OFPPT مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle
et de la Promotion du Travail

Direction Régionale Beni Mellal - Khénifra
Complexe de Formation /EFP

Module N° 03

Conception d'un réseau informatique

Stagiaire :

Nom : ……
Prénom : ……

EFP : ISTA NTIC BENI MELLAL
FILIERE : infrastructure Digitale
NIVEAU : TECHNICIEN SPECIALISE (TS)
ANNEE : 1IERE ANNEE
ANNEE DE FORMATION 2022/2023
FORMATEUR : ISSAKHI MOHAMED

Issakhi.mohamed@gmail.com

Table des matières

INTRODOCTION AUX RESEAUX

1- Réseaux informatiques

Un réseau est par définition un ensemble d'entités (Equipements réseaux) reliées entre elles par l'intermédiaire d'un support de communication. Nous allons nous intéresser dans le cadre de ce cours à ce que l'on nomme des réseaux de données ou réseaux informatiques.

Les avantages d'un réseau informatique :

- Le partage des ressources du réseau :
  - Les fichiers
  - Les applications
  - Les périphériques comme des imprimantes, un scanner, un modem
- La communication entre les membres du réseau :
  - La messagerie interne ou externe
  - L'accès à Internet
  - L'accès à distance au réseau et à ses ressources
- Le travail en groupe :
  - La synchronisation des agendas, des notes de service
  - Le suivi des différentes versions d'un même projet
  - Le travail interactif entre les membres d'une même équipe

2- Terminologie de base des réseaux

2-1- Classification des réseaux

La première classification de réseau que nous allons faire s'établit sur la base des distances entre les communicants.

- Les réseaux LAN (Local Area Network) : (Réseau local)
  - Couvrent une région géographique limitée
  - Permettent un accès multiple aux médias à large bande
  - Ils relient physiquement des unités adjacentes

    Exemple : Une salle de classe
- Les réseaux WAN (Wide Area Network): (Réseau étendu)
  - Couvrent une vaste zone géographique
  - Permettent l'accès par des interfaces séries plus lentes
  - Relient des unités dispersées à une échelle planétaire

    Exemple : Internet

Ces types de réseaux sont les plus courants, néanmoins il en existe d'autres, à l'instar des MAN (Metropolitan Area Network), qui connectent un ou plusieurs LANs dans une même région géographique. On les trouve souvent en ville, situés dans les endroits publics.

2-2- Unités de mesure

Représentation des données informatiques

Unité	Définition	Octets	Bits
Bit (b)	Chiffre binaire 1 ou 0	1 bit	1 bit
Octet (o)	8 bits	1 octet	8 bits
Kilo-octet (Ko)	1 kilo-octet =1024 octets	1024 octets	8192 bits
Méga-octet (Mo)	1 méga-octet =1024 kilo-octets	1 048 576 octets	8 388 608 bits
Giga-octet (Go)	1 gigaoctet =1024 méga-octets	1 048 576 kilo-octets	Env. 8 milliards de bits
Téraoctet (To)	1 téraoctet =1024 giga-octets	1 048 576 méga-octets	Env. 8 trillions de bits

La bande passante et le débit

La bande passante d'un réseau représente sa capacité, c'est-à-dire la quantité de données pouvant circuler en une période donnée sur le réseau. Celle-ci se mesure en bits par seconde. Du fait de la capacité des supports réseau actuels, les différentes conventions suivantes sont utilisées :

Unité de bande passante	Abréviation	Équivalence
Bits par seconde	bits/s	1 bit/s = unité fondamentale
Kilobits par seconde	Kbits/s	1kbit/s = 1000 bits/s
Mégabits par seconde	Mbits/s	1Mbit/s = 1 000 000 bits/s
Gigabits par seconde	Gbits/s	1Gbit/s = 1 000 000 000 bits/s

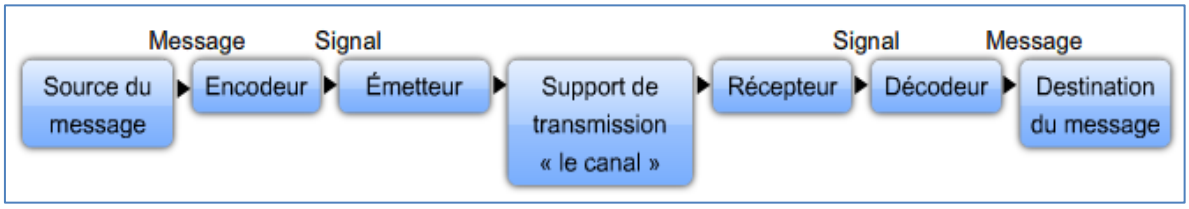
À cette notion de bande s'ajoute celle de débit. Le débit est la bande passante réelle, mesurée à un instant précis de la journée. Ce débit est souvent inférieur à la bande passante.
De ce fait, le temps de téléchargement d'un fichier peut se mesurer de la manière suivante :

- **Temps de téléchargement (s) = Taille du fichier (b) / débit**
- **Calculer le temps de téléchargement d'un fichier de taille 4Gb avec un débit de 20Mb/s**
- **Calculer le temps de téléchargement d'un fichier de taille 4Go avec un débit de 5Mb/s**

2-3- La plateforme pour les communications

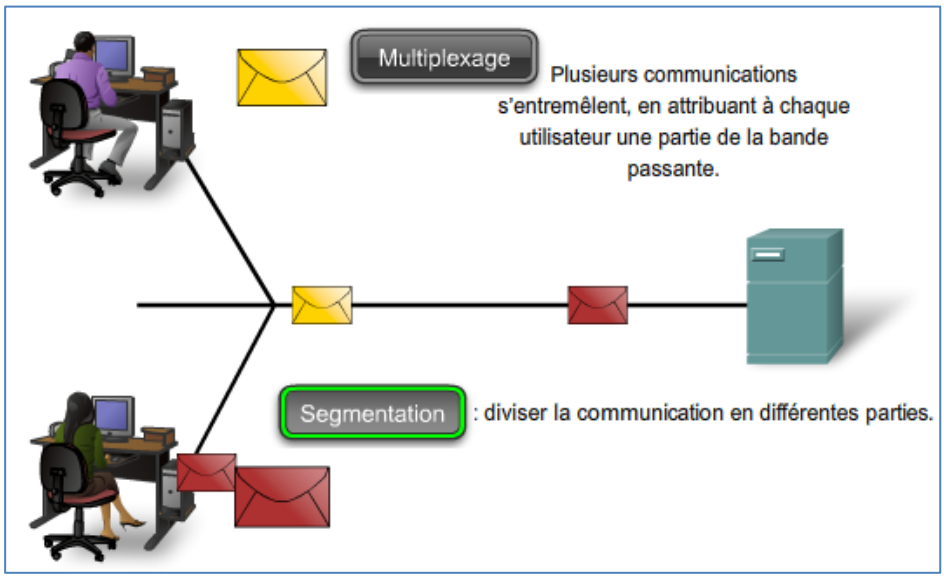
2-3-1- Les éléments de communication

La communication démarre avec **un message** (l'information), qui doit être envoyé d'une **source (émetteur)** à une **destination (Récepteur)** en passant par **un support de transmission (le canal)** et régie par **des règles (protocoles).**



2-3-2- la communication de message

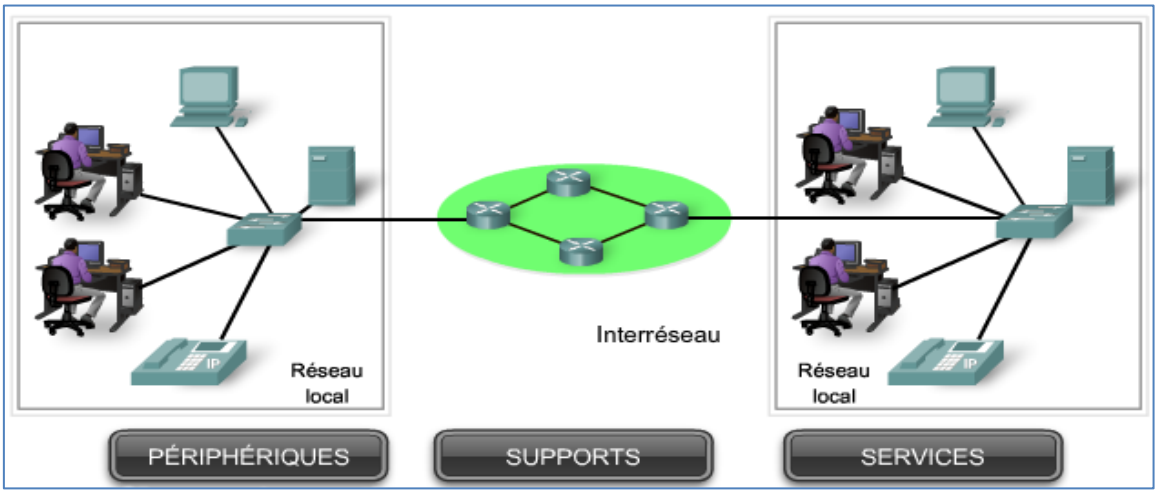
La communication de message consiste à diviser les données en parties de taille moins importante et plus facilement gérables pour les envoyer sur le réseau. Cette division du flux de données en parties plus petites est appelée **segmentation.**
Le processus qui sert à entremêler les parties des différentes conversations entre elles sur le réseau est appelé **multiplexage.**



2-3-3- Composants d'un réseau

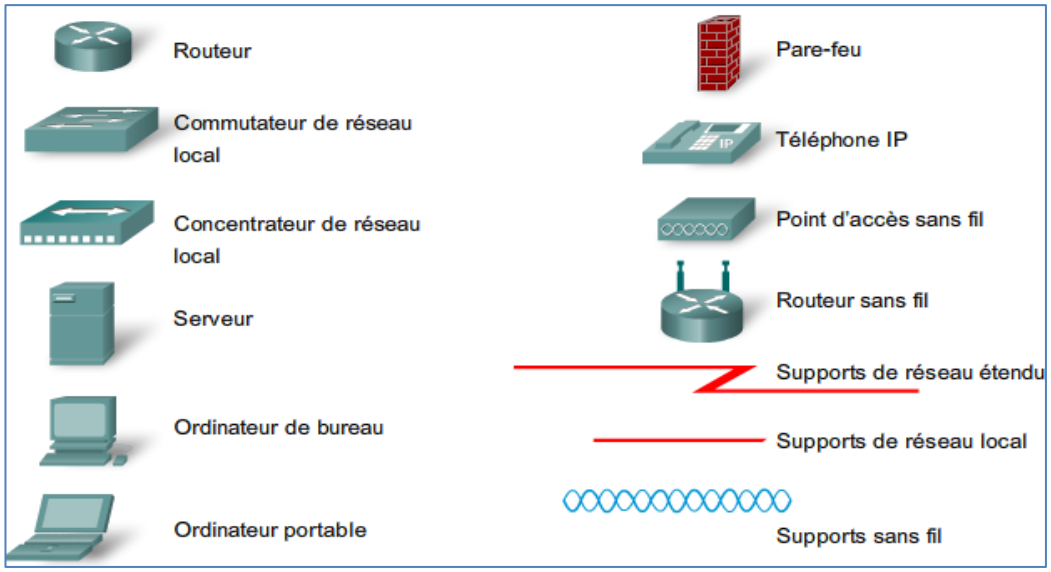
On distingue deux parties :

- Les périphériques et les supports représentent les éléments physiques ou le matériel du réseau.
- Les services et les processus constituent les programmes de communication, appelés logiciels, qui sont exécutés sur les périphériques réseau



2-3-4- Symbole du réseau de données

Les symboles du réseau de données courant sont :



2-3-5- Les protocoles

Les protocoles sont des règles qui régissent le processus de la communication. Afin que des périphériques puissent communiquer correctement, une suite de protocoles réseau doit décrire des exigences et des interactions précises tels que :

- le format ou la structure du message
- la méthode selon laquelle des périphériques réseau partagent des informations sur des chemins avec d'autres réseaux
- comment et à quel moment des messages d'erreur et système sont transférés entre des périphériques
- la configuration et l'arrêt des sessions de transfert de données.

MODELES OSI ET TCP/IP

1- LE MODÈLE OSI

1-1- Introduction

Chaque constructeur de matériels réseau développant sa propre technologie. Le résultat fut une quasi-impossibilité de connecter différents réseaux entre eux.
Pour pallier à ce problème d'interconnections, l'ISO(International Standards Organisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseaux.
Ainsi fût créé le modèle OSI (Open Systems Interconnection), Ce modèle a permis aux différents constructeurs de concevoir des réseaux interconnectables.

Le modèle OSI est un modèle conceptuel. Il a pour but d'analyser la communication en découpant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique.

1-2- Les couches de modèle OSI

Les 7 couches du modèle OSI sont les suivantes :

- Couche 1 : Couche physique

La couche physique définit les spécifications du média (câblage, connecteur, voltage, bande passante…).

- Couche 2 : Couche liaison de donnée

La couche liaison de donnée s'occupe de l'envoi de la donnée sur le média. Cette couche est divisée en deux sous-couches :

  - La sous-couche MAC (Média Access Control) est chargée du contrôle de l'accès au média. C'est au niveau de cette couche que l'on retrouve les adresses de liaison de donnée (MAC, DLCI).
  - La sous-couche LLC (Layer Link Control) s'occupe de la gestion des communications entre les stations et interagit avec la couche réseau.

- Couche 3 : Couche réseau

Cette couche gère l'adressage de niveau trois, la sélection du chemin et l'acheminement des paquets au travers du réseau.

- Couche 4 : Couche transport

La couche transport assure la qualité de la transmission en permettant la retransmission des segments en cas d'erreurs éventuelles de transmission. Elle assure également le contrôle du flux d'envoi des données.

- Couche 5 : Couche session

La couche session établit, gère et ferme les sessions de communications entre les applications.

- Couche 6 : Couche présentation

La couche présentation spécifie les formats des données des applications (encodage, compression, encryptions).

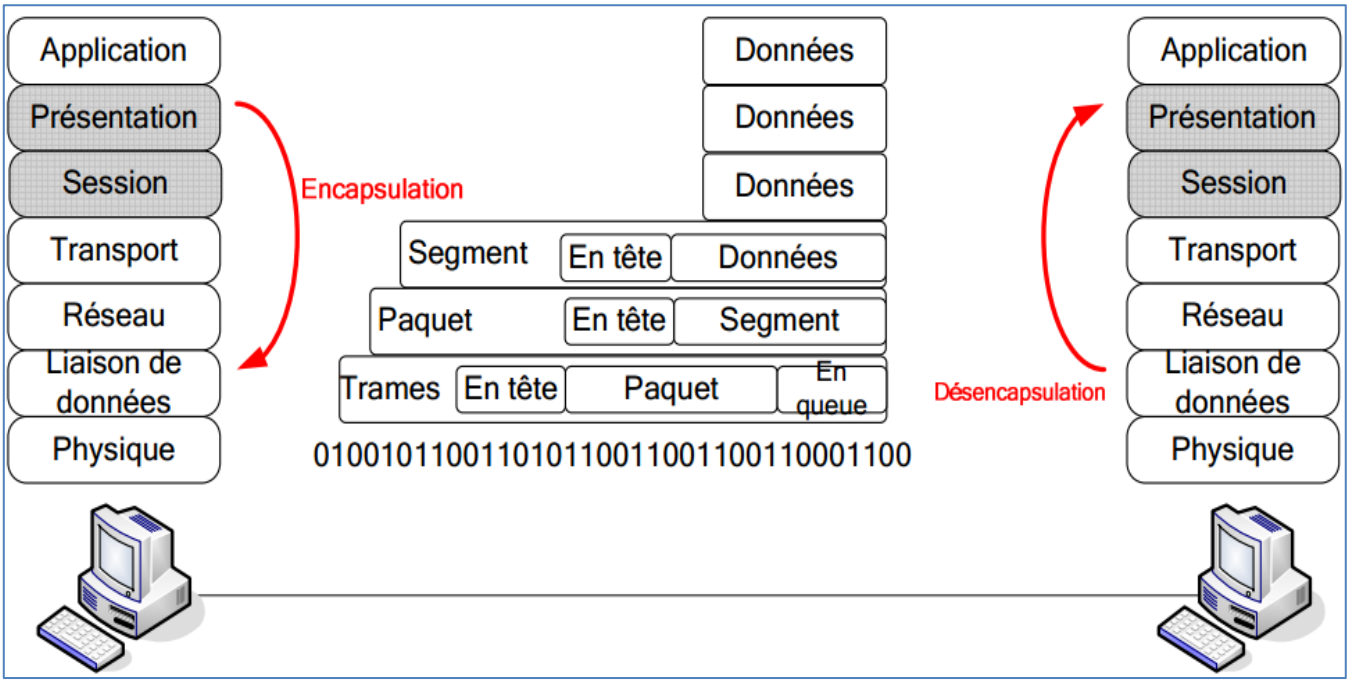
- Couche 7 : Couche Application

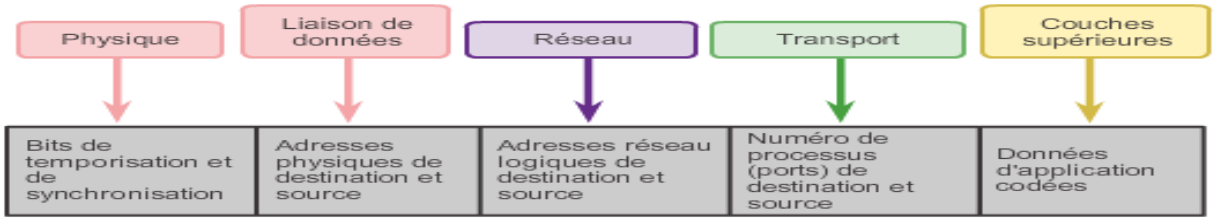
La couche application représente l'interface entre l'utilisateur est le réseau.

1-3- Processus de communication

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

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





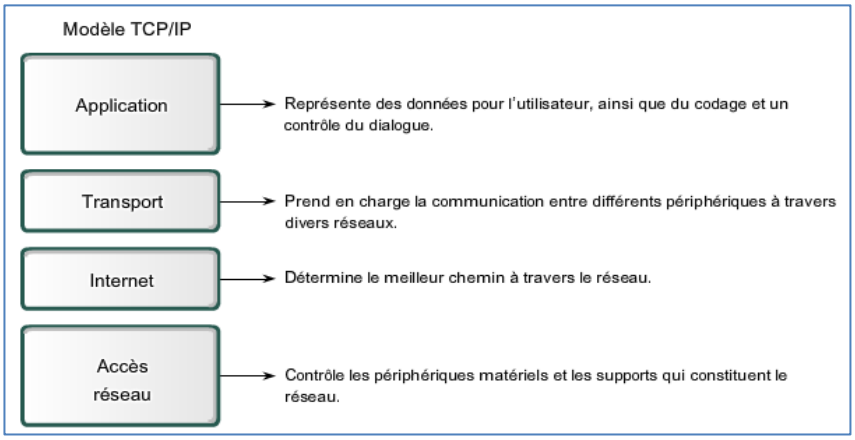
Lorsqu'une couche de l'émetteur construit des données, elle encapsule ces dernières avec ses informations puis les passe à la couche inférieure. Le mécanisme inverse a lieu au niveau du destinataire ou une couche réceptionne les données de la couche inférieure, enlève les informations la concernant, puis transmet les informations restantes à la couche supérieure. Les données transitant à la couche N de la source sont donc les mêmes que les données transitant à la couche N du destinataire.

Pour identifier les données lors de leur passage au travers d'une couche, l'appellation PDU (Unité de données de protocole) est utilisée :

- Données : terme général pour les unités de données de protocole utilisées au niveau de couches application, présentation et session.
- Segment : unité de données de protocole de la couche transport
- Paquet : unité de données de protocole de la couche réseau
- Trame : unité de données de protocole de la couche d'accès au réseau
- Bits : unité de données de protocole utilisée lors de la transmission physique de données à travers le support

2- Modèle TCP/IP

TCP/IP est un modèle comprenant 4 couches :



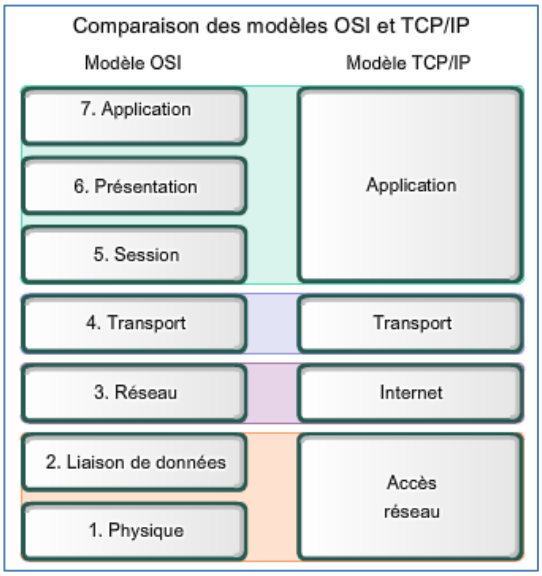
3- Comparaison : TCP/IP et OSI

Ces deux modèles sont très similaires, dans la mesure où les 2 sont des modèles de communication à couche et utilisent l'encapsulation de données.

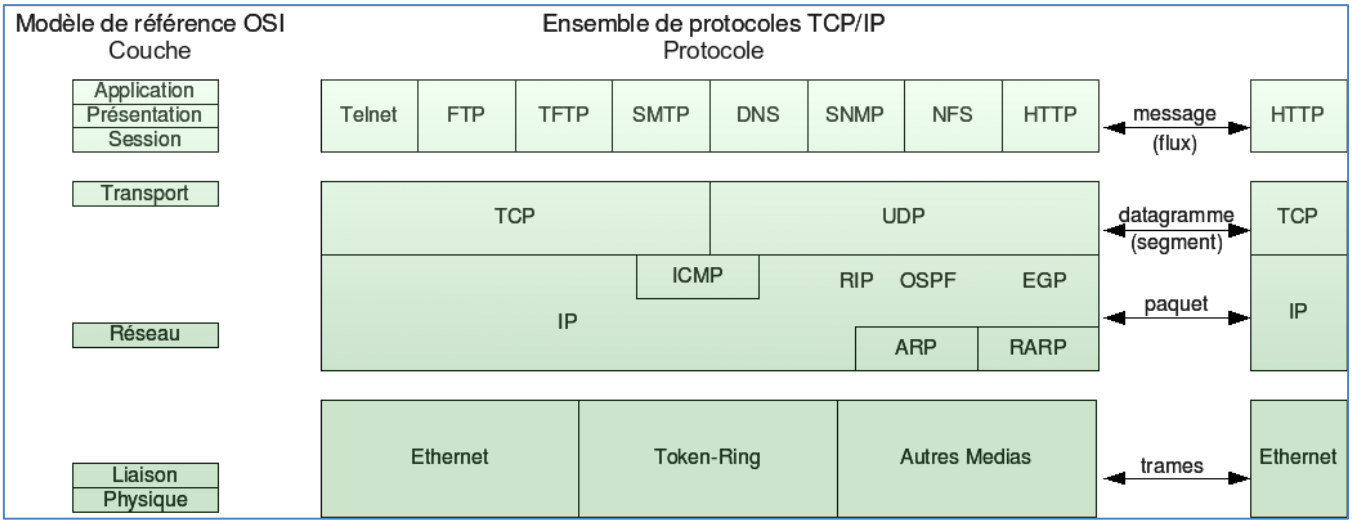
On remarque cependant deux différences majeures :

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

Internet actuel



4- La Pile des Protocoles TCP /IP



- Le protocole **DNS** (Domain Name Service) utilisé pour traduire les adresses Internet en adresses IP.
- Le protocole **HTTP** (Hypertext Transfer Protocol) est utilisé pour transférer les fichiers qui constituent les pages du Web.
- Le protocole **SMTP** (Simple Mail Transfer Protocol) est utilisé pour transférer les courriels et les pièces jointes.
- Le protocole **Telnet**, protocole d'émulation de terminal, est utilisé pour permettre un accès distant aux serveurs et aux périphériques réseau.
- Le protocole **FTP** (File Transfer Protocol) est utilisé pour le transfert interactif de fichiers entre les systèmes.
- Le protocole **DHCP** (Dynamic Host Configuration Protocol) est un service qui assigne aux clients des informations IP d'une manière automatique.
- Le protocole **IP** (Internet Protocol) est un protocole qui se charge de l'acheminement des paquets
- **TCP** (Transmission Control Protocol) est le protocole IP de niveau supérieur le plus répandu. TCP fournit un service sécurisé de remise des paquets. TCP fournit un protocole fiable, orienté connexion, au-dessus d'IP. TCP garantit l'ordre et la remise des paquets, TCP est responsable de la retransmission des paquets altérés ou perdus par le réseau lors de leur transmission.
- **UDP** (User Datagram Protocol) est un complément du protocole TCP qui offre un service sans connexion qui ne garantit ni la remise ni l'ordre des paquets délivrés.

Travail à faire :

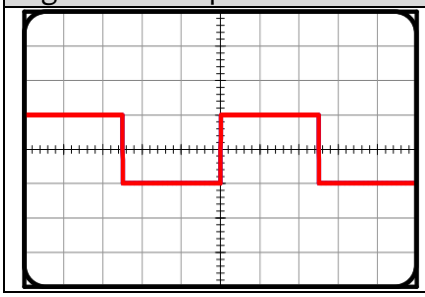
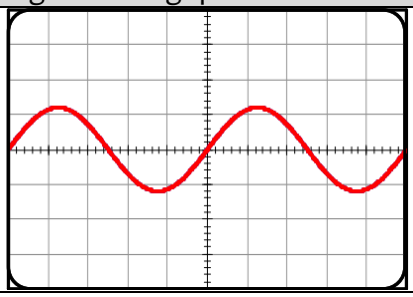
- Lire le chapitre 2
- Tester votre connaissance sur les principaux sujets abordés dans ce chapitre : 2.7.1.2
- Réaliser le questionnaire du chapitre : 2.8.1.1

Couche 1 : La couche physique

1- Les notions de base sur les signaux

1-1- signaux analogique et numériques

Lors de l'envoi de données sur un réseau, celles-ci transitent par des liaisons physiques, il convient donc d'observer comment sont-elles représentés dans ces liaisons.

Signal Numérique	Signal Analogique
	

Les deux caractéristiques importantes d'une onde sont son amplitude (**A**), c'est-à-dire sa hauteur et sa longueur, ainsi que sa période. La fréquence de l'onde peut être calculée avec cette formule : **f = 1/T**.

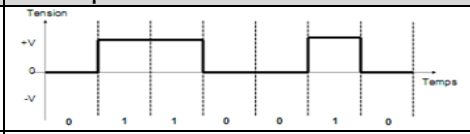
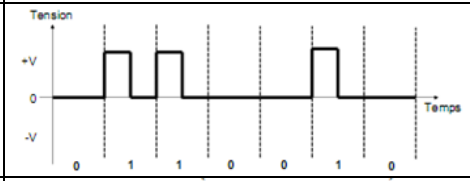
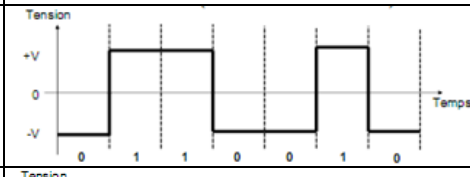
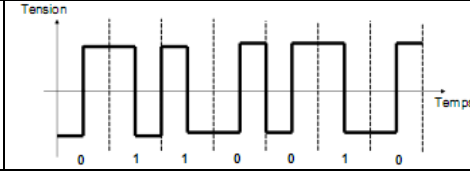
1-2- La représentation d'un bit : Codage et signalisation

Un bloc d'information est un élément binaire, connu sous le nom de bit ou impulsion. Un bit, dans un milieu électrique, est un signal correspondant à uno binaire ou à un 1 binaire. Cela peut être aussi simple que 0 (zéro) volts pour un 0 en binaire, et +5 volts pour un 1 binaire, ou un codage plus complexe.

- Méthodes de signalisation

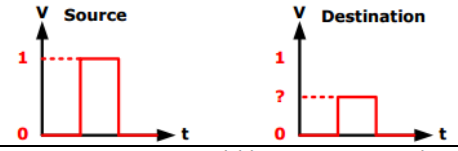
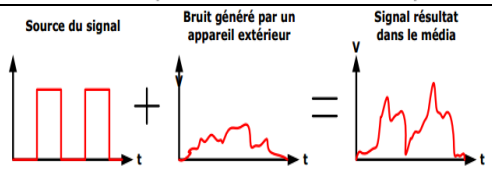
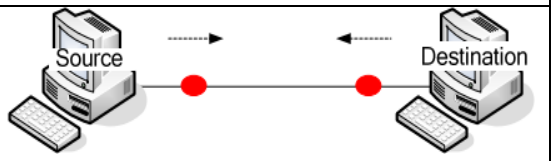
Les bits sont représentés sur le support en changeant une ou plusieurs des caractéristiques suivantes d'un signal : Amplitude, Fréquence et la Phase.

- Exemples de signalisation

Code	Description	Exemple
tout ou rien	Un courant nul code le '0' et un courant positif indique le '1'.	
RZ (Return to Zero)	Le '0' est codé par un courant nul et le '1' par un courant positif qui est annulé au milieu de l'intervalle	
NRZ (Non Return to Zero)	On code le 1 par un courant positif et le 0 par un courant négatif	
Manchester	Au milieu de l'intervalle il y a une transition de bas en haut pour un '0' et de haut en bas pour un '1'.	

1-3- Les facteurs pouvant affecter un bit

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

Nom de l'erreur	Description	figure
L'atténuation	Perte de la force du signal. Ce problème est limitable par un bon choix des médias réseau utilisés	
Le bruit	Ajout indésirable à un signal. Des sources d'énergie situées à proximité du média fournissent un supplément d'énergie venant perturber le signal.	
Les collisions	Se produit lorsque 2 ordinateurs utilisant le même segment de réseau émettent en même temps. Les impulsions se mélangent, détruisant alors les données.	

Il faut aussi savoir qu'une liaison entre 2 équipements A et B peut être :

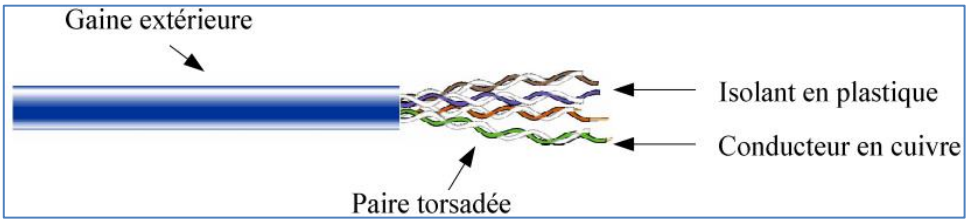
- Simple (unidirectionnelle) : A est toujours l'émetteur et B le récepteur.
- Half-duplex (bidirectionnelle à l'alternat) : Le rôle de A et B peut changer, la communication Change de sens à tour de rôle.
- Full-duplex (bidirectionnelle simultanée) : A et B peuvent émettre et recevoir en même temps.

2- LES SUPPORTS DE TRANSMISSION

2-1- Médias de cuivres

2-1-1- Le câble à paires torsadées non blindées (UTP)

Le câble UTP est composé de 4 paires de fils torsadées 2 à 2, chacune de ses paires étant isolées des autres. Ce câble compte uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal causée par une perturbation électromagnétique

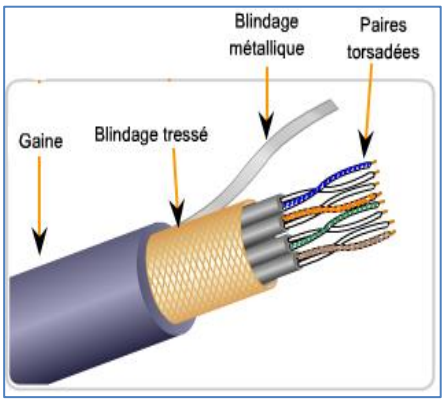


Avantages	Inconvénients
Simple à installer Peu coûteux Petit diamètre	Sensible aux bruits

2-1-2- Le câble à paires torsadées blindées (STP)

Le câble à paires torsadées et blindées, ou STP, ajoute aux spécifications de l'UTP une méthode de Blindage pour annuler l'effet du bruit sur le signal.

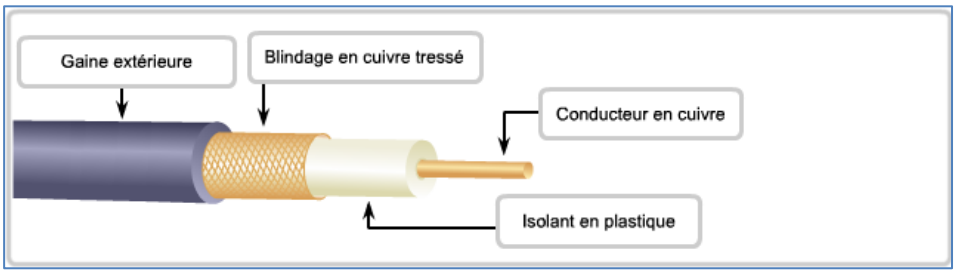
Le câblage STP offre une meilleure protection parasitaire que le câblage UTP, mais à un prix et un diamètre de la gaine relativement plus élevé.



2-1-3- Le câble coaxial

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

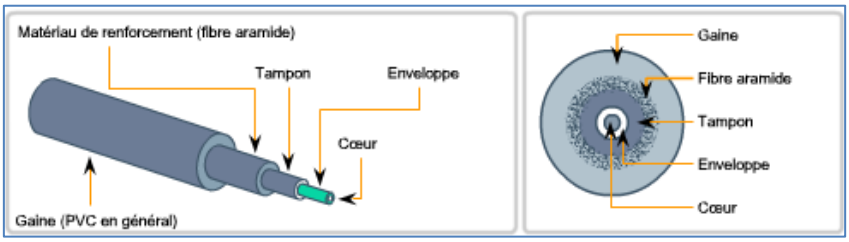
Le câble coaxial offre de nombreux avantages du fait de sa capacité à s'étendre sur une plus grande distance et de son coût parmi les plus faibles.



2-2- Médias Optiques

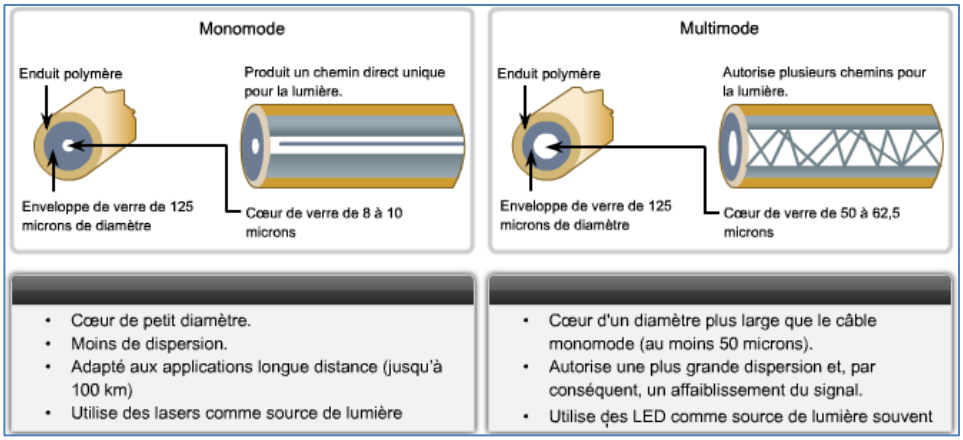
2-2-1- Fibre Optique

Le câblage en fibre optique utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination. Les bits sont codés sur la fibre comme impulsions lumineuses. Le câblage en fibre optique prend en charge des débits très élevés.
Une fibre optique transmet des données dans un sens seulement. Aussi pour que deux entités communiquent en full duplex, un câble optique doit contenir deux fibres optiques : l'une pour transmission et l'autre pour réception. Les fibres réunies ensemble dans un câble ne créent pas de bruit, car elles ne portent pas d'impulsions électriques qui pourraient induire des interférences électromagnétiques.



2-2-2- les types des fibres optiques

Les câbles à fibre optique peuvent être classés en deux grands types : monomode et multimode.



2-3- Mediaş sans fils

2-3-1- Fonctionnement d'un réseau sans fil

Les réseaux sans fils ou WLAN (pour Wireless WAN), réussissent à conjuguer tous les avantages d'un réseau filaire traditionnel comme Ethernet mais sans la limitation des câbles.
Un WLAN à également besoin, tout comme un LAN, d'un média. Au lieu de câbles à paires torsadées, les WLANs utilisent des fréquences radio à 2,4 GHz et 5 GHz.
En Juin 1997, L'IEEE publie les standards 802.11 pour les réseaux locaux sans fils.

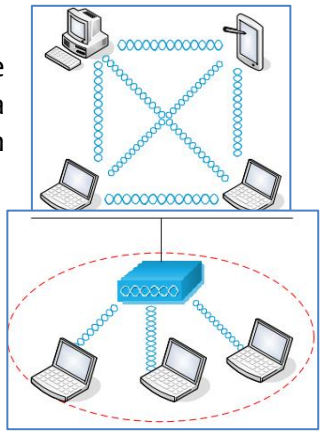
2-3-2- Nomes, fréquences et débits

Tableau récapitulatif des fréquences et débits :

	802.11b	802.11a	802.11g
Bande de fréquence	2,4 Ghz	5 Ghz	2,4 Ghz
Débit maximum	11 Mbps	54 Mbps	54 Mbps

2-3-3- Modes d'implémentations

Considérons deux stations équipées chacune d'une carte Wi-Fi, Nous avons deux possibilités de connecter ces stations entre elles :



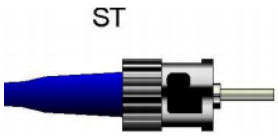
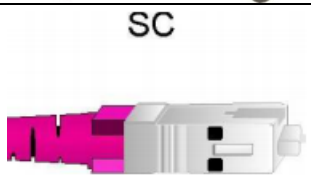
- **Le mode Ad-Hoc** apporte l'avantage de la mobilité. En effet, on peut mettre en réseau deux stations mobiles tant que chacune d'elles se situe dans la zone de couverture de l'autre, on peut donc facilement se déplacer tout en conservant la connectivité par exemple dans une salle de réunion.

- **Le mode infrastructure,** quant à lui, permet de connecter un réseau Wi-Fi à un réseau filaire (internet, ou d'entreprise par exemple). Cependant la mobilité d'une telle configuration est limitée à la zone de couverture de la/ les borne(s) reliée(s) au réseau filaire.

2-3-4- Avantages et inconvénients

Les avantages des technologies de communication de données sans fil sont évidents, en particulier les économies sur le câblage coûteux des locaux et le côté pratique lié à la mobilité des hôtes. Cependant, les administrateurs réseau doivent mettre au point et appliquer des processus et politiques de sécurité stricts pour protéger les réseaux locaux sans fil contre tout accès non autorisé et endommagement.

3- Les connecteurs

Medias	Connecteur	Figure
Media en cuivre UTP/STP	RJ45	
Câble coaxial	BNC	 
Fibre Optique	ST (Straight Tip) SC (Subscriber Connecter)	 
Sans fils	Adaptateur de la carte réseau sans fils	

4- Résumé (Comparatifs)

Voici un tableau récapitulant les différents types de câbles ainsi que leur débit :

Technologie	Type de câble	Débit théorique	Longueur Max	Connecteur	Coût
10 Base 2 (Thinnet)	Coaxial	10 Mbits/s	200 m	BNC	Peu cher
10 Base 5 (Thicknet)	Coaxial	100 Mbits/s	500 m	BNC	Peu cher
10 Base T	UTP cat 5	10 Mbits/s	100 m	RJ45	Bon marché
100 Base TX	UTP cat 5	100 Mbits/s	100 m	RJ45	Bon marché
10 Base FL	Fibre optique	10 Mbits/s	2000 m	SC	Elevé
100 Base FX	Fibre optique	100 Mbits/s	400 m	SC	Elevé

- Lire le chapitre 8
- Tester votre connaissance sur les principaux sujets abordés dans ce chapitre : 8.5.1.2
- Réaliser le questionnaire du chapitre : 8.6.1.1

3- Equipement de la couche Physique

3-1 Répéteur

Le répéteur est un composant actif. Son rôle est de régénérer et de resynchroniser le signal afin de pouvoir étendre la portée des câbles.

3-2 Concentrateur

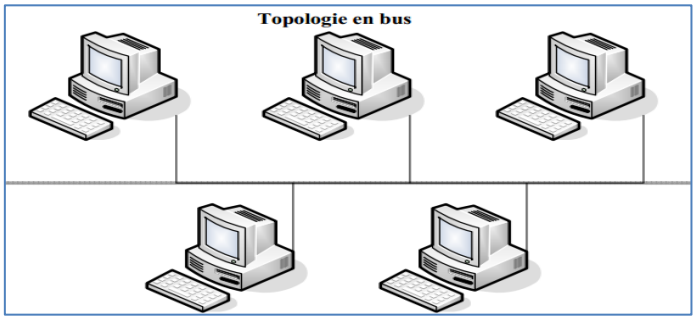
Le concentrateur, ou répéteur multi ports, reprend le fonctionnement du répéteur en ajoutant une fonctionnalité de connectivité. En effet, il dispose de plusieurs ports ce qui permet d'interconnecter plusieurs équipements réseau. Chaque signal arrivant sur un port est régénéré, resynchronisé et réémis Au travers de tous les autres ports.

4- Les topologies de base

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

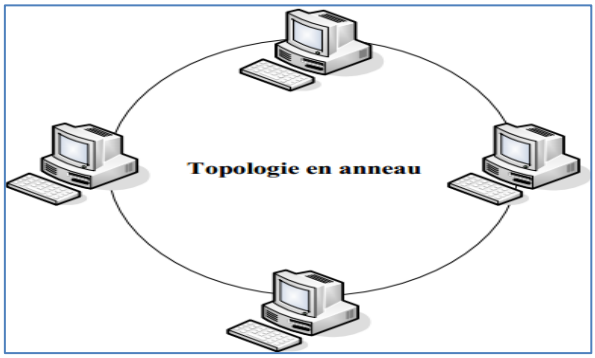
4-1- La topologie en bus

- Perspective physique: Tous les hôtes sont connectés directement à une liaison
- Perspective logique: Tous les hôtes voient tous les signaux provenant de tous les autres hotes



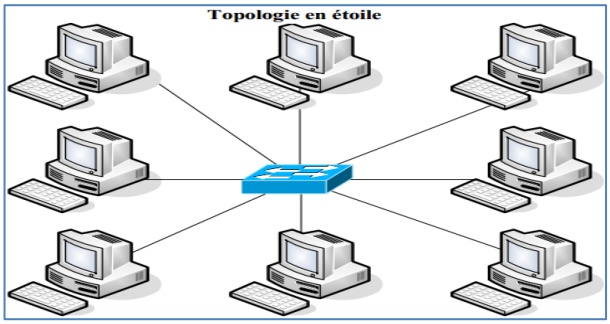
4-2- La topologie en anneau

- Perspective physique: Les éléments sont chaînés dans un anneau fermé
- Perspective logique: Chaque hôte communique avec ses voisins pour véhiculer l'information



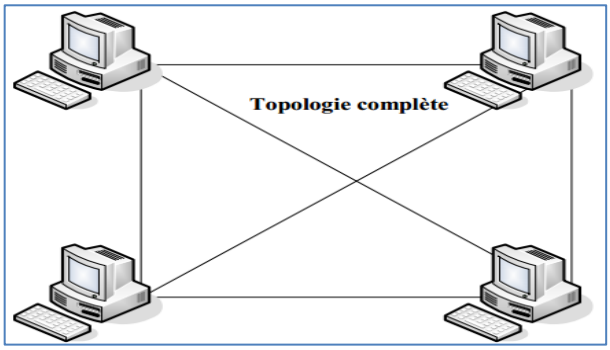
4-3- La topologie en étoile

- Perspective physique: Cette topologie comporte un nœud central d'où partent toutes les liaisons avec les autres nœuds.
- Perspective logique: Toutes les informations passent par un seul équipement, par exemple un concentrateur



4-4- La topologie complète (maillée)

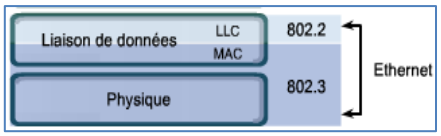
- Perspective physique: Chaque nœud est connecté avec tous les autres
- Perspective logique: Dépend des équipements utilisés



La couche 2 : Couche Liaison de données

1- Technologies Ethernet

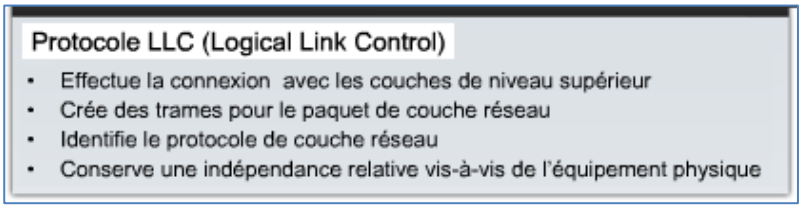
La technologie Ethernet opère au niveau de la couche physique et de la couche liaison de données (la couche MAC seulement).



L'institut IEEE l'a normalisé et adapté dans son modèle IEEE 802.3. Ces deux technologies sont très similaires (elles diffèrent sur un champ de trame seulement).

1-1- Sous Couches : LLC et MAC

Ethernet sépare les fonctions de la couche liaison de données en deux sous-couches distinctes : la sous-Couche LLC (Logical Link Control) et la sous-couche MAC (Media Access Control).



1-2- Spécifications et normes

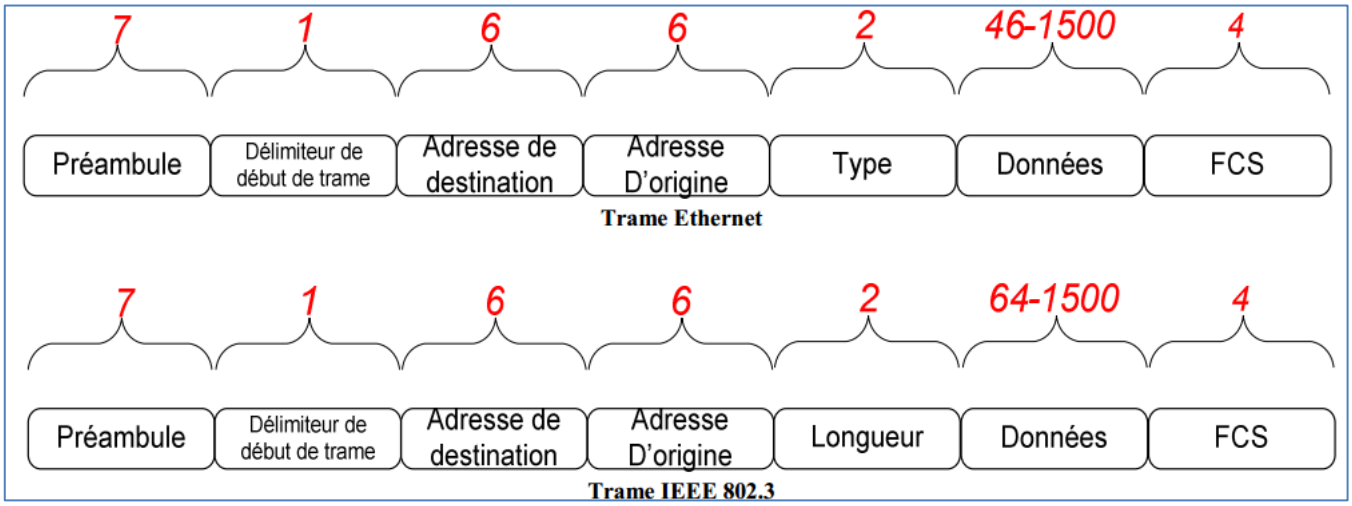
Chaque désignation de technologie utilise une normalisation qui permet d'identifier ses caractéristiques. Celles-ci sont de la forme : vitesse en Mbps – type de signal – type de câble. (ex :100 Base TX)

- Deux types de signalisation existent : Baseband (transmission numérique) ou Broadband (utilisation de porteuse : transmission par ondes par exemple).
- Le type de câble utilisé : cuivre à paires torsadées non blindé (Unshielded Twisted Pairs), ou de type fibre optique (Fiber).
- On exprime aussi sa capacité à supporter le Full Duplex par un X. (à l'exception du 10 Base T qui supporte tout de même le mode Full Duplex).

L'IEEE a défini des normes pour les différentes technologies Ethernet :

Norme	Appellation	Débit	Média utilisé
802.3	Ethernet	10 Mbps	Coaxial / UTP / fibre optique
802.3u	Fast Ethernet	100 Mbps	UTP / Fibre optique
802.3z	Gigabit Ethernet	1000 Mbps	Fibre optique
802.3ab	Gigabit Ethernet	1000 Mbps	Câble UTP
802.3ae	10 Gigabit Ethernet	10 000 Mbps	Fibre Optique

1-3- Trames Ethernet et IEEE 802.3

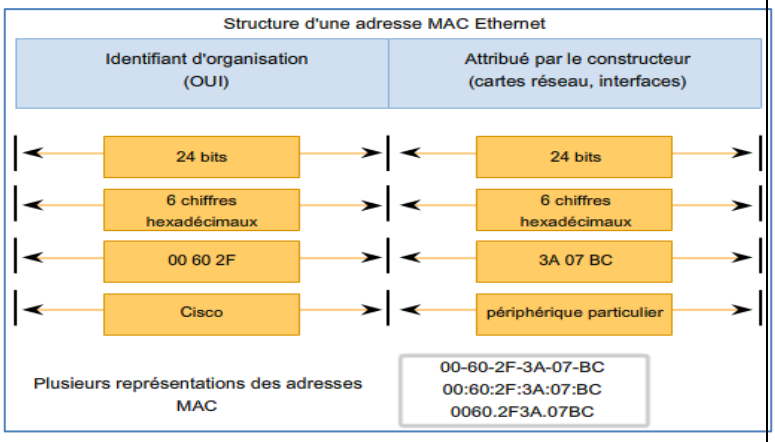


- **Préambule:** annonce si la trame est de type Ethernet ou 802.3
- **Début de trame:** IEEE 802.3 : l'octet séparateur se termine par 2bits à 1 consécutifs, servant à synchroniser les portions de réception des trames de toutes les stations.
- **Champ d'adresse de destination:** peut-être de type unicast, multicast ou broadcast.
- **Champ d'adresse d'origine:** toujours de type unicast.
- **Type (Ethernet):** précise le type de protocole de couche supérieure qui reçoit les données.
- **Longueur (802.3):** indique le nombre d'octets de données qui suit le champ.
- **Données:** ce champs contient les données encapsulées d'une couche supérieure qui est une unité de données de protocole de couche 3
- **FCS:** Séquence de contrôle de trame. Cette séquence contient un code de redondance

Cyclique permettant à l'unité réceptrice de vérifier l'intégrité des données transmises.

1-4- Les adresses MAC (Adresse physique)

Une adresse MAC Ethernet est une valeur binaire de 48 bits exprimées sur 12 chiffres hexadécimaux, elle a été créée pour pouvoir identifier d'une manière unique un équipement sur le réseau.
(L'adresse MAC est souvent dite rémanente car elle est stockée dans la mémoire morte de la carte réseau).

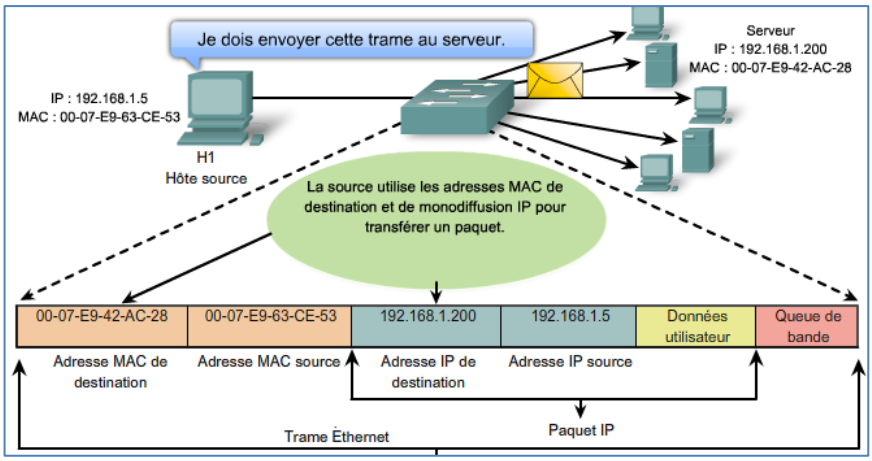


Pour visualiser l'adresse MAC de votre ordinateur, utilisez la commande ipconfig /all :

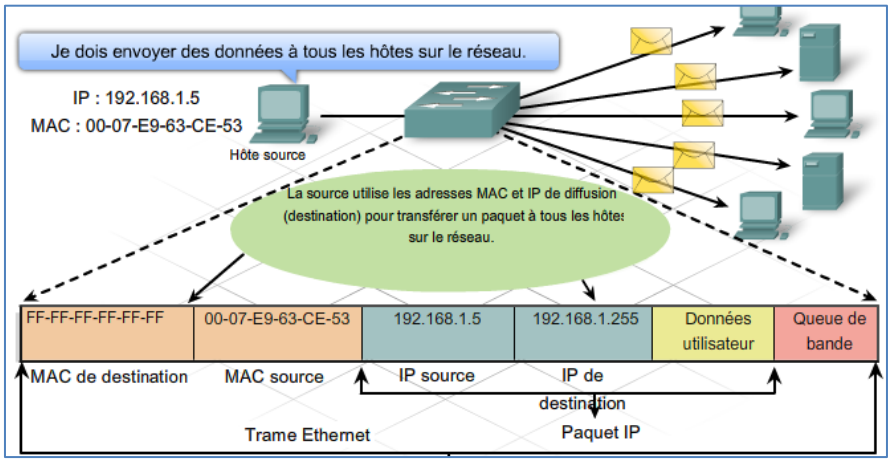
```
C:\>ipconfig /all
Ethernet adapter Network Connection:
        Connection-specific DNS Suffix: example.com
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless
Connection
        Physical Address. . . . . . . . . : 00-18-DE-C7-F3-FB
        Dhcp Enabled. . . . . . . . . . . : Yes
```

1-5- Trame ETHERNET : Monodiffusion-Multidiffusion et Diffusion

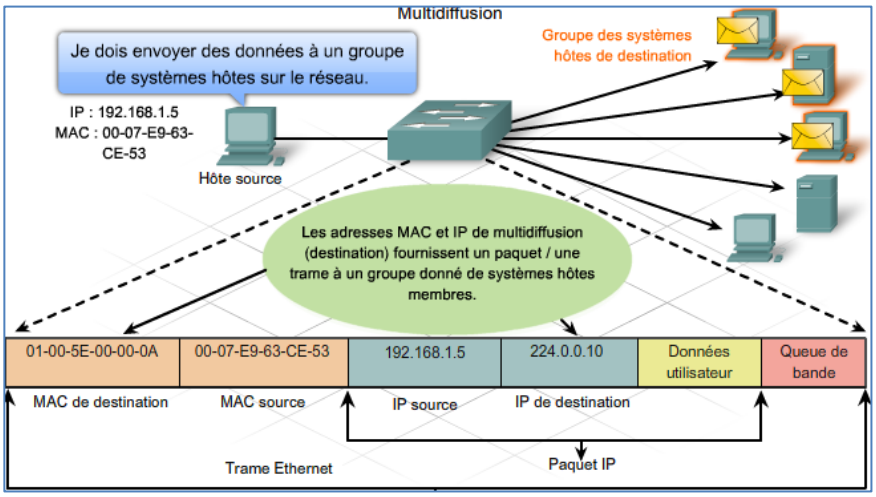
Monodiffusion (monocast): Adresse MAC de monodiffusion utilisée lorsqu'une trame est envoyée à partir d'un seul périphérique de transmission, à un seul périphérique de destination.



Diffusion (broadcast) : Adresse MAC de diffusion utilisée lorsqu'une trame est envoyée à partir d'un seul périphérique de transmission, à tous les périphériques de réseau.



Multidiffusion (multicast) : Adresse MAC de Multidiffusion utilisée lorsqu'une trame est envoyée à partir d'un seul périphérique de transmission, à un groupe des périphériques de réseau.



1-6- la méthode d'accès CSMA/CD

Dans un environnement où plusieurs hôtes se partagent un média unique de communication, un problème de priorité doit être résolu. Le problème est le même que dans une situation courante : lors d'une discussion à l'intérieur d'un groupe de personnes, une seule personne parle à la fois si elle veut être comprise par son ou ses interlocuteurs.
Dans un environnement Ethernet, c'est au niveau de la sous-couche MAC que l'on va utiliser un processus de détection des collisions : plusieurs hôtes émettent en même temps sur le même média. Ethernet et 802.3 utilisent un principe d'accès au média non déterministe : CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
Les hôtes se partagent donc le média. Si l'un d'eux désire émettre, il vérifie au préalable que personne n'est en train de le faire, puis commence à émettre(CSMA).
Si cependant 2 hôtes émettent en même temps, il se produit alors une collision. La première station qui Détecte une collision envoie alors un signal de bourrage, se traduisant par un arrêt d'émission de tous les hôtes. Les paquets concernés sont alors détruits.
Chaque hôte calcule alors une valeur aléatoire définissant la durée avant de recommencer à émettre, puis le mécanisme de CSMA se remet en fonction.

2- PRINCIPE DE COMMUTATION

2-1- Domaine de collision

On appelle domaine de collision la partie d'un réseau comprenant un environnement partagé. C'est dans ce domaine que les hôtes vont accéder en concurrence à une ressource. De ce fait, des collisions vont se créer sur cette partie du réseau. Le domaine de collision s'étend sur la plus grande partie du réseau contenant des équipements de couche 1 interconnectés.

2-2- Segmentation de réseau

Les domaines de collision posent des problèmes, proportionnellement à leur taille. En effet, plus un domaine de collision est grand (mesuré en nombre d'hôtes), plus la bande passante par hôte est faible, et plus le nombre d'erreurs est grand.
Pour diminuer ces effets néfastes, il suffit de segmenter un domaine en plusieurs, de tailles inférieures.
On aura alors moins de collisions par segment, donc une plus grande fiabilité et une meilleure bande passante.
Le principe de la segmentation est de n'envoyer des données que sur la portion de réseau concernée. On va ainsi réduire le trafic inutile, ainsi que le nombre d'utilisateurs concurrents du même média.
Pour la segmentation, des équipements de couche 2 sont nécessaires. C'est à ce niveau que l'on peut prendre des décisions d'adressage (sur quel média transmettre une trame).

2-2-1- Segmentation par pont

Les ponts permettent de segmenter un réseau en n'envoyant les données que sur la partie du réseau concernée. Après avoir appris sur quelle portion setrouvent les hôtes (par leur adresse mac), un pont filtrera le trafic suivant l'adresse de destination. Il laissera donc transiter les données vers la partie du réseau qui contient l'adresse de destination, et bloquera les paquets qui ne sont pas destinés à cette même partie.

2-2-2- Segmentation par Commutateur

Les commutateurs sont l'équivalent de répéteurs multi ports intelligents. Chaque hôte où groupe d'hôtes connecté à un port du commutateur veut envoyer des données. Au lieu de retransmettre ces données

sur chaque port, le commutateur ne va renvoyer que sur le port où se trouve la partie du réseau contenant le(s) destinataire(s).
Pour se faire, le commutateur va apprendre les adresses MAC de chaque hôte connecté à ses ports. Il saura ainsi quels hôtes se trouvent sur chacun de ses ports. Il stocke ces données dans une table d'adresses MAC.
Les commutateurs fonctionnent beaucoup plus vite que les ponts et créent des domaines sans collisions entre 2 ports en interne

Exercice :
Page 9.6.3.1

3- Protocole ARP (Address Resolution Protocol)

Le protocole ARP assure deux fonctions de base :

- la résolution des adresses IPv4 en adresses MAC
- la conservation en mémoire cache des mappages.

Les processus ARP envoient un paquet de requête ARP pour trouver l'adresse MAC du périphérique de destination sur le réseau local. Si le périphérique qui reçoit la requête possède l'adresse IP de destination, il répond à l'aide d'une réponse ARP. Une entrée est créée dans la table ARP. Les paquets à destination de cette adresse IPv4 peuvent à présent être encapsulés dans des trames.

Commande Windows : arp –a => pour voir les entrées Arp

Travail à faire :

- Lire le chapitre 9
- Tester votre connaissance sur les principaux sujets abordés dans ce chapitre : 9.9.1.1
- Réaliser le questionnaire du chapitre : 9.10.1.1

COUCHE 3 : COUCHE RESEAU

1- ADRESSAGE

1-1- Protocoles Orientés connexion et protocoles non orientés connexion

Un protocole orienté connexion (tels que TCP) exige l'échange de données de contrôle pour établir la connexion. Il définit un chemin unique entre l'hôte source et l'hôte de destination. Plus

Un protocole non orienté connexion (tels que UDP) ne nécessite aucun échange initial d'informations pour établir une connexion avant le transfert des paquets. Il ne définit pas un chemin unique pour acheminer les paquets d'un hôte source vers un hôte destination. Les paquets peuvent alors emprunter des chemins différents.

1-2- Protocoles routables et non routables

Un protocole routable : définit la notion d'adressage hiérarchique : un hôte est défini par une adresse unique sur un segment de réseau unique. Les messages envoyés à l'aide de ce protocole peuvent sortir de leur réseau (via un routeur).

Un protocole non routable : les messages envoyés à l'aide de ce protocole ne peuvent pas sortir de leur réseau.
La liste des protocoles routés suivante présente les protocoles les plus connus :

Nom du protocole routé	Protocole routable ?
IP	Oui
IPX	Oui
Appletalk	Oui
NetBEUI	Non
SNA	Non

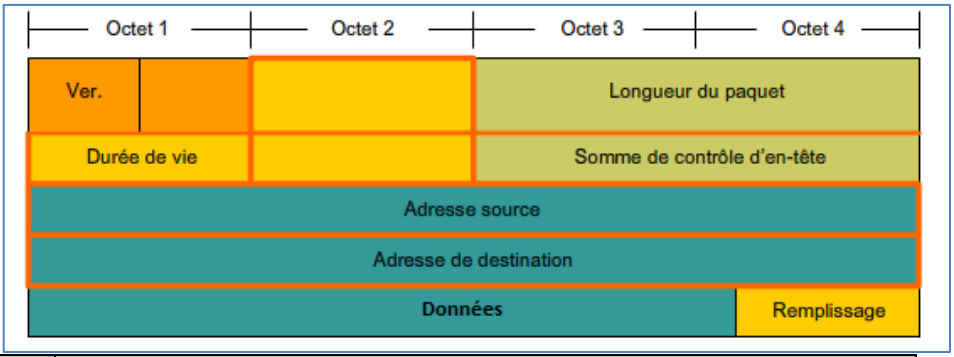
1-3- Le protocole IP (Internet Protocol)

Le protocole IP (IPv4 et IPv6) constitue le protocole de la couche 3 le plus répandu. Les caractéristiques du protocole IP sont :

- **Sans connexion** : aucune connexion n'est établie avant l'envoi de paquets de données.
- **Au mieux (peu fiable)** : aucune surcharge n'est utilisée pour garantir la transmission des paquets.
- **Indépendant des médias** : fonctionne indépendamment du média transportant les données.

1-3-1- Le Paquet IP

Les informations provenant de la couche 4 sont encapsulées dans le PDU de couche 3 : le paquet, dont voici les principaux éléments :

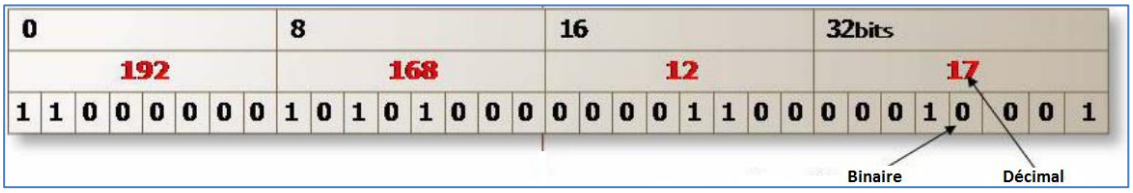


Champs	Description
Version	Indique la version de protocole IP utilisée (4 bits)
Longueur du paquet	Précise la longueur du paquet IP en entier, y compris les données et l'en-tête, en octets (16 bits)
Durée de vie	Un compteur qui décroît graduellement, par incréments, jusqu'à zéro. À ce moment, le datagramme est supprimé, ce qui empêche les paquets d'être continuellement en boucle (8 bits).
Somme de contrôle d'en-tête	Assure l'intégrité de l'en-tête IP (16 bits).
Adresse source	Indique le nœud émetteur (32 bits).
Adresse de destination	Indique le nœud récepteur (32 bits).
Données	Cet élément contient des informations de couche supérieure (longueur variable, maximum 64 Ko).
Remplissage	Des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP soit toujours un multiple de 32 bits.

1-3-2- Les adresses IP

Une adresse IP est une adresse 32 bits notée sous forme de 4 nombres décimaux séparés par des points. On distingue en fait deux parties dans l'adresse IP :

- Une partie réseau (on l'appelle netID)
- Une partie hôte (on l'appelle host-ID)



1-3-3- Le masque de réseau (masque par défaut)

Le masque de réseau permet d'identifier les parties NETID et HOSTID d'une adresse IP. Chaque adresse IP possède un masque réseau.

Règle :
Pour Calculer le masque on met tous les bits du NETID à **1** et les bits de HOSTID à **0**
Exemple :
255.0.0.0 : 8 bits NETID et 24 bits HOSTID
Notation cadencée (CIDR) : Adresse IP / Nombre de bit a 1 dans le masque

1-3-4- Les classes des adresses IP

Classe	1ier Octet	Masque par défaut	NETID	HOSTID	Nbr de SR	Nbr Machines/SR
A	**0 ➔ 127**	**255.0.0.0**	**8 bits**	**24 bits**	2^8	2^{24}-2
B	**128 ➔ 191**	**255.255.0.0**	**16 bits**	**16 bits**	2^{16}	2^{16}-2
C	**192 ➔ 223**	**255.255.255.0**	**24 bits**	**8 bits**	2^{24}	2^8-2
D	**224 ➔ 239**	**Adresses de multicast (multidiffusion)**				
E	**240 ➔ 247**	**Adresses Réservés pour les expérimentations**				

1-3-5- Adresse Réseau

Une adresse Réseau est utilisée pour identifier la partie Réseau (NETID).

Règle :
Pour Calculer une adresse réseau on garde le NETID fixe et on met tous les bits du HOSTID à **0**
Exemple :
Adresse IP : 192.168.30.5, le masque par défaut est 255.255.255.0 ➔ Adresse Réseau : 192.168.30.0

1-3-6- Adresse de Diffusion (Broadcast)

Une adresse de diffusion est utilisée pour envoyer des paquets à tous les hôtes d'un réseau

Règle :
Pour Calculer une adresse de diffusion on garde le NETID fixe et on met tous les bits du HOSTID à **1**
Exemple :
Adresse IP : 192.168.30.5, le masque est 255.255.255.0 ➔ Adresse de diffusion : 192.168.30.255

1-3-7- les Adresses Réservés (Non autorisées)

Adresse	Description
0.0.0.0	Inutilisable car non reconnue sur les réseaux
Plage 127.0.0.0	Adresse de loopback ou boucle locale utilisée pour tester la configuration TCP/IP sur la machine locale.
Adresse Réseau	Utilisée pour identifier un réseau
Adresse de diffusion	Utiliser pour envoyer un paquet de diffusion

1-3-8- les Adresses privés et public

Les Adresses privées sont utilisées dans les réseaux qui ne sont pas directement connectés au réseau internet.

Classe	Plage d'adresse IP
A	10.0.0.0 ➔ 10.255.255.255
B	172.16.0.0 ➔ 172.31.0.0
C	192.168.0.0 ➔ 192.168.255.255

1-3-9- Calcul de nombre des machines et de réseaux

Règle :
- Pour Calculer le nombre des hotes dans un réseau : 2^n-2 (n est le nombre de bits de HOSTID).
- Pour calculer le nombre de Réseau : 2^m (m est le nombre de bits de NETID).

Classe	Masque par défaut	Nombre de machines /R	Nombre de Réseaux
A	255.0.0.0	2^{24}-2	2^8
B	255.55.0.0		
C			

1-4- les protocoles de la couche Réseaux

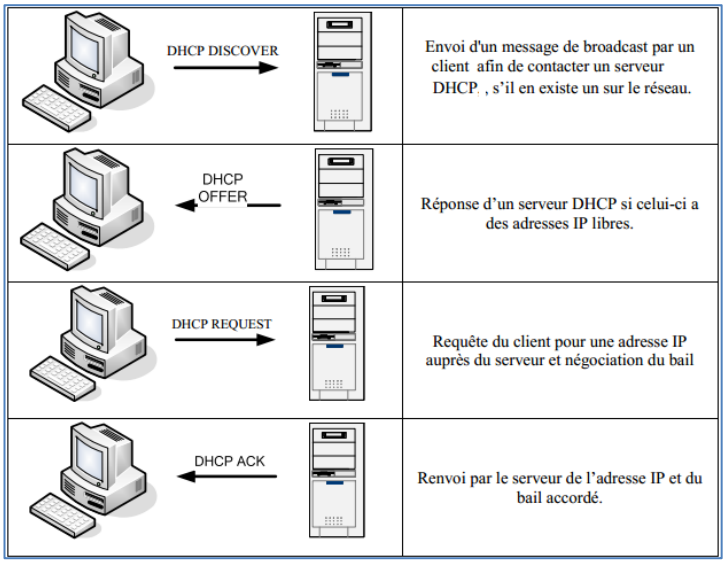
- **Le protocole ICMP** (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs générées au sein d'un réseau IP. Un exemple typique d'utilisation du protocole ICMP est la commande ping.
- **Le protocole RARP** (Reverse Address Resolution Protocol) permet de connaître l'adresse IP d'un hôte, à partir de son adresse physique.
  Lorsqu'une machine ne connaît que l'adresse physique d'un dispositif, elle peut émettre une requête RARP afin d'avoir son adresse IP.
- **Le protocole ARP** (Address Resolution Protocol) permet d'identifier l'adresse physique d'un hôte (adresse MAC unique) à partir de son adresse IP.

1-5- Méthodes d'obtention d'une adresse IP

On distingue 2 méthodes d'attribution d'adresses IPpour les hôtes :

- Statique: chaque équipement est configuré manuellement avec une adresse unique
- Dynamique: On utilise des protocoles qui attribuent des IP aux hôtes (RARP, DHCP, BOOTP)

DHCP: Remplaçant de BOOTP, il permet l'obtention dynamique d'IP. Lorsqu'un ordinateur entre en ligne, il communique avec le serveur qui choisit une adresse et un masque de sous réseau et l'attribue à l'hôte. Il permet de plus d'obtenir des serveurs DNS et la passerelle par défaut.



1-6- Les équipements de couche 3 : les routeurs

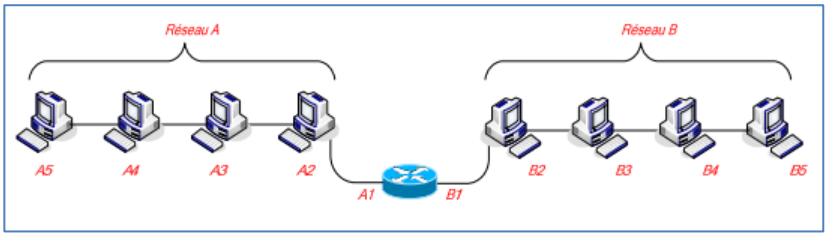
Routeur :

Équipement de couche 3 permettant d'interconnecter deux réseaux ou plus en se basant sur les adresses de couche 3. Le routeur permet également une segmentation des domaines de broadcast et des domaines de collisions.

Le routeur dispose d'une interface (une carte réseau) le reliant au réseau local. Celle-ci dispose d'une adresse IP.

Par exemple, sur le schéma ci-dessous, les adresses des hôtes sont A5, A4, A3 et A2, faisant partie du réseau A. On attribue A1 à l'interface du routeur (**la passerelle par défaut** pour les machines A5, A4, A3 et A2), lui permettant ainsi de se connecter au réseau A.

Un autre réseau, B, est lui aussi connecté au routeur. Ce dernier dispose donc d'une interface ayant pour IP B1 afin de pouvoir communiquer avec le réseau.



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

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

1-7- Domaine de broadcast

Un domaine de broadcast est un domaine logique ou n'importe quels hôtes connectés à un réseau peuvent envoyer des données à une autre machine sans passer par des services de routage.

Plus spécifiquement c'est un segment réseau composé d'hôtes et de dispositifs pouvant être atteint en envoyant un paquet à l'adresse de broadcast. Ces domaines de broadcast sont toujours séparés par des dispositifs de couche 3.

Généralement, les concentrateurs et commutateurs conservent le même domaine de diffusion, alors que les routeurs les divisent.

Rappel : Domaine de collision

Un domaine de collision est une zone logique d'un réseau informatique où les paquets de données peuvent entrer en collision entre eux, dans un reseau Ethernet. Un domaine de collision peut être un seul segment de câble Ethernet, un seul concentrateur ou même un réseau complet de concentrateurs et de répéteurs.
Généralement, un concentrateur forme un seul domaine de collision alors qu'un commutateur ou un routeur en crée un par port, ce qui réduit les risques de collision.

Figure 1 :

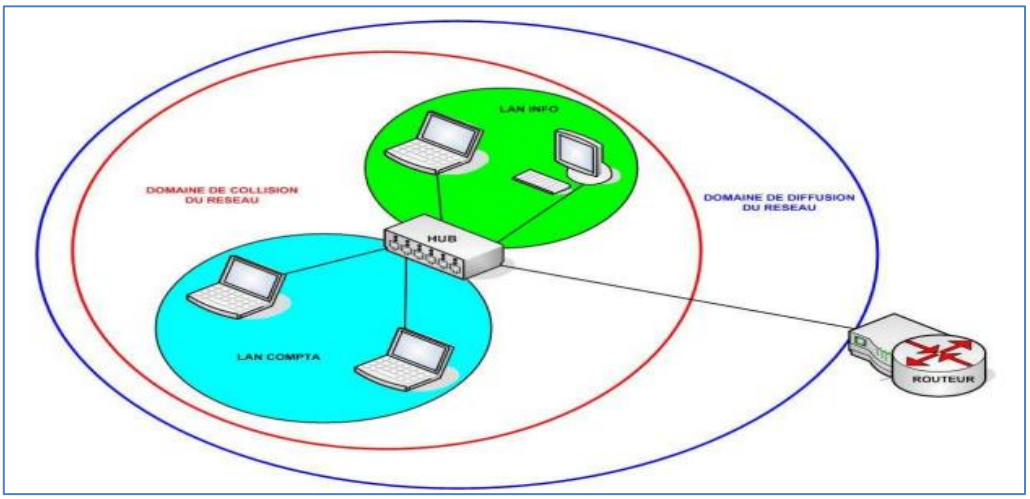


Figure 2 :

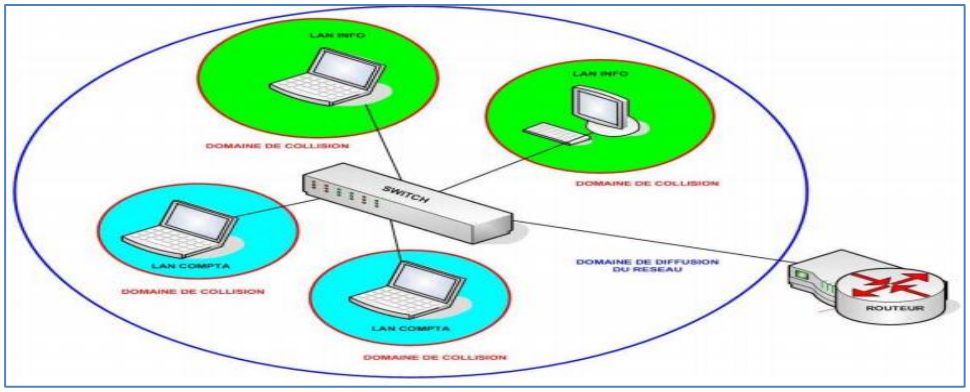


Figure 3 :

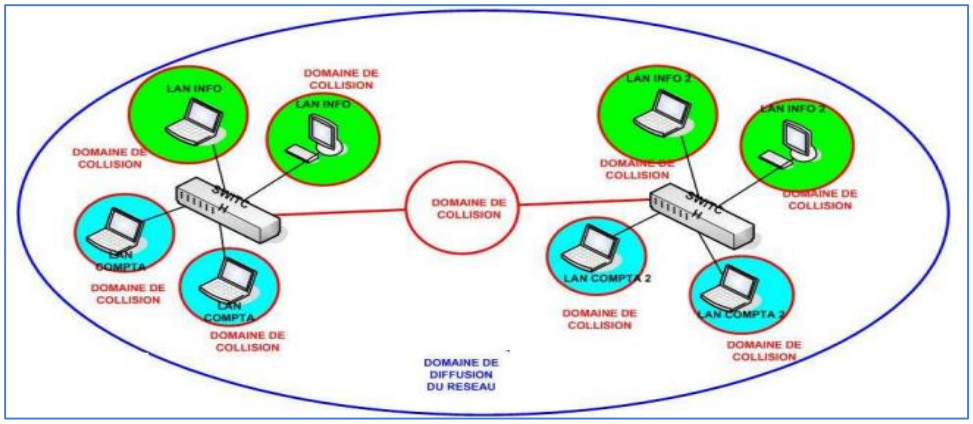


Figure 4 :

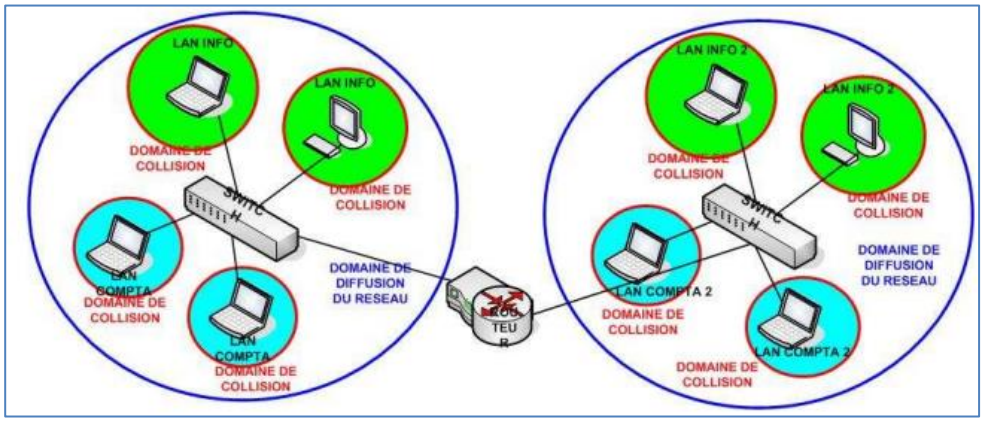


Figure 5 :