Les réseaux

Systèmes de communication

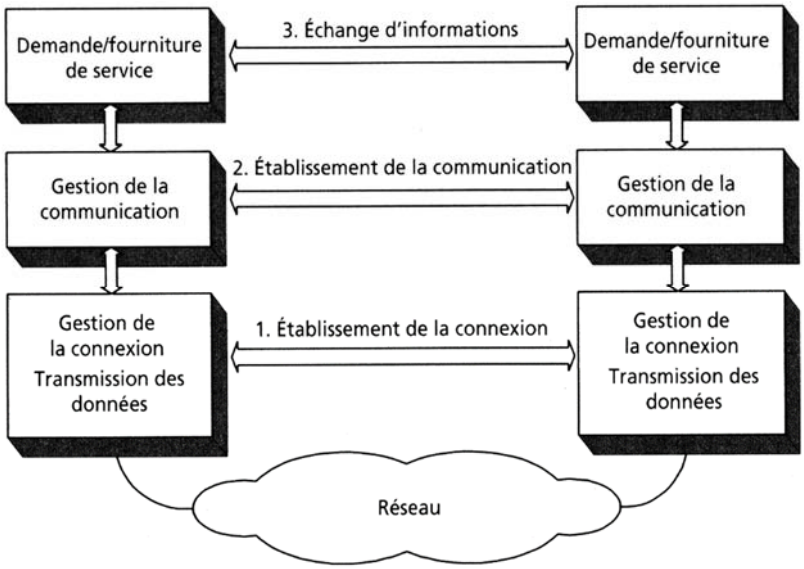
Les systèmes de communication sont nés de besoin de communication entre les systèmes informatiques. Ils vont permettre la transmission des messages, le partages de ressources, le transfert de fichiers, la consultation de bases de données la gestion de diverses transactions (bancaires et autres…), la lecture de vidéos et etc.

Architecture des systèmes de communication

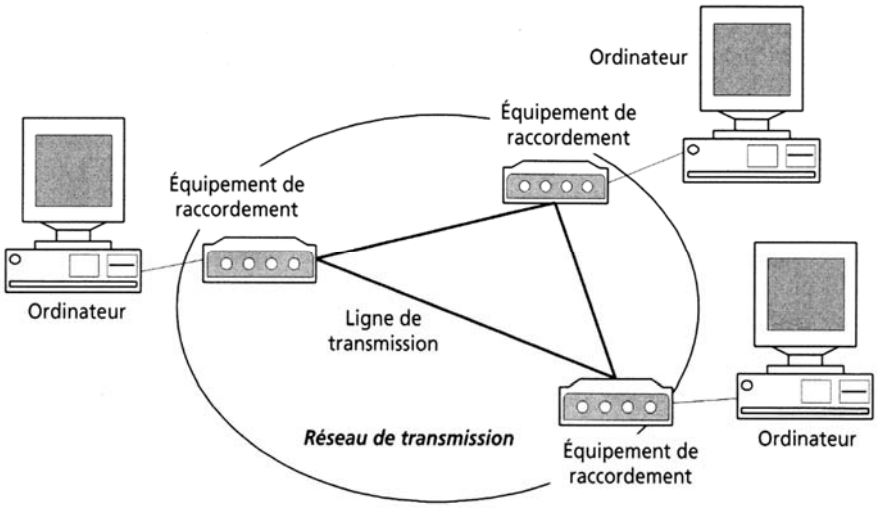
Les systèmes de communication sont organisés en trois blocs fonctionnels qui sont :

- Les applications qui veulent échanger des données.
- Les fonctions destinées à établir les communications.
- Les fonctions assurant la transmission des données.

Le schéma ci-contre illustre la hiérarchie et la mise en communication de deux systèmes.



Réseau de transmission

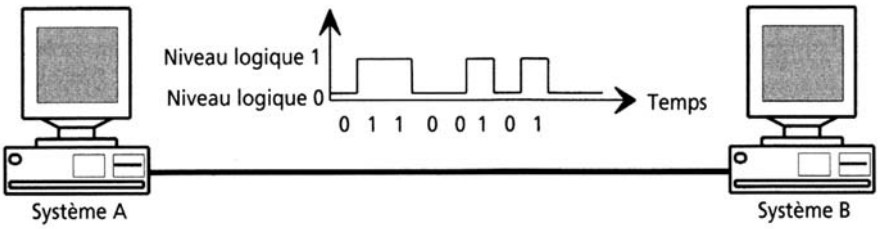


Un réseau de transmission représente l'ensemble des ressources liées à la transmission de données dans une architecture de communication entre systèmes. Le schéma d'un exemple de réseau de transmission est montré ci-contre.

Codage et transmission série

Les données étant de nature numérique, leur transmission d'un système à l'autre sera réalisée de façon série à l'aide du canal de transmission. En fonction du type de canal de transmission ces informations numériques peuvent subir des modifications comme une modulation afin de s'adapter au canal de

transmission. Le schéma ci-dessous montre la communication d'information numérique d'un octet de valeur binaire 01100101 entre deux systèmes informatiques.



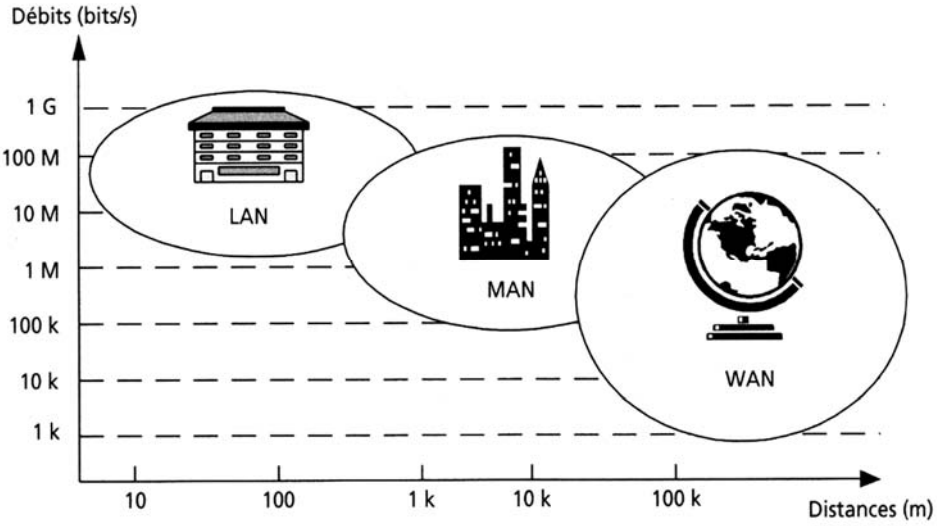
Types de réseaux informatiques

Les réseaux informatiques sont classés par type en fonction des distances entre chaque système et la vitesse de communication exprimée en bits par seconde. Comme le montre le diagramme ci-contre nous nous avons trois types de réseaux :

LAN : réseaux locaux

MAN : réseaux de ville

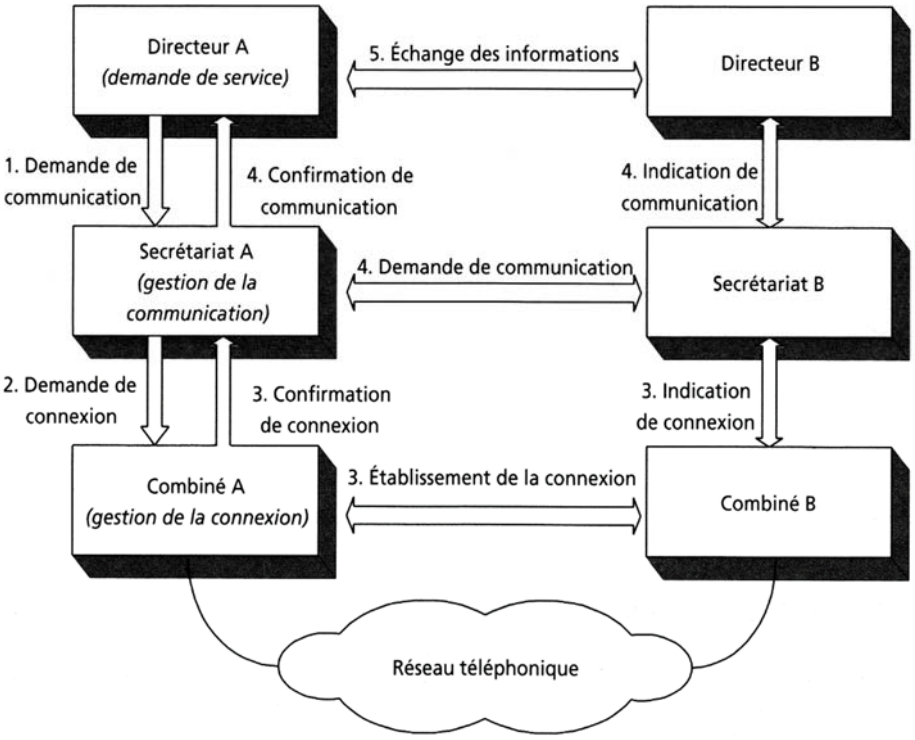
WAN : réseaux mondiaux



Protocole

Le protocole représente l'ensemble des procédures et d'informations échangées pour établir et gérer une communication entre deux systèmes. Le format des informations échangées appartient aussi au protocole.

Ci-contre est illustré un exemple de communication entre deux directeurs qui utilisent leur secrétariat pour gérer la communication. Vous remarquerez l'architecture du système de communication.



Gestion d'une communication

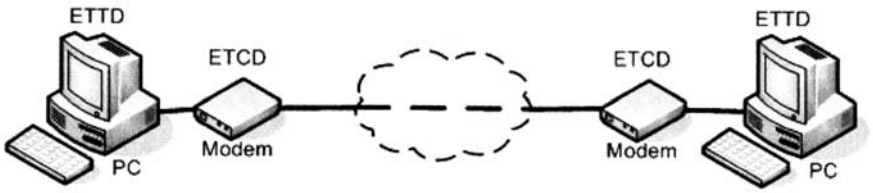
La gestion d'une communication représente les différentes étapes pour l'établissement d'une communication. C'est une suite d'opérations séquentielles comme appeler le correspondant, décrocher le combiné et etc.

Architecture des réseaux

Il existe deux types d'architectures de réseau.

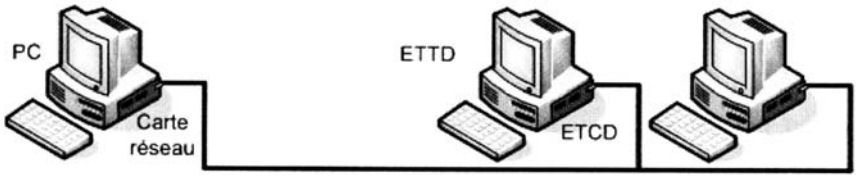
La liaison point à point

Ex : RS232



La liaison multipoints

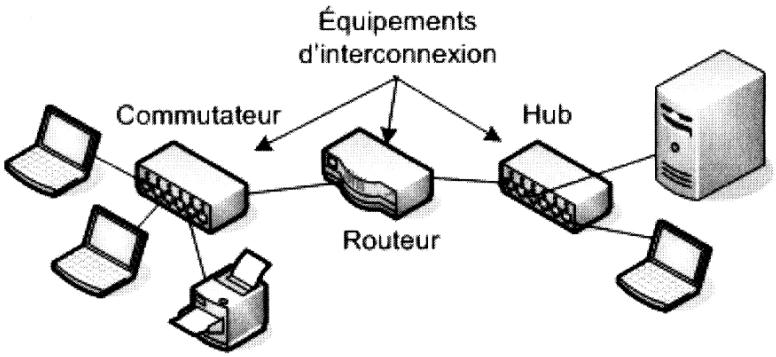
Ex : Bus



Eléments d'un réseau

Comme on peut le voir sur le schéma ci-contre, les équipements qui composent un réseau sont :

- Les terminaux
- Les équipements d'interconnexions
- Les contrôleurs de communication



Equipements terminaux

Les équipements terminaux sont le plus souvent des ordinateurs, des serveurs, des terminaux bancaires, des automates industriels et etc.

Equipements d'interconnexion

Les équipements d'interconnexions comprennent multiplexeurs, concentrateurs, commutateurs et quelques autres dispositifs.

- Un multiplexeur est un équipement qui permet le partage statique d'une ligne de communication. Le partage est fixe et permanent et il peut être réalisé de façon temporelle ou fréquentielle.
- Un concentrateur est un équipement qui permet le partage dynamique d'une ligne de communication en fonction des besoins et il peut être réalisé de façon temporelle ou fréquentielle.
- Un commutateur est un équipement qui permet la liaison entre des équipements terminaux.
- D'autres dispositifs existent comme des routeurs, des ponts, des Hub, des MAU sur des architectures et protocoles particuliers.

Contrôleur de communications

Les contrôleurs de communication sont des équipements qui permettent aux systèmes informatiques de communiquer avec les équipements d'interconnexions. Les différents types de contrôleurs sont listés ci-dessous :

- Les cartes d'interfaces série (synchrones ou asynchrones)
- Les cartes d'interfaces réseau (cartes Ethernet, Token Ring, etc.)
- Les contrôleurs de raccordement aux réseaux publics (réseau RTC, RNIS, etc.)
- Les contrôleurs d'accès distant (connexion d'ordinateurs à un serveur à travers un réseau téléphonique ou autre…)

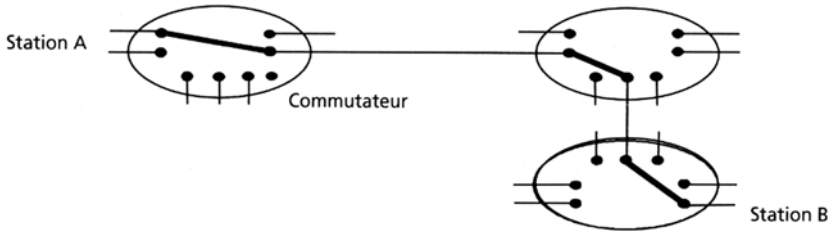
Réseaux à commutation

Les réseaux à commutation permettent à tout équipement de communiquer sur un réseau maillé (réseau ouvert). Il y a trois types de commutation :

- La commutation de circuits
- La commutation de paquets
- La commutation de cellules

Commutation de circuits

Dans la commutation de circuits les données sont transmises sur un circuit. Les commutations sont courtes, le taux de connexions et d'activité sont faibles. La commutation de circuit permet de relier de longue distance mais de réalise pas de mémorisation des données. Les réseaux téléphoniques sont des exemples d'utilisations et un exemple de circuit de commutation est donné ci-dessous :

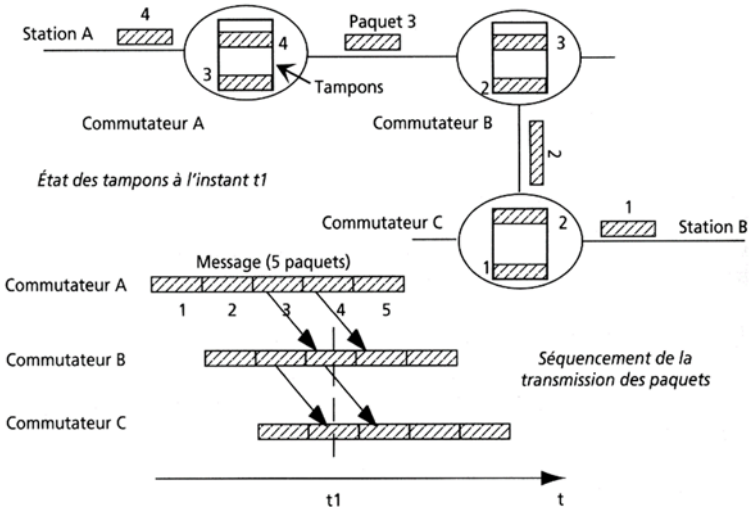


Commutation de paquets

Dans la commutation de paquets les données sont transmises par groupes d'une taille conséquente appelés paquets. La commutation de paquets est la commutation de prédilection des réseaux comme Ethernet ou X_{25} car elle dispose de nombreux avantages qui sont listés ci-dessous :

- Le multiplexage temporel des paquets de plusieurs messages
- La possibilité de reprise en cas d'erreur de transmission (mémorisation des paquets)
- La gestion des transmissions (dialogue)
- La possibilité d'une politique de routage
- L'adaptation de vitesse entre différentes interfaces (grâce à la mémorisation)
- Le taux d'activité et de connexion proche de 100%

Un exemple d'envoi de paquets entre deux systèmes (station A et B) est présenté ci-contre :

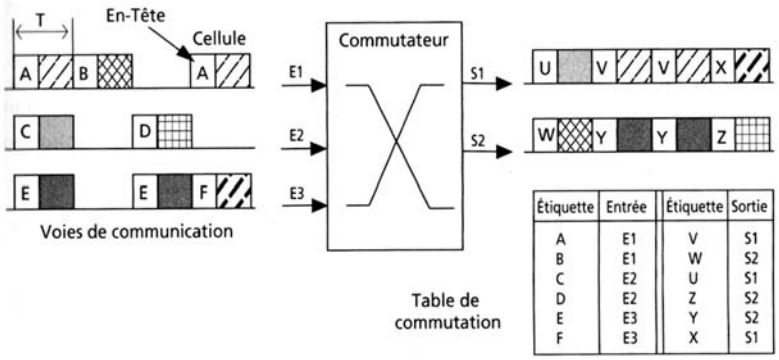


Commutation de cellules

Dans la commutation de paquets les délais de transmissions sont imprévisibles ce qui rend ce mode de commutation incompatible avec le transport de la voix ou de la vidéo.

Cette technique de commutation est normalisée par l'OSI (Open Systems Interconnection). Elle permet d'allier la simplicité de la commutation de circuits à la flexibilité de la commutation de paquets. Ces caractéristiques sont de transmettre des cellules de longueur constante et modérée émises à intervalle de temps fixe. Le réseau ATM (Asynchronous Transfer Mode) utilise la commutation de cellules. L'ATM a remplacé en France le réseau X_{25} base des communications de la société Transpac filiale de France Télécom.

Un exemple d'envoi de cellules est donné ci-contre :

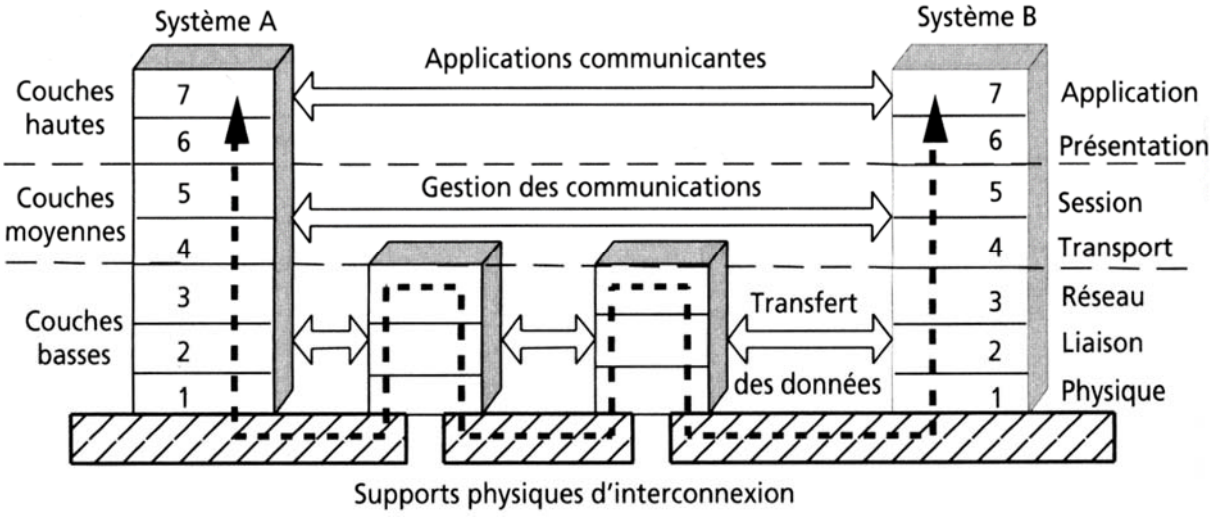


Étiquette	Entrée	Étiquette	Sortie
A	E1	V	S1
B	E1	W	S2
C	E2	U	S1
D	E2	Z	S2
E	E3	Y	S2
F	E3	X	S1

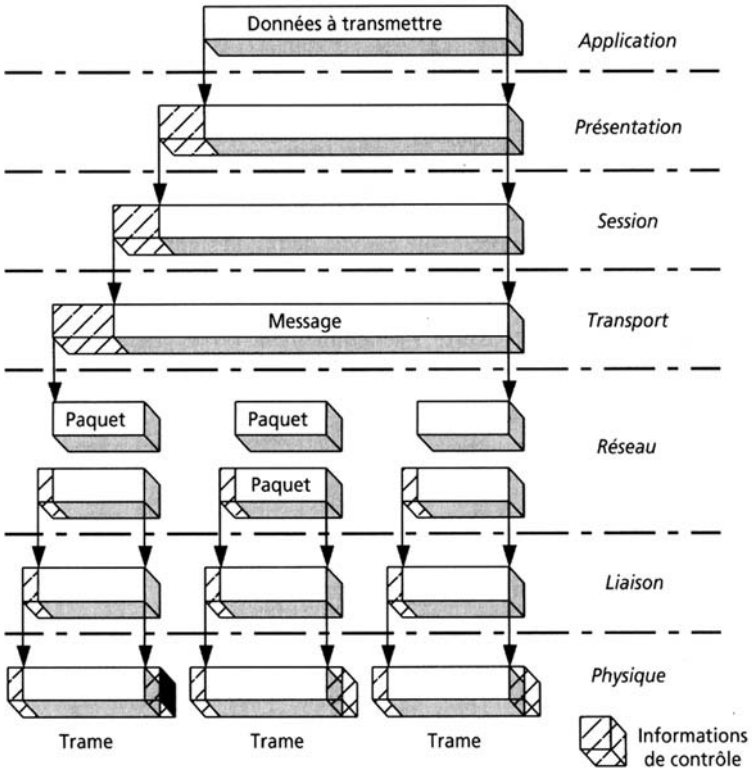
Modèle OSI

	Protocol Data Unit	Couche		Fonction
Couches Hautes (Logicielles)	Données	7	Application	Point d'accès aux services réseau
		6	Présentation	Gère le chiffrement et la compression des données, convertit les données machine en données exploitables par n'importe quelle autre machine
Couches Moyennes		5	Session	Interface qui gère les sessions entre les différentes applications
	Segments / Datagramme	4	Transport	Contrôle de flux et découpage en paquet. Notion de port
Couches Basses (Matérielles)	Paquet	3	Réseau	Détermine le parcours des données et l'adressage logique (Adresse IP)
	Trame	2	Liaison	Adressage physique (Adresse MAC)
	Bit	1	Physique	Transmission des signaux sous forme numérique ou analogique

Le schéma ci-dessous illustre la communication entre les différentes couches pour effectuer une communication entre deux systèmes :

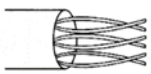
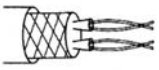
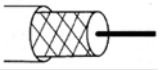
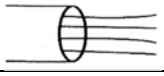


La transmission de données est effectuée entre chaque couche en ajoutant des entêtes qui marquent les données transmises afin de permettre leur extraction à l'arrivé. Le schéma ci-contre montre la transmission des données entre les différentes couches du modèles OSI.



Support physique d'interconnexion

Les critères de choix du support physique d'interconnexion d'un réseau concernent la distance maximale entre deux stations, les débits minimum et maximum, le type de transmission (numérique ou analogique), la nature des informations échangées (données, voix, vidéo, etc.), la connectique, la fiabilité et le coût. Les divers types de supports physiques sont présentés dans le tableau ci-dessous :

Type de support		Débit max	Distance max	Temps de propagation	Immunité aux bruit	Remarques
Paire torsadée non blindé		1 Gbit/s	1 km	~5.3 µs/km	Faible	Affaiblisse-ments importants
Paire torsadée blindé		1 Gbit/s	1 km	~5.3 µs/km	Bonne	Liaisons multifils
Câble coaxial		100 Mbit/s	1 km	~4.1 µs/km	Très bonne	Impédance 50Ω
Fibre optique		10 Gbit/s	10 km	~5 µs/km	Excellente	Débit en progression

Les réseaux locaux

Les réseaux locaux représentent l'ensemble des ressources téléinformatiques pour l'échange de données entre des équipements dans une administration, une entreprise, chez un particulier, etc.

Le débit de tels réseaux est compris entre 100 kbit/s et 1 Gbit/s sur des distances maximales de 10 km. Les équipements interconnectés sont des ordinateurs, des imprimantes, des serveurs, des automates, etc. Les besoins sont le partage de fichiers, l'accès à des bases de données, la lecture de vidéos, l'impression de documents, etc.

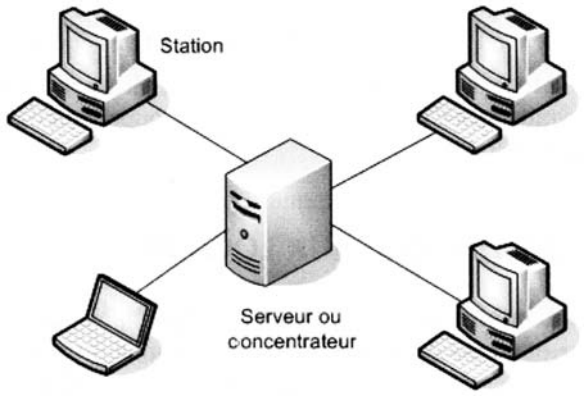
La nature des données échangées concerne :

- Bureautique pour de la messagerie, des bases de données, des documents, des fax, etc.
  - avec un débit maximum de 10 Mbit/s.
- Multimédia pour des images, du son, de la vidéo, etc.

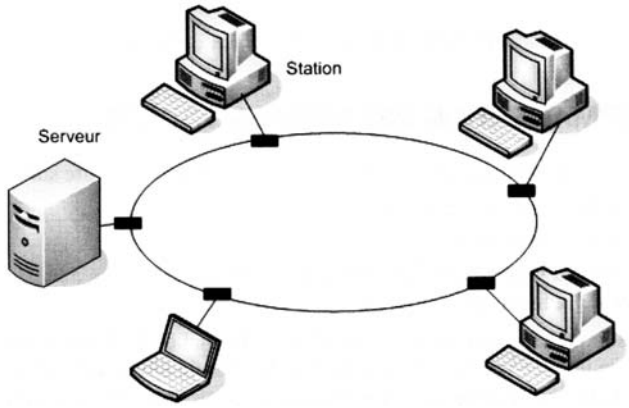
- avec un débit maximum de 10 Gbit/s
- Temps réel pour de la VOIP, des vidéos conférences, du streaming, commandes de processus, etc.
  - Avec un débit maximum de 1 Mbit/s mais des contraintes d'acheminement

Topologie des réseaux locaux

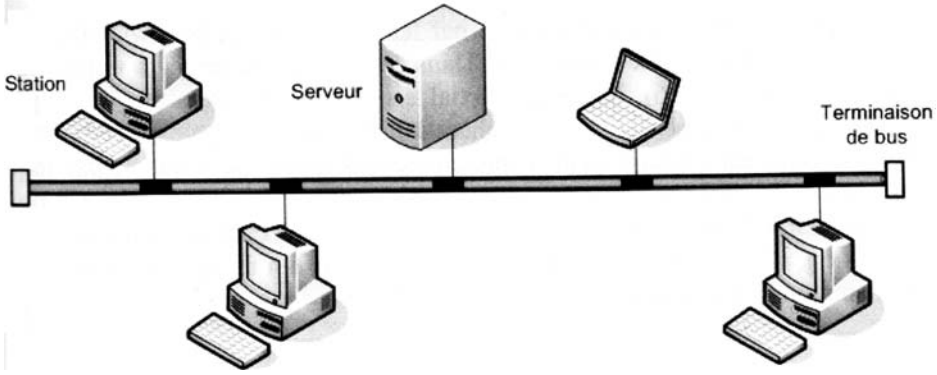
Il existe trois types de topologie réseau qui sont présentées ci-dessous :



En étoile



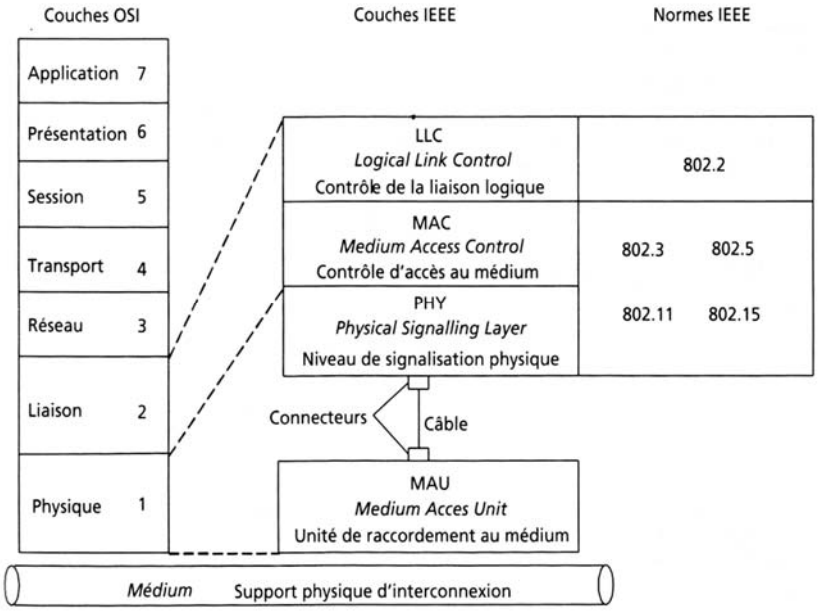
En anneau



En bus

Normalisation des réseaux

Le transfert de données nécessite la mise en forme des informations à émettre, l'identification du récepteur, le décodage des informations par le récepteur, l'annonce de la fin de transmission, des protocoles définis (IEEE, ISO) en correspondance avec le modèle OSI.
Le schéma ci-contre présente la correspondance entre le modèle OSI et les couches de la norme IEEE.



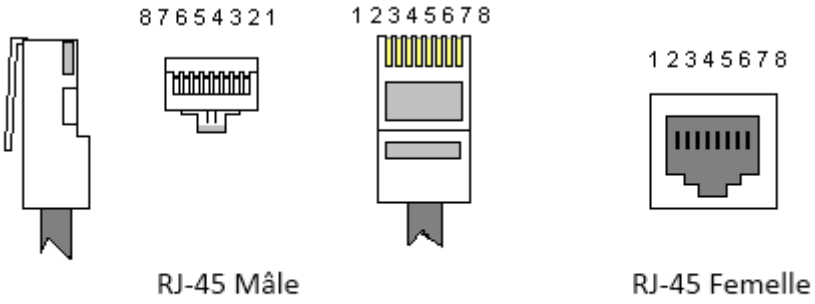
Architecture Ethernet

L'architecture du réseau Ethernet est la plus répandue dans les réseaux modernes. Ces caractéristiques sont présentées ci-dessous :

- Débit 10Mbit/s à 1Gbit/s
- Transmission en bande de base (codage Manchester)
- Topologie en bus
- Méthode d'accès (IEEE 802.3)
- Longueur trame de 64 à 1518 octets
- Support coaxial, paire torsadée ou fibre optique
- Gestion des couches 1 et partiellement 2 de l'OSI

Connectique Ethernet

La connectique Ethernet est essentiellement basée sur des câbles en paires torsadées blindés ou non sertis dans des prises RJ45.

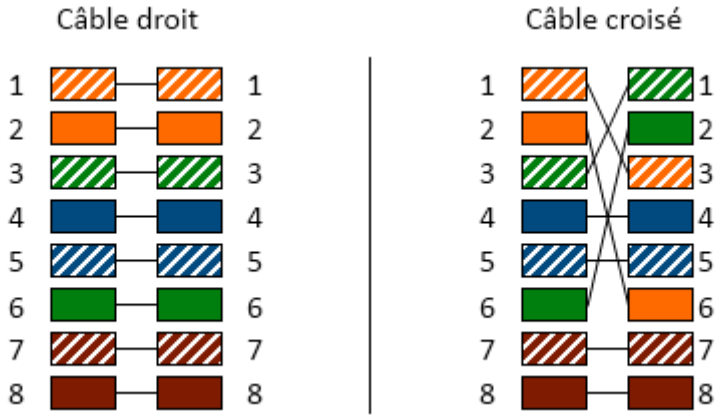


La norme supporte 3 vitesses :

- 10BaseT
- 100BaseT
- 1000BaseT

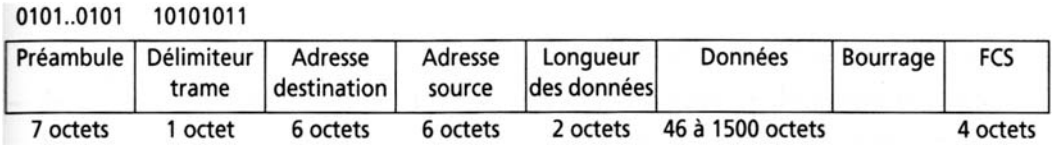
Les paires sont :

- 2 émission (1-2)
- 3 réception (3-6)
- 1 (4-5)
- 4 (7-8)

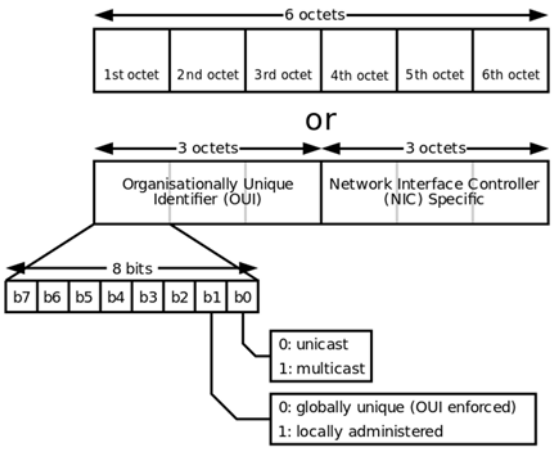


Trame Ethernet

La sous couche MAC correspond au trame niveau 2 du modèle OSI. Elle contient un préambule et un délimiteur, une adresse MAC de destination et de source, la longueur des données, les données et une somme de contrôle (FCS). Son format est présenté ci-dessous :



L'adresse MAC (Medium Access Control) est propre aux interfaces et est codée sur 6 octets comme le montre le schéma ci-contre :



L'adresse MAC est composée de deux champs :

- Un code spécifique fabriquant (OUI)
- Un code spécifique à l'interface (NIC)

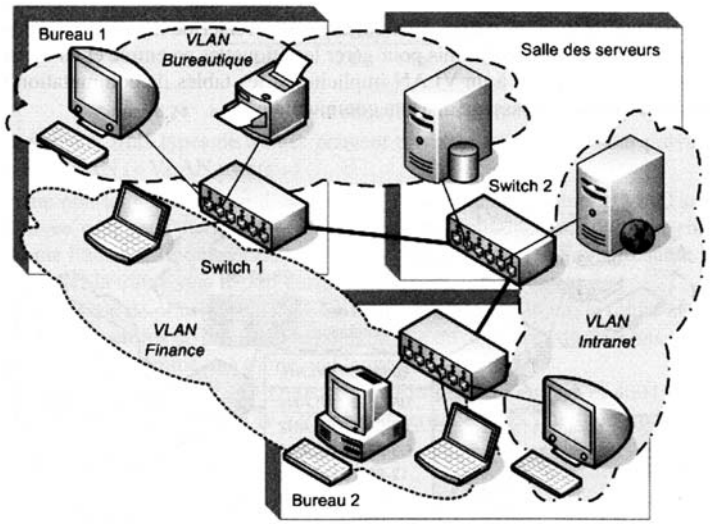
L'adresse MAC de diffusion est :

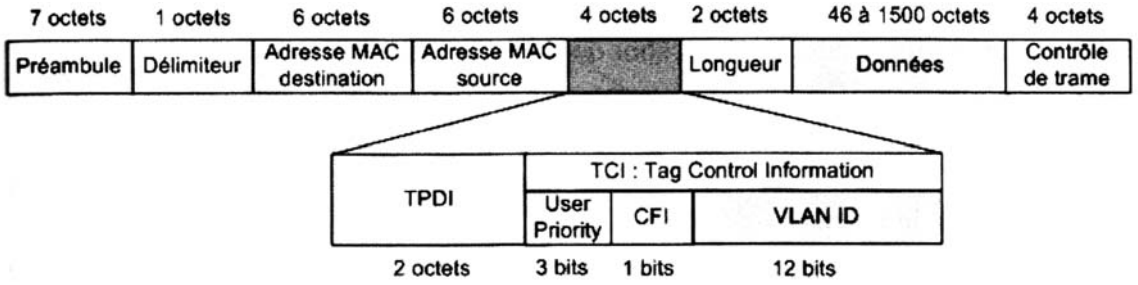
FF FF FF FF FF FF

VLAN

« Virtual Local Aera Network » ou réseau local virtuel est un réseau logique isolé au sien d'un réseau physique plus vaste. Les VLAN permettent principalement d'améliorer la gestion du réseau informatique et sa sécurité. D'autre part, la séparation des flux logiques permet d'optimiser la bande passante et de créer des domaines de diffusion indépendants de l'architecture physique.

La figure ci-contre montre un exemple de réseau avec trois VLAN. On remarque que les regroupements n'ont pas de rapport avec l'architecture physique.





L'information VLAN est contenue dans 4 octets derrière l'adresse MAC source comme le montre 'illustration ci-dessus et contient deux champs principaux :

- Le TPDI ou Tag Protocol Identifier sur 2 octets qui identifie le protocole VLAN
- Le TCI ou Tag Control Information sur 2 octets qui contient :
  - 3 bits de niveau de priorité utilisateur (User Priority)
  - 1 bit CFI qui indique si la trame transporte des données autres qu'Ethernet
  - 12 bits d'identificateur du VLAN

Les dispositifs d'interconnexions

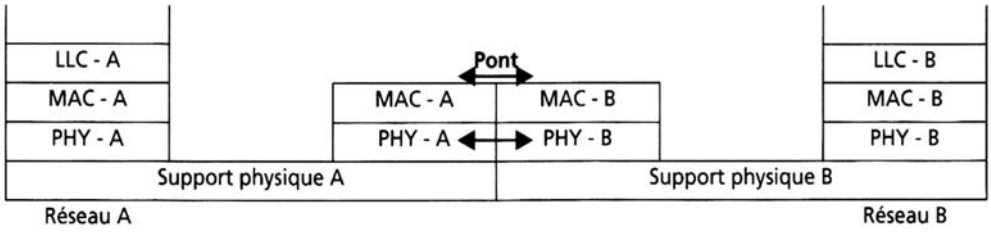
Il existe au moins quatre types de dispositifs d'interconnexions : les répéteurs ou boitiers d'interconnexion (hub), les ponts ou commutateurs Ethernet (switch), les routeurs (router) et les passerelles (gateway).

Le répéteur

C'est un élément passif dans un réseau, il se contente de répéter les bits d'un segment sur l'autre en régénérant le signal électrique. Il permet de changer support physique. Le HUB est un répéteur sur plusieurs ports.

Le pont ou switch

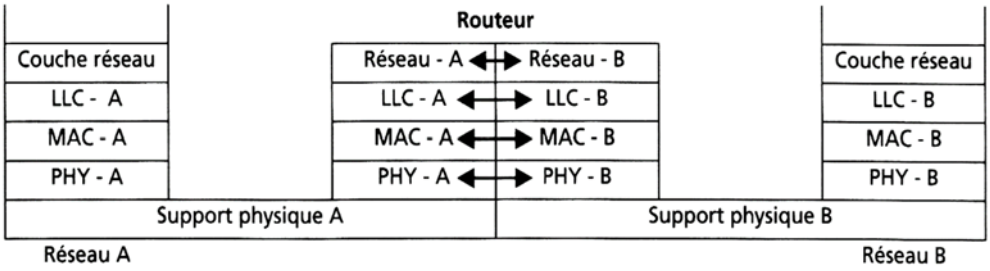
Le pont ou switch est un dispositif d'interconnexion qui intervient au niveau 2 comme le montre le schéma ci-dessous :



Il de modifie pas les adresses MAC de la trame et la diriger vers l'adresse de destination.

Le routeur

Le routeur est un dispositif d'interconnexion qui intervient au niveau 3 comme le montre le schéma ci-dessous :



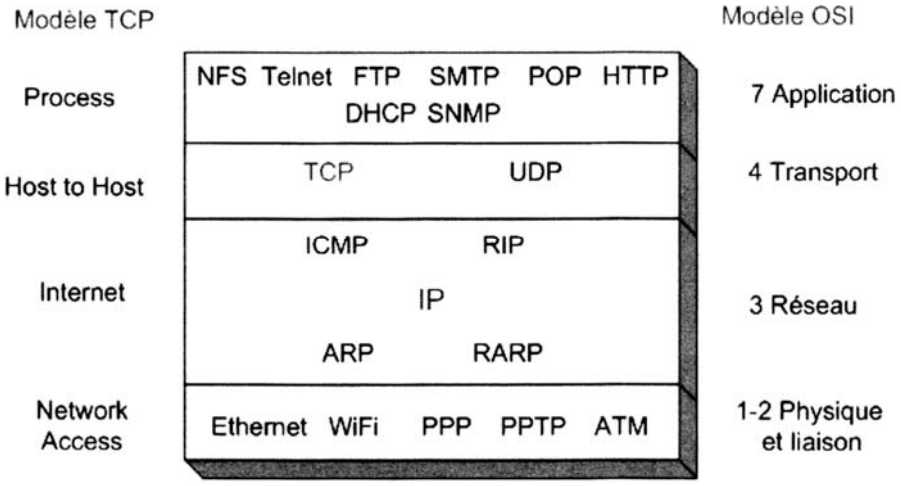
Le routeur redirige les paquets vers le destinataire grâce à une table de routage et à l'adresse MAC du destinataire. Les adresses MAC sont adaptées au réseau du destinataire.

La passerelle

C'est le dispositif d'interconnexion le plus complexe car il intervient sur les 7 couches du modèle OSI et possède une pile complète pour chacun des niveaux servis. La passerelle permet de mettre en œuvre plusieurs types de réseaux et réalise une connexion complète des trames.

Les protocoles TCP/IP

Les protocoles TCP / IP (Transport Control Protocol / Internet Protocol) représentent l'ensemble des protocoles de transfert de données sur Internet.
Le diagramme ci-contre montre certains de ces protocoles.



Les protocoles niveau 1 et 2

Les protocoles de niveau 1 et 2 sont liés aux architectures réseaux comme Ethernet, WiFi et autre...
Le diagramme ci-dessous montre le format de la trame avec la sous-couche LLC d'Ethernet avec les valeurs DSAP et SSAP normalisé par l'IEEE 802.3. Ce diagramme montre aussi que pour l'Ethernet 2 la sous-couche LLC n'existe pas et l'Internet Protocol est indiqué par la valeur de longueur mise à 0800h.

MAC			LLC			IP
Adr. Dest.	Adr. Src.	Longueur	DSAP = 06_H	SSAP = 06_H	Contrôle	

MAC			IP
Adr. Dest.	Adr. Src.	0800_H	

Les protocoles niveau 3

Protocole ARP :

Le protocole ARP (Address Resolution Protocol) est comme sont nom l'indique un protocole de résolution d'adresse IP / MAC. Les adresses MAC ou adresse physique dépendent du matériel et leur répartition n'a pas de lien logique contrairement aux adresses IP.

Les trames ARP, envoyées avant toutes autres trames, permettent à l'ordinateur de récupérer la correspondance adresse IP / MAC qu'il sauvegarde dans une table.
RARP permet l'opération inverse, c'est à dire de récupérer l'adresse IP d'une adresse MAC.

Protocole ICMP :

Le protocole ICMP (Internet Control Message Protocol) permet la collecte d'erreurs sur le réseau. ICMP utilise l'encapsulation IP et sert principalement à la gestion du protocole IP. la commande PING permet sont utilisation simple.

Protocole RIP :

Le protocole RIP (Routing Information Protocol) est un protocole utilisé par les routeurs qui permet à ces derniers de récupérer les informations sur la structure du réseau par diffusion de leur table de routage au routeur voisins.

Les protocoles niveau 4

Protocole TCP :

Le protocole TCP (Transmission Control Protocol) est un protocole en mode connecté qui permet un transfert fiable des données. Il est utilisé par bon nombre de protocole de niveau supérieur.

Protocole UDP :

Le protocole UDP (User Datagram Protocol) est un protocole en mode non connecté qui permet un transfert simple des données en mode datagramme. Il est aussi utilisé par bon nombre de protocole de niveau supérieur qui ne nécessite pas de transmission fiable des données.

Les protocoles niveau 7

Les protocoles de niveau 7 sont les protocoles applicatifs. Quelques uns sont listés ci-dessous :

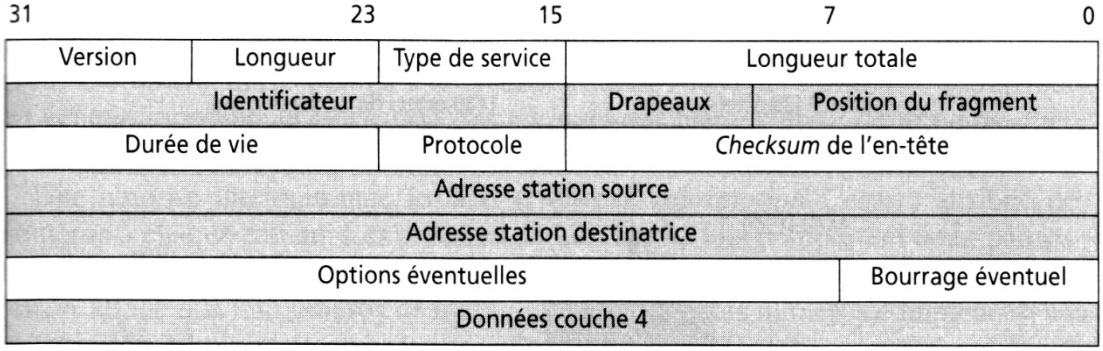
- NFS (Network File Protocol)
- Telnet (Terminal Emulation Protocol)
- FTP (File Transfer Protocol)
- SMTP (Simple Mail Transfert Protocol)
- HTTP (HyperText Transmission Protocol)
- SNMP (Simple Network Management Protocol)
- NTP (Network Time Protocol)

Protocole DCHP :

Le protocole DCHP (Dynamic Host Configuration Protocol) permet l'allocation dynamique d'adresse IP à des clients d'un réseau. DHCP utilise l'encapsulation IP et son rôle est fortement lié à Internet. Dans un réseau un ou plusieurs serveurs DCHP distribuent les adresses IP aux machines connectées au réseau. Ces serveurs concentrent et simplifient la gestion des adresses IP.

Le protocole Internet (IP)

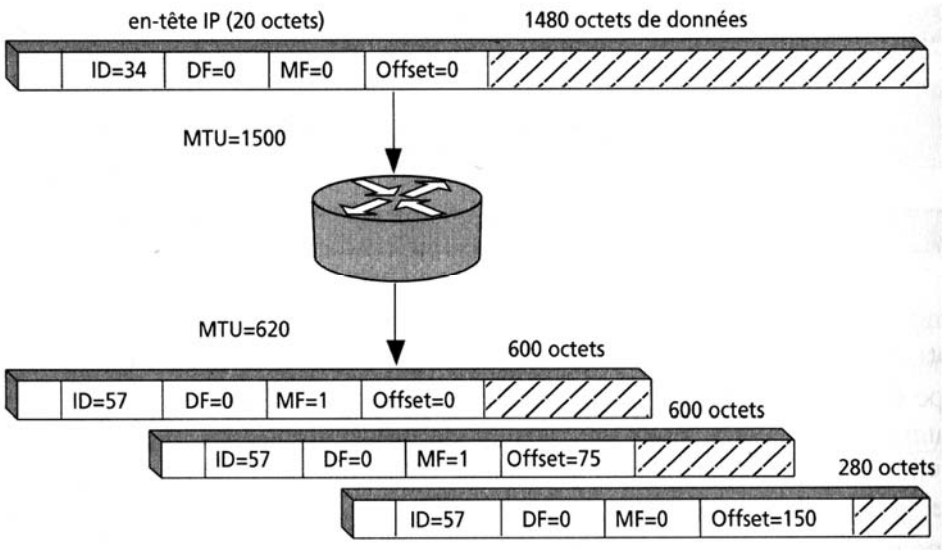
Le protocole IP (Internet Protocol) est un protocole de communication de niveau 3 responsable de la transmission des données en mode non connecté, de l'adressage et du routage des paquets et de la fragmentation des données.
Le format du paquet ou datagramme IP est montré ci-dessous :



Ses fonctionnalités lors de l'émission permettent l'identification du paquet, la détermination de la route à suivre, la vérification du type d'adressage et la fragmentation de la trame.
Ses fonctionnalités lors de la réception lui permettent la vérification de la longueur, le contrôle d'erreurs de la trame, son réassemblage en cas de fragmentation et sa transmission réassemblé au niveau supérieur (le niveau 4, couche transport).
Les différents champs du paquet IP sont listés ci-dessous :

- Version du protocole IP (actuellement 4)
- Longueur de l'entête (généralement 5)
- Type de service : désigne la qualité de service
- Identificateur pour la fragmentation (même numéro pour un paquet)
- Drapeaux (DF= Don't Fragment & MF= More Fragment)
- Position du fragment par multiple de 8 dans le paquet
- Durée de vie du paquet qui est décrémenté par chaque routeur et détruit si =0
- Protocole contient le numéro SAP du destinataire et le protocole de la couche supérieure (1 pour ICMP, 6 pour TCP, 17 pour UDP)
- Options qui sont utilisées pour le contrôle ou la mise au point

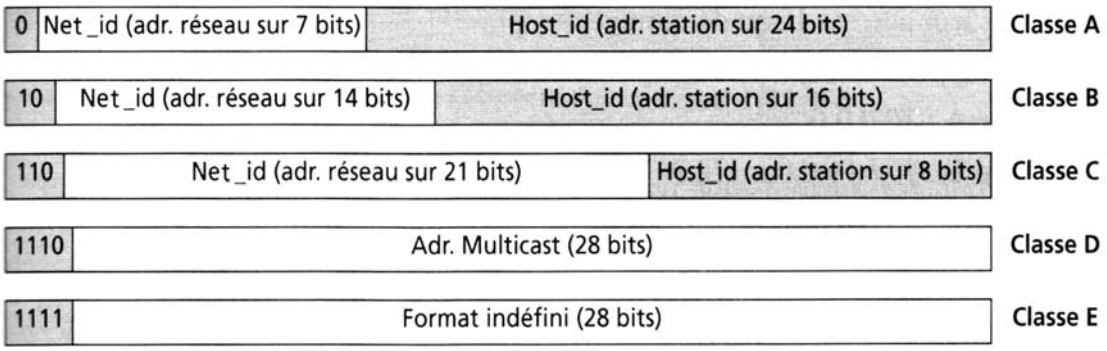
La fragmentation du paquet :



Le schéma ci-dessus illustre la transmission d'un paquet IP par un routeur dont le MTU (Maximal Unit transfert) est de 600 octets. Le paquet initial de 1480 octets sera donc découpé en trois fragments respectivement de 600, 600 et 280 octets.

Adressage Internet :

Le Network Information Center attribut un numéro à chaque réseau. L'adresse IP codé sur 32 bits sera composée d'un identifiant réseau et client. La structure de cette adresse évolue en fonction de la classe de réseau comme indiqué ci-dessous :



Les classes de réseau permettent d'obtenir un certain nombre de réseau et de machines connectées à ces réseaux comme montré ci-après :

- Classe A : 1.0.0.0 à 126.0.0.0
  réseaux de grande envergure (ministère de la défense US, réseaux d'IBM, AT&T, etc.)
  126 réseaux (2^{8-1}-2) et 16777214 machines (2^{32-8}-2)
- Classe B : 128.1.0.0 à 191.254.0.0
  réseaux moyens (université, centre de recherches …)
  16382 réseaux (2^{16-1}-2) et 65534 machines (2^{32-16}-2)
- Classe C : 192.0.1.0 à 223.255.254.0
  petits réseaux (PME, usager …)
  2097150 réseaux (2^{24-3}-2) et 254 machines (2^{32-24}-2)
- Classe D : 224.0.0.1 à 239.255.255.255
  adresse de groupe de diffusion
  268435454 adresses de groupe (2^{32-4}-2)
- Classe E : 240.0.0.0 à 255.255.255.254

Adresses Spéciales :

Un certain nombre d'adresses sont spéciales et réservées à un usage particulier :

Adresse de réseau ➔ partie basse = 0
ex : 212.93.28.0 pour un réseau de classe C

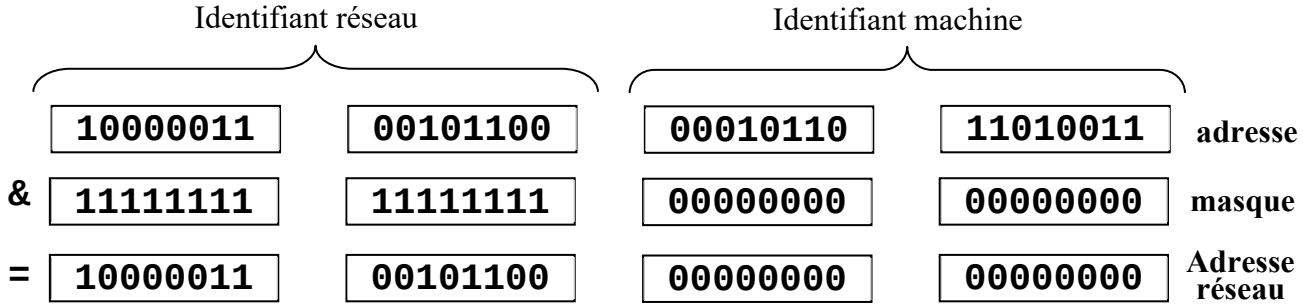
Adresse de diffusion ➔ partie basse = 1
ex : 155.12.255.255 pour un réseau de classe B

Adresse Loopback ou Localhost : 127.0.0.1 (de classe A)
Adresse encore inconnue : 0.0.0.0

Adresses réservées à un usage privé :
Classe A : 10.0.0.0
Classe B : 172.16.0.0 à 172.31.0.0
Classe C : 192.168.0.0 à 192.168.255.0

Masque de réseau et préfixe :

Le masque de réseau est un masque binaire qui permet de produire l'adresse réseau. Donc, il consiste en un nombre sur 32 bits avec tous les bits de poids fort de l'identifiant réseau à 1. L'exemple ci-dessous illustre la construction du masque pour l'adresse de classe B : 131.44.22.211



Donc il faut un masque de valeur 255.255.0.0 pour obtenir à l'aide d'une opération binaire ET l'adresse de réseau 131.44.0.0.

Le préfixe correspond à l'identifiant réseau. Derrière l'adresse de réseau on ajoute le signe / ainsi qu'une valeur. Cette valeur représente le nombre de bits du préfixe.

Par exemple, le réseau noté "212.93.28.0/24" représente toutes les adresses de 212.93.28.1 à 212.93.28.254. Il s'agit donc ici d'un réseau de classe C. Un tableau indiquant des exemples de réseaux privés avec leurs notations est présenté ci-dessous :

Classe	Exemple d'adresse	Adresse réseau	Masque réseau	Plage d'adresses
A	10.0.12.33/8	10.0.0.0/8	255.0.0.0	10.0.0.1 à 10.255.255.254
B	172.25.127.111/16	172.25.0.0./16	255.255.0.0	172.25.0.1 à 172.25.255.254
C	192.168.77.243/24	192.168.77.0/24	255.255.255.0	192.168.77.1 à 192.168.77.254

Adresse APIPA :

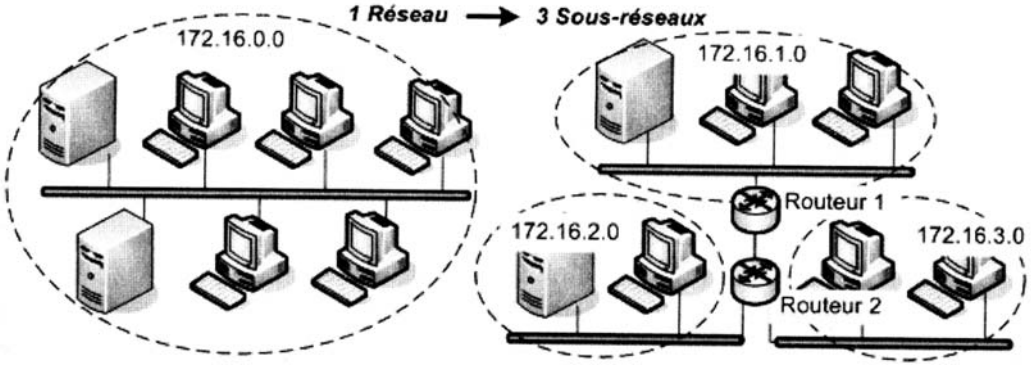
La plage d'adresses APIPA (Automatic Private Internet Protocol Addressing) est la plage correspondant au réseau de classe B d'adresse réseau : 169.254.0.0/16. Il s'agit d'une plage d'adresses utilisées lorsqu'une interface configurée en tant que client DHCP n'obtient pas de réponse d'un serveur DHCP.

L'objectif initial était de permettre à des machines dont le réseau ne dispose pas d'un serveur DHCP de communiquer entre elles.

Les plages d'adresses APIPA ne sont pas routables sur Internet et sont exclusivement dédiées à des communications locales.

Adressage de sous-réseaux :

L'adressage en sous-réseau permet de segmenter un réseau pour regrouper les ordinateurs en domaines et sous-domaines, réduire le nombre de communication et connecter des réseaux d'architectures hétérogènes. L'exemple ci-dessous montre un réseau redécoupé en 3 sous-réseaux :



L'adressage en sous-réseau permet de déterminer si le paquet est destiné à une machine :

- du même réseau
- d'un sous-réseau différent sur le même réseau
- sur un autre réseau

Comme indiqué ci-dessous, le Host ID initial de l'adresse IP est découpé en deux parties :

- Adresse de sous-réseau (subnet ID)
- Numéro de machine dans le sous-réseau (Host ID)

Net ID	Host ID initial	
	SubNet ID	Host ID

Exemple d'adressage de sous-réseau de classe C :

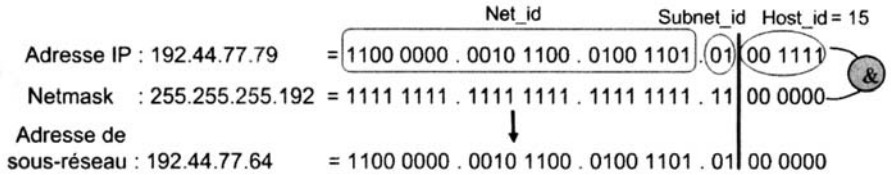
Dans cet exemple deux bits de SubNet Id permettront d'identifier le sous-réseau. Donc quatre sous-réseaux sont possibles. Comme chaque sous-réseau à un Host Id codé sur 6 bits donc 62 (2^6-2) adresses sont disponibles. Les adresses de sous-réseaux sont :

192.44.77.0 / 192.44.77.64 / 192.44.77.128 / 192.44.77.192

Leurs adresses de diffusion sont :

192.44.77.63 / 192.44.77.127 / 192.44.77.191 / 192.44.77.255

Le schéma ci-dessous illustre le découpage binaire de notre sous-réseau :



Pénurie d'adresses IP

Le format des adresses IP étant codée sur 32 bits, il autorise 4 milliards d'adresse IP (2^{32}). Actuellement ce nombre d'adresse est insuffisant pour interconnecter tous les équipements. Plusieurs solutions permettent de remédier à ce problème.

CIDR (Classless Inter Domain Routing)

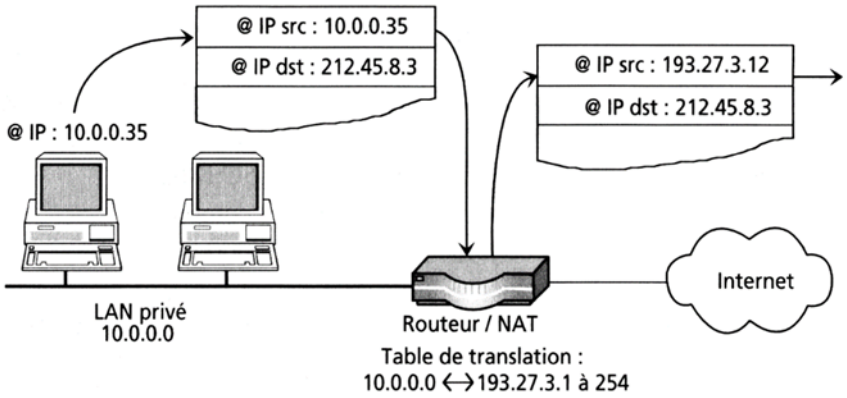
L'idée est d'optimiser les adresses existantes et d'attribuer des réseaux de classe C. Un routeur CIDR va regrouper les sous-réseaux de 254 adresses en un réseau plus global.

Par exemple :

Une entreprise va utiliser deux réseaux 193.127.32.0 et 193.127.33.0
de masque 255.255.255.0
Qui seront agrégés en 193.127.32.0 & 255.255.254.0²
L'agrégat sera noté 193.127.32.0 / 23

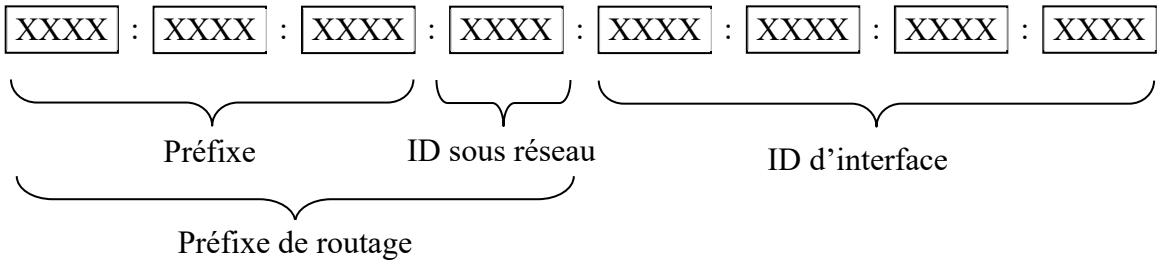
Réseaux privés et NAT

L'utilisation de réseau privé avec un routeur d'adresse qui assurera la translation des adresses IP est une solution à la pénurie d'adresses. Cette technique est illustrée dans l'exemple ci-dessous :

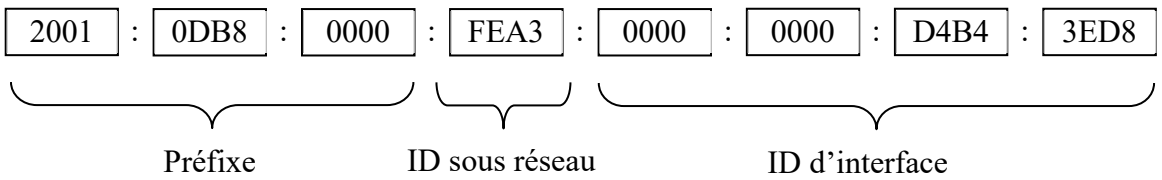


Internet Protocol version 6

L'évolution du protocole IP en version 6 appelé IPv6 est une solution à la pénurie d'adresse IP. L'IPv6 est caractérisée par un codage sur 128 bits de l'adresse IP. L'adresse IPv6 est codée sur 16 octets ou 8 mots de 16 bits. Le nombre d'adresse passe à plus de 10^{28} et il permet de fait une plus grande flexibilité dans l'attribution des adresses et donc du routage des paquets. Le format de base de l'adresse IPv6 est présenté ci-dessous :



Le préfixe de routage correspond à l'adresse de réseau
Exemple :



Ce codage assure la compatibilité avec IPv4 comme le montre l'exemple ci-dessous :

- IPv4 : 212.180.62.226
- IPv6 :
  32.1.13.184.0.0.254.163.0.0.0.0.**212.180.62.216**
  où 2001:db8:0:FEA3:0000:0000:**212.180.62.216**

Pour des raisons pratiques les "0" non significatifs de l'adresse IPv6 ne sont pas représentés (version courte). De plus, il est possible d'omettre les groupes consécutifs à 0 (version abrégée).
IPv6 complète : 2001 : 0DB8 : 0000 : FEA3 : 0000 : 0000 : D4B4 : 3ED8
IPv6 courte : 2001 : DB8 : 0 : FEA3 : 0 : 0 : D4B4 : 3ED8

IPv6 abrégée : 2001 : DB8 : 0 : FEA3 : : D4B4 : 3ED8

Attention, l'écriture suivante est erronée car ambigüe :
IPv6 erronée : 2001 : DB8 : : FEA3 : : D4B4 : 3ED8

Préfixe en IPv6

L'adresse de réseau est identifiée en utilisant la notation de l'IPv4 avec le signe / suivit de la taille du préfixe. Comme en IPv4, le préfixe représente la partie située le plus à gauche de l'adresse IP.

Par exemple l'adresse 2001:DB8::/48 représente le réseau de l'adresse 2001:DB8:0:0:0:0:0:1 à 2001:DB8:0:FFFF:FFFF:FFFF:FFFF

Il est possible de spécifier un préfixe de sous réseau définissant la topologie interne du réseau vers un routeur. Par exemple, le préfixe de sous réseau précédent est :

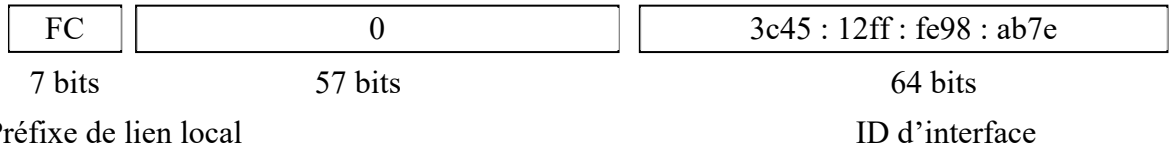
2001:DB8::FEA3::/64

Certains préfixes sont réservés pour des usages spéciaux :
2002::/16, indique un préfixe de routage Ipv6 vers Ipv4.
Fc00::/7, indique une adresse local unique.
fe80::/10, indique une adresse lien-local.
ff00::/8, indique une adresse multidiffusion.

Types d'adresses en IPv6

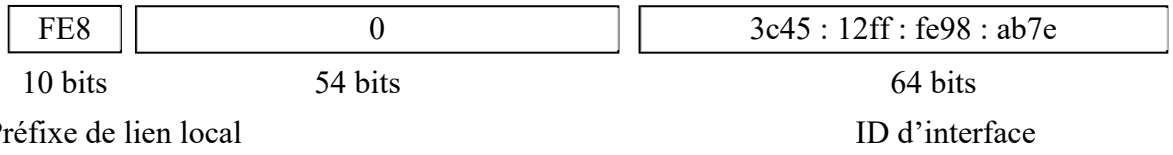
Adresse de réseaux	***Type d'adresses***
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
FC00::/7	Adresses locales uniques (ULA)
FEC0::/10	Adresses locales uniques (ancien)
FE80::/10	Adresses locales lien (auto IP)
FF00::/8	Adresses multicast

Adresse Locale Unique (ULA)



En pratique : FD::/8 car FC ::/8 est réservé.

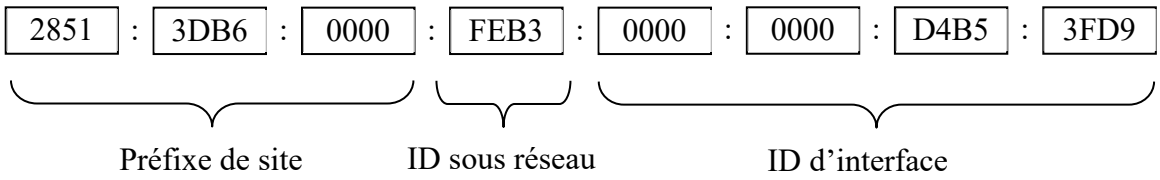
Adresse de lien local



L'ID d'interface peut être dérivée de l'adresse MAC (EUI-64).
Ces adresses équivalentes aux adresses APIPA sont indispensables pour chaque interface.

Adresse unicast globale

Exemple illustrant les 3 parties de l'adresse unicast globale :

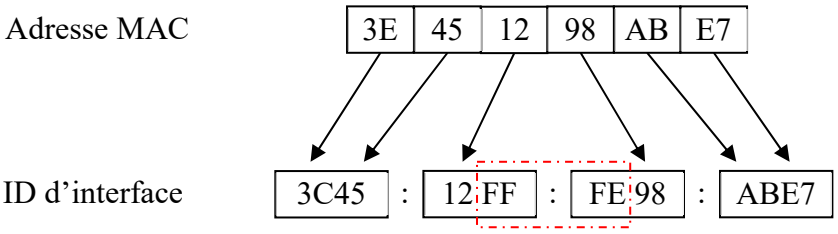


EUI-64 :

Extended Unique Identifier 64bits est un identifiant unique utilisant l'adresse MAC pour former l'ID d'interface. Pour former l'ID d'interface on insère au milieu de l'adresse MAC la valeur hexadécimale FFFE puis le 7ème bit en partant du poids fort est inversé.

Exemple :

Soit le PC d'adresse MAC : 3E451298ABE7



Multicast en IPv6

L'IPv6 autorise le multicast et l'utilise en autre pour la découverte de réseau. En effet, l'IPv6 ne dispose pas du broadcast classique comme l'IPv4 mais utilise le multicast comme NDP (Neighbor Discovery Protocol). Les adresses IPv6 : FF00 : : /8, sont réservées au multicast et cela représente le groupe d'adresse de FF00:0:0:0:0:0:0:0 à FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Le codage des adresses multicast IPv6 est représenté ci-dessous :

Prefix (8bits)	***Flags (4bits)***	***Scope (4bits)***	***Identifiant de groupe (112bits)***
0xFF	XRPT	xxxx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Les bits de flags sont décrits dans la norme RFC 4291 et pour résumer le bit T (Transient) indique si l'adresse est standard (=0) ou pas (=1). En fait, lorsque ces 4 bits sont à 0, il s'agit d'un multicast géré par une autorité comme indiqué dans le tableau ci-dessous :

Valeur du scope	***Adresse ou préfixe***	***Description***
1	FF01::/16	Multicast local à l'hôte
2	FF02::1/64	Tous les hôtes sur un segment
2	FF02::2/64	Tous les routeurs sur un segment
2	FF02::1:FF00/104	Nœuds sollicités par NDP (ARP)
5	FF05::1/64	Tous les hôtes d'un site
8	FF08	Adresse locale à une organisation
7	FF0E	Adresse globale

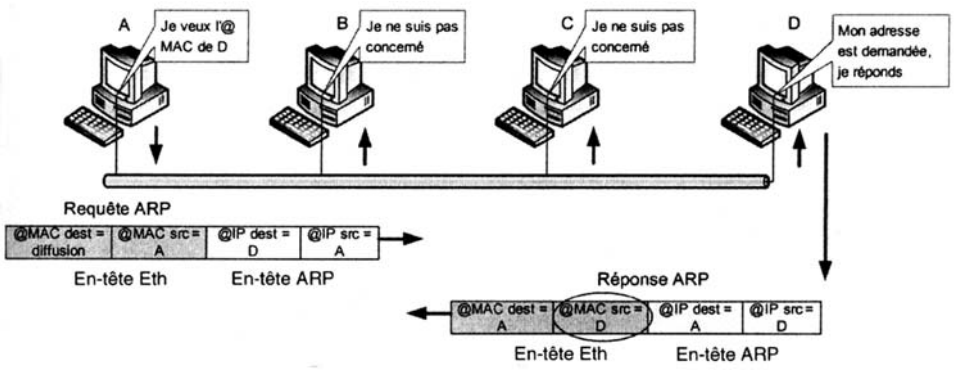
(Attention ! Ce tableau est incomplet...)

Protocole ARP

Le protocole ARP (Address Resolution Protocol) permet de faire la correspondance entre

Adresse logique (IP) ←→ Adresse physique (MAC)

Le dessin ci-dessous illustre la communication entre deux machines A et D pour une résolution d'adresse IP / MAC :



Les ordinateurs possèdent une table ARP qui contient la correspondance entre l'adresse IP et l'adresse MAC. L'adresse MAC est utilisée par les switches qui commutent les paquets grâce à cette dernière (couche 2 ou couche liaison, du modèle OSI).

L'entête ARP montré ci-dessous est composée de 28 octets qui contiennent les informations suivantes :

- Type des adresses physique et logique
- Taille des adresses physique et logique
- Adresse source physique et logique
- Adresse destinataire physique et logique

Type @ phy.	Type @ log.	Taille @ phy.	Taille @ log.	Code ARP	@ phy. source	@ log. source	@ phy. cible	@ log. cible
2 octets	2	1	1	2	(6)	(4)	(6)	(4)

Le code ARP dans la trame Ethernet est 0x806. Dans la trame ARP de demande, l'adresse MAC du destinataire est l'adresse MAC inconnue, c'est-à-dire 00:00:00:00:00:00.

Requêtes ARP gratuites

Elles sont émises par un nouvel arrivant sur le réseau et permettent de vérifier l'unicité de son adresse IP. Aucune réponse n'est attendue et les récepteurs prennent connaissance de l'adresse du nouvel arrivant.

Attention : de nombreuses requêtes d'ARP gratuit peuvent indiquer un problème réseau (problème de connexion ou câble défectueux).

Protocole ICMP

Le protocole ICMP est utilisé pour gérer les infos contrôlant le trafic IP. Il permet aux routeurs d'envoyer des messages de contrôle ou d'erreur à des ordinateurs ou routeurs. Ces principales fonctions sont :

- Le contrôle de flux
- La détection d'inaccessibilité
- La redirection des voies
- La détection d'expiration de paquet
- La détection de paramètre incorrect

Le format de la trame ICMP est montré ci-dessous :

Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
Version / IHL	Type de service	Longueur totale	
Id (fragmentation)		Flags et offset (fragmentation)	
Durée de vie (TTL)	Protocole	Check Sum de l'entête	
Adresse IP source			
Adresse IP destination			
Type de message	Code	Check sum	
Bourrage éventuel			
Données (optionnel et de longueur variable)			

Type de messages ICMP

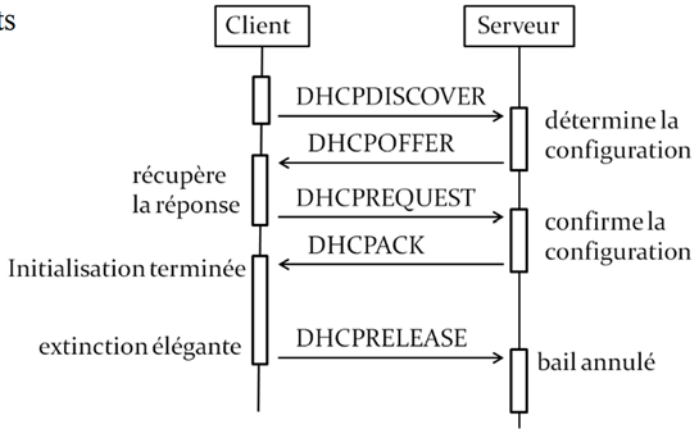
- Type 8 et 0 – demande et réponse écho
- Type 3 – machine inaccessible (code de 0 à 15…)
- Type 4 – extinction de la source
- Type 5 – redirection
- Type 11 – Temps dépassé
- Type 12 – Entête erronée
- Type 13 & 14 – demande et réponse d'heure
- Type 15 & 16 – demande et réponse d'adresse IP
- Type 17 & 18 – demande et réponse de masque de sous-réseau

Protocole DHCP

Le protocole DHCP est un protocole niveau 7 ou application qui permet de gérer l'attribution dynamique des adresses IP et utilise le protocole UDP. Les serveurs DCHP écoutent sur le port 67 et les clients sur le port 68. Un serveur DHCP configuré dans le réseau possède une table d'adresses IP valides localement et attribut dynamiquement une adresse disponible à une machine nouvellement connectée au réseau local. Le serveur DHCP contient les informations suivantes :

- Une table d'adresse IP valides
- Une table d'adresse IP réservées (statiques)
- Des paramètres de configuration des clients
- La durée des baux

Le schéma ci-contre montre le dialogue DHCP :



Le format de la trame DHCP est :

Bits 31-24	Bits 23-16	Bits 15-8	Bits 7-0
Opération hard	Longueur adresse	Type de hard	Opération
Id client (valeur aléatoire)			
Drapeaux divers		Temps écoulé depuis la demande	
Adresse IP client			
Nouvelle adresse IP client			
Prochaine adresse IP du serveur DHCP			
Adresse IP du relais (si connexion direct impossible)			
Adresse hardware client (16 octets)			
Nom du serveur DHCP (optionnel 64 octets)			
Nom du fichier pour le boot (128 octets) / options (variable)			

Les principales requêtes DCHP sont listées ci-dessous :

Sens	Nom	Description
C→S	DHCPDISCOVER	Localiser les serveur DHCP demander une configuration
S→C	DHCPOFFER	Réponse du serveur à DHCPDISCOVER contient la configuration
C→S	DHCPREQUEST	Requête (par ex. prolonger le bail)
C→S	DHCPDECLINE	Adresse déjà utilisée
S→C	DHCPACK	Contient la configuration client dont l'IP
S→C	DHCPNACK	Bail échu ou mauvaise configuration du client
C→S	DHCPRELEASE	Libération de l'IP
C→S	DHCPFORM	Demande de paramètres locaux (IP déjà connue)

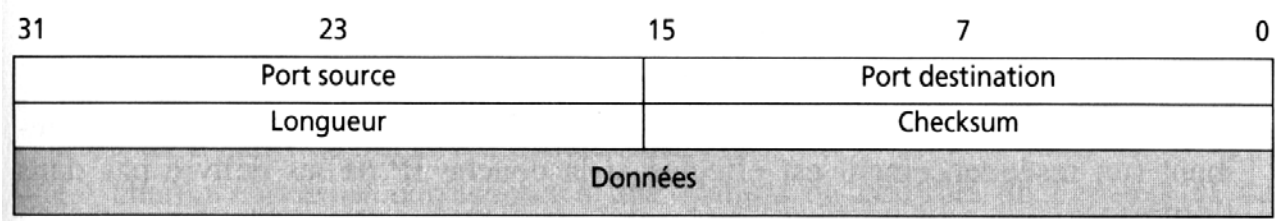
Attention : Certains OS, notamment Windows, peuvent initier une séquence DHCP courte. Cette séquence démarre par un envoi DHCPREQUEST ou l'ordinateur demandeur fait une requête en proposant l'ancienne adresse obtenue précédemment. Cette séquence raccourcie permet d'accélérer grandement la connexion au réseau.

Protocole UDP

Le protocole UDP (User Datagram Protocol) est un protocole de niveau 4 donc de la couche transport du modèle OSI. Ce protocole utilise le protocole IP (couche 3, réseau) donc les adresses IP. Ce protocole est utilisé pour le transfert de données de manière simplifié. Le protocole UDP ne nécessite pas de connexion préalable d'une station à l'autre, les données sont simplement envoyées. L'émetteur des données ne sais pas si elles ont correctement été reçues par le destinataire. Le protocole UDP est dit **sans connexion** et dispose d'un nombre de fonctionnalité minimaliste.
Notion de port : l'émetteur et le destinataire dispose d'un port pour caractériser la communication.
Le protocole UDP est utilisé dans beaucoup de protocoles : DHCP, DNS, SNMP, NTP, …

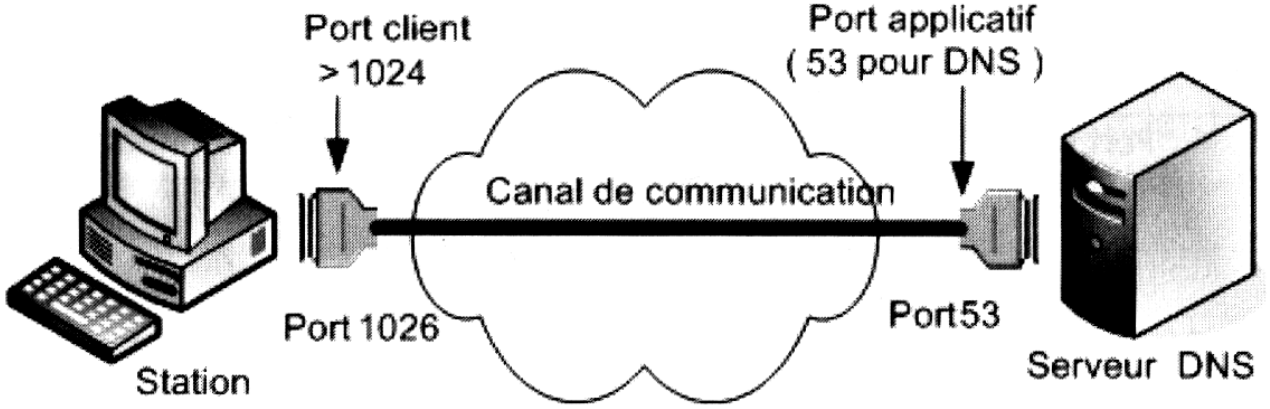
Trame UDP

La trame UDP est contenue dans une trame IP avec le chap de protocole = 17.
La trame UDP contient le port source et destination. La longueur totale des données et une somme de contrôle (checksum). Voir ci-dessous :



Port de communication

Le port de communication est utilisé par les protocoles UDP et TCP de la couche 4 transport. Le port est une référence dans la communication entre applications. Le port permet de distinguer les différents interlocuteurs ou application dans la station qui communique avec une autre. Le serveur écoute sur un port personnel et le client accède au serveur par le port d'écoute. Le client utilise un port source afin que le serveur puisse répondre à l'application qui communique avec lui.
Le schéma ci-dessous illustre la communication d'un client avec un serveur DNS.



La valeur du port de communication est codée sur 16bits de 0 à 65535.
Les ports de 0 à 1023 sont réservés.
Exemples de ports :

- 0 : réservé
- 20 et 21 : données et contrôle FTP (File Transfert Protocol)
- 22 : login à distance SSH
- 23 : Telnet
- 53 : DNS
- 68 : DHCP
- 80 : World Wild Web, HTTP
- 110 : POP3
- 115 : SFTP (Simple File Transfert Protocol)
- 123 : NTP (Network Time Protocol)
- 443 : World Wild Web, HTTPS

Exemples de ports non spécifiques :
1433 : serveur base de données MS SQL
1521 : serveur base de données Oracle Database
1723 : PPP VPN
1863 : MSN Messenger
3306 : serveur base de données MySQL
3307 : serveur base de données MariaDB
3389 : prise de contrôle à distance RDP
5432 : base de données PostgreSQL
6667 : connexion aux serveur IRC
8080 : alternative HTTP
8443 : alternative HTTPS

Détails: www.frameip.com/liste-des-ports-tcp-udp

Protocole TCP

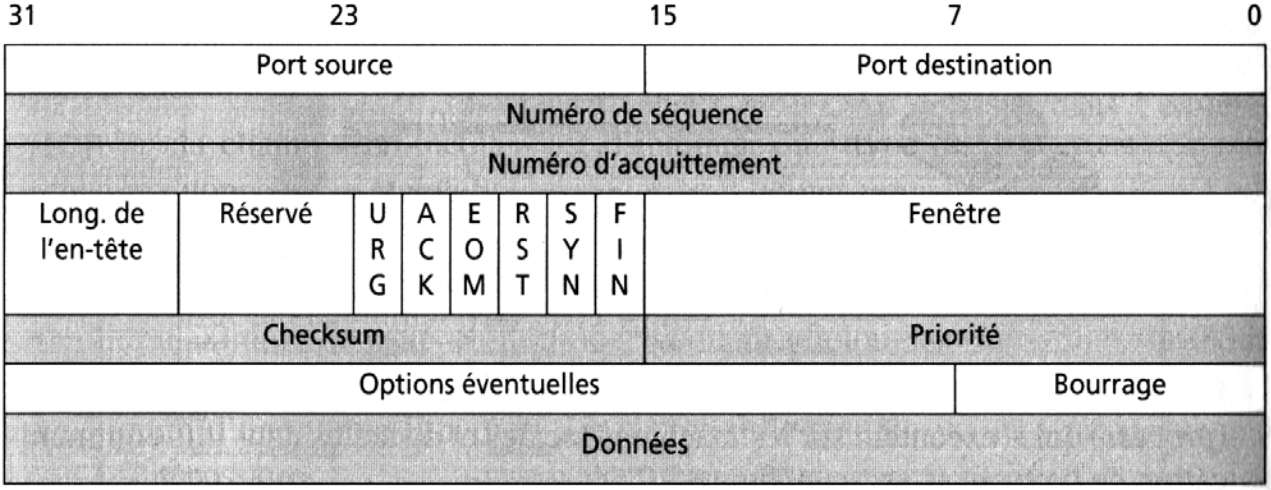
Le protocole TCP (Transmission Control Protocol) est un protocole de niveau 4 donc de la couche transport du modèle OSI. Ce protocole utilise le protocole IP (couche 3, réseau) donc les adresses IP. Le protocole TCP nécessite une connexion préalable d'une station à l'autre, donc il y a un client et un serveur dans ce protocole. Le protocole TCP est dit **avec connexion** et dispose d'un nombre de fonctionnalité plus important que UDP.
Les fonctionnalité de TCP sont les suivantes :

- Ouverture et fermeture de connexion virtuelle
- Segmentation et réassemblage des données
- Acquittement des datagrammes et retransmission en cas d'absence d'acquittement
- Contrôle de flux
- Multiplexage des données des plusieurs hôtes
- Gestion des priorités des données et de sécurité

Notion de port : l'émetteur et le destinataire dispose d'un port pour caractériser la communication.
Le protocole UDP est utilisé dans beaucoup de protocoles : DHCP, DNS, SNMP, NTP, …

Trame TCP

La trame TCP est contenue dans une trame IP avec le chap de protocole = 6.
Le schéma de la trame TCP est illustré ci-dessous :

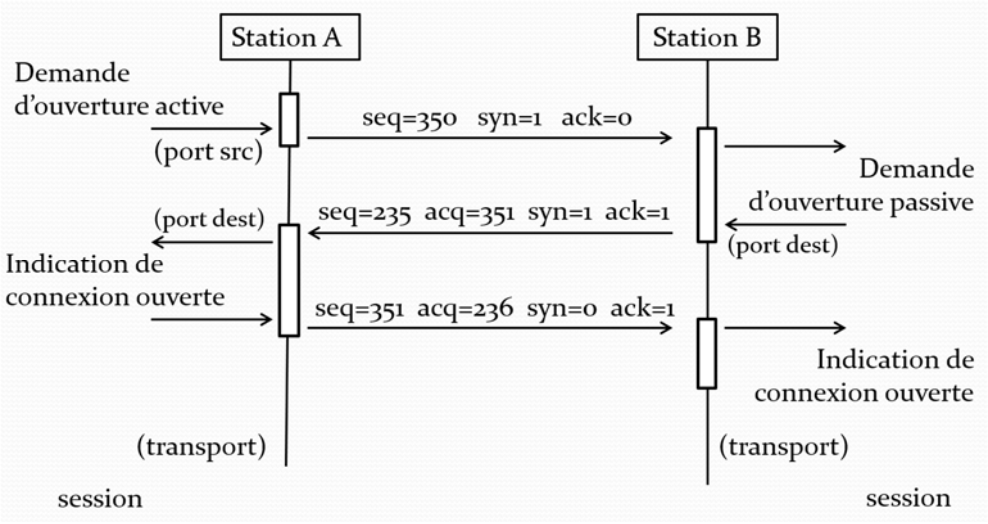


La trame TCP contient :

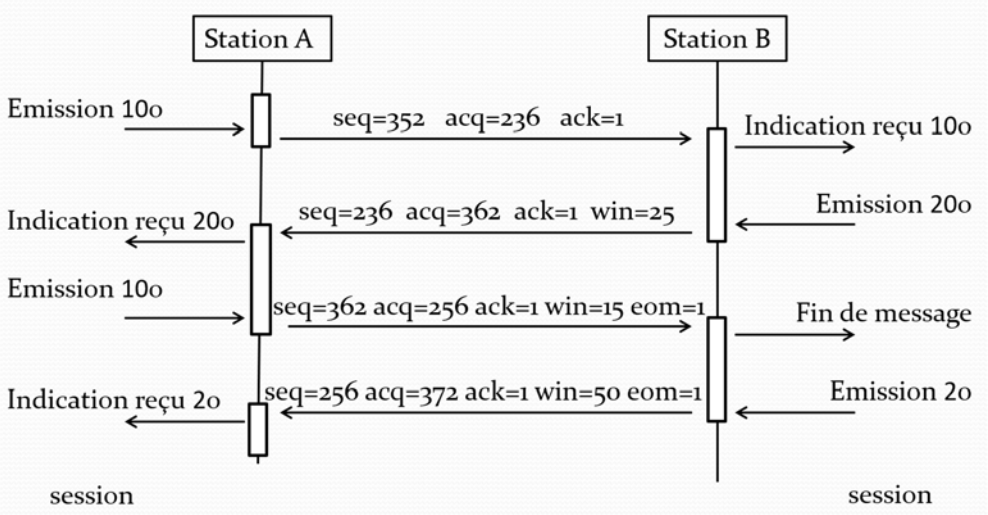
- Port source et destination
- Numéro séquence premier octet de la séquence
- Numéro d'acquittement : numéro séquence suivante
- Longueur de l'entête (4bits) : nombre de mot (32bits) de l'entête

- URG : si le champ des priorités utilisé
- ACK : si le champ d'acquittement significatif
- EOM : fin des messages
- RST : réinitialisation de connexion
- SYN : ouverture de connexion (synchro du numéro de séquence)
- FIN : fin de connexion
- Fenêtre : nombre d'octets que le récepteur peut accepter
- Checksum : somme de contrôle
- Priorité : pointeur sur les données importantes

La séquence ci-dessous montre une connexion à l'aide du protocole TCP :

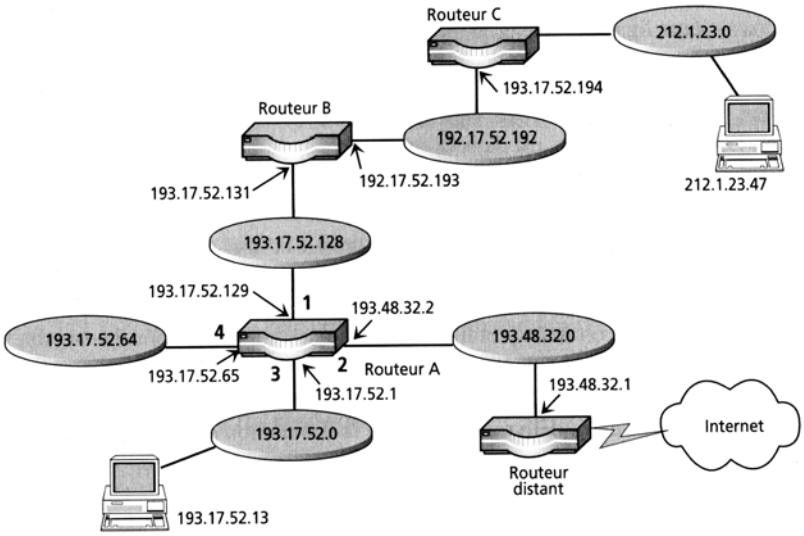


La séquence ci-dessous montre un transfert de données à l'aide du protocole TCP :

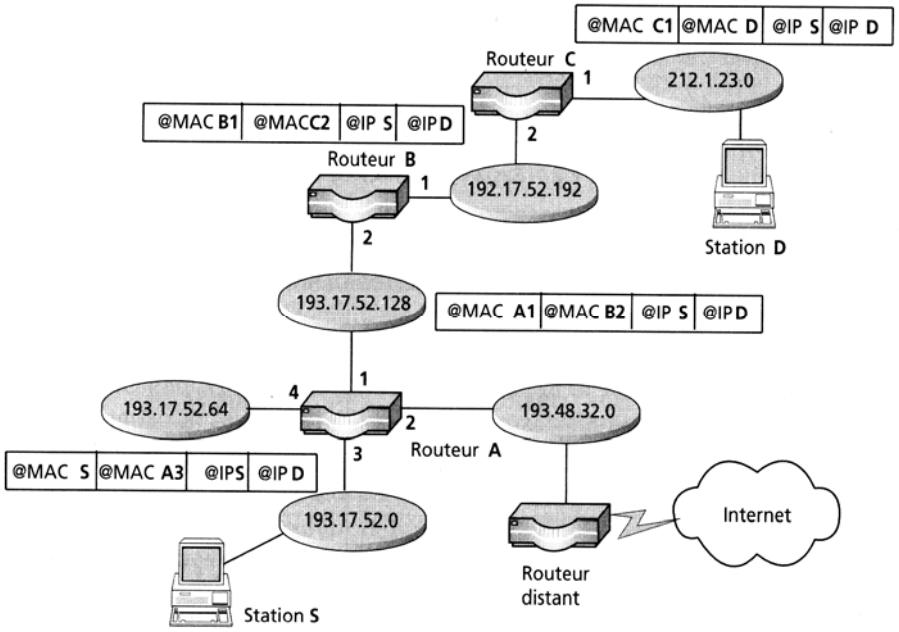


Routage

L'objectif du routage de réseau Internet est de trouver le chemin du destinataire à partir de l'IP.
Si le destinataire n'est pas dans le sous réseau alors les paquets vont être envoyés vers un routeur par défaut. L'adresse du routeur est en général dans les premières adresses du sous réseau. Par exemple : pour le sous réseau 193.17.52.128, l'adresse du routeur serait 192.17.52.129.
Le diagramme ci-après illustre un réseau composé de différents sous-réseaux avec chacun leur routeur :



L'exemple ci-dessous montre le routage d'un paquet de la machine S (source) vers la machine D (destination) à travers plusieurs sous réseaux :



Protocoles de routage :

Il existe plusieurs protocoles de routage :

- Statique : La table de routage est établie une fois pour toutes.
- Dynamique : La table de routage est mise à jour continuellement par des protocoles dédiés.

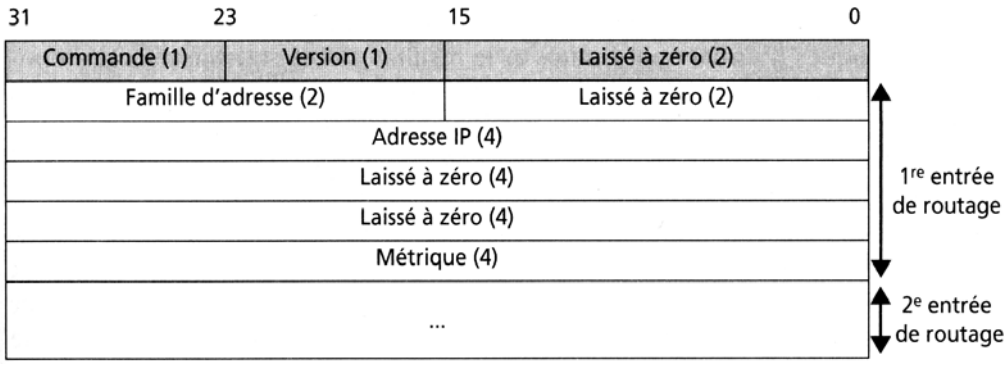
Algorithmes :

- À vecteur de distance : Il permet à chaque routeur de mémoriser la plus courte distance (RIP)
- À état de lien : La transmission de la carte complète des liens possibles. Calcul local de la meilleure route (OSPF)

Protocole RIP

Le Routing Information Protocol (RIP) est un protocole de routage IP à vecteur de distance. Le routeur diffuse les routes connus à ces voisins toutes les 30 secondes en UDP.
Rappel de routage pour un temps supérieur à 3min, on considère une route infinie (=16). La route est définie par l'adresse destination, le routeur et nombre de sauts.

L'entête RIP contient une commande qui peut être une demande ou réponse et le numéro de version du protocole RIP utilisé. Il y a actuellement 2 versions de RIP.
Le dessin ci-après illustre la trame UDP du protocole RIP :



La métrique est une valeur de 1 à 15 (16= infini) et il peut y avoir jusqu'à 25 entrées de routage (512 octets au maximum).

Séquences RIP

- Initialisation
  - Demande des tables aux autres routeurs
  - Famille d'adresse=0 et métrique=16
- Requête reçue
  - Réponse à l'initialisation avec la table de routage
- Réponse reçue
  - Le routeur met à jours sa table de routage
- Mises à jour périodiques
  - Toutes les 30s la table est envoyée aux autres routeurs
- Mises à jour déclenchées
  - Lorsque la métrique d'une route est modifiée les entrées concernées sont transmises aux routeurs voisins

Service DNS

Le Domain Name System (DNS) est un système qui permet d'utiliser des noms symboliques à la place des adresses IP. Le ou les serveurs DNS font la résolution de l'URL en adresse IP. Les noms symboliques ou noms de domaines désignent l'adresse des sites WEB et sont contenus dans URL (Uniform Resource Locator). Ces noms de domaines sont délivrés par l'autorité de nommage de l'Internet ICANN (Internet Corporation for Assigned Names and Numbers). Chaque zone à son responsable et l'autorité française est l'AFNIC (Association Française pour le Nommage Internet en Coopération).

Le dessin ci-dessous illustre la répartition des serveur DNS en fonction des différentes zones.

Nommage hiérarchique :

Serveurs racines

Global Top Level Domain

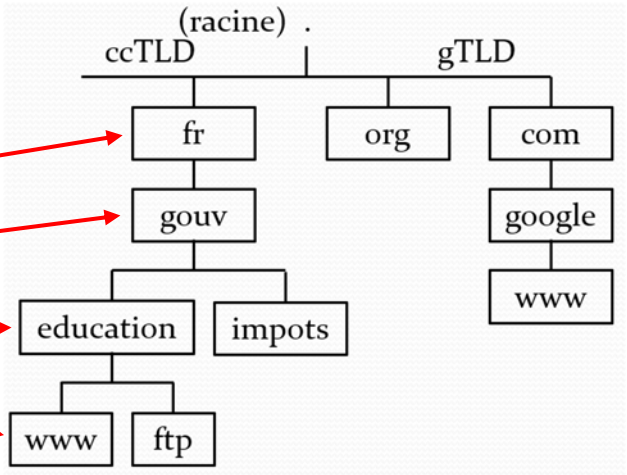
Country TLD

Domaines racines

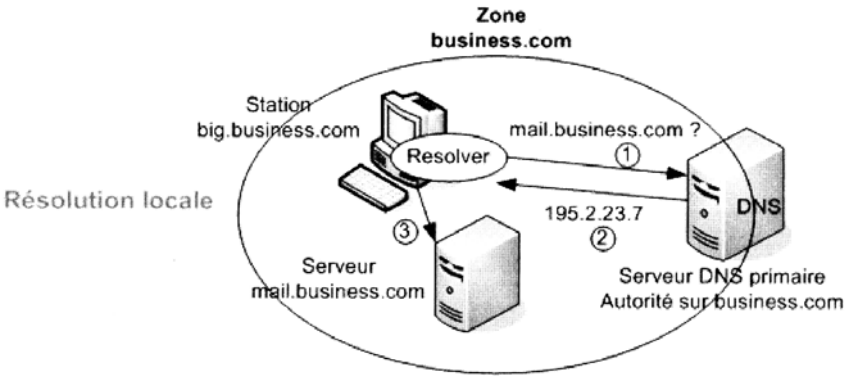
Domaines 2ème niveau

Domaines 3ème niveau

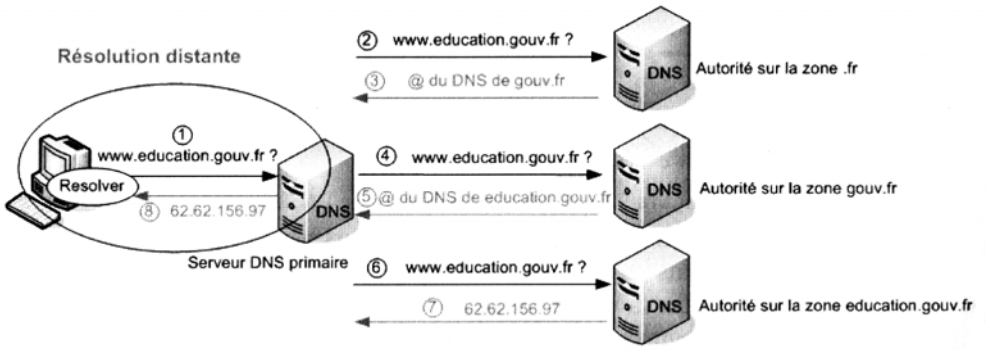
Sous-domaine ou nom de l'hôte



Le schéma ci-après montre un exemple de résolution locale de nom de domaine :



Le schéma ci-dessous montre un exemple de résolution distante de nom de domaine :



Protocole HTTP

Le protocole http (HyperText Transmission Protocol) est un protocole de communication entre un client et un serveur WEB. C'est un protocole de transfert de lien hypertextes composés de :

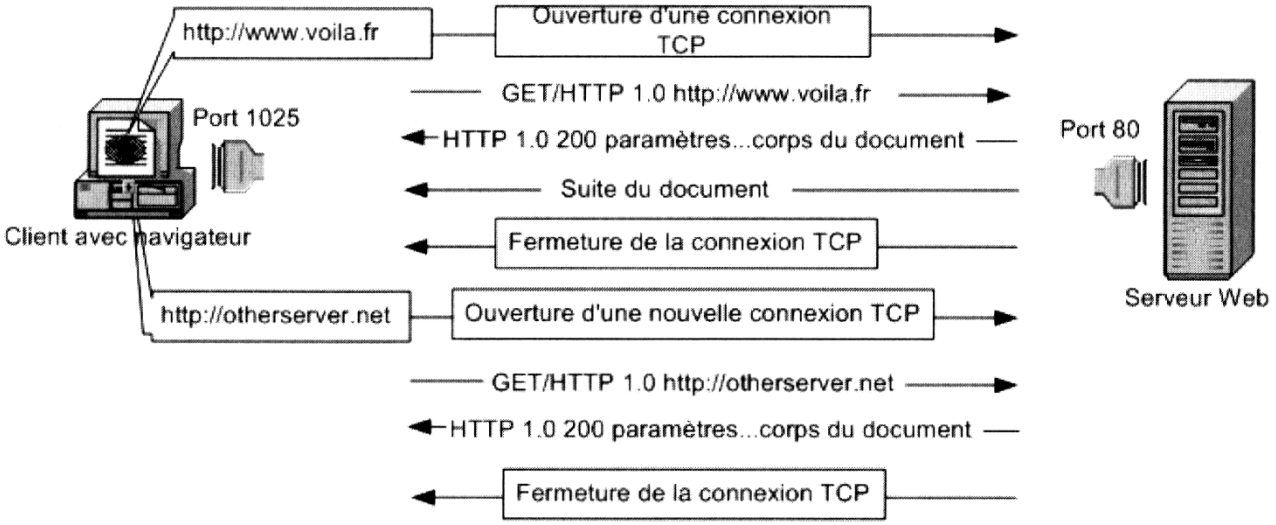
- URL (Uniform Resource Locators)
- Fichier, image, son, …
- Serveur WEB, FTP, mail, news, …

Par exemple :

- http://www.dorian.fr
- ftp://ftp.dorian.fr
- file:////c:/temp/toto.txt
- mailto:n.llaser@wanadoo.fr

Dialogue HTTP

Le schéma ci-dessous montre un exemple de dialogue entre le navigateur d'un ordinateur client et un serveur WEB :



Les informations sont transmises au format texte. Les informations de l'exemple ci-dessus sont listées ci-après :

- Demande client :
  - GET / HTTP/1.0
- Réponse serveur :
  - HTTP/1.1 200 OK
  - Entête de réponse
  - Saut de ligne
  - Données…

Requêtes HTTP

Le protocole HTTP possède 9 requêtes qui sont listées ci-dessous :

- GET
  - Demande de données d'une ressource (sans modification)
- HEAD
  - Demande d'informations sur une ressource
- POST
  - Envoie de données vers le serveur avec modification d'une ressource
- OPTIONS
  - Demande les options du serveur HTTP
- CONNECT
  - Connecte un proxy
- TRACE
  - Demande un écho de la requête
- PUT
  - Ajoute ou remplace une ressource sur le serveur
- PATCH
  - Modification partielle d'une ressource sur le serveur
- DELETE
  - Efface une ressource sur le serveur

Protocole HTTPS

Le protocole HTTPS (Hypertext Transfer Protocol Secure) est le chiffrement TLS de HTTP. Le système de chiffrement TLS utilise un chiffrement basé sur des clefs privées et publiques.

HTTPS permet au navigateur client de vérifier l'identité du site WEB, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable. Le navigateur WEB possède une liste de ces certificats. Il est important de mettre à jour cet liste à travers le navigateur et d'avoir un système informatique à l'heure. HTTPS garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur et reçues du serveur. Il peut permettre de valider l'identité du visiteur, si celui-ci utilise également un certificat d'authentification client émis par une autorité fiable.

Certaines autorités peuvent détenir des certificats qui leur permettent de surveiller les contenus échangés.