ de bouclage locale : Ping 127.0.0.1
- Ping de l'@ IP locale.
- Ping de l'@ de passerelle par défaut.
- Ping de l'@ de l'ordinateur distant.

Navigateurs Web et modules d'extension :

Un navigateur Web est un logiciel conçu pour interpréter les codes des langages de programmation afin d'afficher un résultat compréhensible par l'utilisateur.
→ Afficher des graphiques, lire des fichiers audio ainsi que des films …

Les navigateurs les plus connues : Internet Explorer & Netscape.

Internet Explorer	Netscape
Intégré au SE Microsoft	1er navigateur très répandu
Occupe plus d'espace disque	Occupe moins d'espace disque
Affiche les fichiers HTML, les images, les vidéos …	

- Les liens hypertexte incorporés dans une page Web permettent d'accéder rapidement à un emplacement différent dans une même page ou à une adresse Internet différente.

- Les modules d'extension se sont des logiciels qui fonctionnent conjointement avec les navigateurs afin de lancer les programmes requis par les fichiers spéciaux. (Flash, QuickTime, Real Player …)

Procédure de dépannage PC/réseau :

- Définition du problème
- Assembler les informations nécessaires.
- Etude des possibilités.
- Conception d'un plan d'action.
- Mise en œuvre du plan.
- Observation des résultats.
- Enregistrement des résultats.
- Dépannage.

Présentation binaire des données :

Les ordinateurs gèrent et stockent les données à l'aide de commutateurs électroniques pouvant prendre deux états :

- « En fonction », ON → 0 0 voltes
- « Hors fonction », OFF → 1 +5 voltes

Le code ASCII (*American Standard Code for Information Interchange*) est le plus couramment utilisé pour représenter les données alphanumériques dans les ordinateurs.

Chaque caractère est représenté par une combinaison unique de 8 chiffres binaires (Octet).

Dans un ordinateur, un octet représente un emplacement de mémoire adressable unique.

Systèmes de numération :

Les systèmes les plus utilisés en réseau :

Binaire : 0 et 1
Décimal : 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9
Héxadécimal : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E et F

Conversion des nombres :

Binaire → Décimal :

$(10011)_2 = 1*2^4 + 0*2^3 + 0*2^2 + 1*2^1 + 1*2^0 = 16 + 0 + 0 + 2 + 1 = (19)_{10}$

Décimal → Binaire :

$(19)_{10} = (10011)_2$

19 / 2 = 9	1
9 / 2 = 4	0
4 / 2 = 2	0
2 / 2 = 1	0
1 / 2 = 0	1

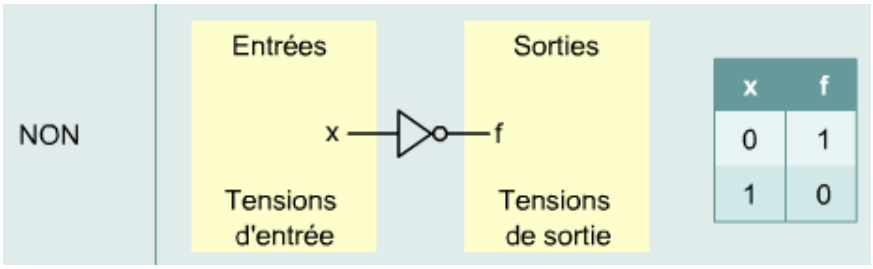
Règle :

Décimal → Base X : division sur la base X jusqu'avoir 0.

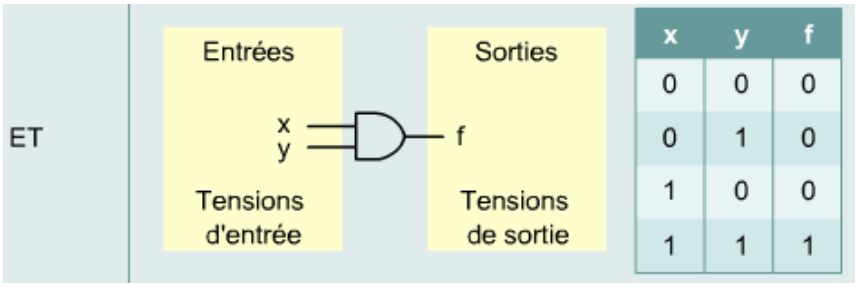
Logique booléenne :

La logique booléenne se rapporte aux circuits numériques acceptant une ou deux tensions électriques d'entrée. Il permet de comparer deux valeurs et d'effectuer un choix d'après ces valeurs.

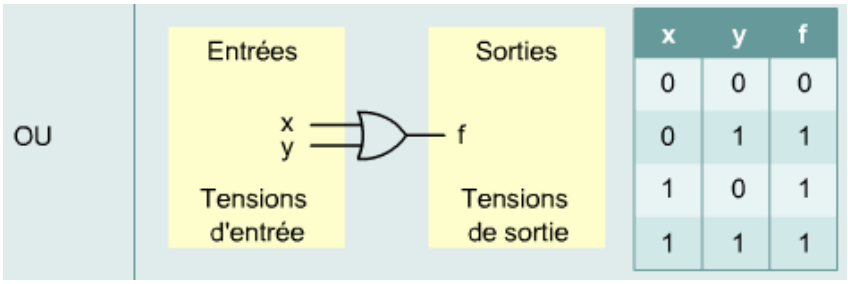
Dans un réseau, deux types d'opérations font appel à la logique booléenne : la création de masques de sous-réseau et de masques génériques, qui permettent de filtrer des adresses.



x	f
0	1
1	0



x	y	f
0	0	0
0	1	0
1	0	0
1	1	1



x	y	f
0	0	0
0	1	1
1	0	1
1	1	1

Module 2

Notions de base sur les réseaux

Evolution des réseaux de données :

Pour les entreprises, il n'était ni efficace ni rentable d'utiliser des disquettes pour partager des données. Le «réseau disquettes» multipliait les copies des données.

Les entreprises ont vite réalisé que la mise en réseau des ordinateurs pouvait augmenter leur productivité.

A ses débuts, le développement des réseaux était quelque peu désorganisé. Chaque société qui créait des matériels et des logiciels de réseau utilisait ses propres normes. (Incompatibilité entre les systèmes réseaux).

Historique des réseaux :

→ Dans les années 40, les ordinateurs étaient de gigantesques machines.

→ En 1947, l'invention du semi-conducteur (réaliser des ordinateurs plus petits + plus fiable)

→ À la fin des années 1950 apparut le circuit intégré, qui combinait alors quelques transistors.

→ En 1977, Apple Computer lança le premier micro-ordinateur, également appelé Mac.

→ En 1981, IBM introduisit son premier PC.

→ Au milieu des années 80, les utilisateurs de PC commencèrent à utiliser des modems pour partager des fichiers avec d'autres ordinateurs (la communication point-à-point).

→ Entre les années 60 et 90, le ministère américain de la Défense (DoD) développa de grands réseaux étendus (WAN) fiables à des fins militaires et scientifiques. Elle permettait à plusieurs ordinateurs de s'interconnecter en empruntant différents chemins

→ Le réseau étendu développé par le DoD devint plus tard le réseau Internet.

Equipements de réseau :

On appelle équipement tout matériel qui se connecte directement à un segment du réseau.

Il y a deux catégories d'équipement :

- **Equipements d'utilisateur final (hôtes)** : Matériels qui fournissent des services directement à l'utilisateur (Ordinateurs, imprimantes, scanneurs …)
- **Equipements de réseau** : Matériel servant à interconnecter les équipements d'utilisateur final (Routeurs, Commutateurs, Hubs …)

* **Un répéteur** est un équipement réseau qui sert à régénérer un signal.

* **Les concentrateurs** se sont des équipements qui concentrent des connexions (passif), Les concentrateurs actifs ajoutent la caractéristique de régénération des signaux.

* **Les ponts** assurent les connexions entre les différents réseaux locaux + convertissent les formats des données réseau + Filtre le trafic.

* **Les commutateurs de groupe de travail** filtrent le trafic + ne convertit pas les formats de transmission de données.

* **Les routeurs** peuvent régénérer les signaux + concentrer plusieurs connexions + convertir les formats de transmission de données + gérer les transferts de données. + se connecter à un réseau étendu.

Topologie de réseau :

La topologie réseau définit la structure du réseau, il existe deux types :

- **Topologie physique** : la disposition des médias et des hôtes sur le réseau.
- **Topologie logique** : la façon dont les hôtes accèdent aux médias.

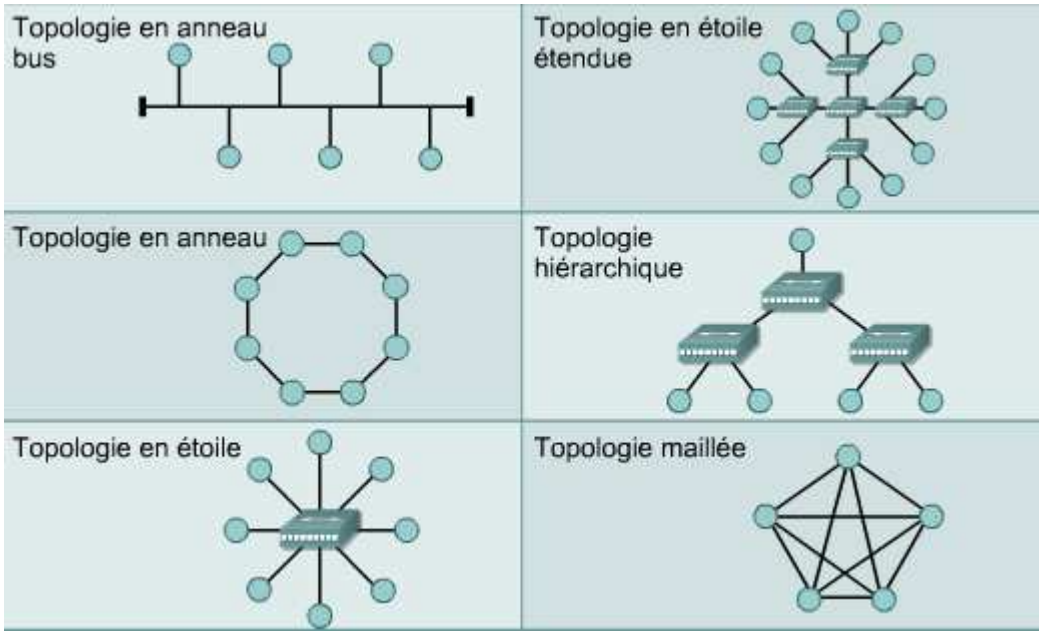
➔ Les topologies physiques couramment utilisées :

- *Une topologie de bus* : tous les hôtes se connectent directement à un seul câble de backbone.
- *Une topologie en anneau* : chaque hôte est connecté à son voisin. Le dernier hôte se connecte au premier.
- *Une topologie en étoile* : tous les câbles sont raccordés à un point central.
- *Une topologie en étoile étendue* relie des étoiles individuelles en connectant les concentrateurs ou les commutateurs.
- *Une topologie hiérarchique* est similaire à une topologie en étoile étendue. Cependant, plutôt que de lier les concentrateurs ou commutateurs ensemble, le système est lié à un ordinateur qui contrôle le trafic sur la topologie.
- *Une topologie maillée* : chaque hôte possède ses propres connexions à tous les autres hôtes.

➔ Les deux types de topologie logiques les plus courants :

- *Le broadcast* : indique que chaque hôte envoie ses données à tous les autres hôtes sur le média du réseau (Ethernet)
- *Le passage de jeton*. : jeton électronique est transmis de façon séquentielle à chaque hôte (Token Ring & FDDI)

NB : Arcnet est une variante de Token Ring et de FDDI. Il s'agit d'un passage de jeton sur une topologie de bus.



Protocoles de réseau :

Les suites de protocoles sont des ensembles de protocoles qui permettent à des hôtes de communiquer sur un réseau.

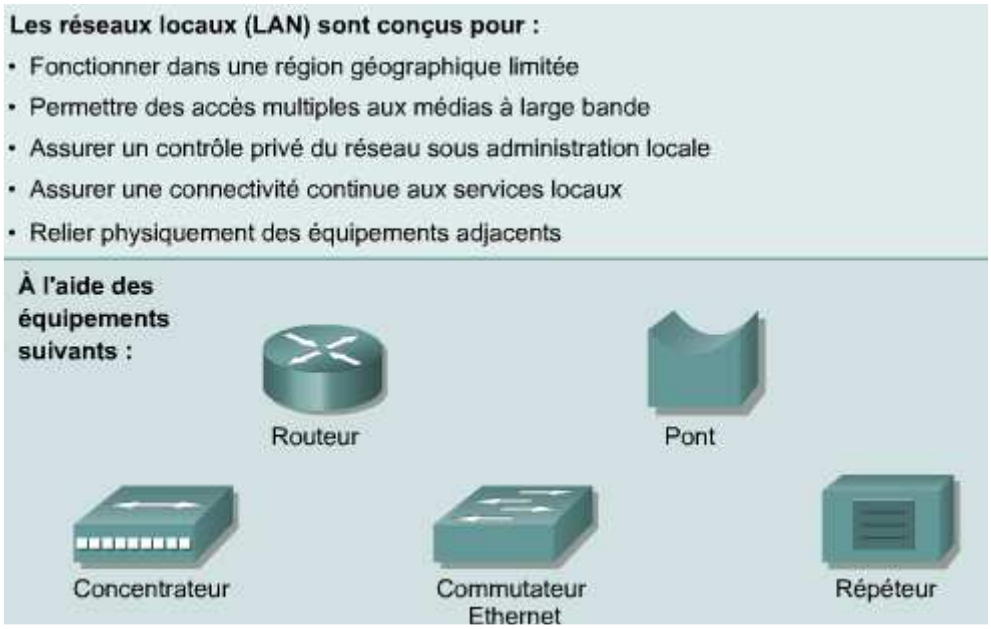
Un protocole est une description formelle d'un ensemble de règles et de conventions qui régissent un aspect particulier de la façon dont les équipements communiquent sur un réseau.

Les protocoles déterminent le format, la chronologie, le séquençage et le contrôle d'erreur dans la communication de données.

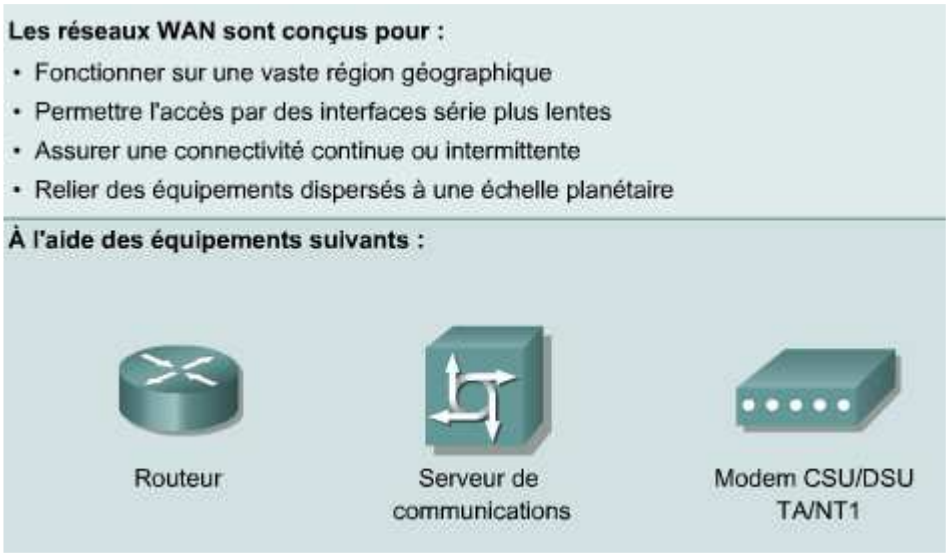
Ces règles de réseau sont créées et actualisées par un grand nombre d'organisations et de comités :

- ***IEEE*** (Institute of Electrical and Electronic Engineers)
- ***ANSI*** (American National Standards Institute)
- ***TIA*** (Telecommunications Industry Association)
- ***EIA*** (Electronic Industries Alliance)
- ***ITU*** (International Telecommunications Union) précédemment nommée CCITT (Comité Consultatif International Téléphonique et Télégraphique).

Réseaux locaux (LAN) :



Réseaux étendus (WAN) :



Réseaux métropolitains (MAN) :

Un réseau MAN est un réseau qui s'étend à une zone métropolitaine telle qu'une ville. Un réseau MAN comprend habituellement au moins deux réseaux LAN situés dans une zone géographique commune. Par exemple, une banque possédant plusieurs agences.

Réseaux de stockage (SAN) :

Un réseau de stockage (SAN) est un réseau à haute performance dédié qui permet de transférer des données entre des serveurs et des ressources de stockage. Du fait qu'il s'agit d'un réseau dédié distinct, il évite tout conflit de trafic entre les clients et les serveurs.

- **Performance** : les réseaux SAN permettent un accès simultané à haut débit, par deux serveurs ou plus, aux matrices de disques et de bandes.
- **Disponibilité** : Les réseaux SAN intègrent la tolérance aux sinistres. Les données peuvent être dupliquées sur un réseau SAN situé jusqu'à 10 km de distance.
- **Évolutivité** : Un réseau SAN peut utiliser les technologies les plus variées. Cela facilite le déplacement des données de sauvegarde, des opérations, la migration des fichiers et la réplication des données entre les systèmes.

Réseaux privés virtuels (VPN) :

Un réseau privé virtuel (VPN) est un réseau privé construit au sein d'une infrastructure de réseau publique (Internet) qui permet de construire un tunnel sécurisé entre les deux extrémités du réseau.

Trois principaux types de VPN :

- *Les VPN d'accès* fournissent aux utilisateurs mobiles et de petits l'accès distant à un intranet ou à un extranet sur une infrastructure partagée.
- *Les VPN d'intranet* font appel à des connexions dédiées pour raccorder des bureaux régionaux et des bureaux distants à un réseau interne sur une infrastructure partagée.
- *Les VPN d'extranet* utilisent des connexions dédiées pour relier des partenaires commerciaux à un réseau interne sur une infrastructure partagée.

Intranets & Extranets :

→ ***Un intranet*** est une configuration de réseau local conçus pour autoriser les utilisateurs qui ont des privilèges d'accès à accéder au réseau local interne de l'organisation.

→ ***Un extranet*** est une extension de deux stratégies intranet au moins, avec une interaction sécurisée entre les entreprises participantes (accès étendu et sécurisé)

Importance de la bande passante

La bande passante est définie comme la quantité d'informations qui peut transiter sur une connexion réseau en un temps donné.

- la bande passante est limitée par des facteurs physiques et technologiques.

- La bande passante n'est pas gratuite (WAN).
- Les besoins en bande passante augmentent.
- La bande passante est critique pour les performances du réseau.

La bande passante proprement dite d'un réseau résulte d'une combinaison des médias physiques et des technologies choisis pour la signalisation et la détection des signaux du réseau.

Analogies présentant la bande passante :

➔ La bande passante est semblable au diamètre d'un tuyau.

La largeur du tuyau détermine sa capacité de transport en eau. Par conséquent, l'eau peut être comparée aux données, et la largeur du tuyau à la bande passante.

➔ La bande passante peut être comparée au nombre de voies d'une autoroute.

Lorsque le système autoroutier est peu fréquenté, chaque véhicule est en mesure de se déplacer librement. Lorsqu'il y a davantage de trafic au contraire, chaque véhicule se déplace plus lentement. C'est sur les routes qui comportent le moins de voies que cela est le plus évident.

Unités de mesure de la bande passante :

L'unité de base de la bande passante est le bit par seconde (bit/s).

1 Kbits/s	10^3 bits/s
1 Mbits/s	10^6 bits/s
1 Gbits/s	10^9 bits/s
1 Tbits/s	10^{12} bits/s

La bande passante et la *vitesse* sont souvent utilisés indifféremment.

Le débit :

Le terme débit se rapporte à la bande passante réelle mesurée, à une heure particulière de la journée en empruntant des routes Internet particulières et lors de la transmission sur le réseau d'un ensemble de données spécifique.

Facteurs déterminants le débit:

- Équipements d'interconnexion
- Type de données transmises
- Topologie de réseau
- Nombre d'utilisateurs
- Ordinateur de l'utilisateur

- Ordinateur serveur
- Conditions d'alimentation
- L'heure du jour.

Meilleur téléchargement

$$D = \frac{T}{BP}$$

Téléchargement type

$$D = \frac{T}{P}$$

BP	Bande passante théorique maximale de la liaison " la plus lente " entre l'hôte source et l'hôte de destination (mesurée en bits par seconde)
P	Débit effectif au moment du transfert (mesuré en bits par seconde)
D	Durée du transfert des fichiers (mesuré en secondes)
T	Taille de fichier en bits

Le résultat n'est qu'une estimation, parce que la taille du fichier n'inclut pas la surcharge due à l'encapsulation.

La bande passante numérique :

Bien que les signaux analogiques soient capables de transporter une grande variété d'informations, ils n'offrent pas autant d'avantages que les transmissions numériques.

Il est possible d'envoyer des quantités illimitées d'informations via un canal numérique, même de faible bande passante. Quel que soit le temps nécessaire à leur transfert et à leur réassemblage, les informations numériques peuvent toujours être visualisées, écoutées ou traitées dans leur forme originale.

Utilisation des couches :

Les modèles OSI et TCP/IP comportent des couches qui spécifient comment les données doivent être communiquées d'un ordinateur à l'autre. (Problèmes de flux)

→ Qu'est ce qui circule ?
→ Quels objets circulent ?
→ Quelles règles régissent le flux ?
→ Où cette circulation se fait-elle ?

Modèle OSI :

Le terme « propriétaire » signifie qu'une entreprise ou un petit groupe d'entreprises contrôle entièrement l'utilisation de la technologie. Les technologies réseau qui suivaient strictement des règles propriétaires ne pouvaient pas communiquer avec des technologies qui respectaient des règles propriétaires différentes.

C'est pourquoi l'OSI (International Organization for Standardization) examina les modèles réseau tels que DECnet (Digital Equipment Corporation net), SNA (Systems Network Architecture) et TCP/IP afin de trouver un ensemble de règles applicable de façon générale à tous les réseaux, c'est le modèle OSI (Open System Interconnection) 1984.

Avantages du modèle OSI :

- il réduit la complexité
- il uniformise les interfaces
- il facilite la conception modulaire
- il assure l'interopérabilité de la technologie
- il accélère l'évolution
- il simplifie l'enseignement et l'acquisition des connaissances

Couches OSI :

Le modèle OSI comprend 7 couches.

Physique → Liaison de donnée → Réseau → Transport → Session → Présentation → Application

Pour les mémoriser « **A**près **P**lusieurs **S**emaines **T**ous **R**espirent **L**a **P**aix »

Avantages de découpage de 7 couches :

- Il permet de diviser les communications sur le réseau en éléments plus petits et plus gérable, ce qui permet de les comprendre plus facilement.
- Il uniformise les éléments du réseau afin de permettre le développement et le soutien multiconstructeur.
- Il permet à différents types de matériel et de logiciel de communiquer entre eux.
- Les modifications apportées à une couche n'affectent pas les autres couches.

Rôles de chaque couche :

Physique : fils, connecteurs, tensions, débits …

Liaison de données : assure un transfert fiable + connecter les hôtes + filtrer le trafic (MAC)

Réseau : adressage logique + routage & choix du meilleur chemin (IP)

Transport : fiabilité du transport des données + détection des pannes + contrôle de flux

Session : établit, gère et ferme les sessions entre les applications

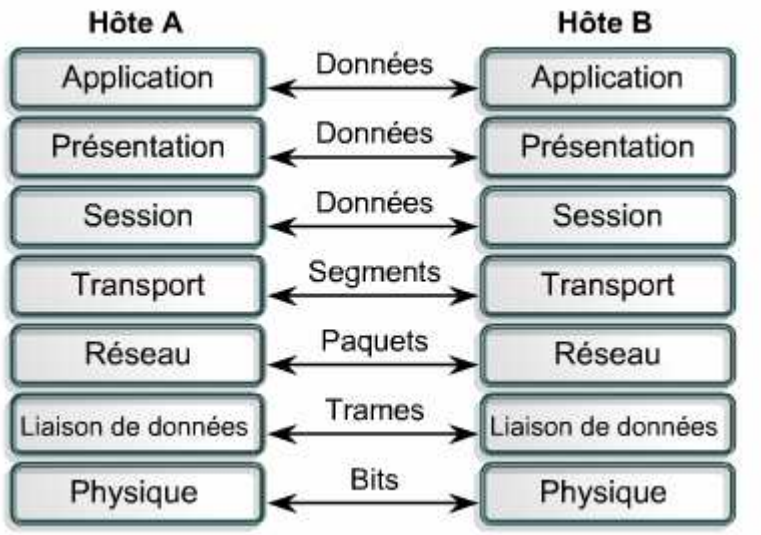
Présentation : lisibilité des données + formatage + compression + cryptage.

Application : fournit des services au processus d'application (courrier, transfert de fichier …)

Communication d'égal à égal :

Afin de permettre l'acheminement des données entre l'ordinateur source et l'ordinateur de destination, chaque couche du modèle OSI au niveau de l'ordinateur source doit communiquer avec sa couche homologue sur l'ordinateur de destination.

Le *PDU* (unité de donnée de protocole) c'est le protocole qui sert à la communication entre les couches homologues



Modèle TCP/IP :

TCP/IP *(Transmission Control Protocol/Internet Protocol)* est une norme ouverte d'Internet qui rend possible l'échange de données entre deux ordinateurs, partout dans le monde.

Couches de TCP/IP :

Le modèle TCP/IP comporte **4 couches** :

- *Application* (Application + Présentation + Session)
- *Transport* (Transport)
- *Internet* (Réseau)
- *Accès au réseau*. (Liaison de données + Physique)

Pour les mémoriser : « **A**vec **T**achefine l'**I**nformatique **A**vance »

Comparaison entre TCP/IP et OSI :

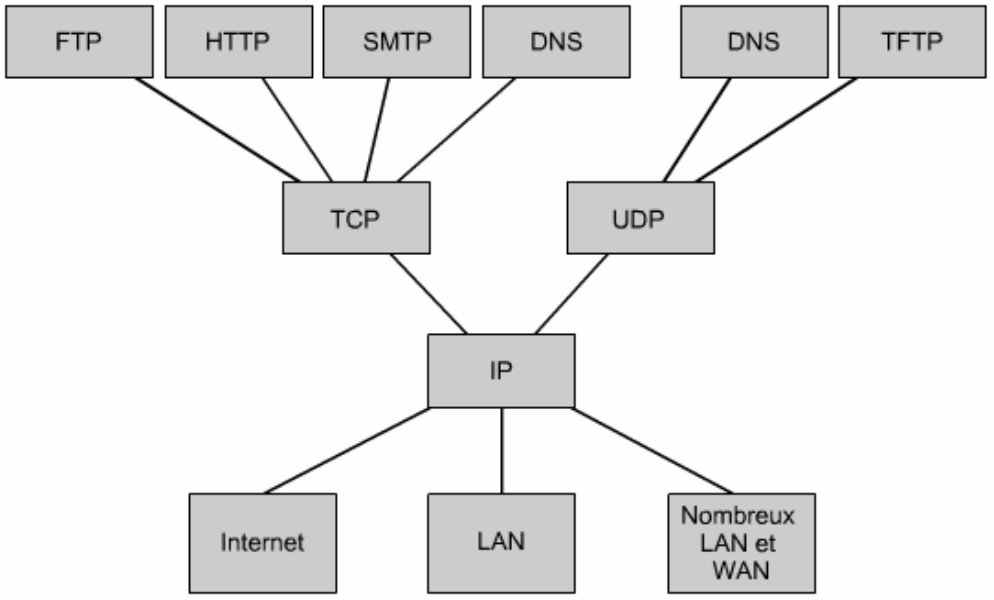
Similitudes	Différences
- comportent des couches. - comportent la couche application et transport mais ils sont différents. - utilisent la technologie commutation des paquets et pas la commutation des circuits.	- le nombre des couches. - TCP/IP intègre la couche présentation et session dans la couche application. - TCP/IP intègre la couche liaison de données et physique dans la couche Accès Réseau.

L'encapsulation :

L'encapsulation est un processus qui consiste à ajouter des en-têtes et des en queux de protocole déterminé avant que ces données soient transmises sur le réseau.

Les cinq étapes de conversion afin d'encapsuler les données:

1. *Construction des données* pouvant circuler dans l'interréseau.
2. *Préparation des données pour le transport de bout en bout* en utilisant des segments.
3. *Ajout de l'adresse IP du réseau à l'en-tête* (paquets, ou datagrammes), contenant un en-tête de paquet constitué des adresses logiques d'origine et de destination.
4. *Ajout de l'en-tête et de l'en-queue de la couche de liaison de données* : placer le paquet dans une trame.
5. *Conversion en bits pour la transmission* pour la transmission sur le média.



Module 3

Médias réseau

Aspects électriques :

Atomes & électrons :

Toute matière est composée d'atomes, chaque atome est composé des trois particules suivantes:

- *Électron* – Particule de charge négative gravitant autour du noyau
- *Proton* – Particule de charge positive
- *Neutron* – Particule neutre sans charge

Proton + neutron = ***Noyau***.

Modèle de Bohr :

→ Si on définit un atome comme étant *un stade* de football (taille)
- Les protons et les neutrons se sont des *ballons* au milieu du terrain.
- Les électrons auraient la taille de *cerises* et graviteraient autour du stade près des sièges les plus éloignés du terrain.

Loi de Coulomb sur la force électrique :

- Des particules de charges *opposées* sont *attirées* l'une vers l'autre
- Des particules de charges *identiques* génèrent une force dite *répulsive*.

Revoyez ces deux théories pour déterminer dans quelle mesure elles s'opposent.
« Les électrons restent en orbite, même si les protons attirent les électrons ».

Le raison :

Les protons restent solidaires en raison de la force nucléaire associée aux neutrons. Cette force extrêmement puissante agit comme une colle pour assurer la cohésion du noyau. Par contre, les électrons sont liés à leur orbite autour du noyau par une force plus faible que la force nucléaire.

→ L'électricité résulte de la libre circulation des électrons.
→ Les électrons libérés qui ne se déplacent pas forment l'électricité statique.

- Si ces électrons statiques entrent en contact avec un conducteur, ils génèrent une décharge électrostatique.
- Les circuits logiques des puces d'un ordinateur sont extrêmement sensibles aux décharges électrostatiques.

Les atomes, ou groupes d'atomes (appelés *molécules*), constituent des matériaux.
Les matériaux sont classés en trois groupes, selon la résistance qu'ils offrent aux électrons libres : isolants, conducteurs, semi-conducteurs.

Tension :

La tension électrique (U) est parfois appelée force électromotrice (FEM). Il s'agit de la force électrique, ou pression, qui s'exerce lors de la séparation des électrons et des protons.

La tension électrique peut également être produite par trois autres procédés : par *friction* (électricité statique), par *magnétisme* (générateur électrique) et par la *lumière* (photopile).

→ L'unité de mesure de la tension est le volt (**V**).

Résistance et impédance :

La résistance (R) au mouvement des électrons varie en fonction des matériaux à travers lesquels circule le courant. Tous les matériaux qui conduisent l'électricité sont dotés d'une mesure de résistance au flux d'électrons qui les traverse.

→ L'unité de mesure de la résistance est l'ohm (**Ω).**

Isolants	Conducteurs	Semi-conducteurs
Les électrons circulent difficilement	Les électrons circulent facilement	Le flux d'électrons peut être contrôlé de manière précise
Matière plastique Caoutchouc Air	Cuivre (Cu) Argent (Ag) Or (Au)	Carbone (C) Germanium (Ge) Arséniure de gallium (AsGa)
Papier Bois sec Verre	Soudure Eau ionisée Corps humain	Silicium (Si)

Courant :

Le courant électrique (I) est le flux de charges créé par le déplacement des électrons.

→ Lorsqu'une tension est appliquée, les électrons se déplacent depuis la borne négative (qui les repousse) vers la borne positive (qui les attire).

→ L'unité de mesure du courant est l'ampère (**A**). « L'ampère est le nombre de charges par seconde passant par un point dans un circuit.»

La combinaison volts-ampères produit des *watts* P=U*I

Les watts indiquent la puissance consommée ou produite par un type d'appareil.

Circuits :

Le courant circule dans des boucles fermées appelées circuits. Ces circuits doivent être composés de matériaux conducteurs et posséder une source de tension.

Une analogie avec l'eau permet de mieux comprendre le concept de l'électricité. Plus l'eau tombe de haut et plus la pression est grande, plus le débit est fort. Le débit de l'eau dépend également de la taille de l'espace à travers lequel elle coule. De même, plus la tension et la pression électrique sont élevées, plus le courant produit est important. Le courant électrique rencontre alors une résistance, à la façon d'un robinet qui réduit le débit de l'eau.

S'il s'agit d'un circuit de courant alternatif, la quantité de courant dépendra de l'impédance du matériau. S'il s'agit d'un circuit de courant continu, la quantité de courant dépendra de la résistance du matériau.

Un *oscilloscope* est un appareil électronique qui permet de mesurer les signaux électriques par rapport au temps. Il trace les ondes et les impulsions électriques, ainsi que les caractéristiques des signaux électriques. L'axe des x représente le temps, et l'axe des y la tension (2 entrées).

Loi d'ohm :

La relation entre la tension, la résistance et le courant est la tension (V) qui est égale au courant (I) multiplié par la résistance (R). Autrement dit : V=R*I

Spécification des câbles :

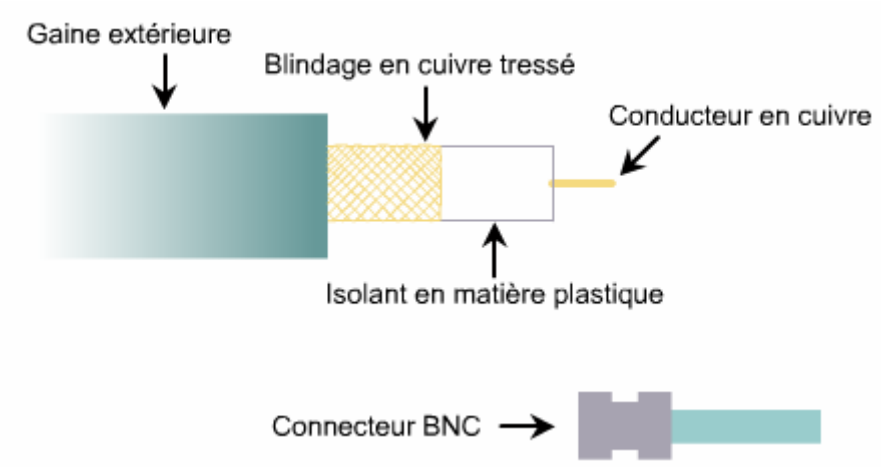
La spécification s'écrit sous la forme : ***XYZ***

X → débit du réseau local (10, 100, 1000)
Y → type de transmission « analogique / numérique » (Broad 'large bande', Base 'bande de base')
Z → Type de câble et distance maximal (T, TX, F, FX, 2, 5)

Par exemple : 10BaseT

Les médias en cuivre :

Le coaxial :



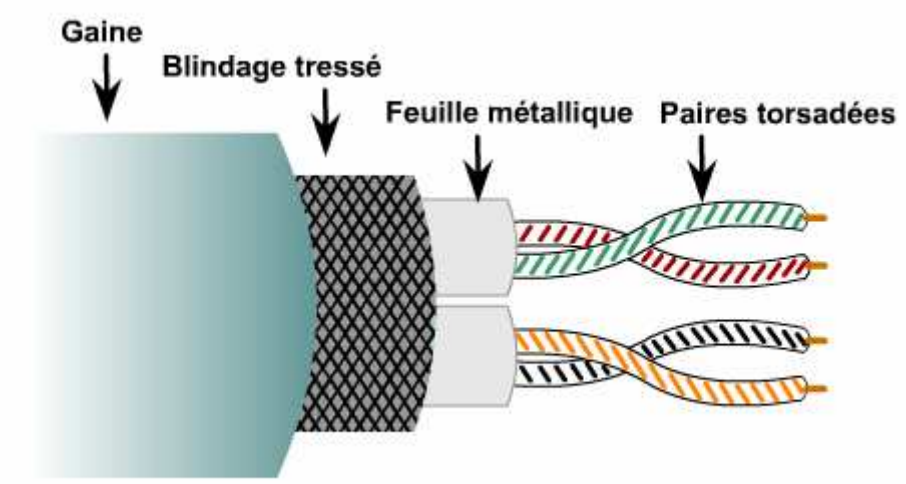
Il est constitué d'un conducteur de cuivre qui est enveloppé d'un isolant flexible qui entouré d'une torsade de cuivre qui agit comme protecteur du conducteur intérieur. La gaine du câble enveloppe ce blindage.

Caractéristiques :

	Epais	Fin
Impédance	50 ohms	75 ohms
Débit	De 10 à 100 Mbits/s	
Facilité d'installation	Moyenne	**Facile**
Coût	**Un peu coûteux**	**Faible**
Taille maximale	**500 m**	**185 m**
Connecteur	BNC	

→ Il peut couvrir des distances plus longues que les câbles à paires torsadées sans nécessiter de répéteurs
→ Le câble coaxial est moins onéreux que le câble à fibre optique.
→ Une connexion blindée défectueuse est une des causes les plus importantes des problèmes de connexion dans l'installation d'un câble coaxial.

La paire torsadée blindée (STP) :



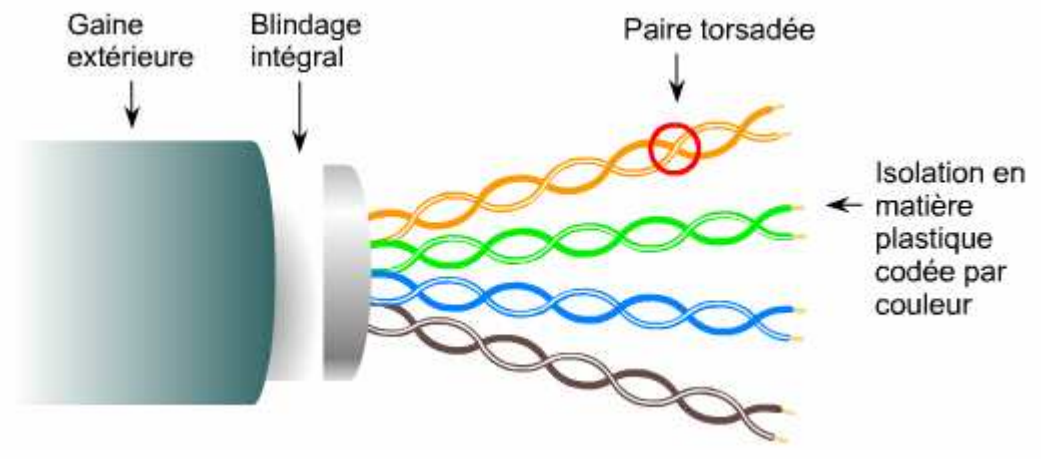
Il est constitué de 8 fils, Chaque paire de fils est enveloppée dans une feuille métallique et les quatre paires sont elles-mêmes enveloppées dans une tresse ou une feuille métallique. La gaine du câble enveloppe le câble.

Caractéristiques :

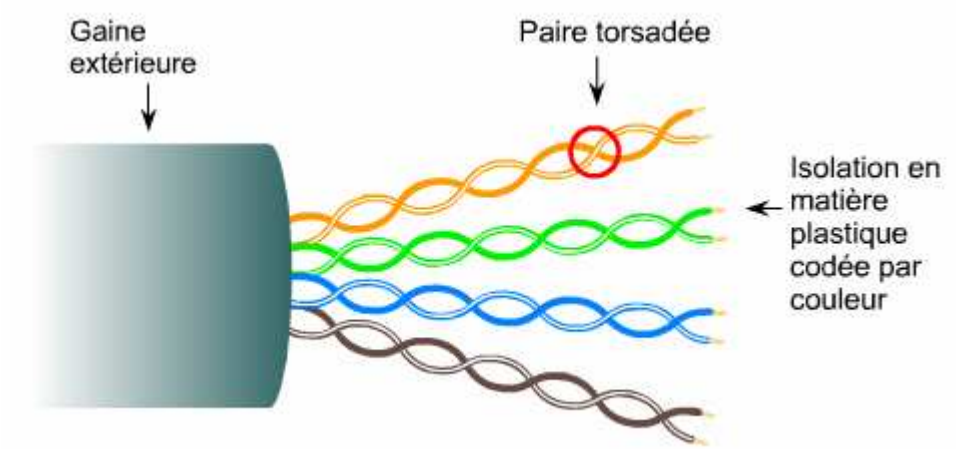
Impédance	150 ohms
Débit	De 10 à 100 Mbits/s
Facilité d'installation	**Moyenne**
Coût	**Moyenne**
Taille maximale	100 m
Connecteur	**RJ-45**
Il **réduit** le **bruit** électrique à l'intérieur, et les interférences électromagnétiques et radiofréquences à l'extérieur du câble.	

- Il peut provoquer des problèmes de bruit, s'il n'est pas mis à la terre (le blindage comporte comme une antenne qui attirant les signaux indésirables).

Le câble ScTP *(screened twisted pair)* ou FTP *(foil screened twisted pair)* est un nouveau type de câble UTP ***hybride***.



La paire torsadée non blindée (UTP) :



Il est constitué de quatre paires de fils. Chacun des 8 fils de cuivre du câble est protégé par un matériau d'isolation. De plus, les paires de fils sont tressées entre elles. (Pas de blindage des paires).

Caractéristiques :

Impédance	100 ohms
Débit	De 10 à 100 Mbits/s
Diamètre	**0.43 cm**
Facilité d'installation	**Facile**
Coût	**Faible**
Taille maximale	100 m
Connecteur	**RJ-45**

Il est *plus* sensible *au bruit électrique* et aux *interférences* que les autres types de média réseau, mais son connecteur joue un rôle important de réduire les bruits (améliorer la fiabilité de connexion).

- *La réduction de la diaphonie* entre les paires d'un câble à paires torsadées non blindées est fonction du *nombre de torsades*.

Aspects physiques de la lumière :

Spectre électromagnétique :

Lorsqu'une charge électrique va et vient ou accélère, elle produit de l'énergie électromagnétique. La lumière utilisée dans les réseaux à fibre optique est un type d'énergie électromagnétique.

Le classement de tous les types d'onde électromagnétique depuis l'onde la plus longue jusqu'à l'onde la plus courte forme un ensemble appelé spectre électromagnétique.

La longueur d'une onde électromagnétique est déterminée par le nombre de va-et-vient de l'onde générés par la charge électrique.

Les ondes électromagnétiques circulent toutes dans le vide à la même vitesse, soit approximativement à 300 000 kilomètres par seconde, qui est aussi la vitesse de la lumière.

L'œil humain ne perçoit que l'énergie électromagnétique avec des longueurs d'onde comprises entre 700 et 400 nanomètres (la lumière visible) 1nanomètre = 10^{-9} mètres

- Les ondes de lumière les plus longues avoisinant les 700 nanomètres sont de couleur rouge
- Les ondes de lumière les plus courtes avoisinant les 400 nanomètres sont de couleur violette.

→ Les ondes non visibles par l'œil humain sont utilisées pour transmettre les données via la fibre optique (de 850, 1 310 ou 1 550 nanomètres sont les longueurs qui circulent le mieux)

Rayons lumineux :

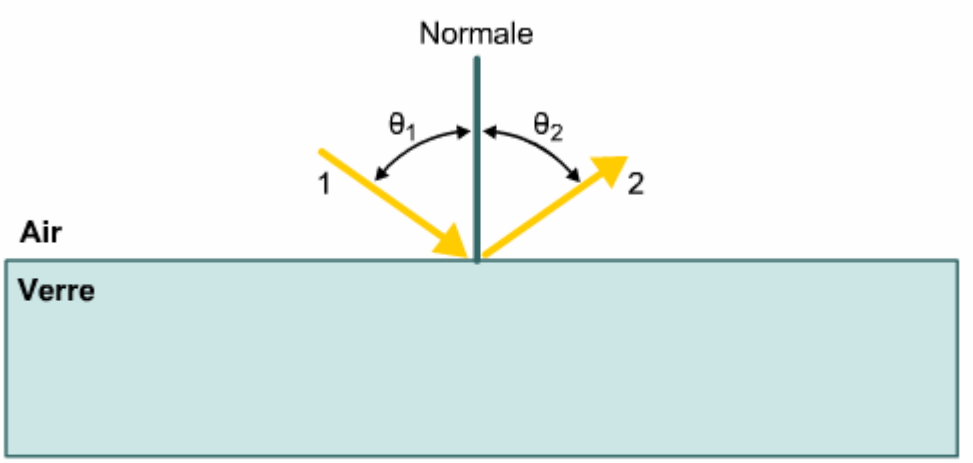
Les ondes électromagnétiques qui sortent d'une source forment des lignes droites appelées rayons.

La lumière circule en ligne droite continue à la vitesse de 300 000 kilomètres par seconde. Cependant, elle circule à des vitesses plus lentes dans des matières telles que l'air, l'eau et la glace.

$$\text{Indice de réfraction} = n = \frac{\text{Vitesse de la lumière dans le vide}}{\text{Vitesse de la lumière dans la matière}}$$

La réflexion :

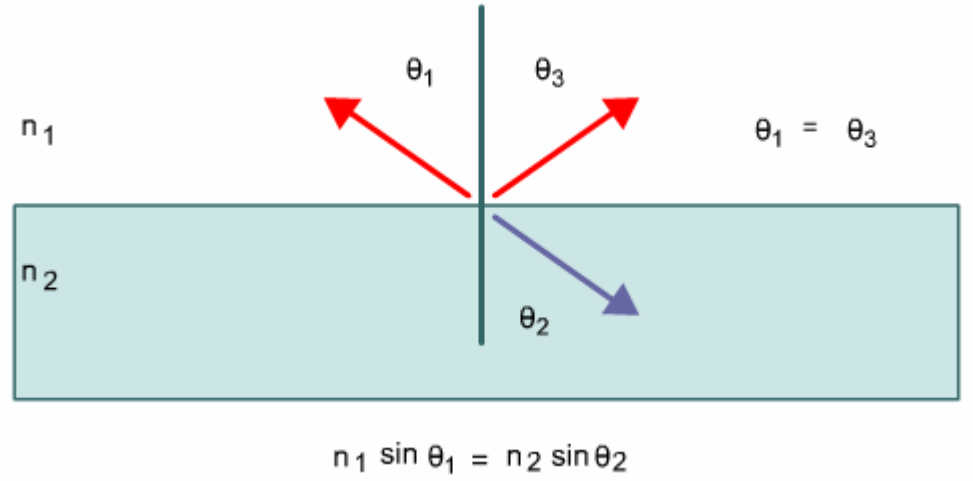
Lorsqu'un rayon lumineux (rayon incident) frappe la surface brillante d'un morceau de verre plat, une partie de l'énergie lumineuse du rayon se réfléchit.



Rayon 1 : Rayon incident, θ_1 degrés mesurés à partir de la normale
Rayon 2 : Rayon réfléchi, θ_2 degrés mesurés à partir de la normale
Loi de la réflexion : $\theta_1 = \theta_2$

La réfraction :

Lorsqu'un rayon lumineux frappe l'intervalle situé entre deux matières transparentes, la lumière se divise en deux parties. Une partie du rayon lumineux se reflète dans la première matière, avec un angle de réflexion égal à l'angle d'incidence. L'énergie restante du rayon traverse l'intervalle et pénètre dans la seconde matière.



$$n_1 \sin \theta_1 = n_2 \sin \theta_2$$

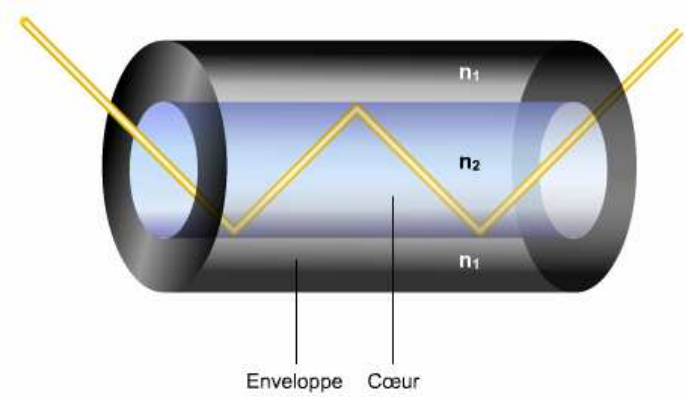
Si la lumière provient d'une matière dont l'indice de réfraction est plus élevé que celui de la matière vers laquelle elle se dirige, le rayon réfracté s'éloigne de la normale.

La réflexion interne total :

La réflexion interne totale entraîne les rayons lumineux circulant dans la fibre hors de la limite cœur-enveloppe et les achemine vers l'extrémité de la fibre.

Les deux conditions suivantes doivent être remplies pour que les rayons lumineux se réfléchissent dans la fibre sans que la réfraction entraîne une perte d'énergie:

- L'indice de réfraction (n) au cœur de la fibre optique doit être supérieur à celui du matériau qui l'enveloppe (l'enveloppe).
- L'angle d'incidence du rayon lumineux est supérieur à l'angle critique du cœur et de son enveloppe.



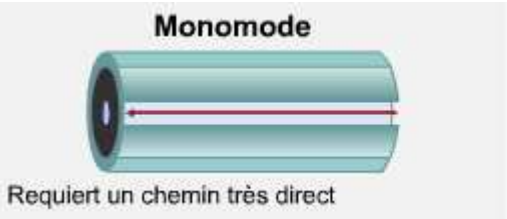
Il est possible de contrôler l'angle d'incidence des rayons lumineux entrant dans le cœur en limitant les deux facteurs suivants:

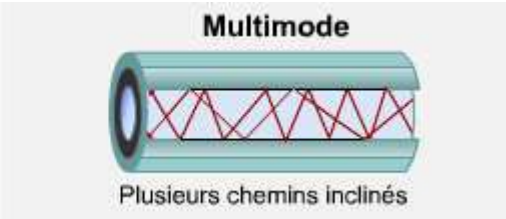
- *Ouverture numérique de la fibre* – c'est l'intervalle des angles des rayons incidents pénétrant dans la fibre qui seront entièrement réfléchis.
- *Modes* – Chemins suivis par un rayon lumineux lorsqu'il se déplace dans une fibre.

Les médias optiques :

La fibre optique :

En général, un câble à fibre optique comprend cinq éléments : le cœur, l'enveloppe, une gaine intermédiaire (plastique), un matériau de résistance (Kevlar) et une gaine externe.





- ***Le cœur*** constitue l'élément de transmission de la lumière au centre de la fibre optique.
- ***L'enveloppe*** qui entoure le cœur contient également de l'oxyde de silicium mais son indice de réfraction est moins élevé que celui du cœur.
- ***Une gaine intermédiaire*** qui entoure l'enveloppe. Elle protège le cœur et l'enveloppe contre tout dommage
- ***Le matériau de résistance*** entourant la gaine intermédiaire empêche le câble de fibre de s'étirer au cours des installations.
- ***La gaine externe*** Elle enveloppe la fibre pour la protéger contre l'abrasion, les solvants et autres contaminants.

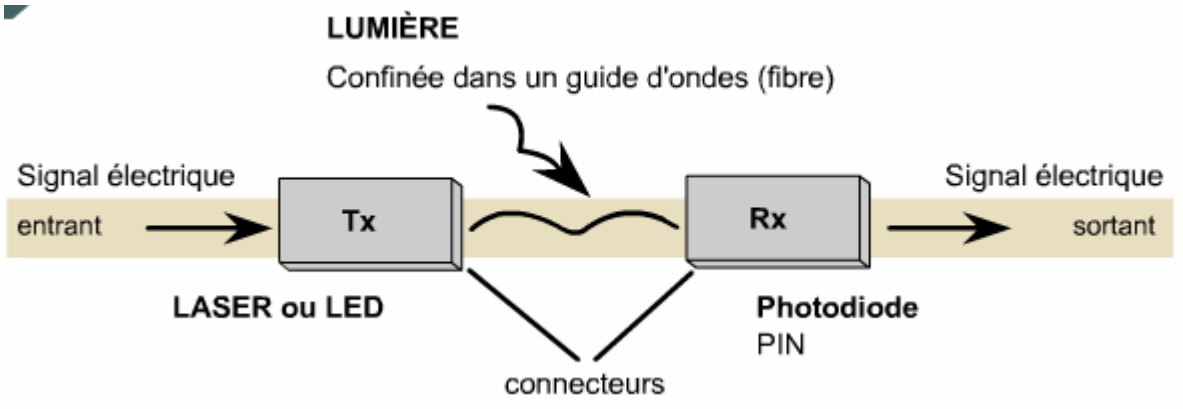
Chaque câble à fibre optique utilisé dans les réseaux comprend deux fibres de verre logées dans des enveloppes distinctes TX & RX, un brin de fibre pour la transmission et un autre pour la réception. Elles assurent ainsi une liaison de communication full duplex.

Il existe deux modèles de câble: le modèle à gaine intermédiaire flottante (loose-tube) et le modèle à gaine intermédiaire serrée (tight-buffered), le 2ème plus utilisé.

La différence entre les deux modèles réside principalement dans leur utilisation : le 1er est surtout utilisé à l'extérieur des bâtiments, alors que le 2ème est utilisé à l'intérieur des bâtiments.

Emetteurs-récepteurs

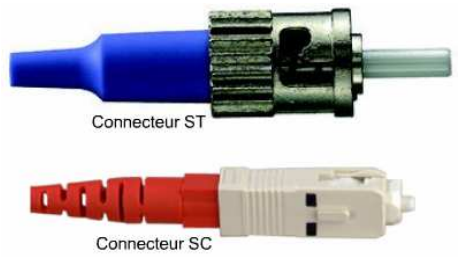
Les liaisons à fibre optique utilisent la lumière pour envoyer des données, il est nécessaire de convertir l'électricité en lumière à une extrémité de la fibre et de reconvertir la lumière en électricité à l'autre extrémité. C'est la raison pour laquelle un émetteur et un récepteur sont nécessaires.



Caractéristiques :

	Monomode	Multimode
Diamètre	62.5/125 ou 100/140 micron	50/125 ou 9/125 micron
Débit	**100+ Mbits/s**	
Facilité d'installation	**Difficile**	
Coût	**Elevé**	
Taille maximale	3000 m	2000 m
Connecteur	ST (*Straight Tip)*	SC *(Subscriber Connector)*
Faisceaux lumineux	Laser	LED
Couleur de la gaine externe	Jaune	Orange
Il est **insensible** aux interférences électromagnétiques et prend en charge des **débits** de données considérablement plus **élevés**, mais le verre dont il est constitué est très **fragile.**		

Avertissement : Le laser utilisé avec la fibre monomode génère une longueur d'onde visible. Le rayon laser est si puissant qu'il peut provoquer de graves lésions oculaires.



Signaux & Bruits dans la fibre optique :

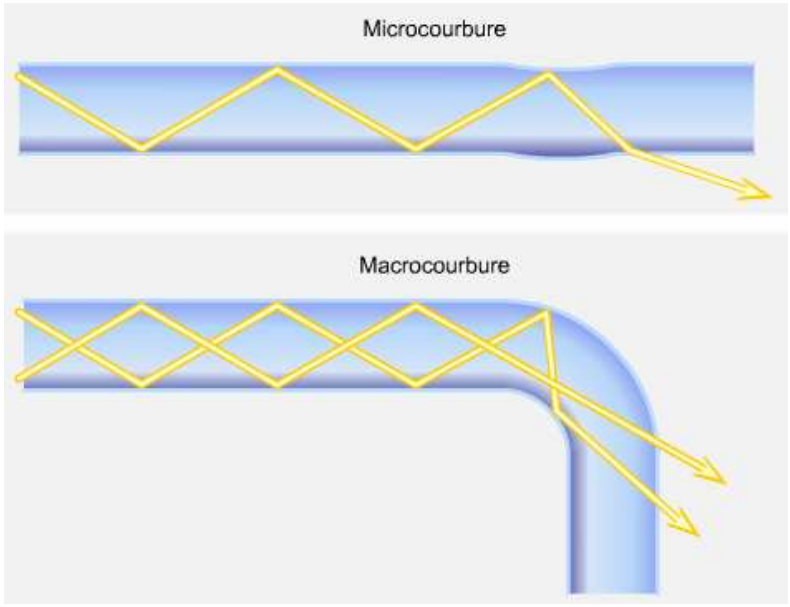
Les problèmes de diaphonie présents dans les câbles de cuivre n'existent pas dans les câbles optiques.

Lorsque la lumière circule dans la fibre, elle perd de son énergie. Plus la distance à parcourir est longue, plus la puissance du signal diminue (atténuation) :

Les facteurs d'atténuation :

- La dispersion de la lumière dans une fibre est provoquée par des inégalités microscopiques (*distorsions*) qui réfléchissent et dispersent l'énergie lumineuse.
- Lorsqu'un rayon lumineux entre en contact avec certaines impuretés dans une fibre, celles-ci absorbent une partie de l'énergie qui est convertie en une petite quantité d'énergie thermique, ce qui affaiblit le signal lumineux (*absorption*)
- Les *rugosités* ou les défauts de fabrication présents entre le cœur et l'enveloppe d'une fibre (les rayons perdent de leur puissance en raison de la réflexion interne totale).
- *La dispersion* d'un flash de lumière utilisé pour désigner la propagation des impulsions lumineuses qui circulent dans une fibre.
- *la dispersion chromatique* engendrée par la circulation de longueurs d'onde à des vitesses différentes dans le verre.
- *La saleté des connecteurs :* males et femelles.

Si la fibre est étirée ou trop courbée, la présence de minuscules craquelures provoquera la dispersion des rayons lumineux. Une fibre trop coudée peut modifier l'ange incident des rayons lumineux qui entrent en contact avec la limite cœur-enveloppe.



Un microscope ou un appareil de test doté d'une loupe permet d'examiner l'extrémité de la fibre et de vérifier qu'elle est correcte.

Les deux modèles de test de fibre optique les plus importants sont les appareils de *mesure de perte optique* et les *réflectomètres* (Optical Time Domain Reflectometer, OTDR).

Le décibel (dB) est l'unité de mesure de la perte de puissance. Il indique le pourcentage de puissance sortant de l'émetteur et entrant réellement dans le récepteur.

Les médias sans fil :

Normes des LAN sans fils :

L'***IEEE*** est le premier éditeur de normes en matière de réseaux sans fil. Ces normes ont été élaborées dans le cadre des réglementations instaurées par la FCC *(Federal Communications Commission)*.

→ Le DSSS *(Direct Sequence Spread Spectrum)* est une technologie clé contenue dans la norme **802.11** qui s'applique aux équipements sans fil fonctionnant dans la gamme des 1 à 2 Mbits/s.
→ La norme **802.11b** (Wi-Fi™) a été ensuite approuvée pour accroître la vitesse à 11 Mbits/s compatible avec la norme 802.11.
→ Les équipements **802.11a** réalisent un débit de données de 54 Mbits/s et peuvent atteindre 108 Mbits/s grâce à la technologie propriétaire qui permet de doubler le débit (incompatible avec la norme 802.11b).

→ Les équipements **802.11g** fournissent la même bande passante que les équipements 802.11a, mais avec une compatibilité en amont pour les équipements 802.11b utilisant la technologie de modulation OFDM (*Orthogonal Frequency Division Multiplexing*)

Equipements & topologies sans fil (WALN) :

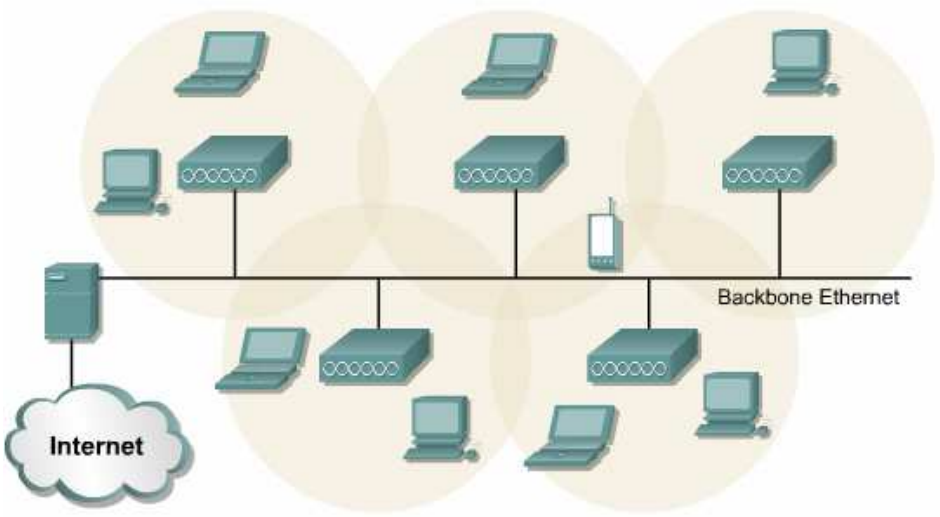
Il suffit de deux équipements pour créer un réseau sans fil.

Il est possible de créer un réseau sur mesure (*ad hoc*) avec des cartes réseau sans fil, comparable à un réseau câblé d'égal à égal (Problèmes d'incompatibilité des cartes NIC).

Pour résoudre le problème d'incompatibilité, un point d'accès est généralement installé pour servir de concentrateur central dans le mode infrastructure des LAN sans fil (*mode infrastructure*).

Les points d'accès sont équipés d'antennes et fournissent la connectivité sans fil sur une zone donnée appelée *cellule*.

La topologie cellulaire :



Le «roaming» entre les cellules

La puissance des antennes est généralement comprise entre 91,44 et 152,4 mètres.

Processus de connexion :

Lorsqu'un client est activé au sein du WLAN, il commence par écouter un équipement compatible auquel il est «associé». Cette «exploration» peut être active ou passive :

* *L'exploration active* entraîne l'envoi d'une demande de sonde de la part du nœud sans fil cherchant à joindre le réseau. Cette demande contient (SSID) du réseau qu'il souhaite joindre. Si un point d'accès ayant le même SSID est trouvé, il émet une réponse de sonde.

* *L'exploration passive* : les nœuds écoutent les trames de gestion Beacon transmises par le point d'accès (mode infrastructure) ou les nœuds d'égal à égal (mode ad hoc). Lorsqu'un nœud reçoit une trame Beacon contenant le SSID du réseau qu'il cherche à joindre, une tentative d'accès au réseau est effectuée.

Modes de communication des réseaux sans fil :

Il existe trois types de trame dans les réseaux sans fil : les trames *de contrôle*, *d'administration* et *de données*.

Seules les trames de données sont similaires aux trames 802.3. Les trames sans fil et 802.3 comportent 1 500 octets de données utiles.

Cependant, une trame Ethernet ne peut dépasser 1518 octets alors qu'une trame sans fil peut atteindre 2 346 octets. En général, la trame d'un LAN sans fil est limitée à 1 518 octets, car elle est connectée la plupart du temps à un réseau Ethernet câblé.

Trame d'administration
- Trame de demande d'association
- Trame de réponse d'association
- Trame de demande de sonde
- Trame de réponse de sonde
- Trame Beacon
- Trame d'authentification

Trames de contrôle
- Demande pour émettre (RTS)
- Prêt à émettre (CTS)
- Accusé de réception

Trames de données

Étant donné que la radiofréquence (RF) est un média partagé, il peut se produire des collisions, alors les LAN sans fil utilisent ***CSMA/CD***, ce qui provoque la perte de 50% de la bande passante initial.

Authentification & Association :

L'authentification des LAN sans fil a lieu au niveau de la *couche 2*. Il s'agit du processus d'authentification d'un équipement et non de l'utilisateur.

Types d'authentification et d'association

- *Non authentifié et non associé* →Le nœud est déconnecté du réseau et non associé à un point d'accès.
- *Authentifié et non associé* → Le nœud a été authentifié sur le réseau mais n'est pas encore associé au point d'accès.
- *Authentifié et associé* → Le nœud est connecté au réseau et peut transmettre et recevoir des données via le point d'accès.

Méthodes d'authentification :

→ Le premier est le système ouvert (open).un *SSID* suffit.

→ Le second processus est la clé partagée (shared key). Ce processus requiert l'utilisation du cryptage *WEP* (Wired Equivalent Privacy), un algorithme simple utilisant des clés de 64 et 128 bits.

Spectres des ondes radioélectriques et des micro-ondes

Les ordinateurs envoient des signaux de données par voie électronique et les émetteurs radio convertissent ces signaux électriques en ondes radioélectriques. La variation des courants électriques dans l'antenne d'un émetteur génère des ondes radioélectriques qui se propagent sous forme de lignes droites à partir de l'antenne.

Dans un émetteur, les signaux électriques en provenance d'un ordinateur ou d'un réseau local ne sont pas envoyés directement à l'antenne de l'émetteur, mais sont utilisés pour modifier un second signal puissant appelé signal porteur.

Le processus de modification du signal porteur entrant dans l'antenne de l'émetteur est appelé *modulation*. Un signal porteur radioélectrique peut être modulé dans trois cas principaux :

- Les stations de radio à modulation d'amplitude (AM) modulent la hauteur du signal porteur.
- Les stations de radio à modulation de fréquence (FM) modulent la fréquence du signal porteur
- Dans les LAN sans fil, un troisième type de modulation appelé modulation de phase permet de superposer le *signal de données* sur le *signal porteur* diffusé par l'émetteur.

Signaux et bruit dans les réseaux LAN sans fil

→ Les ondes radioélectriques peuvent être absorbées par certains matériaux et réfléchies par d'autres (murs).

→ La technologie Bluetooth™

→ Les téléphones sans fil opérant dans le spectre de 2,4 GHz

→ L'humidité, la foudre …

→ Le type d'antenne (puissance)

Sécurité des réseaux LAN sans fil :

Le manque de sécurité a toujours été un inconvénient pour les réseaux sans fil, depuis leur apparition.

- Échange EAP-MD5
- LEAP
- Authentification de l'utilisateur
- Cryptage
- Authentification des données

Un grand nombre de nouveaux protocoles et solutions de sécurité tels que les réseaux privés virtuels (*VPN*) et le protocole *EAP* (Extensible Authentication Protocol) sont désormais disponibles.

Avec le *protocole EAP*, le point d'accès ne fournit plus l'authentification au client, mais transmet les tâches à un équipement plus perfectionné, par exemple à un serveur réservé à cet effet.

Module 4

Test des câbles

Ondes :

Une onde est de l'énergie qui circule d'un endroit à l'autre (peuvent être comparées à des perturbations).

Les vagues de l'océan, comparables à des ondes, se définissent par leur hauteur, c'est-à-dire leur amplitude, mesurée en mètres. Elles peuvent également se définir selon la fréquence avec laquelle elles atteignent le rivage, à savoir leur période et leur fréquence.

- L'amplitude d'un signal électrique correspond toujours à la hauteur de l'onde.
- La période est le temps que met 1 cycle à se dérouler
- La fréquence est le nombre de cycles complets par seconde.

→ Une perturbation provoquée délibérément et impliquant une durée fixe et prévisible est appelée *impulsion*.

Les impulsions jouent un rôle important dans les signaux électriques. En effet, elles constituent la base de la transmission numérique.

Ondes sinusoïdales et ondes carrées :

Sinusoïdale	Carrée
Périodique	Périodique
Varie continuellement	ne varient pas avec le temps
Se répètent naturellement et changent à intervalles de temps réguliers.	Sautillant
Exemple d'onde analogique	Exemple d'onde numérique ou impulsion

Calcul des logarithmes et décibels :

Log (10^{9}) = **9**. Il est possible de calculer le logarithme de nombres qui ne sont pas des puissances de 10. Il n'est pas possible de calculer le logarithme d'un nombre négatif.

Le décibel (dB) est une unité de mesure utilisée pour décrire des signaux réseau.

Deux formules servent à calculer les décibels :

dB = 10 log10 (Pfinal / Préf) Puissance

dB = 20 log10 (Vfinal / Vréf) Tension

La première formule est souvent utilisée pour mesurer les ondes lumineuses dans les fibres optiques ainsi que les ondes radioélectriques dans l'air, tandis que la seconde est utilisée pour mesurer les ondes électromagnétiques dans les câbles de cuivre

dB représente la perte ou le gain de puissance d'une onde. Les décibels peuvent être des valeurs *négatives*, ce qui correspond à une perte de puissance dans la propagation d'une onde, ou des valeurs *positives*, ce qui correspond à un gain de puissance, c'est-à-dire à une amplification du signal.

Temps et fréquence des signaux :

L'analyse des signaux à l'aide d'un oscilloscope s'appelle une *analyse* dans le *domaine temporel*. L'axe des abscisses, ou domaine de la fonction mathématique, représente le temps.

Il faut également *l'analyse* dans le *domaine de fréquence*. Pour cette analyse, l'axe des abscisses représente la fréquence. Un équipement électronique, appelé analyseur de spectre, permet de créer des graphiques pour l'analyse dans le domaine de fréquence.

Signaux analogiques & numériques :

Synthèse de Fourier d'une onde carrée :

Une onde carrée est le résultat de la superposition de plusieurs ondes sinusoïdales.

Bruit dans le temps et la fréquence :

Le bruit est un ajout indésirable à un signal, il peut provenir de sources naturelles ou technologiques.

Les sources de bruit sont très nombreuses :

- Câbles proches acheminant des signaux de données.
- Interférences radioélectriques provenant de signaux tiers proches.
- Interférences électromagnétiques provenant d'une source proche telle qu'un moteur ou une ampoule électrique.
- Bruit de laser à l'émission ou la réception d'un signal optique.

Types de bruit :

- *Un bruit blanc* : Un bruit qui affecte toutes les fréquences de transmission de la même façon.
- *Interférence à bande étroite* : Le bruit n'affectant qu'une petite gamme de fréquences.

Bande passante :

Deux sortes de bandes passantes sont importantes pour l'étude d'un LAN : la *bande passante analogique* et la *bande passante numérique*.

La bande passante analogique permet de décrire la plage de fréquences émises par une station de radio ou un amplificateur électronique (Hz).

La bande passante numérique mesure la quantité de données pouvant circuler d'un endroit à un autre pendant une période donnée.

Signaux transitant par des câbles en cuivre et à fibre optique :

Les niveaux de tension sont mesurés pour l'émetteur et le récepteur à partir d'un niveau de référence de 0 volt. Ce niveau de référence est appelé *terre de signalisation*.

Le blindage dans les câbles de cuivre joue un rôle important pour réduire le bruit et les interférences externes.

Le bruit électrique n'affecte pas les signaux optiques. De plus, il n'est pas nécessaire de mettre la fibre optique à la terre

Atténuation et affaiblissement d'insertion sur un média cuivre :

L'atténuation est la baisse d'amplitude du signal le long d'une liaison. Des câbles longs et des fréquences de signaux élevées contribuent à augmenter l'atténuation.

C'est pourquoi l'atténuation se mesure à l'aide d'un testeur de câble réglé sur les fréquences les plus élevées que les câbles peuvent supporter. L'atténuation est exprimée en décibels (dB) par des nombres *négatifs*. Plus la valeur négative en décibels est petite, plus la performance de la liaison est bonne.

Facteurs provoquant l'atténuation :

- La résistance du câble en cuivre convertit une partie de l'énergie électrique du signal en chaleur.
- Discontinuité d'impédance provoquée par des connecteurs défectueux ou mal installés.

Connecteurs mal installés → Discontinuité → une partie du signal réfléchie (écho) → un effet d'échos multiples frappent le récepteur à différents intervalles de temps → gigue.

L'atténuation du signal + discontinuités d'impédance = *affaiblissement d'insertion*.

La diaphonie :

La diaphonie est la transmission des signaux d'un fil à un autre fil proche.

La diaphonie est plus néfaste sur des fréquences de transmission élevées.

Les appareils de test des câbles mesurent la diaphonie en appliquant un signal test à l'une des paires. Le testeur de câble mesure ensuite l'amplitude des signaux de la diaphonie indésirable sur les autres paires de fils du câble.

Les câbles UTP des catégories supérieures sont dotés de paires aux torsades plus nombreuses afin de réduire la diaphonie pour les fréquences de transmission élevées.

Lorsque les connecteurs sont raccordés aux extrémités de câbles UTP, les paires de fils doivent être détorsadées le moins possible afin d'assurer des communications fiables.

Types de diaphonie :

- *Diaphonie locale (NEXT)*

Calculée selon le rapport d'amplitude entre le signal test et le signal de diaphonie mesurés à la même extrémité de la liaison. La diaphonie locale doit être mesurée entre chaque paire et chacune des autres paires dans une liaison UTP, ainsi qu'à chacune de ses extrémités.

- *Diaphonie distante (FEXT)*

Une diaphonie intervenant à un point éloigné de l'émetteur crée moins de bruit sur un câble qu'une diaphonie locale

- *Diaphonie locale totale (PSNEXT)*

L'effet cumulé d'une diaphonie locale provenant de toutes les paires d'un câble. Pour chaque paire, la diaphonie locale totale se calcule selon les effets de diaphonie locale des trois autres paires.

Normes de test des câbles :

La norme TIA/EIA-568-B préconise dix tests à faire passer à un câble de cuivre :

- le schéma de câblage
- l'affaiblissement d'insertion
- la diaphonie locale (NEXT)
- la diaphonie locale totale (PSNEXT)
- la diaphonie distante de niveau égal (ELFEXT)
- la diaphonie distante totale de niveau égal (PSELFEXT)
- la perte de retour

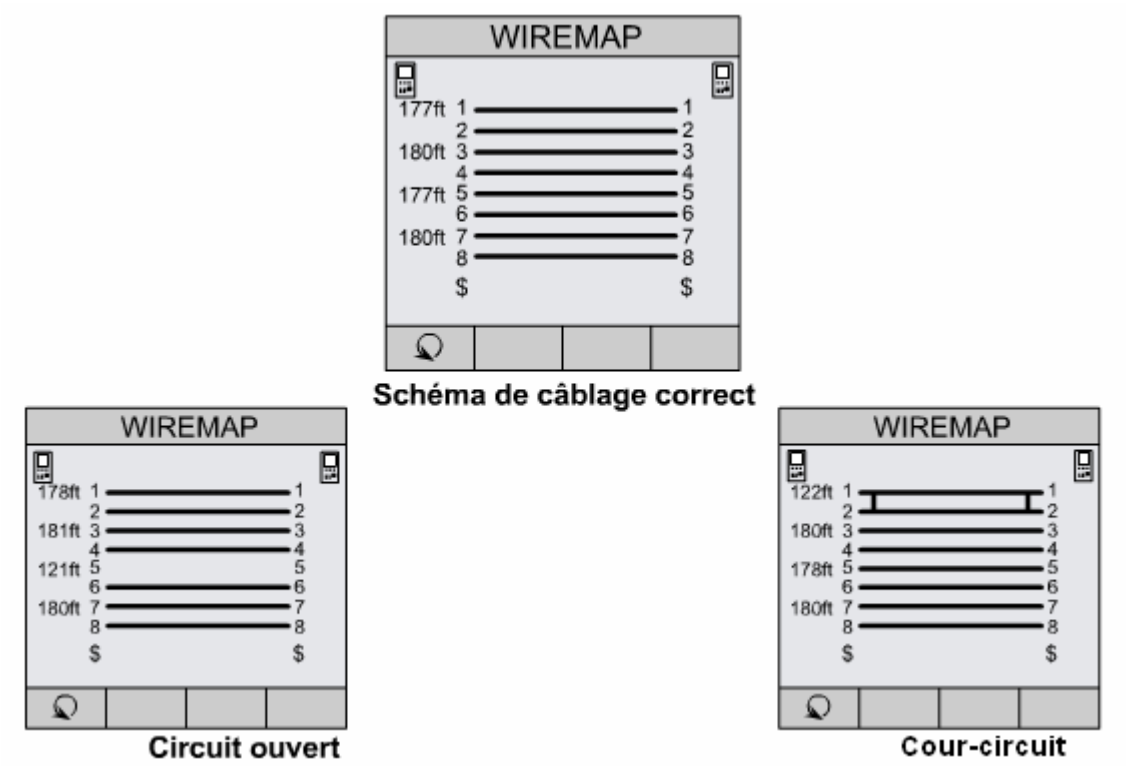
- le délai de propagation
- la longueur de câble
- la distorsion du délai

Remarque :

Bien que les tests de la catégorie 6 soient pour l'essentiel les mêmes que ceux de la catégorie 5, les câbles de catégorie 6 doivent obtenir des résultats supérieurs afin d'obtenir la certification

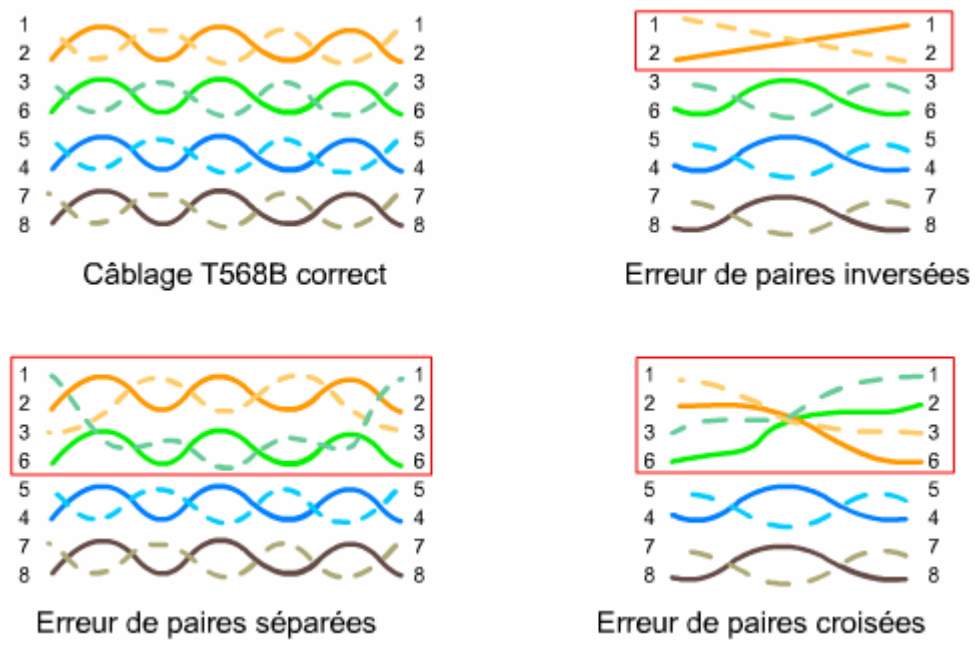
Le test de schéma de câblage garantit qu'il n'y a aucun circuit ouvert ou court-circuit :

- *Un circuit est ouvert* lorsque le fil n'est pas correctement raccordé au connecteur.
- *Un court-circuit* se produit lorsque deux fils sont connectés entre eux.



Il existe différentes erreurs de câblage que le test de schéma de câblage est capable de détecter :
→ *Les erreurs de paires inversées* se produisent lorsqu'une paire est correctement installée sur l'un des connecteurs mais inversée sur l'autre.

→ *Les erreurs de paires séparées* se produisent lorsque l'un des fils d'une paire est commuté avec un fil d'une autre paire aux deux extrémités du câble.



La distorsion :

La différence de délai entre les paires est appelée distorsion de délai. Si la distorsion de délai entre les paires est trop grande, les bits n'arrivent pas en même temps et les données ne peuvent pas être correctement reconstituées.

La fibre optique :

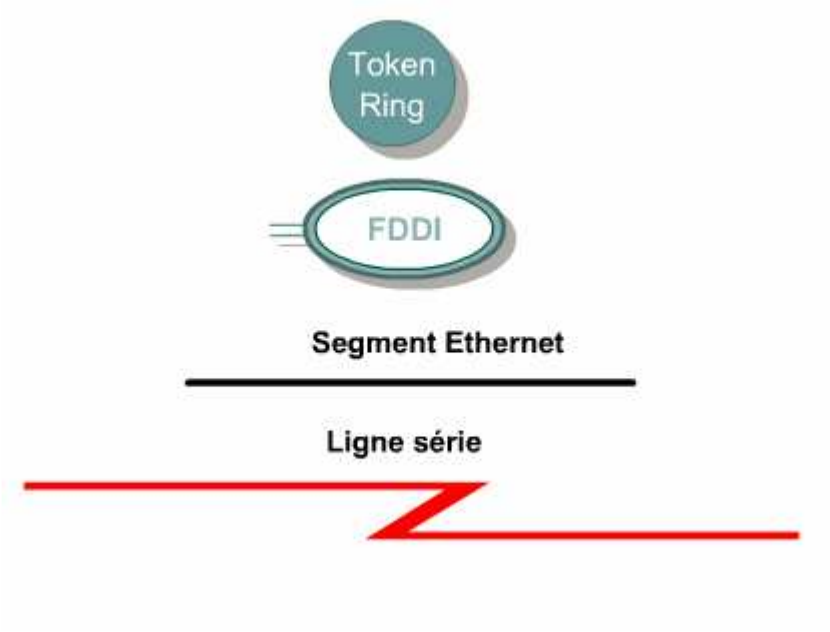
Les câbles à fibre optique ne sont pas sensible des interférences électromagnétiques ou le bruit à l'extérieur ou la diaphonie. Néanmoins, ils sont sensibles à l'atténuation, mais dans une moindre mesure que les câbles en cuivre.

Module 5

Câblage des réseaux LAN & WAN

Médias :

Un média permet d'acheminer un flux d'informations via un réseau. Différents symboles sont utilisés pour représenter les types de média :



Chaque type de média présente des avantages et des inconvénients, basés sur les facteurs :

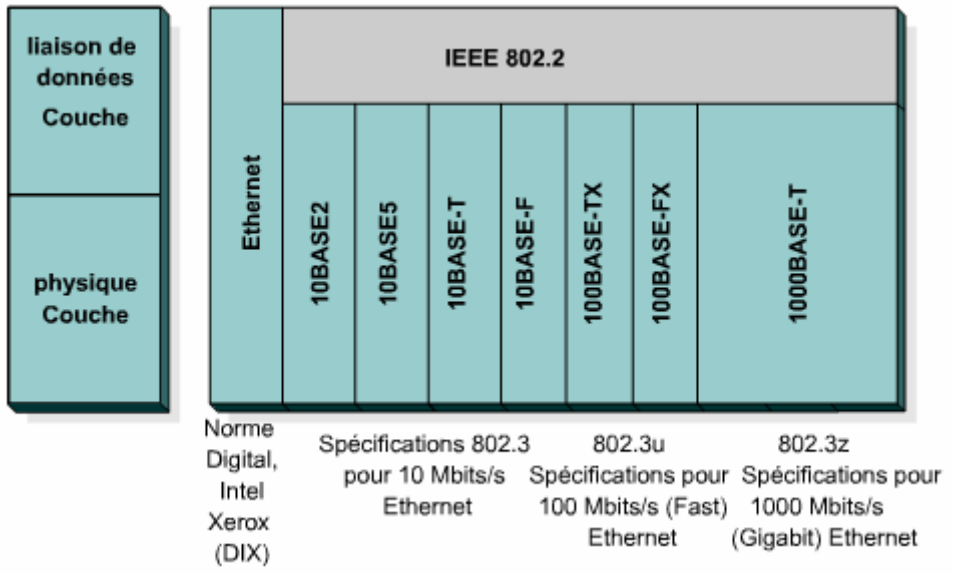
- La longueur de câble
- Le coût
- La facilité d'installation
- La sensibilité aux interférences

Ethernet :

Le groupe *DIX* (*Digital, Intel et Xerox*) a été le premier qui a créé la spécification LAN Ethernet, qui a servi de base à l'élaboration de la norme 802.3 de l'IEEE (*Institute of Electrical and Electronics Engineers*) introduite en 1980.

L'IEEE a étendu la norme 802.3 à trois nouveaux comités :

- *802.3u* pour Fast Ethernet
- *802.3z* pour Gigabit Ethernet sur fibre optique
- *802.3ab* pour Gigabit Ethernet sur câble UTP.



Les technologies Ethernet peuvent être utilisées de différentes façons dans un réseau :

Par exemple :

- Ethernet de 10 Mbits/s au niveau des utilisateurs
- Ethernet de 100 Mbits/s pour les utilisateurs importants.
- Fast Ethernet pour la liaison entre les équipements utilisateur et réseau.
- Fast Ethernet pour relier des serveurs d'entreprise.
- Fast Ethernet ou Gigabit Ethernet pour relier les équipements du backbone.

Médias et connecteurs Ethernet :

	10Base2	10Base5	10BaseT	10BaseTX	100BaseFX	1000BaseCX	1000BaseT	1000BaseSX	1000BaseLX
Média	Coaxial fin 50Ω	Coaxial épais 50Ω	UTP cat 3,4 et 5	UTP cat 5	Fibre multimode 62.5/125	STP	UTP cat 5	Fibre multimode 62.5/50	Fibre multimode 62.5/50 -- monomode 9
Longueur Maximale	185m	500m	100m	100m	400m	25m	100m	550m	550m de 3 à 10Km
Topologie	bus	bus	étoile	étoile	étoile	étoile	étoile	étoile	étoile
Connecteur	BNC	AUI	RJ45	RJ45	ST ou SC	RJ45	RJ45	SC	SC

En règle générale, un *émetteur-récepteur* convertit un connecteur AUI (*Attachment Unit Interface*) en connecteur de type RJ-45, câble coaxial ou fibre optique.

Mise en œuvre d'UTP :

Connecteur RJ45 :

La norme EIA/TIA spécifie un connecteur RJ-45 pour câble UTP :

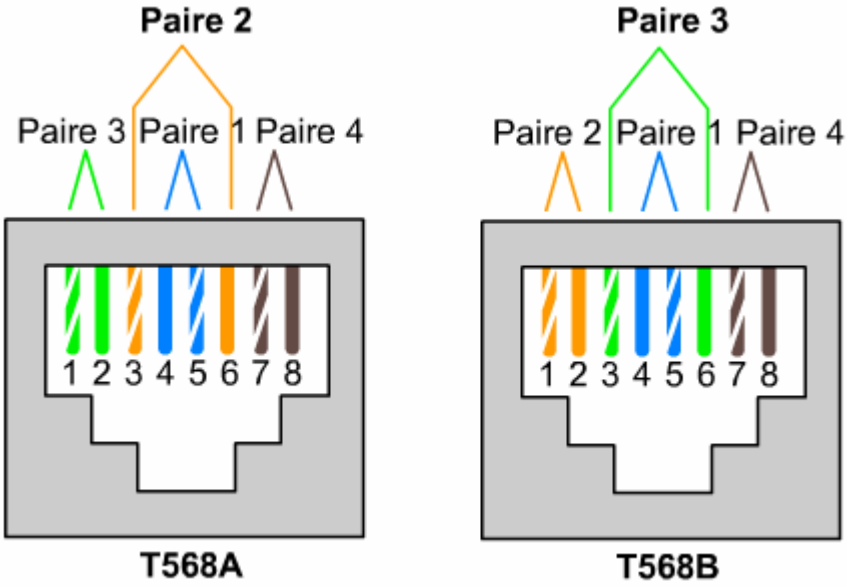
- RJ correspond : Registered Jack
- 45 : un ordre de connexion des fils spécifique.

Le connecteur RJ-45 comporte huit fils de couleur.

- Quatre de ces fils (T1 à T4), appelés «tips», acheminent la tension.
- Quatre autres fils (R1 à R4), appelés «rings», sont mis à la terre.

T1 R1 T2 R2 T3 R3 T4 R4

Pour que l'électricité circule entre le connecteur et la prise, l'ordre des fils doit respecter le code de couleurs T568A ou T568B de la norme *EIA/TIA-568-B.1*



Types de câbles :

Câble de raccordement Droit : Servir à connecter :

- PC → Prise murale
- Tableau de connexions → concentrateur / commutateur.
- PC → concentrateur / commutateur. (Directement)

Norme A	Norme B
Norme A	Norme B

Câble console à paires inversées (console) : Servir à relier :

- PC → Port console d'un routeur / commutateur.

Norme A	Norme B
A inversés	B inversés

Câble de raccordement Croisé: Servir à connecter :

- Concentrateur → Concentrateur
- Commutateur → Commutateur
- Commutateur → Concentrateur
- PC → PC
- Routeur → Routeur
- Routeur → PC

Norme A	Norme B
Norme B	Norme A

Répéteurs :

Les répéteurs sont des équipements de couche 1 qui permettent de régénérer et renforcer les signaux envoyés sur de longues distances.

Les normes Ethernet et IEEE 802.3 mettent en œuvre la règle 5-4-3 relative au nombre de répéteurs et de segments sur les backbones Ethernet à accès partagé dans une topologie arborescente.

La règle 5-4-3 divise le réseau en deux types de segments physiques : les segments (*utilisateur*) avec stations de travail et les segments (*de liaison*) sans stations de travail.

La règle stipule :

5 : segments maximum
4 : répéteurs maximum
3 : segments utilisateurs maximum

La règle étant conçue pour limiter les temps de transmission des signaux. (Laps de temps ajouté à travers chaque répéteur).

Concentrateurs :

Les concentrateurs (Hub) sont, en fait, des répéteurs multiports (entre 4 et 24 ports).

Chaque donnée qui arrive sur le port d'un concentrateur par l'intermédiaire des câbles est électriquement répétée sur tous les autres ports connectés au segment de réseau.

Types de concentrateurs :

- *Passif*: permet uniquement de partager le média physique. Il n'a besoin d'aucune alimentation électrique.
- *Actif*: un concentrateur actif doit être branché à une prise de courant pour pouvoir amplifier un signal avant de l'envoyer aux autres ports.
- *Intelligent*: «smart hubs» fonctionnent de la même façon que les concentrateurs actifs, avec des puces microprocesseurs et des fonctions de diagnostic.

Les technologies sans fil :

Les réseaux sans fil utilisent *la radiofréquence* (*RF*), des *rayons laser*, des ondes *infrarouges* (*IR*), un *satellite* ou des *micro-ondes* pour transporter les signaux entre les ordinateurs sans connexion de câble permanente.

→ Les technologies sans fil IR et RF sont les plus répandues dans le domaine des réseaux.

La technologie ***IR*** présente toutefois des points faibles :

- l'émetteur doit disposer d'une visibilité directe des stations de travail
- les signaux de données peuvent être affaiblis ou masqués par les personnes qui traversent la pièce ou par l'humidité ambiante.

La technologie ***RF*** permet de placer les équipements dans des pièces ou des bâtiments distincts. La plage limitée de signaux radio restreint l'utilisation de ce type de réseau.

La mise en œuvre de l'étalement du spectre pour les transmissions WLAN peut s'effectuer selon l'approche :

- *FHSS* (Frequency Hopping Spread Spectrum) « à sauts de fréquence »
- ou *DSSS* (Direct Sequence Spread Spectrum) « en séquence directe »

Ponts :

Avantage : la diminution du trafic tout en permettant d'étendre la zone géographique.

Un pont doit prendre des décisions intelligentes quant à la transmission des informations :

- Si l'équipement de destination se trouve sur le même segment que la trame, le pont n'envoie pas la trame vers d'autres segments. «*filtrage*».
- Si l'équipement de destination se trouve sur un autre segment, le pont transmet la trame au segment approprié.
- Si le pont ne connaît pas l'adresse de destination, il transmet la trame à tous les segments, excepté à celui par lequel la trame a été reçue. «*diffusion*».

Commutateurs :

Les commutateurs sont parfois qualifiés de «ponts multiports».

La commutation est une technologie qui permet d'atténuer la congestion dans les LAN Ethernet en réduisant le trafic et en augmentant la bande passante.

Une unité de commutation exécute deux fonctions de base :

- la première est *la commutation des trames de données* : recevoir les données et les transmettre.
- La seconde est *la gestion des fonctions de commutation* : créer et gérer des tables de commutation et rechercher des boucles.

Environnement d'égal à égal & client / serveur :

Avantages d'un réseau d'égal à égal	Avantages d'un Réseau client-serveur
Implémentation moins coûteuse	Meilleure sécurité
Ne demande pas d'autre logiciel spécialisé dans l'administration réseau	Plus facile à administrer lorsque le réseau est important car l'administration est centralisée.
Ne demande pas d'administrateur réseau dédié.	Possibilité de sauvegarde de toutes les données dans un emplacement central.

Inconvénients d'un réseau d'égal à égal	Inconvénients d'un réseau client-serveur
Ne s'adapte pas bien aux réseaux importants et complexité de l'administration.	Nécessite un logiciel coûteux, spécialisé pour l'exploitation et l'administration du réseau
Chaque utilisateur doit être formé aux tâches d'administration.	Le serveur nécessite du matériel plus puissant, mais coûteux.
Moins sécurisé	Requires a professional administrator.
Toutes les machines partageant les ressources diminuent les performances	Présente un point de défaillance unique. Indisponibilité des données utilisateur en cas d'arrêt du serveur.

Le réseau d'égal à égal fonctionne bien avec dix ordinateurs au plus.

La couche physique des réseaux WAN :

Les mises en œuvre de couche physique différent selon la distance de l'équipement par rapport à chaque service, la vitesse et le type de service.

Les services WAN sont pris en charge via des connexions série du type lignes louées spécialisées exécutant *PPP* ou *Frame Relay*.

La technologie ***RNIS*** propose l'établissement de connexions à la demande et des services d'appel de secours par l'infrastructure commutée.

Une interface RNIS BRI (*Basic Rate Interface*) se compose de deux canaux Bearer (canaux B) de 64 kbits/s pour les données et d'un canal delta (canal D) de 16 kbits/s utilisé pour la signalisation et d'autres tâches de gestion des liaisons. Le protocole PPP est généralement utilisé pour transporter des données via les canaux B.

Routeurs et connexions série :

Les routeurs sont responsables du routage des paquets de données de la source à la destination au niveau du LAN, ainsi que de la connectivité au WAN.

Il convient de déterminer les connecteurs à utiliser (ETTD ou ETCD) :

→ *L'ETTD* est l'extrémité de l'équipement d'un utilisateur au niveau de la liaison WAN.
→ *L'ETCD* est le point de la diffusion des données reportée sur le fournisseur de services.

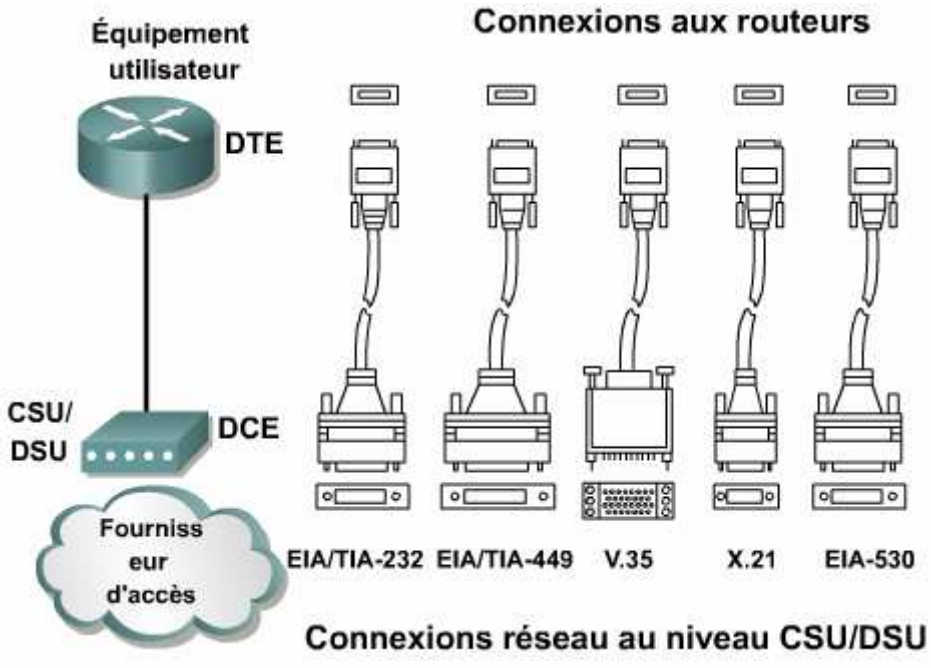
Lorsque vous vous connectez directement à un fournisseur de services ou à un équipement tel qu'une unité CSU/DSU (*channel service unit/data service unit*) qui doit exécuter le signal de synchronisation, le *routeur* constitue un équipement *ETTD* et doit être équipé d'un câble série du même type.

Lorsque vous exécutez un scénario avec des routeurs dos à dos dans un environnement de test, l'un des routeurs est un équipement ETTD et l'autre un équipement ETCD.

Sur les routeurs équipés de ports série modulaires, la dénomination des interfaces est la suivante : «type de port numéro d'emplacement/numéro de port».

Par exemple : serial 1/0

Pour un routeur Cisco, la connectivité physique sur le site du client est mise en œuvre par le biais d'un ou *deux types de connexions série*. Le premier type est un connecteur 60 broches et le second un connecteur « série intelligent » plus compact. Le connecteur du fournisseur peut varier selon le type d'équipement de service.

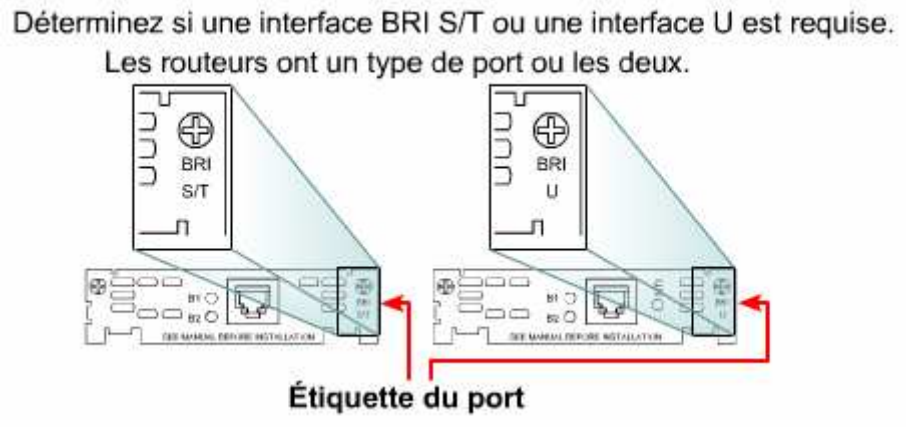


Routeurs et connexions RNIS BRI :

Une connexion RNIS BRI peut faire appel à 2 types d'interfaces: *BRI S/T* et *BRI U*. Pour déterminer le type d'interface à utiliser, il convient de savoir qui fournit l'équipement de terminaison de réseau 1 (*NT1*).

Le NT1 :

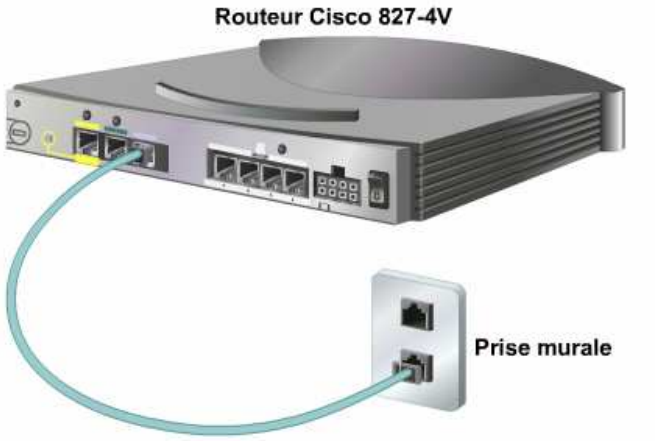
Un *équipement intermédiaire*, situé entre le routeur et le commutateur RNIS de l'opérateur télécom. Cet équipement permet de relier le câblage à quatre fils de l'abonné à la boucle locale traditionnelle à deux fils.



Pour relier le port RNIS BRI à l'équipement de l'opérateur télécom, utilisez un *câble droit* UTP de catégorie 5.

Routeurs et connexions DSL :

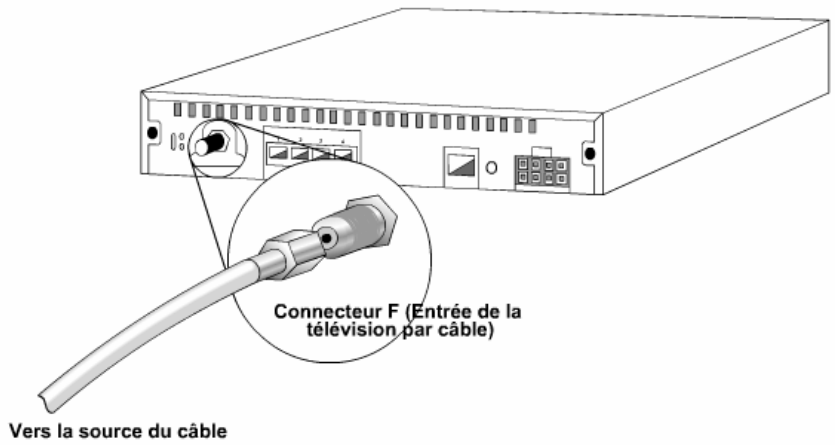
Par exemple : le routeur ADSL Cisco 827 équipé de l'interface ADSL.



On utilise la ligne téléphonique à l'aide d'un connecteur RJ11.

Routeurs et connexions par câble :

Par exemple : le routeur Cisco uBR905.



Le routeur d'accès au câble Cisco uBR905 offre un accès réseau haut débit via la télédiffusion par câble. Le modèle uBR905 comporte une interface câble coaxial, ou connecteur F, qui se raccorde directement au système de câblage (connecteur BNC).

Ne dépasser pas *6 tours* pour maintenir le connecteur BNC.

Configuration des connexions console :

Le port console permet de surveiller et de configurer un concentrateur, un commutateur ou un routeur Cisco avec un câble à paires inversées.

Vous devrez peut-être installer un adaptateur RJ-45 à DB-9 ou RJ-45 à DB-25 pour le PC ou le terminal. Puis, configurez l'application d'émulation du terminal à l'aide des ***paramètres de port COM*** suivants: 9600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.

Le port AUX fournit une gestion hors bande via un modem. Pour pouvoir l'utiliser, vous devez le configurer par le biais du port console. Le port AUX utilise également les mêmes paramètres.

Module 6

Notions de base Ethernet

Introduction à Ethernet :

Le succès d'Ethernet est dû aux facteurs suivants :

- Simplicité et facilité de maintenance
- Capacité à incorporer de nouvelles technologies
- Fiabilité
- Faible coût d'installation et de mise à niveau

À l'origine, l'idée était de permettre à deux hôtes au moins d'utiliser le même média sans aucune interférence entre les signaux.

Le problème d'accès multiple de l'utilisateur à un média partagé a été étudié au début des années 70 à l'Université d'Hawaï (cette étude constitué la base de la méthode *CSMA/CD*)

La première norme Ethernet a été publiée en tant que norme ouverte en 1980 par un consortium de Digital Equipment Company, Intel et Xerox (***DIX***).

En 1985, l'IEEE a modifié la norme Ethernet pour produire la norme 802.3 *compatible* avec les normes ISO.

➔ Pour l'essentiel, les normes Ethernet et IEEE 802.3 sont *identiques*.

En 1995, l'IEEE annonça une norme pour un Ethernet à **100 Mbits/s**. Vinrent ensuite des normes pour **Gigabit** Ethernet en 1998 et 1999.

Alors, Ethernet n'est pas une technologie de réseau unique mais une famille de technologies (le format de la trame reste la même sur toutes les familles Ethernet).

Avantages :

- La BP du réseau pourrait être augmentée plusieurs fois sans entraîner de modification de la technologie Ethernet.
- Toutes les normes sont compatibles avec la norme Ethernet originale.

Chaque fois qu'Ethernet doit être étendu pour ajouter un nouveau média ou une nouvelle capacité, l'IEEE publie un nouveau supplément à la norme 802.3 (p.e : 802.3z).

Ethernet repose sur la signalisation de bande de base. (*BASE*) tandis que la signalisation à large bande est obsolète (p.e : 10Broad36)

Politique de l'IEEE :

- Fournir les informations pour construire des équipements conformes aux normes.
- Promouvoir l'innovation auprès des fabricants

Normes IEEE :

802.7	BBTAG (BroadBand Technical Adv. Group (BBTAG)
802.16	BBWA (Broadband Wireless Access (BBWA)
802.14	Réseau de communication à large bande basé sur le câble de télévision
802.3	CSMA/CD
802.12	Demande de priorité
802.8	FOTAG (Fiber Optics Technical Adv. Group (FOTAG)
802.1	Norme HILI (High Level Interface)
802.9	ISLAN (Integrated Services LAN)
802.2	LLC (contrôle de liaison logique).
802.6	Réseau métropolitain (MAN)
802.17	RPRSG (Resilient Packet Ring Group)
802.0	SEC - Normes IEEE pour les réseaux locaux (LAN) et métropolitains (MAN) : Vue d'ensemble et architecture
802.10	SILS (Standard for Interoperable LAN Security)
802.4	Bus à jeton
802.5	Token Ring
802.11	LAN sans fil (WLAN)
802.15	Réseau personnel (PAN) sans fil

Ethernet & le modèle OSI :

Ethernet opère dans la couche physique et la sous couche MAC de la couche LDD. (OSI)

- Un répéteur transmet le trafic à tous les autres ports. Il n'envoie jamais de trafic par le port qui a servi à le recevoir.
- Toutes les stations du même domaine de collision voient le trafic passant par un répéteur.
- Si le signal subit une dégradation due à l'atténuation ou au bruit, le répéteur tentera de reconstruire et de régénérer le signal.

Afin de garantir une BP et une opérabilité minimales, les normes spécifient :

→ Le nombre maximum de stations par segment
→ La longueur maximum de segments
→ Le nombre maximum de répéteurs entre stations.

- Les stations séparées par des répéteurs se trouvent à l'intérieur du même ***domaine de collision***. Les stations séparées par des ponts ou des routeurs se trouvent dans des domaines de collision différents.

- La sous-couche LLC (*Logical Link Control*) reste relativement indépendante de l'équipement physique qui sera utilisé pour le processus de communication.

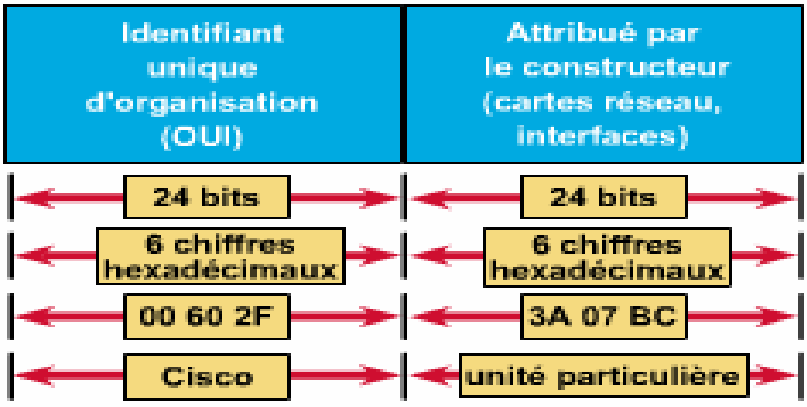
La sous-couche LLC prend un paquet IP, et y ajoute des *informations de contrôle* pour faciliter l'acheminement de ce paquet jusqu'au nœud de destination.

Les adresses MAC :

L'adresse MAC est une adresse matérielle stockée sur une mémoire morte (ROM) de la carte réseau comportent 48 bits et sont exprimées à l'aide de douze chiffres hexadécimaux.

→ Les six premiers chiffres hexadécimaux, identifient le fabricant ou le fournisseur et constituent donc l'*identifiant unique d'organisation* (*OUI - Organizational Unique Identifier*).

→ Les six autres chiffres hexadécimaux forment le numéro de série d'interface administrée par le fournisseur.



Exemple : 0000.0c12.3456 OU 00-00-0c-12-34-56

La carte réseau utilise l'adresse MAC afin de déterminer la destination. Elle n'utilise pas de temps processeur pour effectuer cette évaluation, ce qui améliore les temps de communication sur le réseau Ethernet.

Tous les équipements qui sont connectés à un réseau local Ethernet possèdent des interfaces adressées MAC (sert à l'identification dans un LAN).

Verrouillage de trame de couche 2 :

Le verrouillage de trame (*le processus d'encapsulation de la couche 2*) permet de récupérer des informations essentielles qu'il n'était pas possible d'obtenir uniquement avec les trains binaires codés. Ces informations sont les suivantes:

- Quels sont les ordinateurs en communication?
- Quand commence la communication entre des ordinateurs et quand se termine-t-elle?
- Quelles erreurs se sont produites lors de la communication entre les ordinateurs?
- Quel sera le prochain ordinateur à communiquer?

La structure des trames :

Les schémas de structure de trame font apparaître différents regroupements de bits (ou champs), qui remplissent des fonctions bien précises.

Il existe des champs se trouvant sur toutes les technologies :

- Champs de début et de fin de trame.
- Champs des adresses sources et destination.

La plupart des trames contiennent des champs spécialisés de plus, par exemple :

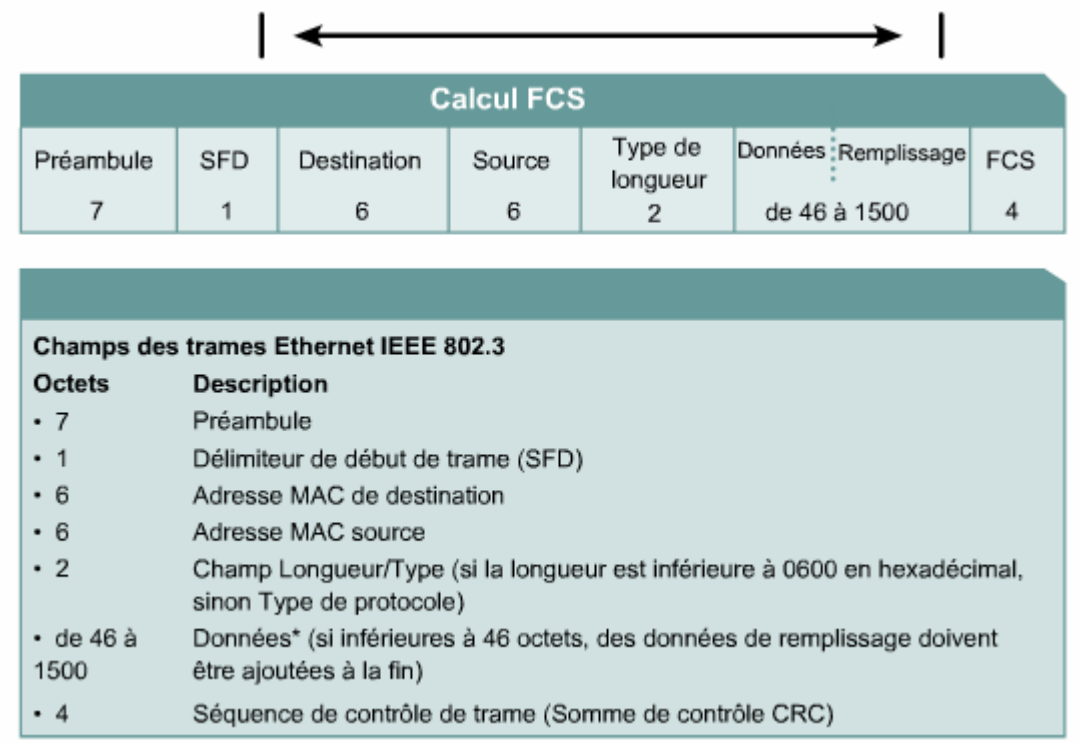
- Un champ type
- Un champ de longueur
- Un champ FCS
- …

Il y a trois façons de calculer le numéro de séquence de contrôle de trame:

- *Code de redondance cyclique (CRC)* – exécution des calculs sur les données.
- *Parité bidimensionnelle* – place des octets individuels dans une matrice bidirectionnelle et effectue des contrôles de redondance verticalement et horizontalement sur la matrice, ce qui crée ainsi un octet supplémentaire produisant un nombre pair ou impair de 1 binaires.
- *Somme de contrôle Internet* – somme résultant de l'addition des valeurs de tous les bits de données.

Structure de trame Ethernet :

Rappel : Sur la couche liaison de donnée, la structure de trame est pratiquement identique pour toutes les vitesses d'Ethernet, de 10 Mbits/s à 10 000 Mbits/s.



Champs des trames Ethernet IEEE 802.3

Octets	Description
• 7	Préambule
• 1	Délimiteur de début de trame (SFD)
• 6	Adresse MAC de destination
• 6	Adresse MAC source
• 2	Champ Longueur/Type (si la longueur est inférieure à 0600 en hexadécimal, sinon Type de protocole)
• de 46 à 1500	Données* (si inférieures à 46 octets, des données de remplissage doivent être ajoutées à la fin)
• 4	Séquence de contrôle de trame (Somme de contrôle CRC)

Dans la version Ethernet qui a été développée par DIX avant l'adoption de la version IEEE 802.3, le ***préambule*** et le délimiteur de début de trame (SOF) ont été combinés en un champ unique (8 Octets).

Le champ de ***longueur/type*** comportait uniquement la longueur dans les premières versions d'IEEE et uniquement le type dans la version DIX.

Fonctions de chaque champ :

-*Préambule* : permet la synchronisation dans les réseaux 10Mbits/s et moins.

-*Délimiteur de début* : indique l'arrivée d'une trame (10101011).

-*Champs d'adresses* : indique l'origine et la destination de la trame (MAC).

-*Le champ de longueur/type* : peut être utilisé de deux façons. Si la valeur est inférieure à 1536 (décimale), soit 0x600 (hexadécimale), alors elle indique la longueur. La longueur indique le nombre d'octets de données qui suit ce champ.

-*Le champ de données* : entre 64 et 1518, lorsqu'il n'y a pas suffisamment de données utilisateur pour que la trame ait la longueur minimale, des données supplémentaires sont appelées données de remplissage s'interposent.

-*FCS* : Dans ce champ, la station source indique une valeur calculée du contenu de la trame. La station de destination recalcule la valeur afin de déterminer si la trame a été endommagée pendant le transport.

Protocoles MAC déterministes et non déterministes :

Il y a deux grandes catégories de protocole MAC :

→ Token Ring et FDDI sont des exemples de *protocoles déterministes*. Dans un réseau Token Ring, les hôtes sont disposés en anneau et un jeton de données spécial circule d'un hôte à l'autre autour de l'anneau. Lorsqu'un ordinateur hôte désire émettre des données, il saisit le jeton, émet les données pendant un temps limité, puis transmet le jeton à l'hôte suivant sur l'anneau.

→ Les protocoles MAC *non déterministes* font appel à la méthode dite du " premier arrivé, premier servi ". Le système CSMA/CD (Carrier Sense Multiple Access with Collision Detection) est simple. La carte réseau guette l'absence de signal sur le média, puis commence à transmettre. Si deux nœuds transmettent simultanément, une collision se produit et aucun d'eux n'est alors en mesure de transmettre.

Les technologies les plus utilisés :

+ **Ethernet** : topologie logique (*bus*) topologie physique (*étoile*/ / *étoile étendue*)
+ **Token Ring** : topologie logique (*anneau*) topologie physique (*étoile*)
+ **FDDI** : topologie logique (*anneau*) topologie physique (*double anneau*)

Règles MAC et détection de collision/réémission temporisée :

La méthode d'accès **CSMA/CD remplit les trois fonctions** suivantes:

- Transmission et réception de trames de données.
- Décodage et vérification des trames de données afin de s'assurer qu'elles ont une adresse valide avant de les transmettre aux couches supérieures du modèle OSI
- Détection d'erreurs à l'intérieur des trames de données ou sur le réseau.

Les équipements de réseau détectent qu'une *collision* s'est produite lorsque *l'amplitude du signal augmente* sur le média réseau.

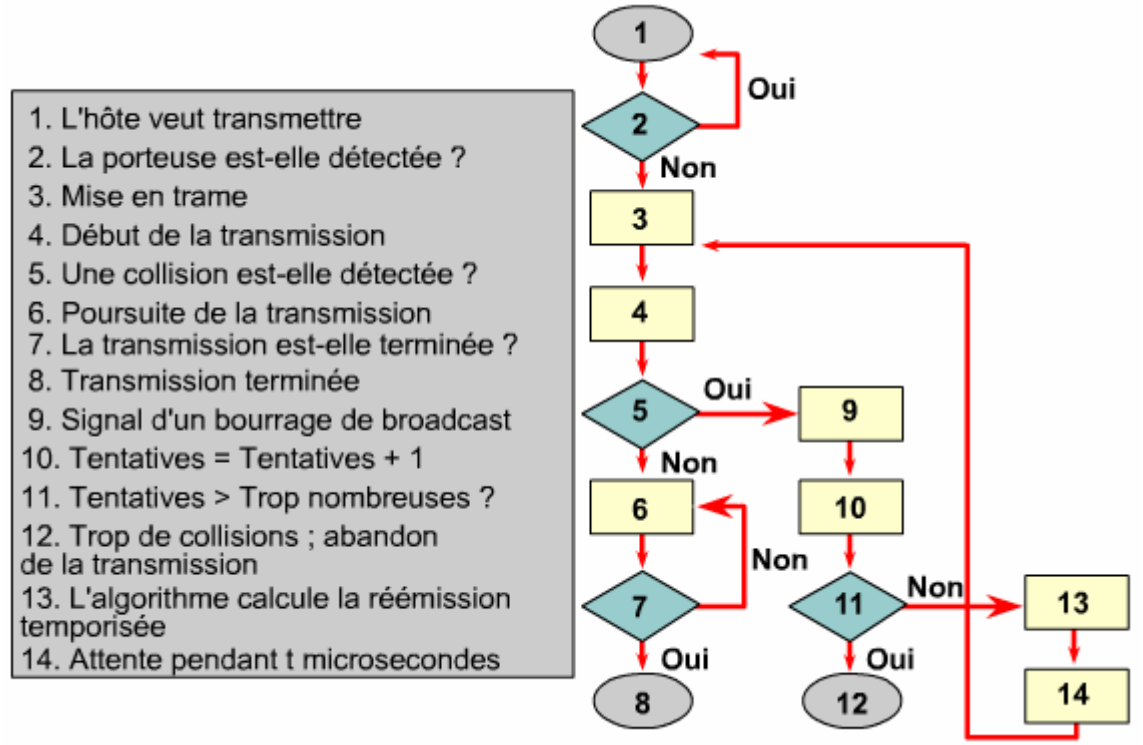
Lorsqu'une collision se produit :

→ Chaque nœud émetteur continue de transmettre des données pendant une courte période afin de s'assurer que tous les nœuds détectent la collision.

→ Lorsque tous les nœuds ont détecté la collision, l'algorithme de réémission temporisée est appelé et la transmission s'arrête.

→ Les nœuds arrêtent de transmettre pendant une période aléatoire, déterminée par l'algorithme de réémission temporisée.

→ À l'expiration du délai, chaque nœud peut tenter d'accéder à nouveau au média réseau. (Les équipements impliqués dans la collision ne sont pas prioritaires).



Synchronisation Ethernet :

Le signal électrique met un certain temps à parcourir le câble (*délai*), et chaque répéteur suivant introduit un bref temps de *latence* lors de la transmission de la trame entre deux ports. → Il est possible pour plusieurs stations de commencer la transmission au même moment, ce qui engendre une ***collision***.

Si la station connectée fonctionne en mode *full duplex*, alors elle peut envoyer et recevoir de façon simultanée et les collisions ne doivent pas se produire. Il élimine le concept de tranche de temps.

En mode *half duplex* est sujet des collisions.

Toutes les implémentations coaxiales sont en half duplex par nature et ne peuvent pas fonctionner en full duplex. Les implémentations UTP et en fibre optique peuvent fonctionner en half duplex. Les implémentations en 10 Gbits/s sont spécifiées pour le full duplex uniquement.

Les versions à 10 Mbits/s ou moins d'Ethernet sont *asynchrones*. Asynchrone signifie que chaque station réceptrice utilisera les huit octets d'informations de synchronisation (préambule) afin de synchroniser le circuit de réception avec les données entrantes.

Les implémentations à 100 Mbits/s et plus d'Ethernet sont *synchrones*. Synchrone signifie que les informations de synchronisation ne sont pas nécessaires.

La tranche de temps :

Pour toutes les vitesses de transmission Ethernet égales ou inférieures à 1000 Mbits/s, la norme stipule qu'une transmission ne peut pas être inférieure à une tranche de temps.

- pour l'Ethernet 10 et 100 Mbits/s est de 512 temps de bit, soit 64 octets.
- pour l'Ethernet 1000 Mbits/s est de 4096 temps de bit, soit 512 octets.

La tranche de temps est calculée en se basant sur des longueurs de câble maximales dans l'architecture de réseau légale la plus étendue.

Tous les délais de propagation sont au maximum légaux et le signal de bourrage 32 bits est utilisé lorsque des collisions sont détectées.

Pour permettre à l'Ethernet 1000 Mbits/s de fonctionner en mode half duplex, le *champ d'extension* a été ajouté aux seules fins d'occuper l'émetteur suffisamment longtemps pour le retour d'un fragment de collision lors de l'envoi de petites trames. Les bits d'extension sont abandonnés par la station réceptrice.

Sur Ethernet 10 Mbits/s, il faut 100 nanosecondes (ns) pour transmettre un bit. Voici des estimations approximatives.

Vitesse Ethernet	Temps de bit
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

→ *La valeur de 20,3 cm par nanoseconde* est souvent utilisée pour calculer le délai de propagation le long d'un câble UTP. Pour cent mètres de câble à paires torsadées non blindées, cela signifie qu'il faut 5 temps de bit.

Pour que l'Ethernet CSMA/CD puisse fonctionner, la station émettrice doit avoir connaissance d'une collision avant d'avoir terminé la transmission d'une trame de taille minimum. À 100 Mbits/s, la synchronisation du système est à peine capable de servir 100 mètres de câble. À 1000 Mbits/s, des ajustements spéciaux sont nécessaires du fait qu'environ une trame de taille minimum serait transmise avant que le premier bit n'atteigne la fin des premiers 100 mètres de câble UTP. Pour cette raison, le mode half duplex n'est pas autorisé dans le 10-Gigabit Ethernet.

Espacement intertrame et réémission temporisée :

L'espacement minimum entre deux trames n'entrant pas en collision est appelé *espacement intertrame*. Cet espacement a pour limites le dernier bit du champ de la FCS de la première trame et le premier bit du préambule de la deuxième trame.

Vitesse	Espacement intertrame	Temps nécessaire
10 Mbps	96 temps de bit	9.6 µs
100 Mbps	96 temps de bit	0.96 µs
1 Gbps	96 temps de bit	0.096 µs
10 Gbps	96 temps de bit	0.0096 µs

Sur les versions plus rapides d'Ethernet, l'espacement reste le même, 96 temps de bit, mais le temps nécessaire pour cet intervalle se réduit de façon proportionnelle. On appelle cet intervalle *écart d'espacement*. Cet écart est prévu pour donner le temps aux stations lentes de traiter la trame précédente et de se préparer pour la suivante.

Un répéteur pose encore un problème : il fait la synchronisation, malgré la perte potentielle de certains bits de début de préambule en raison de la lenteur de la synchronisation. → Une certaine réduction minime de l'écart intertrame est attendue.

Les stations à l'origine de la collision doivent observer un délai supplémentaire. La période d'attente est mesurée par incréments de tranche de temps.

Vitesse	Tranche de temps	Intervalles de temps
10 Mbps	512 temps de bit	51.2 µs
100 Mbps	512 temps de bit	5.12 µs
1 Gbps	4096 temps de bit	4.096 µs
10 Gbps	non applicable	non applicable

Si la couche MAC est incapable d'envoyer la trame après ***seize tentatives***, elle abandonne et génère une erreur sur la couche réseau.

Traitement des erreurs :

Les collisions entraînent une perte de la bande passante réseau qui est équivalente à la transmission initiale et au signal de bourrage de collision.

La grande majorité des collisions se produit au tout début de la trame, souvent avant le délimiteur de début de trame (SFD).

Dès qu'une collision est détectée, les stations émettrices transmettent *un signal de " bourrage "* sur 32 bits (jam) qui signale la collision.

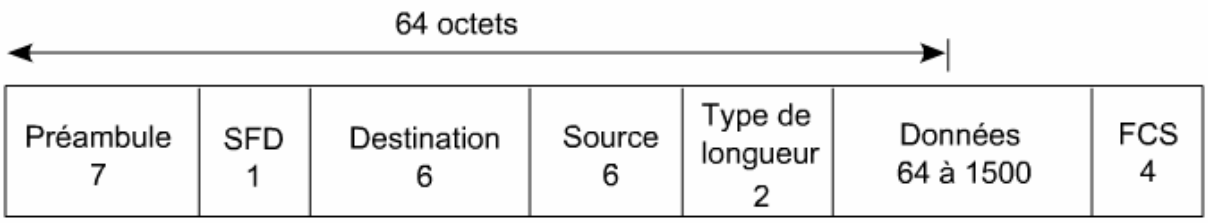
Le modèle de données le plus communément observé pour un signal de bourrage est simplement un modèle répétitif de un, zéro, un, zéro identique au préambule. Les messages corrompus et partiellement transmis sont souvent appelés *fragments de collision* ou *rebuts* (trames inférieures à 64 octets et comportent une FCS invalide)

Types de collision :

Une *collision unique* est une collision qui a été détectée lors d'une tentative de transmission d'une trame, mais qui a abouti à la tentative suivante.

On parle de *collisions multiples* lorsque la même trame est entrée en collision plusieurs fois avant d'être transmise avec succès.

Types de collisions :



Collision tardive	Collision distante	Collision locale
Collision se produisant après que les 64 premiers octets de données ont été envoyés. La carte réseau n'effectuera pas de retransmission pour ce type de collision.	Collision où la taille de la trame est inférieure au nombre minimum d'octets et dont la séquence de contrôle de trame est incorrecte. Elle se produit également à l'extrémité du répéteur.	Collision où un signal est détecté en même temps à la réception et à la transmission.

Erreurs Ethernet :

- ***Collision ou rebut (runt)*** ⌛ Transmission simultanée qui se produit avant que la tranche de temps ne se soit écoulée.
- ***Collision tardive*** ⌛ Transmission simultanée qui se produit après que la tranche de temps se soit écoulée.
- ***Jabber, trame longue et erreurs de plage*** ⌛ Transmission illégalement longue
- ***Trame courte, fragment de collision ou runt*** ⌛ Transmission illégalement courte
- ***Erreur FCS*** ⌛ Transmission corrompue (au moins un bit de la transmission est #)
- ***- Erreur d'alignement*** ⌛ Nombre insuffisant ou excessif de bits transmis (moins de 8)
- ***- Erreur de plage*** ⌛ Le nombre réel et le nombre signalé d'octets du champ longueur de la trame ne correspondent pas(ou la valeur de ce champ est inférieure à la taille minimum légale sans remplissage du champ de données).
- ***→ Out of Range*** ⌛ la valeur du champ de longueur indique une taille de données qui est trop grande pour être légale.
- ***- Fantôme (ghost) ou longueur excessive (Jabber)*** ⌛ Préambule anormalement long (SFD invalide) ou événement de bourrage.

→ Les collisions locales et distantes sont considérées comme faisant partie du fonctionnement normal d'Ethernet contrairement aux collisions tardives.

Le Jabber est défini dans la norme 802.3 comme une transmission d'une durée d'au moins 20 000 à 50 000 temps de bit. Cependant, la plupart des outils de diagnostic signalent ce type d'erreur chaque fois qu'une transmission détectée dépasse la taille de trame légale maximum, qui est bien inférieure à une durée de 20 000 à 50 000 temps de bit. De façon plus appropriée, on parlera de trames longues plutôt que de Jabber.

Une trame longue est une trame, étiquetée ou non, dont la longueur dépasse la taille légale sans tenir considération de la validation de la somme de contrôle FCS.

Une trame courte « runt » est une trame qui est plus petite que la taille minimum légale de 64 octets, et dont la séquence de contrôle de trame est bonne.

Le terme de jargon *runt* désigne en général quelque chose d'inférieur à la taille de trame légale.

Causes possibles :

- **Erreur FCS** : une carte réseau défaillante et/ou de pilotes logiciels défaillants ou corrompus, ou encore d'un mauvais câble reliant cette station au réseau.
- **Erreur d'alignement** : des pilotes incorrects ou à une collision
- **ghosting** : Les boucles de mise à la terre et d'autres anomalies de câblage.

Autonégociation Ethernet :

Lorsqu'Ethernet est passé de 10 à 100, puis à 1000 Mbits/s, il est devenu nécessaire de rendre chaque technologie interopérable.

L'autonégociation Ethernet est un processus qui indique comment deux partenaires de liaison peuvent négocier automatiquement une configuration offrant le meilleur niveau de performances communes. Il présente l'avantage supplémentaire de n'impliquer que la partie inférieure de la couche physique.

La norme 10BaseT exigeait que chaque station transmette une impulsion de liaison toutes les 16 millisecondes environ (impulsion de liaison normale (*NLP*)). Lorsqu'une série de NLP est envoyée en groupe à des fins d'autonégociation, ce groupe est appelé rafale *FLP* (impulsion de liaison rapide). Chaque rafale FLP est envoyée selon le même intervalle de synchronisation qu'une NLP.

La rafale communique les capacités de la station émettrice à son partenaire. Après avoir interprété ce que lui propose son partenaire, chaque station bascule sur la configuration commune la plus performante et établit une liaison à cette vitesse.

Si un incident quelconque interrompt les communications et que la liaison est perdue, les deux partenaires de liaison tentent une seule fois d'établir une nouvelle fois la liaison à la vitesse qu'ils avaient négociée en dernier. Si cette tentative échoue, ou si la liaison a été perdue depuis trop longtemps, le processus d'autonégociation recommence.

Les partenaires sont autorisés à ignorer l'offre de configuration pour laquelle ils sont équipés. Cela permet à l'administrateur réseau de forcer des ports à une configuration de vitesse et de mode duplex donnée, sans désactiver l'autonégociation.

L'ordre des priorités de transmission :

- 1000BaseT full duplex
- 1000BaseT half duplex
- 100BaseTX full duplex
- 100BaseTX half duplex
- 10BaseT full duplex
- 10BaseT half duplex

Les implémentations Ethernet à fibre optique ne figurent pas dans cette liste car il est supposé que la configuration de l'interface dans la fibre optique est fixe. Si les deux interfaces sont en mesure d'autonégocier, c'est qu'elles utilisent déjà les mêmes implémentations Ethernet.

Module 7

Technologies Ethernet

Ethernet 10 Mbits/s :

Les technologies Ethernet 10BASE5, 10BASE2 et 10BASE-T sont considérées comme les versions initiales d'Ethernet.

Elles ont en commun quatre caractéristiques, à savoir les paramètres de synchronisation, le format de la trame, les processus de transmission et la règle de conception de base.

Paramètre	Valeur
Durée d'un bit	100 nanosecondes (ns)
Durée d'une tranche	Durée de 512 bits (64 octets)
Espacement intertrame	96 bits *
Nombre maximum de tentatives après collision	16
Nombre maximum de réémissions temporisées après collision	10
Taille du signal de collision	32 bits
Taille maximale des trames non référencées	1 518 octets
Taille minimale des trames	512 bits (64 octets)

Le signal d'erreur de qualité de ligne est un processus important. Il s'agit d'une transmission renvoyée au contrôleur par un émetteur-récepteur pour lui indiquer si les circuits de collision sont opérationnels. Ce signal d'erreur est également appelé « ***pulsation*** ».

Il est actif dans les cas suivants:

- (4 à 8 microsecondes après transmission) la trame de sortie a été correctement transmise.
- En cas de collision sur le support.
- en cas de signal incorrect sur le support, tel qu'une erreur de message trop long, ou de réflexion due à un court-circuit.
- Lorsqu'une transmission a été interrompue.

Toutes les formes Ethernet de 10 Mbits/s récupèrent les octets provenant de la sous-couche MAC et lancent un processus appelé « ***codage de ligne*** » (codage Manchester). Le codage de ligne décrit le type de signalement des bits sur le câble.

La synchronisation est fonction des types de paramètres suivants:

- La longueur de câble et le délai de propagation.
- Le délai des répéteurs.
- Le délai des émetteurs-récepteurs.
- La réduction des vides intertrames.
- Les délais au sein de la station.

Lorsque plusieurs concentrateurs sont utilisés, il faut les organiser selon une arborescence hiérarchisée. (Réduire le nombre de répéteurs si possible).

Grâce aux commutateurs en chaîne, il est possible d'étendre un LAN indéfiniment.

10 Base 5 :

10Base5 (1980) utilise le coaxial épais (1er support utilisé pour Ethernet).
+ inclus dans la norme 802.3 d'origine.
→ Il fonctionne uniquement en mode half-duplex avec un débit maximum de 10 Mbits/s.
→ Il utilise le codage Manchester.

Avantages : sa longueur de 500m + un peu onéreux

Inconvénients : les cartes réseau sont très difficiles à trouver et ils sont sensibles à la réflexion.

10 Base 2 :

10Base2 (1985) utilise le coaxial fin.
→ Les câbles coaxiaux sont reliés à un connecteur en T de la carte réseau, avec des BNC.
→ Un segment 10BASE2 peut comporter jusqu'à 30 stations
→ Il utilise le codage Manchester.

Avantages : Installation facile + plus légère et plus flexible + peu coûteux

Inconvénients : longueur maximum de 185m.

- La distance minimum entre les « T » 0.5m
- Chaque station doit être raccordée à 4cm maximum du câble coaxial.

10 Base T :

10Base2 (1990) utilise l'UTP cat 3, 4 et 5.
→ Le câble était relié à une unité de connexion centrale qui contenait le bus partagé. Cette unité était un concentrateur (topologie étoile).
→ La technologie 10BASE-T prend en charge un trafic de 10 Mbits/s en mode half-duplex et de 20 Mbits/s en mode full duplex.
→ Il utilise le codage Manchester.

Avantages : Installation facile + plus légère + coût faible

Inconvénients : longueur maximum de 90m.

Ethernet 100 Mbits/s (Fast Ethernet) :

Deux normes sont devenues importantes: 100BASE-TX et 100BASE-FX.

Paramètre	Valeur
Durée d'un bit	10 nanosecondes (ns)
Durée d'une tranche	Durée de 512 bits (64 octets)
Espacement intertrame	96 bits
Nombre maximum de tentatives après collision	16
Nombre maximum de réémissions temporisées après collision	10
Taille du signal de collision	32 bits
Taille maximale des trames non référencées	1 518 octets
Taille minimale des trames	512 bits (64 octets)

Architecture	100BASE-TX	100BASE-FX	100BASE-TX et FX
De station à station, de station à commutateur, de commutateur à commutateur (half ou full duplex)	100 m	412 m	N/A
Un répéteur de classe I (half-duplex)	200 m	272 m	100 m (TX) 160.8 m (FX)
Un répéteur de classe II (half-duplex)	200 m	320 m	100 m (TX) 208 m (FX)
Deux répéteurs de classe II (half-duplex)	205 m	228 m	105 m (TX) 211.2 m (FX)

100 Base TX :

100BaseTX (1995) utilise l'UTP cat 5 et supérieur.

En 1997, la technologie Ethernet a été étendue pour inclure une fonctionnalité ***full duplex*** (200 Mbits/s) qui permettait à plusieurs ordinateurs d'un réseau de transmettre des données simultanément.

La technologie 100BASE-TX utilise le codage *4B/5B*, qui est ensuite mélangé et converti en codage *MLT-3* (*Multi-Level Transmit*).

100 Base FX :

La fibre optique pouvait en effet être utilisée pour les applications de backbone, pour les connexions entre étages, dans les bâtiments, ainsi que dans les environnements où le bruit est important.

100BASE-FX utilise l'encodage *NRZI*.

Les chemins de transmission (TX) et de réception (RX) de la technologie 100BASE-FX à fibre optique permettent chacun des transmissions à 200 Mbits/s.

Un répéteur de classe I peut introduire une latence d'une durée allant jusqu'à 140 bits. Tout répéteur modifié entre une implémentation Ethernet et une autre appartient à la classe I. Les délais de synchronisation d'un *répéteur de classe II* sont plus courts (durée de 92 bits), car ce type de matériel répète immédiatement le signal entrant vers tous les autres ports, sans processus de conversion. Pour pouvoir offrir un tel délai, les répéteurs de classe II peuvent uniquement se connecter à des types de segments qui utilisent la même technique de signalisation.

Ethernet 1000 Mbits/s (Gigabit Ethernet) :

Les normes 1000BASE-TX, 1000BASE-SX et 1000BASE-LX utilisent les mêmes paramètres de synchronisation

Paramètre	Valeur
Types Ethernet	1 ns
Durée d'une tranche	Durée de 4 096 bits
Espacement intertrame	96 bits *
Nombre maximum de tentatives après collision	16
Nombre maximum de réémissions temporisées après collision	10
Taille du signal de collision	32 bits
Taille maximale des trames non référencées	1 518 octets
Taille minimale des trames	512 bits (64 octets)
Limite de débit garanti en rafale	65 536 bits

La norme Gigabit Ethernet à fibre optique (1000BASE-X) utilise le codage 8B/10B, qui est semblable au concept 4B/5B. Il est suivi par le codage de ligne simple de non-retour à zéro (NRZ) de la lumière sur les fibres optiques.

Au niveau de la couche physique, la trame est convertie en *symboles*. Ces symboles peuvent aussi représenter des informations de contrôle, telles que le début de trame, la fin de trame ou les conditions d'inactivité sur une liaison. La trame est codée sous forme de symboles de contrôle et de symboles de données pour augmenter le débit sur le réseau.

1000 Base T :

La norme 1000BASE-T (IEEE 802.3ab) a été développée pour fournir une bande passante supplémentaire afin de désengorger ces goulots d'étranglement.

La première étape de la mise en œuvre de la norme 1000BASE-T consiste à utiliser les quatre paires de fils plutôt que les deux paires généralement utilisées par les normes 10BASE-T et 100BASE-TX (transmissions en mode full duplex sur la même paire de fils). Ainsi, chaque paire dispose d'un débit de 250 Mbits/s. Ainsi, avec les quatre paires de fils, il est possible d'obtenir les 1 000 Mbits/s souhaités.

Le codage 1000BASE-T avec le codage de ligne *4D-PAM5* est utilisé sur un câble sur un câble UTP.

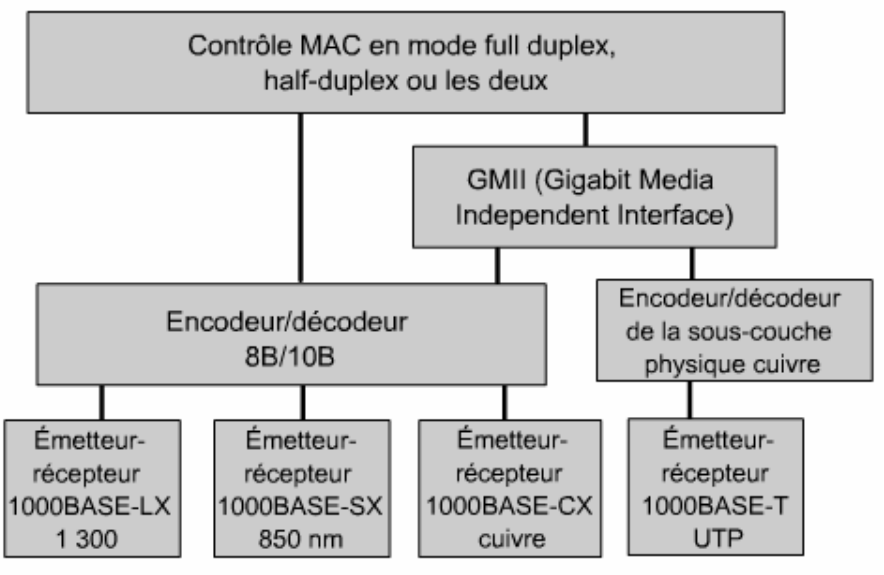
Pendant les périodes d'inactivité, il existe 9 niveaux de tension sur le câble, contre 17 lors de la transmission des données. Avec ce nombre important d'états et les effets de bruit, le signal semble plus analogique que numérique.

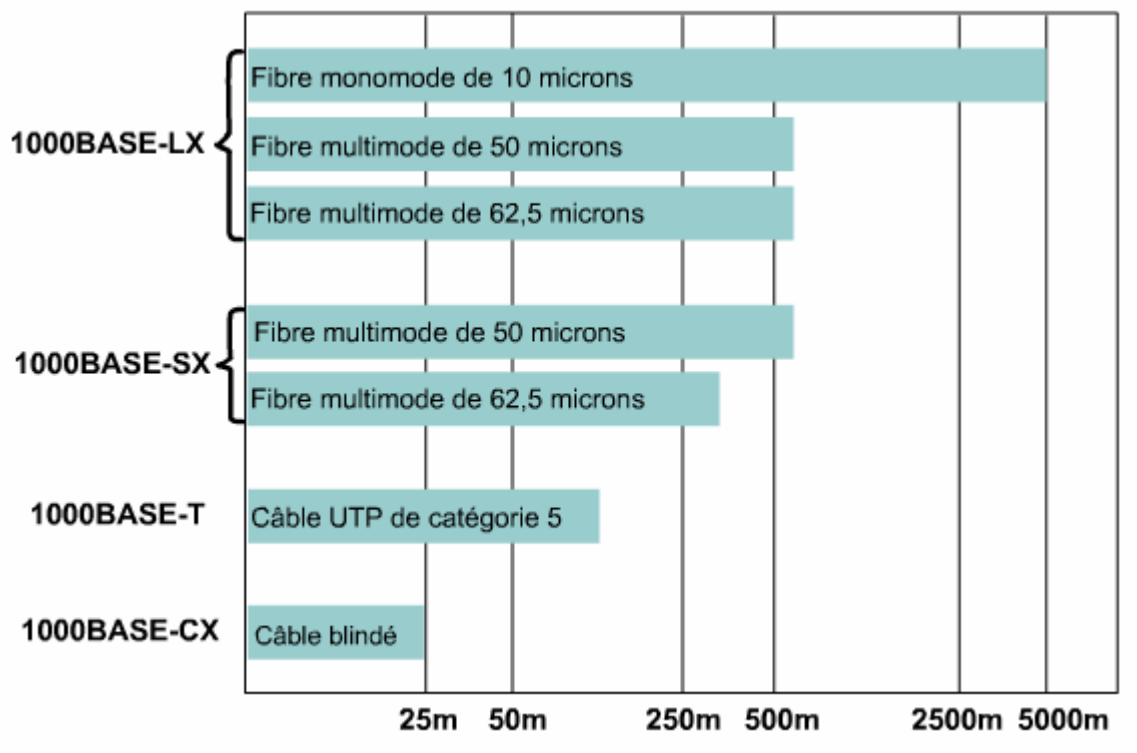
1000 Base LX et SX :

La norme IEEE 802.3 recommande d'utiliser la norme Gigabit Ethernet sur des fibres optiques pour le backbone.

Deux systèmes de codage des signaux sont définis au niveau physique. Le système *8B/10B* est utilisé pour les médias à fibre optique et en cuivre blindés, tandis que la modulation d'impulsions en amplitude *PAM5* (*pulse amplitude modulation 5*) l'est pour les câbles UTP.

La norme 1000BASE-X fait appel au codage *8B/10B* converti en codage de ligne de non-retour à zéro (*NRZ*).





La méthode MAC traite la liaison comme étant de type *point-à-point*. Différentes fibres optiques étant utilisées pour la transmission (Tx) et la réception (Rx), la connexion est, de façon inhérente, en mode full duplex.

La norme Gigabit Ethernet n'autorise qu'un seul répéteur entre deux stations.

La longueur des liaisons en mode full duplex est uniquement limitée par le *support*, et non par le temps de parcours aller-retour entre deux hôtes.

Les points importants sont alors la topologie logique et le flux de données, non la synchronisation ou les restrictions de distance.

Il est conseillé d'autoriser l'autonégociation pour toutes les liaisons entre une station et un concentrateur ou un commutateur pour bénéficier des meilleures performances communes

10 Gigabit Ethernet :

La norme IEEE 802.3ae (juin 2002) a été adaptée pour inclure la transmission en mode full duplex de 10 Gbits/s sur un câblage à fibre optique.

Cette norme 10 Gigabit Ethernet (10GbE) est évolutive non seulement pour les LAN, mais aussi pour les MAN (réseaux SONET et SDH « 40Km ») & WAN (concurrent de l'ATM).

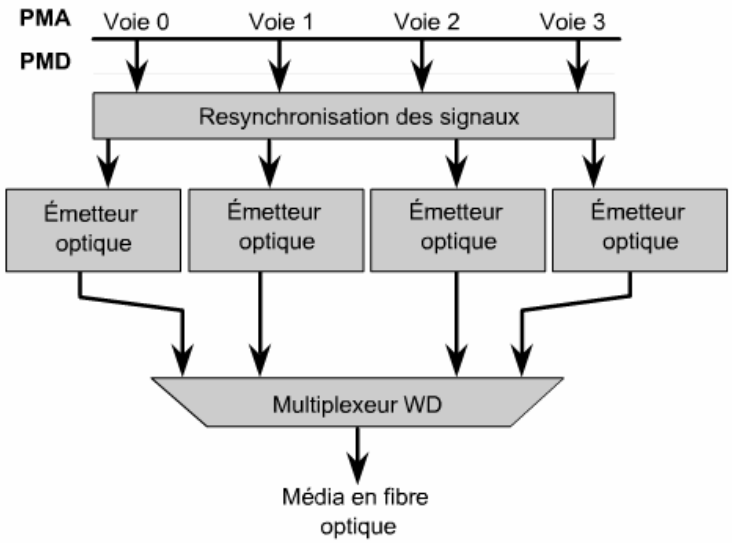
Paramètre	Valeur
Durée d'un bit	0,1 ns
Durée d'une tranche	Non applicable *
Espacement intertrame	96 bits **
Nombre maximum de tentatives après collision	Non applicable *
Nombre maximum de réémissions temporisées après collision	Non applicable *
Taille du signal de collision	Non applicable *
Taille maximale des trames non référencées	1 518 octets
Taille minimale des trames	512 bits (64 octets)
Limite de débit garanti en rafale	Non applicable *
Taux d'extension de l'espacement intertrame	104 bits ***

Technologies 10 Gigabit Ethernet :

- ***10GBASE-SR***: conçue pour les courtes distances sur des fibres optiques multimodes déjà installées, supporte une distance de 26 à 82 m.
- ***10GBASE-LX4***: utilise le multiplexage de longueurs d'onde, supporte une distance de 240 à 300 m sur des fibres optiques multimodes déjà installées et 10 km sur des fibres optiques monomodes.
- ***10GBASE-LR*** et ***10GBASE-ER***: supportent une distance de 10 km et 40 km respectivement sur des fibres optiques monomodes.
- ***10GBASE-SW***, ***10GBASE-LW*** et ***10GBASE-EW***: généralement appelées « 10GBase-W », conçues pour fonctionner avec un équipement de réseaux WAN SONET et SDH, avec module de transport synchrone OC-192.

Actuellement, la plupart des produits 10 Gigabits Ethernet existent sous forme de modules, ou de cartes d'interface, qui sont ajoutés aux commutateurs et aux routeurs haut de gamme.

Pour traiter les questions de synchronisation, de bande passante et de rapport signal/bruit, les systèmes 10 Gigabit Ethernet font appel à deux étapes de codage distinctes.



Lorsque le flux du signal optique atteint le support, il est démultiplexé en quatre flux de signaux optiques distincts. Ces flux sont ensuite convertis en quatre trains de bits électroniques lorsqu'ils effectuent pratiquement le chemin inverse via les sous-couches de la couche MAC.

Avenir d'Ethernet :

La technologie Ethernet a connu l'évolution suivante:

Version initiale —> Fast —> Gigabit —> MultiGigabit

L'avenir des médias réseau peut se décomposer en trois phases:

- La phase *cuivre* (jusqu'à 1 000 Mbits/s, voire plus).
- La phase *sans fil* (approchant les 100 Mbits/s, voire plus).
- La phase *fibre optique* (actuellement à 10 000 Mbits/s, devrait dépasser ce seuil).

Dans les systèmes à fibre optique, ce sont les processus de fabrication des fibres et la technologie électronique (telle que les émetteurs et les détecteurs) qui limitent la vitesse.

Module 8

Commutation Ethernet

Pontage au niveau de la couche 2 :

Plus le nombre de nœuds situés sur un segment augmente, plus le média est utilisé

Problème : la probabilité de collisions est plus forte,

Solution : fragmenter le segment principal en plusieurs domaines de collision distincts.

Un pont établit une table de correspondance MAC / port (table de pontage). Le pont transmet ensuite les trames, ou les rejette, en fonction des entrées de la table.

Le pont ajoute l'adresse source de la trame à sa table de pontage. Sachant que la trame est reçue sur le port X, la trame doit être associée au port X dans la table.

Commutation au niveau de la couche 2 :

En règle générale, un *pont* comprend deux ports et subdivise un domaine de collision en deux segments. Mais il n'a aucun effet sur le domaine logique ou de broadcast.

Dans le cas d'un commutateur, chaque port crée son propre domaine de collision.

Lorsqu'un réseau comporte 20 nœuds, 20 domaines de collision doivent exister si chaque nœud est connecté à son propre port de commutation. Dans le cas où un port uplink est installé, un commutateur crée 21 domaines de collision

Un commutateur crée et gère de façon dynamique *une table de mémoire associative* (***CAM***, *Content Addressable Memory*),

Fonctionnement d'un commutateur :

Un commutateur subdivise un segment en plusieurs *microsegments*.

La plupart des commutateurs prennent en charge le mode *full duplex*, de même que la plupart des cartes réseau.

Développement des commutateurs :

→ Apparition des microprocesseurs.
→ Apparition des mémoires plus performantes.

Un circuit intégré à application spécifique (***ASIC***) est un circuit intégré qui permet à des fonctions logicielles d'être effectuées de façon matérielle (réduire les retards causés par les processus logiciels).

La mémoire ***CAM*** permet à un commutateur de rechercher un port associé à une adresse MAC sans algorithme de recherche.

Latence :

On appelle *latence* le temps qui s'écoule entre le moment où une trame quitte un équipement source et celui où la première partie de la trame atteint sa destination.

Causes possibles :

- Les retards au niveau des médias (causés par la vitesse).
- Les retards au niveau des circuits (causés par les composants électroniques qui traitent le signal).
- Les retards au niveau des applications (causés par les décisions et les protocoles).
- Les retards peuvent être causés par le contenu de la trame (vérification)

Modes de commutation :

Il existe 3 modes de commutation pour un commutateur :

«Cut-through» :

Un commutateur peut commencer à transférer la trame dès que l'adresse MAC est reçue

→ Pas de vérification des erreurs → un temps de latence très faible.

«Store-and-Forward».

Un commutateur peut attendre de recevoir la trame entière avant de la transférer vers le port de destination.

→ Vérifier la séquence de contrôle de trame (FCS). Si la trame n'est pas correcte, elle est rejetée au niveau du commutateur.

«Fragment-Free»

Une solution intermédiaire de commutation. Ce mode lit les 64 premiers octets, incluant l'en-tête de la trame, puis il commence à transmettre le paquet.

→ Vérifie la fiabilité des adresses et des informations relatives au protocole LLC.

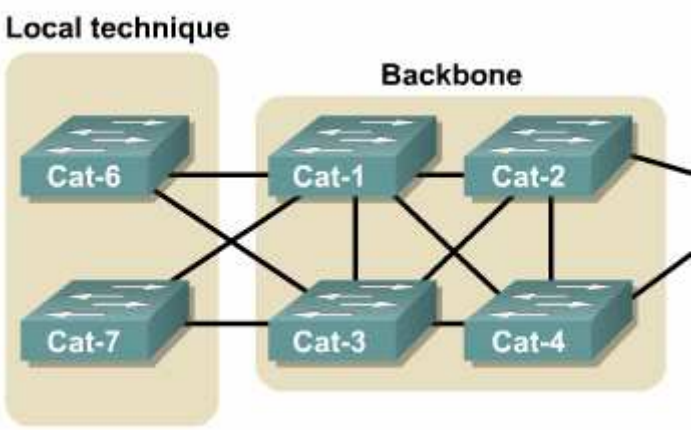
Avec le mode de commutation «Cut-through», les débits des ports source et de destination doivent être identiques pour ne pas endommager la trame (*commutation symétrique*)

Lorsque les débits sont différents, la trame utilise un certain débit pour la réception et un autre pour l'émission (*commutation asymétrique*). Le mode «Store-and-Forward» doit être utilisé dans le cadre d'une commutation asymétrique.

La commutation asymétrique est particulièrement adaptée aux flux de trafic client-serveur où plusieurs clients communiquent avec un serveur simultanément. Une bande passante plus large doit être allouée au port du serveur afin d'éviter qu'un goulot d'étranglement ne se produise au niveau de ce port.

Protocole STP (Spanning-Tree Protocol)

Lorsque plusieurs commutateurs sont placés dans une arborescence hiérarchique simple, il est peu probable que des ***boucles de commutation*** se produisent à cause des chemins redondants (assurer une meilleure fiabilité et une meilleure tolérance aux pannes).



Les boucles de commutation peuvent provoquer des *tempêtes de broadcast* qui risquent de submerger rapidement le réseau.

Le protocole STP est un protocole normalisé qui permet d'éviter les boucles de commutation.

Chaque commutateur d'un réseau LAN qui utilise le protocole STP envoie un message appelé ***BDPU*** (*Bridge Protocol Data Unit*) par le biais de tous ses ports afin que les autres commutateurs soient informés de son existence.

Chaque port d'un commutateur utilisant le protocole STP a pour état :

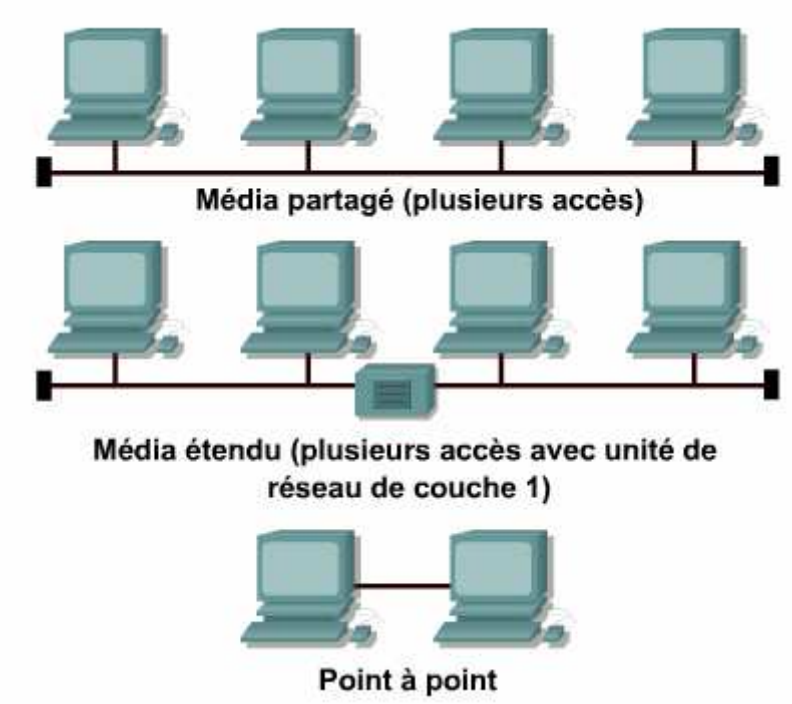
États	Objectif
Blocage	Reçoit uniquement les unités BPDU.
Écoute	Construction d'une topologie " active "
Acquisition	Construction d'une table de pontage
Transmission	Envoi et réception de données utilisateur
Désactivation	Désactivation par un administrateur

Un port change d'état comme suit:

- De l'initialisation au blocage.
- Du blocage à l'écoute ou à la désactivation.
- De l'écoute à l'apprentissage ou à la désactivation.
- De l'apprentissage à l'acheminement ou à la désactivation.
- De l'acheminement à la désactivation.

Environnements de média partagé :

Exemples de réseaux directement connectés et de médias partagés :



Les collisions ne se produisent que dans les environnements partagés.

Domaines de collision :

Un domaine de collision est un segment du réseau physique dans lequel des collisions peuvent se produire.

Les équipements de couche 2 et 3 segmentent les domaines de collision. Ce processus est d'ailleurs appelé «***segmentation***».

Les équipements de couche 1, notamment les répéteurs et les concentrateurs, sont utilisés pour étendre les segments de câble Ethernet → Etendre un domaine de collision.

La règle dite de «***5-4-3-2-1***» requiert que les conditions suivantes soient respectées:

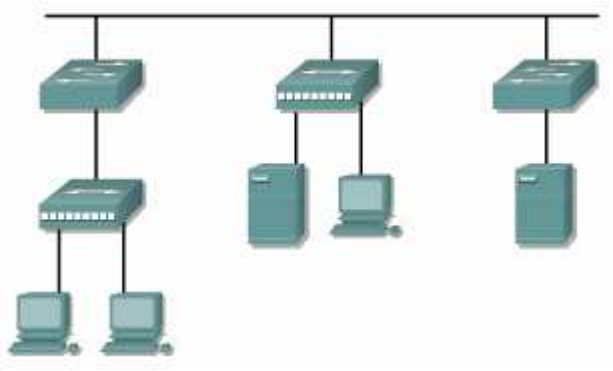
- *Cinq* segments de média réseau.
- *Quatre* répéteurs ou concentrateurs.
- *Trois* segments hôte de réseau.
- *Deux* sections de liaison sans hôte.
- *Un* grand domaine de collision.

Segmentation :

Les équipements de couche 2 segmentent les domaines de collision. Ils utilisent les adresses MAC affectées à chaque équipement Ethernet pour effectuer le contrôle.

Moins il y a d'hôtes dans un domaine de collision, plus la disponibilité du média est élevée.

Les équipements de couche 2 et 3 ne transmettent pas les collisions.



Pour cet exemple, il existe 3 domaines de collisions.

Broadcast au niveau de la couche 2 :

Les équipements de couche 2 doivent diffuser la totalité du trafic de broadcast et de multicast. L'accumulation du trafic de broadcast et de multicast de chaque équipement du réseau s'appelle le *rayonnement de diffusion* (*broadcast radiation*).

Plus le réseau commuté prend de l'importance et plus le risque de tempête de broadcast devient fort.

Les trois sources de broadcasts et de multicast dans les réseaux IP sont les *stations de travail*, *les routeurs* et *les applications* multicast.

Les stations de travail diffusent une requête ARP (*Address Resolution Protocol*) chaque fois qu'elles doivent localiser une @ MAC qui ne se trouve pas dans la table ARP.

Les stations de travail IP peuvent conserver de 10 à 100 adresses dans le cache ARP pendant environ 2 heures.

Si 2 000 stations de travail sont configurées pour exécuter le protocole RIP, ces stations génèrent 3 333 broadcasts par seconde sachant qu'une moyenne de 50 paquets est requise pour transmettre la table de routage.

La diffusion multicast est un moyen efficace d'envoyer un flux de données multimédias à plusieurs utilisateurs d'un concentrateur à média partagé. Toutefois, ce mode n'est pas adapté aux réseaux commutés non hiérarchiques.

Les domaines de Broadcast :

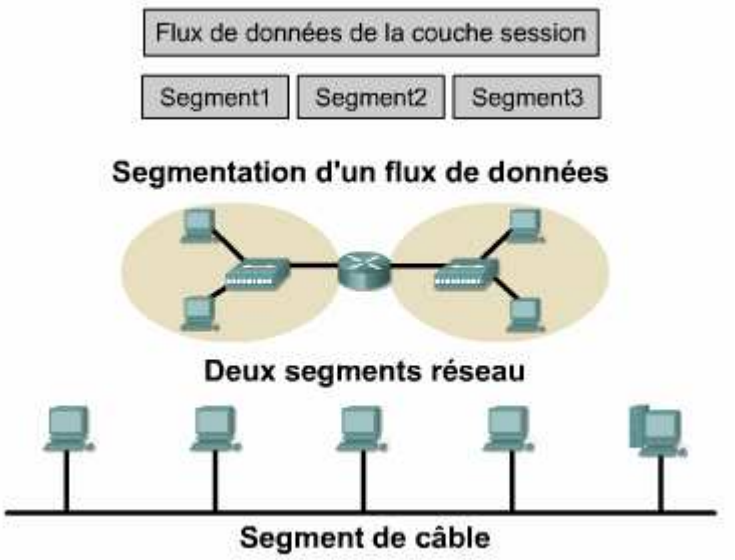
Un domaine de broadcast est un groupe de domaines de collision connectés par des équipements de couche 2.

Les broadcasts doivent être contrôlés au niveau de la couche 3, car les équipements de couche 1 et 2 ne sont pas capables d'effectuer cette opération.

La couche 3 permet aux *routeurs* de segmenter les domaines de broadcast.

Qu'est-ce qu'un segment de réseau ?

- Section d'un réseau reliée par des ponts, des routeurs ou des commutateurs.
- Dans un réseau local à topologie de bus, un segment est un circuit électrique continu souvent connecté à d'autres segments de même type par des répéteurs.
- C'est aussi un terme utilisé dans la spécification TCP pour décrire une unité d'information de la couche de transport.



Module 9

Pile de protocole TCP/IP & Adressage IP

Origine et évolution du protocole TCP/IP :

Le ministère américain de la Défense (***DoD***) a développé le modèle de référence TCP/IP, car il avait besoin d'un réseau pouvant résister à toutes les situations. Depuis lors, le modèle TCP/IP s'est imposé comme la norme Internet.

La version actuelle du protocole TCP/IP a été normalisée en septembre 1981.

Les quatre couches du modèle TCP/IP sont les suivantes: la couche application, la couche transport, la couche Internet et la couche d'accès au réseau.

La couche application :

La couche application gère les protocoles de niveau supérieur, les représentations, le code et le contrôle du dialogue.

Le modèle TCP/IP possède des protocoles prenant en charge les services suivants :

- **FTP** ***(****File Transfer Protocol****)*****:** ce protocole est un service fiable orienté connexion qui utilise le protocole TCP. Il gère les transferts bidirectionnels des fichiers binaires et ASCII.
- **TFTP** ***(****Trivial File Transfer Protocol****)*****:** ce protocole est un service non orienté connexion qui utilise le protocole UDP. Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images IOS Cisco, il s'exécute plus rapidement que le protocole FTP dans un environnement stable.
- **NFS** ***(****Network File System****)*****:** ce protocole est un ensemble de protocoles pour systèmes de fichiers distribués, développé par Sun Microsystems, permettant un accès aux fichiers d'un équipement de stockage distant, tel qu'un disque dur.
- **SMTP** ***(****Simple Mail Transfer Protocol****)*****:** ce protocole régit la transmission du courrier électronique sur les réseaux informatiques. Il ne permet pas de transmettre des données autres que du texte en clair.
- **Telnet (rlogin aussi):** ce protocole permet d'accéder à distance à un autre ordinateur. Cela permet à un utilisateur d'ouvrir une session sur un hôte Internet et d'exécuter diverses commandes.
- **SNMP** ***(****Simple Network Management Protocol****)*****:** ce protocole permet de surveiller et de contrôler les équipements du réseau, ainsi que de gérer les configurations, les statistiques, les performances et la sécurité.
- **DNS** ***(****Domain Name System****)*****:** ce protocole est utilisé par Internet pour convertir en adresses IP les noms de domaine.

La couche transport :

La couche transport fournit une connexion logique entre les hôtes source et de destination.

Le rôle des protocoles TCP et UDP :

- Segmenter les données d'application de couche supérieure.
- Envoyer des segments d'un équipement à un autre.

Le rôle du protocole TCP :

- Etablir une connexion de bout en bout.
- Assurer le contrôle de flux à l'aide des fenêtres glissantes.
- Assurer la fiabilité à l'aide des numéros de séquençage et des accusés de réception

La couche Internet :

Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau.

Les protocoles de la couche Internet du protocole TCP/IP :

- **IP** assure l'acheminement au mieux (best-effort delivery) des paquets, non orienté connexion (*n'effectue aucune vérification d'erreurs et ne fournit aucun service de correction*). Il ne se préoccupe pas du contenu des paquets.
- **ICMP** (Internet Control Message Protocol) offre des fonctions de messagerie et de contrôle.
- **ARP** (Address Resolution Protocol) détermine les adresses de la couche liaison de données ou les @MAC pour les @IP connues.
- **RARP** (Reverse Address Resolution Protocol) détermine l'@ IP pour une @MAC connue.

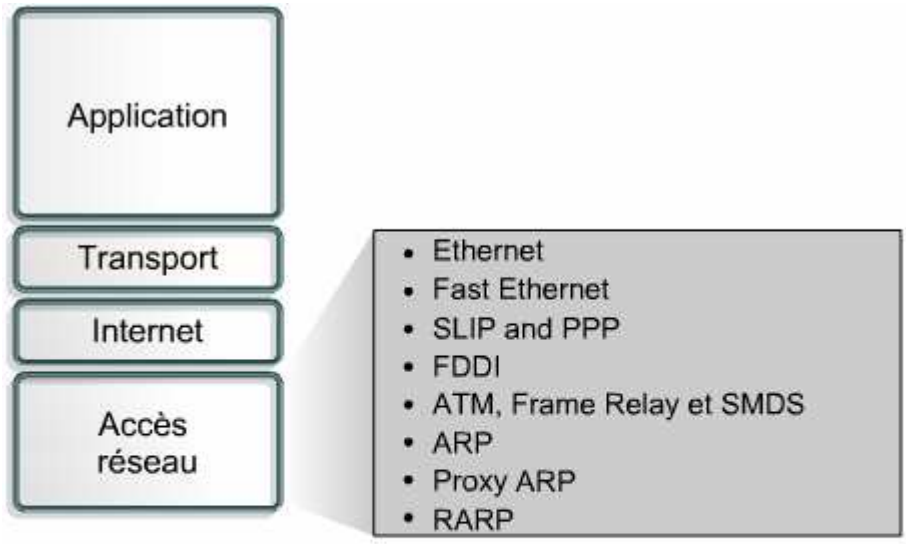
Le protocole IP effectue les opérations :

- Il définit un paquet et un système d'adressage.
- Il transfère des données entre la couche Internet et la couche d'accès au réseau.
- Il achemine des paquets à des hôtes distants.

La couche d'accès au réseau (couche hôte-réseau) :

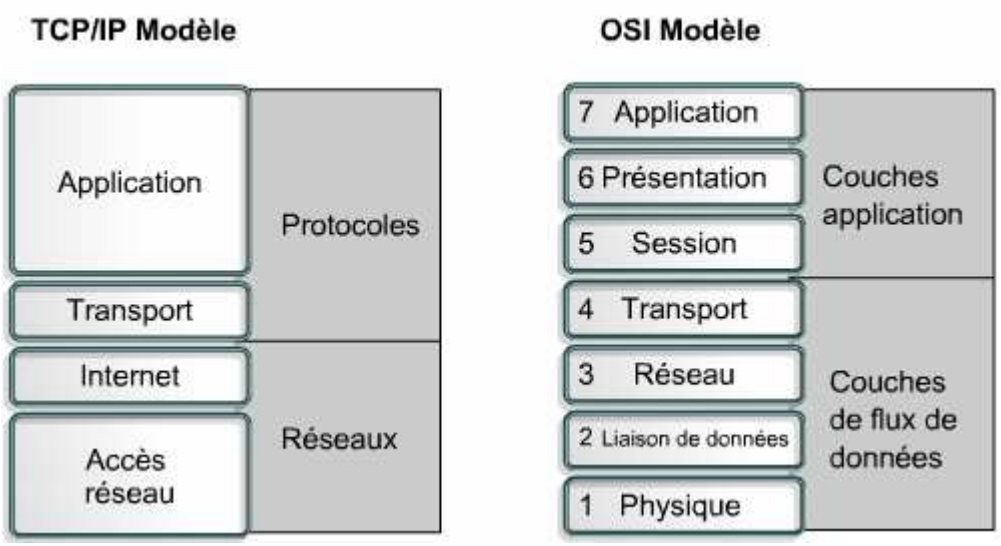
La couche d'accès au réseau permet à un paquet IP d'établir une liaison physique avec un média réseau. Cela comprend les détails sur les technologies LAN et WAN.

Les protocoles de modem, à savoir les protocoles *SLIP* (Serial Line Internet Protocol) et *PPP* (Point-to-Point Protocol) sont utilisés pour accéder au réseau par modem.



Les protocoles ARP et RARP se situent au niveau des couches d'accès réseau et Internet.

Comparaison des modèles TCP/IP et OSI :



Similitudes :

- Tous deux comportent des couches.
- Tous deux comportent une couche application
- Tous deux comportent des couches réseau et transport comparables.
- Tous deux s'appuient sur un réseau à commutation de paquets.
- Les professionnels des réseaux doivent connaître les deux modèles.

Différences :

- TCP/IP intègre les couches application, présentation et session du modèle OSI dans sa couche application.
- TCP/IP regroupe les couches physique et liaison de données du modèle OSI dans sa couche d'accès au réseau.
- TCP/IP semble plus simple, car il comporte moins de couches.
- Lorsque la couche transport du protocole TCP/IP utilise le protocole UDP, la transmission des paquets n'est pas fiable tandis qu'elle est toujours fiable avec la couche transport du modèle OSI.

En règle générale, le modèle OSI ne permet pas de créer des réseaux. Il est utilisé pour aider les étudiants à comprendre le processus de communication.

Internet a évolué rapidement, acceptant de plus en plus d'utilisateurs. Sa capacité d'évolution (plus de 90 000 routes principales et 300 000 000 utilisateurs finaux) traduit l'efficacité de son architecture.

L'adressage IP :

Chaque point de connexion, ou interface, d'un équipement dispose d'une adresse IP associée à un réseau. Cette @ permet à d'autres ordinateurs de localiser cet équipement sur un réseau spécifique.

Une adresse IP est une séquence de 32 bits composée de 1 et de 0, Afin de faciliter leur lecture, les adresses IP sont généralement exprimées sous la forme de quatre nombres décimaux séparés par des points.

Les longues chaînes de 1 et de 0 répétés sont plus propices aux erreurs, c'est pour cette raison qu'on utilise le format décimal pointé.

Adressage IPv4 :

Un routeur utilise l'adresse IP du réseau de destination afin de remettre le paquet au réseau approprié.

Analogie : système postal national.

On parle dans ce cas de système d'adressage hiérarchique, car il contient plusieurs niveaux. Chaque adresse IP regroupe ces deux identificateurs en un seul nombre. La première partie identifie l'adresse réseau du système. La seconde, appelée «partie hôte», identifie la machine sur le réseau.

Les adresses IP sont réparties en ***classes*** afin de définir des réseaux de différentes tailles :

- Les adresses de classe ***A*** sont affectées aux réseaux de grande taille.
- Les adresses de classe ***B*** sont utilisées pour les réseaux de taille moyenne
- Les adresses de classe ***C*** pour les réseaux de petite taille.

Classe d'adresses IP	Bits de valeur supérieure	Plage d'adresses du premier octet	Nombre de bits de l'adresse réseau
Classe A	0	0 - 127 *	8
Classe B	10	128 - 191	16
Classe C	110	192 - 223	24
Classe D	1110	224 - 239	28

→ Le réseau 127.0.0.0 est réservé pour les tests en bouclage.

→ Les adresses de classe D est réservée à la diffusion multicast d'une adresse IP.

→ Les adresses de classe E est réservés à des fins expérimentales par le groupe IETF (*Internet Engineering Task Force*)

Adresses IP réservées :

Les adresses hôte réservées se composent des éléments suivants:

- ***Une adresse réseau*** – pour identifier le réseau lui-même.
- ***Une adresse de broadcast*** – pour diffuser des paquets vers tous les équipements.

→ Une adresse IP dont tous les ***bits hôte*** sont occupés par des ***0*** binaires est réservée pour l'adresse réseau.

→ Une adresse IP dont tous les ***bits hôte*** sont occupés par des ***1*** binaires est réservée pour l'adresse de Broadcast.

Adresses IP publiques et privées :

À l'origine, un organisme portant le nom d'***InterNIC*** (*Internet Network Information Center*) était chargé de la vérification de l'unicité des adresses IP. Celui-ci n'existe plus et a été remplacé par l'***IANA*** (*Internet Assigned Numbers Authority*).

Chaque adresse IP publique étant unique, deux ordinateurs connectés à un réseau public ne peuvent pas avoir la même adresse IP publique.

Les adresses IP publiques doivent être obtenues auprès d'un fournisseur d'accès Internet (FAI) ou d'un registre moyennant une participation.

Pour résoudre le problème de pénurie d'adresses IP publiques

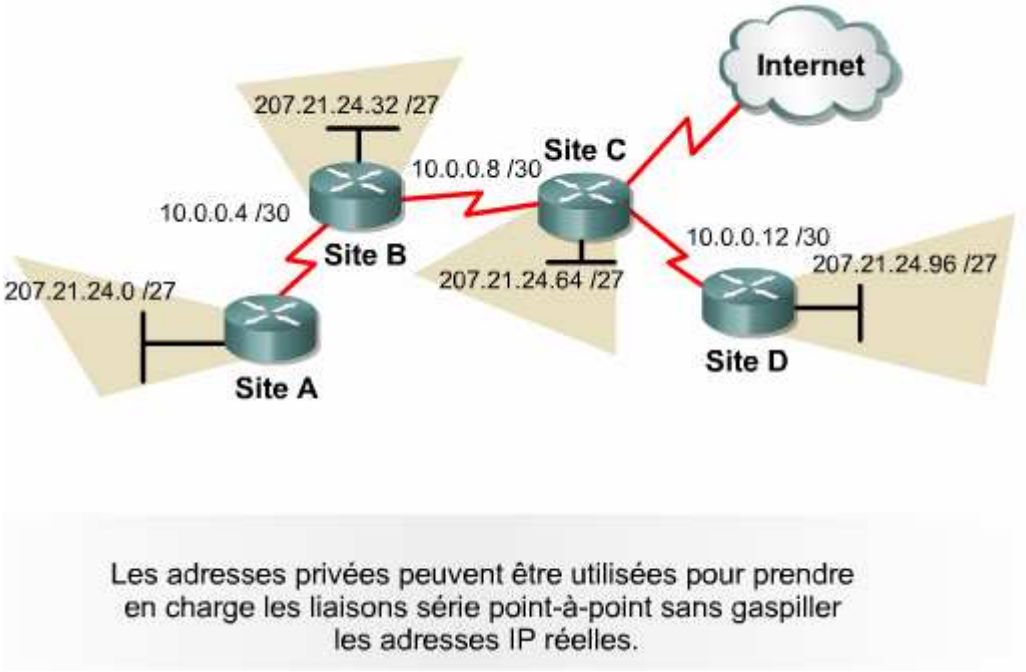
- élaboration du routage CIDR (*Classless interdomain routing*)

- élaboration de la norme IPv6.
- Utilisation des adresses privées.

La spécification RFC 1918 réserve trois blocs d'adresses IP pour une utilisation ***privée*** et interne :

Classe	Plage d'adresses internes RFC 1918
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

Les adresses IP privées peuvent être mélangées aux adresses publiques.



Les adresses privées peuvent être utilisées pour prendre en charge les liaisons série point-à-point sans gaspiller les adresses IP réelles.

La connexion d'un réseau à Internet par le biais d'adresses publiques nécessite la conversion des adresses privées en adresses publiques. Ce processus de conversion est appelé «***NAT***» (*Network Address Translation*).

Introduction aux sous réseaux :

Le découpage d'un réseau en sous-réseaux implique l'utilisation du masque de sous-réseau afin de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces.

Pour créer une adresse de sous-réseau, l'administrateur réseau emprunte des bits au champ d'hôte et les désigne comme champ de sous-réseau.

- Le nombre minimal de bits pouvant être empruntés est deux.

- Le nombre maximal de bits pouvant être empruntés est égal à tout nombre laissant au moins deux bits disponibles pour le numéro d'hôte.

Comparaison entre IPv4 et IPv6 :

Dans les années 80, la stratégie d'adressage proposée par la version IPv4 s'avérait relativement évolutive. Néanmoins, elle ne réussit pas à satisfaire les exigences liées à l'attribution des adresses.

Les adresses de classe A et B représentent 75% de l'espace d'adresses IPv4. Toutefois, moins de 17 000 organisations peuvent recevoir un numéro de réseau de classe A ou B.

Le nombre d'adresses réseau de classe C est nettement plus important que celui des adresses de classe A et B, bien qu'il ne représente que 12,5 % des quatre milliards d'adresses IP disponibles.

Dès 1992, le groupe IETF (Internet Engineering Task Force) a identifié deux problèmes :

- La diminution inquiétante des adresses réseau IPv4 disponibles.
- La hausse importante et rapide du volume des tables de routage d'Internet.

IPv6 encode les adresses sur ***128 bits*** au lieu de 32 (en utilisant des nombres hexadécimaux), ce qui porte le nombre d'adresses possibles à 340 x 10^{36}. Cette version devrait ainsi couvrir l'intégralité des besoins en communication pour les années à venir.

Afin de faciliter la lecture des adresses, il est possible d'omettre les zéros de tête dans chaque champ. Le champ «0003» est écrit «3». La représentation abrégée IPv6 de 128 bits consiste en huit nombres de 16 bits, représentés par quatre chiffres hexadécimaux.

Obtention d'une adresse Internet :

Un hôte réseau doit se procurer une adresse unique mondialement afin de se connecter à Internet. Le routeur n'utilise pas l'adresse MAC pour transmettre des données au-delà du réseau local.

Les administrateurs réseau font appel à deux méthodes différentes pour affecter les adresses IP. Il s'agit des méthodes **statique** et **dynamique**.

Adressage statique :

L'attribution statique convient particulièrement aux réseaux de petite taille qui subissent peu de changements. L'administrateur système effectue manuellement les opérations d'affectation et de suivi des adresses IP pour chaque hôte.

Le serveur, les imprimantes et les routeurs doivent être obligatoirement doté d'une adresse statique.

Attribution d'une adresse IP à l'aide du protocole RARP

Le protocole ***RARP*** associe des adresses MAC connues à des adresses IP.

Le protocole RARP permet à l'équipement de lancer une requête afin de connaître son adresse IP (dans le cas d'une station sans disque dur par exemple).

Les requêtes RARP sont diffusées sur le LAN et c'est le serveur RARP, habituellement un routeur, qui y répond.

Structure d'une requête ARP/RARP :

0 - 15 bits		16 - 31 bits
Type de matériel		Type de protocole
HLen (1 octet)	PLen (1 octet)	Opération
AM expéditeur (octets 1 - 4)		
AM expéditeur (octets 5 - 6)		AP expéditeur (octets 1 - 2)
AP expéditeur (octets 3 - 4)		AM cible (octets 1 - 2)
AM cible (octets 3 - 6)		
AP cible (octets 1 - 4)		
Structure de l'en-tête RARP		

Champ	Description
Type de matériel	Spécifie un type d'interface matérielle pour lequel l'expéditeur attend une réponse.
Type de protocole	Spécifie le type d'adresse de protocole de haut niveau fourni par l'expéditeur.
HLen	Longueur de l'adresse matérielle
PLen	Longueur de l'adresse de protocole
Opération	Les valeurs sont les suivantes : 1 Requête ARP 2 Réponse ARP 3 Requête RARP 4 Réponse RARP 5 Requête RARP dynamique 6 Réponse RARP dynamique 7 Erreur RARP dynamique 8 Requête InARP 9 Réponse InARP
@ Matériel de l'expéditeur	Longueur en Octet HLen
@ de Protocole de l'expéditeur	Longueur en Octet PLen
@ Matériel cible	Longueur en Octet HLen
@ Protocole cible	Longueur en Octet PLen

Exemple :

Requête RARP :

En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	3
FE:ED:F9:23:44:EF	FE:ED:F9:23		
Adresse MAC de destination	44:EF		non défini
FF:FF:FF:FF:FF:FF	non défini		FF:FF
Champ Type	FF:FF:FF:FF		
0X8035 (Ethernet)	non défini		

Réponse RARP :

En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	4
FE:ED:F9:65:33:3A	FE:ED:F9:23		
Adresse MAC de destination	44:EF		192.168
FE:ED:F9:23:44:EF	10.36		FE:ED
Champ Type	F9:65:33:3A		
0X8035 (Ethernet)	192.168.10.98		

Attribution d'une adresse IP à l'aide du protocole BOOTP

Le protocole ***BOOTP*** *(Bootstrap Protocol)* fonctionne dans un environnement client-serveur et ne requiert qu'un seul échange de paquet pour obtenir des informations sur le protocole IP (@IP, @routeur, @serveur …).

Le protocole BOOTP permet à un administrateur réseau de créer un fichier de configuration qui définit les paramètres de chaque équipement. L'administrateur doit ajouter les hôtes et tenir à jour la base de données (pas dynamique 100%).

BOOTP utilise la couche UDP pour transporter les messages.

Lorsqu'un client envoie un message BOOTP, le serveur BOOTP place son adresse IP dans le champ source et une adresse de broadcast dans le champ de destination. Cela permet de récupérer le paquet de réponse BOOTP au niveau de la couche transport en vue de son traitement. Seul un broadcast sera acheminé puisque le client ne connaît pas son adresse IP.

Structure d'une requête BOOTP :

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 octets)			
Secondes (2 octets)		Non utilisé	
Ciaddr (4 octets)			
Yiaddr (4 octets)			
Siaddr (4 octets)			
Giaddr (4 octets)			
Chaddr (16 octets)			
Nom d'hôte du serveur (64 octets)			
Nom du fichier de démarrage (128 octets)			
Zone spécifique du fournisseur (64 octets)			

Structure des messages BOOTP

Champ	Description
Op	Code des messages (BOOTREQUEST ou BOOTREPLY)
Htype	Type d'adresse matérielle.
HLen	Longueur de l'adresse matérielle
Hops	Utilisé par le serveur pour envoyer les requêtes à un autre réseau
Xid	ID de la transaction
Secs	Secondes écoulées lors du processus.
Ciaddr	Adresse IP du client
Yiaddr	Votre adresse IP (Client)
Siaddr	@ IP du serveur servant dans le bootstrap.
Giaddr	@ IP de l'agent de relais
Chaddr	Adresse matérielle du client
Server Host Name	Le serveur qui doit fournir les informations BOOTP
Boot File Name	Fichier de démarrage suivant le SE utilisé
Vendor Specific Area	Informations facultatives sur le fournisseur.

Exemple :

Requête BOOTP :

En-tête de trame	En-tête du paquet	1	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:23:44:EF	Inconnu	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Champ Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Réponse BOOTP :

En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Champ Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

Gestion des adresses IP à l'aide du protocole DHCP

Le protocole ***DHCP*** *(Dynamic Host Configuration Protocol)* a été proposé pour succéder au protocole BOOTP. Contrairement au protocole BOOTP, le protocole DHCP permet à un hôte d'obtenir une adresse IP de *manière dynamique* sans que l'administrateur réseau ait à définir un profil pour chaque équipement. Avec le protocole DHCP, il suffit qu'une plage d'adresses IP soit définie.

Le protocole DHCP dispose d'un avantage majeur sur le protocole BOOTP, car il permet aux utilisateurs d'être mobiles.

Le protocole DHCP offre une relation «***un à plusieurs***» pour les adresses IP.

Structure d'une requête DHCP :

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 octets)			
Secondes (2 octets)		Indicateurs (2 octets)	
Ciaddr (4 octets)			
Yiaddr (4 octets)			
Siaddr (4 octets)			
Giaddr (4 octets)			
Chaddr (16 octets)			
Nom d'hôte du serveur (64 octets)			
Nom du fichier de démarrage (128 octets)			
Zone spécifique du fournisseur (variable)			
Structure des messages DHCP			

Elle est presque semblable à la requête BOOTP

Protocole ARP (Address Resolution Protocol)

Dans un réseau TCP/IP, un paquet de données doit contenir une adresse MAC de destination et une adresse IP de destination. Si l'une ou l'autre est manquante, les données qui se trouvent au niveau de la couche 3 ne sont pas transmises aux couches supérieures.

Les «***tables ARP***» sont stockées dans la mémoire RAM, où les informations en mémoire cache sont mises à jour automatiquement dans chaque équipement (correspondance @IP & @MAC pour les stations du même domaine de Broadcast).

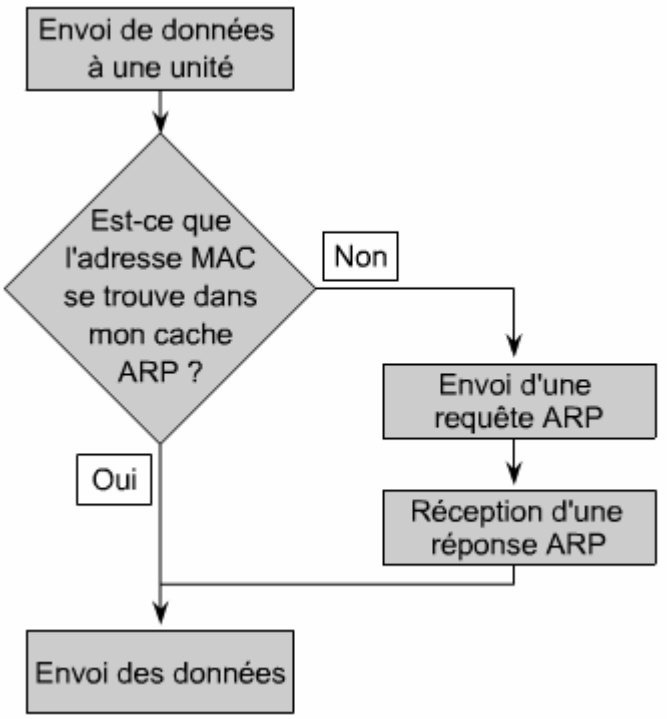
Méthodes pour obtenir les adresses MAC :

- la première consiste à surveiller le trafic existant sur le segment du réseau local et enregistrer les adresses source IP et MAC du datagramme dans une table ARP.
- La deuxième consiste à diffuser une requête ARP.

Les routeurs ne transmettent pas les paquets de broadcast. Lorsque la fonction est activée, le routeur exécute une requête via ***Proxy ARP***.

Proxy ARP est une variante du protocole ARP. Dans cette variante, un routeur envoie une réponse ARP, qui contient l'adresse MAC dont l'adresse IP n'appartient pas à la plage d'adresses du sous-réseau local.

Une autre solution pour envoyer des données à l'adresse d'un équipement situé sur un autre segment du réseau, consiste à configurer une passerelle par défaut.



Module 10

Notions de base sur le routage & les sous-réseaux

Protocole routé et protocole routable :

Un protocole est un ensemble de règles qui définit le mode de communication entre les différents ordinateurs sur les réseaux.

Un protocole décrit les éléments suivants:

- Le format de message requis.
- La manière dont les ordinateurs doivent échanger les messages d'activités spécifiques.

Un protocole routé permet au routeur de transmettre des données entre les nœuds de différents réseaux.

Un protocole routable doit impérativement permettre d'attribuer un numéro de réseau et un numéro d'hôte à chacune des machines.

→ IPX ne requiert que le numéro de réseau, il utilise l'adresse MAC de l'hôte à la place de son numéro.

→ IP, nécessite que l'adresse comporte une partie réseau et une partie hôte. Dans ce cas, un masque de réseau est nécessaire pour différencier ces deux numéros.

L'objectif du masque de réseau est de permettre à des groupes d'adresses IP séquentielles d'être traités en tant qu'une seule et même unité.

→ Exemples des protocoles routables : IP, IPX (*Internetwork Packet Exchange*), AppleTalk, DECnet, Banyan VINES & XNS (Xerox Network Systems) protocoles prennent en charge la couche 3.
→ NetBEUI est un protocole non routable, il ne prend pas en charge la couche 3.

IP comme protocole routé :

IP est le système d'adressage hiérarchique des réseaux le plus largement utilisé. C'est un protocole non orienté connexion, peu fiable et axé sur l'acheminement au mieux.

Au niveau de la couche réseau, les données sont encapsulées dans des paquets. Ces paquets sont appelés des datagrammes.

IP détermine le contenu de l'en-tête du paquet IP, qui contient les informations d'adressage sans préoccuper du contenu des données proprement dit.

Propagation d'un paquet et commutation au sein d'un routeur :

Les unités de données de la couche ***2***, ou trames, sont destinées à l'adressage local, tandis que les unités de données de la couche ***3***, ou paquets, sont destinées à l'adressage de bout en bout.

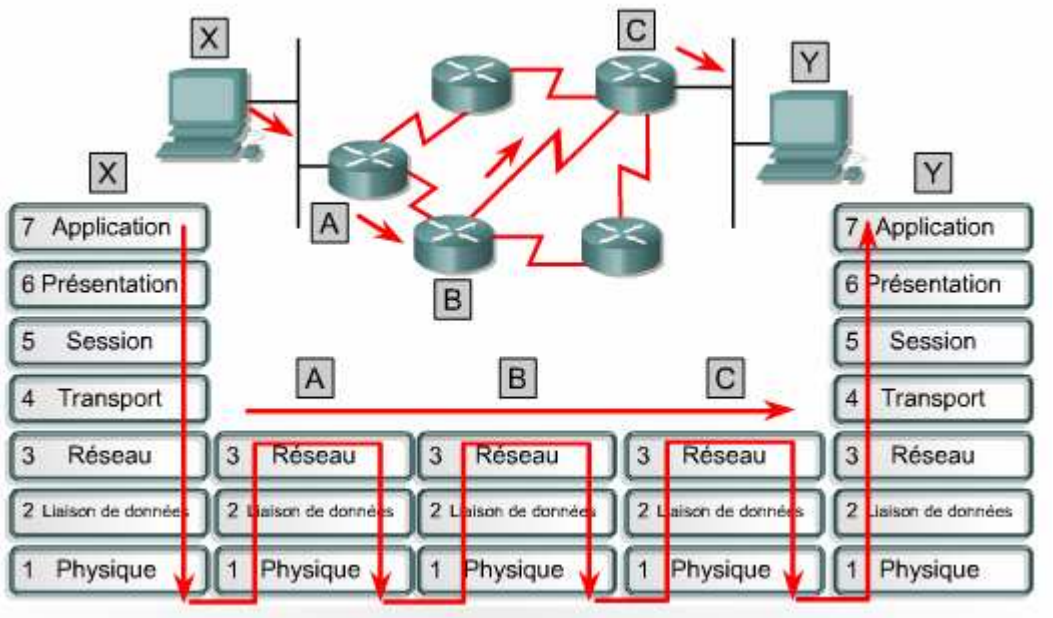
Quel que soit le type d'adressage de couche 2 utilisé, les trames sont conçues pour circuler dans un domaine de broadcast de couche 2.

Lorsque les données sont envoyées vers une unité de couche ***3***, les informations de couche ***2*** sont modifiées.

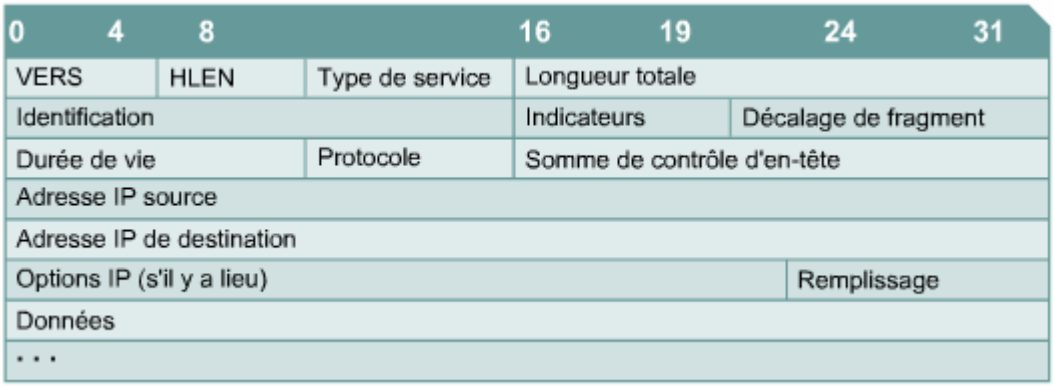
Lorsqu'une interface du routeur reçoit une trame, elle en extrait l'adresse MAC de destination. Cette adresse est vérifiée afin de savoir si la trame est destinée directement à l'interface du routeur ou s'il s'agit d'un broadcast. Dans les deux cas, la trame est acceptée. Si elle est destinée à une autre unité du domaine de collision, elle est rejetée.

Lorsqu'elle est acceptée, les informations de code de redondance cyclique (CRC, Cyclic Redundancy Check) sont extraites de son en-queue. Le CRC est calculé pour vérifier l'intégrité des données de la trame.

Si la vérification échoue, la trame est rejetée. Si elle réussit, l'en-queue et l'en-tête de trame sont retirés, et le paquet est transmis à la couche 3. Ce paquet est ensuite examiné pour savoir s'il est destiné au routeur ou s'il doit être acheminé vers un autre équipement de l'interréseau. Si l'adresse IP de destination correspond à l'un des ports du routeur, l'en-tête de la couche 3 est retiré et les données sont transmises à la couche 4. Dans le cas contraire, l'adresse est comparée à la table de routage. Si une correspondance est établie ou s'il existe un chemin par défaut, le paquet est envoyé à l'interface indiquée dans l'entrée mise en correspondance de la table de routage. Lors de la commutation du paquet vers l'interface de sortie, une nouvelle valeur CRC est ajoutée en en-queue de trame et l'en-tête de trame approprié est ajouté au paquet. La trame est ensuite transmise au domaine de broadcast suivant et continue sa route jusqu'à la destination finale.



Anatomie d'un paquet IP



0 4	8		16 19	24 31
VERS	HLEN	Type de service	Longueur totale	
Identification			Indicateurs	Décalage de fragment
Durée de vie		Protocole	Somme de contrôle d'en-tête	
Adresse IP source				
Adresse IP de destination				
Options IP (s'il y a lieu)				Remplissage
Données				
. . .				

- **Version:** le champ Version (4 bits) contient le numéro 4 s'il s'agit d'un paquet IPv4 ou le numéro 6 s'il s'agit d'un paquet IPv6.
- **Longueur d'en-tête IP (HLEN):** indique la longueur de l'en-tête du datagramme en mots de 32 bits. Ce champ représente la longueur totale des informations d'en-tête et inclut les deux champs d'en-tête de longueur variable.
- **Type de service (ToS):** ce champ codé sur 8 bits indique le niveau d'importance attribué par un protocole de couche supérieure particulier.
- **Longueur totale (16 bits):** ce champ spécifie la taille totale du paquet en octets, données et en-tête inclus.
- **Identification (16 bits):** ce champ comporte le numéro de séquence.
- **Drapeaux (3 bits):** champ dans lequel les deux bits de poids faible contrôlent la fragmentation. Un bit indique si le paquet peut être fragmenté ou non, et l'autre si le paquet est le dernier fragment d'une série de paquets fragmentés.
- **Décalage de fragment (13 bits):** champ permettant de rassembler les fragments du datagramme. Il permet au champ précédent de se terminer sur une frontière de 16 bits.
- **Durée de vie (TTL):** champ indiquant le nombre de sauts par lesquels un paquet peut passer. Ce nombre est décrémenté à chaque passage du paquet dans un routeur. lorsque le compteur atteint zéro, le paquet est éliminé.
- **Protocole (8 bits):** indique quel protocole de couche supérieure, tel que TCP ou UDP, reçoit les paquets entrants une fois les processus IP terminés.
- **Somme de contrôle de l'en-tête (16 bits):** champ qui aide à garantir l'intégrité de l'en-tête IP.
- **Adresse source (32 bits):** champ indiquant l'adresse IP du nœud source de paquet.
- **Adresse de destination (32 bits):** champ indiquant l'adresse IP de la destination.
- **Options:** permet au protocole IP de prendre en charge diverses options, telles que la sécurité. La longueur de ce champ peut varier.
- **Remplissage:** des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP est toujours un multiple de 32 bits.
- **Données:** ce champ contient les informations de couche supérieure. Sa longueur est variable.

Protocoles de routage :

Le routage cherche le chemin le plus efficace d'une unité à une autre. Le matériel au centre du processus de routage est le routeur.

Deux fonctions principales du routeur :

- Le routeur gère les tables de routage et s'assure que les autres routeurs ont connaissance des modifications apportées à la topologie du réseau.
- Le routeur détermine la destination des paquets à l'aide de la table de routage.

Un routeur est une unité de couche réseau qui utilise une ou plusieurs métriques pour déterminer le chemin optimal par lequel acheminer le trafic réseau.

Les métriques de routage sont les valeurs qui permettent de définir le meilleur chemin.

Les phases d'encapsulation et de désencapsulation se produisent à chaque passage d'un paquet dans un *routeur*.

Routage & commutation :

Les commutateurs opèrent au niveau de la couche ***2*** du modèle OSI par contre les routeurs fonctionnent sur la couche ***3***.

Une autre différence entre les réseaux routés et commutés réside dans le fait que ces derniers ne bloquent pas les broadcasts. Du fait, les routeurs offrent une meilleure sécurité et un meilleur contrôle de la bande passante que les commutateurs.

Fonctions	Routeur	Commutateur
Vitesse	Lente	Rapide
Couches OSI	Couche 3	Couche 2
Adressage utilisé	IP	MAC
Broadcasts	Bloqués	Transmis
Sécurité	Élevée	Faible

Chaque ordinateur et chaque interface de routeur gèrent une table ARP pour la communication de couche 2. La table ARP n'est utile que pour le domaine de broadcast auquel elle est connectée. Le routeur est également doté d'une table de routage qui lui permet d'acheminer les données hors du domaine de broadcast. Chaque entrée de table ARP contient une paire d'adresses IP-MAC.

Lorsqu'un hôte possède des données pour une adresse IP non locale, il envoie la trame au routeur le plus proche. Ce routeur est également appelé « ***passerelle par défaut*** ». L'hôte se sert de l'adresse MAC du routeur comme adresse MAC de destination.

Protocoles routé & Protocoles de routage :

Les protocoles routés ou routables sont utilisés au niveau de la couche réseau afin de transférer les données d'un hôte à l'autre via un routeur.

Les protocoles de routage permettent aux routeurs de choisir le meilleur chemin possible pour acheminer les données de la source vers leur destination.

Les protocoles de ***routage*** permettent aux routeurs d'acheminer les protocoles ***routés***.

Les fonctions du protocole de routage :

- Il fournit les processus utilisés pour partager les informations d'acheminement.
- Il permet aux routeurs de mettre à jour et de gérer les tables de routage.

Les protocoles de routage prenant en charge le protocole routé **IP** sont par exemple les protocoles *RIP*, *IGRP*, *OSPF*, *BGP* et *EIGRP*.

Détermination du chemin :

Ce processus permet au routeur de comparer l'adresse de destination aux routes disponibles dans sa table de routage et de choisir le meilleur chemin possible.

{ Les chemins configurés manuellement par l'administrateur réseau : «***routes statiques***».
{ Le routeur a acquis à l'aide d'un protocole de routage «***routes dynamiques***».

Chaque routeur rencontré sur le chemin du paquet est appelé un saut.

Les routeurs vont prendre leurs décisions en fonction de la ***charge***, de ***la bande passante***, du ***délai***, du ***coût*** et de la ***fiabilité*** d'une liaison de réseau.

Processus de sélection du meilleur chemin :

- Le routeur compare l'adresse IP du paquet reçu avec ses tables IP.
- Il extrait l'adresse de destination du paquet.
- Le masque de la première entrée dans la table de routage est appliqué à l'@ de destination.
- La destination masquée est comparée avec l'entrée de la table de routage.
- Si une correspondance est établie, le paquet est transmis au port associé.
- Si aucune correspondance n'est établie, l'entrée suivante de la table est examinée.
- Si le paquet ne correspond à aucune des entrées de la table, le routeur recherche l'existence d'une route par défaut.
- Si une route par défaut a été définie, le paquet est transmis au port qui lui est associé.
- Si aucun chemin par défaut n'existe, le paquet est éliminé. Un message est alors souvent envoyé à l'unité émettrice des données pour signaler que la destination n'a pu être atteinte.

Tables de routage :

Les routeurs conservent les informations suivantes dans leurs tables de routage :

- ***Type de protocole*:** cette information identifie le type de protocole de routage qui a créé chaque entrée.
- ***Associations du saut suivant*:** indique au routeur que la destination lui est directement connectée, ou qu'elle peut être atteinte par le biais d'un autre routeur appelé le «saut suivant» vers la destination finale.
- ***Métrique de routage*:** les métriques utilisées varient selon les protocoles de routage
- ***Interfaces de sortie*:** cette information désigne l'interface à partir de laquelle les données doivent être envoyées pour atteindre leur destination finale.

Algorithmes et métriques de routage

Les algorithmes utilisés pour définir le port auquel envoyer un paquet diffèrent selon les protocoles de routage.

Objectifs des protocoles de routage:

- ***Optimisation***: capacité d'un algorithme de routage à sélectionner le meilleur chemin.
- ***Simplicité*** et ***réduction du temps-système***: plus l'algorithme est simple et plus il sera traité efficacement par le processeur et la mémoire du routeur.
- ***Efficacité*** et ***stabilité***: capacité de fonctionner correctement dans des circonstances inhabituelles ou imprévues, comme les défaillances de matériels, les surcharges et les erreurs de mise en œuvre.
- ***Flexibilité***: capacité de s'adapter rapidement à toutes sortes de modifications du réseau, touchant par exemple la disponibilité et la mémoire du routeur, la bande passante ou le délai réseau.
- ***Rapidité de convergence***: la convergence est le processus par lequel tous les routeurs s'entendent sur les routes disponibles. Une convergence lente des algorithmes de routage peut empêcher la livraison des données.

Généralement, les valeurs métriques faibles indiquent le meilleur chemin

Les métriques les plus communément utilisées par les protocoles de routage :

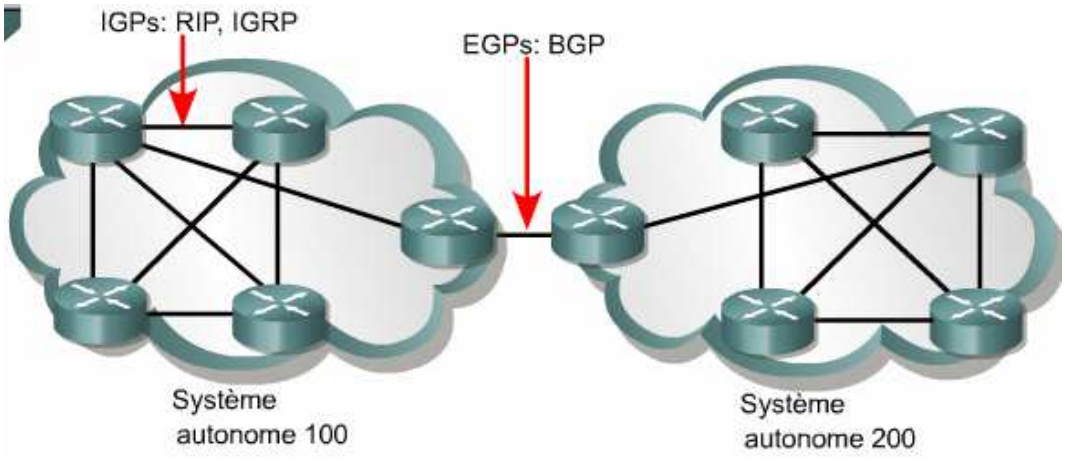
- **Bande passante:** la bande passante représente la capacité de débit d'une liaison.
- **Charge:** la charge est la quantité de trafic sur une ressource réseau telle qu'un routeur ou une liaison.
- **Délai:** Il dépend de la bande passante des liaisons intermédiaires, de la quantité de données pouvant être temporairement stockées sur chaque routeur, de la congestion du réseau et de la distance physique.
- **Fiabilité:** la fiabilité se rapporte habituellement au taux d'erreurs de chaque liaison du réseau.
- **Nombre de sauts:** le nombre de sauts est le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination.

- **Tops:** délai d'une liaison de données utilisant les tops d'horloge d'un PC IBM, un top d'horloge correspondant environ à 1/18 seconde.
- **Coût:** le coût est une valeur arbitraire, généralement basée sur la bande passante, une dépense monétaire ou une autre mesure, attribuée par un administrateur réseau.

Protocoles IGP & EGP :

Un système autonome est un réseau ou un ensemble de réseaux placés sous un même contrôle administratif, tel que le domaine *cisco.com*.

Il existe deux familles de protocoles de routage : les protocoles ***IGP*** (*Interior Gateway Protocol*) et les protocoles ***EGP*** (*Exterior Gateway Protocol*).



Les protocoles IGP acheminent les données au sein d'un système autonome :

- Des protocoles ***RIP*** et ***RIPv2***.
- Du protocole ***IGRP***.
- Du protocole ***EIGRP***.
- Du protocole ***OSPF***.
- Du protocole ***IS-IS*** (Intermediate System-to-Intermediate System).

Les protocoles EGP acheminent les données entre les systèmes autonomes.

- Le protocole ***BGP***.

État de liens et vecteur de distance :

Les protocoles IGP peuvent être subdivisés en *protocoles à vecteur de distance* et en *protocoles à état de liens*.

La méthode de ***routage à vecteur de distance*** (routage par rumeur) détermine la direction (vecteur) et la distance vers n'importe quelle liaison de l'interréseau (mises à jour périodiques)

Exemples de protocoles à vecteur de distance :

- *Routing Information Protocol* ***(RIP):*** le plus utilisé sur Internet..
- *Interior Gateway Routing Protocol* ***(IGRP):*** protocole développé par Cisco
- *Enhanced IGRP* ***(EIGRP):*** propriété de Cisco, «protocole hybride symétrique».

Les protocoles à ***état de liens*** ont pour avantage de répondre rapidement aux moindres changements sur le réseau en envoyant des mises à jour déclenchées uniquement après qu'une modification soit survenue.

Exemples de protocoles à vecteur de distance :

- ***OSPF*** *(Open Shortest Path First)*
- ***IS-IS*** (*Intermediate System-to-Intermediate System*)

Protocoles de routages :

Le protocole RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme métrique pour déterminer le meilleur chemin.

La version 1 (***RIPv1***) n'incluant pas les informations de masque de sous-réseau dans les mises à jour de routage, tous les équipements du réseau doivent nécessairement utiliser le même masque de sous-réseau. On parle dans ce cas de routage par classes.
La version 2 (***RIPv2***) fournit un routage par préfixe et envoie les informations de masque de sous-réseau dans ses mises à jour de routage. On parle ici de routage sans classe.

Le protocole IGRP est un protocole de routage à vecteur de distance mis au point par Cisco. Il peut sélectionner le chemin disponible le plus rapide en fonction du délai, de la bande passante, de la charge et de la fiabilité (utilise uniquement le routage par classes)

EIGRP est un protocole développé par Cisco. Il constitue une version perfectionnée du protocole IGRP. Il offre de meilleures performances d'exploitation comme une convergence plus rapide et une bande passante moins surchargée (à vecteur de distance avancé)

Le protocole OSPF est un protocole de routage à état de liens mis au point par l'IETF (*Internet Engineering Task Force*) en 1988 (très évolutif)

Le protocole IS-IS est un protocole de routage à état de liens utilisé pour les protocoles routés autres qu'IP.

Integrated IS-IS est une extension de IS-IS, qui prend en charge plusieurs protocoles routés dont IP.

Le protocole BGP (*Border Gateway Protocol*) est un exemple de protocole EGP. Il permet l'échange d'informations de routage entre systèmes autonomes tout en garantissant une sélection de chemins exempts de boucle (métrique selon les stratégies de réseau)

BGP4 est la première version de BGP à prendre en charge le routage interdomaine sans classes (CIDR) et le regroupement de routes.

Mécanisme de découpage en sous réseau :

Classes d'adresses réseau IP :

Classe A	Réseau	Hôte		
Octet	1	2	3	4

Classe B	Réseau		Hôte	
Octet	1	2	3	4

Classe C	Réseau			Hôte
Octet	1	2	3	4

Classe D	Hôte			
Octet	1	2	3	4

Pour effectuer un découpage en sous-réseaux, des bits de la partie hôte doivent être réattribués au réseau. Cette opération est souvent appelée « ***emprunt*** » de bits.

Exemple :

Adresse réseau de classe C 192.168.10.0
11000000.10101000.00001010.00000000 N . N . N . H
11000000.10101000.00001010.00000000 N . N . N . sN H Dans cet exemple, trois bits ont été alloués pour désigner le sous-réseau.

Avantages du découpage en sous-réseaux :

- faciliter la gestion du réseau
- confiner le broadcast
- garantir une certaine sécurité sur le réseau LAN.

Détermination de l'adresse d'un masque de sous-réseau :

Le nombre de bits à sélectionner dans le processus de découpage en sous-réseaux dépend du nombre maximal d'hôtes requis par sous-réseau.

Quelle que soit la classe d'adresse IP, les deux derniers bits du dernier octet ne doivent jamais être attribués au sous-réseau. Ces bits constituent les deux derniers bits significatifs.

Le masque de sous-réseau apporte au routeur l'information dont il a besoin pour déterminer le réseau et le sous-réseau auxquels un hôte donné appartient

Le masque de sous-réseau est créé en utilisant des 1 dans les positions du réseau.

255.255.255.224 Au format de ***barre oblique***, ce masque est représenté par /27. Le nombre situé après la barre oblique correspond au nombre total de bits utilisés pour les parties réseau et sous-réseau.

$(2^{\text{nombre de bits empruntés}}) - 2 =$ sous-réseaux utilisables

La soustraction correspond aux deux adresses réservées que sont l'adresse du réseau et l'adresse de broadcast du réseau.

$(2^{\text{nombre de bits hôtes restants}}) - 2 =$ hôtes utilisables

Moins deux (pour les adresses réservées que sont l'adresse du sous-réseau et l'adresse de broadcast du sous-réseau).

Calcul du sous-réseau via l'opération AND

L'opération ***AND logique*** s'agit d'un processus binaire par lequel le routeur calcule l'ID de sous-réseau d'un paquet entrant.

L'opération AND est appliquée entre l'adresse IP et à le masque du sous-réseau avec pour résultat l'ID du sous-réseau.

Adresse du paquet	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Masque	255.255.255.224	11111111.11111111.11111111.11100000
ID du sous-réseau	201.10.11.64	11001001.00001010.00001011.01000000

Module 11

Couche transport & couche application du protocole TCP/IP

Introduction à la couche transport :

La couche transport a pour but :

- D'acheminer les données de la source à la destination. « TCP ou UDP »
- De contrôler le flux de ces données. « Fenêtrage »
- De garantir la fiabilité de ces données. « Accusés de réception »

Analogie :

Imaginez une personne qui apprend une langue étrangère pour la première fois (il faut répéter les mots, parler lentement …)

Services de transport de base :

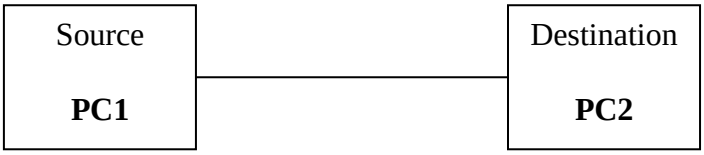
- *Segmentation des données* d'application de couche supérieure.
- *Établissement d'une connexion* de bout en bout.
- *Transport des segments* d'un hôte d'extrémité à un autre.
- *Contrôle du flux* assuré par les fenêtres glissantes.
- *Fiabilité* assurée par les numéros de séquence et les accusés de réception.

Contrôle de flux :

Le ***contrôle de flux*** permet d'éviter le dépassement de capacité des mémoires tampons d'un hôte de destination. Pour ce faire, TCP met en relation les hôtes source et de destination qui conviennent alors d'un taux de transfert des données acceptable.

Sinon, le destinataire va rejeter les segments.

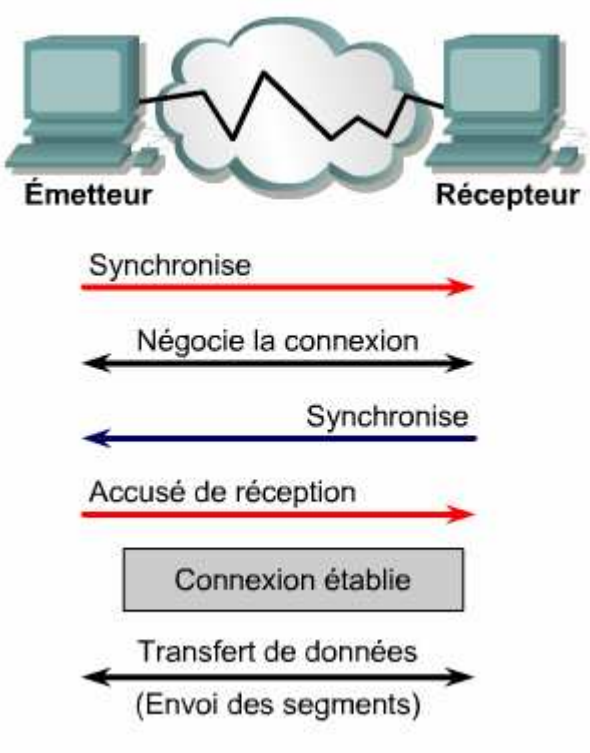
Établissement, maintenance et fermeture de session



Lorsque l'ordinateur PC1 veut envoyer de l'information à l'ordinateur PC2, il doit tout d'abord établir une session avec ce dernier au niveau de la couche transport.

- Premièrement, PC1 envoie un message de synchronisation à PC2.
- PC2 reçoit le message, et négocie la connexion avec PC1, ensuite il va envoyer à son tour un message de synchronisation des paramètres négociés.
- PC1 envoie finalement un accusé de réception comme quoi la connexion est établit.
- A ce moment là, les deux ordinateurs peuvent échanger les données d'une façon bidirectionnelle.

Une fois le transfert des données terminé, PC1 envoie un signal indiquant la fin de la transmission. PC2 accuse la réception et la connexion se termine.



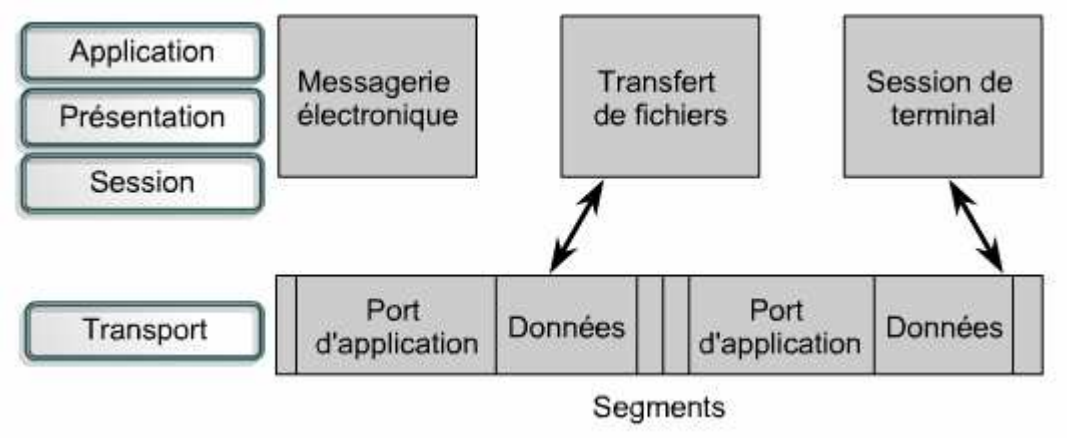
La congestion peut se produire dans deux situations :

- Lorsqu'un ordinateur génère un trafic dont le débit est plus rapide que la vitesse de transfert du réseau.
- Lorsque plusieurs ordinateurs doivent envoyer simultanément des datagrammes à une même destination.

Pour éviter la perte des données, le processus TCP de PC2 envoie un indicateur «***non prêt***» à PC1, afin que ce dernier arrête de transmettre. Lorsque PC2 peut accepter de nouvelles données, il envoie l'indicateur de transport «***prêt***» à PC1 qui reprend alors la transmission des segments.

Le multiplexage :

Les applications envoient des segments de données suivant la méthode du premier arrivé, premier servi. Ce qui est important, c'est que plusieurs applications peuvent partager la même connexion de transport (ça veut dire qu'on peut utiliser deux services d'application ou plus en ouvrant une seule fois la connexion. On parle alors de *multiplexage des conversations de couche supérieure*.



Échange en trois étapes

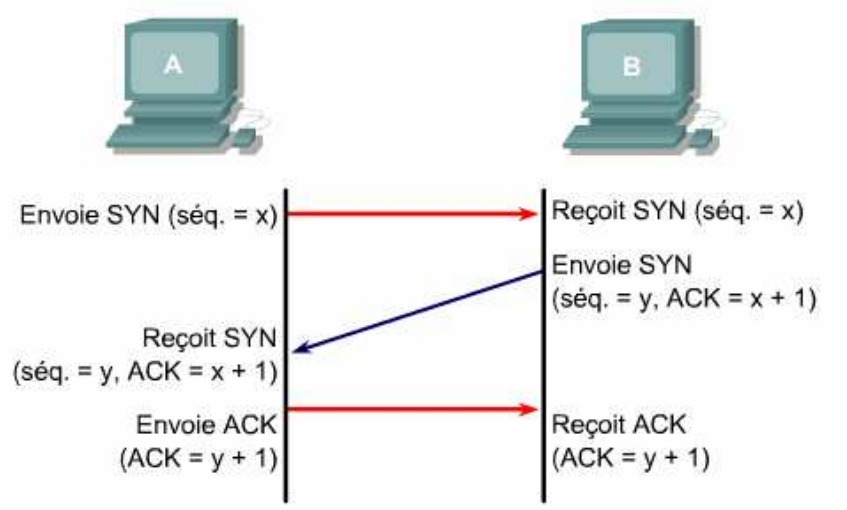
Pour établir une connexion, les deux hôtes doivent synchroniser leurs numéros de séquence initiaux (**ISN** – Initial Sequence Number).

La synchronisation s'effectue via un échange de segments transportant un bit de contrôle SYN et les numéros de séquence initiaux.

La séquence de la synchronisation est la suivante :

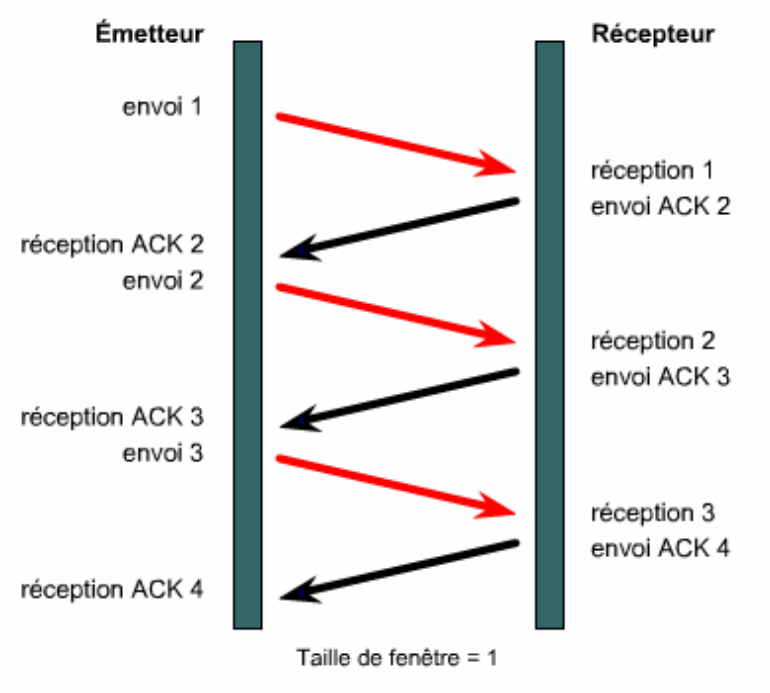
1. L'hôte émetteur (A) initie une connexion *en envoyant un paquet SYN* à l'hôte récepteur (B) indiquant que son numéro de séquence initial ISN = X.
2. B reçoit le paquet, enregistre que la séquence de A = X, répond par un accusé de réception de X + 1 et indique que son numéro de séquence ISN = Y. L'accusé X + 1 signifie que l'hôte B a reçu tous les octets jusqu'à X inclus et qu'il attend l'arrivée de X + 1.
3. L'hôte A reçoit le paquet de B, apprend que la séquence de B est Y et répond par un accusé de Y + 1, qui met fin au processus de connexion:

Cet échange est un ***échange en trois étapes***.

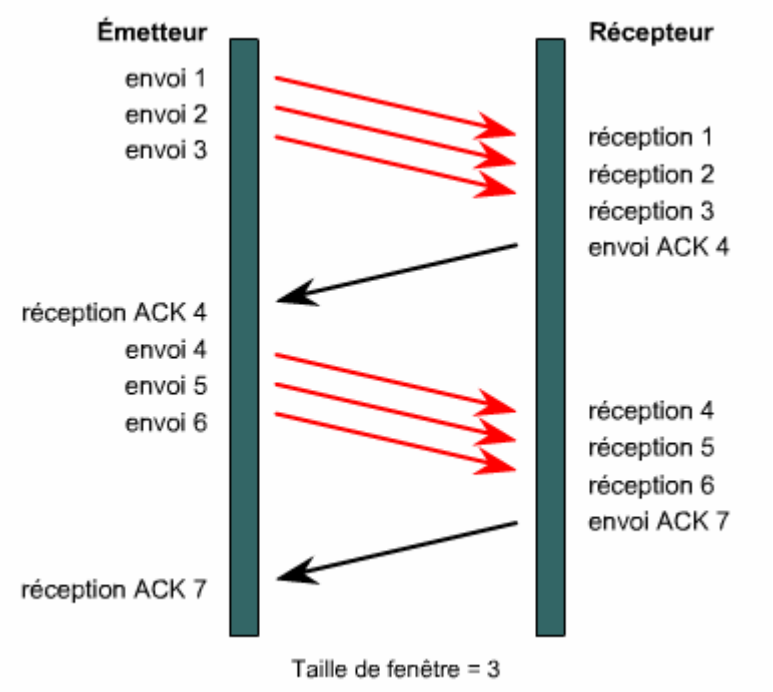


Fenêtrage :

Le ***fenêtrage*** est une solution simple consiste, pour le destinataire, à accuser une réception à chaque transmission d'un nombre bien précis des segments.



Chaque protocole orienté connexion utilise une *taille de fenêtre* (la taille de la fenêtre indique le nombre des segments que l'hôte de destination est prêt à recevoir).



Fenêtre glissante

TCP utilise des accusés de réception prévisionnels. Cela signifie que le numéro de l'accusé indique le paquet suivant attendu.

Le fenêtrage fait référence au fait que la taille de la fenêtre est négociée de manière dynamique pendant la session TCP. Il constitue un mécanisme de contrôle de flux.

Après qu'une certaine quantité de données a été transmise, la machine destination signale une taille de fenêtre à l'hôte source.

Chaque segment est numéroté avant la transmission pour pouvoir réassembler correctement les segments au niveau de la destination. (***Numéros des segments***)

Protocole TCP : (Transfert Control Protocol)

TCP est un protocole orienté connexion de la couche transport, qui assure une transmission fiable des données en full duplex.

Les protocoles utilisant TCP sont les suivants: FTP, HTTP, SMTP, Telnet

Structure d'un segment TCP :

Bit 0	Bit 15 Bit 16	Bit 31
Port source (16)	Port de destination (16)	
Numéro de séquence (32)		
Numéro d'accusé de réception (32)		
Longueur d'en-tête (4) / Réservé (6) / Bits de Code (6)	Fenêtre (16)	
Somme de contrôle (16)	Urgent (16)	
Options (0 ou 32 le cas échéant)		
Données (variable)		

20 octets

- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Numéro de séquence:** numéro d'ordre de chaque segment.
- **Numéro d'accusé de réception:** octet TCP suivant attendu.
- **HLEN:** nombre de mots de 32 bits contenus dans l'en-tête.
- **Réservé:** champ réglé sur zéro.
- **Bits de code:** fonctions de contrôle (l'ouverture et la fermeture d'une session).
- **Fenêtre:** nombre d'octets que l'émetteur acceptera.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Pointeur d'urgence:** indique la fin des données urgentes.
- **Option:** p.ex. : la taille maximale d'un segment TCP (MSS – Maximum Segment Size)
- **Données:** données de protocole de couche supérieure.

Protocole UDP : (User Datagram Protocol)

C'est un protocole simple qui échange des datagrammes sans garantir leur bonne livraison.

UDP n'utilise ni fenêtres ni accusés de réception. La fiabilité est assurée par les protocoles de la couche application. Le protocole UDP est conçu pour les applications qui ne doivent pas assembler de séquences de segments.

Les protocoles utilisant UDP sont les suivants: TFTP, SNMP, DHCP, DNS.

Structure d'un segment UDP :

Bit 0	Bit 15 Bit 16	Bit 31
Port source (16)	Port de destination (16)	
Longueur (16)	Somme de contrôle (16)	
Données (le cas échéant)		

8 octets

Figure 12 : Structure de segment UDP

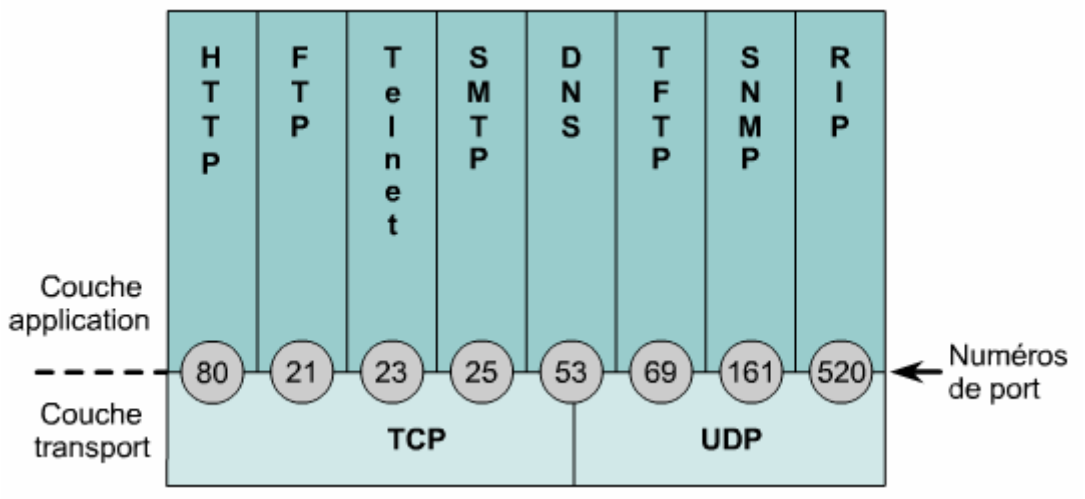
- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Longueur:** nombre d'octets de l'en-tête et des données.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Données:** données de protocole de couche supérieure.

Numéros de port TCP et UDP :

Les numéros de port servent à distinguer les différentes conversations qui circulent simultanément sur le réseau.

Les développeurs d'applications ont convenu d'utiliser les numéros de port reconnus émis par l'IANA (Internet Assigned Numbers Authority).

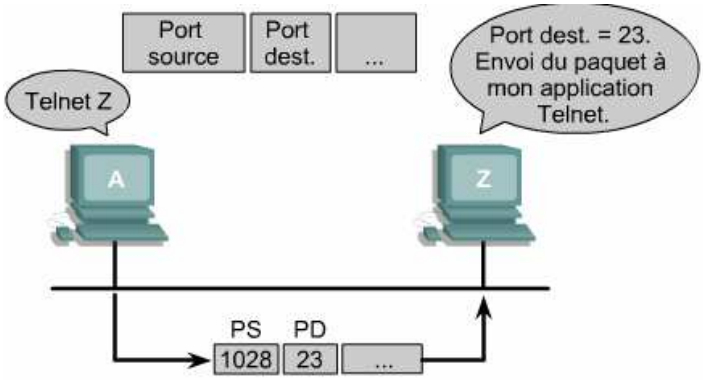
Par exemple : **FTP** fait appel aux numéros de port standard 20 et 21. Le port 20 est utilisé pour la partie « données » et le port 21 pour le « contrôle ».



Les plages attribuées aux numéros de port :

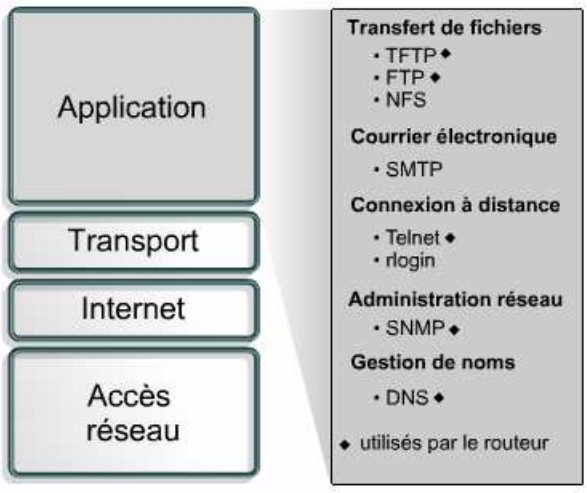
- Les numéros inférieurs à 1024 sont considérés comme des numéros de port reconnus.
- Les numéros supérieurs à 1023 sont des numéros attribués de manière dynamique.
- Les numéros de port enregistrés sont destinés à des applications spécifiques d'un fournisseur. La plupart se situent au-delà de 1024.

Les systèmes d'extrémité utilisent les numéros de port pour sélectionner l'application appropriée. L'hôte source attribue dynamiquement les numéros de port source. Ils sont toujours *supérieurs à 1023*.



Introduction à la couche application :

La couche application est responsable de la représentation, le code et le contrôle du dialogue.



DNS :

Il est difficile de retenir l'adresse IP d'un site, car l'adresse numérique n'a aucun rapport apparent avec le contenu du site. ***DNS*** permet de convertir les @IP en des noms de domaine et l'inverse.

Il existe plus de 200 domaines de niveau supérieur sur Internet, notamment :

.us – États-Unis
.fr – France
.edu – sites éducatifs
.com – sites commerciaux
…

FTP & TFTP :

FTP est un service orienté connexion fiable. L'objectif principal de ce protocole est d'échanger des fichiers dans les deux sens (importation et exportation) entre un ordinateur serveur et des ordinateurs clients en ouvrant une connexion.

TFTP est un service non orienté connexion. Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle IOS Cisco. Ce protocole, conçu pour être léger et facile à mettre en œuvre, (il ne permet pas d'afficher le contenu des répertoires ni d'assurer l'authentification des utilisateurs).

HTTP :

Le protocole ***HTTP*** (*Hypertext Transfer Protocol*) est le support du Web.

Les pages Web sont créées avec un langage de formatage appelé HTML (*HyperText Markup Language*). Le code HTML indique au navigateur comment présenter une page Web pour obtenir un aspect particulier.

Les *liens hypertexte* (ou hyperliens) facilitent la navigation sur le Web. Il peut s'agir d'un objet, d'un mot, d'une phrase ou d'une image sur une page Web.

http://	www.	cisco.com	/edu/
Indique au navigateur le protocole à utiliser.	Indique le nom de l'hôte ou le nom d'un ordinateur précis.	Représente l'entité de domaine du site Web.	Spécifie le répertoire dans lequel la page Web est située sur le serveur. Ainsi, quand aucun nom n'est spécifié, le navigateur charge la page par défaut identifiée par le serveur.

Lorsque vous tapez une adresse, Le navigateur Web examine alors le protocole pour savoir s'il a besoin d'ouvrir un autre programme, puis détermine l'adresse IP du serveur Web à l'aide du système DNS. Ensuite, les couches transport, réseau, liaison de données et physique établissent une session avec le serveur Web.

Le serveur répond à la demande en transmettant au client Web tous les fichiers texte, audio, vidéo et graphique indiqués dans la page HTML. Le navigateur client rassemble tous ces fichiers pour créer une image de la page Web et met fin à la session.

SMTP :

Les serveurs de messagerie communiquent entre eux à l'aide du protocole ***SMTP*** (*Simple Mail Transfer Protocol*) pour envoyer et recevoir des messages électroniques. Ce protocole transporte les messages au format ASCII à l'aide de TCP.

Les protocoles de client de messagerie les plus répandus sont POP3 et IMAP4, qui utilisent tous deux TCP pour transporter les données (récupérer les messages), par contre le client utilise toujours le protocole SMTP pour envoyer des messages.

Pour tester l'accès à un serveur de messagerie, établissez une connexion Telnet au port SMTP : **C:\>telnet 192.168.10.5 25**

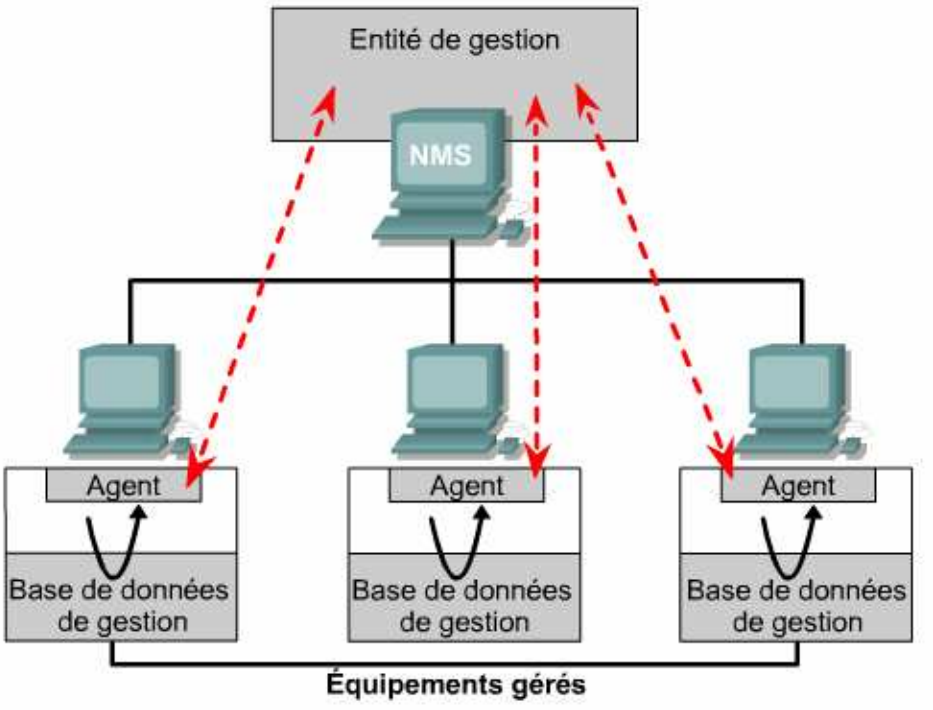
Le protocole SMTP ne propose guère d'options de sécurité et ne nécessite aucune authentification.

SNMP :

Le protocole ***SNMP*** (Simple Network Management Protocol) est un protocole qui facilite l'échange d'information de gestion entre les équipements du réseau. Il permet aux administrateurs réseau de gérer les performances du réseau, de diagnostiquer et de résoudre les problèmes.

Composants SNMP :

- *Le système d'administration de réseaux (NMS, Network Management System):* le composant NMS fournit la quantité de ressources mémoire et de traitements requises pour la gestion du réseau.
- *Les unités gérées*: ces unités sont des nœuds du réseau contenant un agent SNMP. Ces unités peuvent être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des concentrateurs, des ordinateurs hôtes ou des imprimantes.
- *Les agents*: les agents sont des modules logiciels de gestion du réseau résidant sur les unités gérées. Ils contiennent les données locales des informations de gestion et les convertissent en un format compatible avec SNMP.



Telnet :

Le logiciel client ***Telnet*** permet de se connecter à un hôte Internet distant sur lequel est exécutée une application serveur Telnet, puis d'exécuter des commandes à partir de la ligne de commande.

Un client Telnet est qualifié d'hôte local. Le serveur Telnet, qui utilise un logiciel spécial appelé «démon», est considéré comme l'hôte distant.

Les opérations de traitement et de stockage sont entièrement exécutées par l'ordinateur distant.