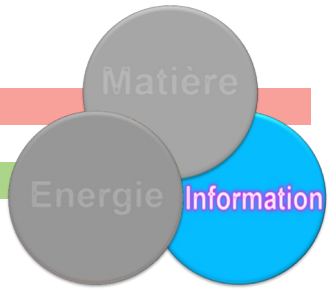
STI2D	Thème N°1.A : Réseaux et communications informatiques	LA MACHE
SIN - Terminale		



Durée prévue : 10h

Objectifs :

- Être capable de caractériser un réseau informatique
- Être capable d'analyser une communication informatique

Prérequis :

- Connaissance du binaire, décimal, ….
- Connaissances de base sur les réseaux (voir les TP)

Modalités :

- cours + TP

Documents ressources :

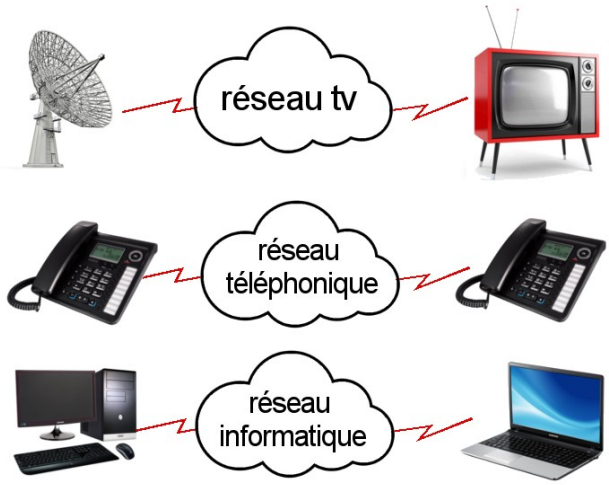
- site internet et fichier numérique

Plan de l'étude :

I. Introduction..... 1
II. Réseaux informatiques..... 2
1. Principes généraux..... 2
2. Éléments d'un réseau..... 5
3. Adresses des éléments d'un réseau..... 7
4. Le modèle de référence OSI..... 11
5. Comparaison des modèles OSI et TCP/IP..... 13
6. Principe de l'adressage et de l'encapsulation..... 13
7. Topologie des réseaux..... 14
IV. Exercices..... 20

I. Introduction

De l'idée de faire communiquer des ordinateurs entre eux est née l'idée de réseau informatique. Au début il s'agissait de faire communiquer 2 ordinateurs puis plusieurs autres. Maintenant avec la généralisation des communications informatiques on constate que des moyens de communication autrefois séparés convergent en un réseau commun (et mondial). De même autrefois, chacun de ces services nécessitait une technologie différente pour acheminer son signal de communication particulier. Ainsi chaque service avait son propre ensemble de règles et de normes destiné à gérer les communications de ses services sur un support spécifique. Les progrès technologiques nous permettent aujourd'hui de réunir ces réseaux disparates sur un même réseau global.



Autrefois les réseaux étaient séparés

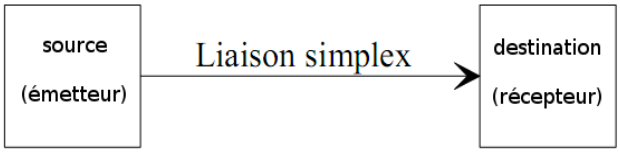
Aujourd'hui on a des réseaux convergents (un réseau global)

II. Réseaux informatiques

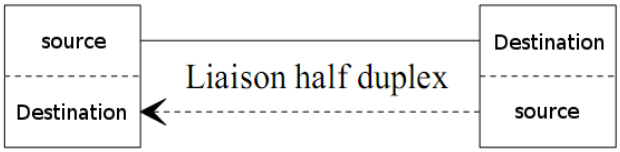
1. Principes généraux

On peut considérer 3 cas de communications entre éléments :

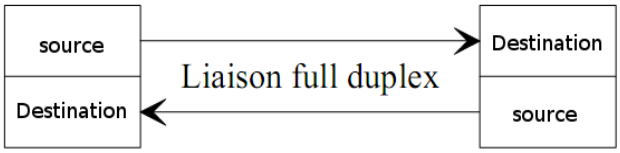
Lorsque l'échange a lieu dans une seule direction, on parle de liaison **simplex**.



Si les éléments peuvent, alternativement, remplir les fonctions d'émetteur et de récepteur, la liaison est dite: **half duplex**.



Lorsque l'échange peut s'effectuer en même temps dans les deux sens la liaison est appelée bidirectionnelle intégrale ou **full duplex**.

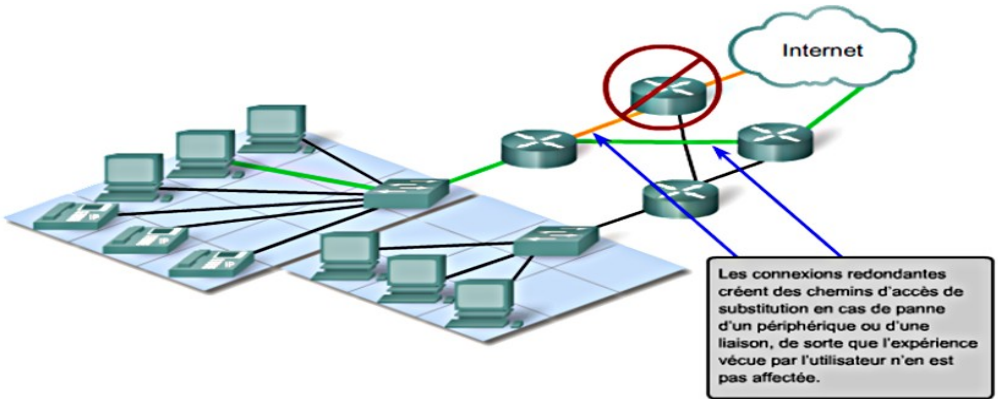


Quelques contraintes :
Les réseaux doivent d'une part prendre en charge une large gamme d'applications et de services et d'autre part fonctionner sur de nombreux types d'infrastructures physiques. Aujourd'hui, l'expression «

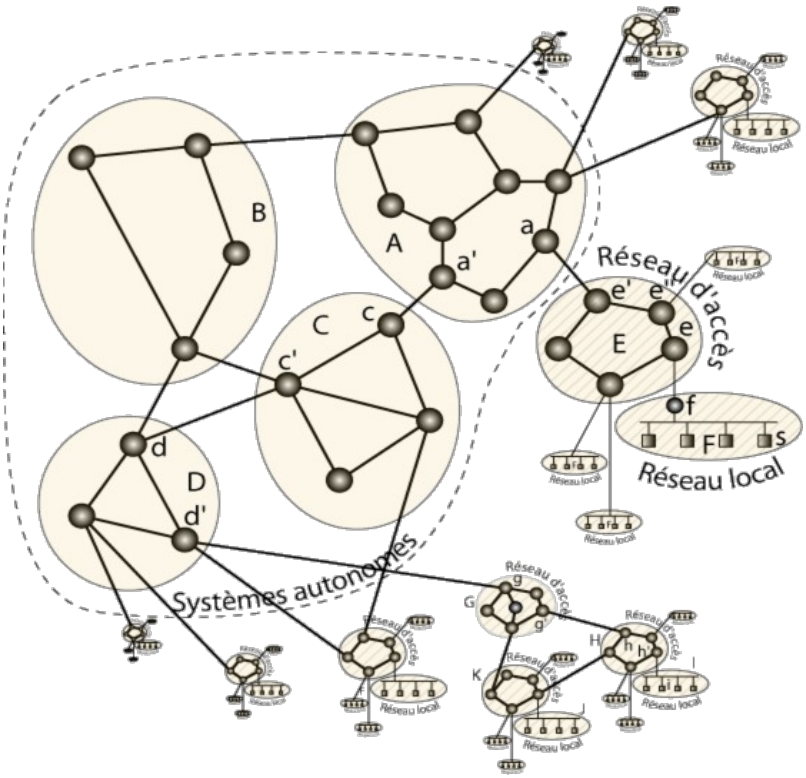
architecture réseau » désigne aussi bien les technologies prenant en charge l'infrastructure (le hardware) que les services programmés et les protocoles qui déplacent les messages dans l'infrastructure (le software). Alors qu'Internet, et les réseaux en général, évoluent, nous découvrons que les architectures sous-jacentes doivent prendre en considération quatre caractéristiques de base si elles veulent répondre aux attentes des utilisateurs : tolérance aux pannes, évolutivité, qualité de service et sécurité.

Tolérance aux pannes (exemple avec le réseau Internet):

Comme des millions d'utilisateurs attendent d'Internet qu'il soit constamment disponible, il faut une architecture réseau conçue et élaborée pour tolérer les pannes. Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes du matériel et des logiciels et qui peut être rétabli rapidement quand des pannes se produisent. De tels réseaux dépendent de liaisons, ou chemins, redondantes entre la source et la destination d'un message. En cas de défaillance d'une liaison (ou chemin), les processus s'assurent que les messages sont instantanément routés sur une autre liaison et ceci de manière totalement transparente pour les utilisateurs aux deux extrémités. Aussi bien les infrastructures physiques que les processus logiciels qui dirigent les messages sur le réseau sont conçus pour prendre en charge cette redondance. Il s'agit d'une caractéristique essentielle des réseaux actuels.

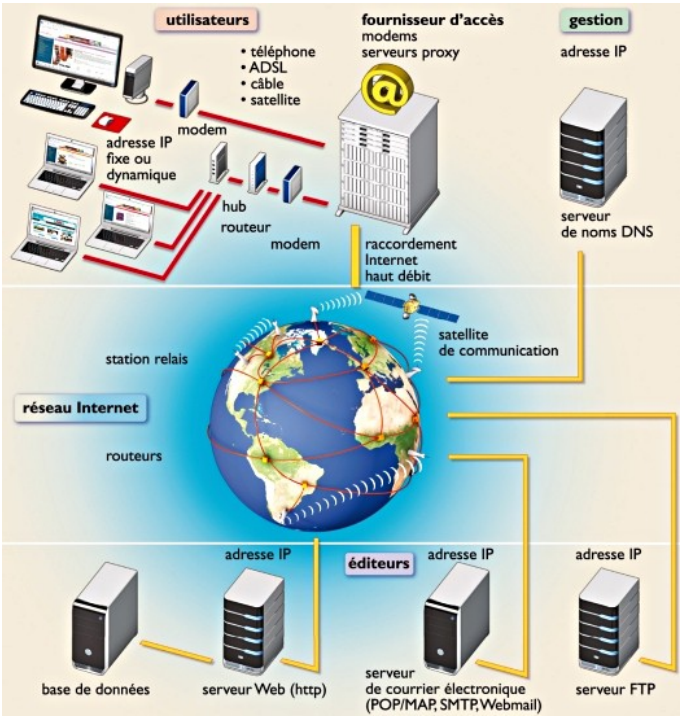


Ainsi le réseau internet ressemble à une immense pieuvre avec de multiples liaisons possibles entre 2 points. Donc, en cas de panne, l'information circule par un autre point (ou nœud) du réseau. Il existe malheureusement quelques points « critiques » où la redondance est faible. Il s'agit notamment des liaisons entre continents. Par exemple il y a une quantité très limité de fibres optiques qui relient l'Europe à l'Amérique. En cas de panne sur l'une d'elle, le trafic s'en trouve forcément impacté.



Dans les faits internet est constitué d'un maillage de réseaux publics et privés. Ainsi l'autorité administrative sur le réseau est partagée et distribuée entre tous les opérateurs parties prenantes; les décisions de ces derniers relèvent de contrats passés entre eux et de l'application de l'ensemble des normes et protocoles de transport et d'adressage dont la gestion est à la charge d'organisations internationales spécialisées.

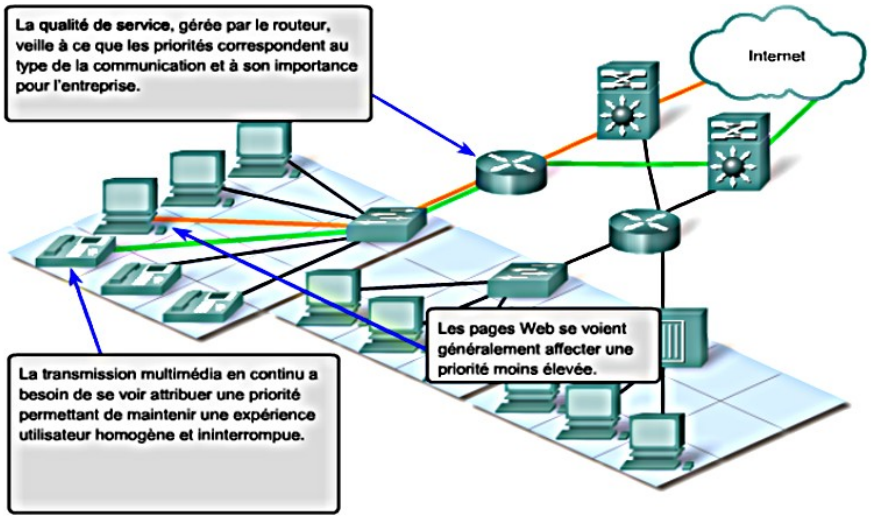
On notera que chaque ordinateur directement connecté à internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 194.153.205.26 mais avec un nom de domaine ou des adresses plus explicites du type [www.lamache.org].
Ainsi, il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name System). On appelle résolution de noms de domaines (ou résolution d'adresses) la corrélation entre les adresses IP et le nom de domaine associé.



La société qui gère ces DNS est l'Internet Corporation for Assigned Names and Numbers (ICANN). Il s'agit d'une autorité de régulation de l'Internet. C'est une société de droit californien à but non lucratif ayant pour principales missions d'administrer les ressources numériques d'Internet, telles que l'adressage IP et les noms de domaines de premier niveau (.org, .com, .fr, …). Le reste de la gestion des DNS est réalisée par différents éléments du réseau.

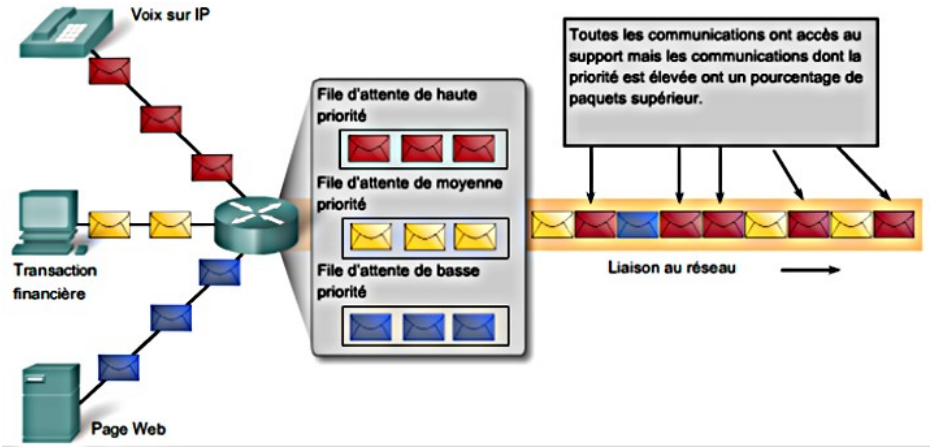
Évolutivité :

Un réseau évolutif est en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants.



Qualité de services

Quand les réseaux ne servaient qu'à des échanges informatiques (données, courriers, …), un service comportant des interruptions était acceptable. Aujourd'hui avec le développement des transmissions audio et vidéo ce

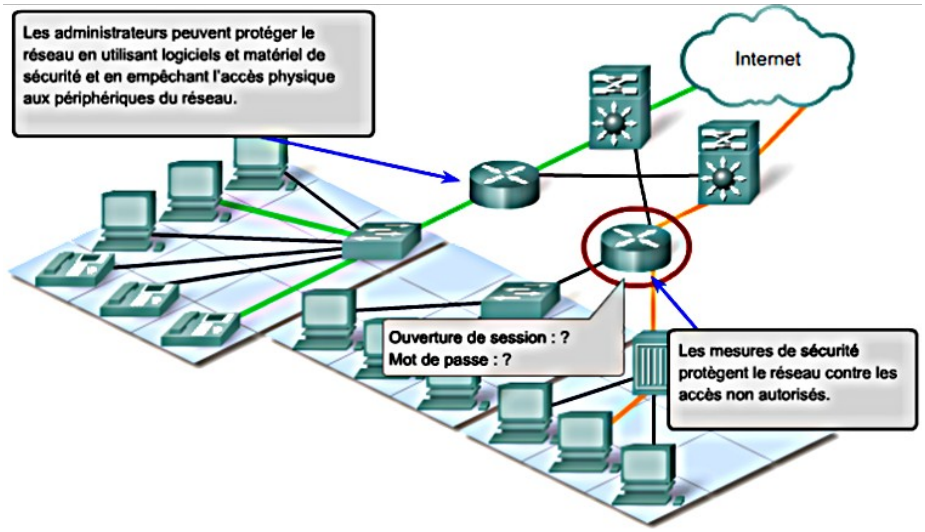


n’est plus possible. Ces transmissions exigent, en effet, un niveau de qualité constant (une grande bande passante) et un service ininterrompu.
C’est pour cela que les périphériques intermédiaires qui assurent la qualité de service gèrent des files d'attentes selon le niveau de priorité des messages. Ainsi, les messages d'un service de voix sur IP seront prioritaires devant ceux d'un service de transaction financière, eux-mêmes prioritaires devant ceux du service web.

Sécurité

L'infrastructure réseau, les services et les données contenues par un réseau relié à des ordinateurs sont des actifs personnels et professionnels essentiels. Toute compromission de l'intégrité de ces actifs pourrait avoir de graves conséquences professionnelles et financières.

En matière de sécurité des réseaux, deux points doivent être pris en considération pour éviter des conséquences graves : la sécurité de l'infrastructure réseau et la sécurité du contenu.



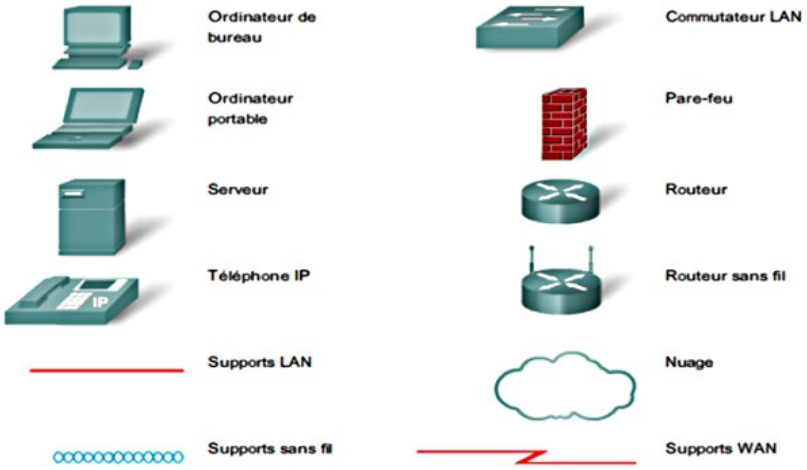
Sécuriser l'infrastructure réseau implique de sécuriser matériellement les périphériques qui assurent la connectivité du réseau et d'empêcher tout accès non autorisé au logiciel de gestion qu'ils hébergent.

Sécuriser le contenu consiste à protéger les informations contenues dans les paquets transmis sur le réseau ainsi que les informations stockées sur des périphériques reliés au réseau par exemple en les cryptant.

2. Éléments d'un réseau

Un réseau est constitué de périphériques, de supports et de services reliés par des règles et qui collaborent pour envoyer des messages. Le terme messages sert à désigner des pages Web, des courriels, des messages instantanés, des appels téléphoniques et toutes autres formes de communication prises en charge par le réseau.

Les éléments du réseau :



On distingue deux types de périphériques :

Les périphériques terminaux :

- Serveurs, Ordinateurs de bureau, Ordinateurs portables, Imprimantes, Téléphones IP, ….

Les périphériques intermédiaires :

- Commutateur (périphérique le plus couramment utilisé pour interconnecter des réseaux locaux),
- Pare-feu (assure la sécurité du réseau),
- Routeur (contribue à orienter les messages transitant sur un réseau),
- Routeur sans fil (type particulier de routeur souvent présent dans les réseaux familiaux),
- Nuage (sert à représenter un groupe de périphériques réseau)
- ….

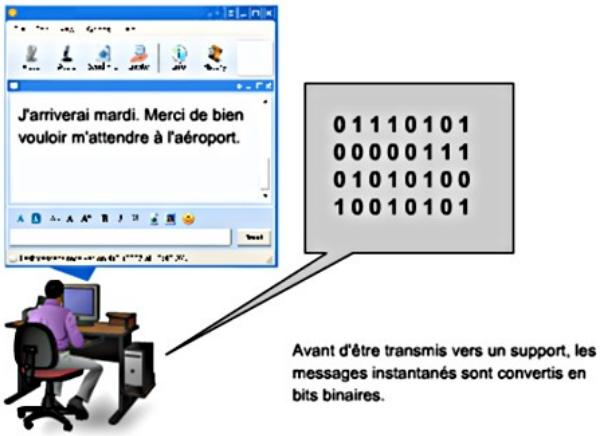
Les connexions :

- Filaires (câble droit, croisé, téléphonique, série, bus, ...)
- Sans-fil - ondes électromagnétiques (WiFi, GSM, Bluetooth, ...)
- Optique (fibre monomode, multimode, ...)

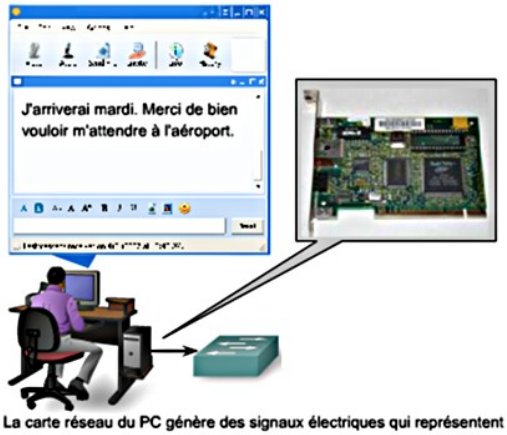
Périphériques et supports de transmission

Pour envoyer et recevoir des messages divers et variés on utilise des applications informatiques qui ont besoin que le réseau leur fournisse certains services. Ces services sont régis par des règles, ou protocoles.

Aujourd'hui, la norme en matière de réseaux est un ensemble de protocoles appelé TCP/IP (Transmission Control Protocol/Internet Protocol). Le protocole TCP/IP est non seulement utilisé dans les réseaux privés et professionnels, mais il est aussi le principal protocole d'Internet. C'est en effet le protocole TCP/IP qui définit les règles de formatage, d'adressage et de routage utilisés pour veiller à ce que les messages soient livrés aux destinataires appropriés.



Avant d'être transmis vers un support, les messages instantanés sont convertis en bits binaires.



La carte réseau du PC génère des signaux électriques qui représentent les bits qu'elle place sur le support. Les bits arrivent sur le premier périphérique réseau.

Les services de haut niveau tels que le World Wide Web, les messageries électroniques, les messageries instantanées et la téléphonie sur IP répondent à des protocoles normalisés.

Avant d'être envoyés vers leurs destinations, tous les types de messages doivent être convertis en bits, c'est-à-dire en signaux numériques codés en binaire. Ceci est obligatoire quel que soit le format d'origine du message : texte, vidéo, audio ou données informatiques, et quelque soit le service sollicité.

3. Adresses des éléments d'un réseau

3.1 L'adresse physique ou adresse MAC

Chaque appareil qui possède une possibilité de raccordement à un réseau informatique possède une adresse unique déterminé lors de sa fabrication.

Cet identifiant unique s'appelle l'adresse MAC (Media Access Control) et se présente sous la forme d'une suite de 6 octets (donc 48 bits) en général noté en hexadécimal.

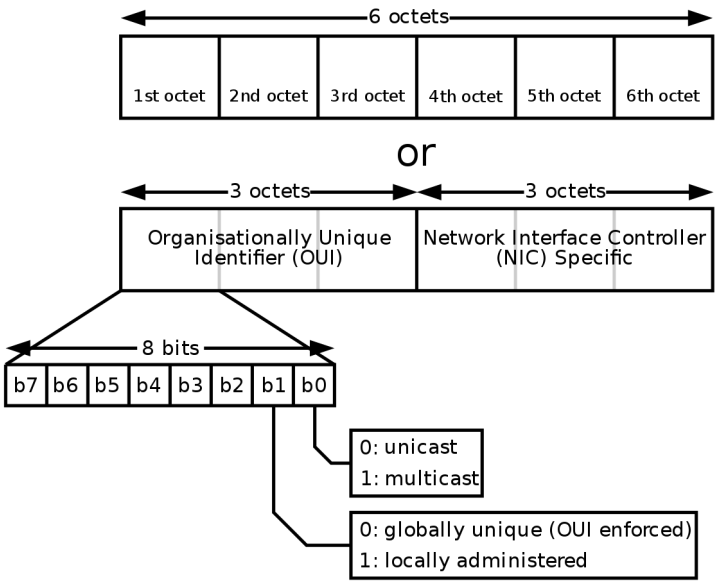
Exemple : sous Windows, quand on fait « ipconfig /all » on obtient :

```
Invite de commandes

   Liste de recherche du suffixe DNS.: home

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : home
   Description. . . . . . . . . . . . . . : Intel(R) Ethernet Connection (6) I219-LM
   Adresse physique . . . . . . . . . . . : 34-48-ED-01-14-D0
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6. . . . . . . . . . . . . .: 2a01:cb14:85f:d100:10e4:efb2:f6aa:a2bf(préféré)
   Adresse IPv6 temporaire . . . . . . . .: 2a01:cb14:85f:d100:b48c:91fd:5895:47fa(préféré)
   Adresse IPv6 de liaison locale. . . . .: fe80::10e4:efb2:f6aa:a2bf%11(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.13(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : lundi 25 mai 2020 09:01:33
   Bail expirant. . . . . . . . . . . . . : mardi 26 mai 2020 09:01:29
   Passerelle par défaut. . . . . . . . . : fe80::7a81:2ff:fe2f:b2f2%11
                                    192.168.1.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
```

L'adresse MAC de notre matériel est donc : **34-48-ED-01-14-D0**

Structure d'une adresse MAC :

- Les 3 premiers octets sont l'OUI (Organizationally Unique Identifier) : il s'agit d'un nombre de 24 bits assigné par l'IEEE (Institute of Electrical and Electronics Engineers). Ce numéro identifie le fabricant.
- Les 3 octets de poids faible correspondent à un identifiant fixé par le fabricant afin que chaque appareil soit unique.



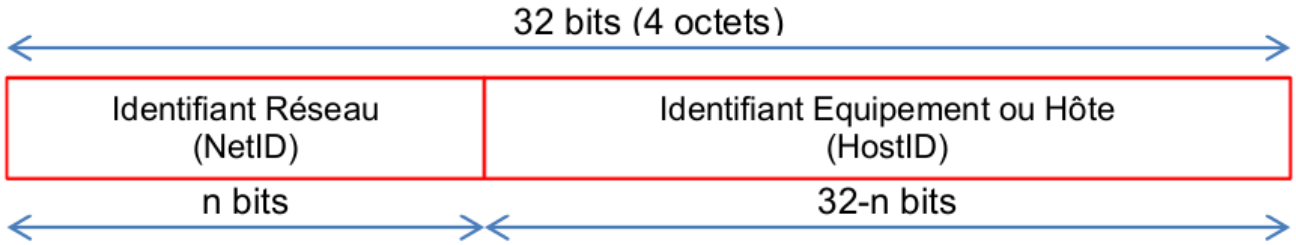
3.2 L'adresse IP

L'adresse IP (Internet Protocol) est une adresse « logique » affectée à une machine manuellement par l'administrateur réseau ou automatiquement par un serveur DHCP (Dynamic Host Configuration Protocol). Cette adresse est modifiable. Ce sera cette adresse IP qui servira pour tous les échanges au sein du réseau.

Le format IPV4

Une adresse IPV4 est constituée d'un nombre binaire de 32 bits. Pour faciliter la lecture et la manipulation de cette adresse on la représente plutôt en notation décimale, par groupe de 8 bits, séparés par un point. Exemple : 192.168.2.6 (en binaire : 11000000.10101000.00000010.00000110)

Un adresse IPV4 est composée d'un identifiant réseau (**NetID**) et d'un identifiant équipement (ou hôte) (**HostID**) :



Il existe au final cinq classes d'adresses IP. Chaque classe est identifiée par une lettre allant de A à E.

Ces différentes classes ont chacune leurs spécificités quant à la répartition du nombre d'octets servant à identifier le réseau ou les ordinateurs connectés à ce réseau :

- Une adresse IP de classe A dispose d'une partie **NetID** comportant uniquement un seul octet.
- Une adresse IP de classe B dispose d'une partie **NetID** comportant deux octets.
- Une adresse IP de classe C dispose d'une partie **NetID** comportant trois octets.
- Les adresses IP de classes D et E correspondent à des adresses IP particulières.

Cela donne :

Classe	Bits de départ	Début	Fin	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	126.255.255.255 (127 est réservé)	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0	239.255.255.255		255.255.255.255
Classe E (réservée)	1111	240.0.0.0	255.255.255.255		non défini

Masques de sous réseau :
Un sous-réseau est une subdivision logique d'un réseau de taille plus importante. Le masque de sous-réseau permet de distinguer la partie de l'adresse commune à tous les appareils du sous-réseau et celle qui varie d'un appareil à l'autre.

Exemple : adresse 192.168.1.13 et masque 255.255.255.0

Le masque de sous réseau va nous permettre, à l'aide de la fonction logique ET, de récupérer l'adresse de notre matériel débarrassé de la partie commune :

	11000000.10101000.00000001.00001101		
ET	00000000.00000000.00000000.11111111		
on obtient :	00000000.00000000.00000000.00000000	0.0.0.13	(**HostID**)

ou l'inverse :

	11000000.10101000.00000001.00001101		
ET	11111111.11111111.11111111.00000000		
on obtient :	11000000.10101000.00000001.00000000	192.168.1.0	(**NetID)**

Notation CIDR :

Une forme plus courte est connue sous le nom de « notation CIDR » (Classless Inter-Domain Routing). Elle donne le numéro du réseau suivi par un slash et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.255.0, équivalent en binaire à 11111111.11111111.11111111.00000000, sera donc représenté par /24 (24 bits à la valeur 1, suivis de 8 bits 0).

La notation 192.168.1.13/24 désigne donc l'adresse IP 192.168.1.13 avec le masque 255.255.255.0, et signifie que les 24 premiers bits de l'adresse sont dédiés à l'adresse du sous-réseau (192.168.1) et le reste à l'adresse de l'ordinateur hôte à l'intérieur du sous-réseau (ici 13).

Résumé pour la classe C :

Bits de départ	Masque de sous réseau par défaut	Nombre de bits de NetID	Nombre de bits de HostID	Nombres d'adresses possibles sur le sous réseau	Nombre d'adresses de réseaux possibles	Plage d'adresses disponibles
110	255.255.255.0	24	8	254 (2^8-2)	2097152 (2^{21})	192.0.0.1 à 223.255.255.254

Explications :
- les trois premiers bits d'une adresse de classe C ont toujours les valeurs 110. En effectuant la conversion en décimal, on obtient pour la classe C un premier octet ayant une valeur comprise entre 192 et 223. (**110**00000 et **110**11111).

- Il y a toujours 2 adresses inutilisables sur un réseau, celle correspondant à la valeur 0 et la dernière dite « de diffusion » (réservée).

Le format IPV6

Le nombre d'adresses IP disponibles avec le protocole IPv4, environ 4 milliard, n'est plus suffisant pour répondre à la demande croissante notamment avec l'arrivée des objets connectés. C'est pourquoi un nouveau protocole internet a été créé: IPv6

L'adressage se fait sur 16 octets (16*8=128 bits), ce qui représente 2^{128} adresses possibles (contre 2^{32} pour l'IPv4).

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

Exemple et règles d'écriture :

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

La notation complète ci-dessus comprend exactement 39 caractères (32 chiffres hexa et 7 deux-points).

Simplification d'écriture :
Il est permis d'omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à :
2001:db8:0:85a3:0:0:ac1f:8001

De plus, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux-points « :: ». Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en :
2001:db8:0:85a3::ac1f:8001

Plus d'information : https://fr.wikipedia.org/wiki/Adresse_IPv6

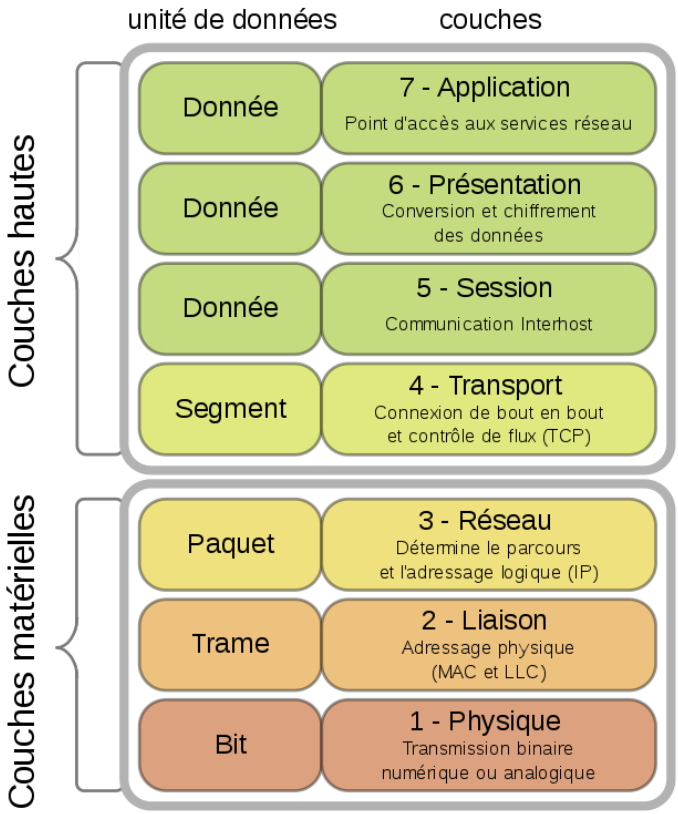
→ Exo : 1, 2, 3, 4

4. Le modèle de référence OSI

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux «propriétaires» si une norme internationale n'était pas établie. Cette norme établie par l'International Standard Organization (ISO) est la norme Open System Interconnection (OSI, interconnexion de systèmes ouverts).

Le modèle de référence OSI est une représentation abstraite en couches servant de guide à la conception des protocoles réseau. Il divise le processus de réseau en sept couches logiques, chacune comportant des fonctionnalités uniques et se voyant attribuer des services et des protocoles spécifiques.

Chaque couche ne peux communiquer qu'avec celle du dessus et celle du dessous.



Description détaillée :

7- Application	Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie...
6- Présentation	Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.
5- Session	La couche session fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.
4- Transport	Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.
3- Routage	La couche réseau fournit des services pour échanger les parties de données individuelles sur le réseau entre des périphériques terminaux identifiés.
2- Liaison	Les protocoles de la couche liaison de données décrivent des méthodes d'échanges de trames de données entre des périphériques sur un support commun.
1- Physique	Les protocoles de la couche physique décrivent les moyens mécaniques, électriques, fonctionnels et méthodologiques permettant d'activer, de gérer et de désactiver des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.

Dans les faits comment cela se passe-t-il ?

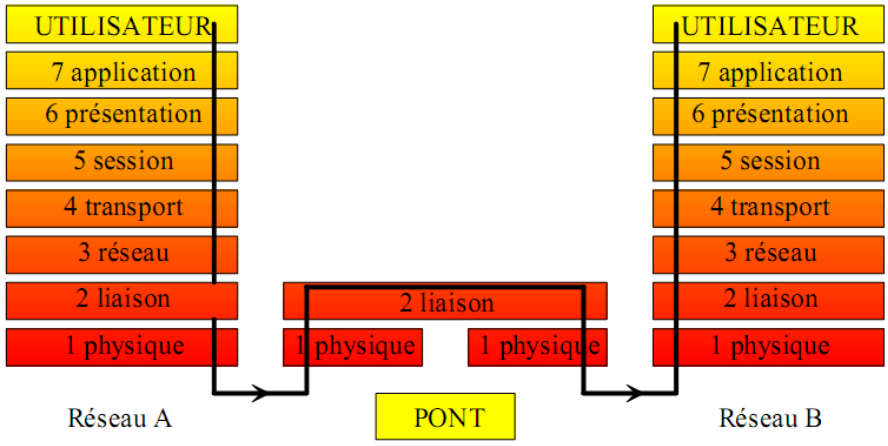
Trois types de dispositifs permettent de remplir la fonction d'interconnexion des réseaux:

- les ponts
- les routeurs
- les passerelles.

Les ponts :

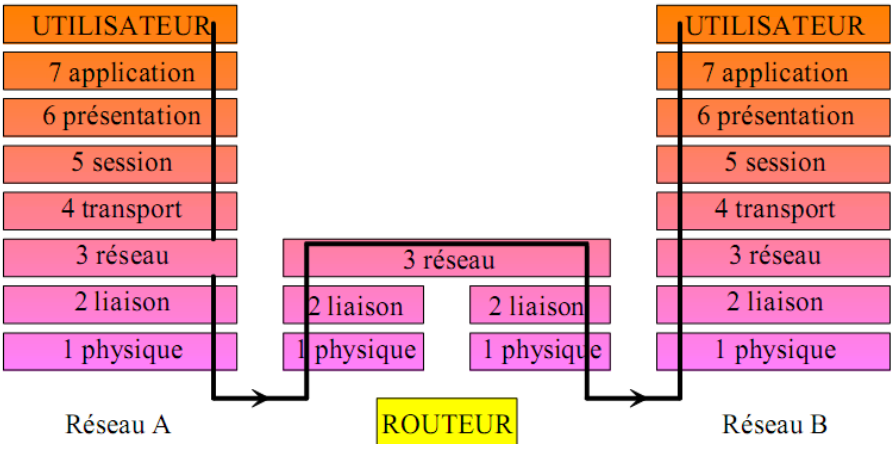
L'objectif du pont est d'interconnecter deux segments de réseaux distincts, soit de technologies différentes, soit de même technologie, mais physiquement séparés à la conception pour diverses raisons (géographique, extension de site etc.). Son usage le rapproche fortement de celui d'un commutateur (switch), à l'unique différence que le commutateur ne convertit pas les formats de transmissions de données.

Ils permettent ainsi d'interconnecter des réseaux ayant la couche 1 et 2 du modèle OSI (couche liaison) différentes, mais les couches supérieures à la 2 identiques.



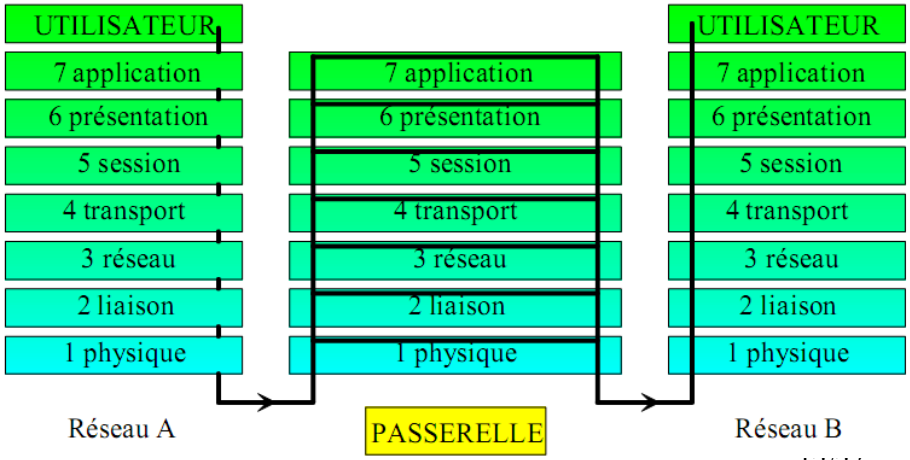
Les routeurs :

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre. Les routeurs opèrent au niveau de la couche 3 (couche réseau) du modèle OSI.



Les passerelles :

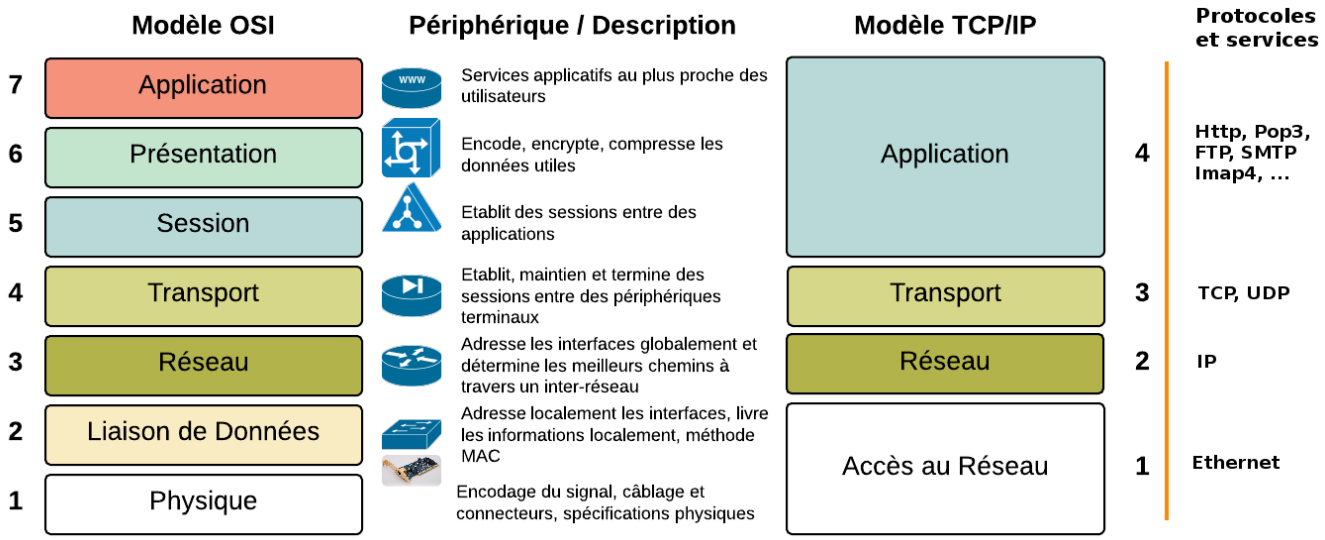
En informatique, une passerelle (en anglais, gateway) est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet.



Elles permettent l'interconnexion de réseau en adaptant l'ensemble des couches du modèle OSI afin de les rendre compatible avec l'autre réseau.

5. Comparaison des modèles OSI et TCP/IP

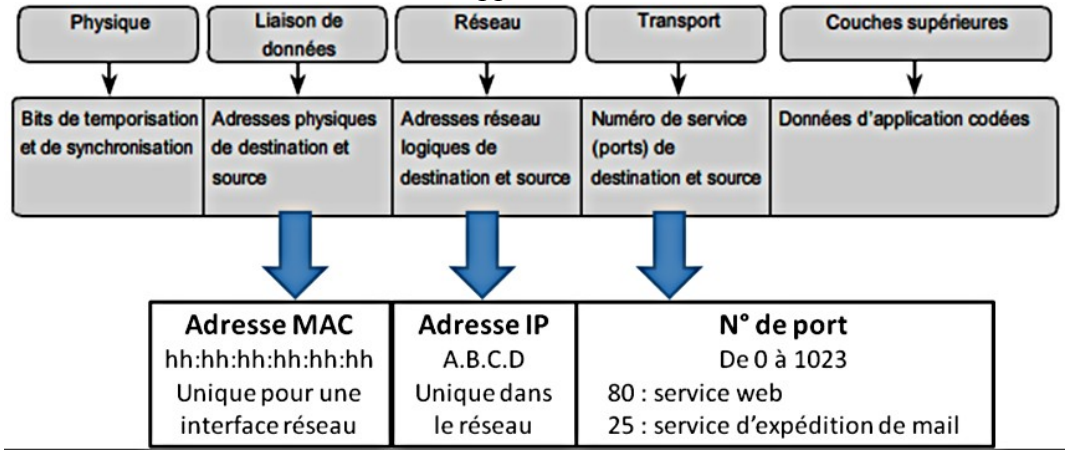
TCP/IP est une suite de protocoles utilisés pour internet. Le sigle TCP/IP signifie «Transmission Control Protocol/Internet Protocol. Ces protocoles qui constituent la suite de protocoles TCP/IP peuvent être décrits selon les termes du modèle de référence OSI :



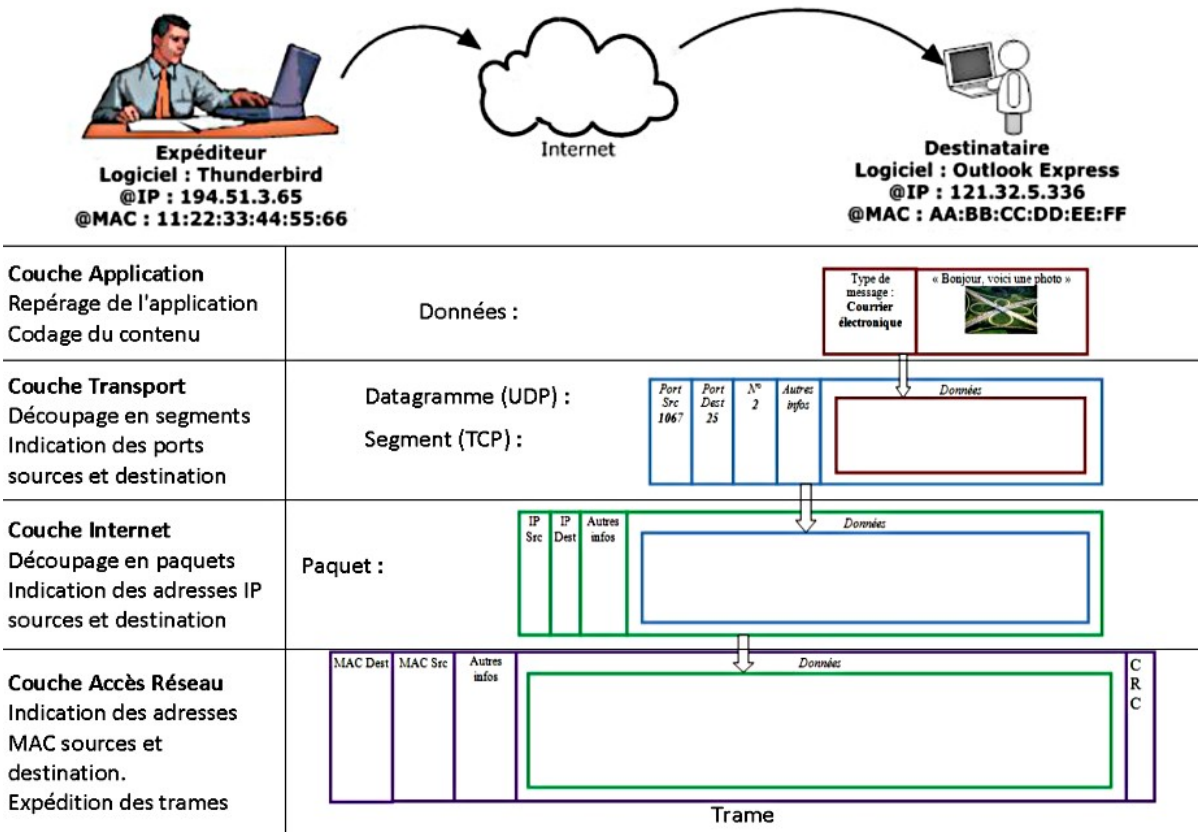
6. Principe de l'adressage et de l'encapsulation

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

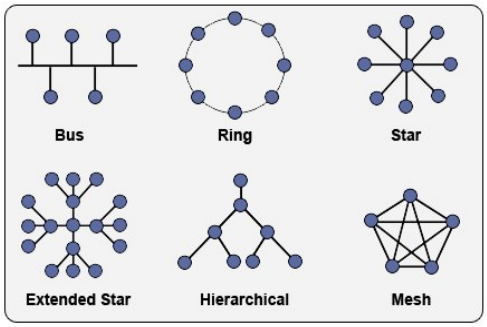
Il existe plusieurs types d'adresses qui doivent être incluses pour livrer correctement les données depuis une application source exécutée sur un hôte à l'application de destination correcte exécutée sur un autre.



Exemple : Un utilisateur veut envoyer un message (mail) conformément au schéma ci-dessous.



7. Topologie des réseaux



La manière dont sont interconnectées les machines est appelée « topologie ». On distingue la topologie physique (la configuration spatiale, visible, du réseau) de la « topologie logique ». La topologie logique représente la manière dont les données transitent dans les câbles.

Les différents types de réseaux

On distingue différents types de réseaux selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On fait généralement trois catégories de réseaux :

- **LAN** (Local Area Network) : réseau local
- **MAN** (Metropolitan Area Network) : réseau à l'échelle d'un ville ou d'un campus universitaire
- **WAN** (Wide Area Network) : il s'agit d'un réseau étendu c'est à dire un réseau informatique (ou de télécommunications) couvrant une grande zone géographique (pays, continent ou la planète entière pour le réseau Internet.

Il existe deux autres types de réseaux :

- TAN (Tiny Area Network) identique au LAN mais moins étendus (2 à 3 machines).
- CAN (Campus Area Network) identiques au MAN (avec une bande passante maximale entre tous les LAN du réseau).

Le réseau local LAN (Local Area Network) :

C'est un réseau informatique à une échelle géographique relativement restreinte, il est utilisé pour relier entre eux les ordinateurs : par exemple d'une habitation particulière, d'une entreprise, d'une salle informatique, d'un bâtiment. L'infrastructure est privée et est gérée localement. À l'intérieur, ou « sur » le réseau local il y a des ordinateurs fixes ou portables connectés par des câbles ou sans fil (Réseaux locaux sans fil : WLAN). Ces deux mondes communiquent par l'intermédiaire d'une box ou modem ADSL (selon le FAI).
La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs. En élargissant le contexte de la définition aux services qu'apportent le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement « paire à paire : P2P » (en anglais peer to peer), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire.
- dans un environnement « client/serveur », dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

Les MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants.

Un **VLAN** (Virtual Local Area Network ou Virtual LAN, en français « Réseau Local Virtuel ») est un réseau local regroupant un ensemble de machines de façon logique et non physique.
Ainsi dans un réseau local la communication entre les différentes machines est normalement régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).
Technologies utilisées : Ethernet (sur câbles de paires torsadées), ou Wifi.

Le réseau MAN (Metropolitan Area Network) :
C'est un réseau métropolitain qui désigne un réseau composé d'ordinateurs habituellement utilisés dans les campus ou dans les villes. Ainsi, un MAN permet à deux nœuds (ordinateurs) distants de communiquer comme si ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits qui utilisent généralement des fibres optiques.
Ces réseaux peuvent être placés sous une autorité publique ou privée comme le réseau intranet d'une entreprise ou d'une ville. Il permet donc pour une société, une ville, de contrôler elle-même son réseau.
Ce contrôle comprend la possibilité de gérer, surveiller et effectuer des diagnostics à distance, à la différence de la connexion WAN, pour laquelle elle doit se fier à son fournisseur d'accès pour gérer et maintenir la liaison entre elle et son bureau distant.
Ce type de réseau, s'il est municipal par exemple, permet une infrastructure multiservice : il permet de véhiculer la téléphonie, la vidéo surveillance urbaine, la télégestion des feux tricolores, les installations de chauffage, les parkings, l'éclairage de l'Hôtel de Ville, ...

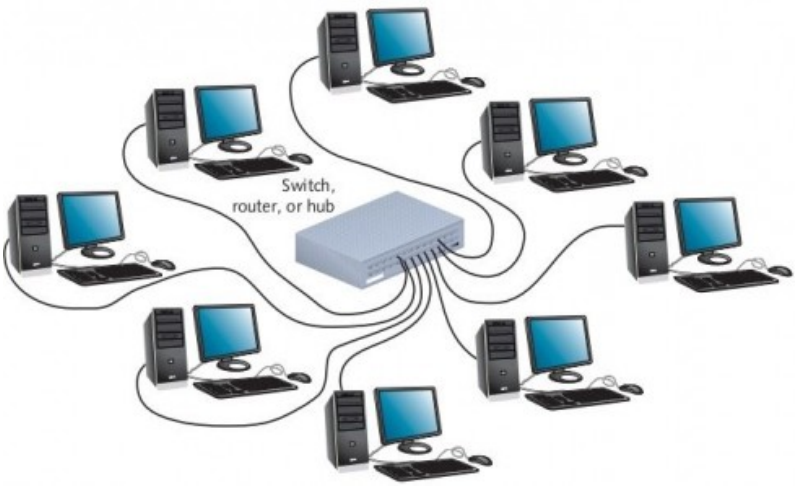
Technologies utilisées : Fibre optique, ondes radios (Wi-Fi).

Le réseau WAN (Wide Area Network) ou réseau étendu :

Le réseau Internet (WAN) est un réseau couvrant une grande zone géographique, à l'échelle d'un pays, d'un continent, voire de la planète entière. Il permet l'interconnexion de réseaux locaux et métropolitains vers l'internet mondial. L'infrastructure est en général publique.
Le plus grand réseau WAN est le réseau internet : à l'extérieur du réseau dit local, c'est à dire de l'autre côté de la « box » il existe un réseau que l'on nomme communément internet. Les fournisseurs d'accès à internet (ou FAI), moyennant finance, procurent un accès à ce réseau.

Technologies utilisées : Câble, fibre optique, satellite, technologie sans fil 3G et ondes hertziennes.

Réseau en étoile



Les équipements du réseau sont reliés à un système matériel central (le nœud). Celui-ci a pour rôle d'assurer la communication entre les différents équipements du réseau. Notamment utilisée par les réseaux Ethernet actuels en RJ45, elle concerne maintenant la majorité des réseaux. Lorsque toutes les stations sont connectées à un commutateur, on parle de topologie en étoile. Les nœuds du réseau sont tous reliés à un nœud central. Dans cette topologie tous les hôtes sont interconnectés grâce à un SWITCH (il y a encore quelques années c'était par un HUB = concentrateur) : sorte de multiprise pour les câbles réseaux placés au centre de l'étoile. Les stations émettent vers ce concentrateur qui renvoie les données vers tous les autres ports réseaux (hub) ou uniquement au destinataire (switch).
Le câble entre les différents nœuds est désigné sous le nom de « paires torsadées » car ce câble qui relie les machines au switch comporte en général 4 paires de fils torsadées et se termine par des connecteurs nommés RJ45.

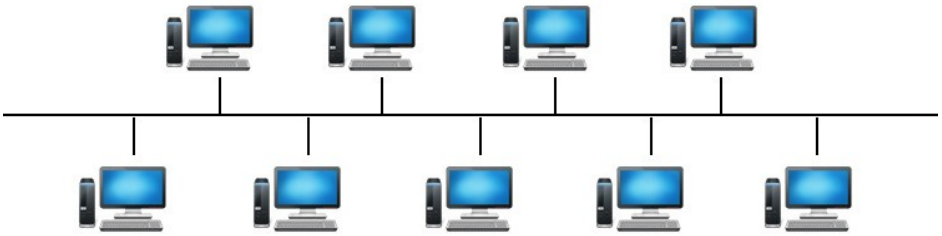
Les avantages :

- ajout facile de postes ;
- localisation facile des pannes ;
- le débranchement d'une connexion ne paralyse pas le reste du réseau ;
- simplicité éventuelle des équipements au niveau des nœuds : c'est le concentrateur qui est intelligent.
- évolution hiérarchisée du matériel possible. On peut facilement déplacer un appareil sur le réseau.

Les inconvénients :

- plus onéreux qu'un réseau à topologie en bus (achat du concentrateur et d'autant de câbles que de nœuds) ;
- si le concentrateur est défectueux, tout le réseau est en panne.
- utilisation de multiples routeur ou switch afin de pouvoir communiquer entre différents réseaux ou ordinateur

Réseau en bus



Un réseau en bus est une architecture de communication où la connexion des matériels est assurée par un bus partagé par tous les utilisateurs.
Les réseaux de bus permettent de relier simplement de multiples matériels, mais posent des problèmes quand deux machines veulent transmettre des données au même moment sur le bus. Les systèmes qui utilisent une topologie en bus ont normalement un arbitre qui gère l'accès au bus.
Cette topologie en bus a été très répandue car son coût d'installation est faible. Il est très facile de relier plusieurs postes d'une même salle, de relier chez soi deux ou trois ordinateurs. Aujourd'hui cette topologie n'est plus adaptée aux réseaux importants.

Avantages :

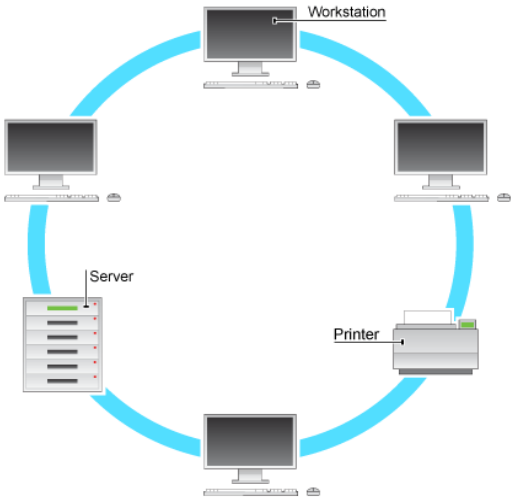
- Facile à mettre en œuvre et à étendre.
- Utilisable pour des réseaux temporaires (installation facile).
- Présente l'un des coûts de mise en réseau le plus bas.

Inconvénients

- Longueur du câble et nombre de stations limités.
- Un câble coupé peut interrompre le réseau.
- Les coûts de maintenance peuvent être importants à long terme.
- Les performances se dégradent avec l'ajout de stations.
- Faible sécurité des données transitant sur le réseau (toutes les stations connectées au bus peuvent lire toutes les données transmises sur le bus).

On remarquera que la technologie « bus » reste très utilisée dans l'industrie pour raccorder par exemple des capteurs à une unité centrale (automate, carte électronique, ordinateur, …). On parle alors de « bus de terrain » par opposition au bus informatique. En effet, le bus de terrain est en général beaucoup plus simple, du fait des faibles ressources numériques embarquées dans les capteurs et actionneurs industriels.Il est également plus robuste face aux perturbations externes. Exemples de bus de terrain : Bus CAN, MODBUS, protocole Dali, Profibus …..

Réseau en anneau



Toutes les machines sont reliées entre elles dans une boucle fermée. Les données circulent dans une direction unique, d'une entité à la suivante. Les ordinateurs communiquent chacun à leur tour. Cela ressemble à un bus mais qui serait refermé sur lui-même : le dernier nœud est relié au premier.
Souvent, dans une topologie en anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui

va gérer la communication entre les ordinateurs qui lui sont reliés en répartissant à chacun d'entre-eux un temps de parole.
Elle utilise la méthode d'accès à "jeton" (Token ring). Les données transitent de stations en stations en suivant l'anneau qui chaque fois régénèrent le signal. Le jeton détermine quelle station peut émettre, il est transféré à tour de rôle vers la station suivante. Lorsque la station qui a envoyé les données les récupère, elle les élimine du réseau et passe le jeton au suivant, et ainsi de suite... La topologie en anneau est dite « topologie active » parce que le signal électrique est intercepté et régénéré par chaque machine.

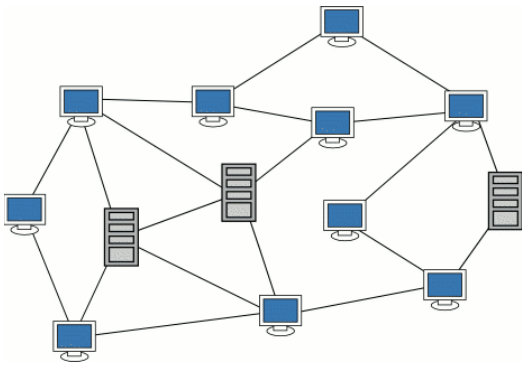
Avantages :

- La quantité de câble nécessaire est réduite
- Le protocole est simple, il évite la gestion des collisions
- Taux d'utilisation de la bande passante optimum (proche de 90%)
- Fonctionne mieux qu'une topologie de bus sous une lourde charge de réseau
- Il est assez facile à installer et à reconfigurer, car ajouter ou retirer un matériel nécessite de déplacer seulement deux connexions.

Inconvénients :

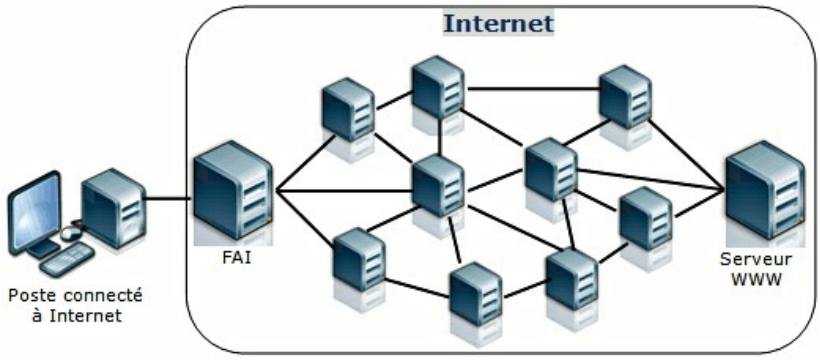
- Le retrait ou la panne d'une entité active paralyse le trafic du réseau.
- Le délai de communication est directement proportionnel au nombre de noeuds du réseau
- Le déplacement, l'ajout et la modification machines connectées peuvent affecter le réseau

Réseau maillé

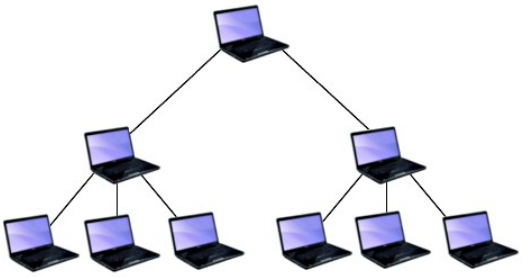


Le réseau maillé est une topologie de réseau qualifiant les réseaux (filaires ou non) dont tous les hôtes sont connectés pair à pair sans hiérarchie centrale, formant ainsi une structure en forme de filet. Par conséquent, chaque nœud doit recevoir, envoyer et relayer les données. Cela évite d'avoir des points sensibles, qui en cas de panne, isolent une partie du réseau. Si un hôte est hors service, ses voisins passeront par une autre route.
Les réseaux maillés utilisent plusieurs chemins de transferts entre les différents nœuds. Cette méthode garantit le transfert des données en cas de panne d'un nœud.

Le réseau Internet est basé sur une topologie maillée (sur le réseau étendu « WAN », elle garantit la stabilité en cas de panne d'un nœud).



Réseau en arbre (ou hiérarchique)

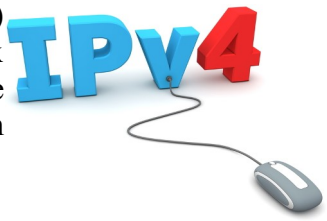


Une topologie en arbre ou topologie arborescente ou hiérarchique peut être considérée comme une collection de réseaux en étoile disposés en hiérarchie. Ce réseau est divisé en niveaux. Le sommet, de haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur.
Comme dans le réseau en étoile conventionnel, des nœuds individuels peuvent ainsi encore être isolés du réseau par une défaillance d'un seul point d'un trajet de transmission vers le nœud. Si un lien reliant une branche échoue, cette branche est isolée; Si une connexion à un nœud échoue, une section entière du réseau devient isolée du reste.

→ Exo : 5 et 6

IV. Exercices

Exercice 1 : adresses IPv4



IPv4 (Internet Protocol version 4) est la première version d'Internet Protocol (IP) à avoir été largement utilisée aussi bien pour internet que pour les réseaux informatiques en général. Elle permet une définition commune (mondialement) de la manière d'écrire les adresses des machines (ordinateur, serveur, …) reliées à un réseau informatique.

Exemple 1 : le réseau d'un particulier

Le réseau des particuliers est en général le suivant :
192.168.1.x où x est l'adresse des éléments connectés au réseau

1. ***'x' pouvant prendre comme valeur 0 à 255 (en décimal), sur combien de bits est-il codé en binaire ?***
2. ***L'adresse de mon ordinateur étant 192.168.1.2, écrivez cette adresse en binaire.***
3. ***Combien de matériels différents puis-je relier sur ce réseau ?***

Exemple 2 : le réseau d'une petite entreprise

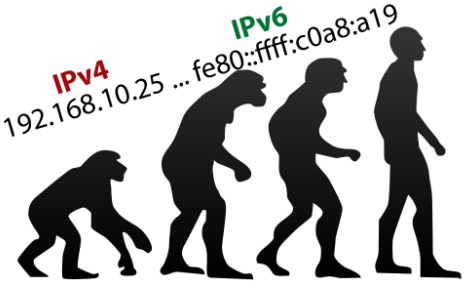
Le réseau de l'entreprise est : 192.168.x.y où x et y sont les octets codant l'adresse des éléments connectés au réseau

4. ***'x' et 'y' pouvant chacun aller de 0 à 255 (en décimal), sur combien de bits au total l'adresse des éléments est-elle codée ?***
5. ***Combien de matériels différents puis-je relier sur ce réseau ?***

Généralisation

6. ***Si tous les élément de l'adresse peuvent être choisi (w.x.y.z), chacun pouvant aller de 0 à 255 (en décimal), sur combien de bits au total l'adresse est-elle codée ?***
7. ***Combien de matériels différents puis-je relier sur le réseau internet avec cette norme IPv4?***

Exercice 2 : adresses IPv6



IPv6 (Internet Protocol version 6) est le protocole réseau qui a été conçu pour succéder à l'IPv4.

La plage des adresses va de 0:0:0:0:0:0:0:0 à FFFF:FFFF:FFFF : …….. :FFFF (l'adresse est en 8 parties séparées par des « deux points », chaque nombre est donné en hexadécimal)

Exemple d'une adresse IPv6 :

2001:0db8:0000:85a3:0010:0a0b:8001:ec1f

Préliminaires :

1. ***Convertissez le chiffre hexadécimal 'E' en décimal puis en binaire***
2. ***Combien faut-il de bits pour coder un 'chiffre' hexadécimal ?***

Étude d'un des 8 éléments composant une adresse IPv6 :
Cet élément peut avoir comme valeur 0000 à ffff. Prenons l'élément 'ec1f'

3. ***Convertissez ce nombre hexadécimal en décimal***
4. ***Convertissez ce nombre hexadécimal en binaire***
5. ***Sur combien de bits est-il codé ?***

Généralisation :

6. ***Sur combien de bits une adresse IPv6 complète est-elle codée ?***
7. ***Combien de matériels différents puis-je relier sur le réseau internet avec IPv6?***

Exercice 3 : généralités

1)Un téléphone portable possède-t-il une adresse MAC ?

2)Combien d'adresses MAC possède un routeur ?

3)Combien d'adresses IP possède un routeur ?

4)Un réseau a comme masque 255.255.255.224. Combien de machines peut- il y avoir sur un tel réseau ?

5)En utilisant l'adressage par classe, l'adresse 190.24.12.8/16 fait partie de quel réseau ?

6)On trouve comme adresse réseau : 74.125.100.80/8. Quel est le masque réseau ?

7)Combien peut-on mettre de machines sur un réseau du type 78.0.0.0/16 ?

8)Soit l'adresse suivante 77.45.234.56/17. Donnez le masque se sous réseau.

9)Quelle adresse réseau (NetID) possède la machine 192.168.5.17/24 (aidez vous de masque de sous réseau)?

10)Quels adresses réseau (NetID) et équipement (HostID) possède la machine 194.45.67.98/26 (aidez vous de masque de sous réseau)?

11)Notre réseau a comme adresse 172.16.0.0/12
11.1. Donnez son masque de sous réseau :

11.2. Donnez son adresse de diffusion (broadcast) en vous aidant du masque de sous réseau.

Exercice 4 : IPV4 classe A et B

voici le résumé pour la classe C :

Bits de départ	Masque de sous réseau par défaut	Nombre de bits de NetID	Nombre de bits de HostID	Nombres d'adresses possibles sur le sous réseau	Nombre d'adresses de réseaux possibles	Plage d'adresses disponibles
110	255.255.255.0	24	8	254 (2^8-2)	2097152 (2^{21})	192.0.0.1 à 223.255.255.254

Complétez le résumé pour la classe A :

Bits de départ	Masque de sous réseau par défaut	Nombre de bits de NetID	Nombre de bits de HostID	Nombres d'adresses possibles sur le sous réseau	Nombre d'adresses de réseaux possibles	Plage d'adresses disponibles
					126 (2^7-2)	

Complétez le résumé pour la classe B :

Bits de départ	Masque de sous réseau par défaut	Nombre de bits de NetID	Nombre de bits de HostID	Nombres d'adresses possibles sur le sous réseau	Nombre d'adresses de réseaux possibles	Plage d'adresses disponibles
					16384 (2^{14}-2)	

Exercice N°5 Topologie des réseaux

soit le réseau d'une petite entreprise:

Entourez, en les nommant, les 3 types de topologie de réseau présent sur le réseau.

Exercice N°6 Des question de bits, de débits, ….

Remarque : dans les questions suivantes on partira du principe qu'un Kb = 1000bits, qu'un Mbits=1000000, ….

Sur une liaison hertzienne urbaine à 1200 bits/s (débit max) on envoie des messages de 8 octets. La fréquence d'émission est de 12 messages par seconde.

1. ***Calculez le débit réel (en bits/s) de la ligne avec l'utilisation précédente.***
2. ***En déduire le taux d'utilisation de la ligne (en%)***

Différents réseaux Ethernet

3. ***Quel est le temps de transmission de 1Kb sur un réseau dont le débit est 10 Mb/s***
4. ***Quel est le temps de transmission de 1Kb sur un réseau dont le débit est 100 Mb/s***

On considère maintenant un réseau dont le débit est de 10 Mbits/s. Les messages envoyés sur ce réseau ont une taille maximale de 1000 bits dont un champ de contrôle de 16 bits.

5. ***Quel est le nombre de messages nécessaires pour envoyer un fichier de 4 Mbits d'un ordinateur à l'autre?***