INF 309 : Introduction aux réseaux

L'objectif général de ce cours est de prodiguer aux étudiants les connaissances de base sur les réseaux informatiques. L'architecture, les modèles, les fonctions, et les composants de l'Internet et des réseaux d'ordinateurs en général sont décrites. Les principes et la structure de l'adressage IP, les concepts fondamentaux d'Ethernet et WIFI, les supports utilisés, et les opérations mis en œuvres sont présentés.

A la fin de ce cours l'étudiant doit être capable de :

- ✓ Présenter les modèles de communication réseau en couche OSI et TCP/IP et les concepts mis en œuvre dans chaque couche de ces modèles.
- ✓ Comprendre et décrire les composants et services utilisés pour permettre la communication dans un réseau de données et l'Internet.
- ✓ Comprendre et décrire l'importance de l'adressage et d'un schéma de nommage à différentes couches d'un réseau aussi bien dans les environnements IPv4 qu'IPv6.
- ✓ Concevoir, calculer et appliquer des masques et adresses de sous-réseau en fonction d'un certain nombre d'exigence.
- ✓ Expliquer les fondamentaux de la technologie Ethernet (IEEE802.3) et sans fil (IEEE802.11) supports de transmission, services et opérations.
- ✓ Comprendre et décrire le principe de routage dynamique et statique.
- ✓ Concevoir un réseau local à base d'Ethernet et WIFI en se servant de routeur et commutateur.
- ✓ Fait usage des utilitaires réseaux pour vérifier le fonctionnement d'un réseau, analyser le trafic et le dépanner au besoin.

Profil : Etudiant L3 informatique.
Nombre de crédit : 5cr
Nombre d'heure : CM = 30; TD = 30; TP =30.
Evaluation : CC 20% ; TP 30% ; EE 50%
Période : Jeudi 9h45 – 11h45 AIII (cours magistral), Vendredi 13h30 – 15h30 S06 (TD G1) et 15h30 – 17h30 S06 (TD G2)

Programme

I. Généralités
II. Modèle OSI (Approche top – down)
1. Introduction (Pourquoi un modèle)
2. Couches applicatives
3. Couche Transport
4. Couche Réseau

5. Couche Liaison de données
6. Couche Physique

III. Conception des réseaux locaux

1. Technologie Ethernet
2. Système d'adressage IP
3. Notion de routage et transfert des paquets
4. Réseau locaux sans fils

IV. Ateliers pratiques et étude de cas.

1. Configuration de base des commutateurs.
2. Configuration de base des routeurs
3. Mise en place d'un réseau local

Bibliographie :

1. Les réseaux. Guy Pujolle, Edition 2008 – **Eyrolles**.
2. Réseaux. Andrew Tanenbaum, 4è Edition – **Pearson Education**.
3. Technologie des ordinateurs et des réseaux. Alain Goupille (cours et exercices corrigés), 6è Edition – **DUNOD**.
4. Réseaux informatiques : Notions fondamentales (Normes, architectures, modèle OSI, TCP/IP, WI-FI, …). Philippe Atelin, 3è Edition – **ENI Editions**.
5. Cisco Press – CCNA Exploration v4.1

1- Généralités

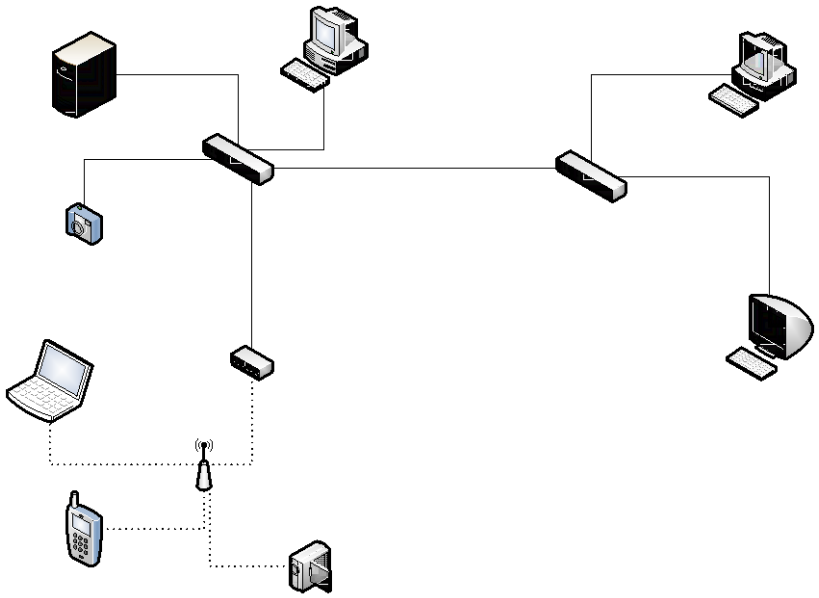
1. Origines et évolution des réseaux informatiques

Les réseaux informatiques sont aujourd'hui répandus partout, et font partie intégrante de la vie quotidienne des Hommes. Cette généralisation de l'utilisation des réseaux a bouleversé les habitudes et la façon dont nous communiquons, achetons, travaillons, étudions, nous amusons, etc. La naissance et le développement des réseaux informatiques dates du début des années 70 avec les nombreux projets du DoD, dont l'objectif était de connecter les ordinateurs devenu autonomes. Les informations (sous formes numériques) sont transportées d'un point à l'autre (équipements finaux/terminal) du système d'information à l'aide de supports (média) de toutes sortes et suivant des règles bien établies (protocoles). A ces débuts les plateformes matérielles et les méthodes de transmission différaient d'un constructeur à l'autre (incompatibilité), il a fallu développer des règles (protocoles) et standards (normes) pour permettre à des équipements quelconques (constructeurs) d'échanger à travers l'infrastructure réseau.

2. Organisation des réseaux

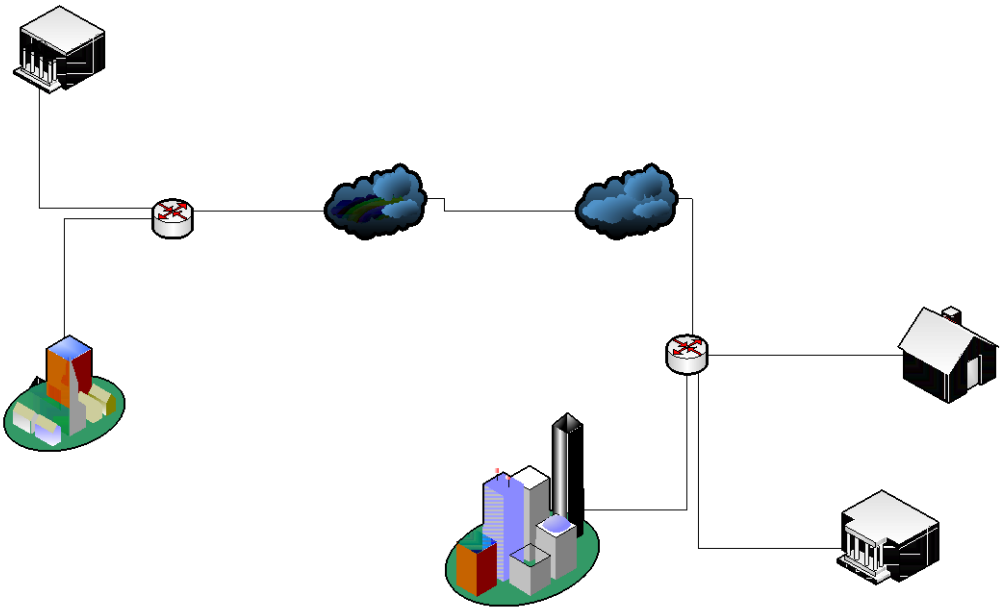
Les réseaux informatiques se différencient selon le type et la topologie. Le type fait principalement référence à l'étendu du réseau, ainsi on distingue les réseaux

locaux dont l'étendue est réduite à un environnement géographique restreint (salle, un bâtiment). On appelle encore ce type de réseau LAN (*Local Area Network*).



Réseau Local

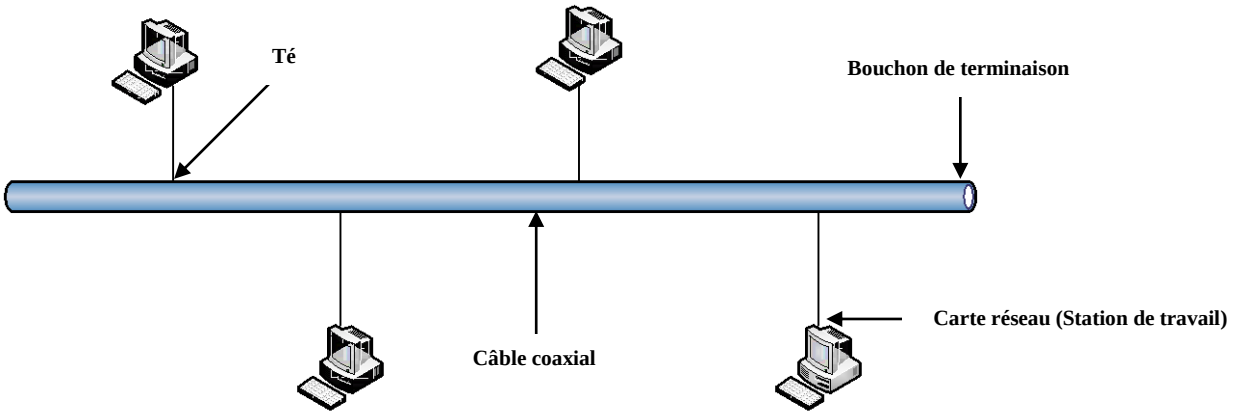
Lorsqu'il s'agit de transporter les informations et signaux à de grandes distances on a des réseaux grandes distances ou WAN (*Wide Area Network*). Dans un réseau local la brique de base est constituée des stations de travail (machine, serveur, imprimantes) tandis que dans un réseau grande distance elle est constituée de réseaux locaux.
NB : A l'intermédiaire (entre réseau local et réseau grande distance) on a généralement des réseaux métropolitains qui s'étendent à l'échelle d'une ville (quelques centaines de km). Ils sont encore appelés MAN (*Metropolitan Area Network*).



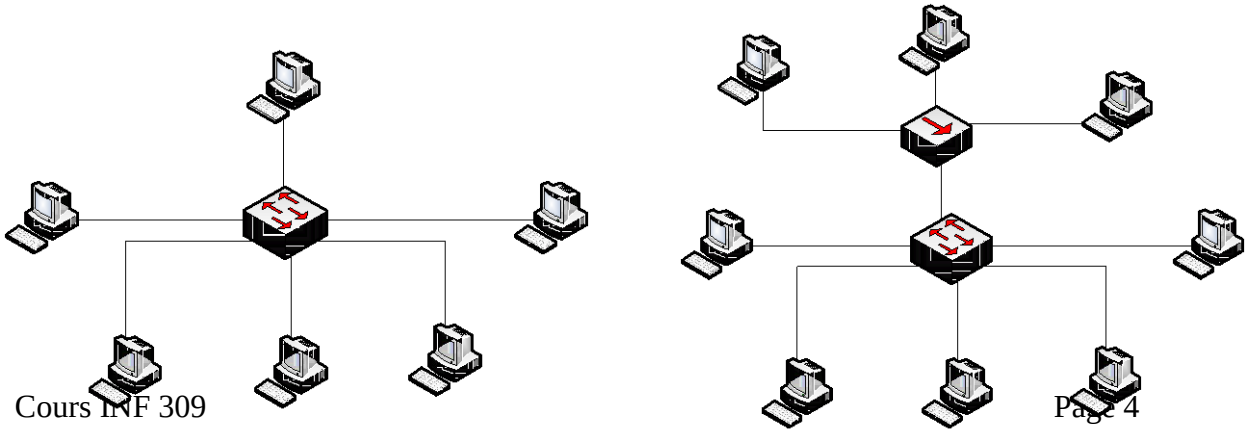
Réseau grande distance

La topologie d'un réseau fait référence à l'organisation des composants du réseau. Ainsi on distingue les topologies en bus, en étoile (et étoile étendue), en anneau, en maille, etc.

a. **Topologie en bus :** tous les équipements sont connectés le long d'une tige principale, qui sert de conducteur de l'information. Cette topologie a été utilisé pour l'architecture des premiers réseaux faisant usage du câble coaxial comme média de transmission : 10 base 5 (câble coaxial épais ou thicknet) et 10 base 2 (câble coaxial fin ou thinnet). Le débit maximal de transmission dans ces réseaux était de 10Mbits/s et la distance maximale entre deux extrémités de câble est de 500m (thicknet), 185m (thinnet).

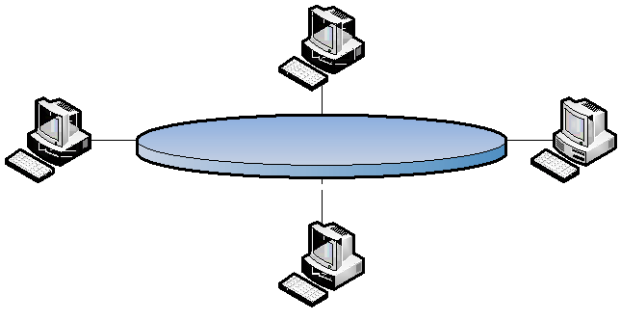


b. **Topologie en étoile :** les équipements sont organisés autour d'un nœud central qui est un équipement spécialisé. C'est la topologie la plus utilisé de nos jours dans les réseaux locaux. L'équipement spécialisé est un commutateur (switch) ou un concentrateur (hub). L'étoile étendue est une variante de cette topologie où l'on cascade des commutateurs ou des concentrateurs entre eux.

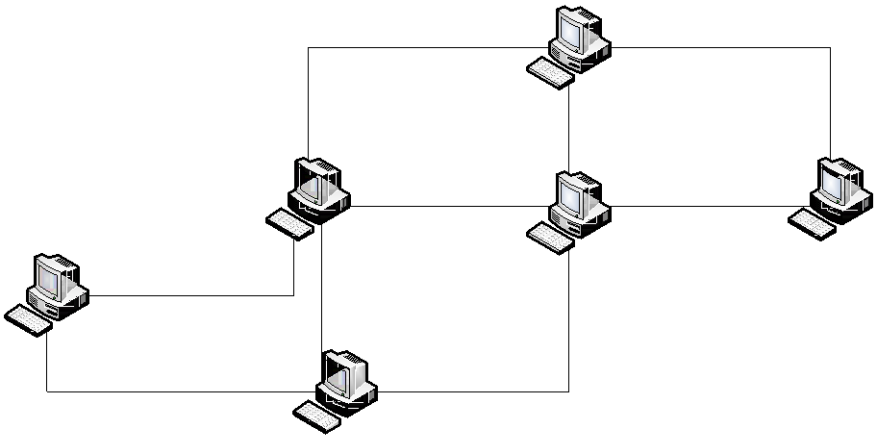


Réseau en étoile **Réseau en étoile étendue**

c. **Topologie en anneau :** les équipements sont organisés autour d'un anneau physique. L'information circule dans un sens bien déterminé (d'un nœud à l'autre), tout nœud ne transmettant l'information que lorsqu'il s'agit de son tour. Le réseau Token Ring utilise cette topologie. Une variante de celle-ci est le double anneau : le réseau FDDI en est un exemple.



d. **Topologie maillée :** Dans cette topologie, les nœuds sont connectés les uns aux autres dans une structure évoquant une toile d'araignée. La maille peut être partielle ou complète. Les réseaux WAN (en particulier Internet) sont construits suivant cette topologie.



NB : Toutes ces topologies sont des topologies physiques et concerne la façon dont les nœuds sont connectés physiquement. Il existe un autre type de topologie qui concerne la façon dont l'information est échangée (topologie logique). **Cf.** : Partage de jeton ou accès aléatoire (contention). La première utilise des algorithmes déterministe en tandis que dans la seconde l'accès au médium est non déterministe.

3. **Quelques caractéristiques des architectures réseaux :**

L'un des principaux objectifs lors de la mise en œuvre d'une infrastructure réseau est d'assurer la transmission des informations à tout moment, et n'importe où. De plus, il doit offrir une large gamme d'applications et services variées (navigation, messagerie instantanée, transfert de fichier de toute sorte, vidéo à la demande, voix sur IP (*VoIP)*, outils de collaboration, réseau sociaux, etc.). Pour garantir une plateforme fonctionnelle offrant toutes ces possibilités et répondre aux attentes des utilisateurs finaux, quatre principales caractéristiques doivent être prise en compte lors de la conception/planification du réseau : tolérance aux pannes, évolutivité (*scalability*), qualité de service (QoS) et sécurité.

a. **Tolérance aux pannes**

Un réseau est tolérant aux pannes s'il limite l'impact des pannes (matérielles ou logicielles) et peut être rétabli rapidement lorsque celle-ci surviennent. Des exemples de mécanismes mis en œuvre dans les réseaux pour assurer cette propriété et la redondance (équipement et services) et l'utilisation de chemins multiples. Exemple de réseau tolérant aux pannes : réseau téléphonique, réseau Internet.

b. **Evolutivité**

Un réseau évolutif (qui passe à l'échelle) est un réseau extensible, c'est-à-dire qu'il peut prendre en compte de nouveaux utilisateurs et service sans que ceci n'affecte *gravement* les performances du réseau. Pour offrir cette possibilité, la conception des architectures réseaux sont généralement basée sur une organisation hiérarchique. Exemple de réseau évolutif : Internet. Chaque jour de milliers de nouveaux utilisateurs et fournisseurs de service se connecte à ce réseau sans ce que ceci n'impacte les performances des services et des utilisateurs existants.

c. **Qualité de service**

Même si le réseau est tolérant aux pannes et passe à l'échelle, la prise en compte d'application exigeant des performances et niveau de services différents peut être compromise par l'ajout de nouvelles applications. Celles ci rajoutent des délais supplémentaires dans le traitement des demandes des utilisateurs ou des services. Des exemples de service ou applications exigeant en qualité de service les transmissions audio (*VoIP*) et vidéo (streaming) qui nécessite un débit constant, et qui lorsque cette constante n'est pas assurée, dégrade la qualité de la transmission. Pour garantir cette propriété, les réseaux doivent fournir des services prévisibles, mesurables et parfois garantis. Une architecture réseau capable de transporter à la fois des données, du son et de la vidéo est appelée ***réseau convergeant***. Dans ce type de réseau la QoS est mise en œuvre par des techniques de gestion de trafic avancées telles que la classification et la « *prioritisation* » (attribution des priorités) du trafic.

d. **Sécurité**

Les réseaux étant aujourd'hui ouvert et accessible par tous, la nécessité de protéger les informations confidentielles contre toute forme d'intrusion ou d'utilisation illicite. Des techniques de chiffrement (cryptographie) permettent d'assurer la confidentialité de l'information, tandis que les techniques d'authentification assurent l'accès sécurisé aux ressources. L'intégrité de l'information est quand à elle mise en œuvre par des techniques et fonction de hachage.

2- Modèle OSI : Approche Top - Down

1. Introduction : Pourquoi un modèle [en couches] :

Tout comme l'on procède avec les algorithmes (décomposition en bloc logiques moins complexe) pour la résolution des problèmes, le réseau est un système complexe intégrant de nombreuses entités (équipements, protocoles, constructeurs, supports de transmissions, messages échangés, etc.) et nécessite une décomposition pour mieux cerner les interactions entre tous ces éléments. Dans le monde des réseaux cette décomposition utilise la notion de couches. Chaque couche regroupe un ensemble de processus et protocoles qui assurent la fonction de cette dernière et définit l'interface de communication avec les couches voisines (celle de dessous et celle de dessus). Ces couches sont superposées les unes sur les autres sous forme d'un pile. Elles constituent juste un modèle pour décrire et mieux comprendre les mécanismes qui interviennent dans la conception d'un réseau.

Les avantages d'une utilisation d'un modèle en couches sont nombreux :

- Facilite de développement de nouveaux protocoles
- Encourage une concurrence « saine » entre les constructeurs d'équipements réseaux
- Assure une indépendance de l'évolution d'une technologie (d'une couche) vis-à-vis des autres couches

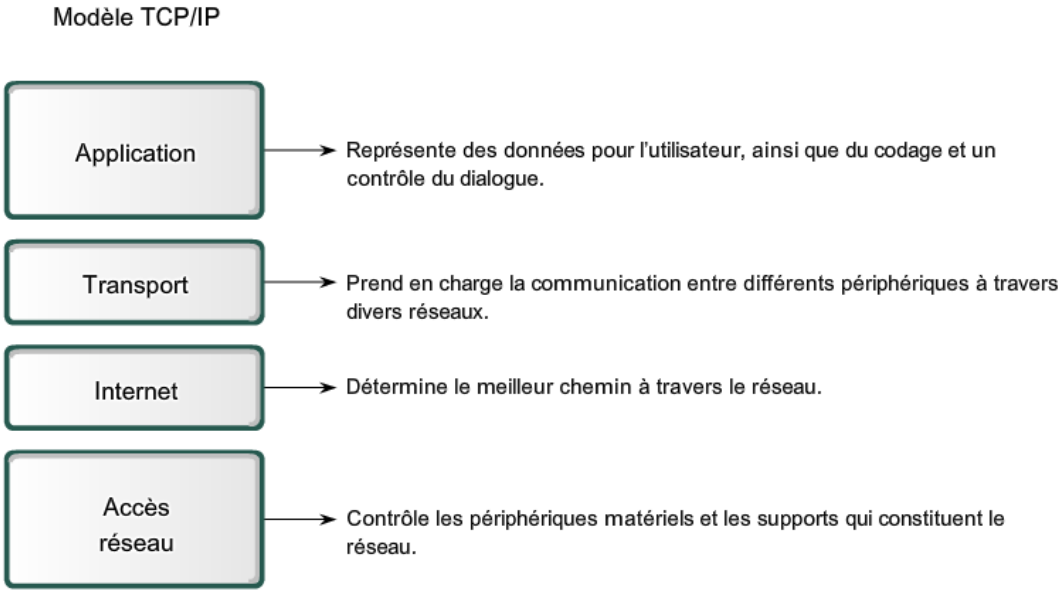
Il existe deux types de modèles en couches généralement utilisés pour décrire le réseau : le modèle OSI et le modèle TCP/IP.

a. Le modèle OSI (Open Systems Interconnection)

Il s'agit encore du modèle dit « de référence », il a été proposé par l'organise de normalisation ISO (International Standard Organization) dans le but de permettre la conception des protocoles pour les systèmes ouverts. Il n'est pas destiné à une implémentation spécifique mais plutôt de permettre une compréhension claire des fonctions et processus impliqués dans le réseau. Ce modèle est constitué de 7 couches comme illustré par la figure ci-contre :

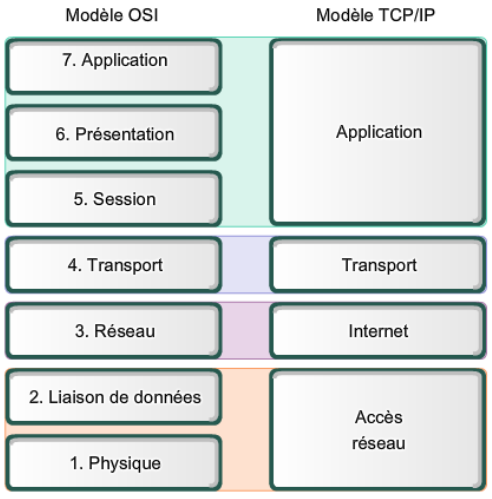
b. <u>Le modèle TCP/IP</u> (Transmission Control Protocol/Internet Protocol)

C'est un modèle de protocole sur lequel repose la conception/implémentation d'Internet. Il reste également ouvert et n'est contrôlé par aucun organisme. Les normes sont pour la plupart publié par l'IETF (Internet Engineering Task Force) sous forme de document RFC (Request For Comments). Ces documents décrivent les protocoles et spécification formelle et technique pour leur fonctionnement. Ce modèle est repose sur quatre couches, illustrées ci-dessous :



c. <u>Regard croisé des deux piles de protocoles</u>

Il existe une certaine correspondance (illustrée par la figure) entre les couches du modèle TCP/IP et celles du modèle OSI. Les couches du modèle OSI sont généralement référencées par leur numéro (Ex : couche 3 pour désigner la couche réseau) tandis que celle du modèle TCP/IP le sont par leur nom.



Les principaux parallèles concernent les couches transport et réseau.

Chaque couche est caractérisée par un certain nombre de paramètres :

- ✓ Les protocoles utilisés à cette couche,
- ✓ Les équipements mettant en œuvre ces protocoles,
- ✓ L'unité de données (en anglais PDU : Protocol Data Unit) utilisée au niveau de cette couche,
- ✓ L'adressage utilisé au niveau de cette couche.

Ainsi en considérant le modèle OSI ont rencontre au fur et à mesure que l'on descend dans les couches :

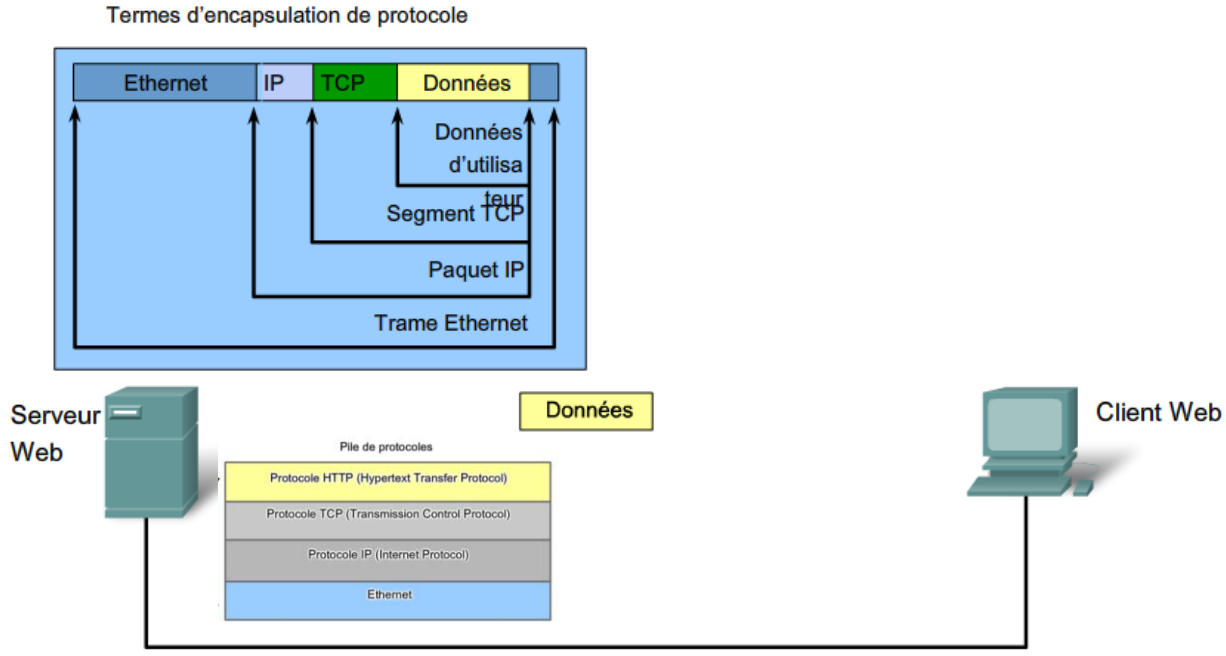
- Couche 7 : le PDU = Donnée
- Couche 4 : le PDU = Segment (informations d'adressage numéro de port)
- Couche 3 : le PDU = Paquet (informations d'adressage adresse IP ou adressage logique)
- Couche 2 : le PDU = Trame (informations d'adressage : l'adresse physique [@MAC dans le cas d'Ethernet])
- Couche 1 : le PDU = suite de bits.

NB :

d. Le processus qui consiste à ajouter les informations dans un PDU avant de le transmettre à la couche inférieure s'appelle **encapsulation.** Le processus inverse se déroule au niveau du périphérique cible (**décapsulation**).

e. Le processus de communication entre un équipement source et une cible se réalise toujours entre couches homologues.

Illustration : Echange de donnée entre un serveur et un client Web.



TD – TP N° 1 : (Deux groupes ce Vendredi 03 Mai 13h30 – 15h30 et 15h30 – 17h30 S006)

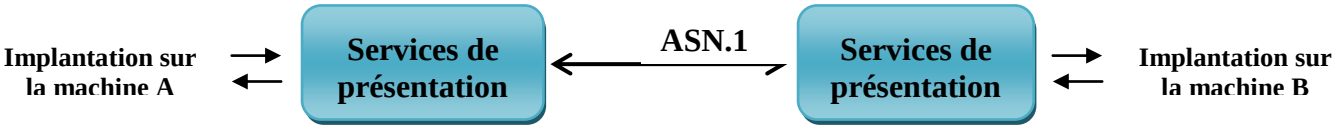
- Utilisation du simulateur de réseau Packet Tracert (6.0)
  - Installation
  - Familiarisation avec l'interface
  - Ajout d'équipement, retrait, mode réel, mode simulation
  - Mise en œuvre d'un réseau simple client – serveur (web).
  - Dérouler la pile de protocole en mode simulation
  - Réaliser des tests simples (ping, traceroute).
- Interaction client/serveur (http, DNS, FTP, etc.)
- Utilisation d'un analyseur de protocole (wireshark) pour capturer en live les paquets qui circule dans le réseau et visualiser la pile protocolaire.

2. Couches applicatives

Dans cette section il s'agit de la couche application tel que dans le modèle TCP/IP et intègre donc les trois couches supérieures du modèle OSI (session, présentation et application).

La couche session fournit des services à la couche présentation et gère les dialogues, l'ouverture et la fermeture des sessions entres les entres services et utilisateurs. Une session est une connexion logiques entre deux entités nécessitant une synchronisation et regroupe un ensemble d'activités ou transactions. Les outils utilisés à ce niveau peuvent intégrer RPC, CORBA, SQL, etc.

La couche présentation assure la cohérence de représentation de l'information entre les différentes architectures matérielles du réseau (hétérogènes). Elle va donc gérer les services de codage, de cryptage et de compression de données. La convention/langage de représentation de donnée indépendante de toute architecture matérielle généralement utilisé est le codage ASN.1 (Abstract Syntax Notation One).



La couche application intègre les services et programmes utilisateurs : ces services sont mis en œuvre par des protocoles tels que : HTTP (service www) ; FTP, TFTP (transfert de fichier) ; SMTP, POP3 (messagerie électronique) ; DHCP ; DNS ; Telnet, ssh (terminal distant) ; etc. Ces services constituent l'interface entre le réseau et l'utilisateur humain et sont généralement intuitifs c'est-à-dire que nous les utilisons très souvent sans savoir comment ils fonctionnent, cependant un professionnel de réseau doit en connaitre les mécanismes sous jacent. La plupart de ces protocoles fonctionnent en mode client/serveur. La connexion est dans ce cas toujours initiée par le client, toutefois le serveur est toujours en écoute en attentes

des demandes d'éventuels clients. Ces protocoles définissent le type de message échangés entre les parties, leurs formats, la syntaxe des commandes et les erreurs qui surviennent.

a. Service www et protocole http

Ce service permet de localiser et d'accéder aux ressources web (sous forme de document html intégrant des liens hypertexte). Pour être identifié n'importe où dans le monde ces ressources web utilisent une adresse : URL (Uniform Ressource Locator) dans laquelle on retrouve : le protocole, le domaine et l'emplacement dans le serveur de la ressource. **Exemple** : http://www.netcomuting.com/access/index.html

Le protocole http spécifie comment sont échangé les messages entre le client web (qui est un navigateur) et le serveur web (apache par exemple). Le serveur dispose d'un répertoire dans lequel se trouve les pages web qu'il met à disposition des clients. Une fois la page transférée (copie) au client celui-ci interprète le code HTML qui y est contenu et le présente à l'utilisateur final.

b. Service de transfert de fichier

Il existe deux protocoles couramment utilisés pour le transfert de fichiers (binaire et autres types) entre un client et un serveur : FTP et TFTP. Le premier nécessite un service de livraison fiable (cf. prochaine section) comme TCP tandis que le second s'appuie sur UDP pour cette livraison. TFTP est surtout utilisé dans un environnement à priori stable (moins sujet aux erreurs de transmission) et permet la mise à jour du SE des équipements réseaux ou la copie des fichiers de configurations.

c. Service de messagerie

C'est un service de plus en plus répandu dans la communauté Internet de par sa simplicité. Il utilise principalement deux protocoles pour fonctionner :

- SMTP : utilisé par l'agent de messagerie pour envoyer les messages vers le serveur.
- POP : utilisé pour la réception des messages du serveur de messagerie vers le client.

d. Service DNS (Domain Name System)

Les protocoles réseaux utilisent des adresses IP pour identifier les différents hôtes du réseau, ces identifiants sont moins communs aux humains. Le protocole DNS a été proposé dans le but d'offrir un système de nommage plus familier et proche du langage et interface humain qui soit facile à mémoriser. Dans ce système un serveur stocke les correspondances nom – adresse IP et effectue les conversions sollicitées par des clients. Ce processus de conversion est transparent pour l'utilisateur final, qui n'a pas conscience de celui-ci.

Lors de la configuration d'un hôte réseau très souvent au moins un serveur DNS doit être spécifié, pour cette résolution de nom. Ce protocole fonctionne de manière hiérarchique : lorsqu'un serveur est incapable de résoudre un nom il sollicite d'autres serveurs DNS, qui à leur tour peuvent en solliciter d'autres (chaque serveur étant spécialisé pour un domaine de nom précis).

Exemple de domaine de premier niveau : .com, .cm, .fr, .jp, .org, .gouv etc.
La commande ***nslookup*** permet de résoudre en ligne de commande un nom et fournit en résultat l'adresse IP correspondante et le serveur DNS utilisé pour cette réponse.

e. Service DHCP

Il est utilisé pour permettre aux stations du réseau d'obtenir de façon automatique leurs paramètres de configuration (adresse IP, masque, passerelle, serveurs DNS, etc.) Ceci permet

de diminuer la charge administrative dans les réseaux disposant de plusieurs hôtes ou dont les utilisateurs sont très mobiles. Les paramètres sont en général loués aux hôtes pour une durée donnée appelé **bail.** Le service peut être localisé dans une machine dédiée ou un équipement intermédiaire comme un routeur.

Malgré sa praticité il peut représenter un risque à la sécurité du réseau. Attention certains équipements du réseau (serveurs, routeurs, commutateurs, etc.) ont besoin des paramètres de configuration IP fixes et connus à tout moment par les autres hôtes du réseau. DHCP fonctionne suivant quatre phases :

- DHCP DISCOVER : émis en diffusion (broadcast) par le client pour solliciter un serveur.
- DHCP OFFER : Réponse du serveur au client.
- DHCP REQUEST : Sélection par le client des paramètres d'un serveur (si plusieurs réponses).
- DHCP ACKNOWLEDGE : Confirmation de la transaction par le serveur.

f. Service de connexion à distance

Il permet d'émuler un terminal distant ceci permettant de configurer un équipement réseau à distance à l'aide de la ligne de commande (CLI) comme si l'on y était physiquement. Contrairement à Telnet qui transporte les messages en clair entre le client et le serveur, ssh utilise un mécanisme de chiffrement pour encrypter les informations de configuration. Ce dernier doit obligatoirement être utilisé dans tout système où la sécurité est un souci majeur.

3. Couche Transport

Elle se place entre les couches basses (1 à 3) et les couche hautes (5 à 7) du modèle OSI. Elle est chargée de fournir les services de livraison d'informations aux couches supérieures, en donnant la possibilité à plusieurs processus clients s'exécutant sur la même machine de communiqué en même temps avec un ou plusieurs serveurs. Pour ce faire elle s'appuie sur deux protocoles TCP et UDP. En fonction du niveau de fiabilité requis cette livraison peut être orienté connexion (TCP) ou non orienté connexion (UDP). D'autres mécanismes mis en œuvre dans cette couche sont la segmentation, l'adressage et la négociation du flux d'information.

a. Fonction de la couche transport :

- **Segmentation des données :** Elle est chargée de découper les données provenant des couches applicatives pour maximiser l'utilisation du canal de communication. Cette fonction est couplée avec le multiplexage des flux de communication. Elle utilise pour ce faire un champ dans l'en-tête du PDU de cette couche : le numéro de séquence (d'ordre) qui l'aide dans la reconstitution du message originel au niveau de l'équipement de réception.

- **Identification des applications :** Le flux d'information reçu dans cette couche peut provenir de diverses application de la couche 7, pour différencier ces application, la couche transport utilise un autre champ d'en-tête : le numéro de port. Ainsi chaque application répertorié se voit attribué un numéro d'identification unique. Ce numéro fonctionne en doublon : un qui identifie

l'application sur la machine émettrice (port source) l'autre sur la machine destinatrice (port de destination). L'IANA (Internet Assigned Numbers Authority) est chargé de contrôler l'attribution de ces identifiants. On distingue trois blocs d'identifiant :

- Numéro de port réservé : 0 à 1023. Utilisé par les services bien connus, généralement côté serveur de la communication.
  Ex : HTTP (80), FTP (20 et 21), SMTP (25), Telnet (23) DNS (53), HTTPS (443), TFTP (69), SNMP (161), DHCP (49) etc.
- Numéro de port inscrit : 1024 à 49 151. Utilisé par les processus clients et sont pour la plupart octroyé par le SE ou généré dynamiquement par les applications clientes.
- Numéro de port privés ou dynamique : 49152 à 65535. Utilisé par certaines application particulière comme le service peer to peer et sont négocié dynamiquement par les parties.

NB : La commande ***netstat [-n]*** permet d'afficher les connexions actives sur un hôte.

- Fiabilisation des communications : Cette couche fournit deux protocoles en fonction du niveau de fiabilité requis.

b. Le protocole TCP

Il dispose d'une structure de message plus complexe qu'UDP et définit également des mécanismes plus complexes. La taille du champ d'en-tête est de 20 octets et illustré par la figure ci-dessous :

En-têtes TCP et UDP

Segment TCP

Bit (0)	Bit (15)	Bit (16)	Bit (31)
Port source (16)		Port de destination (16)	
Numéro d'ordre (32)			
Numéro de reçu (32)			
Longueur de l'en-tête (4)	Réservé (6) Bits de code (6)	Fenêtre (16)	
Somme de contrôle (16)		Urgent (16)	
Options (0 ou 32 le cas échéant)			
DONNÉES DE LA COUCHE APPLICATION (Taille variable)			

20 octets

Datagramme UDP

Bit (0)	Bit (15)	Bit (16)	Bit (31)
Port source (16)		Port de destination (16)	
Longueur (16)		Somme de contrôle (16)	
DONNÉES DE LA COUCHE APPLICATION (Taille variable)			

8 octets

Les propriétés de TCP sont :

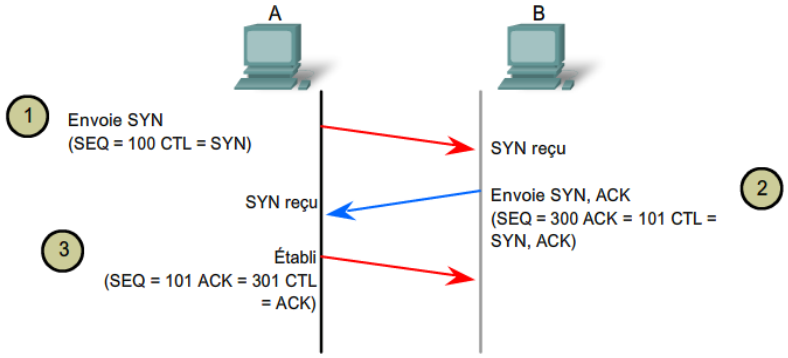
(1) L'orienté connexion : Etablissement de la connexion avant tout processus d'échange de message.

(2) L'acheminement fiable des segments : Utilise des numéros d'accusé de réception (ACK) pour acquitter les messages reçus.

(3) Livraison ordonnée des messages : Numéro de séquence

(4) Contrôle de flux : Pour contrôler l'utilisation des ressources (taille des tampons, bande passante) au niveau du serveur et gérer la vitesse de connexion. Champ d'en-tête : Taille de la Fenêtre. Ce mécanisme anticipe la perte des messages et évite de surcharger le serveur par les requêtes des clients. Les pairs peuvent négocier la taille de la fenêtre on parle de ***fenêtre glissante.***

Processus de connexion TCP en trois étapes



CTL = Indique quels bits de contrôle de l'en-tête TCP sont configurés sur 1.

c. Le protocole UDP

UDP est un protocole beaucoup plus simple que TCP qui ne se souci pas d'établir la connexion avant l'envoie des informations, n'envoie pas d'ACK, ne gère pas l'ordre de livraison ni le contrôle de flux. Si une application souhaite utiliser ces fonctions elle doit s'appuyer sur TCP ou (dans le cas où UDP est utilisé) les mettre en œuvre elle-même. Malgré sa pauvreté UDP est utilisé dans de contextes particuliers (VoIP : SIP port 5060 ; VoD et VoIP : RTP port 5004 ; TFTP, SNMP) est plus rapide que TCP et n'engendre qu'une faible surcharge sur réseau (8 octets d'en-tête).

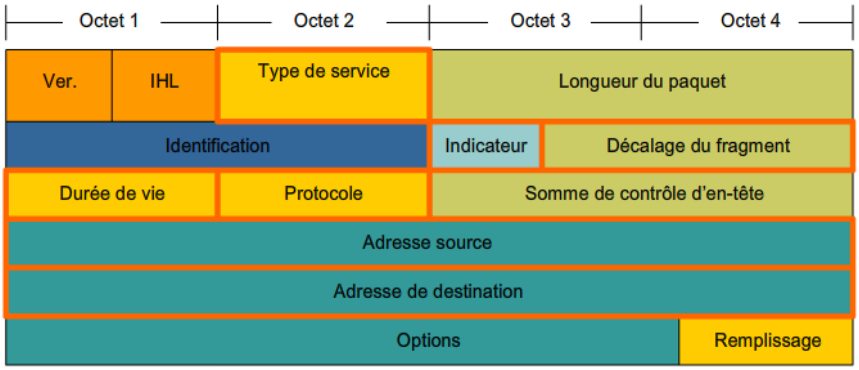
4. Couche réseau

Elle définit les mécanismes devant transporter les données des utilisateurs d'un point à l'autre de l'inter réseau. Le protocole IP (autres IPX, AppleTalk) est le protocole le plus répandu pour ce transport des informations de la couche réseau : c'est un protocole routé. Il décrit la technique d'adressage utilisé pour identifier les hôtes dans le réseau ainsi l'organisation hiérarchique du réseau. D'autres processus impliqués dans cette couche : les protocoles de routage, qui définissent les mécanismes d'échange d'information entre les routeurs.

a. Protocole IP :

Le protocole assure un transport des informations d'un point à l'autre de manière non fiable, il doit s'appuyer sur les couches supérieures s'il a besoin de fiabilité : il est dit protocole d'acheminement au mieux et reste indépendant vis-à-vis du média de

transmission. Il existe en fonction du format de message et du système d'adressage en deux versions (IPv4 et IPv6). Les champs d'en-tête pour IPv4 sont nombreux (voir figure ci contre) :



b. Adressage de base

Les réseaux et les hôtes au niveau de cette couche sont repérés par des adresse logiques ou adresse IP. L'objectif d'une subdivision en réseau peut être justifié par un besoin de performance, de sécurité et localité/gestion. Le système d'adressage proposé est un système hiérarchique car une partie permet de localiser le réseau (bits de poids fort) l'autre identifie l'hôte (bits de poids faible).

Format d'une adresse IP : suite de 32 bits sous forme de 4 groupes d'octets représenté en décimale pointée. En fonction de la façon dont on affecte les groupes d'octet pour représenter le réseau et/ou la partie hôte on distingue trois classes d'adresse principalement utilisé pour les réseaux de donnée.

- ✓ Classe A : Bit de poids fort à 0 → 0.0.0.0 à 127.255.255.255

- ✓ Classe B : 2 Bits de poids forts à 10 → 128.0.0.0 à 191.255.255.255

- ✓ Classe C : 3 bits de poids forts 110 → 192.0.0.0 à 223.255.255.255

NB : il existe la classe D (multicast) et E (expérimental) dont les adresse ne sont pas destiné à être attribué à des hôtes spécifiques du réseau.

Adresses particulières :

- **Adresse hôte :** Identifie un équipement terminal dans le réseau.
- **Adresse réseau :** Fait référence au réseau, obtenu en remplaçant l'écriture binaire de la partie hôte par des 0.
- **Adresse de diffusion :** Permet d'envoyer une information à tous les hôtes d'un réseau particulier (ou du réseau). Deux types : diffusion généralisée

(255.255.255.255) ou diffusion dirigée (spécifique à un réseau), obtenu en remplaçant l'écriture binaire de la partie hôte par des 1.

Adresses spéciales :

Certaines des adresses de ces plages (Classe A, B et C) sont réservées à une utilisation spéciale :

- **Adresse réseau et diffusion**
- **Adresse de boucle locale :** 127.0.0.1 Désigne la machine hôte elle-même.
- **Route par défaut :** 0.0.0.0
- **Adresse de lien local :** attribué à l'hôte par le SE lorsqu'aucun paramètres IP n'est explicitement défini : 169.254.0.0 à 169.254.255.255

c. Paramètres IP :

Toute machine pour communiquer dans le réseau a besoin d'être configuré. Celle-ci se fait en définissant les paramètres IP de ce dernier :

- **Adresse IP hôte :** Identifie un hôte de façon unique dans son réseau.
- **Masque de sous-réseau :** Permet à un hôte de calculer son propre réseau. Il peut encore être exprimé sous forme de préfixe, dans ce cas il correspond au nombre de bits qui représente la partie réseau de l'adresse IP.
- **Adresse IP de la passerelle :** sert d'équipement de sortie vers les autres réseaux.
- **Optionnel : les serveurs DNS.**

Pour consulter les paramètres IP d'un poste on utilise la commande **ipconfig [/all]** (sous Windows) ou **ifconfig** (sous Linux).

5. Couche Liaison de données

Dans les sections précédentes nous avons vu que : pour que deux hôtes échangent dans le réseau :

- la couche application génère le flux de données et présente une interface aux utilisateurs finaux ;
- Données qui seront transportées après une fragmentation et numérotation de la couche transport ;
- La couche réseau assure le voyage des informations entre les différents réseaux rencontrés (séparant l'hôte source et l'hôte destination) ;

Le rôle de la couche liaison de donnés est de préparer les données qui seront transportées sur le support physique. Etant donné la différence des supports et technologies rencontrés l'adaptation réalisée dépendra de ceux-ci. Cette couche assure ainsi l'indépendance du protocole de couche réseau (tel qu'IP) vis-à-vis du support utilisé. Parmi les fonctions offertes par cette couche nous pouvons citer : le contrôle d'accès au support et le verrouillage de trame.

a. Contrôle d'accès au support

La méthode de contrôle d'accès au support (**MAC** : Medium Access Control) définit comme les trames sont placés et retiré sur un support physique. Etant donné les différentes caractéristiques des supports rencontrés, la fonction dont ce dernier est partagé et la topologie physique du réseau, on distingue deux principales techniques de contrôle d'accès au support : accès contrôlé et accès basé sur le conflit.

i. Accès contrôlé

Dans cette méthode les nœuds accèdent au support tour à tour, un mécanisme est mis en œuvre pour contrôler cet accès dit déterministe (car prévisible). Bien qu'offrant l'avantage d'être organisé et prévisible, cette méthode est très souvent inefficace car offrant des débits peux élevés (chaque périphérique devant attendre son tour avant de transmettre même si aucun nœud n'est entrain de le faire).
Exemple de technologie : Token Ring, FDDI.

ii. Accès basé sur le conflit

Dans cette méthode, chaque nœud qui a des données à transmettre essaye d'accéder au support, s'il est libre la transmission est possible sinon il faut attendre. Cette méthode est dite non déterministe et très souvent des conflits surviennent entrainant des **collisions**. Pour gérer/limiter ceux-ci des techniques sont proposées comme le CSMA (Carrier Sense Multiple Access). Exemple de technologie : Ethernet (CSMA/CD) et IEEE 802.11 (CSMA/CA).

Les méthodes d'accès basé sur le conflit offrent en général des performances meilleurs que leur semblable (méthodes contrôlés), mais celles-ci s'écroulent lorsque le réseau est surchargé.

NB : Lorsque seuls deux équipements sont connecté en point à point sur le même support la couche liaison de donnée définit le modèle de communication à mettre en œuvre : half duplex (bidirectionnel non simultané) ou full duplex (bidirectionnel simultané).
Half duplex : chaque nœud impliqué sur le support peut recevoir et transmettre, mais pas simultanément.
Full duplex : chacun des nœuds peut transmettre et recevoir à tout moment, éventuellement simultanément.

b. Verrouillage de trame

Les données sont envoyées sur le support comme un train de bit incompréhensible entant que tel, le verrouillage de trame permet de diviser ce flux en groupe de bits déchiffrable. Pour ce faire on a besoin d'un adaptateur au niveau du nœud qui accède au réseau qui se traduit très souvent en **carte réseau.** Parmi les champs rencontrés en dehors des données provenant des couches supérieures la plupart sont des champs de contrôle indiquant :

- Quand ce produit la communication ? **Préambule ou SOF**

- Quels nœuds doivent communiquer ? **Adresses physique ou @MAC**
- Quelles erreurs sont survenues pendant la communication ? **FCS**

Ces champs sont organisés en en-tête et queue de bande. La structure de la trame varie avec le support physique rencontré, mais les champs génériques rencontrés sont illustrés par la figure ci-dessous.

c. Technologies et protocoles de couche 2

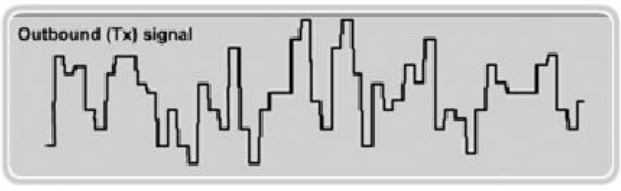
Dépendant du média les protocoles et technologie implémenté au niveau de la couche liaison de donnée qui définissent chacun sont format de trame sont : Ethernet (IEEE 802.3), HDLC, PPP, Frame relay, IEEE 802.11, RNIS, et ATM.

6. Couche physique

Elle est responsable de transmettre le flux de données provenant de la couche supérieure (liaison de données) comme un train de bits codé en un signal qui dépend du média utilisé (impulsion électrique, lumineuse ou ondes électromagnétiques). C'est également cette couche qui est responsable de ramasser ces signaux sur le support au niveau de l'équipement récepteur et les transmettre Cette transmission met en jeu un certain nombre de concepts :

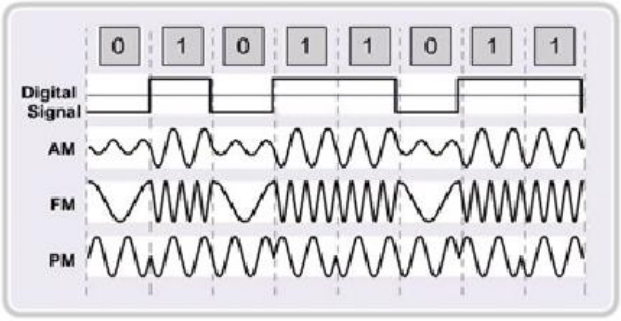
- Les équipements physiques (ports et circuits) chargé de l'envoie et de la réception du signal binaire,
- La représentation des informations sous forme binaire et la technique de codage mis en œuvre,
- Les caractéristiques physiques du support utilisé pour la transmission.

Représentations de signaux sur les supports physiques



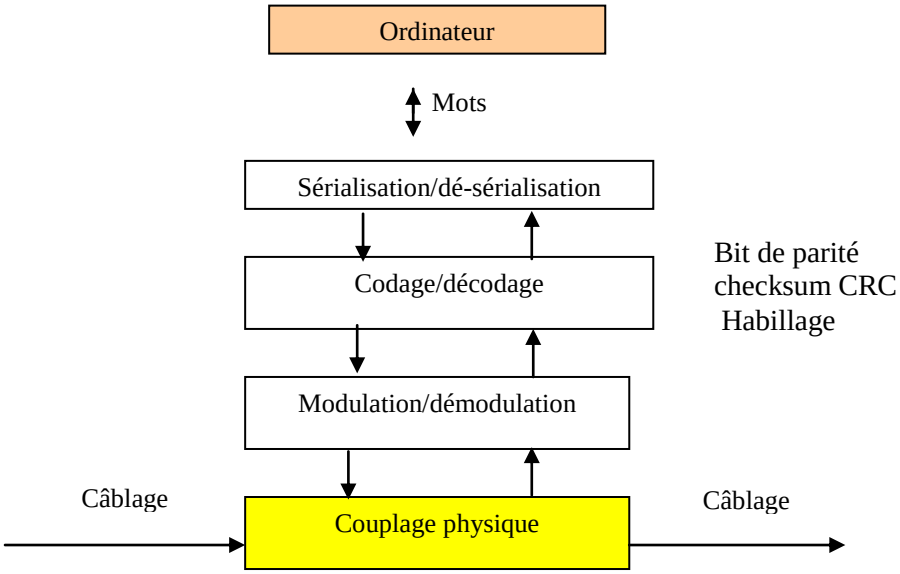
Exemple de signaux électriques transmis sur un câble en cuivre

Signaux représentatifs de fibre optique par impulsion lumineuse



Signaux micro-ondes (sans fil)

Cc



Processus mis en œuvre par la couche physique

a. Signalisation et Codage :

- **Signalisation**

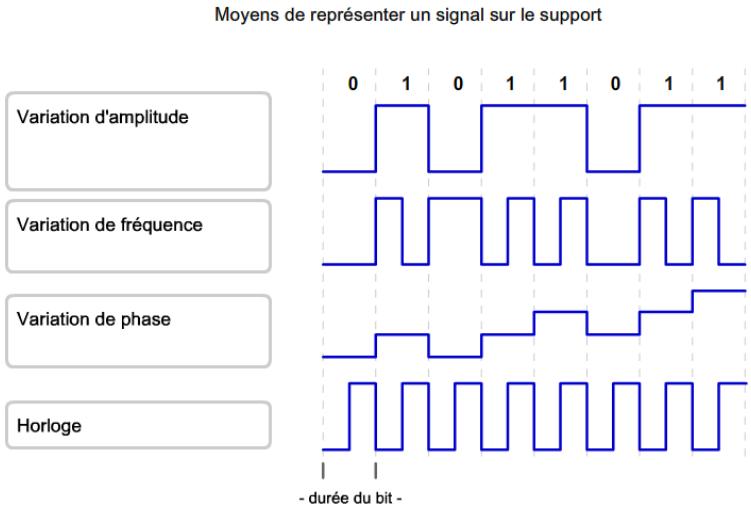
L'information est transmise de façon discrète (1 et 0), la signalisation et le codage sont deux techniques utilisées pour transporter ce dernier sur le support. La signalisation permet à la couche physique de faire correspondre aux états logiques (1 et 0) deux états physiques. Cette correspondance peut se faire au moins de deux façons :

- A chaque état logique, l'on fait correspondre un état physique,
- A chaque état logique, l'on fait correspondre une transition entre états physiques.

Exemple : pour la norme RS 232 on a : 0 ≈ 3 ± 0,5 v et 1 = 6± 0,5 **v**

Pour le placement du signal sur le support, les méthodes de signalisation qui définit les différents états physiques peuvent être :

- La modulation d'amplitude,
- La modulation de phase,
- La modulation de fréquence.

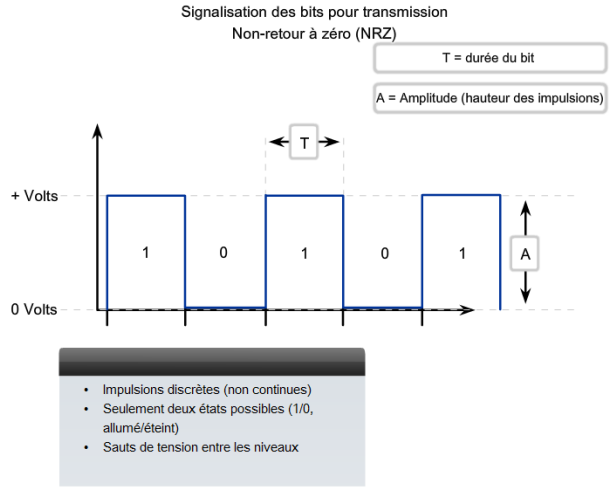


Chaque signal (binaire) envoyé sur le support met un temps spécifique d'occupation du support appelé **temps bit** ou **durée du bit.**

<u>Quelques exemples de signalisations concrètes :</u>

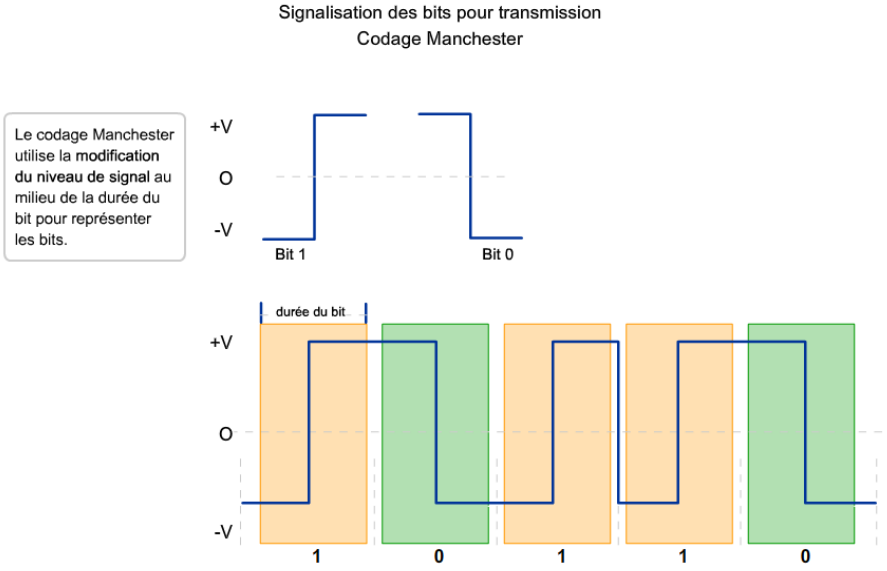
- ✓ **Le NRZ (Non Retour à Zéro) :**

Dans cette signalisation, une valeur de tension faible représente un 0 logique, une valeur de tension élevée représente un 1 logique. Cette signalisation n'est adaptée qu'à des communications bas débits.



- ✓ **Le code Manchester :**

Au lieu de représenter les bits comme impulsions de valeurs de tension simples, le système de codage Manchester représente les valeurs binaires comme transitions de tension. Une transition d'une tension faible à une tension élevée représente la valeur binaire 1. Une transition d'une tension élevée à une tension faible représente la valeur binaire 0.



Le codage Manchester n'est pas assez efficace pour être utilisé à des vitesses de transmission supérieures, mais il est meilleur que le NRZ. C'est la méthode de signalisation employée par Ethernet 10BaseT (Ethernet s'exécutant à 10 mégabits par seconde).

- **Codage**

Lorsqu'on veut transmettre à des débits très élevés, l'utilisation d'une étape de codage avant de placer les signaux sur le support améliore l'efficacité lors de transmissions de données à plus haut débit. Le codage est une méthode de conversion d'un flux de bits de données en code prédéfini. Les codes sont des groupements de bits utilisés pour fournir un modèle prévisible pouvant être reconnu à la fois par l'expéditeur et le récepteur. L'utilisation de modèles prévisibles aide à distinguer les bits de données des bits de contrôle et à offrir une meilleure détection des erreurs de support. Par exemple, les bits de code 10101 peuvent représenter les bits de données 0011. Bien que l'utilisation de groupes de codes introduise une surcharge sous la forme de bits supplémentaires à transmettre, ils améliorent la robustesse d'une liaison de communication.

Les avantages de l'utilisation de groupes de codes comprennent :

- Réduction des erreurs au niveau du bit
- Limitation de l'énergie effective transmise sur le support
- Meilleure distinction entre les bits de données et les bits de contrôle
- Meilleure détection d'erreur sur le support

Exemple de codage : 4B/5B

Cette technique, 4 bits de données sont transformés en symboles de code à 5 bits pour transmission sur le système de support. Ces symboles représentent les données à transmettre ainsi qu'une série de codes facilitant le contrôle de la transmission sur le support. La plupart des codes utilisés dans le système 4B/5B équilibrent le nombre de 1 et de 0 utilisés dans chaque symbole.

Symboles de code 4B/5B

Codes de données

Code 4B	Symbole 5B
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Codes de contrôle et non valides

Code 4B	Symbole 5B
inactif	11111
début de flux	11000
début de flux	10001
fin de flux	01101
fin de flux	00111
erreur de transmission	00111
non valide	00000
non valide	00001
non valide	00010
non valide	00011
non valide	00100
non valide	00101
non valide	00110
non valide	01000
non valide	10000
non valide	11001

Comme l'illustre la figure, 16 des 32 combinaisons possibles de groupes de codes sont allouées aux bits de données, et les groupes de codes restants sont utilisés pour les symboles de contrôle et symboles non valides. Six des symboles sont utilisés pour des fonctions spéciales identifiant la transition de l'inactivité aux données de trame et le délimiteur de fin de flux. Les 10 symboles restants indiquent des codes non valides.

b. Supports de transmission

On distingue deux types de supports pour la transmission d'information dans un réseau : les supports matériels et les supports immatériels. Les normes pour les supports spécifient :

- le type de câblage en cuivre utilisé,
- la bande passante de la communication,
- le type de connecteurs utilisés,
- le brochage et les codes couleur des connexions avec le support,
- la distance maximale du support.

- **Supports matériels**

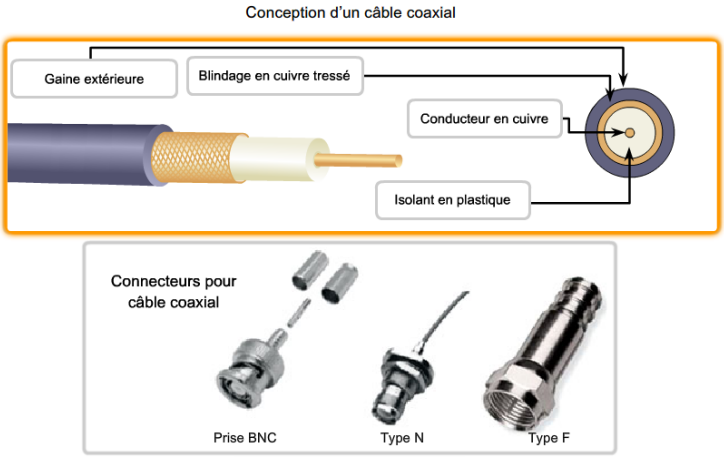
Dans cette catégorie on rencontre : les supports à base de cuivre et la fibre optique.

✓ **Support en cuivre**

C'est le type de support le plus utilisé pour les transmissions dans le réseau. Il utilise des fils en cuivre. On rencontre deux types de support en cuivre : Le câble coaxial et la paire torsadée.

Câble coaxial

Il s'agit d'un conducteur principal en cuivre, recouvert d'une gaine isolante et d'un blindage tressé. Ce type de support était utilisé pour les premiers réseaux informatiques (Ethernet à au plus 10Mbits/s) avec des connecteurs de type BNC au niveau de la station de travail. Aujourd'hui il est plus utilisé dans les réseaux étendus pour la connexion d'un client à l'équipement du fournisseur de service ou de l'opérateur télécom. **Exemple :** Communication large bande comme CATV.

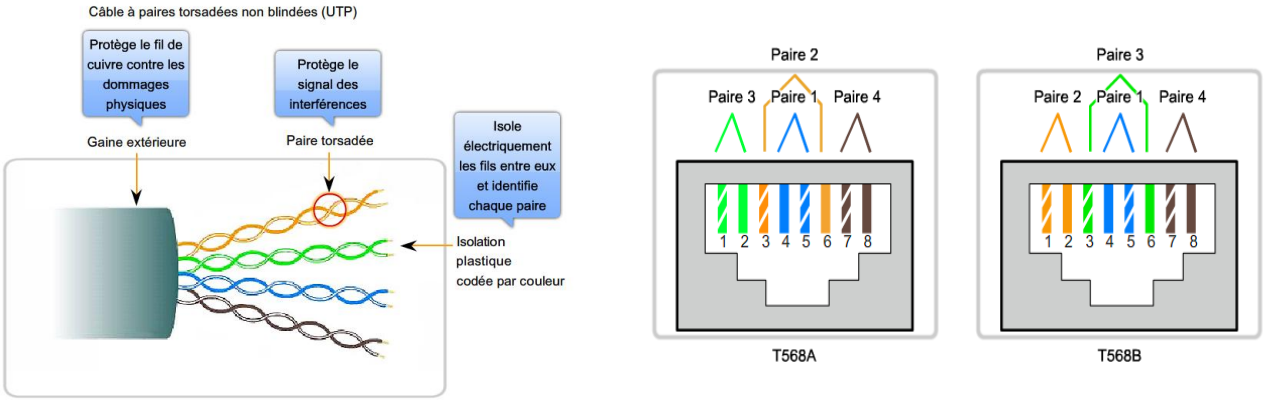


Paire torsadée

Le câble à paire torsadée existe en deux variantes : une blindée (UTP : Unshielded twisted-pair), l'autre non blindée (STP : Shielded Twisted-Pair).
Le câble UTP est utilisé pour les réseaux locaux à basé de la technologie Ethernet. Il est constitué de 8 fils regroupé en 4 paires torsadées, chacun fils protégé dans une gaine en plastique souple. La torsion a pour but d'annuler les signaux indésirables dus à l'interférence générée par le passage du signal électrique dans chaque fils : **diaphonie.**
Ce type de câbles existe en plusieurs catégories en fonction de la version d'Ethernet supportée :
Catégorie 3 et 4 → Ethernet à 10Mbits/s (10Base-T ou Ethernet)
Catégorie 5 → Ethernet à 100Mbits/s (100Base-TX ou FastEthernet)
Catégorie 5e et 6 → Ethernet à 1000Mbits/s (1000Base-T ou GigabitEthernet)
La longueur maximale de câble sans amplification de signal est de 100m. Le connecteur utilisé est un connecteur de type RJ-45.

Les différentes paires de câble sont codé par des couleurs : Orange/Orange-Blanc ; Vert/Vert-Blanc ; Bleu/Bleu-Blanc et Marron/Marron-Blanc qui définissent le type de câble (croisé ou droit) à utiliser. Il existe deux normes pour la fabrication des câbles UTP : Norme T568A et Norme T568B.
Classement des fils pour la norme T568A : Vert-Blanc ; Vert ; Orange-Blanc ; Bleu ; Bleu-Blanc ; Orange ; Marron-Blanc et Marron.
Classement des fils pour la norme T568B : Orange-Blanc ; Orange; Vert-Blanc; Bleu ; Bleu-Blanc ; Vert ; Marron-Blanc et Marron.

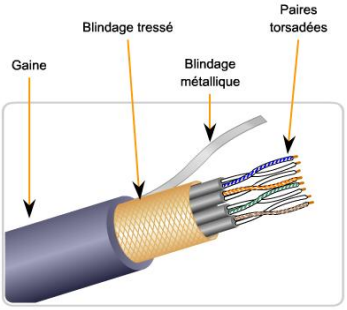
Fabrication de câble droit : Utiliser la même norme aux deux extrémités.
Fabrication de câble croisé : Utiliser des normes différentes aux deux extrémités.



La version blindé (STP) est utilise pour la conception des réseaux Token Ring. Le câble est mieux protégé que UTP et les coûts d'acquisition et d'installation sont plus élevés.

Câble à paires torsadées blindées (STP)

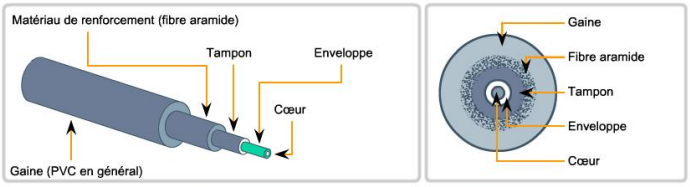
Fiches UTP RJ-45



✓ **Fibre optique**

La fibre optique est constituée d'un conducteur central en verre ou plastique, protégé par plusieurs couches de gaine qui empêche la lumière de s'échapper du conduit central. Ce support existe en deux variantes : la fibre optique monomodale (débits plus élevé et distances plus importantes jusqu'à 100km) et la fibre optique multimodale.

Conception d'un câble de support en fibre optique



Connecteurs pour fibre optique

La fibre optique les caractéristiques suivantes :

- Coûts d'acquisition élevés,
- Très longues distances sans régénération du signal,
- Nécessite des compétentes élevé pour la préparation des terminaisons de câble,
- Des débits de données très élevés.
- Absence d'interférence ou bruits.

Les câbles en fibre optique fonctionnent en paire pour le transport bidirectionnel du signal (câble TX et RX). Le principal problème que l'on rencontre dans le support à fibre optique est appelé **distorsion modale**, qui limite la longueur des segments de fibre multimode.

- **Supports immatériels**

Il est essentiellement caractérisé par l'utilisation des ondes électromagnétiques et micro-ondes pour le transport du signal dans l'air. Etant donné la nature versatile du médium radio et la nature ouverte de l'infrastructure, des mécanismes de contrôle et de sécurité robuste doivent être mis en œuvre pour exploiter pleinement ces

technologies. Les principales technologies existantes pour le transport des informations sont :

- IEEE 802.15.1 : Spécification Bluetooth
- IEEE 802.11 (a, b, g, n): Spécification WIFI
- IEEE 802.16 : Technologie WiMax
- GPRS, GSM, CDMA, UMTS, etc. : Réseaux Télécoms et cellulaires.
- Etc.

Des réglementations (nationales et internationales) rigoureuses sont mises en place pour le contrôle d'utilisation de ces ondes radios.

3- Conception des réseaux locaux

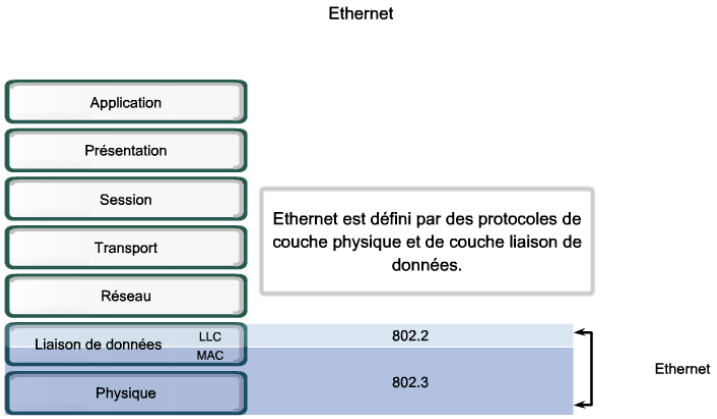
1. La technologie Ethernet

Ethernet est la technologie dominante en matière de réseaux locaux, elle est mise en œuvre au niveau des couches inférieures du modèle OSI : la couche physique et la couche liaison de données. La technologie définit : la méthode d'accès au support, la structure de la trame, et les mécanismes d'adressage au niveau de la couche 2 ; mais aussi les spécifications de couche 1 (spécificités liées au type de support). Cette technologie a beaucoup évolué dans le temps (souci d'avoir des versions prenant en charge des débits de plus en plus élevés).

1.1. Principe de base et fonctionnement

1.1.1. Norme Ethernet et origine

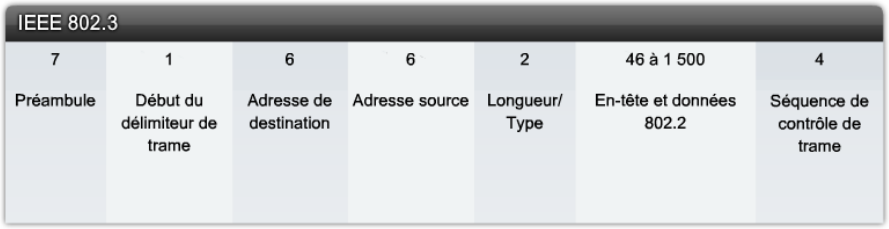
Les origines du protocole Ethernet remontent au début des années 70 (Robert Metcalfe), en 80 le consortium DIX (DEC : *Digital Equipment Corporation*, Intel et Xerox) publie la première norme Ethernet qui sera reprise en 85 par l'IEEE. Le protocole est normalisé sous les références IEEE 802.2 (sous-couche LLC) et IEEE 802.3 (sous-couche MAC). La sous-couche LLC (Logical Link Control) est indépendante du média physique utilisé et elle définit les fonctions logicielles et la communication avec le protocole de couche réseau (pilotes de la carte).
La dépendance vis-à-vis du support est gérée par la sous-couche MAC qui : définit les trames, assure le mécanisme d'adressage, contrôle les erreurs de transmission. Cette sous-couche englobe la couche physique et la moitié inférieure de la couche liaison de donné.



1.1.2. Trame Ethernet

La structure de la trame Ethernet prévoit des champs d'en-tête et d'en-queue autour de la PDU de couche 3. Une trame Ethernet doit posséder une longueur minimale de 64 octets et maximale de 1518 octets (préambule non inclus). Les trames plus courtes ou trop longues sont abandonnées par le récepteur (traitées comme invalide ou résultat de collision).

Champs de trame Ethernet



L'adresse MAC est une suite de 48 bits (6 octets noté comme une série de 6 groupes de chiffre hexadécimaux) permettant d'identifier de façon unique un équipement physique. Cette adresse gravée dans la ROM de la carte est constitué de deux parties : OUI (Organization Unique Identifier attribué par l'IEEE) et le numéro spécifique attribué par le constructeur.

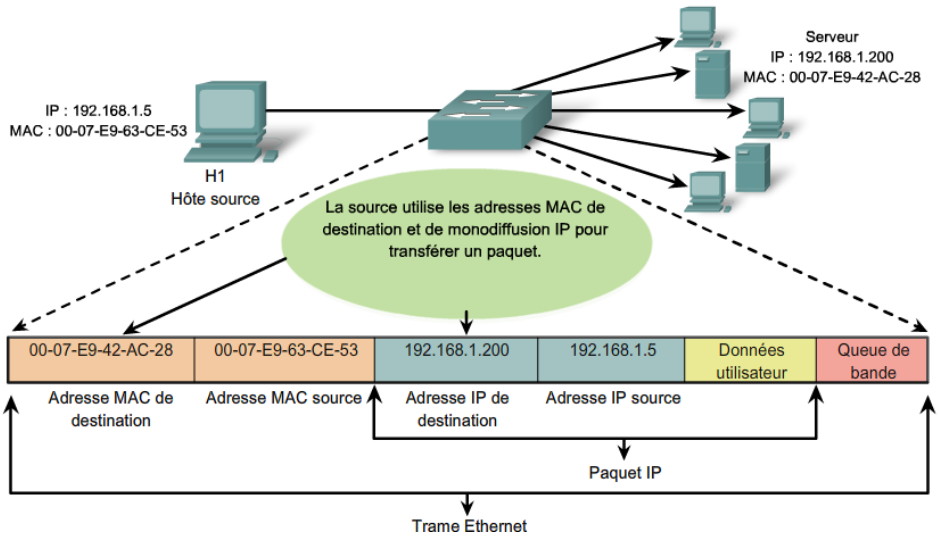
Exemple : 00 – FA – 1B – 40 – 72 – E0 ou 00 : FA : 1B : 40 : 72 : E0 ou encore 00FA.1B40.72E0 (OUI = 00 – FA – 1B et Numéro spécifique : 40 – 72 – E0)

Comment lire la valeur de l'@ MAC d'une carte ? Commande ***ipconfig /all*** ou ***ifconfig***

NB :

- La couche 2 utilise également les modes de communication monodiffusion, multidiffusion et diffusion. Une adresse MAC de diffusion possède de 1 sur toutes les 48 positions (correspond à FF–FF – FF –FF–FF – FF).
- Une adresse MAC de multidiffusion commence toujours par 01 – 00 – 5E (partie OUI), la suite définie l'identifiant de groupe.
- Une communication de diffusion de couche 3, se traduira en une diffusion de couche 2 ; idem pour la multidiffusion.

[Faire une illustration] (Monodiffusion, multidiffusion et diffusion)



1.1.3. Contrôle d'accès au support

La méthode d'accès au support utilise un mécanisme CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Dans cette technique tous les nœuds qui

partagent le support ont une garantie d'accéder à ce dernier (aucun nœud n'étant prioritaire). La mise en œuvre de la technique, se fait en plusieurs phases :

- **Ecoute de la porteuse :** Tous les nœuds qui souhaitent transmettre, écoute le support pour détecter une éventuelle transmission en cours. S'il est occupé, attendre un temps aléatoire avant une nouvelle écoute, sinon transmettre les données.
- **Accès multiple :** Si plus d'un nœud sont en transmission au même moment (latence non nulle sur le support), une collision de produit.
- **Détection de collision :** Tous nœuds à l'écoute est capable de détecter si une collision s'est produite (amplitude du signal plus importante). Les nœuds participant à la collision amplifient ce signal de collision (brouillage ou jam).
- **Attente aléatoire ou réémission temporisée :** Tous les nœuds qui détectent une collision déroule un algorithme d'attente (entrée : période aléatoire) avant d'écouter à nouveau le support. Une fois le délai expiré, le processus recommence.

NB : Les nœuds ayant occasionné la collision sont défavorisée pour une nouvelle tentative d'émission. 16 tentatives sont autorisées avant un abandon définitif de transmission (situation en cas de surcharge extrême du réseau).

1.2. Commutateurs et concentrateur

1.2.1. Concentrateur et domaine de collision

La possibilité de collision présuppose un média partagé. La probabilité pour cette dernière de survenir est accrue avec le nombre de périphérie qui partage le support. D'autres facteurs qui participent à augmenter le nombre de collision est la distance maximale (diamètre du segment réseau) qui sépare deux périphérique partageant le même support, il y a également la volonté pour les nœuds de communiquer le plus souvent.
Pour les raisons évoquées ci – dessous, l'utilisation des concentrateurs dans un réseau augmente l'étendue du domaine de collision. Un domaine de collision est la portion du réseau pour lequel deux périphérique en communication entrainerai une collision. Lors de la conception d'un réseau, il est souhaitable d'avoir plusieurs domaines de collision de petite étendue. L'utilisation de concentrateur dans un réseau Ethernet moderne n'est pas recommandée.
Exercice d'application : détermination de domaine de collision.

1.2.2. Commutateur Ethernet

Ethernet dans sa version classique (tel que définit par le standard d'origine) engendre un très grand nombre de collision. A ce problème on peut ajouter

l'évolutivité limité et la latence importante. Les concentrateurs ne prenant pas en compte un mécanisme de filtrage de trame, les commutateurs ont été introduit et leur utilisation de nombreux avantages :

- Segmentation du réseau en des domaines de collision plus petit (chaque port du commutateur définit un domaine de collision),
- Bande passante dédié par port,
- Possibilité de communications simultanées (sur des ports différents et même sur le même port [en mode full-duplex]),
- Mécanisme de contrôle élémentaire (filtrage de trame basé sur l'@MAC).

Un commutateur Ethernet, lorsqu'il reçoit une trame utilise les champs adresses MAC source et destination pour assurer sa fonction de transmission. Il gère une table appelé Table de pontage ou de commutateur (@MAC → N° Port). Initialement cette table est vide, elle est remplie au fur et à mesure que les communications sont initiées dans le réseau. L'adresse MAC source de chaque trame est examinée pour identifier le port d'appartenance des nœuds finaux. Dès qu'un trame est reçue, le commutateur examine le champ @ MAC Dst, puis cherche dans sa table de pontage le port de sortie. Si une entrée est définit, la trame est acheminé vers ce port uniquement, sinon elle est retransmise sur tous les ports excepté le port de réception. Pour assurer sa fonction le commutateur peut réaliser les opérations suivantes : apprentissage, inondation, réacheminement sélectif et filtrage. (**Question** pour quelle raison un commutateur peut-il abandonner une trame reçue ?)
[Illustration de transfert de trame et apprentissage d'@MAC]

1.3. Processus ARP (Address Resolution Protocol)

La transmission d'une trame par un nœud, nécessite que ce dernier spécifie toujours une @MAC de destination. Pour une communication monodiffusion celle-ci peut à un moment donné être inconnue de la station émettrice, le processus ARP est le mécanisme mis en œuvre par un hôte pour demander l'@MAC d'une autre, connaissant son @IP. Chaque station gère une table ARP (cache ARP) contenant des entrées @IP → @MAC, pour une transmission de trame, la station consulte d'abord ce cache (commande d'affichage du cache: ***arp -a***).
Le cache ARP est mis à jour de trois façons :

- Par surveillance du trafic en cours sur le réseau et en enregistrant pour chaque communication identifiée la correspondance @IP → @MAC
- Par processus ARP.
- L'administrateur spécifie manuelle une entrée dans le cache.

Les entrées de la table ARP sont horodaté et expire avec le temps (2 min sous Windows par défaut, augmenté à 10 si l'entrée est réutilisée entretemps).

Exemple : A veut envoyer un message à B, mais ne dispose pas de l'@MAC de B (A et B sont supposés être dans le même réseau).
Les phases de la requête ARP seront :

- A effectuera une diffusion de couche 2, en spécifiant dans le paquet IP l'hôte B comme destination [@MAC$_{Diff}$, @MAC$_A$, @IP$_A$, @IP$_B$, requête_ARP]
- La trame sera reçu par tous les hôtes du sous-réseau, seul B répondra en monodiffusion à A, en lui spécifiant son @MAC [@MAC$_A$, @MAC$_B$, @IP$_B$, @IP$_A$, réponse_ARP]
- L'hôte A enregistrera l'@MAC de B dans son cache, et constituera une trame contenant le message destiné à B.

Exercice d'application : Expliciter le processus mis en œuvre si les deux hôtes sont dans des réseaux différents.

Le protocole ARP est intégré à IP et reste transparent pour les utilisateurs finaux.

1.4. Version d'Ethernet

La plus grande partie du trafic sur Internet débute et aboutit sur des connexions Ethernet. Depuis son introduction dans les années 70, Ethernet a dû évoluer pour pouvoir répondre à la demande grandissante des réseaux LAN haut débit. Lorsque les supports à fibres optiques sont apparus, Ethernet s'est adapté à cette nouvelle technologie pour tirer parti de la très large bande et du faible taux d'erreur offert par les fibres. Aujourd'hui, le même protocole qui transportait des données à 3 Mbits/s peut le faire à 10 Gbits/s. Quelque soit la version d'Ethernet utilisée la compatibilité est assurée (la structure de la trame reste la même). La différence entre les diverses normes d'Ethernet apparaissent au niveau de la couche physique (encore appelé PHY Ethernet). La figure ci-dessous résume les caractéristiques principales de quelques versions d'Ethernet.

Version	Bande passante	Type de câble	Bidirectionnel	Codage	Distance Max.
10 Base – 5	10 Mbits/s	Coaxial Epais	Non simultané		500 m
10 Base – 2	10 Mbits/s	Coaxial Fin	Non simultané		185 m
10 Base – T	10 Mbits/s	UTP cat3 – 5	Non simultané	Manchester	100 m
100 Base – Tx	100 Mbits/s	UTP cat5	Non simultané	4B/5B	100 m
100 Base – Fx	100 Mbits/s	Fibre mult.	Non simultané	4B/5B	400 m
1000 Base – T	1 Gbit/s	UTP cat5e – 6	Simultané	PAM5	100 m
1000 Base – Sx	1 Gbit/s	Fibre mult.	Simultané	8B/10B	550 m
1000 Base – Lx	1 Gbit/s	Fibre mono.	Simultané	8B/10B	2 km
10G Base –T	10 Gbits/s	UTP 6a – 7	Simultané	/	100 m
10G Base – Cx4	10 Gbits/s	Axial Double	Simultané	/	100 m
10G Base – Lx4	10 Gbits/s	Fibre mono.	Simultané	/	10 km

2. Système d'adressage IP

2.1. Présentation

L'adressage IP est la première fonction de la couche réseau. Le principal problème qui se pose avec les adresses IP est le problème de pénurie d'adresse, la plage d'adresse étant très limité pour les utilisations courantes (vu le succès de TCP/IP). Le système d'adressage IP hérité suivant la spécification d'origine (RFC 1700) regroupe les adresses IP par classe (A, B, C, D et E), ce système d'adressage appelé **adressage par classe** favorise un gaspillage d'adresse IP. Pour résoudre le problème de pénurie (éviter le gaspillage d'adresses IP) plusieurs méthodes intérimaires ont été proposées, la solution ultime demeurant le remplacement d'IPv4 par le nouveau système d'adressage IPv6.

2.2. Adresses publiques VS Adresses privées

Les adresses privées sont détaillé par le document RFC 1918. Cette proposition donne la possibilité pour des hôtes de disposer d'une adresse IP (privée) sans que ceux soient « connus » sur Internet. Un hôte souhaitant héberger des services publics ou voulant être connu par les hôtes Internet doit se voir attribuer une adresse publique par l'autorité appropriée : l'IANA (AfriNIC, RIPE, APNIC, ARIN, LACNIC).

Le bloc d'adresse réservé à cette utilisation, et pouvant être utilisé par toute personne sans faire l'objet d'une réservation est :

- Classe A : 10.0.0.0 à 10.255.255.255 → 10.0.0.0 /8
- Classe B : 172.16.0.0 à 172.31.255.255 → 172.16.0.0 /12
- Classe C : 192.168.0.0 à 192.168.255.255 → 192.168.0.0 /16

NB :

- Les paquets provenant d'un hôte disposant une adresse privée sont bloqués par les routeurs Internet.
- Les hôtes disposant d'une adresse IP privées peuvent accéder aux services Internet grâce au mécanisme NAT (Network Address Translation).
- La majorité des adresses IP d'hôte sont des adresses publiques.

2.3. Adressage sans classe et technique VLSM

Le découpage en sous réseau et la technique VLSM (Variable Length Subnet Mask) sont deux autres techniques introduites pour minimiser le gaspillage des adresses IP. Avec le découpage en sous-réseau il est désormais possibles de créer plusieurs réseaux logiques à partir d'un seul bloc d'adresse (de classe A, B ou C). La technique VLSM permet d'ajuster la taille des sous-blocs aux besoins spécifiques du réseau. Avec l'introduction de ces deux techniques, la notion de classe n'est plus d'actualité et le maque de sous réseau doit chaque fois être précisé : on parle d'**adressage sans classe.**

<u>Atelier N°1 :</u> Découpage en sous-réseau.

On considère le bloc d'adresse réseau : 192.168.1.0 /24, en faire des sous-réseaux de taille diverses.

<u>Exercice :</u> On considère les blocs d'adresses réseaux suivants :

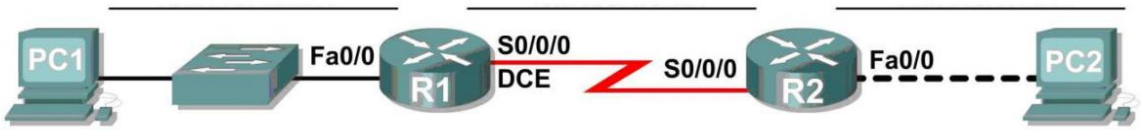
- **Bloc 1 :** 178.3.128.0 /19 en faire des sous-réseaux pouvant contenir chacun 500 machines chacun. Combien peut-on avoir de sous-réseaux ? Donnez l'adresse de chacun des ces sous-réseaux et pour chaque sous-réseau, donnez l'adresse de diffusion, l'adresse du premier et du dernier hôte utilisable.

- **Bloc 2 :** 184.157.168.0 /22. Mêmes question pour des sous-réseaux de 60 machines chacun.

<u>Atelier N°2 :</u> Schéma d'adressage VLSM.

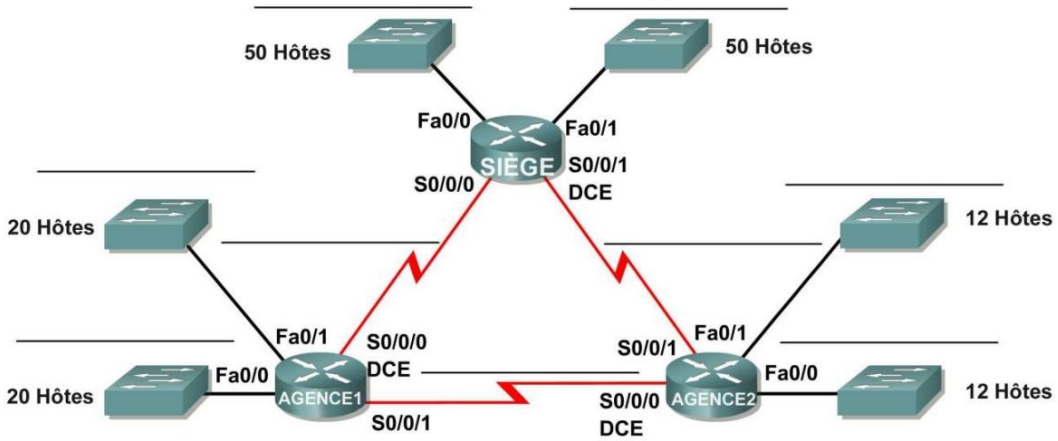
On considère le schéma représentant la topologie d'un réseau. Proposer un schéma d'adressage VLSM permettant de répondre aux besoins spécifiés.

- **Scénario 1 :** Bloc d'adresse fournit 192.168.1.0 /24



LAN R1 : 15 hôtes
LAN R2 : 30 hôtes
Liaison série : 2 hôtes
Les Routeurs dispose de la première adresse hôte du réseau dans leur LAN et les PC de la dernière. R1 a la première adresse hôte dans la liaison WAN et R2 la dernière.

- **Scénario 2 :** Bloc d'adresse fournit 172.16.192.0 /24



2.4. Adressage IPv6

En 90 l'IETF a commencé à se pencher sur le développement d'un nouveau système d'adressage IP. Aujourd'hui ce système est prêt et son utilisation est introduite de façon progressive dans le matériel et les plateformes logicielles réseaux. En dehors du problème de pénurie d'adresse qui était à résoudre, d'autres critères qui ont justifiées ce développement sont :

- Amélioration du traitement de paquet (moins de champs)
- Intégration de la sécurité (optimisation)
- Prise en compte de la mobilité

Une adresse IPv6 est codée sur 128 bits, et organisé en 8 blocs d'hexadécimaux séparés par des « : »
Exemple : 2001 : 0DB8 :0 :0 :0 :0 :1428 : 57A8

Il existe une écriture plus compacte lorsque l'adresse IPv6 comporte de nombreux zéro consécutifs : remplacer ces zéro par le symbole :: (seule restriction on n'a le droit de s'en servir qu'une seule fois).
L'adresse de l'exemple précédent peut se récrire 2001 :0DB8 :1428 :57A8
Exercice : A quoi correspondent les adresses FF01 :: 1 ; :: 1 et :: ?

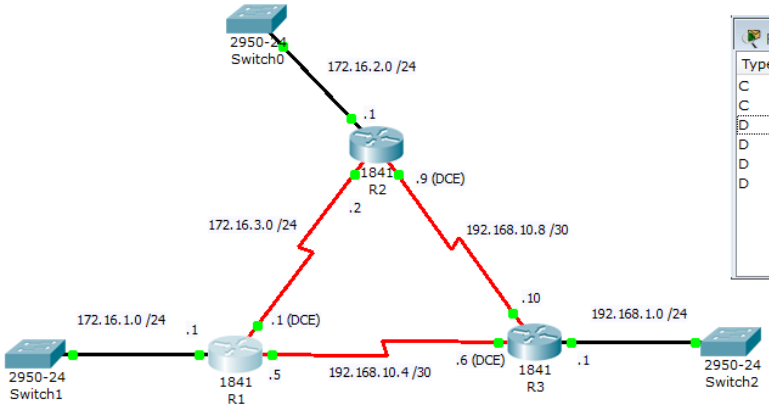
Il existe une diversité de mécanismes proposés pour la transition IPv4 vers IPv6. Parmi les plus courants on peut citer :

- La double pile,
- Les mécanismes basés sur le tunnel (6to4, ISATAP, Toredo)
- La traduction : NAT-PT

3. Notion de routage

3.1. Présentation

Dans un réseau local, les hôtes n'ont pas besoin de périphérique intermédiaire de couche réseau : il communique directement. Lorsque les hôtes sont dans des réseaux différents (séparé par un ou plusieurs autres réseaux), un périphérique intermédiaire : le routeur joue le rôle de passerelle pour assurer cette communication. Pour remplir sa fonction qui consiste à acheminer les paquets vers le destination finale, le routeur utilise une table de routage : structure de donnée dont chaque entrée (la route) décrit comment accéder à un réseau et les paramètres d'accès à ce dernier (@ du réseau distant/masque, @du tronçon suivant, coût de la route, source d'apprentissage). Lorsqu'un routeur reçoit un paquet, la destination de celui est mise en correspondance avec les entrées de la table de routage, si une entrée est trouvée le paquet est transmit conformément aux spécifications de la route sous forme d'un trame dont le type dépend de l'interface de sortie. Si aucune correspondance n'est trouvée le paquet est détruit. Le routeur prend des décisions en utilisant les informations d'en-tête de couche 3, cependant à l'exception du TTL ces champs ne sont pas modifiés.



Routing Table for R1

Type	Network	Port	Next Hop IP	Metric
C	172.16.1.0/24	FastEthernet0/0	---	0/0
C	172.16.3.0/24	Serial0/0/0	---	0/0
D	172.16.0.0/16	Serial0/0/0	172.16.3.2	90/3708416
D	172.16.2.0/24	Serial0/0/0	172.16.3.2	90/2172416
D	192.168.1.0/24	Serial0/0/0	172.16.3.2	90/2684416
D	192.168.10.8/30	Serial0/0/0	172.16.3.2	90/2681856

Lors de la recherche de correspondance dans la table de routage le routeur cherche la plus longue correspondance @ réseau de destination vs masque de sous réseau.

Remarque : La route par défaut par défaut est un moyen de spécifier le tronçon suivant en cas d'échec de correspondance avec toutes les routes spécifiques.
Syntaxe : 0.0.0.0 /0

Affichage de la table de routage :

- Sur un PC : ***netstat –r*** ou ***route PRINT***
- Sur un routeur (Cisco) : ***show ip route***

3.2. Etapes de traitement d'un paquet par le routeur

(1) Le routeur reçoit une trame et y supprime l'encapsulation de couche 2
(2) Le routeur extrait l'@ IP de destination du paquet
(3) Le routeur recherche la meilleure correspondance dans la table de routage
(4) Si celle-ci est trouvé aller à (5) sinon supprimer le paquet.
(5) Le routeur ré-encapsule le paquet dans une trame (dépendant de l'interface de sortie)
(6) Envoyer cette trame sur la sortie associée à l'interface de sortie.

Pour assurer cette fonction de routage les trois principes suivant sont vrai concernant les routeurs :
Principe 1 : Chaque routeur prend sa décision seul, en se basant sur les informations dont il dispose dans sa table de routage.
Principe 2 : Le fait qu'un routeur dispose de certaines informations dans sa table de routage ne signifie pas que d'autres routeurs ont les mêmes informations.
Principe 3 : Les informations de routage concernant un chemin d'un réseau à l'autre ne fournissent aucune information de routage sur le chemin inverse (ou de retour).

3.3. Protocole de routage

Pour remplir sa table de routage le routeur utilise divers mécanisme. La source de la route revêt une des trois natures suivantes :

- ***Réseau directement connecté :*** la route directement connecté est automatiquement installé dans la table de routage dès lors que la configuration de l'interface est bien réalisée.
- ***Route statique :*** Pour les routes à destination des réseaux distants l'administrateur peut définir manuellement les routes à installer dans la table de routage.
  Exemple : La route par défaut est en général configurée de façon statique.
- ***Route dynamique :*** les routeurs peuvent coopérer grâce à un protocole de routage pour échanger les informations de routage pour apprendre la topologie du réseau et prendre des décisions d'acheminement.

3.3.1. Routage statique

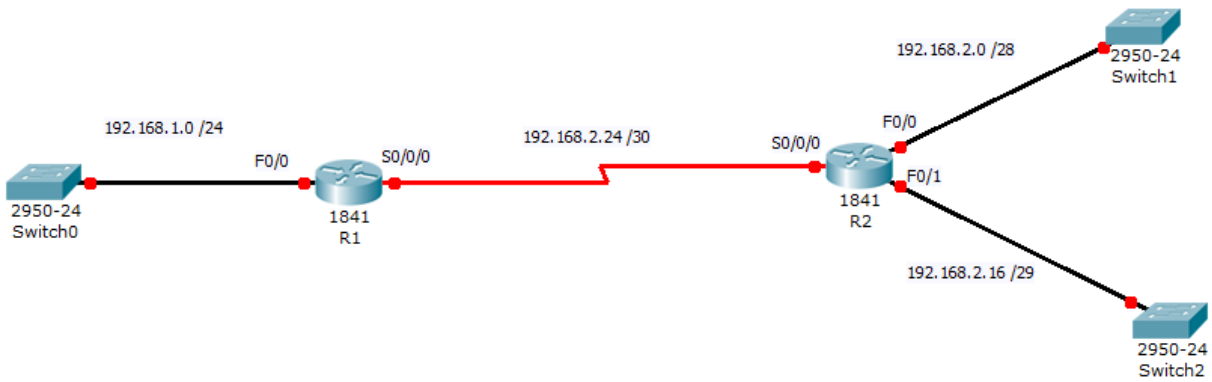
Cette méthode peut être avantageusement utilisé lorsque le réseau est de petite taille, ou dans le cas de configuration d'une route statique. Elle offre les avantages suivants :

- Les routes statiques aussitôt configurées sont installé dans la table de routage (pas de consommation de banda passante pour les mises à jour de routage, ni d'utilisation du temps processeur pour le calcul des meilleures routes).
- Il est sécurisé (pas de possibilité d'interception de messages, car ceux-ci ne sont pas envoyé)

Le principal inconvénient du routage statique est le fait qu'il ne passe pas à l'échelle : la charge administrative augmente avec la taille du réseau, de plus les modifications de la topologie du réseau ne sont pas prises en compte de façon automatique.
Dans un routeur Cisco, l'une ou l'autre des commandes suivantes est utilisée pour configurer une route statique :

ip route <@_reseau_dest> <masque> <@_tronçon_suiv>
ip route <@_reseau_dest> <masque> <interface_de_sortie>

Application : Configurer les routeurs R1 et R2 grâce au routage statique de sorte à permettre une connectivité complète du réseau. Après ces configurations quelles est l'état de la table de routage de chacun ?



3.3.2. Routage dynamique

Il arrive très souvent que la topologie du réseau soit complexe ou que des modifications topologiques surviennent, dans ces situations l'utilisation d'un protocole de routage dynamique permet de réduire la surcharge administrative liée à l'utilisation exclusive des routes statiques. Suivant la classe de protocole de routage dynamique mis en place les échanges de message de mise à jour permettront aux différents routeurs de construire leur table de routage. Les protocoles de routage dynamique utilisent trois éléments pour leur fonctionnement :

- Des structures de donnée pour conserver des BD particulières (table de routage, table de voisinage, table topologique, etc.)
- Un algorithme qui s'applique aux structures de données précédentes pour construire la table de routage.
- Les mises à jour de routage pour partager certaines informations permettant la construction des structures de donnée ou BD.

On distingue deux grandes classes de protocole de routage :

i. Protocole de routage à vecteur de distance

Les routeurs qui utilisent cette catégorie de protocole de routage s'envoient des mise à jours périodique à intervalles réguliers. Ils ont l'avantage d'être simple à mettre en œuvre et consomme moins de ressources (temps processeurs et mémoire) que la seconde classe de protocole de routage. L'algorithme de calcul des meilleures route est moins complexe également (de type BELLMAN-FORD). Leur principal inconvénient est la convergence lente et la consommation importante de la bande passante pour les mises à jour de routage.

Exemple de protocole de cette classe : RIP (v1, v2 et RIPng), IGRP, EIGRP

ii. Protocole de routage à état de lien

Ils sont indiqués pour des topologies réseaux très complexes car plus robustes que les protocoles à vecteur de distance (ceux-ci pouvant produire des boucles de routage dû à la lenteur de convergence). Grâce à des mises à jour particulières (non périodique mais déclenchées) chaque routeur a la vue complète du réseau (table topologique) sur laquelle est appliquée l'algorithme de DIJKSTRA pour le calcul des meilleures routes. La vitesse de convergence est meilleure mais ils ont l'inconvénient d'être plus difficile à mettre en œuvre et nécessite des routeurs puissants pour l'exécution de l'Algo. du plus court chemin.

Exemple de protocole de cette classe : OSPF, IS-IS.

4. Réseaux locaux sans fils.

4.1. Réseaux sans fil pour quoi faire ?

La mise en réseau des machines par une infrastructure filaire peut s'avérer complexe : cela nécessite de tirer un câble d'un nœud de concentration à l'emplacement du nouvel équipement. La mise en place de l'infrastructure physique

d'interconnexion doit être prise en compte dans l'architecture du bâtiment, et dans des cas de mise à jour ceci peut s'avérer coûteux. Les réseaux locaux sans fil permettent de s'affranchir des câbles et facile le déploiement de nouveaux réseaux pour l'interconnexion d'équipements (**Exemple** : connexion d'une nouvelle salle de réunion). Avec la généralisation des équipements informatique et la prise en charge par ceux des protocoles de communication, l'accessibilité à l'information pendant son déplacement (mobilité et itinérance) est désormais possible.
Dans la plupart des cas, le réseau local sans fil permet d'étendre l'infrastructure filaire aux postes sans fils grâce un équipement : le point d'accès sans fil (Access Point : AP). Tout comme la technologie Ethernet, ils sont normalisés par IEEE (IEEE 802.11) et ont tous la même origine. La technologie sans fil a évoluée et existe en plusieurs versions. Le tableau ci-contre résume les points de comparaison entre le réseau filaire et le réseau sans fil :

Caractéristique	Réseau local sans fil	Réseau Ethernet
Couche physique	Radiofréquence	Câble
Accès au support	Détection des collisions	Evitement des collisions
Signaux parasites et interférence	Très sensible	Faible impact
Réglementation	Organismes internationaux (IEEE, ITU) et nationaux	IEEE

4.2. Fonctionnement de la technologie réseau local sans fil

Pour mettre en œuvre un réseau local sans fil, il est nécessaire de disposer d'un minimum d'équipement : hôtes doté d'une interface sans fil (adaptateur sans fil : intégré ou de type PCI, USB, ou PCMCIA), et suivant la topologie un point d'accès sans fil (comme point de concentration des connexions). La topologie du réseau peut être avec ou sans infrastructure (mode ad hoc). La technique MAC est de type CSMA/CA, contrôlé par le point d'accès. Dans le mode infrastructure, pour communiquer les nœuds sans fil doivent s'associer à un point d'accès. Cette association passe par une série d'étapes :

- Le point d'accès annonce sa présentation grâce à des trames particulières (beacon) contenant le SSID (Service Set ID), les débits supportés, les paramètres de sécurité, etc.
- Les clients envoient des trames de type probe (analyseur) contenant les paramètres du réseau sur lequel il veut s'associer.
- Une phase d'authentification est possible (auquel cas le client doit s'authentifier pour être accepté par point d'accès).
- La dernière phase (association) consiste en une validation de la connexion du client sur le point d'accès et les paramètres de cette connexion (Débit, adresse physique du client, l'adresse physique de l'AP etc.)

Les versions de la norme IEEE 802.11 spécifient comment les radiofréquences de la bande de ISM (Industrial, Scientific, Medical) sont utilisées. Le tableau ci-contre résume les principales caractéristiques des versions IEEE 802.11

	802.11a	**802.11b**	**802.11g**	**802.11n**
Bande de Freq.	5.5GHz	2.4 GHz	2.4 GHz	2.4 et 5.5 GHz
Débit de données	Jusqu'à 54 Mbit/s	Jusqu'à 11 Mbit/s	Jusqu'à 11 Mbit/s	Jusqu'à 248 Mbit/s
Sortie	1999	1999	2003	2008
Avantages	Rapide, Moins sujettes aux interférences	Faible coût, bonne portée	Rapidité, bonne portée, peu sensible aux obstacles	Excellent débit de donnée, porté accrue
Inconvénients	Coût élevé, faible porté, faible perf. en cas d'obstacle.	Lenteur, plus sujette aux interférences.	Interférence avec les appareils dans la bande des 2.4 GHz	

NB : La certification WIFI (délivré par la WIFI Alliance, consortium de constructeurs) permet de valider l'interopérabilité de divers composants issus de constructeurs différents utilisant la norme IEEE 802.11.

4.3. Mécanisme de sécurité dans IEEE 802.11

La sécurité doit être un souci majeur pour tout administrateur devant mettre en œuvre un réseau local sans fil, de part sa nature inhérente ouverte (toute personne à porté d'un point d'accès est capable d'accéder au réseau). Les mécanismes de sécurité pour les réseaux sans fil ont évolués avec la technologie et les besoins des utilisateurs finaux. Le tableau ci-dessous résume les différents mécanismes de sécurité dans les réseaux locaux sans fil.

Accès ouvert	**WEP**	**WPA**	**WPA2**
Aucun chiffrement Pas d'authentification **Contre mesure :** Filtrage des @ MAC Désactivation du broadcast SSID	Clés configurés statiquement Non évolutif et cassable Authentification non efficace	Chiffrement amélioré Algorithme TKIP Mécanisme standardisé	Chiffrement très robuste (AES), Clés dynamiques, Supporte le standard d'authentification IEEE 802.1x