مكتب التكوين المهني وإنعاش الشغل
OFPPT
Office de la Formation Professionnelle et de la Promotion du Travail
www.tri.on.ma

ISTA Mohamed EL FASSI - Errachidia

Filière : Techniques de Réseaux Informatiques

Module N° 16 :
ARCHITECTURE ET FONCTIONNEMENT D'UN RÉSEAU INFORMATIQUE

Elaboré par : A. EL GHATTAS

Février 2008

http://adnaneadnane.ifrance.com/

super.adnane@hotmail.fr

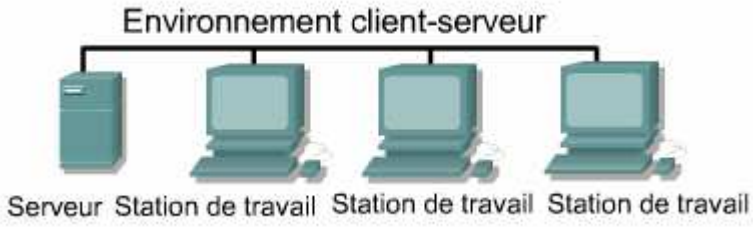
TABLE DES MATIERES

I. Notions de base en réseau
I.1. Terminologie de réseau

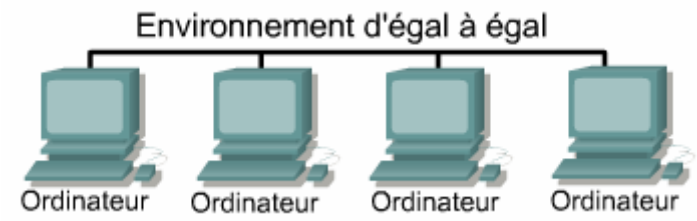
i. Définition
Un réseau est par définition un ensemble d'entités communicant entre elles. Nous allons nous intéresser dans le cadre de ce cours à ce que l'on nomme des réseaux de données ou réseaux informatiques.
Un réseau de données est donc un ensemble d'entités informatiques communicant ensemble.

ii. Pourquoi un réseau ?
1. Partage des ressources physiques : Imprimante, Lecteur de CD-ROM,…
2. Partage des ressources logicielles : Accès de plusieurs utilisateurs à des applications sans avoir à les installer sur leur propre poste.
3. Partage des données : Plusieurs utilisateurs peuvent accéder aux mêmes données et peuvent faire des modifications en temps réel.
4. Communication entre personnes distantes par le son, le texte et l'image : messagerie, conférence, chat…
5. Recherche d'informations : Internet
6. etc.…

iii. Types de réseaux
On distingue généralement deux types de réseaux :
• **Réseaux organisés autour de serveurs (Client/Serveur)** : c'est un réseau où des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, ...
Dans un environnement purement Client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est un des principaux atouts de ce modèle.



• **Réseaux poste à poste (peer to peer / égal à égal)** : Dans une architecture peer to peer, contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau est un peu serveur et un peu client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder via le réseau.



Avantages et inconvénients

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.

On distingue aussi différents types de réseaux (privés) selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue.
Nous différencions principalement :

- **réseau LAN** (**L**ocal **A**rea **N**etwork) : est le type le plus commun de réseau trouvé dans les entreprises. Il relie des ordinateurs et des dispositifs situés près de l'un l'autre, tel que dedans un même bâtiment, bureau,…
- **réseau MAN** (**M**etropolitan **A**rea **N**etwork) : une collection de réseaux locaux. Les MAN relient des ordinateurs situés dans le même secteur géographique tel qu'une ville. (LAN + LAN, Village,…)
- **réseau WAN** (**W**ide **A**rea **N**etwork) : relie des réseaux locaux et métropolitaines ensemble. Les réseaux qui composent d'un réseau étendu peuvent être situés dans tout un pays ou même autour du monde (LAN + LAN + MAN)

D'autres types de réseaux existent :

- **réseau de stockage SAN (S**torage **A**rea **N**etwork**)** qui est un réseau à haute performance dédié qui sert à transférer des données entre des serveurs et des ressources de stockage. Un réseau SAN fournit des performances système améliorées, il est évolutif et il intègre la tolérance aux sinistres.
- **réseau privé virtuel VPN** (**V**irtual **P**rivate **N**etwork) : un réseau privé, qui offre une connectivité sécurisée et fiable, construit au sein d'une infrastructure de réseau publique. Les VPN d'accès, d'intranet et d'extranet sont les trois principaux types de VPN. Les VPN d'accès fournissent aux utilisateurs mobiles et de petits bureaux/bureaux à domicile, l'accès distant à un intranet ou à un extranet. Les intranets sont uniquement disponibles pour les utilisateurs qui ont des privilèges d'accès au réseau interne de l'organisation. Les extranets sont conçus pour délivrer aux utilisateurs et entreprises externes des applications et des services qui sont basés sur intranet.
- **…**

I.2. La bande passante numérique et le débit

La bande passante d'un réseau représente sa capacité, c'est-à-dire la quantité de données pouvant circuler en une période donnée.
La bande passante du réseau est généralement exprimée en milliers de bits par seconde (kbits/s), millions de bits par seconde (Mbits/s), milliards de bits par second (Gbits/s).
A cette notion de bande s'ajoute celle de débit. Le débit est la bande passante réelle, mesurée à un instant précis de la journée. Ce débit est souvent inférieur à la bande passante ; cette dernière représentant le débit maximal du média ; en raison :

- o des unités d'interconnexion de réseaux et de leur charge
- o du type de données transmises
- o de la topologie du réseau
- o du nombre d'utilisateur
- o de l'ordinateur de l'utilisateur et du serveur
- o des coupures d'électricité et autres pannes

De ce fait le temps de téléchargement d'un fichier peut se mesurer de la manière suivante :

Temps de téléchargement (s) = Taille du fichier (b) / débit

I.3. Les médias de réseau local

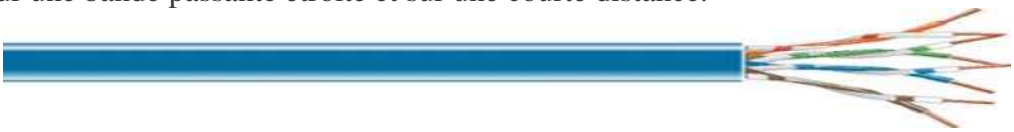
Les médias sont les supports physiques de la transmission utilisés dans le réseau. Ils servent à lier et à mettre en contact l'ensemble des nœuds avec le réseau. On appelle nœud tout point de connexion d'un élément d'émission ou de réception au réseau.
La liaison entre le média et l'ordinateur (le nœud) se fait en général par des connecteurs.

i. Le câble à paires torsadées non blindées

Fiche technique :

Désignation	: UTP (Unshielded Twisted Pair)
Vitesse	: 10 – 100 Mbits/s
Longueur max.	: 100m
Raccordement	: Connecteur RJ-45
Impédance	: 100 Ohms
Coût	: Faible

Le câble UTP est composé de 4 paires de fils torsadées 2 à 2, chacune de ses paires étant isolé des autres.
La paire torsadée non blindée utilisée comme média de réseau a une impédance de 100 ohms. Ceci la différencie des autres types de câblage à paires torsadées comme ceux utilisés pour le câblage téléphonique.
Comme le câble à paires torsadées non blindées a un diamètre extérieur d'environ un demi centimètre et un coût relativement faible, sa petite taille peut s'avérer avantageuse lors d'une installation.
Relativement à d'autres câbles, l'UTP est la moins chère et la plus facile à installer. Son connecteur est petit et il est surtout utilisé quand la transmission va se faire avec un débit faible sur une bande passante étroite et sur une courte distance.



Câble UTP

ii. Le câble à paires torsadées blindées

Fiche technique :

Désignation : STP (Shielded Twisted Pair)
Vitesse : 10 – 100 Mbits/s
Longueur max. : 100m
Raccordement : Connecteur RJ-45
Impédance : 100 Ohms
Coût : Moyennement cher

Le câble à paires torsadées et blindées ; ou STP ; ajoute aux spécifications de l'UTP une méthode de blindage, d'annulation et de torsion de câbles. Le câble est blindé pour réduire toute interférence électromagnétique et interférence de radiofréquences sans toutefois augmenter sensiblement la taille ou le poids du câble.
Le câble à paires torsadées blindées présente tous les avantages et désavantages du câble à paires torsadées non blindées en assurant cependant une plus grande protection contre toute interférence externe au prix certes d'un diamètre plus élevé.
Le STP n'est pas très exploitée sur le marché. Son véritable avantage relativement à l'UTP est qu'elle résiste mieux aux perturbations

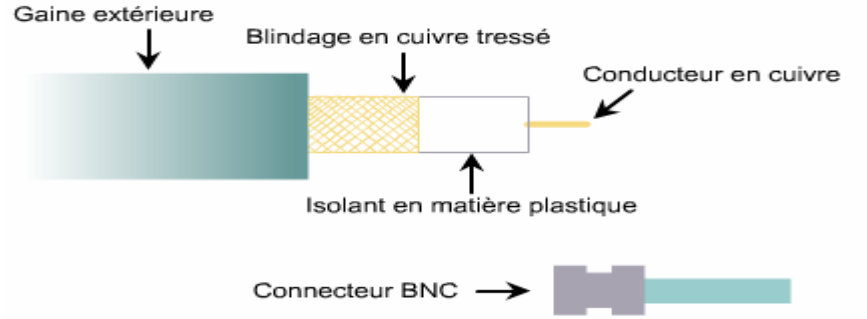
Câble STP

iii. Le câble coaxial

Fiche technique :

Désignation : Coaxial
Vitesse : 10 – 100 Mbits/s
Longueur max. : 500m
Raccordement : Connecteur BNC (British Naval Connector)
Impédance : 150 Ohms
Coût : Peu cher

Un câble coaxial est constitue d'un fil de cuivre entouré d'un isolant flexible, lui-même entouré d'une torsade de cuivre ou d'un ruban métallique qui agit comme le second fil du circuit et comme protecteur du conducteur intérieur. Cette deuxième couche ou protection peut aider à réduire les interférences externes. Une gaine de câble enveloppe ce blindage.



Le câble coaxial offre de nombreux avantages du fait de sa capacité à s'étendre sur une plus grande distance et de son coût parmi les plus faibles. Mais le rapport qualité prix fait que les entreprises utilisent surtout l'UTP.

Le câble coaxial existe en plusieurs variantes :

- Thicknet : Epais et raide à cause de son blindage, il est recommandé pour l'installation de câble fédérateur. Sa gaine est jaune.
- Thinnet : D'un diamètre plus réduit, il est plus pratique dans des installations comprenant des courbes. De plus il est plus économique mais dispose d'un blindage moins conséquent.
- Cheapernet : Version économique et de faible diamètre du câble coaxial.

Câble Thinnet

iv. La fibre optique

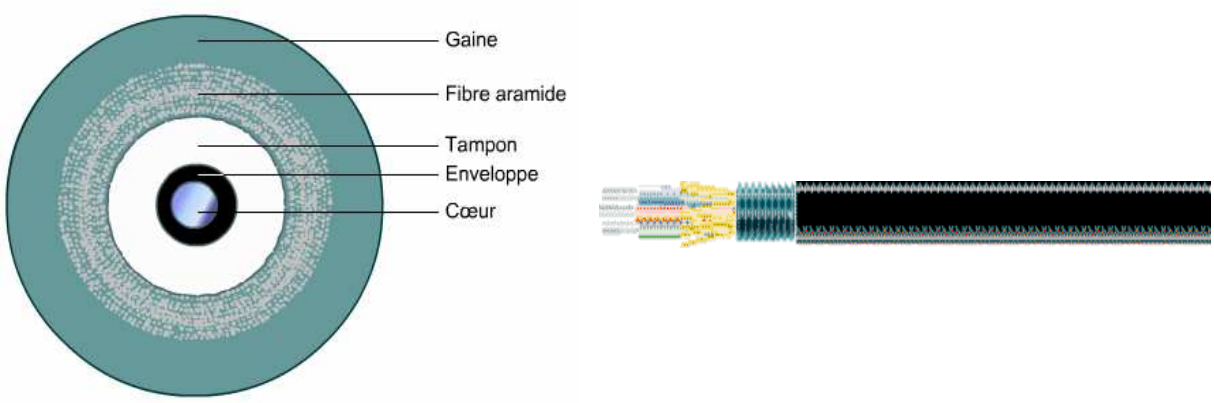
Fiche technique :

Désignation	: Fibre Optique
Vitesse	: 100+ Mbits/s
Longueur max.	: 2km en multimode et 3km en monomode
Raccordement	: Connecteur multi mode ou monomode
Coût	: Cher

Le câble à fibre optique est un support transmettant des impulsions lumineuses. Ce type de média est très coûteux, mais est insensible aux interférences électromagnétiques et peut acheminer des données à un débit très élevé.

Le câble à fibre optique utilisé pour les réseaux comprend deux fibres encapsulées dans des enveloppes distinctes. En examinant la coupe transversale, d'un câble optique, il est possible de voir que chaque fibre est entourée de couches de revêtements optiques réfléchissants, un enduit de plastique fait en Kevlar, et que l'ensemble est entouré d'une gaine extérieure assurant la protection de l'ensemble du câble.

Les parties de la fibre optique qui conduisent la lumière portent le nom de cœur et d'enveloppe. Le cœur est habituellement en verre pur à haut indice de réfraction. Ce cœur de verre est enrobé d'une enveloppe de verre ou de plastique à faible indice de réfraction, afin d'emprisonner la lumière dans le cœur optique. Cette différence d'indice crée un phénomène de réflexion totale qui permet à la fibre optique d'agir comme un tuyau, sans perte ou presque, guidant la lumière sur de grandes distances, même s'il décrit des courbes.



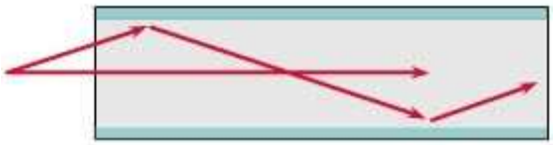
Fibre optique

Connecteur de câble à fibre optique

On distingue 2 types de fibre optique :
- Monomode : un seul faisceau parcourt la fibre, les lasers sont utilisés comme émetteurs récepteurs.

La fibre monomode

- Multimode : plusieurs faisceaux parcourent la fibre avec des angles différents, selon leur angle de pénétration. Dans le cas d'une fibre multimode, les émetteurs récepteurs utilisés sont des LED.



La fibre multimode

vi. Les communications sans fil

Les signaux sans fil sont des ondes électromagnétiques qui peuvent circuler dans le vide ou dans des médias tels que l'air. De ce fait, ils ne requièrent aucun média physique.
Pour communiquer, un réseau LAN sans fil utilise :

- des ondes radios (ex : 902MHz)
- des micro-ondes (ex : 2.4GHz)
- des ondes infrarouges (ex : 820 nanomètres)

I.4. Spécifications et raccordement des câbles

Dans le but d'ajouter aux spécifications de l'ISO des normes visant à standardiser les équipements, divers organismes ont mis en place différentes normes. Ces organismes sont :

- IEEE : Institute of Electrical and Electronics Engineers
- UL : Underwriters laboratories
- EIA : Electronic Industries Alliance
- TIA : Telecommunications Industry Association

i. Les normes TIA/EIA

Elles définissent les configurations minimales d'installation tout en laissant toute liberté quand au choix du fournisseur d'équipement

Les principales normes sont :

- TIA/EIA-568-A : norme de câblage pour les télécommunications dans les édifices commerciaux
- TIA/EIA-569-A : Norme relative aux espaces et aux voies de télécommunications dans les édifices commerciaux
- TIA/EIA-570-A : Norme de câblage pour les télécommunications dans les résidences et les petits édifices commerciaux
- TIA/EIA-606 : Norme relative à l'administration de l'infrastructure de télécommunication dans les édifices commerciaux
- TIA/EIA-607 : Norme de mise à la terre et de liaison pour les télécommunication dans les édifices commerciaux

ii. Les spécifications de câblage de la norme TIA/EIA-568-A

Câblage horizontal : câblage situé entre la prise murale et une interconnexion horizontale. Il inclut le média réseau installé horizontalement, la prise ainsi que les terminaisons mécanique. Il comprend donc le média réseau allant de l'armoire de câblage jusqu'à une zone de travail.

La norme autorise les longueurs suivantes :

- Longueur maximale d'un câblage horizontal : 90m
- Longueur maximale des câbles d'interconnexion : 6m
- Longueur maximale des câbles de raccordement (pour relier les unités réseau au câblage horizontal) : 3m

De plus la norme exige la mise à la terre de tous les câbles.

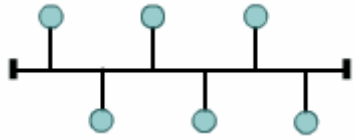
En ce qui concerne le choix du type de câblage, la norme comprend des spécifications définissant les performances des câbles : CAT1, CAT2, CAT3, CAT4 et CAT5. De nos jours, seules les catégories 3, 4 et 5 sont reconnues pour les réseaux locaux.

I.5. Les topologies physiques

Topologie : décrit la manière dont les équipements réseaux sont connectés entre eux. Nous distinguerons les topologies physiques ; décrivant la manière dont les équipements sont reliés par des médias ; des topologies logiques ; décrivant la manière dont les équipements communiquent.

i. La topologie en bus

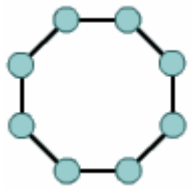
Une topologie de bus fait appel à un câble de backbone unique qui est terminé aux deux extrémités. Tous les hôtes se connectent directement à ce backbone.



Topologie en bus

ii. La topologie en anneau

Dans une topologie en anneau, chaque hôte est connecté à son voisin. Le dernier hôte se connecte au premier. Cette topologie crée un anneau physique de câble.

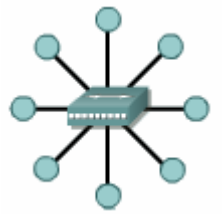


Topologie en anneau

Une variante de cette topologie est le double anneau ou chaque hôte est connecté à 2 anneaux. Ces 2 anneaux ne communiquent pas entre eux. Le deuxième anneau est utilisé comme lien redondant en cas de panne sur le premier.

iii. La topologie en étoile

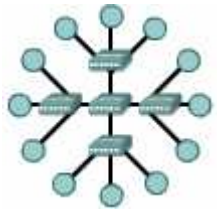
Dans une topologie en étoile, tous les câbles sont raccordés à un point central, par exemple un concentrateur ou un commutateur.



Topologie en étoile

iv. La topologie en étoile étendue

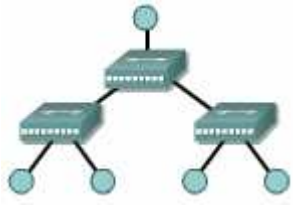
Cette topologie est identique à la topologie en étoile si ce n'est que chaque nœud connecté au nœud central est également le centre d'une autre étoile.



Topologie en étoile étendue

v. La topologie hiérarchique

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.



Topologie hiérarchique

vi. La topologie complète (maillée)

Dans la topologie maillée chaque hôte possède ses propres connexions à tous les autres hôtes.

Topologie maillée

vii. Comparaison entre les principales topologies physiques

	Avantages	Inconvénients
bus	▪ Facile à installer. ▪ Un seul câble pour l'ensemble. ▪ Branchement de nouveaux nœuds sans perturbation du réseau.	▪ Difficulté de localisation des pannes. ▪ En cas de rupture, le réseau entier s'arrête.
anneau	▪ Un seul câble.	▪Toute panne au niveau d'un élément ou coupure de câble bloque le réseau. ▪Le temps de réponse se dégrade à l'ajout d'un nouveau nœud.
étoile	▪ Facilité de localisation des pannes. ▪ Possibilité d'extension : les nœuds s'y ajoutent facilement.	▪ Il y'a autant de câbles que d'équipements, cela peut coûter cher pour des nœuds éloignés.

I.6. Les topologies logiques

i. CSMA/CD (Carrier Sense Multiple Access / Collision Detect)

Toute information envoyée par un hôte atteindra tous les autres hôtes du réseau. Chaque hôte a une adresse unique. Il reste constamment en écoute du câble pour détecter les signaux qui passent sur le réseau. Au passage d'un signal, il vérifie si l'adresse destinataire est son adresse. Si c'est le cas, il prend le message et le lit, sinon il le néglige.

Si l'un des hôtes désire émettre, il vérifie au préalable que personne n'est en train de le faire, puis commence à émettre.

Si cependant 2 hôtes émettent en même temps, il se produit alors une collision. La première station qui détecte une collision envoie alors un signal de bourrage, se traduisant par un arrêt d'émission de tous les hôtes. Les paquets concernés sont alors détruits.

Chaque hôte calcule alors une valeur aléatoire définissant la durée avant de recommencer à émettre, puis le mécanisme de CSMA se remet en fonction. Ce temps aléatoire fait de CSMA/CD une méthode non déterministe.

Ethernet fonctionne ainsi, comme nous l'expliquerons plus loin dans le cours.

ii. Le passage de jeton

La deuxième topologie logique est le passage de jeton.

Un jeton = un signal qui circule constamment sur le réseau, de poste en poste.

Lorsqu'une station désire émettre, elle doit attendre de recevoir le jeton dans un état libre. Elle le charge avec les informations, le marque occupé et elle le renvoie sur le réseau à la station suivante. Cette station vérifie le message, trouve que c'est occupé, contrôle si il lui est destiné.

Si c'est le cas, elle lit les informations, rajoute une indication qui va informer la station expéditrice que son message a été reçu. Si, par contre, le message ne lui est pas destiné, elle le réécrit et le laisse passer à la station à côté.
Ce travail se refait par chaque station jusqu'à ce que le jeton arrive à la station émettrice qui vérifie si le message a été reçu. Si c'est le cas, elle libère le jeton et le renvoie sur le câble.
Token Ring et FDDI (Fiber Distributed Data Interface) sont deux exemples de réseaux qui utilisent le passage de jeton.

I.7 Ethernet et Token Ring

i. Ethernet

Ethernet est la technologie la plus répandue dans les réseaux actuels. Au début des années 80 fut mis en place par l'IEEE la norme IEEE 802.3 à partir d'Ethernet.
Ethernet et IEEE 802.3 définissent des technologies semblables :
-Utilisation de CSMA/CD pour l'accès au média
-Concept de réseaux de broadcast (voir plus loin)
Il existe au moins 18 types d'Ethernet, qui ont été définis ou qui doivent encore l'être. Le tableau suivant illustre certaines technologies Ethernet parmi les plus répandues et les plus importantes.

	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX
Médias	Câble coaxial de 50 ohms (Ethernet à câble fin)	Câble coaxial de 50 ohms (Ethernet épais)	Câble EIA/TIA Catégorie 3, 4, 5 UTP, deux paires	Câble EIA/TIA Catégorie 5 UTP, deux paires	Fibre multimode de 62,5/125
Longueur maximale du segment	185 m	500 m	100 m	100 m	400 m
Topologie	En bus	En bus	En étoile	En étoile	En étoile
Connecteur	BNC	AUI (Attachment Unit Interface)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Connecteur d'interface média duplex Connecteur ST ou SC

	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
Médias	STP	Câble EIA/TIA catégorie 5 UTP, quatre paires	Fibre multimode de 62,5/50 microns.	Fibre multimode de 62,5/50 microns ; fibre monomode de 9 microns.
Longueur maximale du segment	25 m	100 m	275 m pour la fibre de 62,5 microns ; 550 m pour la fibre de 50 microns	440 m pour la fibre de 62,5 microns ; 550 m pour la fibre de 50 microns ; de 3 à 10 km pour la fibre monomode.
Topologie	En étoile	En étoile	En étoile	En étoile
Connecteur	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Connecteur SC	Connecteur SC

ii. Token ring

La technologie des réseaux Token-Ring fut développée par IBM. Elle a été normalisée par l'IEEE sous la norme IEEE 802.5. Contrairement à Ethernet, il n'existe pas, sur le marché, de normes concernant l'implantation de ce type de réseau. Pour ces raisons, on adopte en général les spécifications IBM. Les types ci-dessous ne sont pas des normes mais des recommandations IBM.

	Type 1	**Type 2**	**Type 3**
méthode d'accès	à jeton	à jeton	à jeton
débit	4 ou 16 Mbps	4 Mbps	4 Mbps
câble	STP	STP + une paire de fils	UTP
connecteur	IBM Hermaphrodite	IBM	RJ45
utilisateurs	260 stations par Anneau		260 stations par Anneau
topologie (avec MSAU)	Etoile	Etoile	Etoile
distance nœud - MSAU	145 m max.	375 m max.	100 m max.
distance MSAU - MSAU	200 m	400 m max.	300 m max.

Remarque : la MSAU (Multi Station Access Unit) transforme une topologie physique Etoile en Anneau.

I.8 Composants et équipements d'un réseau local

Des nos jours, les 3 technologies LAN les plus répandues sont :

- Ethernet
- Token Ring

Ethernet étant le plus répandu, nous allons étudier des composants de cette technologie. Le support physique de cette technologie est le câble à paires torsadées.

Composant passif : Qui n'a pas besoin d'une source d'alimentation externe pour fonctionner Composant actif : Qui nécessite une alimentation externe pour remplir ses fonctions.

i. Les cartes réseau ou NIC

Se connectant sur la carte mère, la carte réseau assure la connexion physique entre l'ordinateur et le réseau. Elle contient également l'adresse MAC.

Trois facteurs différencient les types de cartes :

-le type de réseau

Exemple : Ethernet, Token Ring

-le type de média

Exemple : Fibre optique, UTP, coaxial

-le type de bus système

Exemple : PCI, ISA, PCMCIA

Cartes réseau PCMCIA et ISA

ii. Les connecteurs RJ45

Le raccordement 10BaseT standard (le connecteur de point d'extrémité sans prise) est le RJ-45. Il réduit les parasites, la réflexion et les problèmes de stabilité mécanique et ressemble à une prise téléphonique, sauf qu'il compte huit conducteurs au lieu de quatre.

Il s'agit d'un composant réseau passif, car il sert uniquement au passage du courant entre les quatre paires torsadées de câble torsadé de catégorie 5 et les broches du connecteur RJ-45.

Les connecteurs RJ-45 s'insèrent dans les réceptacles ou les prises RJ-45. Les prises mâles RJ-45 ont huit connecteurs qui s'enclenchent avec la prise RJ-45.De l'autre côté de la prise RJ-45, il y a un bloc où les fils sont séparés et fixés dans des fentes avec l'aide d'un outil semblable à une fourche. Ceci offre un passage de courant en cuivre aux bits.

Connecteurs RJ45 et prise murale

iii. Les connecteurs

Pour regrouper un grand nombre de prises RJ-45 des tableaux de connexions sont utilisés. Généralement fournis avec 12, 24 ou 48 ports, ils comprennent une face avant permettant de brancher les connecteurs RJ45 et une face arrière permettant de relier les câbles.

Vue du dessus d'un tableau de connexions

iv. Les émetteurs-récepteurs

Un émetteur-récepteur (tranceiver) convertit un signal en un autre. Il est souvent intégré aux cartes réseaux.

Emetteurs-récepteurs

v. Les répéteurs

Un signal ne peut pas se propager infiniment sur le câble. Il s'affaiblit jusqu'à s'atténuer complètement. Cette atténuation est fonction du type de câble et c'est d'ailleurs un critère de choix des câbles.

Pour prolonger les réseaux au delà des limites d'un câble, on utilise un **répéteur** (en anglais repeter). Un répéteur ne fait que régénérer le signal. Il n'est pas responsable de la détection des erreurs ou de leur correction. Quand un signal est présent sur un câble, le répéteur l'amplifie et le véhicule sur un autre câble de même type ou de type différent.

vi. les concentrateurs

Le concentrateur (hub en anglais) ; ou répéteur multi ports ; reprend le fonctionnement du répéteur en ajoutant une fonctionnalité de connectivité. En effet, il dispose de plusieurs ports ce qui permet d'interconnecter plusieurs équipements réseaux. Chaque signal arrivant sur un port est régénéré, re-synchronisé et ré émis au travers de tous les autres ports.

Concentrateur

vii. Les ponts

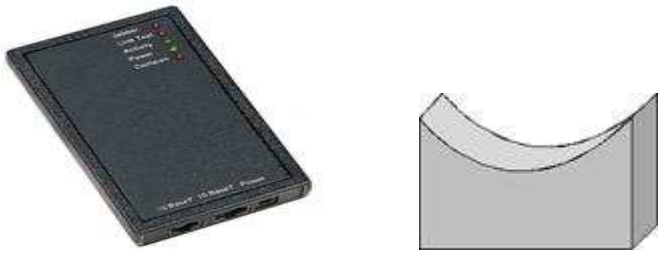
Pour soulager un réseau où les flux sont devenus très importants et donc le temps de réponse trop long, il faut le segmenter et utiliser des ponts.

Un pont (bridge en anglais) permet d'interconnecter deux ou plusieurs segments d'un réseau. Son rôle principal est de filtrer les différentes requêtes et de distinguer les informations destinées à un élément d'un même segment de celles destinées aux éléments d'un autre segment. En fait, chaque nœud est identifié avec une adresse unique. Dans les anciennes générations de ponts, l'administrateur réseau devait introduire manuellement ses adresses pour que les ponts puissent reconnaître les nœuds et leur emplacement dans les segments du réseau.

Les nouvelles générations sont plus intelligentes. Les ponts gardent automatiquement l'adresse de chaque trame qui transite par le réseau et apprend à localiser le nœud ; ainsi après une étape d'auto apprentissage, il ne laissera passer que les trames destinées à l'autre segment du réseau.

Les ponts contribuent également à étendre les limites d'un réseau en reliant plusieurs segments du réseau. Ils limitent aussi les problèmes de collision, si une collision a lieu dans un segment, elle ne sera pas filtrée et l'autre segment pourra fonctionner correctement.

Remarque : les ponts ne peuvent pas connecter des réseaux hétérogènes.



Pont Ethernet

viii. Les commutateurs

Le commutateur (en anglais switch) est un pont multiports. Le commutateur analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (on parle de **commutation** ou de **réseaux commutés**).

On distingue 2 types de commutations :

-cut through : dès que le commutateur connaît l'adresse de destination, il commence l'envoi de la trame sur le bon segment.

-Store and forward : le commutateur attend l'arrivée complète de la trame pour acheminer celle ci au bon segment.

Si bien que le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

Commutateur Ethernet

ix. Les passerelles

Les passerelles (en anglais "**gateways**") sont des systèmes matériels et logiciels permettant de faire la liaison entre deux réseaux, servant notamment à faire l'interface entre des protocoles différents.

Lorsqu'un utilisateur distant contacte un tel dispositif, celui-ci examine sa requête, et si jamais celle-ci correspond aux règles que l'administrateur réseau a définies, la passerelle crée un pont entre les deux réseaux. Les informations ne sont donc pas directement transmises, mais "traduites" afin d'assurer la continuité des deux protocoles.

Ce système offre, outre l'interface entre deux réseaux hétérogènes, une sécurité supplémentaire car chaque information est passée à la loupe (pouvant causer un ralentissement) et parfois ajoutée dans un journal qui retrace l'historique des événements.

x. Les routeurs

Les routeurs sont les machines clés d'Internet car ce sont ces dispositifs qui permettent de "choisir" le chemin qu'un message va emprunter.

Ils utilisent une table de routage qui contient les meilleurs chemins à suivre pour chaque nœud du réseau et à partir de tous les nœuds du réseau.

Les routeurs permettent plus d'un chemin et déterminent la meilleure route en fonction de différents critères (rapidité, données). Ils sont très adaptés aux réseaux complexes et gèrent simultanément plusieurs lignes de communication en optimisant l'utilisation de ces lignes et en répartissant les transmissions en fonction des occupations de chaque ligne.

Routeurs

II. Le modèle OSI

II.1. Présentation du modèle de référence OSI

i. Le modèle général de communication à couche

La première évolution des réseaux informatiques a été des plus anarchiques, chaque constructeur développant presque sa propre technologie. Le résultat de cela était une quasi-impossibilité de connecter différents réseaux entre eux. Pour palier à cela, l'ISO (Institut de normalisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseaux : le modèle OSI.

Le but de ce modèle est d'analyser la communication en découpant les différentes étapes en 7 couches ; chacune de ces couches remplissant une tâche bien spécifique :

n°	Nom	Description
7	Application	Communication avec les logiciels
6	Présentation	Gestion de la syntaxe
5	Session	Contrôle du dialogue
4	Transport	Qualité de la transmission
3	Réseau	Sélection du chemin
2	Liaison de données	Préparation de l'envoi sur le média
1	Physique	Envoi sur le média physique

Les 7 couches du modèle OSI

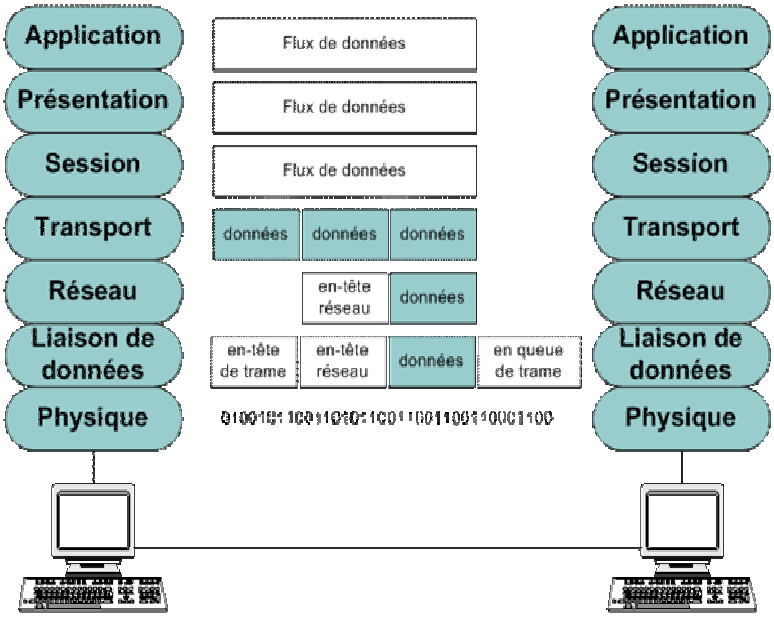
Les avantages de ce modèle sont :

- Une division de la communication réseau en éléments plus petits et plus simple pour une meilleure compréhension
- L'uniformisation des éléments afin de permettre le développement multi constructeur
- La possibilité de modifier un aspect de la communication réseau sans modifier le reste (Exemple : un nouveau média)

ii. L'encapsulation

Pour communiquer entre les couches et entre les hôtes d'un réseau, OSI a recourt au principe d'encapsulation.

Encapsulation : processus de conditionnement des données consistant à ajouter un en tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure :



Principe de l'encapsulation

Lorsque 2 hôtes communiquent, on parle de communication d'égal à égal ; c'est-à-dire que la couche n de la source communique avec la couche n du destinataire.
Lorsqu'une couche de la source reçoit des données, elle encapsule ces dernières avec ses informations puis les passe à la couche inférieur. Le mécanisme inverse a lieu au niveau du destinataire ou une couche réceptionne les données de la couche inférieur ; enlève les informations la concernant ; puis transmet les informations restantes à la couche supérieure. Les données transitant à la couche n de la source sont donc les mêmes que les données transitant à la couche n du destinataire.
Pour identifier les données lors de leur passage au travers d'une couche, l'appellation « Unité de données de protocole (PDU) » est utilisée.

<table>
<tr><th>Couche</th><th>Désignation</th></tr>
<tr><td>7</td><td rowspan="3">Données</td></tr>
<tr><td>6</td></tr>
<tr><td>5</td></tr>
<tr><td>4</td><td>Segment</td></tr>
<tr><td>3</td><td>Paquets</td></tr>
<tr><td>2</td><td>Trame</td></tr>
<tr><td>1</td><td>Bits</td></tr>
</table>

Les PDU des différentes couches

II.2. Le modèle TCP/IP

i. Présentation de TCP/IP

La forme actuelle de TCP/IP résulte du rôle historique que ce système de protocoles a joué dans le parachèvement de ce qui allait devenir Internet. A l'instar des nombreux développements de ces dernières années, Internet est issu des recherches lancées aux Etats-Unis par le DOD, département de la défense.
A la fin des années 60, les officiels du DOD se rendent compte que les militaires du département de la défense possèdent une grande quantité de matériel informatique très divers, mais ces machines travaillent pour la plupart de manière isolées ou encore en réseaux de taille très modeste avec des protocoles incompatibles entre eux, ceci rendant une interconnexion impossible.
Les autorités militaires se sont alors demandé s'il était possible, pour ces machines aux profils très différents, de traiter des informations mises en commun. Habitués comme ils le sont aux problèmes de sécurité, les responsables de la défense ont immédiatement réalisé qu'un réseau de grande ampleur deviendrait une cible idéale en cas de conflit. La caractéristique principale de ce réseau, s'il devait exister, était d'être non centralisé.
Ses fonctions essentielles ne devait en aucun cas se trouver en un seul point, ce qui le rendrait trop vulnérable. C'est alors que fut mis en place le projet Arpanet (Advanced Research Projects Agency du DOD), qui allait devenir par la suite le système d'interconnexion de réseau qui régit ce que l'on appelle aujourd'hui l'Internet : TCP/IP.
TCP/IP est un modèle comprenant 4 couches :

n°	Nom	Description
4	Application	Couches 7 à 5 du modèle OSI
3	Transport	Qualité de transmission
2	Internet	Sélection du chemin
1	Accès au réseau	Reprend les couches 1 et 2 du modèle OSI

Les 4 couches de TCP/IP

ii. Protocole orienté/non orienté connexion

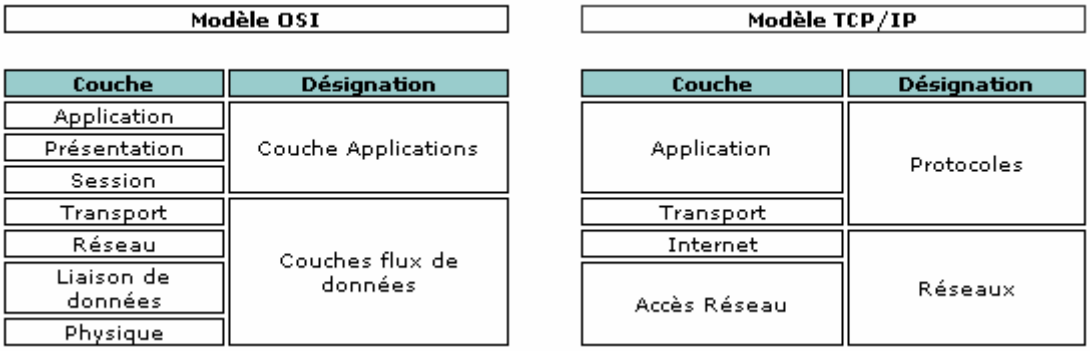
Protocole : Ensemble formel de règles et de conventions qui régit l'échange d'informations entre des unités en réseau

Dans un protocole orienté connexion, TCP/IP établit un dialogue entre la source et le destinataire pendant qu'il prépare les informations de la couche application en segments. Il y a alors un échange de segments de couche 4 afin de préparer une communication et donc une connexion logique pendant un certain temps.
Cette communication faisant appel à un circuit logique temporaire est appelé commutation de paquets, en opposition à la commutation de circuits supposant elle un circuit permanent.
Un protocole non orienté connexion envoie les données sur le réseau sans qu'un circuit ait été établi au préalable.

iii. Comparaison entre OSI et TCP/IP

Ces deux protocoles sont très similaires, dans la mesure ou les 2 sont des modèles de communication à couche et utilisent l'encapsulation de données.
On remarque cependant deux différences majeures :

- TCP/IP regroupe certaines couches du modèle OSI dans des couches plus général
- TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau Internet actuel

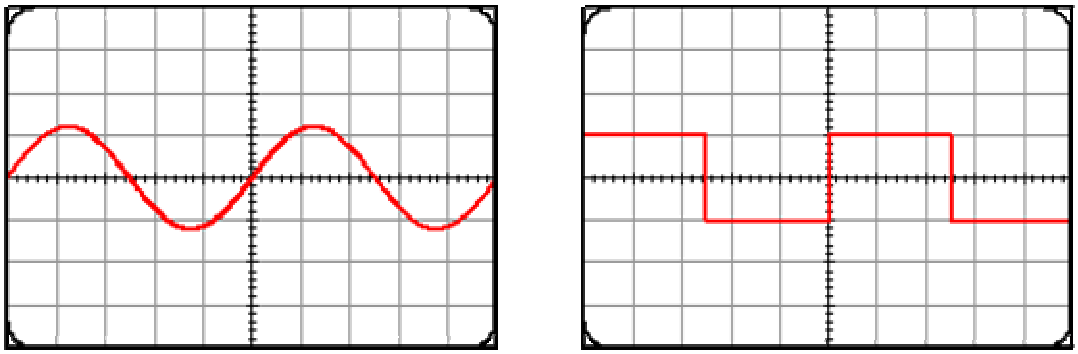


Les modèles OSI et TCP/IP

II.3 La couche physique

1. Les notions de base sur les signaux et le bruit dans les systèmes de communication

i. Comparaison des signaux analogiques et numériques



Représentation d'un signal numérique et d'un signal analogique

Signal : tension électrique souhaitée, modèle d'impulsions lumineuses ou encore onde électromagnétique modulée. Il permet d'acheminer les données dans le média.

Le signal analogique présente les caractéristiques suivantes :
o il oscille
o son graphique de tension varie constamment en fonction du temps et peut être représenté par une sinusoïde
o il est utilisé pour les télécommunications depuis le début
Exemple : téléphone et radio

Le signal numérique dispose d'un graphique de tension que l'on va définir comme « sautillant », il se rapproche d'une onde carrée ou la tension passe quasi-instantanément d'un état de basse tension à un état de haute tension.

Pour créer des signaux numériques, il est possible de combiner des ondes sinusoïdales (Synthèse de Fourrier)

ii. La représentation d'un bit dans un média physique

La composante de base de l'information dans les réseaux est le bit. Dans le cas d'un signal électrique, un bit correspond à une impulsion signifiant 0 ou 1.
Exemple :

- 0 : 0 volt et 1 +5 volts dans le cas d'un signal électrique
- 0 : faible intensité et 1 forte intensité dans le cas d'un signal optique
- 0 : courte rafale d'onde et 1 rafale d'onde plus longue dans le cas de transmission sans fil

Mise à la terre de référence : masse électrique permettant d'établir la ligne 0 dans les graphiques de signalisation

iii. Les facteurs pouvant affecter un bit

Il existe différents facteurs pouvant affecter le signal et de ce fait les bits transportés sur le média :

o **La propagation de signaux réseau :**

Le terme de propagation fait référence au temps que met un bit ; c'est-à-dire une impulsion ; à se déplacer dans le média. Il est impératif que la propagation soit homogène dans le réseau.

o **L'atténuation du signal réseau :**

Perte de la force du signal. Ce problème est limitable par un bon choix des médias réseaux utilisés

o **La réflexion réseau :**

Retour d'énergie causé par le passage des impulsions dans le média. Si ce retour est trop fort, il peut perturber le signal des impulsions suivantes. Le système binaires ; et donc à 2 états ; peut être perturbé par ces énergies supplémentaires se déplaçant dans le média.

o **Le bruit :**

Ajout indésirable à un signal. Des sources d'énergie situées à proximité du média fournissent un supplément d'énergie venant perturber le signal.

 Diaphonie : bruit ajouté au signal d'origine d'un conducteur par l'action du champ magnétique provenant d'un autre conducteur

 Paradiaphonie : diaphonie causée par un conducteur interne au câble.

Le bruit peut être causé par des sources d'alimentations externes, des variations thermiques, des interférences électromagnétiques ou encore des interférences de radio fréquences.

- **La dispersion :**

Etalement des impulsions dans le temps. Si la dispersion est trop forte, le signal d'un bit peut recouper le signal du précédent ou du suivant. La durée d'une impulsion est fixe, la dispersion correspond à une modification de cette durée au fur et à mesure que le signal se propage dans le média.

- **La gigue :**

Les systèmes numériques sont synchronisés, tout est réglé par des impulsions d'horloge. Si les horloges de la source et du destinataire ne sont pas synchronisées, on obtient alors une *gigue de synchronisation*.

- **La latence :**

Retard de transmission. Principalement du au déplacement du signal dans le média et à la présence de composants électroniques entre la source et la destination.

- **Les collisions :**

Se produit lorsque 2 ordinateurs utilisant le même segment de réseau émettent en même temps. Les impulsions se mélange, détruisant alors les données.

Dès qu'un bit accède au média, il est sujet à tous ces paramètres pouvant perturber la transmission. Dans la mesure où le but n'est pas de transmettre un bit mais des quantités gigantesques (parfois 1 milliard de bits à la seconde) ; ces paramètres ne sont pas à négliger car le moindre défaut peut avoir des conséquences importantes sur la qualité de la transmission

2. Notions de base sur le codage de signaux réseau

Nous allons donc nous intéresser ici aux méthodes de transmission de bits de façon brute entre l'émetteur et le récepteur.

Tout d'abord une liaison entre 2 équipements A et B peut être :

- Simple (unidirectionnelle) : A est toujours l'émetteur et B le récepteur. C'est ce que l'on trouve par exemple entre un banc de mesure et un ordinateur recueillant les données mesurées.
- Half-duplex (bidirectionnelle à l'alternat) : Le rôle de A et B peut changer, la communication change de sens à tour de rôle (principe talkies-walkies).
- Full-duplex (bidirectionnelle simultanée) : A et B peuvent émettre et recevoir en même temps (comme dans le cas du téléphone).

La transmission de plusieurs bits peut s'effectuer :

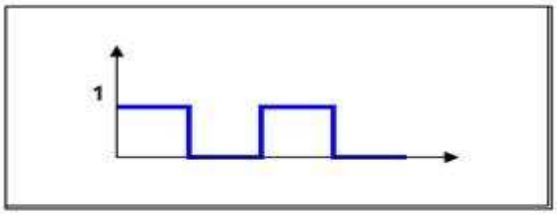
- En série : les bits sont envoyés les uns derrière les autres de manière synchrone ou asynchrone :
  - Dans le mode synchrone l'émetteur et le récepteur se mettent d'accord sur une base de temps (un top d'horloge) qui se répète régulièrement durant tout l'échange. À chaque top d'horloge (ou k tops d'horloge k entier fixé définitivement) un bit est envoyé et le récepteur saura ainsi quand arrivent les bits.
  - Dans le mode asynchrone, il n'y a pas de négociation préalable mais chaque caractère envoyé est précédé d'un bit de start et immédiatement suivi d'un bit de stop. Ces deux bits spéciaux servent à caler l'horloge du récepteur pour qu'il échantillonne le signal qu'il reçoit afin d'y décoder les bits qu'il transmet.
- En parallèle : Les bits d'un même caractère sont envoyés en même temps chacun sur un fil distinct, mais cela pose des problèmes de synchronisation et n'est utilisé que sur de courtes distances (bus par exemple).

Quel que soit le mode de transmission retenu, l'émission est toujours cadencée par une horloge dont la vitesse donne le débit de la ligne en bauds, c'est-à-dire le nombre de tops d'horloge en une seconde. Ainsi, une ligne d'un débit de 100 bauds autorise 100 émissions par seconde. Si à chaque top d'horloge un signal représentant 0 ou 1 est émis, alors dans ce cas le débit en bit/s est équivalent au débit en baud.

Cependant, on peut imaginer que le signal émis puisse prendre 4 valeurs distinctes (0, 1, 2, 3) dans ce cas le signal a une valence de 2 et le débit en bit/s est double de celui en baud. D'une manière générale, si le signal peut prendre 2n valeurs distinctes on dit alors que sa valence est de n, ainsi à chaque top n bits peuvent être transmis simultanément et si le débit de la ligne est de x bauds il est en fait de n.x bit/s.

i. Transmission en bande de base

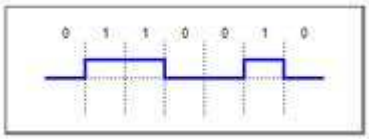
La transmission en bande de base consiste à envoyer directement les suite de bits sur le support à l'aide de signaux carrés constitués par un courant électrique pouvant prendre 2 valeurs (5 Volts ou 0 Volts par exemple).
L'émetteur envoie sur la ligne un signal carré du type de celui de la figure ci-dessous pour la séquence de bits 1010 :



Signal carré de la séquence de bits 1010

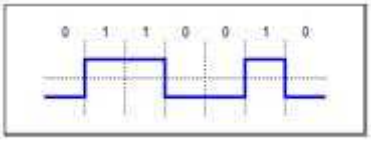
Il existe de nombreuses possibilités de coder sur le signal sur un média, voici différents exemples :

- **Le code tout ou rien :** c'est le plus simple, un courant nul code le 0 et un courant positif indique le 1



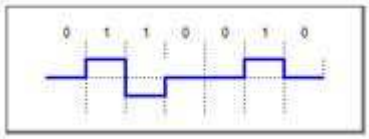
Le code tout ou rien

- **Le code NRZ :** (non retour à zéro): pour éviter la difficulté à obtenir un courant nul, on code le 1 par un courant positif et le 0 par un courant négatif.



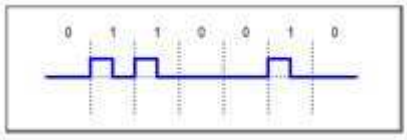
Le code NRZ

- **Le code bipolaire :** c'est aussi un code tout ou rien dans lequel le 0 est représenté par un courant nul, mais ici le 1 est représenté par un courant alternativement positif ou négatif pour éviter de maintenir des courants continus.



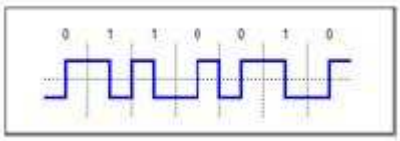
Le code bipolaire

- **Le code RZ :** le 0 est codé par un courant nul et le 1 par un courant positif qui est annulé au milieu de l'intervalle de temps prévu pour la transmission d'un bit.



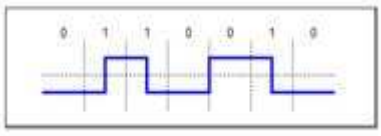
Le code RZ

- **Le code Manchester :** ici aussi le signal change au milieu de l'intervalle de temps associé à chaque bit. Pour coder un 0 le courant sera négatif sur la première moitié de l'intervalle et positif sur la deuxième moitié, pour coder un 1, c'est l'inverse. Autrement dit, au milieu de l'intervalle il y a une transition de bas en haut pour un 0 et de haut en bas pour un 1.



Le code Manchester

- **Le code Miller :** on diminue le nombre de transitions en effectuant une transition (de haut en bas ou l'inverse) au milieu de l'intervalle pour coder un 1 et en n'effectuant pas de transition pour un 0 suivi d'un 1. Une transition est effectuée en fin d'intervalle pour un 0 suivi d'un autre 0.



Le code Miller

ii. Principe de transmission modulée

Le principal problème de la transmission est la dégradation du signal très rapide en fonction de la distance parcourue.
C'est pourquoi sur les longues distances on émet un signal sinusoïdal qui, même s'il est affaibli, sera facilement décodable par le récepteur.

Ce signal sinusoïdal est obtenu grâce à un modem (modulateur - démodulateur) qui est un équipement électronique capable de prendre en entrée un signal en bande de base pour en faire un signal sinusoïdal (modulation) et l'inverse à savoir restituer un signal carré à partir d'un signal sinusoïdal (démodulation). Autrement dit il permet de passer de signaux numériques discrets (0 ou 1) à des signaux analogiques continus.

Il existe trois types de modulation :

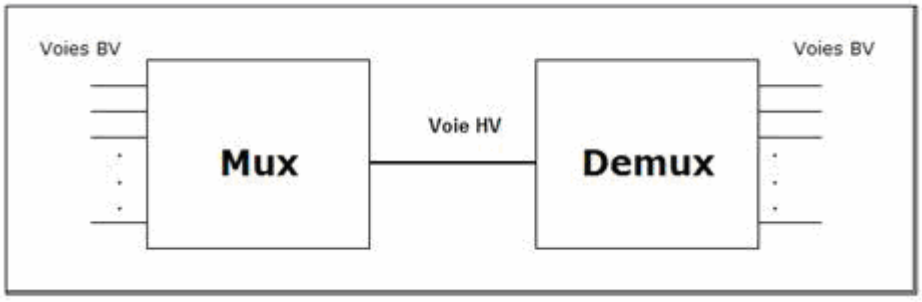
- La modulation d'amplitude : envoie un signal d'amplitude différente suivant qu'il faut transmettre un 0 ou un 1. Cette technique est efficace si la bande passante et la fréquence sont bien ajustées. Par contre, il existe des possibilités de perturbation (orage, lignes électriques...), car si un signal de grande amplitude (représentant un 1) est momentanément affaibli le récepteur l'interprétera à tort en un 0.
- La modulation de fréquence : envoie un signal de fréquence plus élevée pour transmettre un 1. Comme l'amplitude importe peu, c'est un signal très résistant aux perturbations (la radio FM est de meilleure qualité que la radio AM) et c'est assez facile à détecter.
- La modulation de phase : change la phase du signal (ici de 180) suivant qu'il s'agit d'un 0 (phase montante) ou d'un 1 (phase descendante).

Dans les exemples donnés nous avons seulement 2 niveaux possibles à chaque fois, donc on a uniquement la possibilité de coder 2 valeurs différentes à chaque instant, dans ce cas 1 baud = 1bit/s.

De manière plus sophistiquée il existe des modems capables de moduler un signal suivant plusieurs niveaux, par exemple 4 fréquences différentes que le modem récepteur saura lui aussi distinguer. Dans ce cas, chaque signal envoyé code 2 bits donc 1 baud = 2bit/s. Il est même possible de transmettre des signaux mêlant les différentes modulations présentées comme dans le cas de la norme V29 qui module à la fois l'amplitude du signal sur 2 niveaux et la phase sur 8 niveaux (0,45,...,315). En combinant les 2 modulations, on obtient ainsi 16 signaux différents possibles à chaque instant, permettant de transmettre simultanément 4 bits à chaque top d'horloge (1 baud = 4 bit/s).

iii. Le multiplexage

Le multiplexage consiste à faire transiter sur une seule et même ligne de liaison, dite voie haute vitesse, des communications appartenant à plusieurs paires d'équipements émetteurs et récepteurs comme représenté dans la figure ci dessous. Chaque émetteur (respectivement récepteur) est raccordé à un multiplexeur (respectivement démultiplexeur) par une liaison dit voie basse vitesse.



Multiplexages d'une ligne

Plusieurs techniques sont possibles :

- Le multiplexage fréquentiel consiste à affecter à chaque voie basse vitesse une bande passante particulière sur la voie haute vitesse en s'assurant qu'aucune bande passante de voie basse vitesse ne se chevauche. Le multiplexeur prend chaque signal de voie basse vitesse et le ré émet sur la voie haute vitesse dans la plage de fréquences prévues. Ainsi plusieurs transmissions peuvent être faites simultanément, chacune sur une bande de fréquences particulières, et à l'arrivée le démultiplexeur1.6est capable de discriminer chaque signal de la voie haute vitesse pour l'aiguiller sur la bonne voie basse vitesse.

- Le multiplexage temporel partage dans le temps l'utilisation de la voie haute vitesse en l'attribuant successivement aux différentes voies basse vitesse même si celles-ci n'ont rien à émettre. Suivant les techniques chaque intervalle de temps attribué à une voie lui permettra de transmettre 1 ou plusieurs bits.
- Le multiplexage statistique améliore le multiplexage temporel en n'attribuant la voie haute vitesse qu'aux voies basse vitesse qui ont effectivement quelque chose à transmettre. En ne transmettant pas les silences des voies basses cette technique implantée dans des concentrateurs améliore grandement le débit global des transmissions mais elle fait appel à des protocoles de plus haut niveau et est basée sur des moyennes statistiques des débits de chaque ligne basse vitesse.

3. Collisions et domaines de collision

Si 2 hôtes du réseau émettent en même temps sur un même segment de réseau, les informations se chevauchent : c'est ce que l'on appelle une collision.
Lorsque cela survient, un hôte le détecte. A ce moment, il envoi un signal de bourrage annonçant le problème à tous les autres. A la réception de ce signal, tous les hôtes arrêtent d'émettre. Chacun calcule alors une valeur aléatoire correspondant au délai précédent une nouvelle tentative d'émission.
L'autre terme pour décrire un environnement de média partagé est « Domaine de collision », à savoir une section de réseau ou tous les hôtes partagent le même média.
Des équipements comme le répéteur ou le concentrateur n'effectuant aucun filtrage étendent ce domaine de collision.

II.4. Couche 2 : La couche liaison de données

1. Les normes de réseau local

Le modèle OSI comprend 2 couches dites « matérielles » ; en opposition aux couches logicielles. La couche 1 englobe les médias, les signaux ainsi que les bits se déplaçant sur diverses topologies.
La couche Liaison de données a pour fonction de combler tous les manques de la couche physique afin de permettre la communication réseau

i. IEEE et le modèle OSI

Les normes IEEE sont actuellement les normes pré dominantes. Selon l'IEEE, on divise la partie matérielle du modèle OSI en 2 parties :

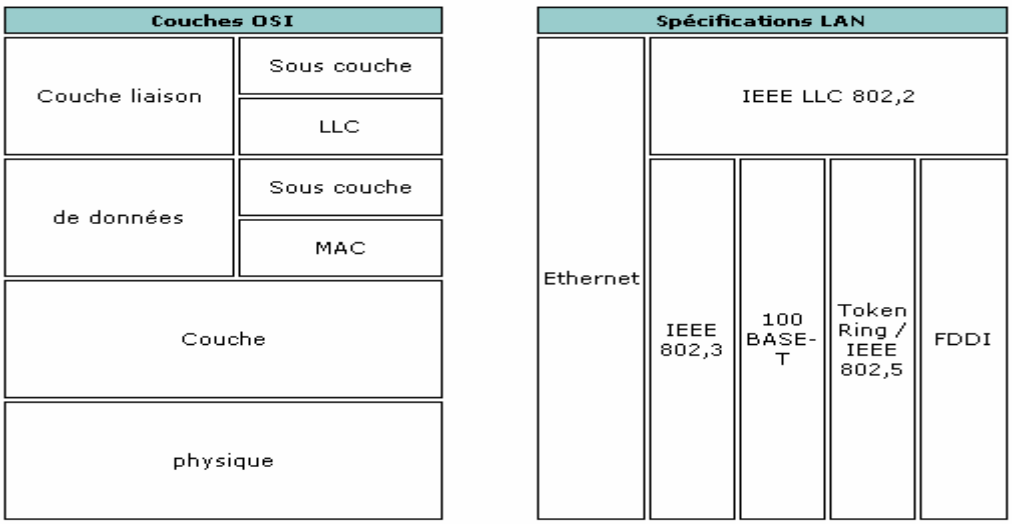
- La norme LLC 802.2, ne dépendant pas de la technologie du média utilisé
- Les éléments spécifiques, tributaires de la technologie, qui intègrent la couche physique du modèle OSI

De plus cette division sépare la couche Liaison de données en 2 parties :

- Média Access Control (MAC) : transmission vers le bas jusqu'au média
- Logical Link Control (LLC) : transmission vers le haut jusqu'à la couche réseau

La norme IEEE définit ses propres PDU, ses interfaces, et ses protocoles qui chevauchent les couches 1 et 2 du modèle OSI.

La principale raison de cette différence est le fait qu'OSI est un modèle convenu et que l'IEEE a écrit ses normes après afin de faire face à différents problèmes réseaux.
L'autre différence à noter est au niveau de la carte réseau. En effet, une carte réseau contenant l'adresse matérielle (MAC) de couche 2, elle devrait être classé dans les équipements de couche 2. Cependant, elle comprend également un émetteur récepteur de couche 1. Dès lors, il serait exact de dire qu'elle appartient aux couches 1 et 2 du modèle OSI.



Différences entre le modèle OSI et les spécifications de l'IEEE

ii. Les adresses MAC

Une adresse MAC est une adresse matérielle ; c'est-à-dire une adresse unique non modifiable par l'administrateur et stockée sur une mémoire morte (ROM) de la carte réseau.
Les adresses MAC comportent 48bits et sont exprimées sous la forme de 12 chiffres hexadécimaux :

- 6 chiffres sont administrés par l'IEEE et identifient le fabricant de la carte
- 6 chiffres forment le numéro de série de la carte

On peut les représenter de 2 manières différentes : par groupe de 4 chiffres séparés par des points ou par groupe de 2 chiffres séparés par des tirets
Exemple : 0000.0c12.3456 OU 00-00-0c-12-34-56

Les LANs de type Ethernet et 802.3 sont dés réseaux dits de broadcast, ce qui signifie que tous les hôtes voient toutes les trames. L'adressage MAC est donc un élément important afin de pouvoir déterminer les émetteurs et les destinataires en lisant les trames.
Le principal défaut de l'adressage MAC est qu'il est non hiérarchique, on ne peut pas faire de classement des adresses.

iii. Le verrouillage de trames

Une Trame est le PDU de couche 2. Le verrouillage de trame est un concept permettant de récupérer les informations essentielles normalement impossible à obtenir avec les trains binaires comme par exemple :

- Quels sont les ordinateurs en communication ?
- Début et fin de la communication
- Quelles sont les erreurs survenues ?
- Qui est autorisé à parler ?

Une trame st donc comme un tableau encadrant les bits et ajoutant les informations nécessaires à la compréhension de ces bits par les hôtes.

iv. Structure de trame générique

A	B	C	D	E	F
Champ de début de trame	Champ d'adresse	Champ de type/ longueur	Champ de Données	Champ TCS	Champ de fin de trame

Les champs d'une trame générique

- Champ de début de trames : annonce l'arrivée d'une trame
- Champ d'adresse : contient les informations d'identification (source et destination)
- Champ de longueur/type : dépend de la technologie, il peut indiquer la longueur de la trame, le protocole de couche 3 ou encore rien du tout
- Champ de données : contient les informations à transmettre, parfois accompagnés d'octets de remplissage pour que les trames aient une longueur minimale à des fins de synchronisation
- Champ de FCS : permet de détecter les erreurs, c'est une séquence de contrôle permettant au destinataire de vérifier le bon état de la trame.
    - **Exemple** : le CRC ou code de redondance cyclique : calculs polynomiaux sur les données.
- Champ de fin de trame : permet d'annoncer la fin de la trame

2. Les sous couches LLC et MAC

i. Le contrôle de lien logique (LLC)

La sous couche LLC a été crée afin de permettre à une partie de la couche liaison de données de fonctionner indépendamment des technologies existantes.

Cela assure la polyvalence des services fournis aux protocoles de couche réseau situés en amont de cette couche tout en communiquant avec les différentes technologies utilisés pour véhiculer les informations entre la source et la destination.

Le rôle de cette sous-couche est de réceptionner le paquet IP et d'y ajouter les informations de contrôle pour en faciliter l'acheminement jusqu'à la destination. Elle ajoute 2 éléments d'adressage décrit dans la spécification LLC 802.2 :

- Le point d'accès DSAP : point d'accès SAP du nœud réseau désigné dans le champ de destination du paquet
- Le point d'accès SSAP : point d'accès au service du nœud réseau désigné dans le champ source du paquet

SAP : point d'accès au service : champ de la spécification d'une adresse définie par la nome IEEE 802.2

La sous couche LLC gèle les communications entre les dispositifs sur une seule liaison réseau.
La norme IEEE 802.2 définit un certain nombre de champs dans les trames, lesquels permettent à plusieurs protocoles de couche supérieur de partager une liaison de données physique.
Ce paquet IP encapsulé se rend ensuite à la sous-couche MAC ou la technologie utilisée effectue une encapsulation supplémentaire.

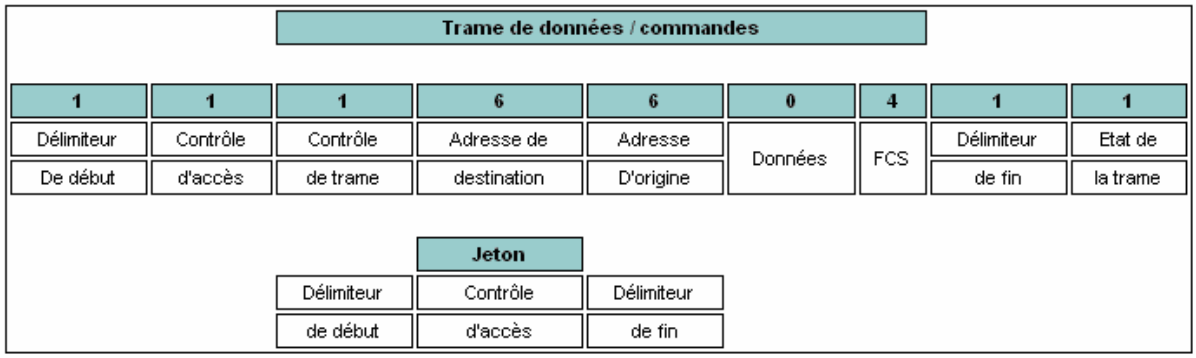
ii. La sous-couche MAC

La sous-couche MAC concerne les protocoles que doit suivre un hôte pour accéder au média. Dans un environnement de média partagé, il permet de déterminer quel ordinateur peut parler. On distingue 2 types de protocoles MAC :

- Déterministes : chacun son tour
  - Exemple : Token Ring
- Non déterministe : premier arrivé premier servi

  Exemple : Ethernet

3. Structure de trame Token ring



Structure de la trame Token Ring

Les jetons (3 octets) : composés d'un début et d'une fin de trame et d'un octet de contrôle d'accès

- octet de contrôle d'accès : comprend un champ priorité, un champ réservation, et un bit représentant le jeton plus un bit de comptage moniteur
- Le bit représentant le jeton fait la distinction entre le jeton et la trame de données/contrôle
- Le bit de comptage moniteur détermine si la trame circule constamment autour de l'anneau
- Le délimiteur de fin de trame indique la fin du jeton ou de la trame. Il contient des bits indiquant une trame endommagée et d'autre indiquant la dernière trame d'une séquence logique

Les trames de données/contrôle : leur taille varie selon la taille du champ d'information. Elles comportent des information a l'intention des protocoles de couches supérieures (trames de données) ou des informations de contrôle (trame de contrôle).

- Un octet de contrôle de trame suit l'octet de contrôle d'accès. Il indique le type de la trame. Si c'est une trame de contrôle, il indique aussi le type de contrôle
- Champs d'adresse : indique l'origine et la destination de la trame, ces adresses ont une taille de 6 octets.
- Champ de données : sa taille est limité par le jeton de l'anneau qui spécifie le temps maximal durant lequel une station peut conserver le jeton.
- FCS : contrôle d'erreur
- Délimiteur de fin de trame : indique la fin de la trame
- Etat de la trame : permet de vérifier si le destinataire a bien reçu la trame

4. Structure de trame Ethernet

Trame Ethernet

?	1	6	6	2	46-1500	4
Préambule	Délimiteur de début de trame	Adresse de destination	Adresse d'origine	Type	Données	FCS

Trame IEEE 802.3

?	1	6	6	2	64-1500	4
Préambule	Délimiteur de début de trame	Adresse de destination	Adresse d'origine	Longueur	Données	FCS

Structure de trames Ethernet et IEEE 802.3

- Préambule : composé de 1 et de 0 en alternance, annonce si la trame est de type Ethernet ou 802.3.
- Début de trame : IEEE 802.3 : l'octet séparateur se termine par 2 bits 1 consécutifs servant à synchroniser les portions de réception des trames de toutes les stations.
- Champ d'adresse d'origine : toujours de type unicast
- Champ d'adresse de destination : peut être de type unicast, multicast ou broadcast
- Type (Ethernet) : précise le type de protocole de couche supérieure qui reçoit les données
- Longueur (802.3) : indique le nombre d'octets de données qui suit le champ.
- Données :
  - Ethernet : une fois le traitement de couche 1 et 2 terminé, les données sont transmises au protocole de la couche supérieure indiqué dans le champ type. On peut avoir recours à des octets de remplissage s'il n'y a pas assez de données pour remplir les 64 octets minimaux de la trame
  - IEEE 802.3 : une fois le traitement de couche 1 et 2 terminé, les données sont transmises au protocole de la couche supérieure indiqué dans le champ donnée de la trame on peut aussi ici avoir recours a du remplissage
- FCS : Séquence de contrôle de trame. Cette séquence contient un code de redondance cyclique de 4 octets permettant à l'unité réceptrice de vérifier l'intégrité des données.

II.5 Couche 3 : La couche réseau

1. Principe de sélection du chemin

Le rôle de la couche réseau est d'acheminer les données entre l'émetteur et le destinataire au travers de différents réseaux en mettant en place un système d'adressage hiérarchique pour combiner aux manques de l'adressage MAC

Les protocoles de la couche réseau utilisent un système d'adressage garantissant l'unicité des adresses sur le réseau et définissant une méthode d'acheminement des informations entre les réseaux.

i. La sélection du chemin

Les méthodes de sélection du chemin permettent aux équipements de couche 3 ; les routeurs ; de déterminer la route à suivre pour acheminer les informations au travers de différents réseaux.

Les services de routage utilisent les informations de topologie du réseau pour évaluer les chemins. Ce processus est aussi appelé routage des paquets et prend en compte divers paramètres ; ou métriques ; comme :

- Densité du trafic
- Nombre de routeurs à franchir pour joindre la destination
- Vitesse des liaisons
- Etc….

ii. L'adressage de la couche réseau

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole TCP/IP qui utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits), on les note donc sous la forme xxx.xxx.xxx.xxx où chaque xxx représente un entier de 0 à 255.

Ces numéros servent aux ordinateurs du réseau pour se reconnaître, ainsi il ne doit pas exister deux ordinateurs sur le réseau ayant la même adresse IP.

iii. Protocoles routables, non routables

Un protocole routable est un protocole pouvant être acheminé au travers de différents réseaux.
Exemple :

- IP
- IPX
- Appletalk

Par opposition, un protocole non routable ne peut être routé
Exemple :

NetBEUI

2. Principe de l'adressage IP

Il existe deux versions d'adresse IP dans l'utilisation aujourd'hui. Presque tous les réseaux emploient l'adresse IP version 4 (IPv4), mais un nombre croissant d'éducatif et les réseaux de recherches ont adopté l'adresse IP version 6 (IPv6). Nous allons présenter le détail de l'IPv4 dans ce chapitre.

L'adresse IP d'une machine est appelée une adresse logique

Elle est codée sur 32 bits soit 4 octets. La notation consiste à indiquer chaque octet en décimal et à les séparer par des points ".".

L'adresse IP d'un ordinateur est composée de deux parties :

-La première partie est appelée NetID, correspond à l'adresse du réseau, aussi appelé identifiant réseau. L'identifiant réseau identifie les systèmes qui sont situés sur le même réseau physique. NetID doit être unique au segment local.

-La deuxième partie est appelée HostID, correspond à l'adresse de la machine sur le réseau, aussi appelé identifiant machine. L'identifiant machine identifie un poste de travail, le serveur, le routeur, ou tout autre dispositif de TCP/IP dans un réseau. Le HostID pour chaque dispositif doit être unique à l'identifiant de réseau. Un ordinateur relié à un réseau de TCP/IP emploie le NetID et le HostID pour déterminer quels paquets il devrait recevoir ou ignorer et déterminer quels dispositifs doivent recevoir ses transmissions.

Les adresses IP ne peuvent communiquer qu'avec des adresses ayant le même numéro de réseau, y compris si des stations se trouvent sur le même segment.

Voici un exemple:

11000100	11101001	11111101	01111011
196	233	253	123

196.233.253. 123
NetID HostID

Chaque octet dans des chaînes d'une adresse IP est en valeur d'un minimum de 0 au maximum de 255. Le champ complet des adresses IP est de 0.0.0.0 à 255.255.255.255. Cela représente un total de 4.294.967.296 adresses IP possibles.

i. Les classes d'adresse IP

Actuellement l'organisme chargé d'attribuer les adresses IP est l'INTERNIC (Internet Network Information Center)
Les adresses IP sont réparties en plusieurs classes, en fonction des bits qui les composent :
Classe A : Dans une adresse IP de classe A, le premier octet représente le réseau. Le bit de poids fort (le premier bit, celui de gauche) est à zéro, ce qui signifie qu'il y a 27 (00000000 à 01111111) possibilités de réseaux, c'est-à-dire 128.
Toutefois le réseau 0 (00000000) n'existe pas et le nombre 127 est réservé pour désigner votre machine, les réseaux disponibles en classe A sont donc les réseaux allant de 1.0.0.0 à 126.0.0.
Les trois octets de droite représentent les ordinateurs du réseau, le réseau peut donc contenir:
224-2 = 16777214 ordinateurs.
Une adresse IP de classe A, en binaire, ressemble à ceci:
0 xxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Classe B : Dans une adresse IP de classe B, les deux premiers octets représentent le réseau. Les deux premiers bits sont 1 et 0, ce qui signifie qu'il y a 214 (10 000000 00000000 à 10 111111 11111111) possibilités de réseaux, c'est-à-dire 16384.
Les réseaux disponibles en classe B sont donc les réseaux allant de 128.0.0.0 à 191.255.0.0
Les deux octets de droite représentent les ordinateurs du réseaux, le réseau peut donc contenir:
216-21 = 65534 ordinateurs.
Une adresse IP de classe B, en binaire, ressemble à ceci:
10 xxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Classe C : Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1,1 et 0, ce qui signifie qu'il y a 221 possibilités de réseaux, c'est-à-dire 2097152. Les réseaux disponibles en classe C sont donc les réseaux allant de 192.0.0.0 à 223.255.255.0
L'octet de droite représente les ordinateurs du réseau, le réseau peut donc contenir:
28-21 = 254 ordinateurs.
Une adresse IP de classe C, en binaire, ressemble à ceci:
110 xxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Classe D :

Cette classe d'adresse est réservée pour le multicast : la diffusion vers des machines d'un même groupe.
L'adressage est de 224.0.0.0 à 239.255.255.255
Le multicast est plutôt utilisé dans les réseaux de recherche. Il n'est pas utilisé dans le réseau normal.

Classe E :
Réservée pour le futur.
Elles ne devraient pas être employées sur des réseaux IP. Quelques organisations de recherche utilisent les adresses de la classe E pour des buts expérimentaux.

Il arrive fréquemment dans une entreprise qu'un seul ordinateur soit relié à Internet, c'est par son intermédiaire que les autres ordinateurs du réseau accèdent à Internet (on parle généralement de proxy).
Dans ce cas, seul l'ordinateur relié à Internet a besoin de réserver une adresse IP auprès de l'INTERNIC. Toutefois, les autres ordinateurs ont tout de même besoin d'une adresse IP pour pouvoir communiquer ensemble de façon interne.
Ainsi, l'INTERNIC a réservé une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à Internet sans risquer de créer de conflits d'adresses IP sur le réseau. Il s'agit des adresses suivantes:

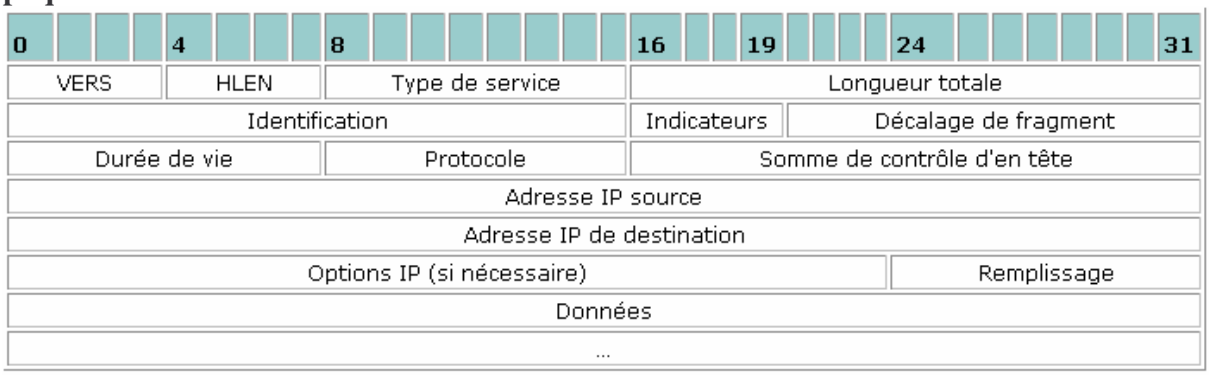
- 10.0.0.1 à 10.255.255.254
- 172.16.0.1 à 172.31.255.254
- 192.168.0.1 à 192.168.255.254

ii - Adresse de réseau et adresses de broadcast
Une adresse réseau est une adresse IP dont tous les bits hôtes sont occupés par des 0 binaires. Cette adresse désigne le réseau lui-même et non pas un hôte précis.
Exemple, dans un réseau de classe A, 113.0.0.0 désigne le réseau comprenant l'hôte 113.1.2.3.
L'adresse de broadcast est une adresse utilisée pour joindre en même temps tous les hôtes d'un réseau. Tous les bits hôtes de celle-ci sont à 1.
Exemple : pour le réseau 192.168.10.0, l'adresse de broadcast est 192.168.10.255

Broadcast : envoi de données à tous les hôtes d'un réseau

Ces adresses ne peuvent donc pas être utilisée pour identifier un hôte sur le réseau

iii - Les datagrammes de la couche réseau
Les informations provenant de la couche 4 sont encapsulés dans le PDU de couche 3 : **le paquet**



Structure de l'en-tête IP

- Version : - Indique la version de protocole IP utilisée (4 bits).
- HLEN (IP header length) : - Longueur de l'en-tête IP - indique la longueur de l'en-tête du datagramme en mots de 32 bits (4 bits)
- Type de service : - Indique l'importance qui lui a été accordée par un protocole de couche supérieure donné (8 bits).

- Longueur totale : - Précise la longueur du paquet IP en entier, y compris les données et l'en-tête, en octets (16 bits).
- Identification : - Contient un nombre entier qui identifie le datagramme actuel (16bits).
- Indicateurs : - Un champ de 3 bits dont les 2 bits inférieurs contrôlent la fragmentation :
  - un bit précise si le paquet peut être fragmenté
  - le second indique si le paquet est le dernier fragment d'une série de paquets fragmentés.
- Décalage de fragment : - Ce champ sert à rassembler les fragments du datagramme (13 bits
- Durée de vie :
  - Un compteur qui décroît graduellement, par incréments, jusqu'à zéro. À ce moment, le datagramme est supprimé, ce qui empêche les paquets d'être continuellement en boucle (8 bits)
- Protocole :
  - Précise le protocole de couche supérieure qui recevra les paquets entrants après la fin du traitement IP (8 bits).
- Somme de contrôle d'en-tête :

- Assure l'intégrité de l'en-tête IP (16 bits).
- Adresse d'origine :

- Indique le nœud émetteur (32 bits).
- Adresse de destination :

- Indique le nœud récepteur (32 bits).
- Options :
  - Cet élément permet au protocole IP de supporter différentes options, telles que la sécurité (longueur variable).
- Données :
  - Cet élément contient des informations de couche supérieure (longueur variable, maximum 64 Ko).
- Remplissage :
  - Des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP est toujours un multiple de 32 bits.

3. Les sous réseaux

Subnetting : On utilise une seule adresse IP pour créer d'autres sous réseaux.

Pourquoi subnetting ou pourquoi le sous-réseau?

- Ils permettent aux réseaux locaux physiquement à distance d'être reliés.
- Un mélange des architectures de réseau peut être relié, comme l'Ethernet sur un segment et le Token ring sur des autres.
- Ils permettent à un nombre illimité de machines de communiquer en combinant des sous-réseaux, par contre, le nombre de machines sur chaque segment est limité par le type de réseau utilisé.
- La congestion de réseau est réduite comme les diffusions et chaque trafic local de réseau est limité au segment local.

Caractéristique

- Un réseau IP de classe A, B ou C peut être découpé en sous-réseaux.
- Chaque sous-réseau peut être découpé en sous-sous-réseaux et ainsi de suite.
- Il y a de même notion pour le réseau et le sous-réseau.
- Chaque sous-réseau a un seul identifiant réseau unique et il exige un masque de réseau pour le sous-réseau.

i. Les masques de réseau

Pour connaître la partie réseau (NetID) et la partie machine (HostID) de l'adresse IP, il suffit d'utiliser le "NetMask" ou masque de réseau. Pour obtenir NetID, il faut effectuer un ET (AND) bit à bit entre l'adresse IP et le NetMask. Pour obtenir l'identifiant machine, il faut effectuer un ET bit à bit entre l'adresse IP et le masque de réseau complémenté à 1.

Exemple : Une adresse IP de classe C : 192.168.4.211 avec le masque de réseau 255.255.255.0

11000000 10101000 00000100 11010011
Et
11111111 11111111 11111111 00000000

11000000 10101000 00000100 00000000
192 . 168 . 4 . 0

L'identifiant réseau est : 192.168.4, on peut également écrire NetID : 192.168.4.0
L'identifiant machine est : 211

ii - Création de sous réseau

Il est nécessaire de bien déterminer les points suivants avant de faire Subnetting :

- Déterminer le nombre d'identifiant réseau requises pour l'usage courant et également pour l'évolution dans le futur
- Déterminer le nombre maximum des machines de chaque sous-réseau, tenant compte encore de la croissance dans le futur
- Définir un masque de réseau pour le sous-réseau entier
- Déterminer les identifiants sous-réseau qui sont utilisables
- Déterminer les identifiants machines valides et assigner les adresses IP aux postes de travail

Exemple :

Le réseau de classe C, NetID : 192.168.1.0 avec le masque par défaut 255.255.255.0. On veut découper ce réseau en 2 sous-réseaux.

+ Calculer le nombre de sous-réseau

Si l'on utilise 1 bit -> 2^1 = 2 sous-réseaux, mais le bit de haut et le bit de bas ne sont pas utilisés. Donc, il faut au moins deux bits.

Si l'on utilise 2 bits -> 2^2 = 4 sous-réseaux, mais il n'y a que deux qui sont utilisables. Donc, on utilise maintenant 2 bits pour pouvoir découper en 2 sous-réseaux.

+ Calcul du masque de sous-réseau

Le masque de chaque sous-réseau est obtenu en rajoutant 2 bits à 1 au masque initial.

Le masque de réseau par défaut est 255.255.255.0 :

Soit 11111111 11111111 11111111 00000000

En ajoutant 2 bits on obtient

11111111 11111111 11111111 11000000

En fin, on a le masque de sous-réseau : 255.255.255.192

+ Calcul du NetID de chaque sous-résseau

- Le NetID de chaque sous-réseau sera constitué de 26 bits
- Les 24 premiers bits seront ceux de l'écriture en binaire de 192.168.1.
- Les 2 bits suivants seront constitués du numéro du sous-réseau 00, 01, 10, 11
- Parmi les 4 numéros de sous-réseaux, 2 seront interdits (00 et 11) : bits de haut et bit de bas.
- Il reste donc 2 numéros de sous-réseau utilisables.

+ Calcul des adresses des sous-réseaux

192.168.1.00xxxxxx - Non utilisable
192.168.1.01xxxxxx - Utilisable
192.168.1.10xxxxxx - Utilisable
192.168.1.11xxxxxx - Non utilisable
Les deux identifiant sous-réseaux sont 192.168.1.64 et 192.168.1.128

+ Calcul des HostID des sous-réseaux

- Adresse IP de Premier sous-réseau : 192.168.1.64

192.168.1.01000000 : Non utilisable
192.168.1.01000001 = 192.168.1.65
192.168.1.01000010 = 192.168.1.66 _
. |
. | 62 machines
. |
192.168.1.01111110 = 192.168.1.126 ¯
192.168.1.01111111 : Non utilisable

L'adressage du premier sous-réseau est de 192.168.1.65 à 192.168.1.126

- Adresses IP de Deuxième sous-réseau : 192.168.1.128

192.168.1.10000000 : Non utilisable
192.168.1.10000001 = 192.168.1.129
192.168.1.10000010 = 192.168.1.130 _
. |
. | 62 machines
. |
192.168.1.10111110 = 192.168.1.190 ¯
192.168.1.10111111 : Non utilisable

L'adressage du deuxième sous-réseau est de 192.168.1.129 à 192.168.1.190

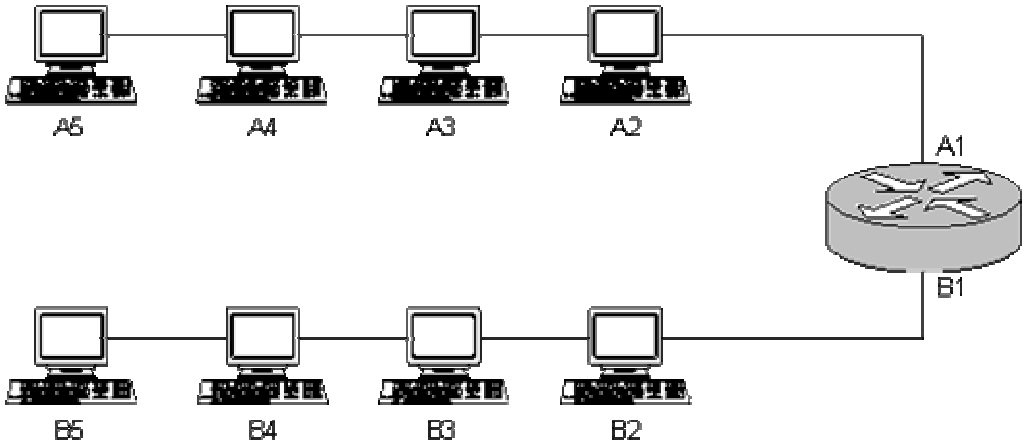
- Adresses de diffusion

Pour obtenir l'adresse de diffusion dans chaque sous-réseau; on met à 1 tous les bits de HostID.
L'adresse de diffusion de premier sous-réseau est 192.168.1.01111111, soit 192.168.1.127.
L'adresse de diffusion de deuxième sous-réseau est 192.168.1.10111111, soit 192.168.1.191

4. Les équipements de couche 3 : les routeurs

Routeur : équipement de couche 3 permettant d'inter connecter 2 réseaux ou plus en se basant sur les adresses de couche 3. Le routeur permet également une segmentation des domaines de broadcasts

Le routeur dispose d'une interface (une carte réseau) le reliant au réseau local. Celle-ci dispose d'une adresse IP. Par exemple, sur le schéma ci-dessous, les adresses des hôtes sont A5, A4, A3 et A2, faisant partie du réseau A. On attribue A1 à l'interface du routeur, lui permettant ainsi de se connecter au réseau A.
Un autre réseau ; B ; est lui aussi connecté au routeur. Ce dernier dispose donc d'une interface ayant pour IP B1 afin de pouvoir communiquer avec le réseau.



Exemple de topologie

Supposons maintenant que l'on souhaite envoyer des données de A vers B :

- Le routeur reçoit la trame de couche 2, supprime l'en tête de liaison de données
- Il examine l'adresse de couche 3 afin de déterminer le destinataire
- Il effectue un ET logique entre l'adresse IP et le masque de sous réseau afin de déterminer le réseau de destination
- Il consulte sa table de routage pour déterminer l'interface par laquelle les données doivent être envoyées.

C'est pour cela que chaque interface du routeur doit être sur un réseau différent. Sinon le routeur ne pourra pas déterminer par quelle interface envoyer les informations.

5. Les communications de réseau à réseau

i. Les méthodes d'attribution d'adresse IP

On distingue 2 méthodes d'attribution d'adresses IP pour les hôtes :

- Statique : chaque équipement est configuré manuellement avec une adresse unique
- Dynamique : On utilise des protocoles qui attribue des IP aux hôtes
  - RARP : protocole associant les adresses MAC aux adresses IP. Il permet à des stations ans disque dur local connaissant leur adresse MAC de se voir attribuer une IP.
  - BOOTP : Ce protocole permet à un équipement de récupérer son adresse IP au démarrage. L'émetteur envoi un message de broadcast (255.255.255.255) reçu par le serveur qui répond lui aussi par un broadcast contenant l'adresse MAC de l'émetteur ainsi qu'une IP.

- DHCP : Remplaçant de BOOTP, il permet l'obtention dynamique d'IP. Lorsqu'un ordinateur entre en ligne, il communique avec le serveur qui choisit une adresse et l'attribue à l'hôte. Avec le protocole DHCP, il est également possible pour un ordinateur de récupérer sa configuration complète (adresse, masque de sous réseau, etc.)

Démarrage du client
Initialisation
Envoi d'un message de broadcast **(DHCP DISCOVER)**
(Paquet UDP utilisant le port de BOOTP)
Passage à l'état de sélection, récupère les messages du serveur **(DHCPOFFER)**
Négociation de la durée du bail (durée d'attribution de l'IP)
Envoi de l'accusé de réception
Réception par le serveur, renvoi d'un accusé de réception **(DHCPACK)**

Séquence d'initialisation DHCP

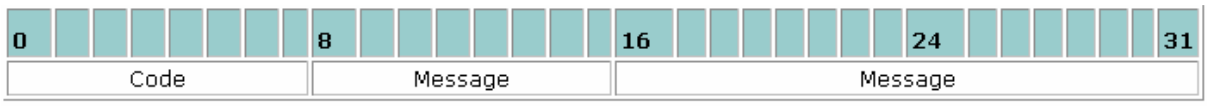
ii. Le protocole ARP

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse (en anglais ARP signifie Address Resolution Protocol).
Chaque machine connectée au réseau possède un numéro d'identification de 48 bits. Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte en usine. Toutefois la communication sur Internet ne se fait pas directement à partir de ce numéro (car il faudrait modifier l á'adressage des ordinateurs à chaque fois que l'on change une carte réseau) mais à partir d'une adresse dite logique attribuée par un organisme: l'adresse IP.
Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.
Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance. Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête sur le réseau. L'ensemble des machines du réseau vont comparer cette adresse logique à la leur. Si l'une d'entre-elles s'identifie à cette adresse, la machine va répondre à ARP qui va stocker le couple d'adresses dans la table de correspondance et la communication va alors pouvoir avoir lieu...

iii. Le protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées. Etant donné le peu de contrôles que le protocole IP réalise il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour reporter une erreur (appelé Delivery Problem).
Les messages d'erreur ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi, les messages d'erreur peuvent eux-mêmes être á sujet d'erreurs.

Toutefois en cas d'erreur sur un datagramme transportant un message ICMP, aucun message d'erreur n'est délivré pour éviter un effet "boule de neige" en cas d'incident sur le réseau.



Structure d'un paquet ICMP

6. Les protocoles de routage

Pour sélectionner le chemin, nous avons vu que le routeur utilisait sa table de routage. Une table de routage fait la correspondance entre les réseaux et les interfaces du routeurs qui leur sont connectés. Il existe 2 manières de mettre à jour ces tables. La première est le routage statique, ou l'administrateur configure manuellement les routes que le routeur doit utiliser. La seconde consiste en l'utilisation de protocoles dits de « routage », permettant l'échange d'informations sur la topologie du réseau entre les différents routeurs.

Ces protocoles permettent donc aux routeurs de cartographier le meilleur chemin vers n'importe quel autre routeur ou segment réseau dans le même réseau ou encore sur Internet.

Ces échanges de messages sont consommateurs de bande passante ; ce qui présente un désavantage par rapport au routage statique ; cependant, le routage dynamique permet une meilleure réactivité du réseau aux pannes car celui-ci peut d'adapter de lui-même aux changements de topologie.

Il existe de nombreux protocoles de routage, chacun utilisant certaines caractéristiques du réseau pour fonder ses décisions. Ces caractéristiques ; pouvant être la bande passante, la fiabilité ou encore l'encombrement d'un segment ; sont appelées des métriques.

i. Exemple de protocole de routage : le protocole RIP

RIP est le protocole le plus utilisé à ce jour dans les réseaux actuels. Il calcule la distance jusqu'à un hôte en mesurant le nombre de sauts (routeurs) et privilégie le chemin le plus court.

On appelle ce type de protocole basé sur le nombre de sauts des protocoles de routage à vecteur de distance.

Le protocole RIP met à jours les tables de routage toutes les 30 secondes et autorise un nombre de saut maximal de 15.

ii. Les différents protocoles de routage

Système autonome : ensemble d'équipements gérés par la même administration

Une première classification se fait entre les protocoles de routage selon qu'ils soient :

IGP : Interior Gateway Protocol (dans un système autonome)

EGP : Exterior Gateway Protocol (entre les systèmes autonomes)

Parmi les protocoles IGP les plus courant, on retrouve :

- IGRP : développé pour résoudre les problèmes associés au routage dans de grands réseaux multi fournisseurs, c'est un protocole à vecteur de distance, cependant il prend également en compte d'autres métriques qu'il est possible de pondérer afin de privilégier certains aspects du chemin :
- bande passante
- charge
- délai
- fiabilité

- EIGRP : version améliorée d'IGRP.
- OSPF : Open Shortest Path First. Protocole dit de « routage à état de lien », il incluse des métriques de coûts tenant compte de :
- la vitesse d'acheminement
- du trafic
- de la fiabilité
- de la sécurité

7. Les services réseau de la couche 3

i. Les services réseau non orientés connexion (commutation de paquets)

La plupart des services réseaux utilisent de livraison non orientée connexion. Ils traitent chaque paquet séparément. Il se peut que les paquets empruntent des chemins différents et sont rassemblés lorsqu'ils arrivent à destination.
Dans un système non orienté connexion le destinataire n'est pas contacté avant la réception des paquets, comme c'est le cas par exemple pour les services postaux.
Internet est un immense réseau non orienté connexion au sein duquel le protocole IP transporte les paquets. Le protocole TCP (couche 4) y ajoute des services orientés connexion au dessus du protocole IP afin d'assurer une distribution fiable des données.

ii. Les services réseau orientés connexion (commutation de circuits)

Une connexion est établie entre l'émetteur et le destinataire avant le transfert des données. Un exemple de ce système est le système téléphonique.
Tous les paquets sont donc acheminés dans le même circuit physique ou ; plus souvent ; dans le même circuit virtuel.

iii. Le routage indirect

Le protocole IP permet également l'utilisation d'une « passerelle par défaut » c'est-à-dire l'utilisation d'une route à utiliser si le routeur ne connaît pas le réseau de destination.
Si un routeur reçoit un paquet dont il ne connaît pas le réseau de destination, il le transmet donc à un autre routeur susceptible de le connaître.

II.6 Couche 4 : La couche transport

1. La couche transport

i. Fonction de la couche transport

Nous avons vu dans les chapitres précédents comment TCP/IP envoie les informations de l'émetteur au destinataire. La couche transport ajoute à ce mécanisme la notion de « qualité de service », à savoir la garantie d'un acheminement fiable des informations au travers du réseau.

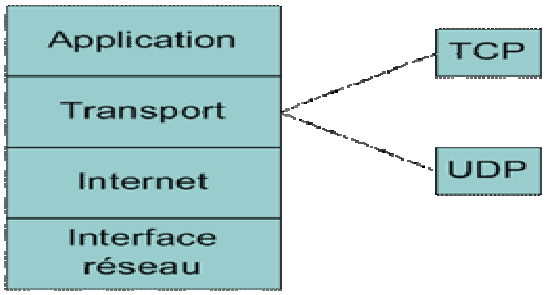
ii. Les protocoles de couche 4

Le protocole TCP/IP de la couche 4 comprend 2 protocoles : TCP et UDP
TCP est un protocole orienté connexion, c'est-à-dire qu'il associe aux transport des informations la notion de qualité en offrant les services suivants :
- fiabilité
- division des messages sortants en segments
- ré assemblage des messages au niveau du destinataire
- ré envoi de toute donnée non reçu

Segments : PDU de couche 4

UDP est lui un protocole non orienté connexion, c'est-à-dire qu'il n'offre pas de fonction de contrôle du bon acheminement :
- aucune vérification logicielle de la livraison des messages
- pas de réassemblage des messages entrants
- pas d'accusé de réception
- aucun contrôle de flux

Cependant, UDP offre l'avantage de nécessiter moins de bande passante que TCP. Il peut donc être intéressant d'utiliser ce protocole pour l'envoi de messages ne nécessitant pas de contrôle de qualité.



TCP et UDP

iii. TCP comme complément d'IP

A IP qui offre un service sans connexion de couche 3 permettant l'acheminement des données au sein d'un réseau s'ajoute TCP ; un protocole de couche 4 ; qui ajoute les capacités de contrôle de flux et de fiabilité de transmission.
Pour faire une analogie avec le système postal, IP serait un exemple d'envoi de courrier ordinaire auquel TCP ajoute le service d'envoi recommandé, garantissant à l'émetteur la remise de la lettre.

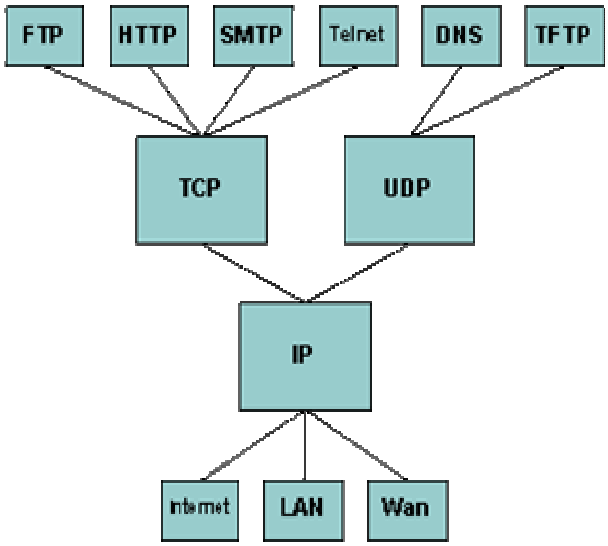


Schéma de protocoles

2. TCP et UDP

i. Les numéros de ports

Afin que plusieurs communications puissent circuler en même temps, TCP et UDP utilisent des numéros de ports. Des conventions ont été établies pour des applications :

Protocole	n° de port	Description
ftp-data	**20**	**File Transfer [données par défaut]**
ftp	**21**	**File Transfer [contrôle]**
ssh	22	SSH
telnet	**23**	**Telnet**
smtp	**25**	**Simple Mail Transfer**
time	37	Time
nicname	43	Who Is
domain	**53**	**Domain Name Server**
sql*net	66	Oracle SQL*NET
gopher	70	Gopher
http	**80**	**World Wide Web http**
pop3	**110**	**Post Office Protocol - Version 3**
auth	113	Authentication Service
sftp	115	Simple File Transfer Protocol
sqlserv	118	SQL Services
nntp	119	Network News Transfer Protocol
ntp	123	Network Time Protocol
imap2	143	Interactive Mail Access Protocol v2
news	144	NewS
ipx	213	IPX
https	**443**	**Protocole HTTP sécurisé**

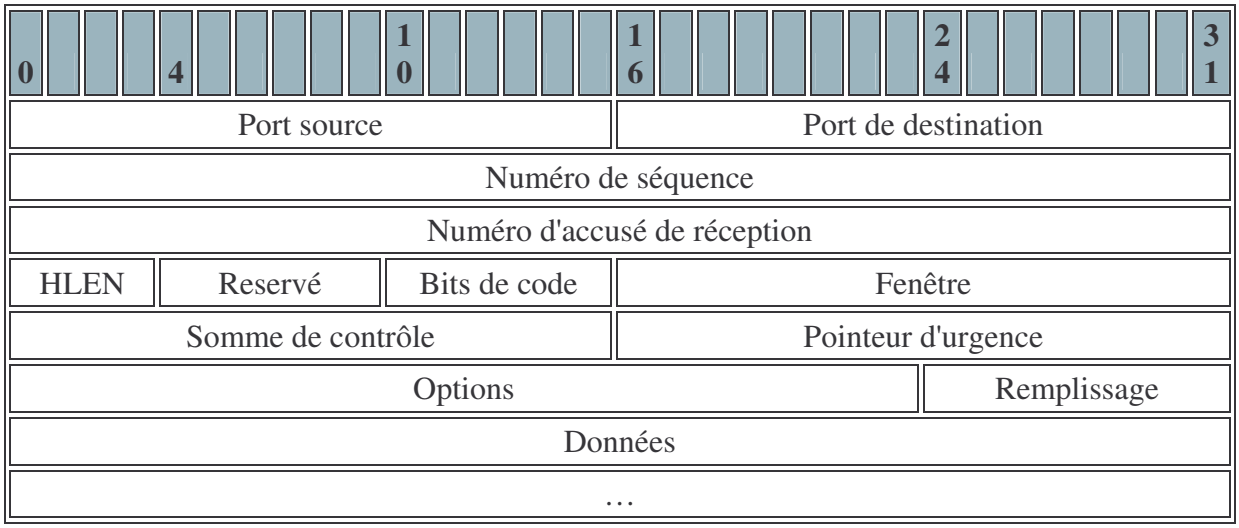
Numéros de ports

Toute application n'ayant pas un numéro de port définit et reconnu se voient attribué un numéro de port aléatoire.
Les ports ont été attribués de la manière suivante :

- 0 à 255 réservés aux applications publiques
- 255 à 1023 attribué aux entreprises pour les applications commerciales
- 1023 à + utilisés pour les attributions dynamiques

ii. Structure d'un segment TCP

Le protocole TCP encapsule les informations provenant de la couche supérieure dans des segments dont voici la structure :



Structure d'un segment TCP

- Port d'origine à Numéro du port appelant
- Port de destination à Numéro du port appelé
- Numéro de séquence à Numéro utilisé pour assurer le séquençage correct des données entrantes
- N° d'accusé de réception à Prochain octet TCP attendu
- HLEN à Nombre de mots de 32 bits contenus dans l'en-tête
- Réservé à Défini sur zéro
- Bits de code à Fonctions de contrôle (telles l'ouverture et la fermeture d'une session
- Fenêtre à Nombre d'octets que l'émetteur est prêt à accepter
- Somme de contrôle à Somme de contrôle calculée des champs d'en-tête et de données
- Pointeur d'urgence à Indique la fin des données urgentes
- Données à Données du protocole de couche supérieure

iii. Structure d'un datagramme UDP

UDP étant un protocole non orienté connexion, il dispose d'un en tête de taille réduite par rapport aux en têtes des segments TCP :

16	16	16	16	,,,
Port Source	Port de destination	Longueur	Somme de contrôle	Données

Structure d'un datagramme UDP

Le protocole UDP est conçu pour les applications ne devant pas assembler de séquences de segments. Il laisse aux protocoles de la couche application le soin d'assurer la fiabilité.

3. Les méthodes de connexion TCP

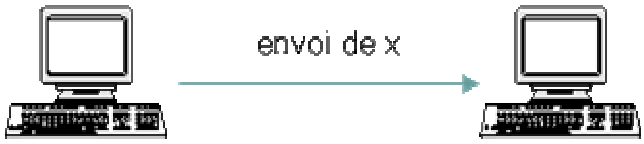
Un service orienté connexion comportent 3 points importants :

- Un chemin unique entre les unités d'origine et de destination est déterminé
- Les données dont transmises de manière séquentielle et arrivent à destination dans l'ordre
- La connexion est fermée lorsqu'elle n'est plus nécessaire

i. Connexion ouverte/échange à trois

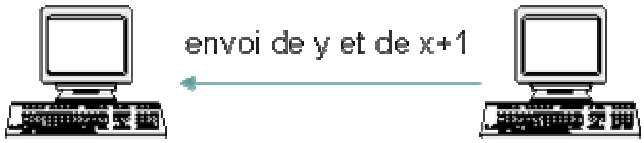
Les hôtes TCP établissent une connexion en 3 étapes, appelé aussi « connexion ouverte » :

- L'émetteur envoie un paquet avec un numéro de séquence initial (x) avec un bit dans l'en-tête pour indiquer une demande de connexion.



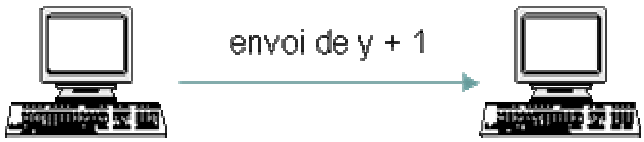
Etape n°1 de la connexion TCP

- Le destinataire le reçoit, consigne le numéro de séquence initial, répond par un accusé de réception «x+1 » et inclut son propre n° de séquence (y).



Etape n°2 de la connexion TCP

- L'émetteur reçoit x+1 et renvoie y+1 pour dire au destinataire que la réception s'est bien passée.

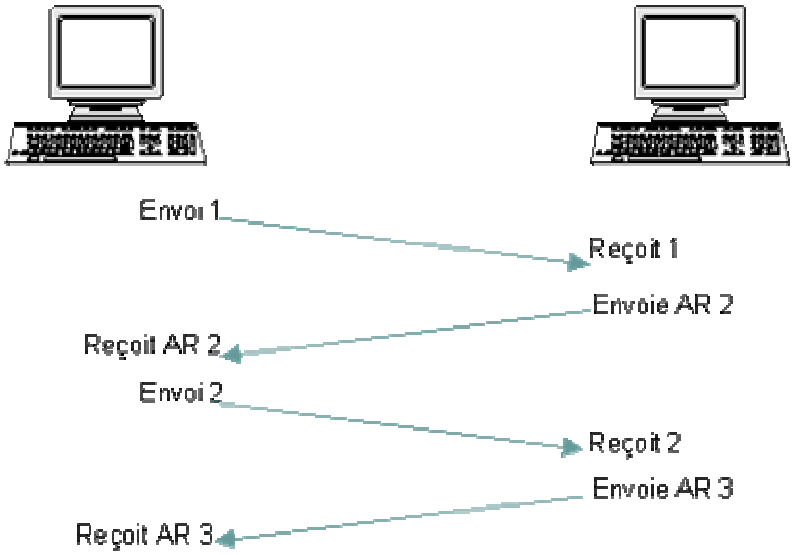


Etape n°3 de la connexion TCP

Quand l'émetteur reçoit x+1, cela signifie que le destinataire a bien reçu tout les paquets ayant pour n° de séquence x et moins et attend la suite.
Il existe également des méthodes garantissant la fiabilité des protocoles

ii. Positive Acknowledgement Retransmission

La technique Positive Acknowledgement Retransmission ; ou PAR ; consiste à envoyer un paquet, démarrer un compteur puis attendre un accusé de réception avant d'envoyer le suivant.
Si le compteur arrive à expiration avant l'arrivé de l'accusé, les informations sont alors retransmises et un nouveau compteur est déclenché.
Cependant, cette technique est consommatrice de bande passante ; c'est alors qu'intervient le mécanisme de fenêtrage.



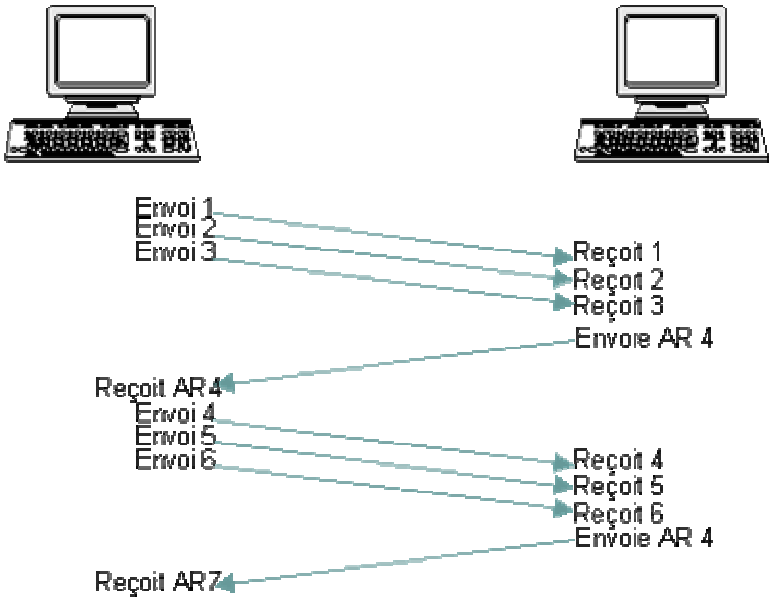
Principe de PAR

iii - Le Fenêtrage

Le Fenêtrage est un mécanisme dans lequel le récepteur envoi un accusé de réception après avoir reçu un certain nombre de données. Si le destinataire n'envoi pas d'accusé, cela signifie pour l'émetteur que les informations e sont pas parvenues correctement et dans ce cas sont retransmises.

La taille de la fenêtre détermine la quantité de données que l'on peut transmettre avant de recevoir un accusé de réception.

TCP utilise un système d'accusé de réception prévisionnel, ce qui signifie que le numéro d'accusé renvoyé indique la prochaine séquence attendue



Echange TCP fenêtrée avec une fenêtre de 3

II.7. Couche 5 : La couche session

1. Présentation

Une session est un ensemble de transaction entre deux unités réseau ou plus.
Une analogie pour comprendre la couche session est une communication entre plusieurs individus. Si l'on souhaite que la conversation se déroule correctement, il est impératif de mettre en place diverses règles, afin que les interlocuteurs ne s'interrompent pas par exemple.
Cette notion de contrôle du dialogue est le point essentiel de la couche session.
Le rôle de la couche session est d'ouvrir, gérer et fermer les sessions entre les applications. Cela signifie que c'est elle qui prend en compte :

- le lancement des sessions
- la resynchronisation du dialogue
- l'arrêt des sessions

Elle coordonne donc les applications qui communiquent au travers des hôtes.
Une communication entre ordinateurs suppose de nombreuses conversations courtes (commutation de paquets) avec en plus de cela d'autres communications pour s'assurer de l'efficacité de la communication.
Ces conversations nécessite que les hôtes jouent à tour de rôles de client (demandeur de services) et de serveur (fournisseur de services).
Le contrôle du dialogue consiste en l'identification des rôles de chacun à un moment donné.

2. Le contrôle du dialogue

La couche session décide si la conversation sera de type bidirectionnel simultané ou alterné. Cette décision relève du contrôle du dialogue.

- Si la communication bidirectionnelle simultanée est permise :

- La gestion de la communication est assurée par d'autres couches des ordinateurs en communication.

- Si ces collisions au sein de la couche session sont intolérables, le contrôle de dialogue dispose d'une autre option : la communication bidirectionnelle alternée

- Ce type de communication est rendu possible par l'utilisation d'un jeton de données au niveau de la couche session qui permet à chaque hôte de transmettre à tour de rôle.

3. La synchronisation du dialogue

Cette étape est des plus importante, elle permet aux hôtes communicants dans marquer une pause pour par exemple sauvegarder la communication en cours et re synchroniser le dialogue.
Pour cela est utilisé un « point de contrôle », envoyé par l'un des interlocuteurs à l'autre pour enregistrer la conversation, vérifier l'heure de la dernière portion de dialogue effectuée. Ce processus est appelé *la synchronisation du dialogue.*
Comme dans le langage humain ; il est important dans une discussion de montrer à son interlocuteur le début d'une conversation (« allo » dans le cas d'une conversation téléphonique) ainsi que de signifier que l'on se prépare à mettre fin à la conversation. C'est pour cela que les deux contrôles principaux sont :

- lancement ordonné
- fin de la communication

4. La division du dialogue

La division du dialogue englobe le lancement, la fin et la gestion ordonnés de la communication.

Notre schéma représente une petite synchronisation. Au niveau du point de contrôle, la couche session de l'hôte A envoie un message de synchronisation à l'hôte B, et les deux hôtes exécutent la séquence qui suit :

- sauvegarder les fichiers donnés
- sauvegarder les paramètres réseau
- sauvegarder les paramètres de synchronisation
- noter le point d'extrémité de la conversation.

Les points de contrôle sont semblables à la manière dont un logiciel de traitement de texte fait une pause d'une seconde pour effectuer la sauvegarde automatique d'un document sur un ordinateur autonome. Ces points de contrôle servent toutefois à séparer les parties d'une session, préalablement appelées dialogues.

II.8 Couche 6 : La couche présentation

1. Fonction et normes de la couche présentation

L'un des rôles de la couche présentation est de présenter les données dans un format que le dispositif récepteur est capable de comprendre. La couche présentation joue donc un rôle d'interprète entre les unités qui doivent communiquer par le biais d'un réseau.

La couche 6, la couche présentation, assure trois fonctions principales, à savoir :

- Le formatage des données (présentation)
- Le cryptage des données
- La compression des données

Après avoir reçu les données de la couche application, la couche présentation exécute certaines ou toutes ces fonctions avant d'acheminer les données à la couche session.

Au niveau de la station de réception, la couche présentation reçoit les données de la couche session et exécute les fonctions nécessaires avant de les faire suivre à la couche application.

Les normes de la couche 6 définissent également la présentation des graphiques. Les trois principaux formats graphiques sont :

- PICT - Format d'image servant à transférer des graphiques QuickDraw entre des applications exécutées sous le système d'exploitation MAC-OS
- TIFF (Tagged Image File Format) - Format de fichier graphique utilisé pour les images " bitmap " haute résolution.
- JPEG (Joint Photographic Experts Group) - Format graphique le plus utilisé pour la compression des images fixes complexes et des photographies.

D'autres normes de la couche 6 concernent la présentation des sons et des séquences animées. Les normes suivantes appartiennent à cette catégorie :

- MIDI (Musical Instrument Digital Interface) - Format pour la musique électronique.
- MPEG (Motion Picture Experts Group) - Format de compression et de codage de vidéo animée pour CD ou tout autre support de stockage numérique.
- QuickTime - Format de données audio et vidéo destiné aux applications exécutées sous les systèmes d'exploitation MAC et PC.

Les normes de la couche présentation établissent donc des standards de formats de fichier afin que les hôtes soient en mesure de comprendre les informations.

2. Cryptage et compression des données
La couche 6 est également responsable du cryptage et de la compression des données.

i. Le cryptage des données
Le cryptage permet de protéger la confidentialité des informations pendant leur transmission.
Exemple : Les transactions financières, surtout celles qui sont faites avec des cartes de crédit, doivent être cryptées afin de protéger les données sensibles transmises sur Internet.
Une clé de cryptage est utilisée pour crypter les données à la source et pour les décrypter à destination. Un algorithme est donc utilisé pour rendre ces données incompréhensible a quiconque ne disposant pas de la clé.

ii. La compression des données
La couche présentation assure également la compression des fichiers.
La compression applique des algorithmes (formules mathématiques complexes) pour réduire la taille des fichiers. L'algorithme cherche certaines séquences de bits répétitives dans les fichiers et les remplace par un " jeton ".

Le jeton est une séquence de bits raccourcie qui est substituée à la séquence complète.
Exemple : Remplacer "Techniques de Réseaux Informatiques" par "TRI"

II.9. Couche 7 : La couche application
1. Présentation
Le rôle de cette couche est d'interagir avec les applications logicielles. Elle fournit donc des services au module de communication des applications en assurant :

- L'identification et la vérification de la disponibilité des partenaires de communication voulus
- La synchronisation des applications qui doivent coopérer
- L'entente mutuelle sur les procédures de correction d'erreur
- Le contrôle de l'intégrité des données

Dans le modèle OSI, la couche application est la plus proche du système terminal.
Celle-ci détermine si les ressources nécessaires à la communication entre systèmes sont disponibles. Sans la couche application, il n'y aurait aucun support des communications réseau. Elle ne fournit pas de services aux autres couches du modèle OSI, mais elle collabore avec les processus applicatifs situés en dehors du modèle OSI.
Ces processus applicatifs peuvent être des tableurs, des traitements de texte, des logiciels de terminaux bancaires, etc.
De plus, la couche application crée une interface directe avec le reste du modèle OSI par le biais d'applications réseau (navigateur Web, messagerie électronique, protocole FTP, Telnet, etc.) ou une interface indirecte, par le biais d'applications autonomes (comme les traitements de texte, les logiciels de présentation ou les tableurs), avec des logiciels de redirection réseau.

2. Principes de la couche application
i. Les applications réseau directes
La plupart des applications exécutées dans un environnement réseau sont de type client serveur. Ces applications (logiciels FTP, navigateurs Web ou applications de messagerie électronique) se composent de deux modules, l'un jouant le rôle du client et l'autre, le rôle du serveur.

- Le module client tourne sur l'ordinateur local : c'est le " demandeur de services ".
- Le module serveur tourne sur un ordinateur distant et fournit des services en réponse aux demandes du client.

Une application client serveur répète constamment la boucle d'itération suivante :

- demande du client
- réponse du serveur

Ainsi, un navigateur accède à une page Web en envoyant une demande d'adresse Web (URL) à un serveur Web distant. Après avoir localisé la page grâce à l'adresse URL fournie, le serveur Web associé à l'adresse répond à la demande. Ensuite, en fonction des informations reçues du serveur Web, le client pourra demander des pages supplémentaires du même serveur Web ou accéder à une autre page associée à un serveur Web différent.

ii. Le support indirect du réseau

Dans un environnement LAN, le support indirect des applications réseau est une fonction client-serveur.

Ainsi, si vous souhaitez sauvegarder un fichier texte sur un serveur de réseau, le logiciel de redirection permet à l'application de traitement de texte de devenir un client réseau.

Le logiciel de redirection est un protocole qui interagit avec les systèmes d'exploitation et les clients réseau plutôt qu'avec des applications particulières.

Voici quelques exemples de logiciels de redirection :

- Le protocole AFP (Apple File Protocol)
- L'interface NetBEUI (NetBIOS Extended User Interface)
- Les protocoles IPX/SPX de Novell
- Le système NFS (Network File System) de la suite de protocoles TCP/IP

Description d'un processus de redirection :

1. Le client demande au serveur de fichiers du réseau d'autoriser le stockage du fichier.
2. Le serveur répond en copiant le fichier sur son disque ou en rejetant la demande du client.
3. Si le client demande au serveur d'imprimer un fichier de données sur une imprimante distante (réseau), le serveur répond en imprimant le fichier sur l'une de ses imprimantes, ou en rejetant la demande.

Le logiciel de redirection permet à un administrateur réseau d'associer des ressources distantes à des noms logiques du client local.

Lorsque vous spécifiez l'un de ces noms logiques pour exécuter une opération d'enregistrement ou d'impression d'un fichier, le logiciel de redirection réseau achemine le fichier choisi à la ressource distante appropriée du réseau afin qu'il soit traité.

Si la ressource est sur un ordinateur local, le logiciel de redirection ignore la demande et laisse au système d'exploitation local le soin de la traiter.

L'avantage d'utiliser un logiciel de redirection réseau sur un client local est que les applications du client n'ont pas à communiquer avec le réseau. De plus, l'application qui fait la demande de service est située sur l'ordinateur local et le logiciel de redirection achemine la demande à la ressource réseau appropriée pendant que l'application la traite comme s'il s'agissait d'une demande locale.

Les logiciels de redirection permettent d'étendre les fonctionnalités des logiciels autonomes. Ils permettent également aux utilisateurs de partager des documents, des modèles, des bases de données, des imprimantes et diverses autres ressources sans avoir à utiliser des applications spéciales.

Les réseaux ont fortement contribué au développement de programmes tels que les traitements de texte, les tableurs, les logiciels de présentation, les bases de données, les logiciels graphiques et les outils de productivité.

Bon nombre de ces progiciels sont désormais intégrés au réseau ou compatibles avec ce dernier. Ils peuvent lancer des navigateurs Web intégrés ou des outils Internet, et enregistrer leurs résultats au format HTML en vue de les diffuser aisément sur le Web.

Il importe de souligner que dans chacun des exemples précédents, la connexion au serveur est maintenue juste assez longtemps pour traiter la transaction :

- Dans l'exemple du Web, la connexion est maintenue juste assez longtemps pour télécharger la page Web en cours.
- Dans l'exemple de l'impression, la connexion est maintenue juste assez longtemps pour envoyer le document au serveur d'impression.

Une fois le traitement terminé, la connexion est interrompue. Elle doit être rétablie pour acheminer une nouvelle demande de traitement. C'est l'une des deux méthodes de gestion des communications. C'est la méthode qu'utilise par exemple le protocole DNS.
L'autre méthode consiste à conserver la connexion établie jusqu'à ce que l'utilisateur décide que la connexion doit être terminée. C'est ce fonctionnement qu'utilisent les protocoles Telnet et FTP.

3. Le protocole DNS

i. Présentation du protocole DNS

Chaque station possède une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses IP mais avec des noms de stations ou des adresses plus explicites comme par exemple http://www.ofppt.org.ma
Pour répondre à cela, le protocole DNS permet d'associer des noms en langage courant aux adresses numériques.
Résolution de noms de domaines : Corrélation entre les adresses IP et le nom de domaine associé.

ii. Les noms d'hôtes et le « domain name system »

Aux origines de TCP/IP, étant donné que les réseaux étaient très peu étendus, c'est-à-dire que le nombre d'ordinateurs connectés à un même réseau était faible, les administrateurs réseau créaient des fichiers appelés tables de conversion manuelle (fichiers généralement appelé hosts ou hosts.txt), associant sur une ligne, grâce à des caractères ASCII, l'adresse IP de la machine et le nom littéral associé, appelé nom d'hôte.
Ce système à l'inconvénient majeur de nécessiter la mise à jour des tables de tous les ordinateurs en cas d'ajout ou modification d'un nom de machine. Ainsi, avec l'explosion de la taille des réseaux, et de leur interconnexion, il a fallut mettre en place un système plus centralisé de gestion des noms. Ce système est nommé Domain Name System, traduisez Système de nom de domaine.
Ce système consiste en une hiérarchie de noms permettant de garantir l'unicité d'un nom dans une structure arborescente.
On appelle nom de domaine, le nom à deux composantes, dont la première est un nom correspondant au nom de l'organisation ou de l'entreprise, le second à la classification de domaine (.fr, .com, ...). Chaque machine d'un domaine est appelée hôte. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré (le serveur web d'un domaine porte généalement le nom www).
L'ensemble constitué du nom d'hôte, d'un point, puis du nom de domaine est appelé adresse FQDN (Fully Qualified Domain, soit Domaine Totalement Qualifié). Cette adresse permet de repérer de façon unique une machine. Ainsi www.ofppt.org.ma représente une adresse FQDN.

Les machines appelées serveurs de nom de domaine permettent d'établir la correspondance entre le nom de domaine et l'adresse IP sur les machines d'un réseau. Chaque domaine possède ainsi, un serveur de noms de domaines, relié à un serveur de nom de domaine de plus haut niveau. Ainsi, le système de nom est une architecture distribuée, c'est-à-dire qu'il n'existe pas d'organisme ayant à charge l'ensemble des noms de domaines. Par contre, il existe un organisme (l'InterNIC pour les noms de domaine en .com,.net,.org et .edu par exemple). Le système de noms de domaine est transparent pour l'utilisateur, néanmoins il ne faut pas oublier les points suivants:
Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée Domain Name Server.
L'adresse IP d'un second Domain Name Server (secondary Domain Name Server) peut également être introduite: il peut relayer le premier en cas de panne.

iii. Codes des domaines internet

La classification du domaine, parfois appelées TLD (Top Level Domain, soit domaines de plus haut niveau), correspond généralement a une répartition géographique. Toutefois, il existe des noms, créés pour les Etats-Unis à la base, permettant de classifier le domaine selon le secteur d'activité, par exemple:

- .arpa correspond aux machines issues du réseau originel
- .com correspond aux entreprises à vocation commerciales (désormais ce code de domaine ne rime plus à grand chose et est devenu international)
- .edu correspond aux organismes éducatifs
- .gov correspond aux organismes gouvernementaux
- .mil correspond aux organismes militaires
- .net correspond aux organismes ayant trait aux réseaux
- .org correspond aux entreprises à but non lucratif

4. Le protocole Telnet

i. Présentation du protocole Telnet

Le protocole Telnet est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un interpréteur de commande (côté serveur).
Le protocole Telnet s'appuie sur une connexion TCP pour envoyer des données au format ASCII codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet. Il fournit ainsi un système orienté communication, bidirectionnel alterné (half-duplex), codé sur 8 bits facile à mettre en oeuvre.
Le protocole Telnet repose sur trois concepts fondamentaux :

- Le paradigme du terminal réseau virtuel (NVT)
- Le principe d'options négociées
- Les règles de négociation

Ce protocole est un protocole de base, sur lequel s'appuient certains autres protocoles de la suite TCP/IP (FTP, SMTP, POP3, ...).
Les spécifications de Telnet ne mentionnent pas d'authentification car Telnet est totalement séparé des applications qui l'utilisent (le protocole FTP définit une séquence d'authentification au-dessus de Telnet).
En outre le protocole Telnet est un protocole de transfert de données non sûr, c'est-à-dire que les données qu'il véhicule circulent en clair sur le réseau (de manière non chiffrée). Lorsque le protocole Telnet est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, ce protocole est assigné au port 23.

Hormis les options et les règles de négociation associées, les spécifications du protocole Telnet sont basiques. La transmission de données à travers Telnet consiste uniquement à transmettre les octets dans le flux TCP (le protocole Telnet précise tout de même que les données doivent par défaut, c'est-à-dire si aucune option ne précise le contraire, être groupées dans un tampon avant d'être envoyées. Plus exactement cela signifie que par défaut les données sont envoyées ligne par ligne). Lorsque l'octet 255 est transmis, l'octet suivant doit être interprété comme une commande. L'octet 255 est ainsi nommé IAC (Interpret As Command, traduisez Interpréter comme une commande). Les commandes sont décrites plus loin dans le document.

ii. La notion de terminal virtuel

Aux débuts d'Internet, le réseau (ARPANET) était composé de machines dont les configurations étaient très peu homogènes (claviers, jeux de caractères, résolutions, longueur des lignes d'affichage). D'autre part, les sessions des terminaux possèdaient également leur propre façon de contrôler les flux de données en entré/sortie.

Ainsi, au lieu de créer des adaptateurs pour chaque type de terminal afin qu'il puisse y avoir une interopérabilité de ces systèmes, il a été décidé de mettre au point une interface standard, appelée NVT (Network Virtual Terminal, traduisez Terminal réseau virtuel), fournissant une base de communication standard, composée de :

- Caractères ASCII 7 bits auxquels s'ajoutent le code ASCII étendu
- Trois caractères de contrôle
- Cinq caractères de contrôle optionnels
- Un jeu de signaux de contrôle basique

Le protocole Telnet consiste ainsi à créer une abstraction du terminal, permettant à n'importe quel hôte (client ou serveur) de communiquer avec un autre hôte sans connaître ses caractéristiques.

A. EL GHATTAS
Errachidia, Le 10 Février 2008