Lycée des métiers de l'électricité et de l'électronique
Alphonse BENOIT – Cours Victor HUGO – 84803 L'ISLE SUR LA SORGUE

Formation réseau Ethernet

Du lundi 1 au mercredi 3 février 2010

Livret de cours

La communication Ethernet est devenue un standard dans de nombreuses applications électroniques.

La connaissance de l'architecture des réseaux, du matériel et des protocoles utilisés est devenue indispensable pour leur mise en œuvre.

Ce stage vous permettra de vous familiariser avec le vocabulaire et le matériel, au travers d'activités de cours et de travaux pratiques :

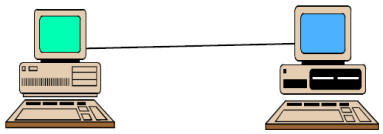
- Architecture réseau : topologie, supports physiques (câbles, fibre optique, ondes électromagnétiques).
- Adressage matériel et logique (différence entre adresse MAC et IP)
- Commandes de bases pour le réseau (ipconfig, ping, ...)
- Electronique active (concentrateur, commutateur, routeur, ...)
- Différence entre station de travail et serveur.
- Les principaux services réseaux (DHCP, DNS, serveur web, firewall, ...)
- Mise en applications sur systèmes (panneau d'affichage, téléphonie IP, vidéo surveillance, passerelle webdyn, ...).

Réseaux – Présentation générale

1 Qu'est-ce qu'un réseau ?

1.1 Définition

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs industriels ou personnels ou de simples terminaux graphiques.

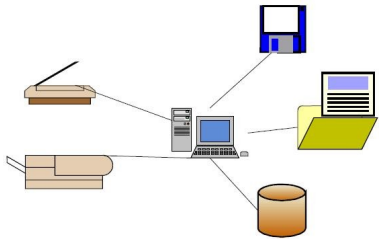


1.2 Utilité

Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (industries, banques, gestion, commerce, bases de données, recherche, etc...) et des particuliers (messagerie, loisirs, services d'informations par minitel et Internet ...).

Services les plus courants :

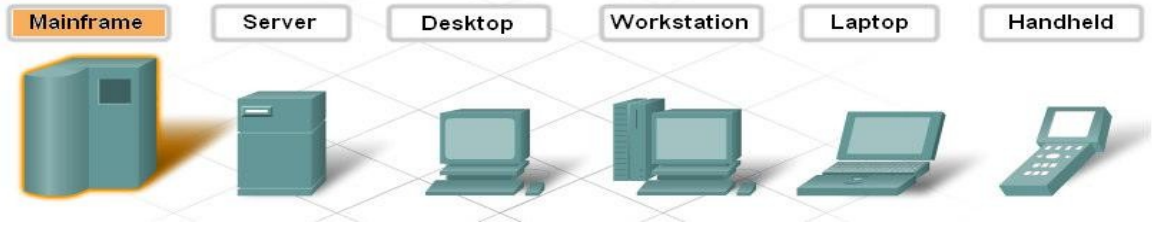
- Partage de matériels, de logiciels, de fichiers,
- communication, messagerie,
- sécurisation (accès, données).



2 Acteurs

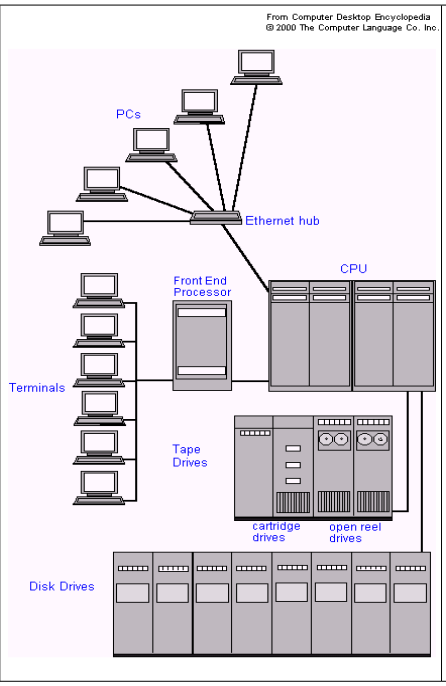
2.1 Les ordinateurs

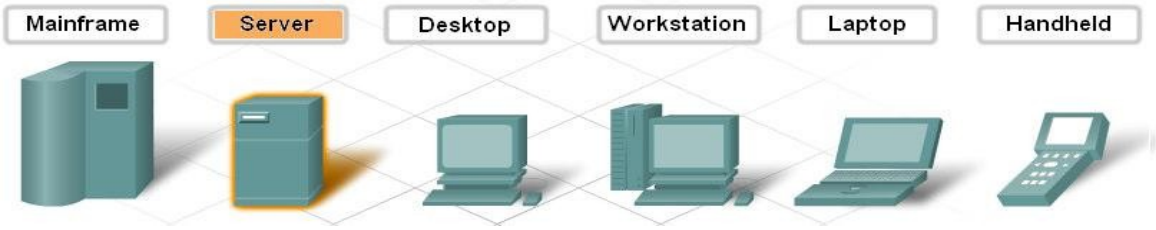
Les équipements les plus nombreux à être interconnectés dans un réseau informatique sont les ordinateurs. Ils existe de nombreux types d'ordinateurs :



Le terme Ordinateur Central (**mainframe** en anglais) est utilisé en informatique pour définir un ordinateur de grande puissance de traitement.

- Relié à des terminaux ou clients légers (PC sans disque dur ou avec un système d'exploitation minimum)
- Applications métiers lourdes : très grandes entreprises (banques, compagnies d'assurances, compagnies aériennes, sociétés de services, mairies ...). De par leur fiabilité et leur puissance, ils sont parfois les seuls ordinateurs capables de répondre aux besoins de leurs utilisateurs (traitement de très grandes banques de données accédées par des dizaines ou des centaines de milliers d'utilisateurs).
- Architecture propriétaire (IBM).





Un serveur est à la fois un ensemble de logiciels et l'ordinateur les hébergeant dont le rôle est de répondre de manière automatique à des demandes envoyées par des clients.

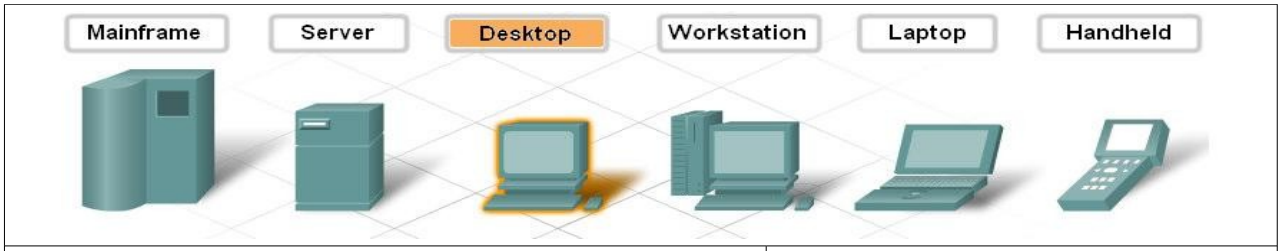
- Caractéristiques techniques hautes performances (plusieurs CPU et disques, beaucoup de RAM).
- Capable de répondre aux requêtes reçues par le réseau.
- Multiples usages (utilisateurs du réseau, impression, fichier, BD, web, DNS, DHCP, …)
- Ils peuvent être équipés de dispositifs de prévention des pannes et de pertes d'informations, tels que les dispositifs RAID : les informations sont copiées sur plusieurs disques durs, en vue d'éviter leur perte irrémédiable en cas de panne d'un des disques durs.

Standalone server :
Un serveur est un ordinateur destiné à répondre aux demandes faites via un réseau. Divers constructeurs et assembleurs tels que HP, Sun ou IBM vendent des ordinateurs optimisés à cet effet.
Ce sont typiquement des machines haut de gamme conçues pour servir simultanément de nombreux clients. Les machines sont équipées d'un processeur puissant voire de plusieurs processeurs, de mémoires et de disque durs rapides et de grande capacité, et bien sûr d'une ou plusieurs interfaces réseau.
Les serveurs fonctionnent sans intervention, 24 heures sur 24, 99,9 % du temps. La durée moyenne d'arrêt des serveurs varie entre 36 minutes et 10 heures par année.

Rackmount server :
Serveurs montés dans des rack 19 ou 20 pouces, ce qui permet de les empiler.
Le regroupement de plusieurs serveurs en une grappe (en anglais cluster) permet de répartir la charge, et assure que les clients sont servis même en cas d'arrêt d'un des serveurs.

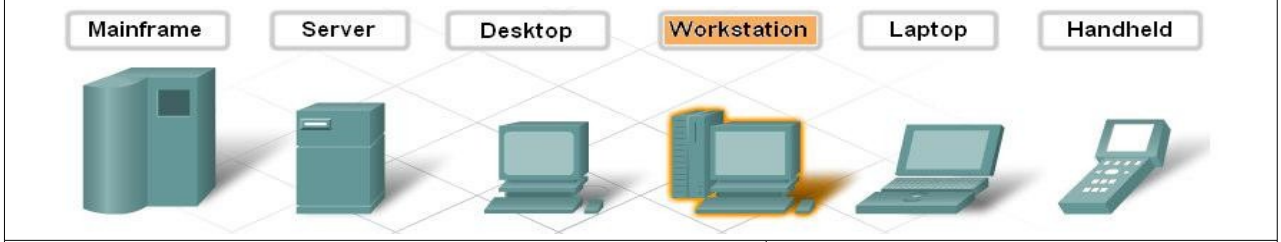
Blade server :

Serveur de la taille d'une carte d'extension PCI, intégrant processeur, mémoire vive, interface réseau et disque dur, dont la compacité simplifie la gestion de l'espace et autorise l'installation d'un grand nombre de serveurs. Tenant sur une simple carte PCI, le serveur lame permet de ranger dans un seul châssis des dizaines de serveurs. Insérer dix cartes dans le châssis d'un serveur lame revient donc à brancher entre eux dix serveurs, mais sans avoir à régler les problèmes de câbles et d'alimentation. En effet, les serveurs lames partagent la carcasse, les blocs d'alimentation, les ventilateurs et le câblage avec les autres serveurs lames présents dans l'armoire.



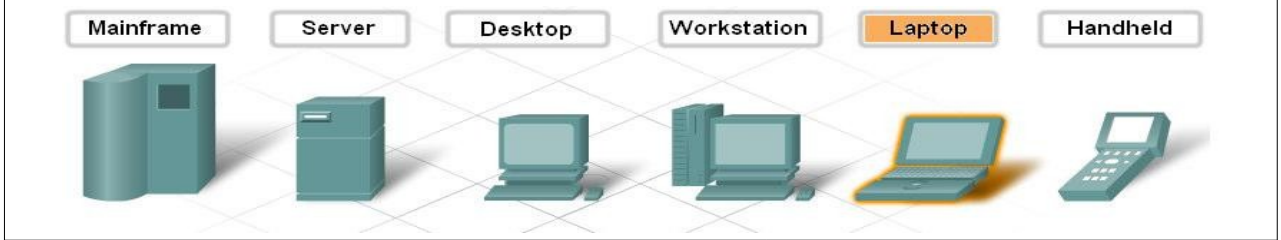
Un ordinateur de bureau (de l'anglais **desktop** computer ; aussi appelé ordinateur fixe) est un ordinateur personnel (Personal Computer ou PC) destiné à être utilisé pour la bureautique et la navigation sur internet.

L'ordinateur de bureau peut être démonté pour y changer des composants.



Les stations de travail sont des ordinateurs puissants dont le rôle est de faire fonctionner des applications spécifiques telle que :

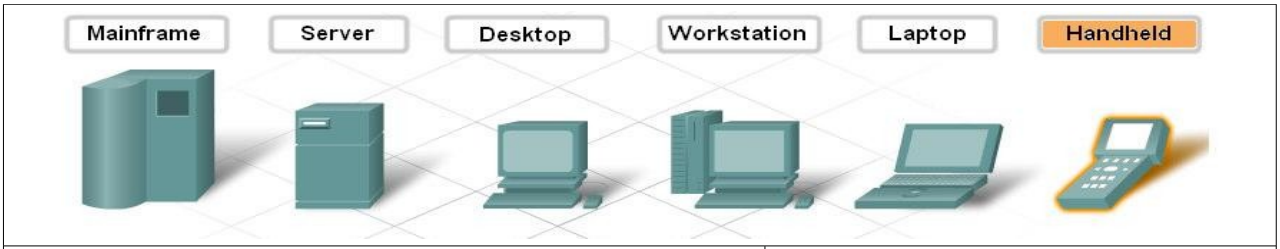
- la CAO-DAO,
- l'imagerie 3D ou médicale,
- le montage vidéo,
- la simulation, ...



Un ordinateur portable ou Laptop est un ordinateur personnel qui, grâce à un poids (<4kg) et un encombrement limités, peut être transporté très facilement.

Ils coûtent plus cher que les ordinateurs de bureau à cause de la miniaturisation des composants, et sont plus lents car il faut éviter de dégager trop de chaleur et éviter de consommer trop d'énergie pour une meilleure autonomie.

Ils sont peut évolutifs et fragiles.

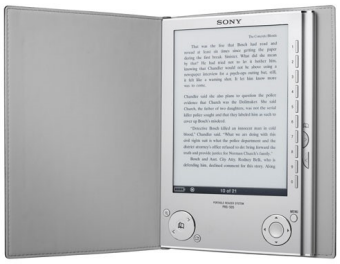


Ce sont les Tablet PC, Pocket PC, PDA, … qui désigne une nouvelle classe d'ordinateurs portables et ultraportables se présentant sous la forme d'un écran tactile et d'un stylet.

Ils sont plus petit et moins puissant que les portable.

Ils sont très souvent équipés d'un système d'exploitation Microsoft et possèdent en standard un certain nombre d'applications préinstallées tels que Pocket Word, Pocket Excel, Pocket Outlook, Pocket Internet Explorer et Pocket MSN, permettant un usage quotidien (agenda, notes, mail, internet, …).

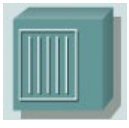
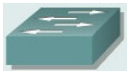
Ils ne sont équipés que de ports « modernes » (USB, PCMCIA/PC Card, FireWire, Wi-Fi, IrDA, Bluetooth...).



2.2 Les équipements d'interconnexion

Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation comporte généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux. Dans ce cas, des équipements spécifiques sont nécessaires.

Les principaux équipements matériels mis en place dans les réseaux locaux sont :

Matériel	Symbole	Exemples	
Les répéteurs, permettant de régénérer un signal			 Répéteurs de fibres optique
Les concentrateurs (hubs), permettant de connecter entre eux plusieurs hôtes			
Le pont (bridge) lit les adresses MAC des trames Ethernet et décide en fonction de l'adresse destination s'il doit les transmettre ou les filtrer.			
Les commutateurs (switches) permettant de relier divers éléments tout en segmentant le réseau			
Les routeurs, permettant de relier de nombreux réseaux locaux de telles façon à permettre la circulation de données d'un réseau à un autre.			

3 Les supports de transmission.

3.1 Ethernet.

La plupart des réseaux locaux utilisent aujourd'hui Ethernet. Cette appellation désigne un protocole de communication entre machines, identifiées par une adresse unique : **l'adresse MAC (Media Access Control)**.

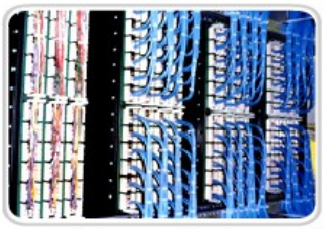
Ces machines sont reliées entre elles par un câble en cuivre, des ondes radios ou, dans certains cas, par des fibres optiques. Ce cours portera donc sur les supports et connecteurs utilisés dans un réseau de type Ethernet

Nous traiterons les types de supports suivants:

Cuivre : *coaxial et paire torsadée*

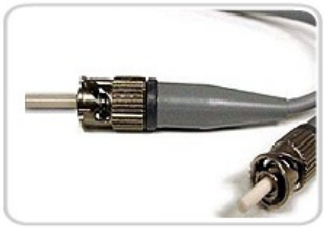
Verre : *fibre optique*

Ondes : *sans fil*

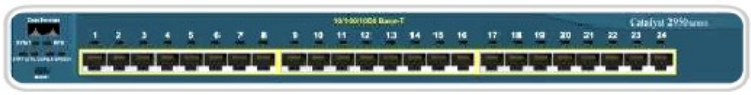


Panneaux de brassage à paires torsadées non blindées dans une baie

Commutateurs Ethernet



Connecteurs pour fibre optique Ethernet



Commutateur Ethernet

3.2 Un peu de vitesse.

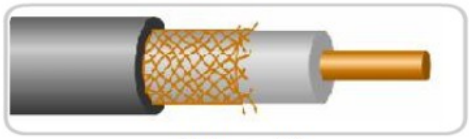
Selon la technologie utilisée, on peut atteindre des vitesses de transmission plus ou moins élevées. Le tableau ci-dessous présente les technologies "cuivre" et "fibre optique".

Type d'Ethernet	Bande passante	Type de câble	Bidirectionnel	Distance maximale
10Base-5	10 Mbits/s	Câble Ethernet coaxial épais	Non simultané	500 m
10Base-2	10 Mbits/s	Câble Ethernet coaxial fin	Non simultané	185 m
100Base-TX	10 Mbits/s	Câble à paires torsadées non blindées (UTP) Cat3/Cat5	Non simultané	100 m
100Base-TX	100 Mbits/s	Câble à paires torsadées non blindées (UTP) Cat5	Non simultané	100 m
100Base-FX	200 Mbits/s	Câble à paires torsadées non blindées (UTP) Cat5	Simultané	100 m
100Base-FX	100 Mbits/s	Fibre multimode	Non simultané	400 m
1000Base-T	200 Mbits/s	Fibre multimode	Simultané	2 km
1000Base-TX	1 Gbit/s	Câble à paires torsadées non blindées (UTP) Cat5e	Simultané	100 m
1000Base-SX	1 Gbit/s	Câble à paires torsadées non blindées (UTP) Cat6	Simultané	100 m
1000Base-LX	1 Gbit/s	Fibre multimode	Simultané	550 m
10GBase-CX4	1 Gbits/s	Fibre monomode	Simultané	2 km
10GBase-T	10 Gbits/s	Axial double	Simultané	100 m
10GBase-LX4	10 Gbits/s	Câble à paires torsadées non blindées (UTP) Cat6a/Cat7	Simultané	100 m
10GBase-LX4	10 Gbits/s	Fibre multimode	Simultané	300 m
10 Mbits/s	10 Gbits/s	Fibre monomode	Simultané	10 km

4 Le cuivre.

Le support le plus souvent utilisé pour les communications de données est un câblage qui utilise des fils de cuivre. Il existe deux sortes de câbles utilisant le cuivre :

Le câble coaxial.

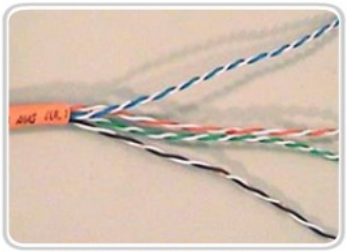


Câble coaxial

Le câble à paires torsadées

Les données sont transmises sur les câbles en cuivre sous forme *d'impulsions électriques* mais sont soumises à des interférences diverses.

On peut atténuer ou éliminer ces interférences en utilisant des techniques particulières comme la *torsade* ou le *blindage*



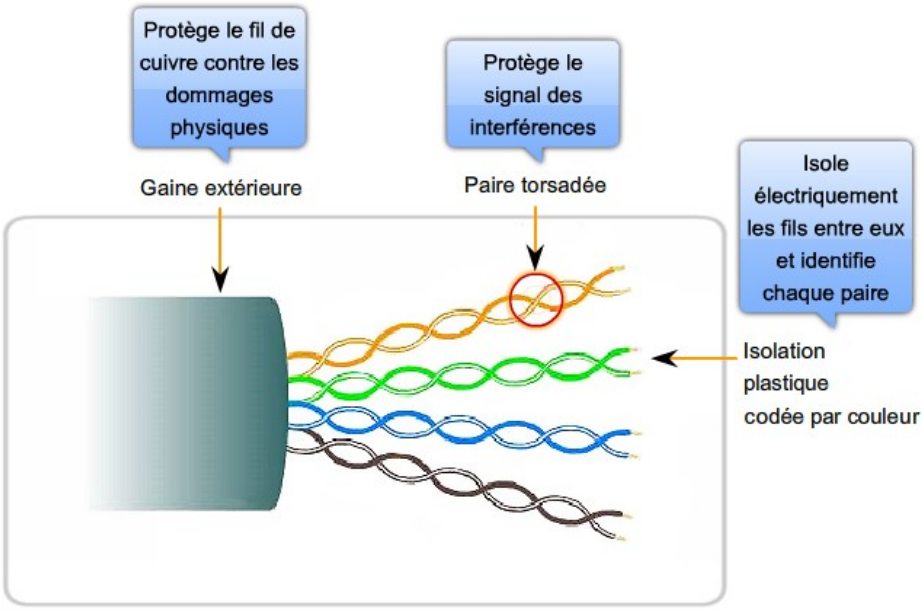
Câble à paires torsadées non blindées

Connexions RJ-45

4.1 Le câble à paire torsadées.

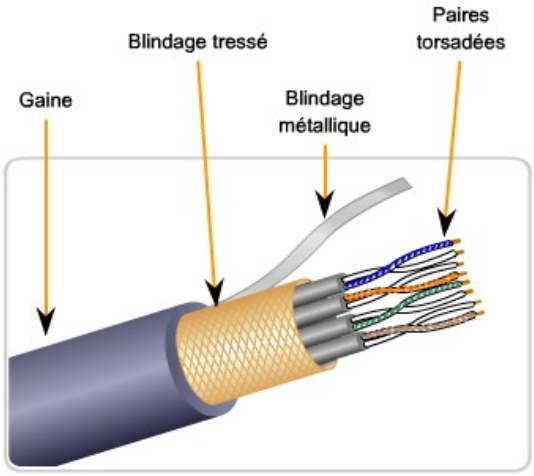
Le câble à paire torsadée est utilisé pour les communications téléphoniques et pour la plupart des réseaux Ethernet récents. Une paire de fils forme un circuit qui peut transmettre des données. Les paires sont torsadées afin d'empêcher la *diaphonie*, c'est-à-dire le bruit généré par les paires adjacentes (voisines)

Le câble utilisé dans les réseaux Ethernet est composé de *4 paires de fils* :



La figure ci-dessus représente un câble **UTP :** *Unshield Twisted Pair*

Paire torsadée sans blindage



Un autre type de câblage utilisé dans les réseaux est le câble à paires torsadées blindées (STP). Comme l'illustre la figure, la norme STP utilise deux paires de fils enveloppées dans un revêtement tressé ou un film métallique.

STP : *Shield Twisted Pair*

Paires torsadées blindée

Parfois, le blindage n'est pas constitué avec une tresse métallique mais avec une simple feuille d'aluminium appelée "écran". On parle alors de câble

FTP : *Foiled Twisted Pair*

Paires torsadées écrantées

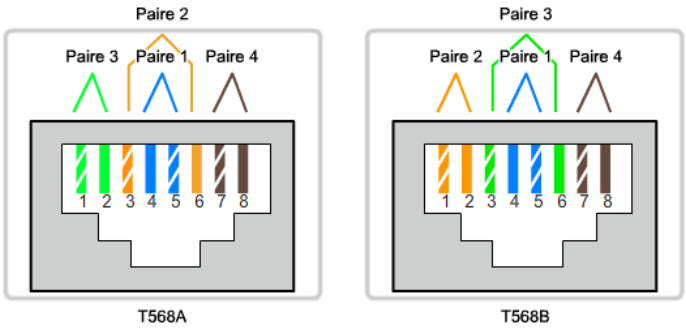
Ces deux types de câbles offrent une meilleure immunité aux interférences mais sont plus couteux et difficiles à mettre en œuvre.

4.2 La connectique des câbles UTP, FTP, STP.

Le câblage UTP, terminé par des connecteurs *RJ-45*, est un support en cuivre courant pour l'interconnexion de périphériques réseau, tels que des ordinateurs, avec des périphériques intermédiaires, tels que des routeurs et commutateurs réseau.

Il existe deux normes de câblage qui détermine la position des fils dans le connecteur : *568A et 568B*

La seconde norme est la plus couramment utilisée.



Selon les appareils que l'on veut connecter, il faut utiliser des câbles droits (même câblage de chaque côté) ou des câbles croisés

Type de câble	Norme	Application
Ethernet direct	T568A à une extrémité, T568B à une autre extrémité	Connexion d'un hôte réseau à un périphérique réseau tel qu'un commutateur ou un concentrateur.
Croisement Ethernet	T568A aux deux extrémités ou T568B aux deux extrémités	Connexion de deux hôtes réseau. Connexion de deux périphériques intermédiaires réseau (un commutateur à un commutateur, ou un routeur à un routeur).

Remarque : Le connecteur RJ45 ressemble au *RJ11* utilisé dans la téléphonie mais ce dernier est plus petit et ne possède que 4 broches.

4.3 Catégories.

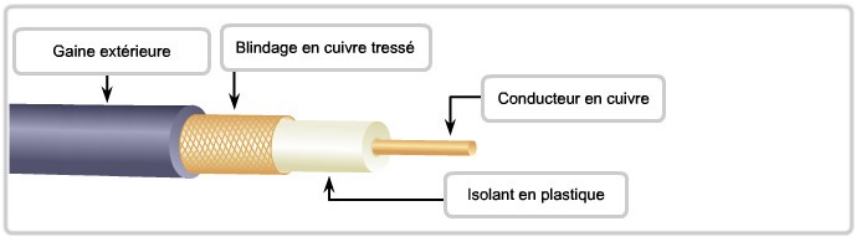
Il existe plusieurs catégories de câbles UTP. Elles sont déterminées par le nombre de fils et le nombre de torsades de ces fils. Cela influe directement sur la vitesse de transmission. Le tableau ci-dessous présente les catégories et leur utilisation.

Catégorie UTP	Vitesse de transmission maximale	Caractéristiques et utilisations
Catégorie 3	16 Mbits/s	Qualité de données la plus basse ; utilisé pour la plupart des câblages téléphoniques
Catégorie 4	20 Mbits/s	Adaptée aux réseaux Ethernet 10 Mbits/s
Catégorie 5	100 Mbits/s - 1 Gbits/s	Qualité la plus utilisée pour les réseaux locaux, tout particulièrement Fast Ethernet (100 Mbits/s)
Catégorie 5e (améliorée)	155 Mbits/s	Utilisée pour Fast Ethernet et ATM (Asynchronous Transfer Mode) 155 Mbits/s
Catégories 6 et 7	1 Gbits/s minimum	Utilisée pour les nouvelles technologies Gigabit Ethernet

4.4 Le câble coaxial.

Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.

Le câble coaxial est un type couramment utilisé dans les technologies sans fil et d'accès par câble. Il permet par exemple de relier des antennes à des périphériques sans fil. Le câble coaxial transporte de l'énergie en radiofréquence (RF) entre les antennes et le matériel radio.



Le câble coaxial est également le support le plus largement employé pour le transport par fil de signaux de radiofréquence élevée, en particulier les signaux de télévision par câble.

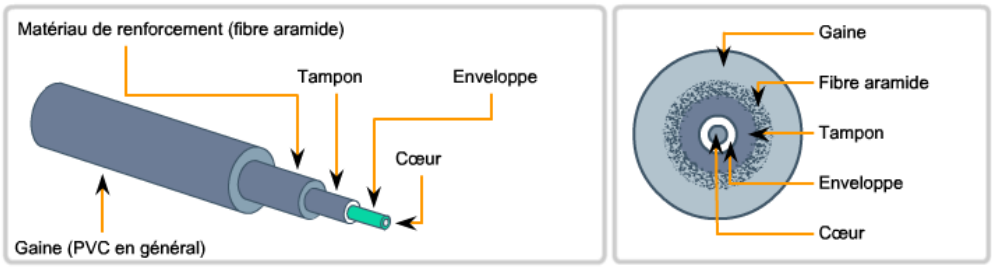
5 La fibre optique.

5.1 Constitution.

Contrairement aux autres supports de réseau composés de fils de cuivre, le câble à fibre optique ne transporte pas d'impulsions électriques. Les signaux représentant les données sont convertis en *faisceaux lumineux*.

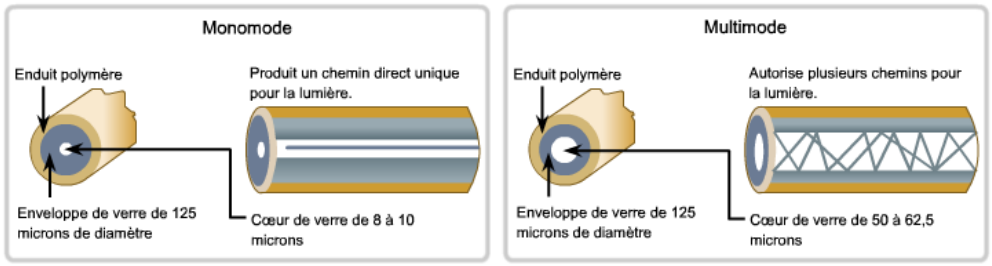
Le câblage en fibre optique utilise des fibres de *verre* ou de *plastique* pour guider des impulsions lumineuses de la source à la destination.

Les fibres présentent de nombreux avantages par rapport au cuivre au niveau de la largeur de bande passante et de l'intégrité du signal sur la distance. Cependant, le câblage en fibre est plus difficile à utiliser et plus coûteux que le câblage en cuivre. Les connecteurs sont onéreux, tout comme la main d'œuvre pour terminer les extrémités des câbles.



5.2 Monomode, multimode.

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

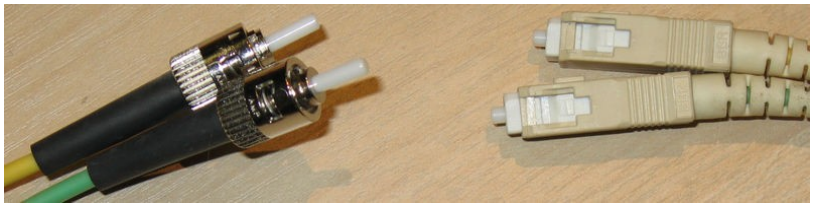


- Cœur de petit diamètre.
- Moins de dispersion.
- Adapté aux applications longue distance (jusqu'à 100 km)
- Utilise des lasers comme source de lumière souvent dans des réseaux fédérateurs de campus pour une distance de plusieurs milliers de mètres.

- Cœur d'un diamètre plus large que le câble monomode (au moins 50 microns).
- Autorise une plus grande dispersion et, par conséquent, un affaiblissement du signal.
- Adapté aux applications longue distance, mais sur une distance plus courte que la fibre monomode (jusqu'à 2 km environ).
- Utilise des LED comme source de lumière souvent dans des réseaux locaux ou des distances de quelques centaines de mètres au sein d'un réseau de campus.

5.3 Connecteurs pour fibre optique.

Il existe nombre de connecteurs pour la fibre optique. Les plus répandus sont les connecteurs *ST (rond) et SC (carré)*.



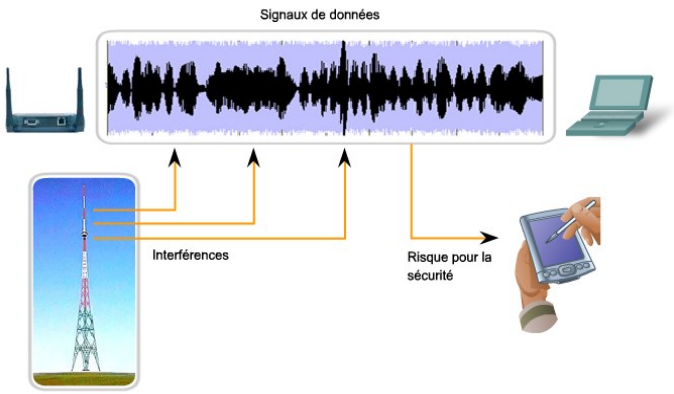
6 Les ondes radios.

Les supports sans fil transportent des signaux électromagnétiques qui représentent les chiffres binaires des communications de données.

Le principal avantage des communications sans fil est *l'absence de support (câble)*. Mais cela présente aussi des inconvénients:

Les signaux électromagnétiques sont sensibles à *l'environnement et aux interférences*.

Tout le monde peut accéder aux données émises. Les réseaux sans fil doivent donc être sécurisés avec soin.



6.1 Différents types de réseaux sans fil.

Plusieurs technologies permettent les liaisons sans fil. Chacune correspond à un usage différent.

6.1.1 DECT (Digital Enhanced Cordless Telecommunications)

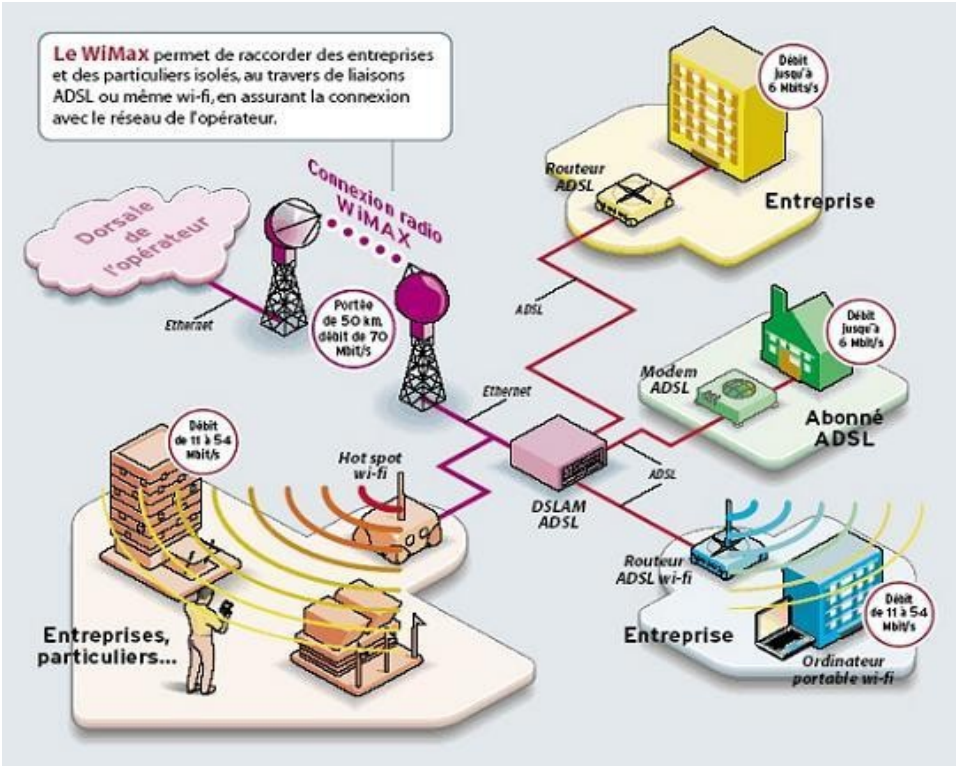
Norme européenne de transmission numérique à courte distance utilisée pour les postes téléphoniques sans-fil domestiques. Il existe deux générations de téléphones DECT, la dernière ayant une portée de 300 m et permettant de relier jusqu'à 9 postes dans un mini-réseau intérieur. Le DECT est une technologie économique et éprouvée qui ne concerne que les communications téléphoniques et n'inclue aucun service supplémentaire.

6.1.2 GSM, GPRS, UMTS.

Ces réseaux sont utilisés par le système de téléphonie cellulaire. Ils offrent un débit et des services différents selon la norme utilisée

6.1.3 WiMax (Worldwide Interoperability for Microwave Access), IEEE 802.16

WiMax est une des technologies de BLR (Boucle Locale Radio). C'est une norme de transmission à plus grande distance que Wi-Fi (10 km). L'utilisation du Wi-Max se justifie pour connecter des locaux situés dans des régions à faible densité de population.



6.1.4 Bluetooth, IEEE 802.15

La technologie Bluetooth est intégrée dans une puce de moins d'1 cm2. Elle est donc peu encombrante et peu consommatrice d'énergie. Sa portée est faible (au plus, quelques mètres) et le débit modéré (57 kbit/s à 1 Mbit/s).

Ses utilisations sont déjà nombreuses :

- *téléphones portables,*
- *oreillettes sans fils,*
- *PDA*
- *clavier et souris sans fils,*
- *imprimante individuelle.*

6.2 Wifi, 802.11.

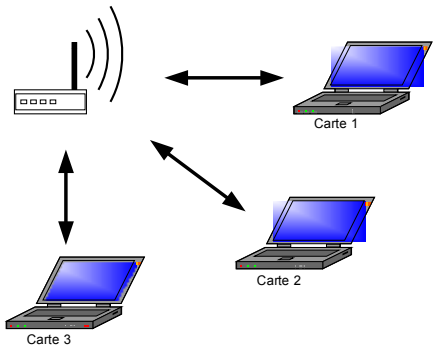
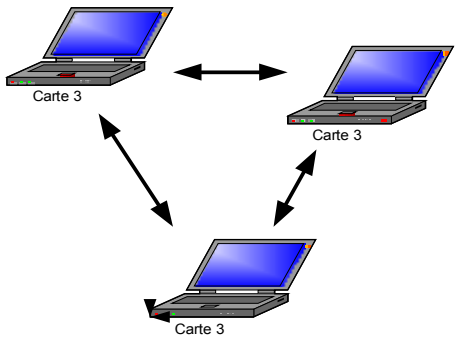
Apparu en 1999 et aujourd'hui largement utilisé, le système Wifi permet la transmission sur des distances inférieures à 100. L'utilisation du Wi-Fi se justifie partout où l'on ne souhaite pas installer de câbles : salles de réunion, lieux publics, locaux temporaires, domiciles...

6.2.1 Trois normes.

Il existe plusieurs normes Wifi mais les trois plus utilisées sont les suivantes:

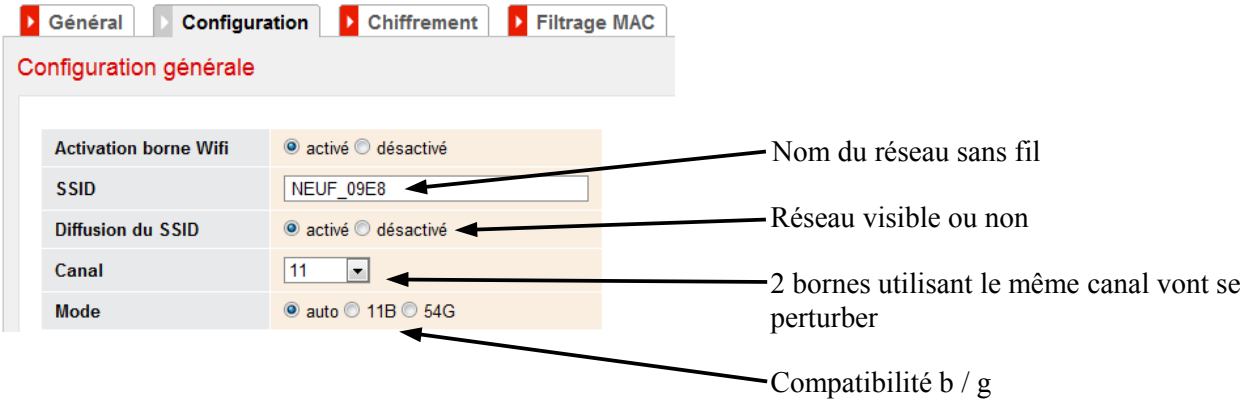
Nom de la norme	Description
802.11b	La norme ***802.11b*** est une norme très répandue. Elle propose un débit théorique de *11 Mbps* avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 13 canaux radio disponibles.
802.11g / g+	La norme ***802.11g*** offre un haut débit (*54 Mbps* théoriques) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g pourront fonctionner en 802.11b. La norme g+ permet des débits de 108 Mbps mais est propriétaire (liée au constructeur)
802.11n	La norme ***802.11n*** vise à faire passer les débits à 540Mbps. Cette technique en développement utilise la technologie MIMO (Multiple - Inpout Multiple - Outpout) qui repose sur l'utilisation de plusieurs antennes au niveau de l'émetteur et du récepteur. 802.11n *n'est pas compatible* avec les deux précédentes car les fréquences utilisées sont différentes (5GHz)

6.2.2 Modes de fonctionnement.

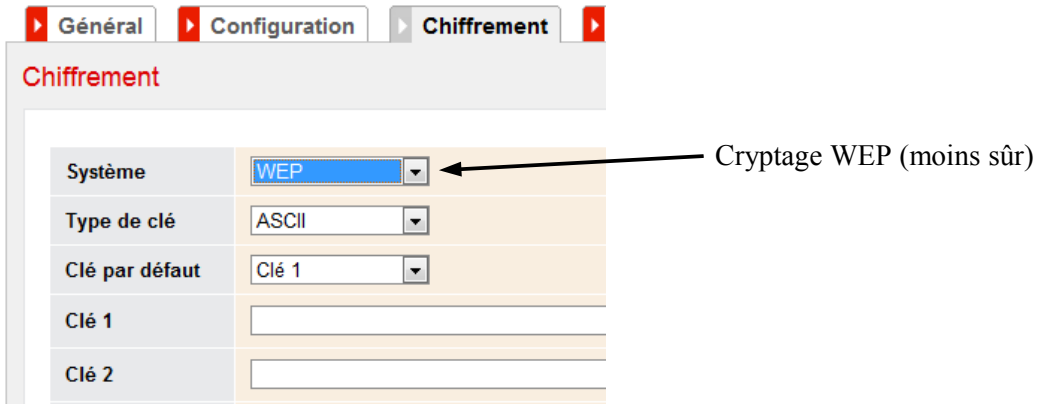
Mode infrastructure : *un point d'accès (AP) gère l'ensemble de stations.*	
Mode Ad-hoc : Pas de point d'accès. *Les stations communiquent directement entre elles.*	

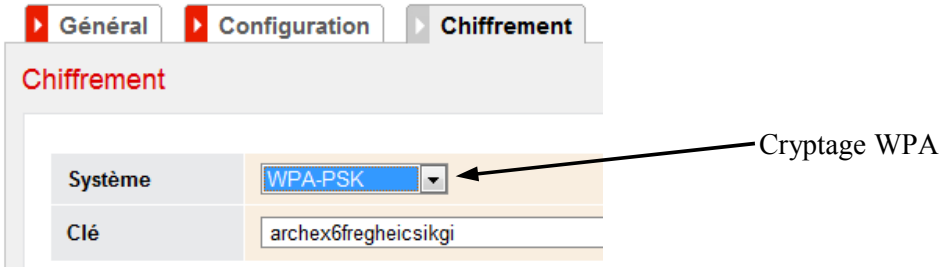
6.2.3 Paramètres importants en Wifi

Configuration générale

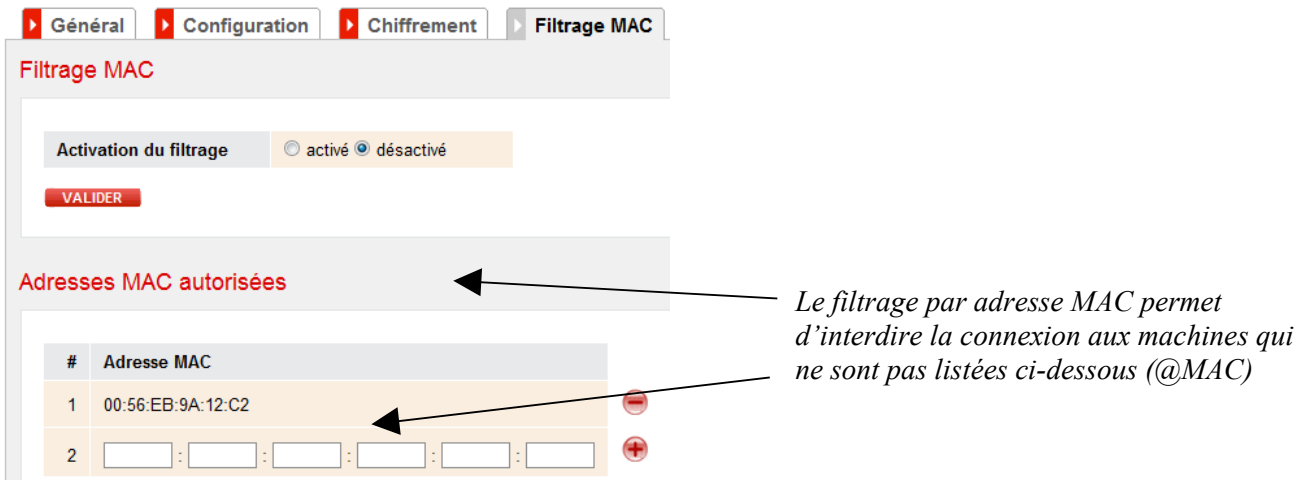


Chiffrement



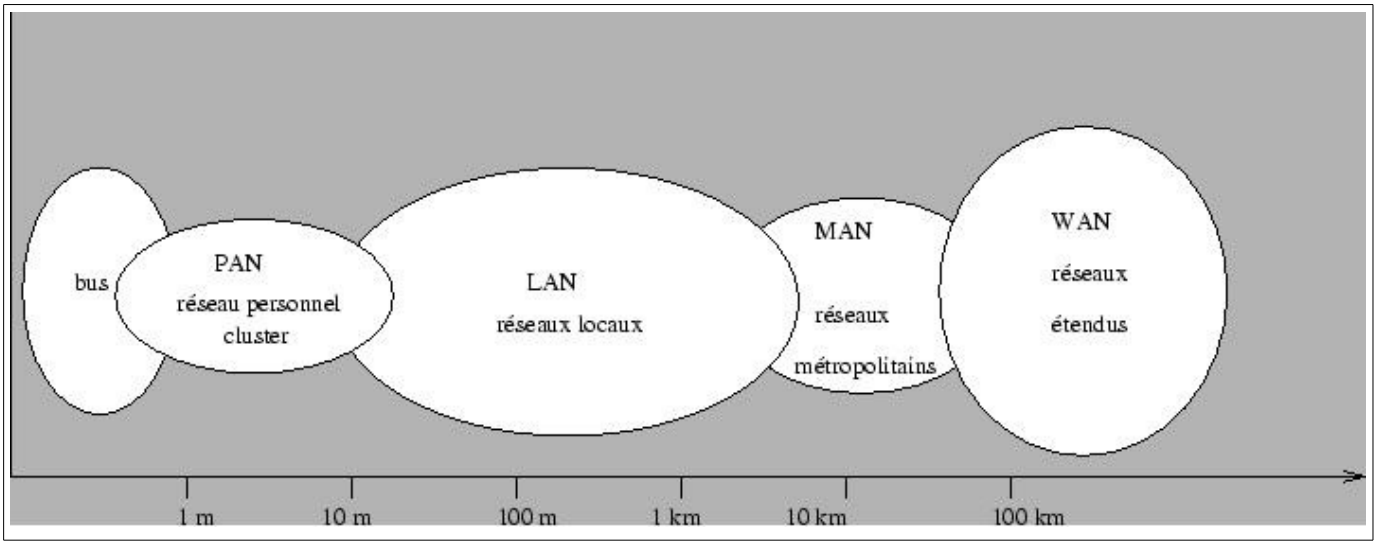


Contrôle d'accès



7 Classification des réseaux

On peut faire une première classification des réseaux à l'aide de leur taille comme on peut le voir dans la figure ci-dessous.



Les **bus** que l'on trouve dans un ordinateur pour relier ses différents composants (mémoires, périphériques d'entrée-sortie, processeurs, ...) peuvent être considérés comme des réseaux dédiés à des tâches très spécifiques. Certains réseaux industriels sont aussi appelés **bus de terrain** ou **réseau de terrain**.

- **Un réseau personnel (Personnal Area Network)** interconnecte (souvent par des liaisons sans fil) des équipements personnels comme un ordinateur portable, un agenda électronique... Un cluster est un groupe d'unités centrales reliées entre elles de manière à agir comme un seul ordinateur soit pour pouvoir faire de la répartition de charges soit du calcul distribué.
- **Un réseau local (Local Area Network)** peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.
- **Un réseau métropolitain (Metropolitan Area Network)** interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.
- **Un réseau étendu (Wide Area Network)** permet de communiquer à l'échelle d'un pays, ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications.
- **Un réseau de terrain** permet à des systèmes électronique de communiquer entre eux sur des distances pouvant aller jusqu'à quelques km (électronique dans les véhicules, ateliers, usines, bâtiments, ouvrages d'arts…). Les éléments reliés au réseau sont des calculateurs, automates, capteurs, actionneurs,…. Il existe deux types de réseaux de terrain : les standards de fait (**Interbus-S, ASI, Lonworks**, ...) et les standards internationaux (WorldFip, Profibus, …). Tous les réseaux de terrain ont un ancêtre commun : **la boucle de courant 4-20mA**.

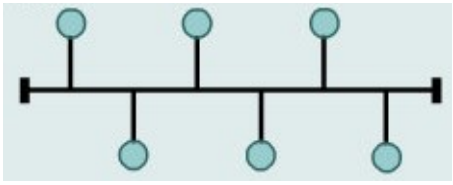
8 Topologie d'un réseau

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.

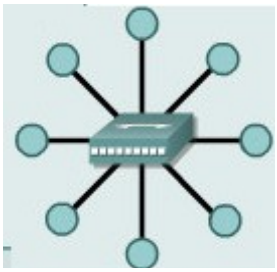
Les topologies logiques les plus courantes sont **Ethernet, Token Ring** et **FDDI**.

Les principales topologies physiques sont les topologies en **bus**, en **étoile** et en **anneau**.

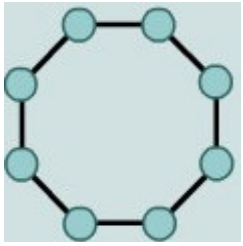
8.1 Topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantages d'être facile à mettre en oeuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.	

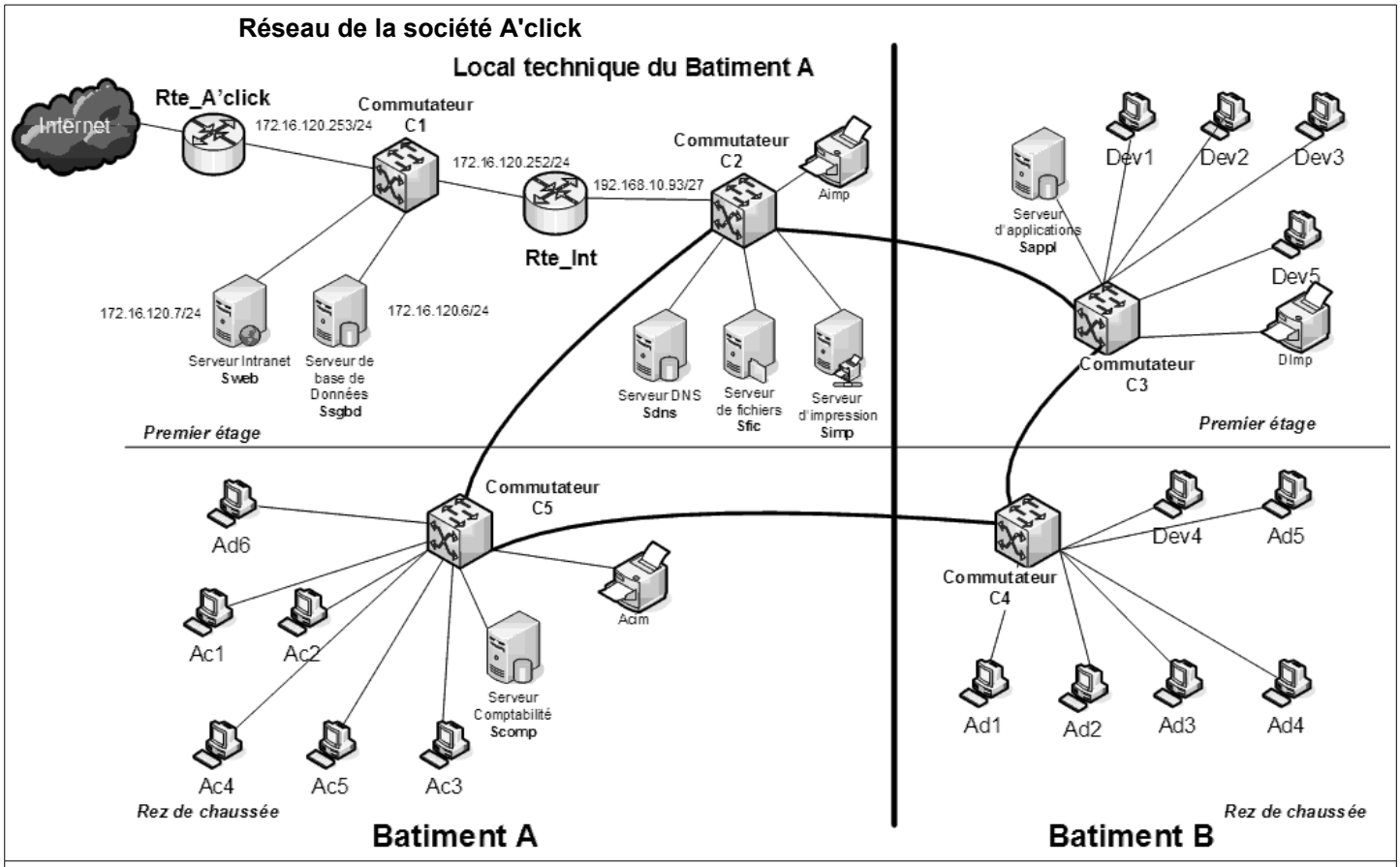
8.2 Topologie en étoile

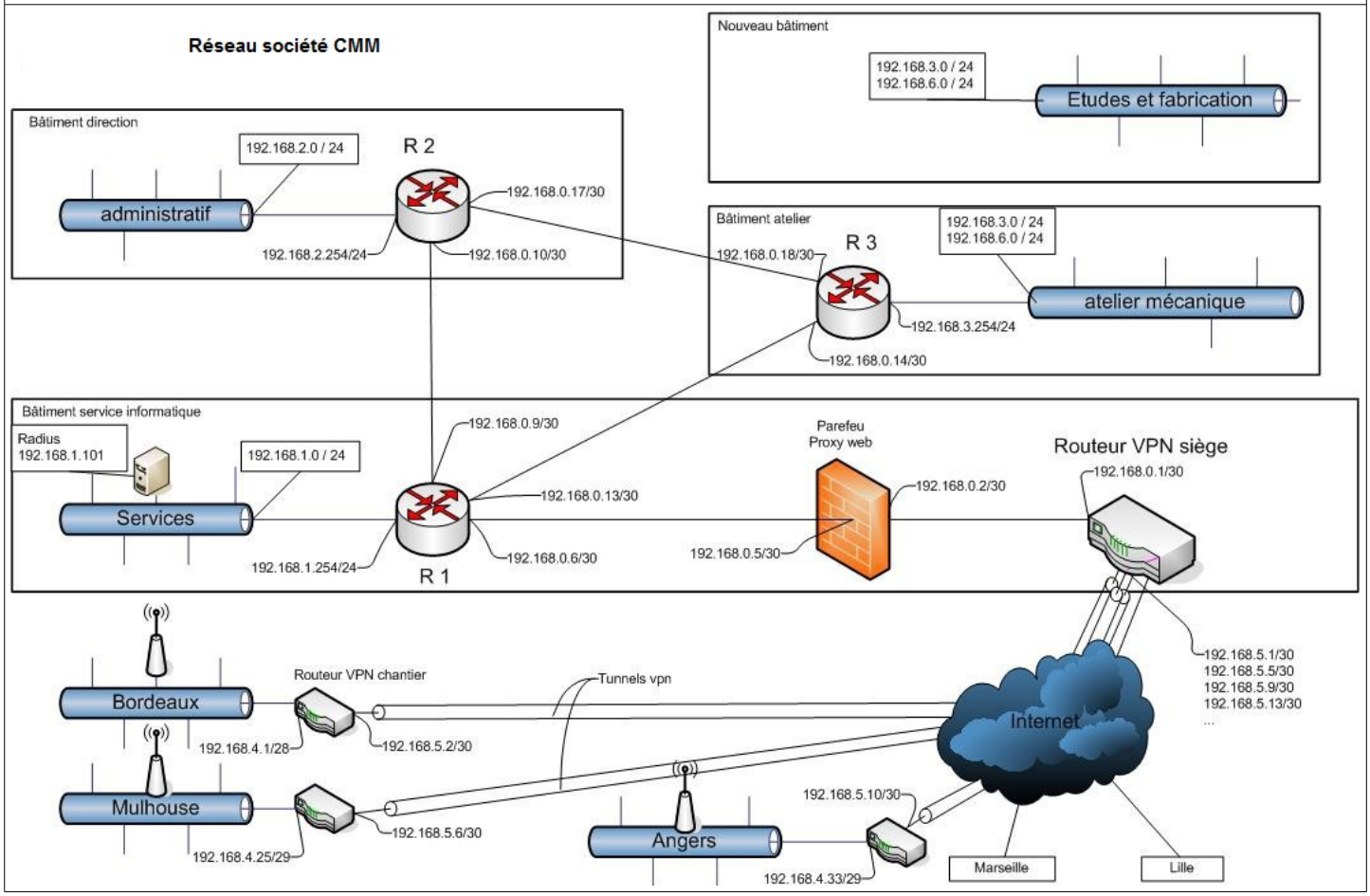
Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé nœud. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions. Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions en la débranchant du nœud sans pour autant paralyser le reste du réseau. Concrètement, le nœud est un **hub** (**concentrateur**) ou un **switch** (**commutateur**).	

8.3 Topologie en anneau

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre-eux va "avoir la parole" successivement. En réalité les ordinateurs d'un réseau en topologie anneau 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 impartissant à chacun d'entre-eux un temps de parole.	

9 Exemples d'architectures réseaux





10 Fonctionnement d'un réseau

10.1 Le modèle de référence OSI de l'ISO

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés (**SNA d'IBM, DECnet de DEC, DSA de Bull, TCP/IP du DoD**,...) 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).

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des informations avec d'autres équipements hétérogènes et issus de constructeurs différents.

Le premier objectif de la norme OSI a été de définir un modèle de toute architecture de réseau basé sur un découpage en sept couches, chacune de ces couches correspondant à une fonctionnalité particulière d'un réseau. Les couches 1, 2, 3 et 4 sont dites basses et les couches 5, 6 et 7 sont dites hautes.

Chaque couche est constituée d'éléments matériels et logiciels et offre un service à la couche située immédiatement au-dessus d'elle en lui épargnant les détails d'implémentation nécessaires.

Couches	Description
Application	est chargé de l'exécution de l'application et de son dialogue avec la couche 7 du destinataire en ce qui concerne le type ou la signification des informations à échanger (transfert de fichiers, interrogation de base de données,...)
Présentation	met en forme les informations échangées pour les rendre compatibles avec l'application destinatrice, dans le cas d'un dialogue entre systèmes hétérogènes.
Session	assure l'ouverture et la fermeture des sessions (des communications) entre usagers, définit les règles d'organisation et de synchronisation du dialogue entre les abonnés.
Transport	responsable du contrôle du transfert des informations de bout en bout, réalise le découpage des messages en paquets pour le compte de la couche réseau ou le réassemblage des paquets en messages pour les couches supérieures. **Utilise un numéro de port**
Réseau	assure le cheminement ou le routage des données groupées en paquets à travers le réseau. **Utilise l'adresse IP**
Liaison	assure un service de transport des trames sur la ligne et dispose de moyens de détection et de correction d'erreurs. **Utilise l'adresse MAC**
Physique	réalise le transfert physique des éléments binaires constitutifs des trames sur le support suivant des caractéristiques physiques, électriques et mécaniques définies par des normes.

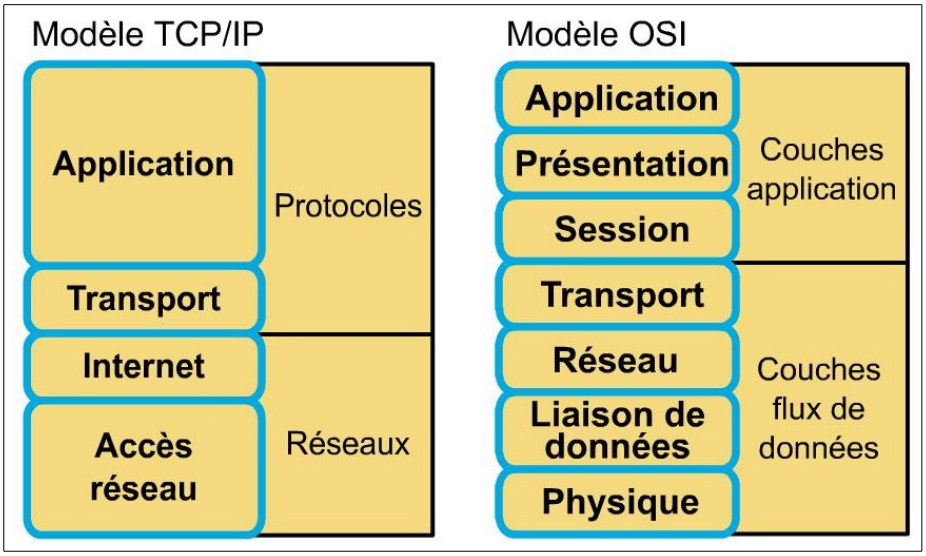
10.2 Le modèle TCP/IP

TCP/IP représente l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des données. La suite TCP/IP permet :

- Le fractionnement des données en paquets.
- L'utilisation d'un système d'adresses (IP).
- L'acheminement des données sur le réseau (routage).
- La détection et la correction des erreurs de transmission.

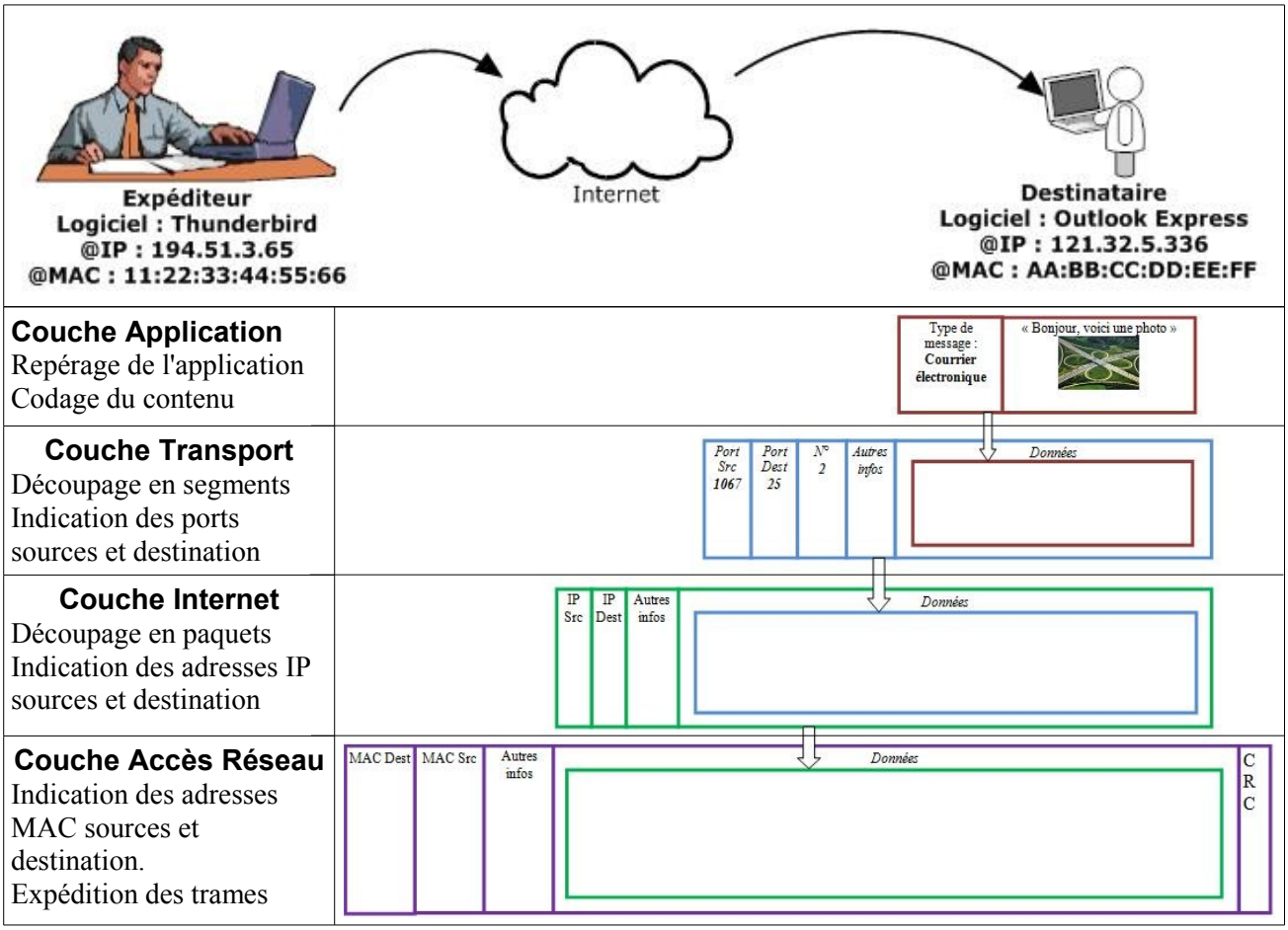
10.3 Comparaison OSI – TCP/IP

Les deux modèles ont un certain nombre de point communs et on peut établir un parallèle entre les deux :



10.4 Fonctionnement de TCP/IP

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



10.5 Principe de l'encapsulation

Chaque couche ajoute des informations à celles fournies par la couche précédente qui constituerons les « Données ». Ces informations sont appelées en-tête si elles sont rajoutées devant ou en-queue si elles sont ajoutées à la fin.

La réception, il se produit le phénomène inverse : **la décapsulation**.

10.6 Notion de protocole.

Une définition du terme « protocole » est la suivante :

Description des formats de messages et règles selon lesquelles deux ordinateurs échangeront des données.

Concrètement, cela permet, par exemple :

- L'envoi d'un message avec Outlook Express et sa lecture avec Thunderbird car le format (codage) du message est le même pour les deux logiciels.
- L'envoi des données par une carte réseau IBM sur un PC et la réception des données par une carte réseau 3COM sur un Macintosh car la façon d'ordonner les informations à transmettre est la même pour les deux cartes.
- L'envoi d'un message d'un ordinateur à un autre situé à des milliers de km car ils possèdent tous les deux une adresse IP compatible (ils utilisent et respectent le protocole IP).

10.7 Quelques protocoles.

Dans les réseaux actuels, dont Internet, les communications utilisent et respectent un certain nombre de protocoles, parmi lesquels on peut citer :

Protocoles	Utilisation
IP	
ARP, DNS	
HTTP, HTTPS	
FTP	
TCP, UDP	
ICMP	
RIP, OSPF	

Adressage IP

1 Adressage d'une machine.

Chaque hôte, que ce soit une station de travail, un routeur ou un serveur, doit avoir une adresse IP **unique**. Cette adresse ne dépend pas du matériel utilisé pour relier les machines ensemble, c'est une adresse logique notée sous forme de : w.x.y.z où ww, x, y et z sont des entiers compris entre 0 et 255.

Exemple d'adresses IP : **212.217.0.12** **193.49.148.60** **87.34.53.12**

2 Anatomie d'une adresse IP.

- Une adresse IP est un nombre de 32 bits codé sur 4 octets (octet = 8 bits) séparés par un point. On trouve souvent cette adresse avec des valeurs décimales. On appelle cette notation **le décimal pointé**. Mais il est possible de l'écrire sous forme binaire (c'est même parfois indispensable !)

Exemple : L'adresse IP **212.217.0.1** correspond à la notation binaire :

212	**217**	0	1
11010100	**11011001**	**00000000**	**00000001**

- Chaque nombre est compris entre 0 et 255, soit en binaire entre 00000000 et 11111111
- Toute adresse IP est composée de deux parties distinctes:
  - Une partie nommée Identificateur (ID) du réseau : **net-ID** située à gauche, elle désigne le réseau contenant les ordinateurs.
  - Une autre partie nommée identificateur de l'hôte : **host-ID** située à droite et désignant les ordinateurs de ce réseau.

←----------4 octets----------→

Net ID	**Host ID**
Identifiant du réseau	Identifiant du hôte

- Pour savoir où se situe la limite entre net-ID et host-ID, il faut connaitre **la classe du réseau**.

3 Deux adresses particulières.

Parmi les adresses possibles, deux sont spécifiques et ne doivent pas être utilisées par des machines :

- Tous les bits de la partie Host-ID sont à **0 : C'est l'adresse du réseau**

*Ex : **192.168.10.0*** = ***192.168.10.00000000***

- Tous les bits de la partie Host-ID sont à **1 : C'est l'adresse de diffusion (broadcast)** utilisée pour communiquer avec toutes les machines du réseau.

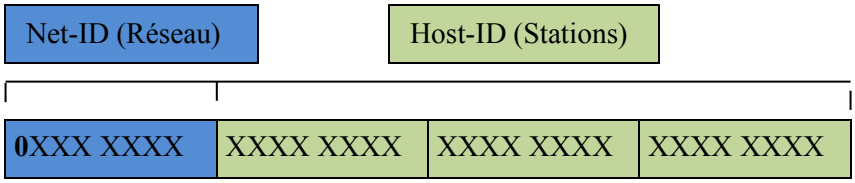
*Ex : **172.27.255.255*** = ***172.27.11111111.11111111***

4 Classes d'adresses IP.

Les réseaux TCP/IP se divisent en trois grandes classes qui ont des tailles prédéfinies, ces 3 classes de réseau sont notées **A, B** et **C** et se différencient par le nombre d'octets désignant le réseau.

4.1 Les adresses de classe A.

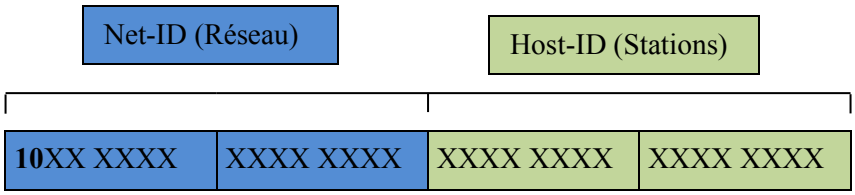
Les adresses de classe A ont une partie réseau sur 8 bits, et une partie hôte sur 24 bits.
Leur bit de poids le plus fort est 0, ce qui permet de les distinguer des autres classes.



1ère adresse de réseau	
Dernière adresse de réseau	
Nombre de réseaux possibles	
Nombre de bits pour les stations	
Nombre de stations possibles	

4.2 Les adresses de classe B.

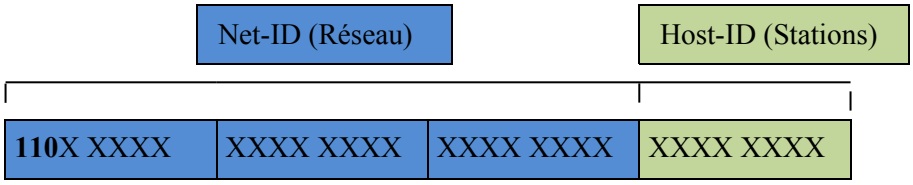
Les adresses de classe B ont une partie réseau sur 16 bits, et une partie hôte de même taille.
Leurs deux bits de poids forts sont 10, ce qui permet de les distinguer des autres classes.



1ère adresse de réseau	
Dernière adresse de réseau	
Nombre de réseaux possibles	
Nombre de bits pour les stations	
Nombre de stations possibles	

4.3 Les adresses de classe C.

Les adresses de classe C ont une partie réseau sur 24 bits, et une partie hôte sur 8 bits.
Leurs trois bits de poids fort sont 110, ce qui permet de les distinguer des autres classes.



1ère adresse de réseau	
Dernière adresse de réseau	
Nombre de réseaux possibles	
Nombre de bits pour les stations	
Nombre de stations possibles	

4.4 Autres classes.

Il existe une classe D (qui commence par 1110) mais cette classe d'adresse n'est pas utilisée pour adresser des machines individuelles. Ce sont des adresses appelées multicast qui permettent par exemple d'envoyer de la vidéo sur plusieurs machines simultanément.

1ère adresse de réseau	
Dernière adresse de réseau	

Enfin, les réseaux dont l'adresse commence par 11111 sont des réseaux de classe E. Ces adresses sont réservées pour la recherche et donc ne sont pas utilisées pour adresser des machines.

1ère adresse de réseau	
Dernière adresse de réseau	

4.5 Adresses non utilisées :

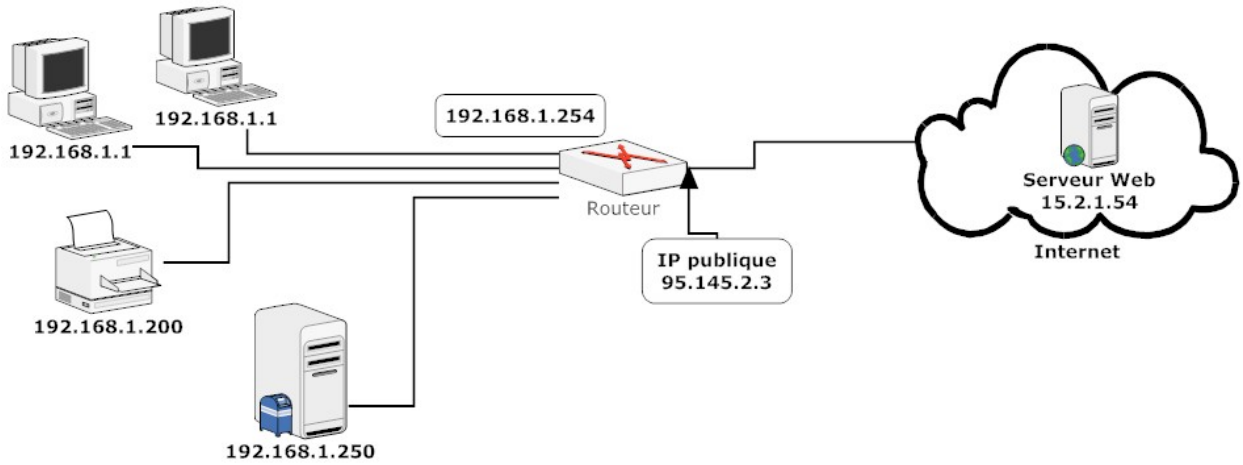
Certaines adresses réseaux ne sont pas utilisées pour adresser des machines. Il s'agit des réseaux :

- **0.X.X.X** Le premier réseau. La première adresse **0.0.0.0 désigne les réseaux inconnus**.
- **127.X.X.X** Ce réseau désigne l'ordinateur lui-même (localhost=127.0.0.1). Cette adresse est dite **de bouclage.** Elle permet notamment d'effectuer des tests.

5 IP publique, IP privée.

Le schéma ci-dessous présente un réseau local relié à Internet par un routeur.
Ce routeur possède deux adresses IP :

- Une IP publique, achetée ou fournie par le FAI.
- Une IP privée, librement paramétrée par l'administrateur du réseau local.



L'organisme gérant l'espace d'adressage public (adresses **IP** routables) est :

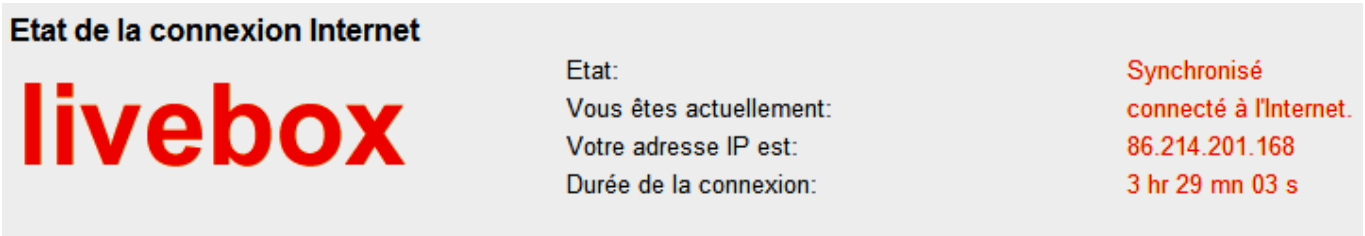
Internet Assigned Number Authority (**IANA**).

La RFC 1918 définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses **IP** aux machines de son réseau interne sans risque d'entrer en conflit avec une adresse **IP publique** allouée par l'IANA. Ces adresses dites non-routables correspondent aux plages d'adresses suivantes :

- **Classe A : plage de 10.0.0.0 à 10.255.255.255 ;**
- **Classe B : plage de 172.16.0.0 à 172.31.255.255 ;**
- **Classe C : plage de 192.168.0.0 à 192.168.255.55**

En résumé :

Les adresses publiques sont utilisées sur Internet (et sont donc uniques) alors que les adresses privées ne peuvent pas circuler sur Internet. Un modem-routeur connecté à Internet possède donc une IP privée (coté LAN) et un IP publique (côté WAN). Voir schéma ci-dessus.



6 Masque de réseau.

Pour que le réseau Internet puisse router (acheminer) les paquets de données, il faut qu'il connaisse l'adresse du réseau de destination. Pour déterminer cette adresse réseau à partir de l'adresse IP de destination, on utilise le masque de sous réseau.

6.1 Masque par défaut.

A chaque classe d'adresses est associé un **masque de réseau par défaut**, ou **netmask**, qui est constitué de 32 bits. Le tableau suivant fournit les différents masques pour les trois classes traditionnelles.

Classes d'adresses	Bits utilisés pour le masque de sous-réseau				Notation décimale
Classe A	1111 1111	0000 0000	0000 0000	0000 0000	
Classe B	1111 1111	1111 1111	0000 0000	0000 0000	
Classe C	1111 1111	1111 1111	1111 1111	0000 0000	

Un « **ET** » logique appliqué entre le masque de réseau et l'adresse IP permet d'obtenir l'adresse d'un réseau correspondant.

6.2 Calcul de l'adresse réseau.

Adresse IP	**193** 1100 0001	**252** 1111 1100	**19** 0001 0011	**3** 0000 0011
Masque				
Adresse du réseau				

6.3 Calcul de l'adresse hôte en binaire

Adresse IP				
Complément du masque				
Adresse de l'hôte				

Ainsi, à l'aide du masque de réseau, on peut donc définir, pour toute adresse IP :

- L'adresse réseau associée,
- La partie hôte associée,
- L'adresse de diffusion associée qui désigne tous les hôtes de ce réseau (partie hôte à 1)

7 Trois adresses spéciales

Il existe dans les réseaux trois types d'adresses, les adresses locales, les adresses de broadcast, et les adresses multicast.

Pour résumer :

- **Je parle directement à quelqu'un (unicast)**
- **Je parle à tout le monde (broadcast)**
- **Je parle à un groupe restreint (multicast)**

8 En bref

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques

Administrer un réseau

1 Le réseau local

Un réseau informatique est un ensemble d'au moins deux ordinateurs reliés les uns aux autres afin qu'ils puissent échanger des informations. Le réseau permet de :

☞ **Partager les fichiers** : Les données circulent par un câble et non par disquettes (source d'infection par virus). Données copiées de manière permanente sur un ordinateur et tous les ordinateurs du réseau pourront y accéder
☞ **Partager les ressources** : Imprimante, CDRom, modem, Disque Dur…
☞ **Partager les applications** : Travail dans un environnement multi-utilisateurs (exemple de Word sur un disque partagé)
☞ **Limite la perte de temps** : Mise à jour plus facile lors du changement de version
☞ **Limite la perte de place** : Libère de l'espace sur les postes de travail
☞ **Gain financier** : Souvent une imprimante pour tous, 10 licences réseau moins chères que 10 licences individuelles
Il existe 2 grands types de réseau **WAN** (**Wide Area Network**) et **LAN** (**local Area Network**).
Ce deuxième type est lui-même divisé en 2 sous types : **poste à poste** et **serveur dédié**.

1.1 Station de travail et serveur

La station de travail

C'est un microordinateur disposant de ses propres **ressources**, c'est-à-dire lecteur de CD/DVD, disque dur, … et pouvant accéder à celles du serveur (du moins à celles autorisées par l'administrateur du réseau).
Elle est souvent appelée **nœud** du réseau.
Les stations entre elles peuvent également se partager des fichiers.

Le serveur

C'est le microordinateur qui héberge les ressources **partagées** (espace disque, imprimante, unité de sauvegarde, lecteur de CD-Rom).
Il est souvent plus **performant** au niveau capacité matérielle que les autres ordinateurs du réseau. Dans certains réseaux, un ordinateur peut être à la fois station et serveur.

Le fait de répartir le travail entre plusieurs serveurs permet d'optimiser les différentes tâches, d'où la mise en place de serveurs **spécialisés** :

- Serveurs de fichiers et d'impression,
- Serveurs d'applications,
- Serveurs de messagerie,
- Serveurs de télécopie,
- Serveurs de communication
- Serveurs de services d'annuaire.

1.2 Réseaux poste à poste

C'est un réseau sur lequel on ne fait aucune distinction entre les **postes**. Sur ces réseaux, tous les ordinateurs sont considérés **égaux** en droits, capables de jouer le rôle de **client**, de **serveur** ou des deux à la fois. Chaque ordinateur du réseau est un poste qui peut partager ses **fichiers** et ses **imprimantes** avec les autres ordinateurs du réseau et, dans le même temps, utiliser d'autres **ressources partagées** du réseau.

1.3 Réseaux à serveur dédié (c'est celui que l'on va étudier)

Chaque ordinateur du réseau fait office soit de **serveur**, soit de **client**, mais pas les deux.
Les ordinateurs classés dans la catégorie des serveurs se consacrent exclusivement à leur rôle de serveur ; ils ne sont pas utilisés en tant que clients.
Le serveur **partage** ses **imprimantes**, ses **fichiers** et ses **applications** avec les autres ordinateurs. Les autres ordinateurs sont des **clients**, qui accèdent aux **ressources** que le serveur partage avec eux.
De la même manière, sur un réseau à serveur dédié, les ordinateurs clients ne font jamais office de serveurs. Toutes les ressources partagées sur le réseau sont offertes par le serveur et utilisées par les clients.

1.4 Facteurs de choix entre un réseau poste à poste et un serveur dédié

- **La taille de l'entreprise (>10 ➔ serveur dédié),**
- **Le niveau de sécurité,**
- **La nature du travail,**
- **Le niveau de compétences administratives disponibles,**
- **Le volume de trafic sur le réseau,**
- **Les besoins des utilisateurs,**
- **Le budget alloué pour le réseau.**

1.5 Logiciel réseau ou gestionnaire

Pour gérer le partage des ressources du serveur, le réseau fonctionne sous le contrôle d'un logiciel appelé **gestionnaire**.
Son rôle est, entre autre, de gérer les droits des utilisateurs accédant aux ressources partagées
Une personne est chargée d'assurer la gestion du réseau c'est **l'administrateur**.

2 Rôle de l'administrateur de réseau

- ☞ Gérer les **utilisateurs**
- ☞ Gérer les **ressources**
- ☞ Configurer les **postes**
- ☞ Surveiller le **réseau**

3 Les outils d'administration

- ☞ Le moniteur système
- ☞ L'observateur réseau
- ☞ L'éditeur de stratégie système
- ☞ L'outil tâches planifiées
- ☞ L'éditeur du registre
- ☞ L'outil Systems Management Server

4 Gérer les ressources partagées d'un réseau

Les points suivants, dépendent des serveurs de réseau :

- ☞ Gérer des fichiers partagés
- ☞ Gérer des lecteurs partagés
- ☞ Gérer des imprimantes partagées

5 Sécuriser un réseau

- ☞ Élaborer une stratégie de sécurisation
- ☞ Signaler les problèmes de sécurité
- ☞ Minimiser les pertes de données accidentelles
- ☞ Prévoir les infections par les virus
- ☞ Prévenir les attaques de pirates

6 Protéger contre les catastrophes

- ☞ Élaborer une stratégie de sauvegarde
- ☞ Précautions contre les problèmes d'alimentation électrique
- ☞ Élaborer une stratégie de redondance

7 Les différents systèmes d'exploitation multiutilisateurs

Windows 2000 Server, 2003 Server, 2007 Server de Microsoft, UNIX de Sun, Linux OpenSource ou Netware de Novell.

8 Concepts Réseaux

8.1 Domaine

Bien que la notion de « Groupe de travail » (au sens Workgroup) soit maintenue c'est désormais la notion de domaine qui s'impose dans une architecture réseau. Il s'agit de **l'ensemble** des machines, des services et des utilisateurs travaillant autour d'un (ou plusieurs) serveurs. Ce domaine est nommé et il est requis à la **connexion**.

8.2 Serveur

Au sens traditionnel du terme, c'est une machine qui offre des services aux utilisateurs (clients). Trois types de serveurs :

- **serveur primaire de domaine** : il est obligatoire et unique dans un domaine. C'est lui qui maintient la base des comptes utilisateurs (SAM)
- **serveur secondaire de domaine** : il peut y en avoir plusieurs. Il vient en secours d'un serveur primaire (en cas de besoin). Il maintient une copie de la base des comptes utilisateurs (SAM).
- **serveur autonome** : serveur banalisé ; serveur d'application, serveur d'impression, serveur d'accès distant, serveur DNS,...

2000 et 2003 Server ne hiérarchise plus les serveurs, mais parle d'arborescence de serveurs qui contiennent tous une copie en lecture/écriture de la base **d'annuaire** :

- **contrôleur de domaine** : au moins un par domaine. C'est lui qui maintiendra la base des comptes utilisateurs (SAM). Il peut y en avoir plusieurs. Ils viendront en secours du 1er serveur installé (en cas de besoin). Il maintient une copie de la base des comptes utilisateurs.
- **serveur autonome :** serveur banalisé; serveur d'application, serveur d'impression, serveur d'accès distant, serveur DNS,...

Linux reprend la notion de contrôleur de domaine qui à travers le service **Samba** va authentifier les postes clients et les utilisateurs, tout en leur permettant l'accès aux données partagées.

- Les fichiers SMBusers et SMBpasswd contiennent les utilisateurs et leur mot de passe.
- Le fichier SMB.conf contient la configuration du contrôleur avec les partages et les droits des utilisateurs.

8.3 Active Directory

Active Directory est le nom du service **d'annuaire** de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire *Active Directory* est basé sur les standards TCP/IP, DNS, LDAP (*Lightweight Directory Access Protocol*, protocole qui permet d'accéder de façon standard aux différents services de l'annuaire), Kerberos (protocole d'authentification réseau à clé secrète développé par le MIT dans le cadre du projet « Athéna »), etc.
Il s'agit d'une base d'annuaire qui va regrouper tous les objets **réseaux** (données utilisateur, serveurs, imprimantes, applications, bases de données, groupe, ordinateurs et stratégies de sécurité, etc).
Les bénéfices de cette base d'annuaire sont :

- l'administration simplifiée du réseau : AD permet l'accès à toutes ces ressources à partir d'un seul et unique point d'administration.
- les utilisateurs n'ont pas à se préoccuper de la structure physique du réseau pour accéder aux ressources
- une structure hiérarchique flexible
- la capacité de montée en charge qui autorise le stockage de plusieurs millions de ressources
- une forte tolérance de pannes : AD est distribuée sur chaque serveur du domaine

8.4 NTFS (NT File System)

C'est la sécurité au sens NT du terme. C'est un type de formatage du disque (ou de certaines partitions) requis pour pouvoir mettre en oeuvre cette sécurité
SGF (Système de Gestion de Fichiers) natif de Windows NT, et de la plupart des versions suivantes des systèmes de Microsoft, utilisant une **MFT** (Master File Table, table des fichiers principales). À l'origine, c'était surtout de la FAT un peu améliorée, puis de nombreuses améliorations lui ont été intégrées :

- le support des noms Unicode (codage des caractères sur 16 bits),
- la sécurité,
- la compression,
- le chiffrement,
- une gestion de quotas (sous W2000Server)

8.5 Utilisateur

Une personne connue dans le **domaine**. Elle a accès aux ressources du domaine en fonction des **permissions** qui lui sont accordées. Il est recommandé de les rassembler en **groupes**.

8.6 Groupe

Un ensemble d'**utilisateurs** d'un même domaine ayant des points communs. Le but du groupe est de simplifier l'administration. On distingue :

- les groupes locaux (définis localement dans un domaine)
- les groupes globaux (qui peuvent s'exporter vers d'autres domaines)
- les groupes spéciaux : prédéfinis dans 2000Server.

Exemple : le groupe « tout le monde »

8.7 Profil

C'est l'environnement de l'**utilisateur**. Généralement, ce profil est maintenu sur le « client » : **profil local**.
Il peut être mémorisé sur un **serveur** du domaine. Il est alors baptisé **profil errant** car il est téléchargé lors de la 1ère connexion de l'utilisateur sur un poste client.
Il peut, éventuellement, être défini, restreint et figé par l'administrateur, il est alors dit **obligatoire**.

8.8 Partage

Point d'accès dans une arborescence. Se caractérise par un **nom de partage** (*Ex : APPS pour le répertoire des applications sur le serveur*) et des **permissions de partage** accordées aux utilisateurs sur cette arborescence (ne pas confondre avec les **permissions NTFS**).

8.9 Permissions

- permissions de sécurité NTFS : les droits posés sur des fichiers et des répertoires pour définir (limiter) les accès aux utilisateurs.
- permissions de partage : notion identique à la précédente mais qui ne s'applique que dans le cadre d'un accès au travers d'un « partage », classiquement un accès via le réseau (depuis un client) à une ressource et décrite sous la forme \\serveur\partage\ressource

8.10 Nommage des ressources - UNC (Universal Naming Ressource)

Syntaxe : \\serveur\ressource\répertoire\fichier
Exemple : \\W2000S\APPS\Office\excel.exe

8.11 Principales commandes réseaux

- **PING : tester la connectivité réseau avec une adresse IP distante w.x.y.z**

```
ping w.x.y.z

ping -t w.x.y.z
```

L'option -t permet de faire des pings en continu jusqu'à Ctrl-C.

- **TRACERT : affiche toutes les adresse IP intermédiaires par lesquelles passe un paquet entre la machine local et l'adresse IP spécifiée w.x.y.z**

```
tracert w.x.y.z

tracert -d w.x.y.z
```

Pour tester la connectivité réseau et si la commande ping ne donne pas de réponse, il convient de lancer cette commande pour voir à quel niveau le paquet ou la connectivité est défaillante.

- **IPCONFIG : afficher ou rafraîchir la configuration réseau TCP/IP**

```
ipconfig [/all][/release][/renew][/flushdns][/displaydns][/registerdns][-a]
```

Cette commande exécutée sans option, affiche l'adresse IP en cours, le masque réseau ainsi que la passerelle par défaut au niveau des interfaces connues sur la machine.

`/all`	affiche toute la configuration réseau y compris les serveurs DNS, WINS, bail DHCP, etc ...
`/renew`	renouvelle la configuration DHCP de tous les cartes
`/release`	Envoie un message DHCPRELEASE au serveur DHCP pour libérer la configuration DHCP actuelle et annuler la configuration d'adresse IP de toutes les cartes. Ce paramètre désactive TCP/IP pour les cartes configurées de manière à obtenir automatiquement une adresse IP.
`/flushdns`	Vide et réinitialise le contenu du cache de résolution du client DNS. Au cours de la résolution des problèmes DNS, vous pouvez utiliser cette procédure pour exclure les entrées de cache négatives ainsi que toutes les autres entrées ajoutées de façon dynamique.
`/displaydns`	Affiche le contenu du cache de résolution du client DNS, qui inclut les entrées préchargées à partir du fichier des hôtes locaux ainsi que tous les enregistrements de ressources récemment obtenus pour les requêtes de noms résolues par l'ordinateur. Le service Client DNS utilise ces informations pour résoudre rapidement les noms fréquemment sollicités, avant d'interroger ses serveurs DNS configurés
`/registerdns`	Actualise tous les baux DHCP et réinscrit les noms DNS.