1 INTRODUCTION

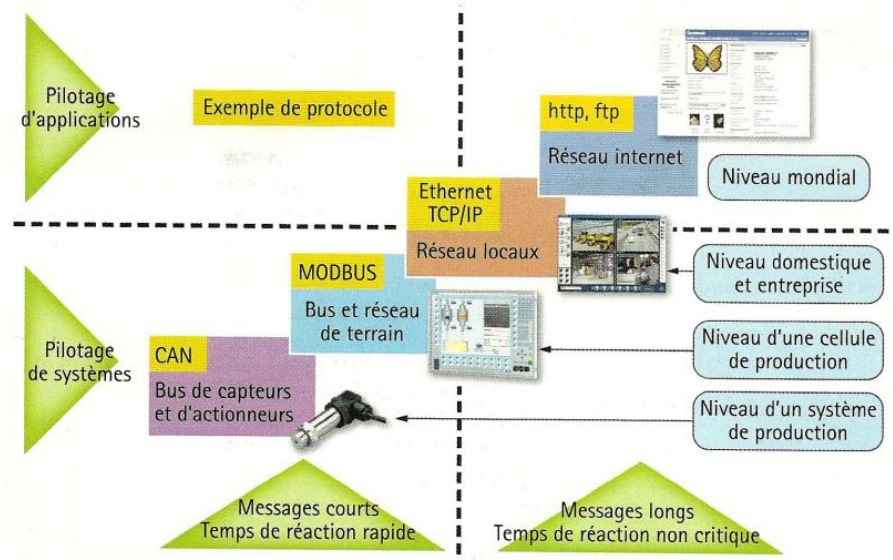


Fig.1 Quelques exemples de réseaux – *source Nathan*

Un réseau permet d'interconnecter entre eux différents hôtes afin d'échanger des informations (fig.1). Il existe des réseaux adaptés à la nature des échanges et des équipements connectés. Il est en effet possible d'interconnecter et de faire communiquer quantité d'équipements capteurs et actionneurs industriels, caméras, imprimantes ou ordinateurs avec différents systèmes d'exploitation (Windows, Mac, Linux …etc.).

Dans le monde de l'automobile (fig.2), par exemple, les principaux organes d'un véhicule sont reliés en **réseau de terrain** afin de pouvoir communiquer entre eux de façon très rapide (on parle de temps réel) et fiable (pas de perte de données) afin de pouvoir fournir en permanence des informations sur l'état du véhicule.

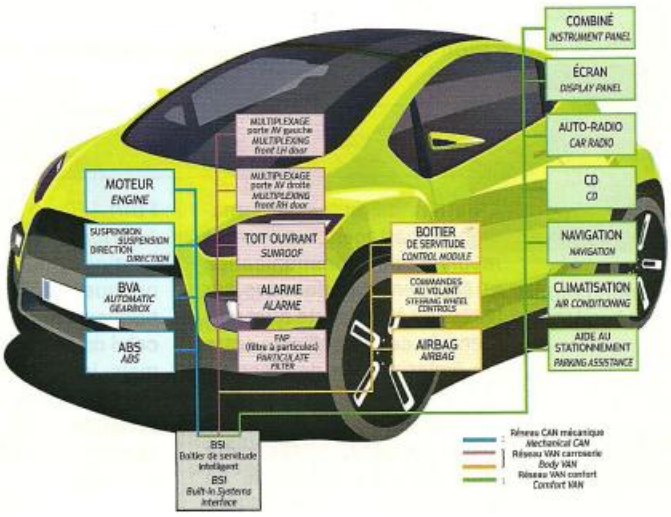


Fig.2 Réseaux de terrain – véhicule PSA *source Hachette*

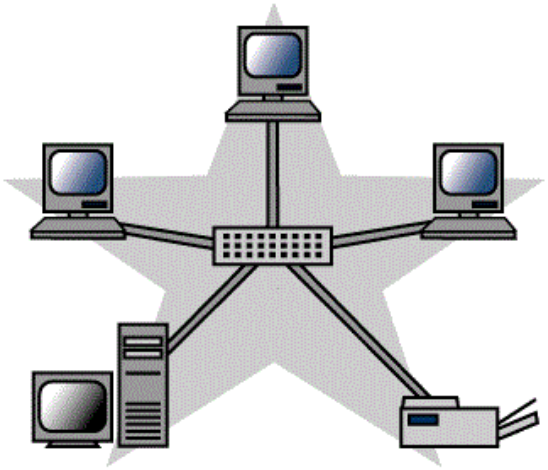


Fig.3 Réseaux local - *source Google image*

A l'inverse, la plupart des services réseau offerts sur **réseau local** ou sur Internet (fig.3) ne seront pas perturbés en cas de perte de données pendant la transmission (données renvoyées).

Le point commun entre tous ces réseaux réside dans le fait que tous les éléments sont reliés entre eux par une **liaison de communication** commune. Il est nécessaire de gérer la façon dont les constituants du réseau vont pouvoir transmettre des données sans interférence. Il faudra aussi coordonner les échanges afin d'éviter des pertes de données.
Il convient alors de mettre en œuvre un langage commun aux différents éléments communicants, appelé **protocole de communication**. En fonction des hôtes du réseau certains langages ou protocoles seront adaptés.

CC BY NC SA

2 TOPOLOGIE

2.1 Réseaux locaux / réseaux distants

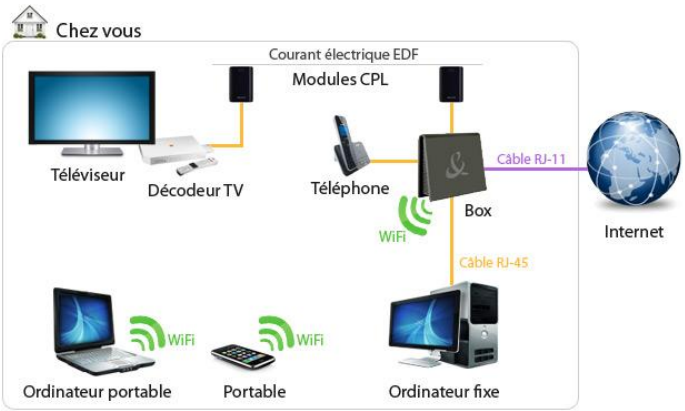
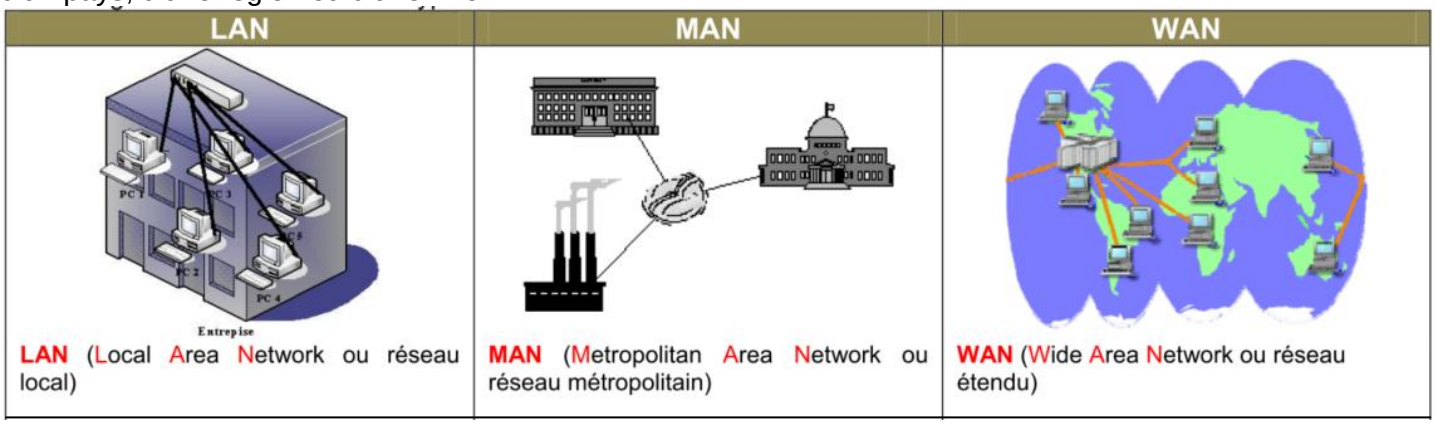


Fig.4 Réseau informatique domestique

On parle de **réseau local (LAN Local Area Network)** pour un ensemble d'équipements informatiques, appartenant à une même société ou bien le matériel composant le réseau informatique domestique (fig.4). L'infrastructure est privée et elle est gérée localement.

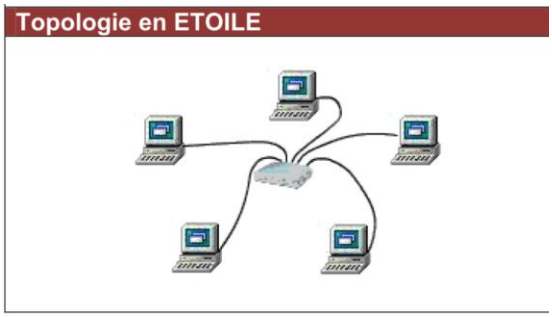
- Si les liaisons de communication sont des liens physiques (câble RJ45, fibre optique, CPL Courants Porteurs en Ligne), on parle de **réseau fixe**.
- Si les liaisons de communication sont des liens sous forme d'ondes hertziennes (Wifi, WiMax) on parle **de réseau sans fil**.

Les réseaux métropolitains (MAN: Metropolitan Area Network).
Ce type de réseau est apparu relativement récemment et peut regrouper un petit nombre de réseau locaux au niveau d'une ville ou d'une région. L'infrastructure peut être privée ou publique. Par exemple, une ville peut décider de créer un 'MAN' pour relier ses différents services disséminés sur un rayon de quelques kilomètres et en profiter pour louer cette infrastructure à d'autres utilisateurs.
Les réseaux distants (WAN: Wide Area Network).
Ce type de réseau permet l'interconnexion de réseaux locaux et métropolitains à l'échelle de la planète, d'un pays, d'une région ou d'une ville.



2.2 Différentes topologies physiques

Une topologie, ou architecture physique d'un réseau caractérise l'arrangement physique des **nœuds** constituants le réseau.
noeud : Equipement (ordinateur, commutateur, imprimante réseau, …etc.) du réseau informatique possédant une interface de communication.



Les réseaux suivant une topologie en étoile ne sont pas vulnérables car on peut aisément retirer une des connexions en la débranchant sans pour autant paralyser le reste du réseau.
Chaque machine est connectée à un concentrateur (HUB)* ou un commutateur (SWITCH) situé au centre de "l'étoile". S'il y a une interruption de la connexion vers une machine, celle-ci sera la seule à être déconnectée. Le reste du réseau continue de fonctionner normalement. Les réseaux de topologie en étoile ne sont pas vulnérables.
Concentrateur/Hub : matériel obsolète remplacé par le commutateur/switch.

De nos jours la plupart des réseaux informatiques sont dans une topologie en étoile.

2.3 Matériels actifs

On appelle matériel actif tout le matériel comportant un équipement électronique chargé d'assurer la répartition des signaux entre les différentes branches d'un réseau informatique.
Il s'agit principalement des concentrateurs (hubs), commutateurs (switches) et routeurs.

Baie de brassage avec un switch 24 ports

Définitions sommaires :

Un concentrateur ou hub est un répéteur de données multiports.

Un **commutateur réseau**, ou **switch**, est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il transmet les données reçues sur un port, seulement vers le port sur lequel la station destinatrice est connectée, alors qu'un hub diffuse ces informations sur l'ensemble des ports de l'appareil.

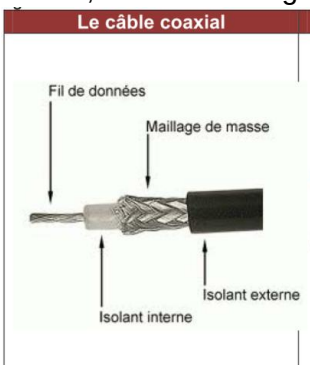
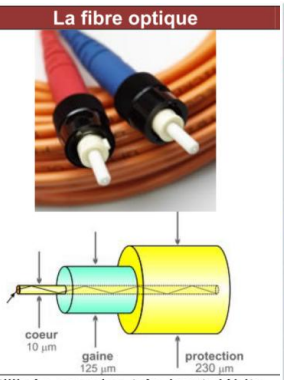
Contrairement au hub, on peut donc dire qu'il est « intelligent », car il capable de savoir qui est le destinataire d'un message.

Un **routeur** assure le passage de l'information entre deux réseaux distincts en choisissant le meilleur chemin. Il permet l'acheminement optimal des paquets de données entre différents réseaux.
En général les routeurs intègrent un switch de petite capacité.
Les « box » des F.A.I. (Fournisseurs Accès Internet) contiennent un routeur, un switch (4 ports), un modem ADSL et parfois une borne d'accès WIFI.
Ces « box » permettent d'interconnecter le réseau local de l'utilisateur au WAN.
Un routeur dispose en général (au moins) de 2 adresses IP, une pour le réseau local LAN et une autre pour sa connexion au deuxième réseau (LAN ou WAN).

Les appareils cités ci-dessus sont rangés dans la catégorie du <u>matériel actif</u>, par opposition, les câbles, les coffrets, les cordons et panneaux de brassages sont rangés dans la catégorie du *<u>matériel passif</u>*.

2.4 Matériels passifs

Pour relier les diverses entités d'un réseau, plusieurs supports physiques de transmission de données peuvent être utilisés. Une de ces possibilités est l'utilisation de câbles. Il existe de nombreux types de câbles, mais on distingue généralement :

Le câble coaxial	Les paires torsadées	La fibre optique
		
quasiment abandonné	technique la plus répandue	utlilisée pour les très haut débits

Type câble	Distance maxi	Débit
Coaxial	185 m	10 Mb/s
Paire torsadée non blindée	100 m	10 Mb/s
Paire torsadée blindée (cat 5)	100 m	100 Mb/s
Paire torsadée blindée (cat 6)	100 m	1000 Mb/s
Fibre optique	60 km	Jusqu'à 10 Gb/s

D'autres techniques de liaison sont disponibles telles que :

- CPL (courants Porteurs en Ligne) utilisant des lignes d'alimentation électriques : techniques réservée le plus souvent aux réseaux domestiques (« indoor »).
- Par ondes électromagnétiques : liaisons RF (Radio Frequency) permettant de réaliser des réseaux locaux sans fils ou WLAN (Wireless Local Area Network). On rencontre la technique :
  - Wi-Fi (Wireless Fidelity) : ses protocoles sont régis par la norme IEEE 802.11 et ses déclinaisons.
  - Bluetooth avec son service RFCOMM

3 TRANSMETTRE DES INFORMATIONS

Quelque soit le réseau, le principe de transmission de l'information reste le même : les données numériques sont envoyées les une après les autres en série, sous forme d'une succession de bits, à une cadence donnée.

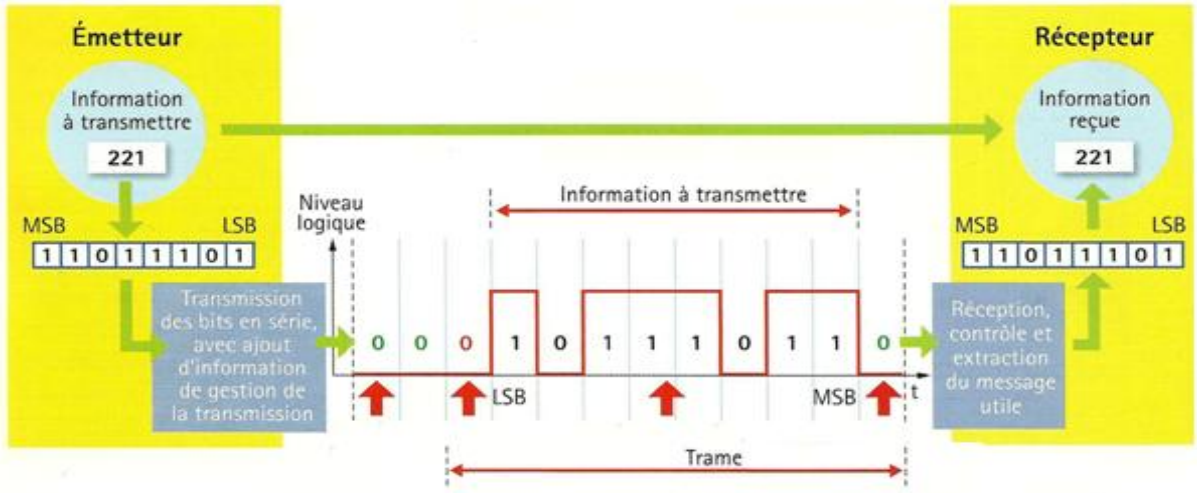


Fig.5 Transmission de données sur 8 bits + 1 bit début + 1 bit fin

A cette information que l'on doit envoyer, il est nécessaire d'en ajouter d'autres qui vont gérer la bonne marche de la transmission. On rajoutera au minimum : le début de la transmission, bonne transmission et fin de transmission. Ces informations là ne seront prises en compte que par les interfaces qui prennent charge l'émission et réception des données

Comme le montre l'exemple ci-dessus (fig.5), il nécessaire d'ajouter des informations supplémentaire au message à transmettre pour assurer le transport de l'information jusqu'au destinataire. Ces informations supplémentaires sont classées par couches.

De façon simplifiée, on peut faire l'analogie avec l'envoi par la poste d'une lettre dans une enveloppe timbrée (fig.6). Le contenu de la lettre est l'information à transmettre au destinataire. Pour assurer son acheminement sans se soucier du moyen de transport utilisé (train, avion, …etc.), ce message est **encapsulé** dans une enveloppe dont la fonction est d'indiquer l'adresse du destinataire, celle de l'émetteur au cas où la lettre ne pourrait pas être délivrée, ainsi que le timbre qui définit l'autorisation d'émettre.

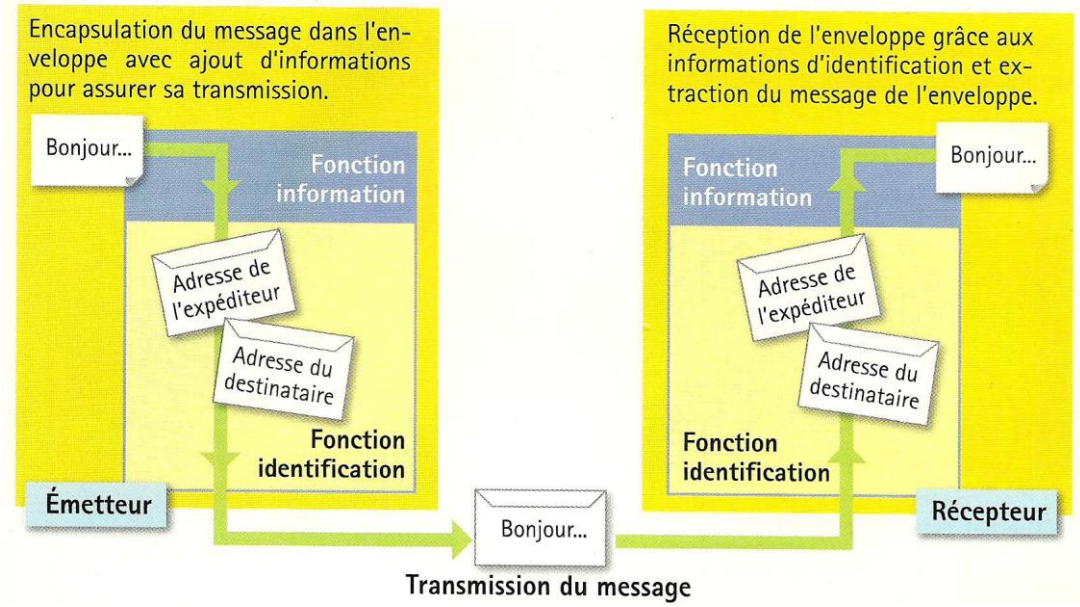


Fig.6 Encapsulation d'une donnée - Analogie avec l'envoi par la poste d'une lettre dans une enveloppe timbrée

L'information « adresse » ne concerne que la fonction d'identification du courrier, et n'a aucun rapport avec le message lui-même. En fait, chaque couche ne s'adresse qu'à son homologue chez le récepteur.

4 Modèle OSI (OPEN SYSTEMS INTERNCONNECTION) et le modèle TCP/IP

Le réseau doit permettre au système d'exploitation de gérer la transmission de données et de fournir aux applications des interfaces standards pour leur permettre d'exploiter les ressources du réseau : des PC sous Windows et des machines sous linux doivent pouvoir dialoguer ensemble. Pour arriver à cette interopérabilité, il faut que les divers protagonistes se mettent d'accord sur les fonctionnalités à implanter dans leurs applications et leurs fonctions réseau. C'est le rôle des normes. Le **modèle OSI (Open Systems Internconnection)** e été créé dans ce but. Il décrit l'architecture en sept couches logicielles présentant chacune des interfaces standards pour communiquer entre elles. Chaque couche à son tour, ajoute une information relative à l'un des aspects de la transmission.

Modèle OSI			
	Type de Donnée	Couche	Fonction
Couches Hôte	Donnée	7. Application	Point d'accès aux services réseaux
		6. Présentation	Gère l'encryptage et le décryptage des données, convertit les données en données exploitables par n'importe quelle machine
		5. Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment	4. Transport	Connexions bout à bout, connectabilité et contrôle de flux
Couches Matérielles	Paquet/Datagramme	3. Réseau	Détermine le parcours des données et l'adressage logique
	Trame	2. Liaison	Adressage physique
	Bit	1. Physique	Transmission des signaux sous forme binaire

Les 7 couches du modèle OSI

Ce modèle général tient compte de tous les cas de figure, mais la plupart des protocoles de communication l'ont adapté à leur besoin (nous verrons, par la suite, le protocole TCP/IP Transfert Control Protocol / Internet Protocol).

Ce mécanisme d'ajout d'information est appelé **encapsulation**. Chaque couche est spécialisée dans une tâche donnée et s'adresse à son homologue chez le récepteur qui sera le seul à pouvoir interpréter la commande. Une fois les informations destinées à une couche donnée prises en comptes, le reste du message est transmis vers la couche supérieure.

Fig.7 Modèle OSI – *Cas général (théorique)*

C'est à partir du cas général (fig.7) que sont déclinés tous les protocoles de communication.

Chaque couche est conçue de manière à dialoguer avec son homologue du poste distant. Chaque couche dialogue avec la couche juste au dessus et celle juste au dessous.

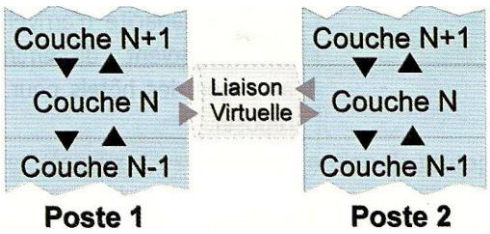


Fig.8 Modèle en couche

Les sept couches peuvent être regroupées en trois blocs fonctionnels :

- les couches 1, 2 et 3 assurent la transmission et l'acheminement des informations à travers le réseau.
- les couches 4 et 5 gèrent les communications et les ressources (processus et mémoire) nécessaires à l'échange des messages équipements terminaux (stations ou serveurs).
- les couches 6 et 7 traitent les données échangées (exécution de commandes, mise en forme).

L'encapsulation (fig.9)

C'est un mécanisme de transmission de données. Lorsqu'une application envoie des données vers le réseau, chaque couche traversée exécute un processus d'encapsulation de l'unité de données fournie par la couche supérieure en ajoutant un entête. Réciproquement à la réception, chaque couche exécutera une désencapsulation pour en final ne restituer que les données utilisateurs à l'application.

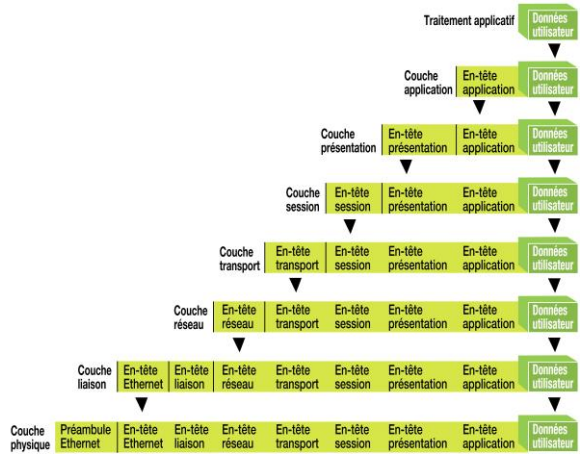
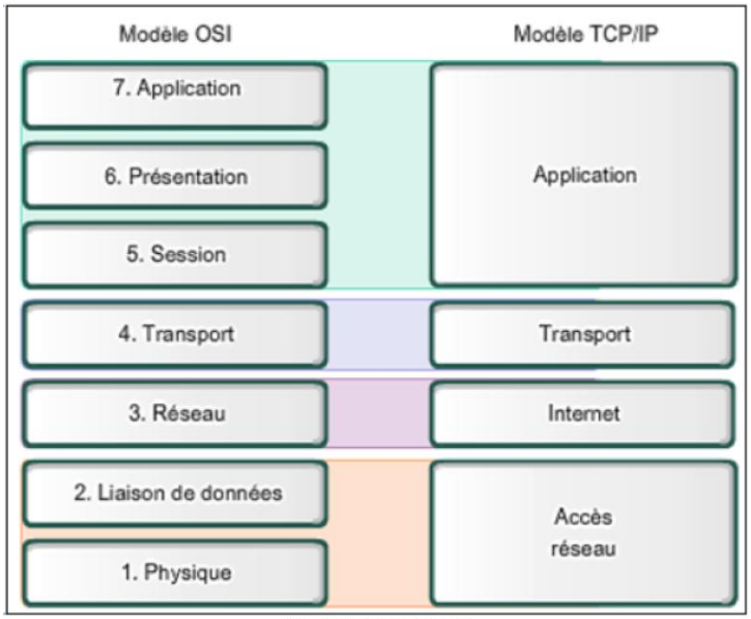


Fig.9 Mécanisme d'encapsulation

Le modèle TCP/IP (appelé aussi modèle Internet), qui date de 1976 a été stabilisé bien avant la publication du modèle OSI en 1984.

Il présente aussi une approche modulaire (utilisation de couches) mais en contient uniquement quatre :

1. Couche Physique
2. Couche Réseau
3. Couche Transport
4. Couche Services



Comparaison OSI - TCP/TP

Les protocoles qui constituent la suite de protocoles TCP/IP peuvent être décrits selon les termes du modèle de référence OSI. Dans le modèle OSI, la couche d'accès réseau et la couche application du modèle TCP/IP sont encore divisées pour décrire des fonctions discrètes qui doivent intervenir au niveau de ces couches.

Au niveau de la couche d'accès au réseau, la suite de protocoles TCP/IP ne spécifie pas quels protocoles utiliser lors de la transmission à travers un support physique ; elle décrit uniquement la remise depuis la couche Internet aux protocoles réseau physiques. Les couches OSI 1 et 2 traitent des procédures nécessaires à l'accès aux supports et des moyens physiques pour envoyer des données à travers un réseau.

Les principaux parallèles entre les deux modèles de réseau se situent aux couches 3 et 4 du modèle OSI. La couche 3 du modèle OSI, la couche réseau, est utilisée presque partout dans le monde pour traiter et documenter la plage des processus qui interviennent dans tous les réseaux de données afin d'adresser et d'acheminer des messages à travers un interréseau. Le protocole IP est le protocole de la suite TCP/IP qui contient la fonctionnalité décrite à la couche 3.

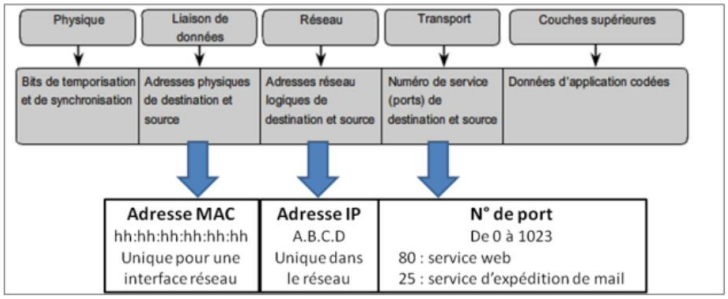
La couche 4, la couche transport du modèle OSI, sert souvent à décrire des services ou des fonctions générales qui gèrent des conversations individuelles entre des hôtes source et de destination. Ces fonctions incluent l'accusé de réception, la reprise sur erreur et le séquencement. À cette couche, les protocoles TCP/IP de contrôle de transmission et UDP fournissent les fonctionnalités nécessaires.

La couche application TCP/IP inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques à plusieurs applications d'utilisateur final. Les couches 5, 6 et 7 du modèle OSI sont utilisées en tant que références pour les développeurs et les éditeurs de logiciels d'application, afin de créer des produits qui doivent accéder aux réseaux pour des communications.

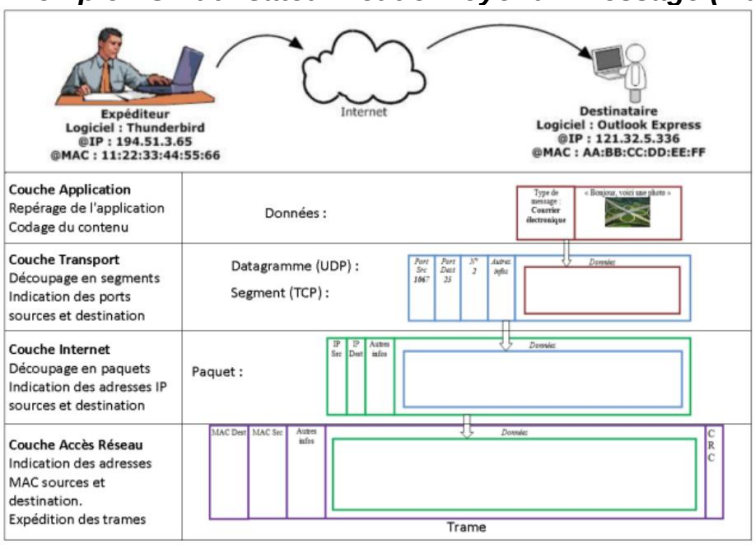
5 Principe de l'adressage et protocoles

Le modèle OSI décrit des processus de codage, de mise en forme, de segmentation et d'encapsulation de données pour la transmission sur le réseau. Un flux de données envoyé depuis une source vers une destination peut être divisé en parties et entrelacé avec des messages transmis depuis d'autres hôtes vers d'autres destinations. À n'importe quel moment, des milliards de ces parties d'informations se déplacent sur un réseau. Il est essentiel que chaque donnée contienne les informations d'identification suffisantes afin d'arriver à bonne destination.

Il existe plusieurs types d'adresses qui doivent être incluses pour livrer correctement les données depuis une application source exécutée sur un hôte à l'application de destination correcte exécutée sur un autre. En utilisant le modèle OSI comme guide, nous apercevons les différents identificateurs et adresses nécessaires à chaque couche.



Exemple : Un utilisateur veut envoyer un message (mail)



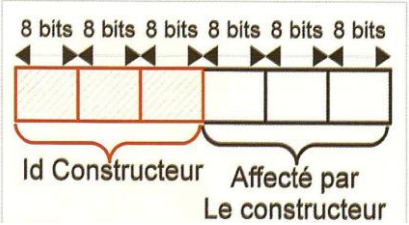
Exemple encapsulation

Lorsque des réseaux sont interconnectés, les quatre premières couches sont concernées. Pour chacune de ces couches, certains protocoles sont courants dans les réseaux locaux et sur internet.

5.1 Le protocole Ethernet

Ethernet est un protocole de réseau local qui concerne les couches 1 et 2 (prise en charge des couches physique et liaison). Il assure tous les mécanismes nécessaires à la transmission des trames sur un bus. Il propose :

- Plusieurs vitesses de transmission (10, 100, 1000 Mbit/s selon les possibilités du matériel).
- Une gestion d'écoute de bus, nommée CSMA/CD (carrier sense multiple access with collision detection) capable de détecter si celui-ci est libre avant d'émettre et de renvoyer une trame si plusieurs hôtes du réseau émettaient en même temps (collision).
- **Une adresse physique, appelée adresse MAC (média acces control)** unique au monde pour chaque coupleur utilisant ce protocole. L'adresse MAC est l'élément essentiel permettant d'identifier l'émetteur et le récepteur d'une trame réseau.
  La longueur de l'adresse MAC est de 48 bits soit 6 octets codés en hexadécimal (par exemple : 08 :00 :14 :57 :69 :69).
  L'adresse MAC identifie de manière unique un nœud dans le monde. Elle est physiquement liée au matériel (carte réseau).



Adresse MAC Ethernet

5.2 Le protocole IP

C'est un protocole de niveau réseau responsable de la transmission des données (datagrammes) en mode sans connexion. Il va établir l'adressage des datagrammes puis le routage des paquets entre réseau distinct se fera par l'intermédiaire de routeurs. Ce protocole est aussi responsable de la fragmentation des données.

6 L'adressage IP V4 et V6

Tous les périphériques appartenant à un même réseau doivent être identifiés de manière unique.

Bien que la majorité des adresses d'hôte IPv4 soient des **adresses publiques** utilisées dans les réseaux accessibles sur Internet, d'autres blocs d'adresses sont attribués à des réseaux locaux LAN (entreprises / maison) ces adresses sont appelées des **adresses privées**.

Une **adresse IP** (avec IP pour *Internet Protocol*) est un numéro d'identification qui est attribué à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. Il existe des adresses **IP de version 4 et de version 6**. La version 4 est actuellement la plus utilisée.

6.1 Les adresses IP V4

Une adresse Internet (IP) est composée d'une suite d'entiers soigneusement choisis pour assurer un routage efficace. L'adresse IP inclut l'identification du réseau (Net_id) ainsi que celle de la machine (Host_id) appartenant au réseau.

Chaque adresse IP est codée sur 32 bits (norme IPV4). La notation couramment utilisée pour représenter ces adresses est notation « décimale pointée » (avec quatre nombres compris entre 0 et 255, séparés par des points). Ce qui donne par exemple : 212.85.150.134.

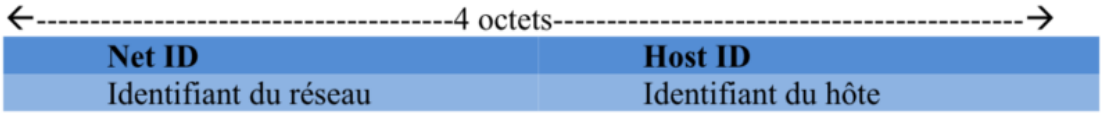
6.1.1 Attribution de l'adressage IP

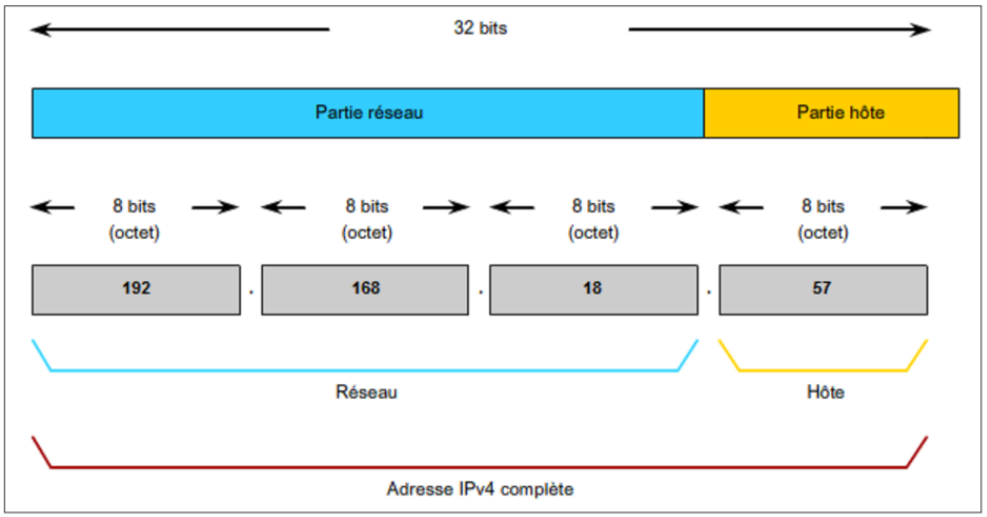
Les adresses IP peuvent être attribuées de **manière statique** (configuration manuelle de l'administrateur réseau) ou de **manière dynamique** (automatique via un service DHCP sur un serveur ou bien sur un box qui attribue de façon automatique les informations d'adressage : IP, masque, passerelle, …etc. Quand un pc se connecte au LAN).

6.1.2 Constitution de l'adressage IP

Toute adresse IP est composée de deux parties distinctes :

- Une partie nommée Identificateur (ID) du réseau : net-ID située à gauche, elle désigne le réseau contenant les ordinateurs.
- Une autre partie nommée identificateur de l'hôte : host-ID située à droite et désignant les ordinateurs de ce réseau.





Pour définir les parties réseau et hôte d'une adresse, les périphériques utilisent une configuration de 32 bits appelée « **masque de sous-réseau** ». Le masque de sous-réseau s'exprime dans le même format décimal pointé que celui de l'adresse IPv4. Le masque de sous-réseau est créé en plaçant le nombre binaire 1 dans chaque position de bit qui représente la partie réseau et en plaçant le nombre binaire 0 dans chaque position de bit qui représente la partie hôte.

6.1.3 le masque de sous réseau

Le système d'exploitation doit pouvoir distinguer, l'information désignant le sous-réseau de celle désignant la machine, afin de savoir si deux machines se trouvent sur le même sous-réseau.

Une adresse IP est en réalité constituée d'une **adresse réseau (Net_id) et d'une adresse de l'hôte (Host_id).** Chaque nœud sur un réseau représentant un hôte.

Un **masque de sous-réseau** (désigné par *subnet mask*, *netmask* ou *address mask* en anglais) est un masque indiquant le nombre de bits d'une adresse IPv4 utilisés pour identifier le sous-réseau, et le nombre de bits caractérisant les hôtes (ce qui indique aussi le nombre d'hôtes possibles dans ce sous-réseau).

Le masque de sous-réseau a le même format que l'adresse IP. Il peut servir à séparer localement deux sous-réseaux. Les bits à 1 désignent le sous-réseau et ceux à 0 le numéro de la machine (255_{10}=11111111_2). **Par défaut** on trouve :

- **pour la classe A : 255.0.0.0**
- **pour la classe B : 255.255.0.0**
- **pour la classe C : 255.255.255.0**

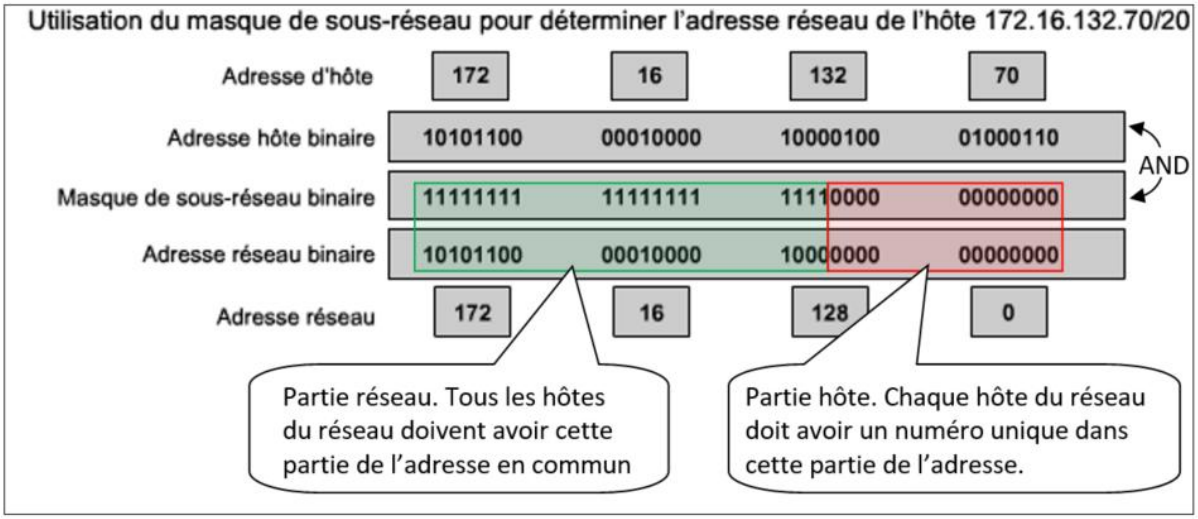
Une forme plus courte est connue sous le nom de « notation CIDR » (*Classless Inter-Domain Routing*). Elle donne le numéro du réseau suivi par une barre oblique (ou *slash*, « / ») et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par **/19** (19 bits à la valeur 1, suivis de 13 bits 0).

La notation 91.198.174.2/19 désigne donc l'adresse IP 91.198.174.2 avec le masque 255.255.224.0, et signifie que les 19 premiers bits de l'adresse sont dédiés à l'adresse du sous-réseau, et le reste à l'adresse de l'ordinateur hôte à l'intérieur du sous-réseau.

Deux adresses IP appartiennent à un même sous-réseau si elles ont en commun les bits du masque de sous-réseau.

6.1.4 Détermination de l'adresse de réseau à partir de l'adresse IP et du masque
Pour déterminer l'adresse du réseau auquel appartient un hôte, on effectue le masquage de son adresse IP par son masque de sous-réseau. Le masquage est obtenu en effectuant une opération AND bit à bit entre les deux adresses.

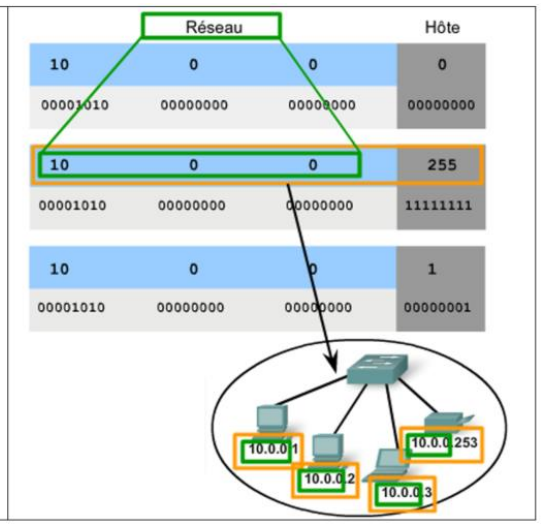
Exemple : Déterminer l'adresse de réseau de l'hôte 172.16.132.70/20



Conclusion : L'hôte **172.16.132.70/20** fait partie du réseau **172.16.128.0/20**

L'adresse de diffusion IPv4 est une adresse spécifique, attribuée à chaque réseau. Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau. Pour cela, un hôte peut envoyer un seul paquet adressé à l'adresse de diffusion du réseau.

L'adresse de diffusion correspond à la plus grande adresse de la plage d'adresses d'un réseau. Il s'agit de l'adresse dans laquelle les bits de la partie hôte sont tous des « 1 ».



6.1.4 Les anciennes classes réseau
Il existait **<u>5 classes d'adresses</u>**. Bien que cette façon de faire soit désormais obsolète (remplacée par le « cidr »).

Classe	Adresses
A	0.0.0.0 à 127.255.255.255
B	128.0.0.0 à 191.255.255.255
C	192.0.0.0 à 223.255.255.255
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

- **Limites de l'adressage par classe**

Les besoins de certaines entreprises ou organisations n'étaient pas toujours couverts par ces trois classes. L'attribution par classe des adresses IP gaspillait souvent de nombreuses adresses, ce qui épuisait la disponibilité des adresses IPv4. Par exemple, une entreprise avec un réseau de 260 hôtes devait se voir attribuer une adresse de classe B avec plus de 65 000 adresses.

Bien que ce système par classe ait été abandonné à la fin des années 90, il n'a pas entièrement disparu dans certains des réseaux modernes. Par exemple, lorsque vous attribuez une adresse IPv4 à un ordinateur, le système d'exploitation examine l'adresse en question pour déterminer si elle appartient à la classe A, B ou C. Le système d'exploitation devine ensuite le préfixe utilisé par cette classe et attribue le masque de sous-réseau correspondant.

6.1.5 Plages d'adresse IPv4 exclues de l'adressage des hôtes

Pour diverses raisons, certaines adresses ne peuvent pas être attribuées à des hôtes. D'autres le peuvent, mais avec des restrictions concernant la façon dont les hôtes interagissent avec le réseau.

- **Adresses réseau et de diffusion**
  La première et la dernière adresse ne peuvent pas être attribuées à des hôtes. Il s'agit respectivement de **l'adresse réseau** et de **l'adresse de diffusion**.
  Tous les bits de la partie Host-ID sont à 0 : **C'est l'adresse du réseau**
  Ex : 192.168.10.0 = 192.168.10.00000000
  Tous les bits de la partie Host-ID sont à 1 : **C'est l'adresse de diffusion (broadcast)** utilisée pour communiquer avec toutes les machines du réseau.
  Ex : 172.27.255.255 = 172.27.11111111.11111111 (attention c'est une écriture qui mélange la notation décimal pour les deux premiers octet et la notation binaire pour les deux derniers octets).

- **Route par défaut**
  0.0.0.0. Utilisé seulement pendant les phases d'initialisation (DHCP)

- **Bouclage**
  L'adresse de bouclage IPv4 127.0.0.1 est une autre adresse réservée. Il s'agit d'une adresse spéciale que les hôtes utilisent pour diriger le trafic vers eux-mêmes.
  Bien que seule l'adresse 127.0.0.1 soit utilisée, les adresses de la plage 127.0.0.0-127.255.255.255 sont réservées. Toutes les adresses de cette plage sont envoyées en boucle sur l'hôte local. Aucune des adresses de cette plage ne devrait jamais apparaître sur un réseau quel qu'il soit.

- **Adresses locales-liens**
  Les adresses IPv4 du bloc d'adresses 169.254.0.0 à 169.254.255.255 (169.254.0.0 /16) sont conçues pour être des adresses locales-liens. Elles peuvent être automatiquement attribuées à l'hôte local par le système d'exploitation, dans les environnements où aucune configuration IP n'est disponible. Celles-ci peuvent être utilisées dans un réseau Peer to peer de petite taille ou pour un hôte qui ne peut pas obtenir d'adresse automatiquement auprès d'un serveur DHCP.

- **Les adresses de multidiffusion**
  Les adresses de multidiffusion IPv4 du bloc 224.0.0.0 - 224.0.0.255 sont des adresses de liaison locales réservées. Ces adresses s'appliquent aux groupes de multidiffusion d'un réseau local.

- **Les adresses expérimentales**
  La plage d'adresses expérimentales IPv4 s'étend de 240.0.0.0 à 255.255.255.254. Actuellement, ces adresses sont répertoriées comme étant réservées pour une utilisation future. Cela laisse à penser qu'elles pourraient être converties en adresses utilisables. Pour l'instant, leur utilisation dans des réseaux IPv4 n'est pas permise. Toutefois, ces adresses pourraient s'appliquer à la recherche.

- **Les adresses publiques**
  Les adresses publiques sont routables sur internet et ne peuvent par conséquent pas être utilisées sur un réseau privé. Ces adresses étaient à l'origine réparties sur les trois classes de monodiffusion (A, B et C).

Finalement, Les seules adresses utilisables dans un réseau privé sont les suivantes :

- **10.0.0.0 à 10.255.255.255 (10.0.0.0 /8)**
- **172.16.0.0 à 172.31.255.255 (172.16.0.0 /12)**
- **192.168.0.0 à 192.168.255.255 (192.168.0.0 /16)**
-

6.1.5 Adresses publique : le modèle CIDR

La façon de faire précédant aboutit malheureusement à un formidable gaspillage d'adresses IP dans la mesure où, à la belle époque, une entreprise pouvait se voir attribuer une classe complète et n'en utiliser qu'une partie.

Le Classless Inter-Domain Routing (CIDR), est mis au point en 1996, la distinction entre les adresses de classe A, B ou C a été ainsi rendue obsolète, de sorte que la totalité de l'espace d'adressage unicast puisse être gérée comme une collection unique de sous-réseaux indépendamment de la notion de classe. Le masque de sous-réseau ne peut plus être déduit de l'adresse IP elle-même, les protocoles de routage compatibles avec CIDR, dits classless, doivent donc accompagner les adresses du masque correspondant.

Avec ce modèle (Classless Inter-Domain Routing), la notion de classe n'existe plus, si ce n'est pour les classes réservées à l'usage privé. Les adresses sont désormais distribuées par bloc, sans tenir compte de leur classe originelle.

L'IANA distribue donc désormais des blocs d'adresses contiguës, délimitées par un masque, toujours de 32 bits, dont les x bits de gauche sont à 1 et les autres à 0. Dans ce modèle, un bloc d'adresse se définit ainsi : adresse.de.base/x. Ainsi, pour notre exemple 192.168.25.0/255.255.255.0, on peut aussi écrire 192.168.25.0/24, car 24 bits sont significatifs de la partie réseau de l'adresse.

6.2 Les adresses IP V6

L'**adresse IPv6** est une adresse IP, dans la version 6 du protocole IP (IPv6). Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits pour IPv4.

IPv6 a été principalement développé en réponse à la demande d'adresses Internet qu'IPv4 ne permettait pas de contenter. En effet, le développement rapide d'Internet a conduit à la pénurie du nombre d'adresses IPv4 disponibles.

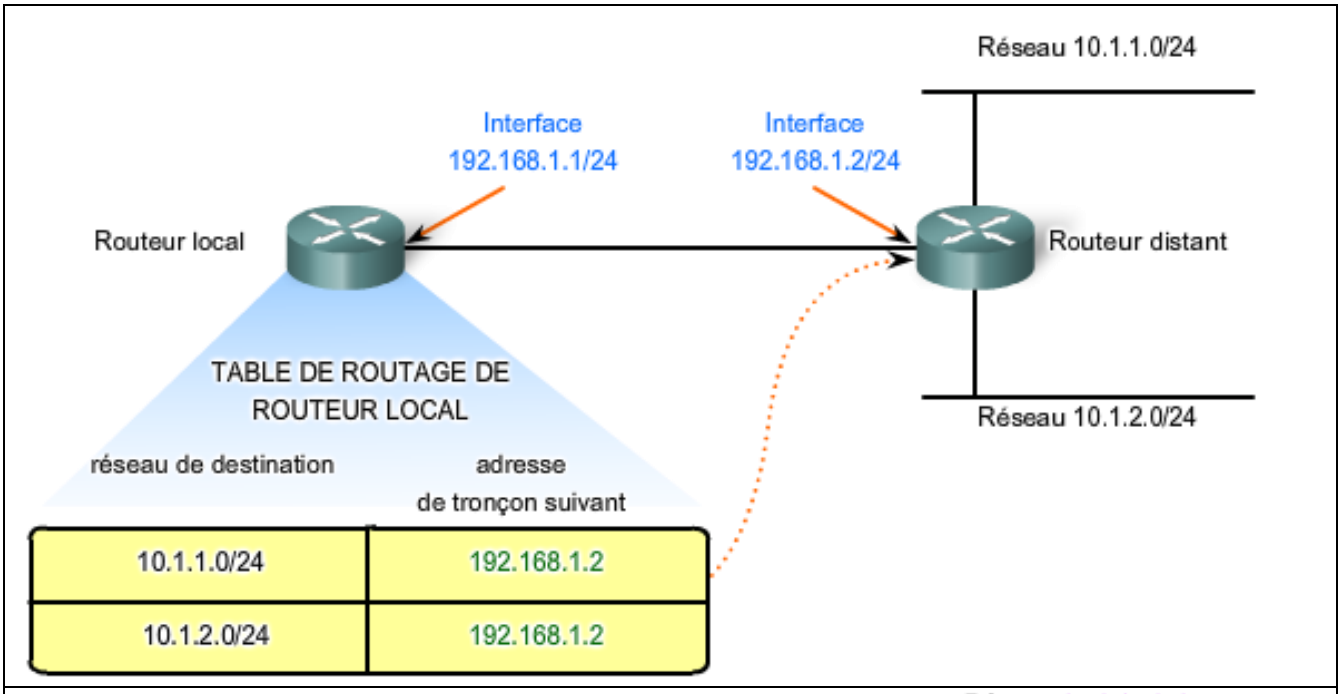
La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points :

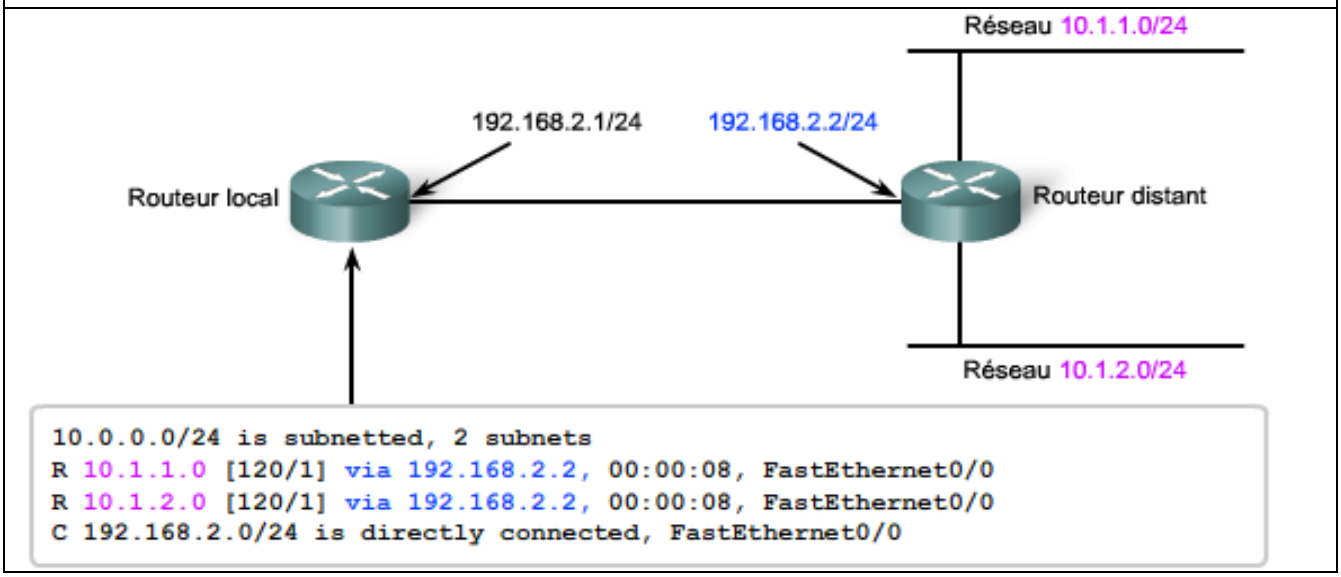
2001:0db8:0000:85a3:0000:0000:ac1f:8001

La notation complète ci-dessus comprend exactement 39 caractères (32+7 « deux points : »).

7 Principe du routage

Si l'hôte de destination se trouve sur le même réseau que l'hôte source, le paquet est acheminé entre les deux hôtes sur le support local sans nécessiter de routeur.
Cependant, si l'hôte de destination et l'hôte source ne se trouvent pas sur le même réseau, le réseau local achemine le paquet de la source vers son **routeur de passerelle**. Le routeur examine la partie réseau de l'adresse de destination du paquet et achemine le paquet à l'interface appropriée. Si le réseau de destination est connecté directement à ce routeur, le paquet est transféré directement vers cet hôte. Si le réseau de destination n'est pas connecté directement, le paquet est acheminé vers un second routeur qui constitue le routeur de tronçon suivant.
Le transfert du paquet devient alors la responsabilité de ce second routeur. De nombreux routeurs ou sauts tout au long du chemin peuvent traiter le paquet avant qu'il n'atteigne sa destination.
Aucun paquet ne peut être acheminé sans route. Que le paquet provienne d'un hôte ou qu'il soit acheminé par un routeur intermédiaire, le routeur a besoin d'une route pour savoir où l'acheminer. S'il n'existe aucune route vers un réseau de destination, le paquet ne peut pas être transféré. Les routeurs utilisent des tables de routage qui contiennent les routes qu'ils connaissent.



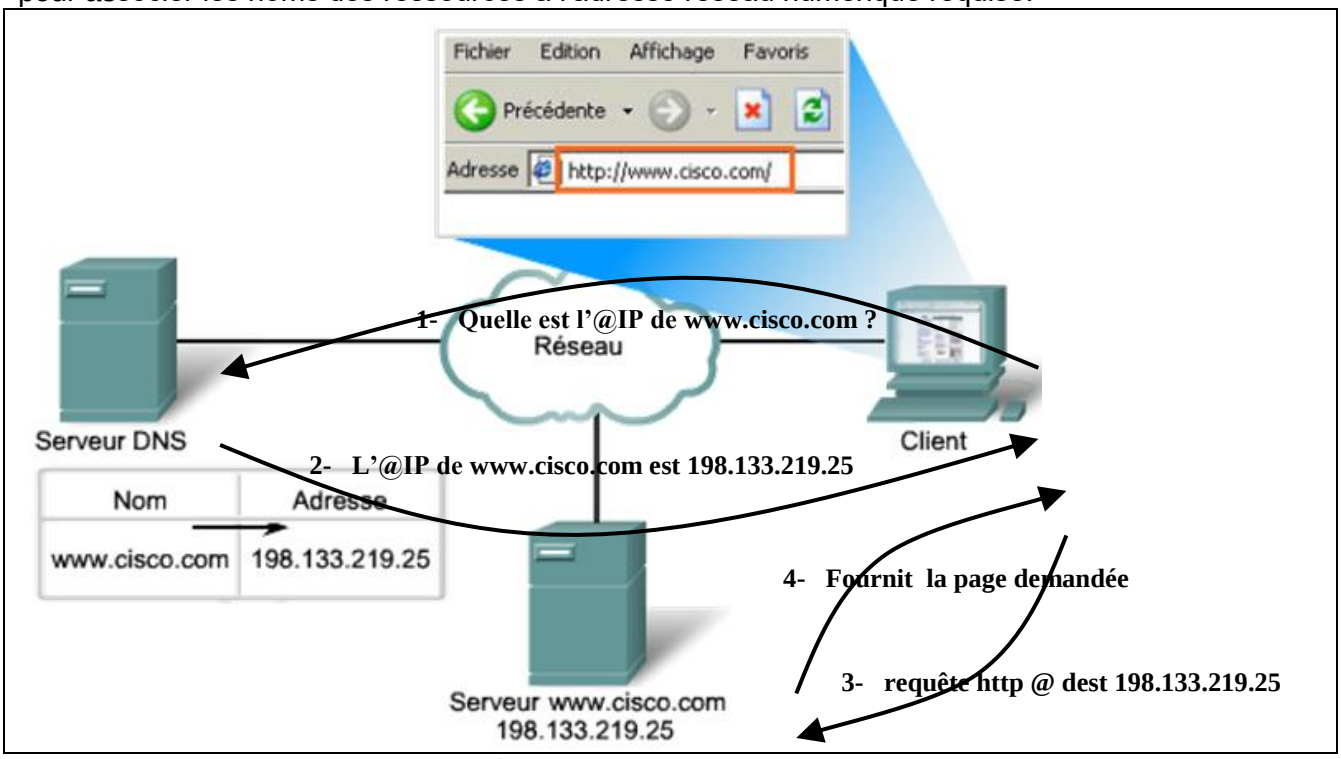


8 Principe du nommage – Service DNS (Domaine Name System)

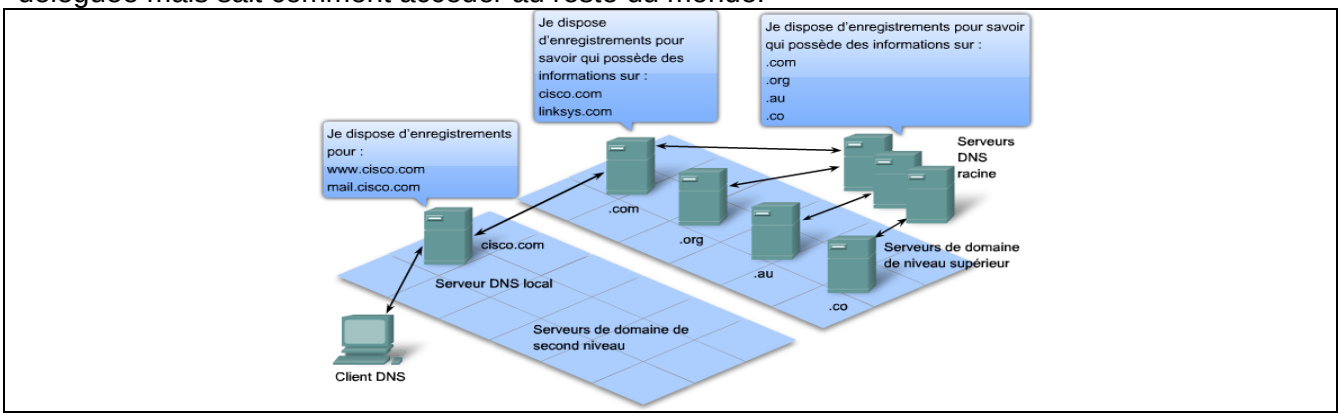
Sur les réseaux de données, les périphériques sont étiquetés par des adresses IP numériques, ce qui leur permet de participer à l'envoi et à la réception de messages via le réseau. Cependant, la plupart des utilisateurs mémorisent très difficilement ces adresses numériques. Pour cette raison, des noms de domaine ont été créés pour convertir les adresses numériques en noms simples et explicites.

Sur Internet, ces noms de domaine (par exemple, www.cisco.com) sont beaucoup plus faciles à mémoriser que leurs équivalents numériques (par exemple, 198.133.219.25, l'adresse numérique du serveur de Cisco). De plus, si Cisco décide de changer d'adresse numérique, ce changement est transparent pour l'utilisateur car le nom de domaine demeure www.cisco.com. La nouvelle adresse est simplement liée au nom de domaine existant et la connectivité est maintenue. Lorsque les réseaux étaient de petite taille, il était simple de maintenir le mappage entre les noms de domaine et les adresses qu'ils représentaient. Cependant, les réseaux étant aujourd'hui de plus grande taille et le nombre de périphériques plus élevé, ce système manuel ne fonctionne plus.

Le protocole DNS (Domain Name System) a été créé afin de permettre la résolution des adresses pour ces réseaux. Il utilise un ensemble distribué de serveurs qui assurent un service automatisé pour associer les noms des ressources à l'adresse réseau numérique requise.



Il est impossible de stocker les données DNS du monde entier sur une seule machine. C'est pour cela qu'on été mis en place les délégations : Chaque serveur ne connait que la zone qui lui a été déléguée mais sait comment accéder au reste du monde.



9 Principe d'adressage dynamique – Service DHCP (Dynamic Host Configuration Protocol)

Il permet d'allouer dynamiquement des adresses IP aux machines qui se connectent au réseau. Le but étant de simplifier l'administration réseau.

Un serveur DHCP ayant une adresse fixe va distribuer les adresses IP aux machines effectuant une requête DHCP.

10 Découverte du protocole ARP

Le protocole ARP (Adress Resolution Protocol) permet de trouver l'adresse MAC à partir d'une adresse IP.

Soit A et B deux ordinateurs sur le même réseau Ethernet. L'ordinateur A veut envoyer un datagramme IP à l'ordinateur B. A connait l'adresse IP de B, mais pas son adresse MAC pourtant absolument nécessaire à la couche physique pour construire la trame qui transportera le datagramme.

Le protocole ARP intervient alors pour trouver l'adresse MAC de B :

- il consulte son cache ARP pour savoir s'il ne dispose pas déjà de l'adresse physique de B.
- si ce n'est pas le cas, A envoie une trame de diffusion (broadcast) qui demande l'adresse Mac de B, en indiquant l'adresse IP de B. L'adresse MAC de destination est constituée que de bit à 1, ce qui donne en hexa : ff :ff :ff :ff :ff :ff.
- toutes les machines du réseau reçoivent la trame mais seul B répond à A en lui donnant son adresse MAC.
- A reçoit l'adresse Mac de B, la stocke dans sa table ARP (cache ARP) et l'utilise pour construire sa trame Ethernet.