ISN
Informatique et Sciences du Numérique

Académie d'Aix-Marseille - Formation ISN

INITIATION AU RESEAUX

Niveau 1

Programme de formation :

- Notions de paquet et de protocole.
- Transmission d'information point à point, (liaison sérielle), détection et correction d'erreurs de transmission.
- Réseaux local, réseau global, différents types d'adressage.
- Routage, nommage, TCP / IP.
- Équipement réseau (hub, switch, routeur, ...).

Questions didactiques :

- Observation et simulation d'un réseau en fonctionnement au moyen de logiciels dédiés ;
- Analyse des problèmes posés par la supranationalité des réseaux ;
- Questions juridiques et philosophiques liées à la circulation de l'information.

Les compétences suivantes doivent être développées :

- Établir une communication sérielle entre deux machines ;
- Analyser le trafic sur une liaison sérielle ;
- Décrire une situation d'adressage sur un type de réseau particulier ;
- Analyser les entêtes de messages électroniques, pour décrire le chemin suivi par l'information ;
- Piloter un système de lecture et d'écriture de données numériques.

Sommaire

1 Vivre dans un monde en réseau

1.1 Adaptation des réseaux à notre mode de vie :

Parmi les éléments essentiels à l'existence humaine, le besoin de communiquer arrive juste après le besoin de survie. Le besoin de communiquer est aussi important pour nous que l'air, l'eau, la nourriture et le gîte.

Les méthodes dont nous nous servons pour partager idées et informations changent et évoluent sans cesse. Si le réseau humain se limitait autrefois à des conversations en face à face, aujourd'hui les découvertes en matière de supports étendent sans cesse la portée de nos communications. De la presse écrite à la télévision, chaque innovation a développé et amélioré nos moyens de communication.

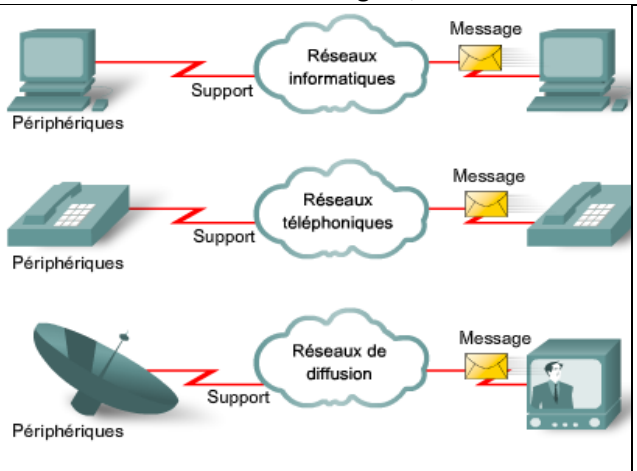
Pierre de Rosette
British Museum

Phidippidès annonce la victoire de Marathon
Luc-Olivier Merson, 1869

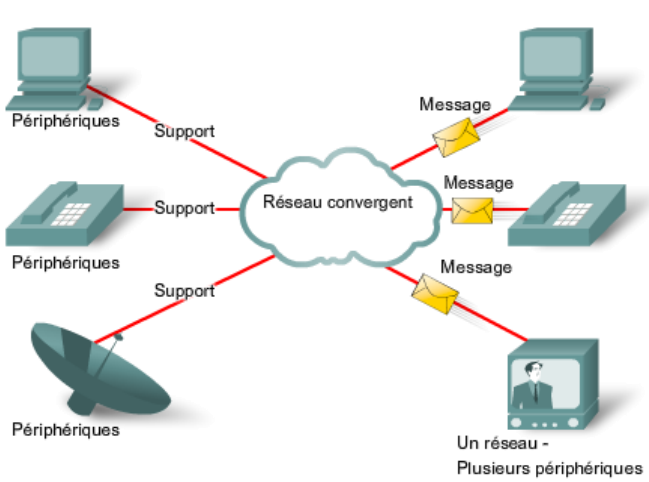
Installation satellite de la quatrième conférence Panafricaine Mondiale des Radios Communautaires
Côte d'Ivoire 2009

Des moyens de communication autrefois séparés et bien distincts convergent maintenant sur une plateforme commune. Les réseaux classiques de transfert de données téléphoniques, de radio, de télévision ou informatiques intègrent tous leur propre version des éléments de base constituant les réseaux. Autrefois, chacun de ces services nécessitait une technologie différente pour acheminer son signal de communication particulier. En outre, chaque service avait son propre ensemble de règles et de normes destiné à assurer le succès des communications de ses services sur un support spécifique.

Les progrès technologiques nous permettent aujourd'hui de réunir ces réseaux disparates sur une même plateforme, une plateforme définie comme étant un réseau convergent. Le fait que les flux (circulation) vocaux, vidéo et de données empruntent le même réseau rend inutile la création et la maintenance de réseaux séparés. Si de nombreux points de contact et périphériques spécialisés (par exemple des ordinateurs personnels, téléphones, télévisions, assistants personnels et lecteurs sur le point de vente) continuent à cohabiter sur un réseau convergent, l'infrastructure réseau, quant à elle, est unique et commune.



Autrefois, réseaux de communications séparés



Aujourd'hui, réseaux convergents

À l'image de tous les progrès dans le domaine des technologies de la communication, la création et l'interconnexion de réseaux de données ont un profond impact sur la société.

La nature instantanée des communications sur Internet encourage la formation de communautés internationales. Ces communautés favorisent à leur tour des interactions sociales pour lesquelles géographie et fuseaux horaires n'ont aucune importance.

« *Après les élections américaines, qui avaient démontré au monde la puissance mobilisatrice des réseaux sociaux (Facebook et MyBarackobama.com), c'est la crise iranienne qui a sensibilisé la planète au pouvoir d'information des sites dits de "microblogging", dont Twitter.com est le premier à toucher une audience internationale. Depuis les rues de Téhéran, les témoignages en temps réel ont afflué sur Twitter pour étancher la soif d'expression des jeunes Iraniens, et combler l'appétit d'information de médias classiques empêchés de faire leur travail sur place. …* » Internet et son potentiel démocratique – Le Monde (21/08/09).

La rapidité avec laquelle Internet s'est intégré à notre quotidien est tout simplement stupéfiante. Les interconnexions complexes entre périphériques et supports électroniques qui constituent le réseau sont transparentes pour les millions d'utilisateurs qui ont fait d'Internet un élément important et personnel de leur vie.

Les réseaux de données, destinés à l'origine au transport d'informations d'une entreprise à une autre, ont acquis une nouvelle finalité : ils améliorent la qualité de vie des individus partout dans le monde. Au cours d'une seule journée, les ressources disponibles sur Internet peuvent nous aider à :

- choisir en ligne ce que nous allons porter en fonction des conditions météorologiques du jour ;
- déterminer le trajet le moins embouteillé en visualisant les vidéos du trafic routier et des conditions météo transmises par les webcams ;
- consulter notre compte bancaire et payer nos factures en ligne ;
- recevoir et envoyer des courriels ou passer un appel téléphonique via Internet de quasiment partout ;
- rechercher des informations médicales et obtenir des conseils nutritionnels d'experts du monde entier, puis publier un message sur un forum pour partager des renseignements sur une maladie ou un traitement ;
- télécharger de nouvelles recettes et techniques de cuisson pour préparer un dîner mémorable ;
- publier des photographies, vidéos personnelles et expériences et les partager avec des amis ou avec le monde entier.
- …

L'apparition puis l'adoption généralisée d'Internet ont entraîné la création de nouvelles formes de communication qui permettent à l'utilisateur de créer des informations pouvant être lues par le plus grand nombre.

- Messagerie instantanée (chat),
- Blogs (cyber carnet, page web perso régulièrement mise à jour et offrant la possibilité de discussion),
- Wikis (site web dont les pages sont modifiables par les visiteurs, site collaboratif),
- Podcast (fichiers multimédia téléchargeable pour consultation sur baladeur numérique,
- Outils de collaboration (permettent le travail sur des documents partagés. des personnes résidant dans des régions éloigner peuvent collaborer à la création d'un document commun),
- Sites sociaux (réseaux sociaux, partage multimédia, sites de rencontre, …) ;
- …

1.2 Etablir une connexion

Dans notre vie quotidienne, les communications revêtent bien des formes et se produisent dans de nombreux environnements différents. Nos attentes sont différentes selon que nous discutons sur Internet ou participons à un entretien d'embauche. À chaque situation correspondent des comportements et des styles attendus.

Avant de commencer à communiquer, nous établissons des règles, ou conventions, qui régissent la conversation. Ces règles ou protocoles doivent être respectés pour que le message soit correctement transmis et compris. Parmi les protocoles qui régissent nos communications pour qu'elles se déroulent correctement, citons :

- l'identification de l'expéditeur et du destinataire ;
- le recours à une méthode de communication convenue (face-à-face, téléphone, lettre, photographie) ;
- l'utilisation d'une langue et d'une syntaxe communes ;
- la vitesse et le rythme d'élocution ;
- la demande de confirmation ou d'accusé de réception.

Les règles régissant la communication peuvent varier en fonction du contexte. Si un message mentionne un fait ou un concept important, il est nécessaire de confirmer que le message a été reçu et compris. Les messages moins importants n'exigent pas toujours d'accusé de réception de la part du destinataire.

Les techniques utilisées dans le cadre des communications réseaux partagent ces mêmes exigences fondamentales avec les conversations directes entre personnes. Étant donné qu'un grand nombre des protocoles s'appliquant aux communications humaines sont implicites ou intégrés à notre culture, certaines règles n'ont pas besoin d'être précisées. Mais lorsque nous établissons des réseaux de données, nous devons être beaucoup plus explicites sur la façon dont la communication s'effectuera et sur ce qui en assurera le succès.

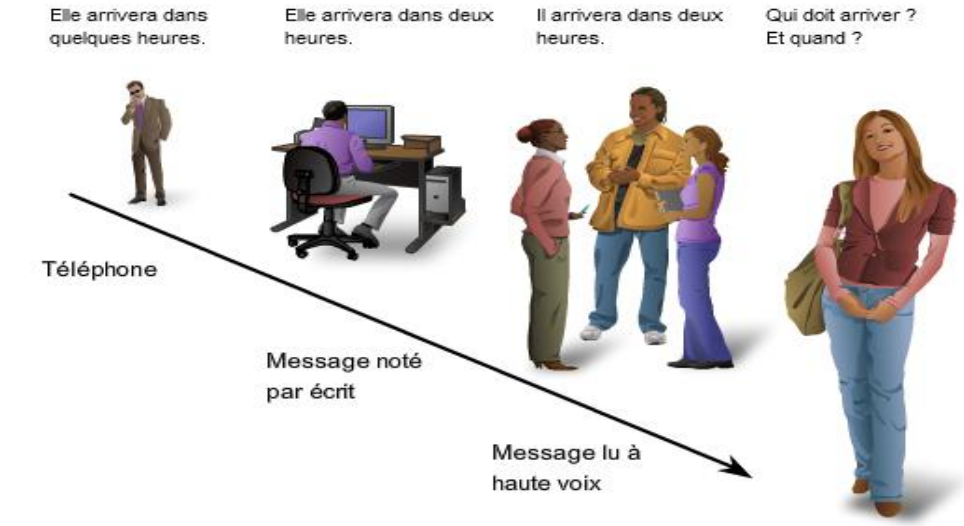
Première étape : Se mettre d'accord sur la méthode à utiliser pour communiquer.	
Deuxième étape : Se mettre d'accord sur le langage à utiliser pour se comprendre.	

Troisième étape : Transmettre le message et accuser réception.	

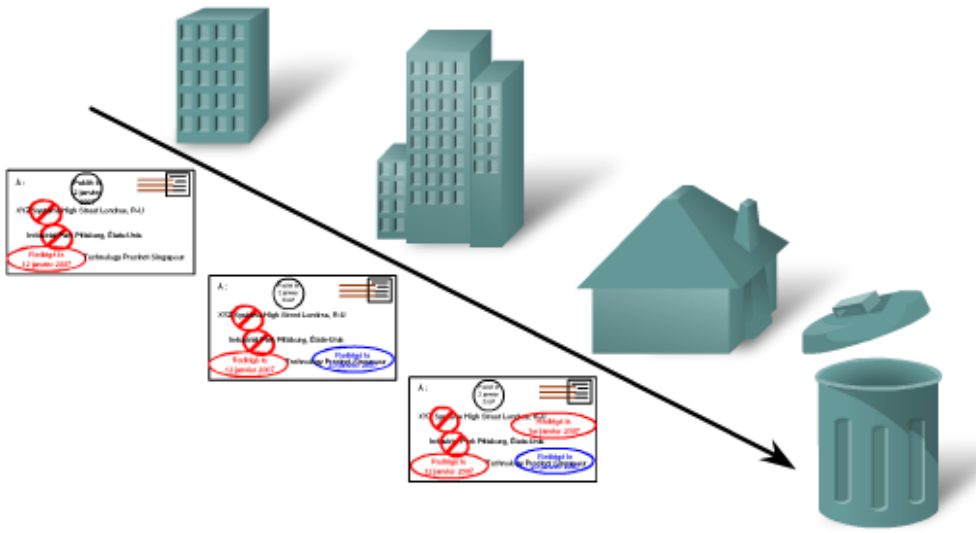
1.3 Qualité des communications : Facteurs externes

Les facteurs externes qui affectent la communication sont liés à la complexité du réseau et au nombre de périphériques par lesquels le message doit transiter avant d'atteindre sa destination finale.

- Parmi les facteurs externes affectant la réussite d'une communication, citons :
- la qualité du chemin d'accès séparant l'expéditeur du destinataire ;
- le nombre de fois où le message doit changer de forme ;
- le nombre de fois où le message doit être redirigé ou réadressé ;
- la quantité d'autres messages transmis simultanément sur le réseau de communications ;
- le délai alloué à une communication réussie.



Les informations ayant été encodées et décodées à plusieurs reprises risquent de ne pas être transmises correctement.



Les messages ayant été réadressés et redirigés à plusieurs reprises risquent de ne pas être remis correctement.

1.4 Qualité des communications : Facteurs internes

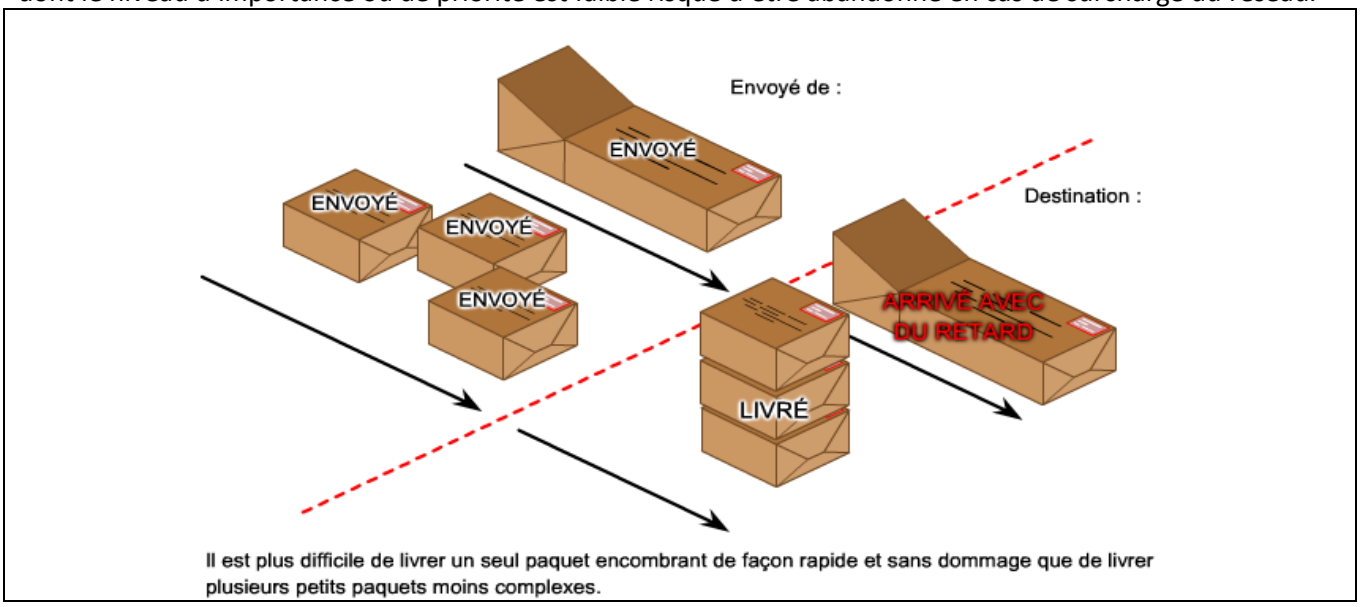
Les facteurs internes gênant la communication réseau sont liés à la nature même du message.

La complexité et l'importance des différents types de messages peuvent varier. Il est généralement plus facile de comprendre des messages clairs et concis que des messages complexes. Il faut apporter plus de soins aux communications importantes pour veiller à ce qu'elles soient reçues et comprises par leurs destinataires.

Parmi les facteurs internes affectant la réussite d'une communication sur le réseau, citons :

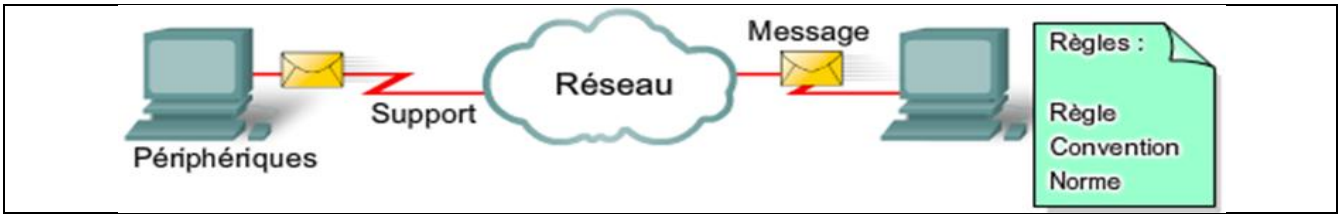
- la taille du message ;
- la complexité du message ;
- l'importance du message.

Les messages volumineux peuvent être interrompus ou retardés en plusieurs points du réseau. Un message dont le niveau d'importance ou de priorité est faible risque d'être abandonné en cas de surcharge du réseau.



1.5 Eléments 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.



L'étude des réseaux fait largement appel aux représentations graphiques et des symboles sont couramment employés pour représenter les périphériques réseau et leurs connexions.

On distingue deux types de périphériques :

Les périphériques terminaux :

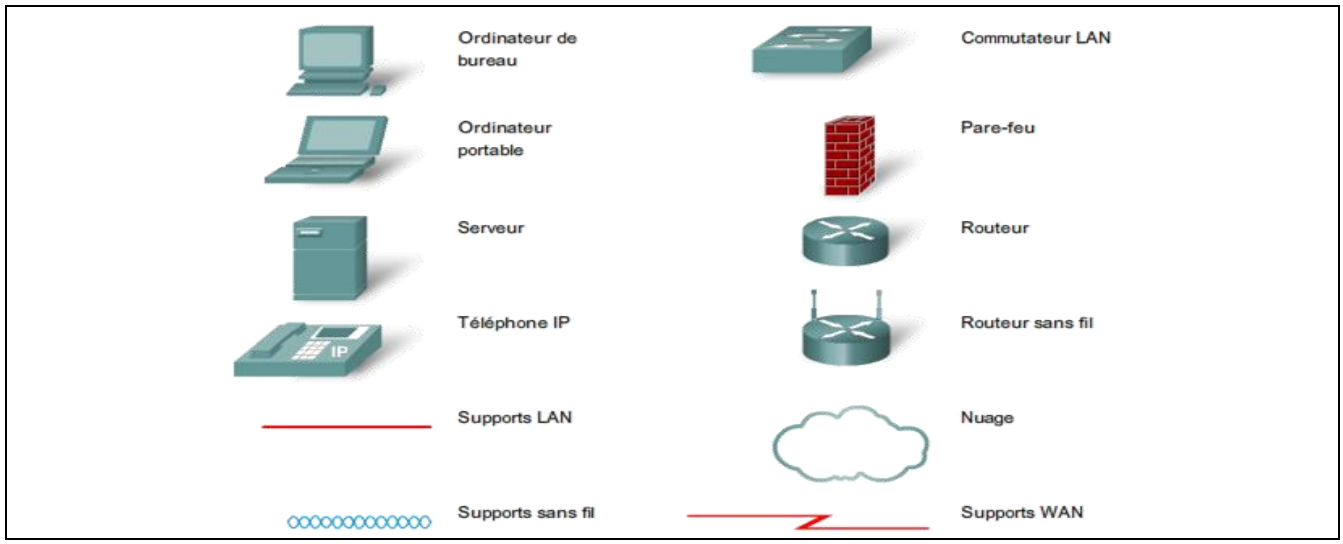
- Serveurs,
- Ordinateurs de bureau,
- Ordinateurs portables,
- Imprimantes,
- Téléphones IP,
- PDA, web phone,
- …

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 et dont les détails ne présentent peut-être pas d'intérêt pour la discussion en cours)
- …

Les connexions :

- Filaires (câble droit, croisé, téléphonique, série, …),
- Sans-fil (WiFi, GSM, GPRS, Bluetooth, ZigBee, …),
- Optique (fibre monomode, multimode, …).



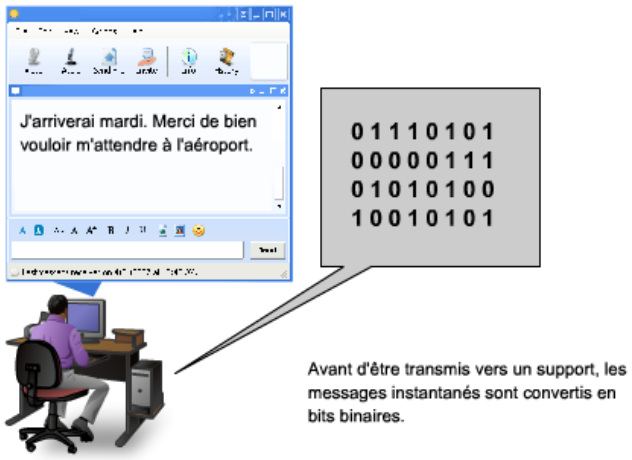
Pour envoyer et recevoir des messages divers et variés on utilise des applications informatiques qui ont besoin que le réseau leur fournisse certains services. Ces services sont régis par des règles, ou protocoles.

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.

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.

Service	Protocole (« Règle »)
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
Courriel	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Message instantané (Jabber, AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
Téléphonie sur IP	SIP (Session Initiation Protocol)

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.



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

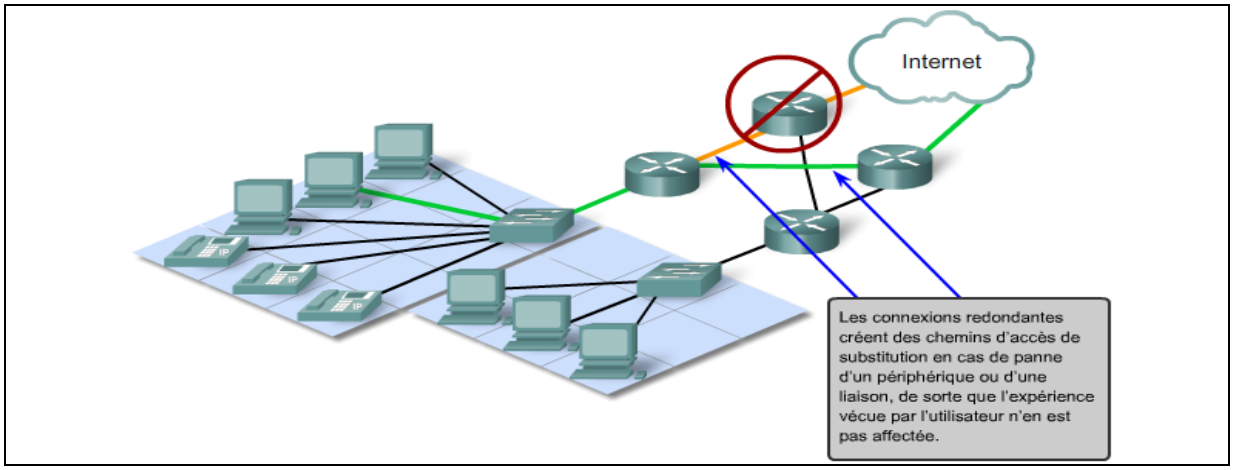
La carte réseau du PC génère des signaux électriques qui représentent les bits qu'elle place sur le support. Les bits arrivent sur le premier périphérique réseau.

1.6 Architecture réseau

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. Dans le contexte actuel, l'expression « architecture réseau » désigne aussi bien les technologies prenant en charge l'infrastructure que les services programmés et les protocoles qui déplacent les messages dans l'infrastructure. 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.

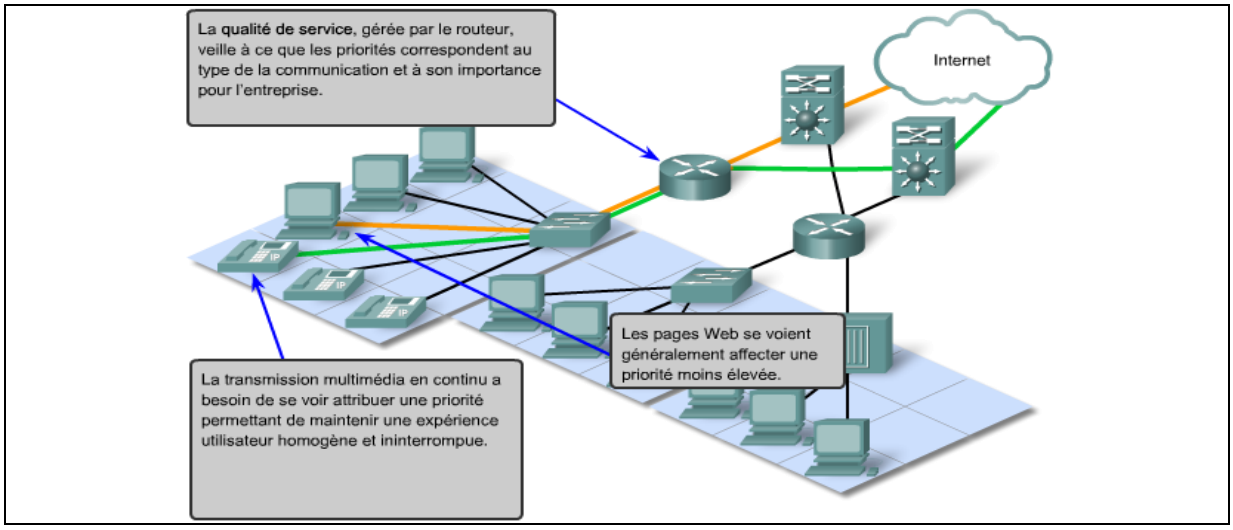
- **Tolérance aux pannes :**

  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 logiques 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.



- **Évolutivité :**

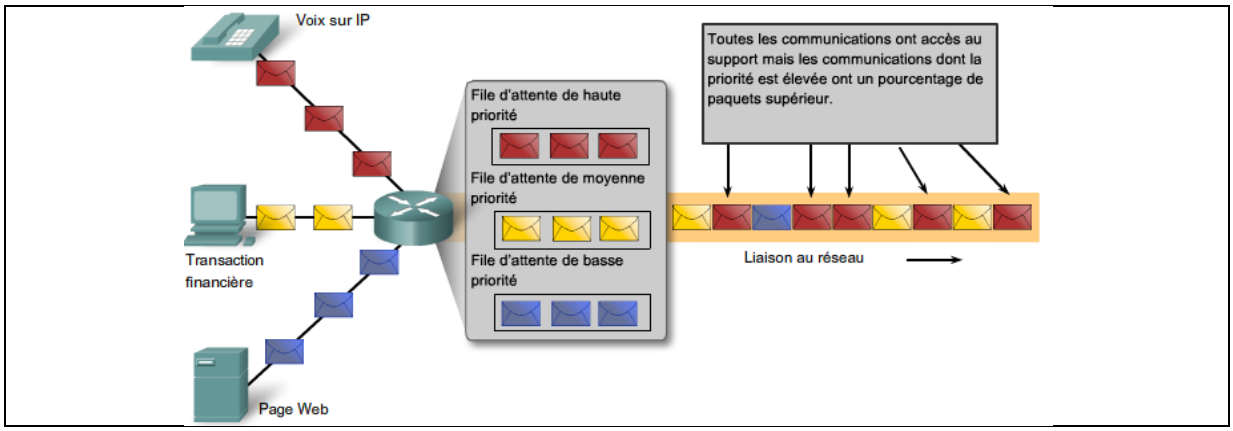
  Un réseau évolutif est en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants.



- **Qualité de service (QOS)**

  Les transmissions audio et vidéo en direct exigent un niveau de qualité constant et un service ininterrompu qui n'était pas indispensable aux applications informatiques traditionnelles. La qualité de ces services est évaluée par rapport à la qualité que l'on obtiendrait en assistant en personne à la même présentation audio ou vidéo. Les réseaux audio et vidéo traditionnels sont conçus pour ne prendre en charge qu'un seul type de transmission. Ils peuvent donc offrir un niveau de qualité acceptable. Sur un réseau convergent, les services nécessitant un haut niveau de qualité de service seront prioritaires devant les autres.

  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.



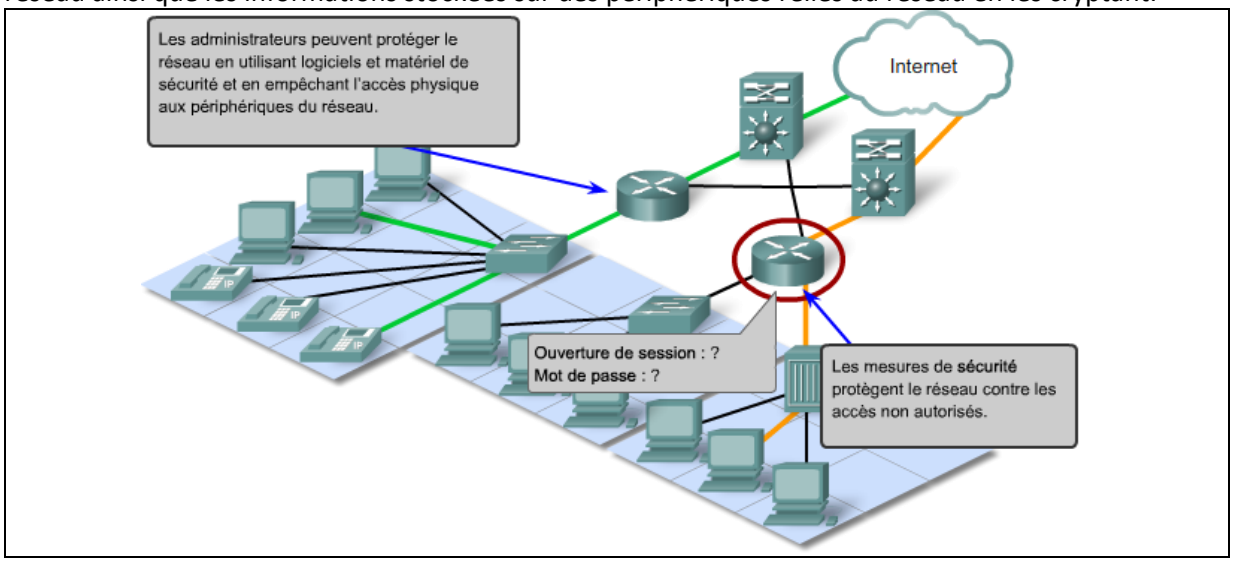
- **Sécurité**

  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 en les cryptant.



2 Connexion des périphériques

2.1 Les supports de transmission

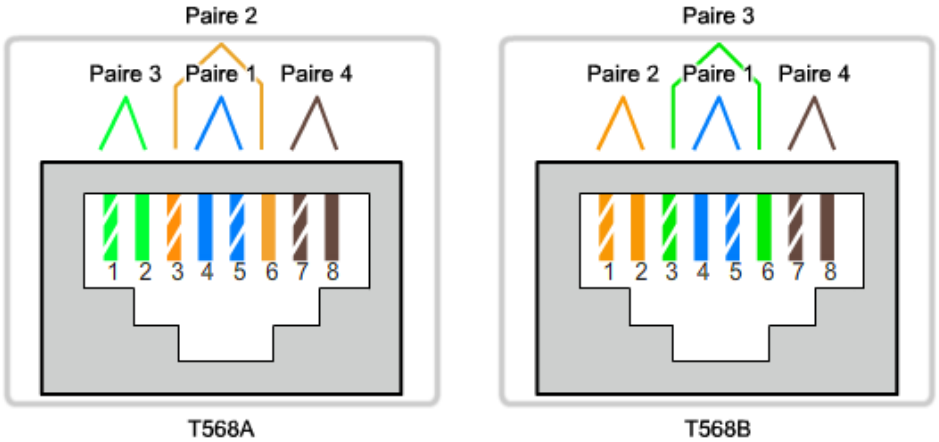
- **Le cuivre : câbles coaxiaux ou à paires torsadées**

Divers organismes de normalisation contribues à la définition des propriétés physiques, électriques et mécaniques des supports disponibles pour différentes communications de données. Ces spécifications garantissent que les câbles et connecteurs fonctionnent comme prévu avec différentes mises en œuvre.

Par exemple, des normes pour les supports en cuivre sont définies pour :

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

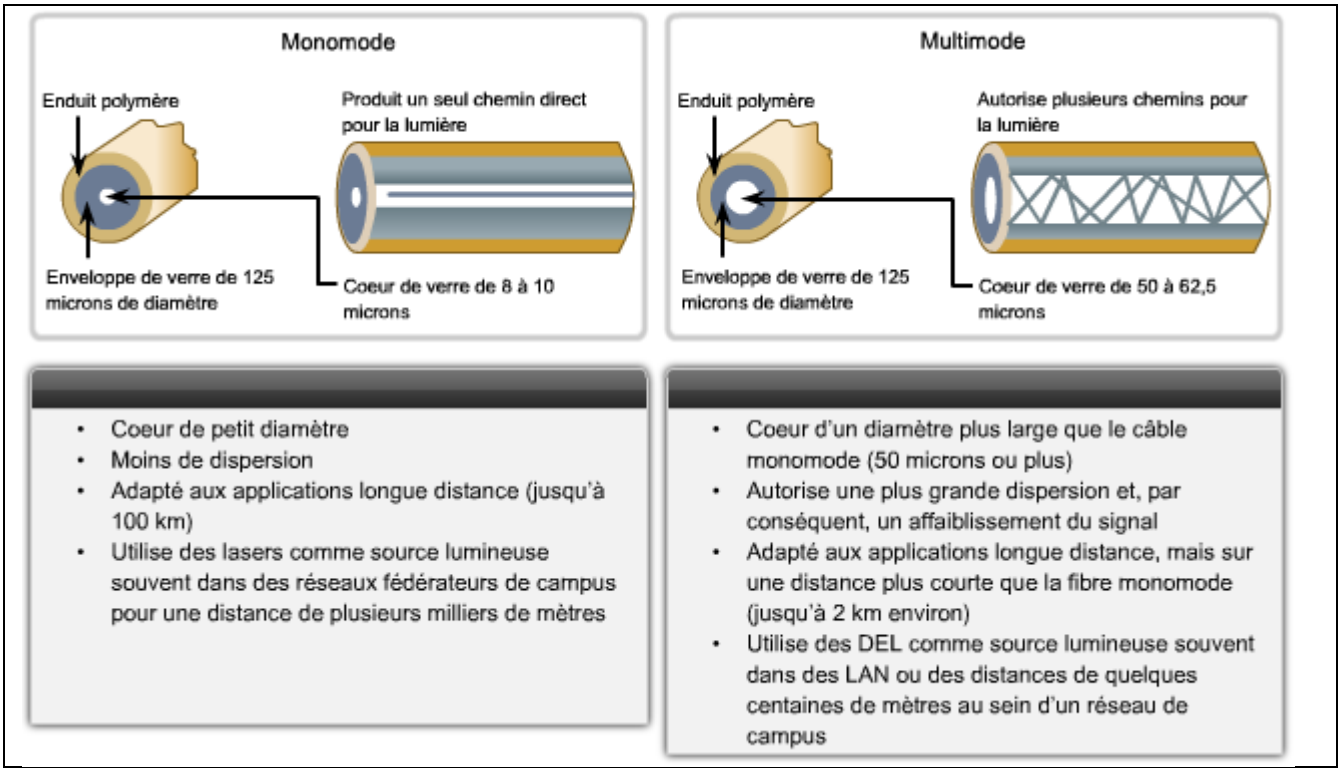
	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T
Supports	EIA/TIA catégorie 3, 4, 5 UTP, quatre paires	EIA/TIA catégorie 5 UTP, deux paires	Fibre multimode de 50/62.5 microns	STP	EIA/TIA catégorie 5 (ou supérieure) UTP, quatre paires
Longueur maximale des segments	100 m	100 m	2 km	25 m	100 m
Topologie	En étoile	En étoile	En étoile	En étoile	En étoile
Connecteur	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	



- **Le verre : fibre optique**

Le câblage en fibre optique utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination. Les bits sont codés sur la fibre comme impulsions lumineuses. Le câblage en fibre optique prend en charge des débits de bande passante de données brutes très élevés.

Des lasers ou des diodes électroluminescentes (DEL) génèrent les impulsions lumineuses utilisées pour représenter les données transmises sous forme de bits sur le support. Des dispositifs à semi-conducteur électronique appelés photodiodes détectent les impulsions lumineuses et les convertissent en tensions qui peuvent ensuite être reconstituées en trames de données.

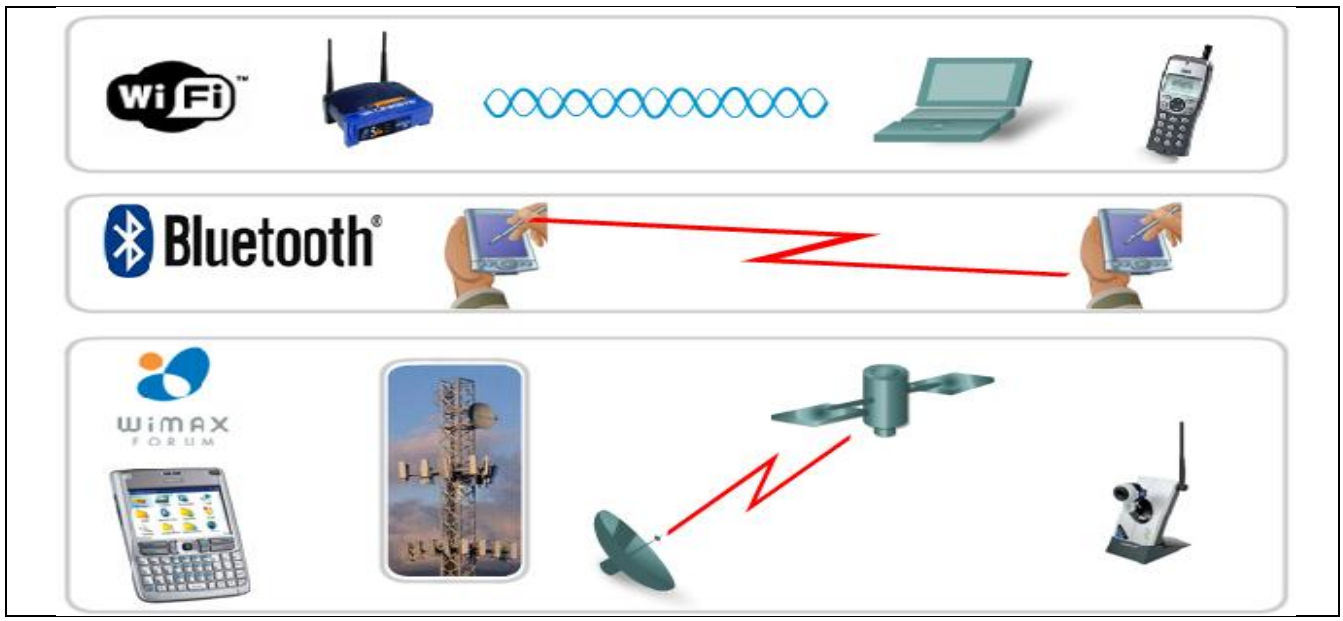


- **Ondes électromagnétiques : sans fil**

Les supports sans fil transportent des signaux électromagnétiques à des fréquences radio et micro-ondes qui représentent les chiffres binaires des communications de données. En tant que support réseau, la transmission sans fil n'est pas limitée aux conducteurs ou voies d'accès, comme les supports en cuivre et à fibre optique.

Les technologies de communication de données sans fil fonctionnent bien dans les environnements ouverts. Cependant, certains matériaux de construction utilisés dans les bâtiments et structures, ainsi que le terrain local, limitent la couverture effective. De plus, la transmission sans fil est sensible aux interférences et peut être perturbée par des appareils aussi courants que les téléphones fixes sans fil, certains types d'éclairages fluorescents, les fours à micro-ondes et d'autres communications sans fil.

En outre, la couverture de communication sans fil n'exigeant aucun accès à un fil physique de support, des périphériques et utilisateurs non autorisés à accéder au réseau peuvent accéder à la transmission. La sécurité du réseau constitue par conséquent un composant essentiel de l'administration de réseau sans fil.



Normes	Bluetooth 802.15	802.11 (a, b, g, n), HiperLAN 2	802, 11, MMDS, LMDS	GSM, GPRS, CDMA, 2.5- 3G
Vitesse	<1 Mbits/s	1 - 54+ Mbits/s	22 Mbits/s+	10 - 384 Kbits/s
Plage	Courte	Moyenne	Moyenne - Longue	Longue
Applications	Peer to peer entre périphériques	Réseaux d'entreprise	Accès fixe à la boucle locale	Assistants numériques personnels, téléphones mobiles, accès cellulaire

2.2 Mode de transmission

La transmission des données via un périphérique peut s'effectuer de deux manières différentes : soit en mode parallèle, soit en mode série. Ce sont principalement les critères d'éloignement et de rapidité qui prédominent dans le choix de ces modes de transmission. Ainsi, on utilise :

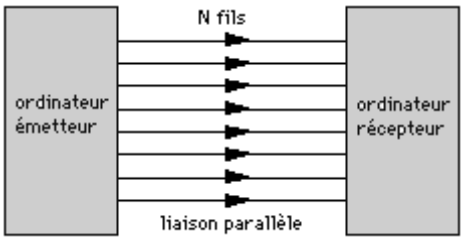
- Le mode de transmission parallèle pour un éloignement inférieur à **2m**.
- Le mode de transmission série pour un éloignement inférieur à **50m**.

Au-delà de cette longueur, on utilise des modes de transmissions particuliers dont les réseaux sont les plus courants.

La transmission des données peut se faire de manière unidirectionnelle (**simplex**), alternée (**half-duplex**) ou simultanée (**full-duplex**).

2.2.1 Mode de transmission parallèle

Dans ce mode de transmission, les données sont transmises par mot entier, la plupart du temps de **8 bits** (**octet**) sur autant de fils, ce qui lui confère une grande facilité d'usage, et une bonne vitesse de transmission.



Sur les ordinateurs, le port parallèle est dédié à la connexion d'une imprimante. On l'appelle souvent « port imprimante » ou « Centronics ». Il utilise des protocoles appelés **ECP/EPP** (**Extended Capabilities Port/Enhanced Parallel Port**), qui offrent des débits jusqu'à **1 Mo/sec** en mode Full Duplex, ce qui signifie qu'il peut transmettre et recevoir des données en même temps.

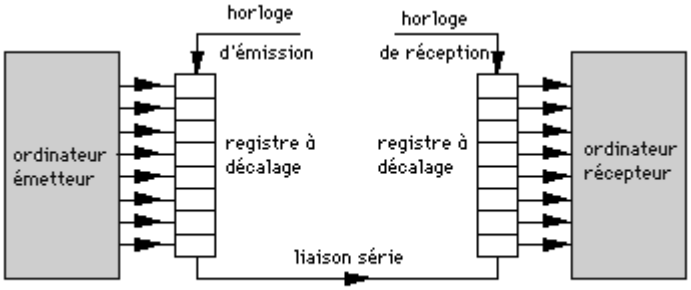
Le besoin de connecter d'autres appareils que des imprimantes sur ce type de port s'est très vite fait ressentir. D'autres normes que la « **Centronics** » ont alors été mise en place. C'est le cas de la norme **IEE488** aussi appelée **GPIB**. Au départ, le **GPIB** (**General Purpose Interface Bus**) fut développé par **HP** au début des années 70, pour connecter et contrôler des instruments programmables produits par **HP**. Cependant, avec l'introduction de commandes numériques et d'équipements de test programmables, il a été nécessaire de créer un standard, le **IEEE 488**, qui réponde à certaines spécifications : C'est une interface de communication parallèle de **8 bits**, avec des taux de transfert pouvant atteindre **8 Moctets** par seconde. Le système d'interface du **GPIB** est constitué de **24** lignes :

- **8** pour le transfert de données codées sur 8 bits,
- **8** pour la masse,
- **3** pour le **handshake**,
- **5** pour la gestion des interfaces

Ce port tend à disparaitre des PC grand-public mais est toujours présent sur les PC industriels.

2.2.2 Mode de transmission série

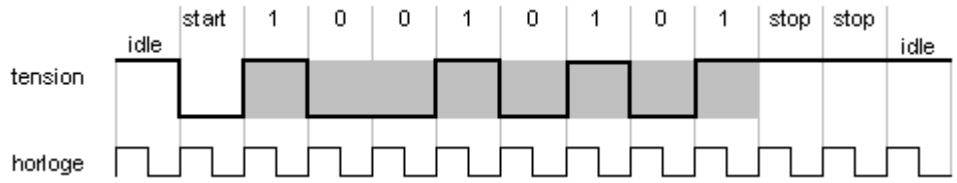
Dans ce mode de transmission, les bits constituant la donnée sont transmis les un après les autres sur le même fil. La structure physique mise en œuvre s'en trouve donc considérablement allégée et le câblage coûte moins cher. Cependant, la vitesse de transmission est réduite et se pose le problème de la synchronisation entre l'émetteur et le récepteur du message.



On distingue deux types de transmission série :

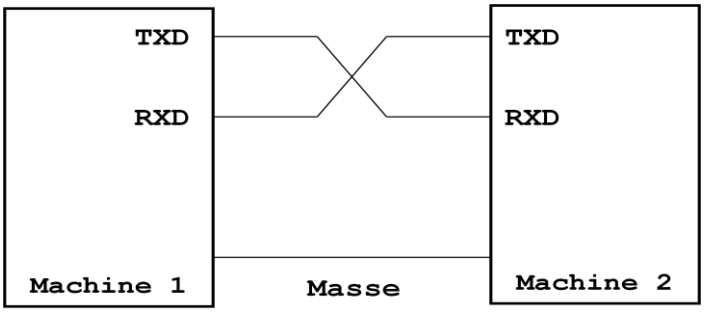
- **Transmission série asynchrone** : Dans ce mode de transmission, on suppose que la fréquence de l'horloge de l'émetteur est la même que celle du récepteur.

  Elle consiste en la transmission d'une succession de blocs courts de bits (1 caractère - en grisé sur la figure ci-dessous) avec une durée indéfinie entre l'envoi de deux blocs consécutifs. Un bit **`START`** annonce le début du bloc (polarité inverse de celle de la ligne au repos - **`idle`**), un ou deux bits **`STOP`** annoncent la fin du bloc (polarité inverse de celle du bit **`STOP`**). Un bit de parité peut être ajouté en fin de message pour contrôler la transmission.



  C'est ce type de liaison série qui est utilisée sur les ordinateurs **`PC`**. Elle répond à la norme **`RS232C`** ou **`V24/V28`** :

  - Valeurs des tensions que doivent fournir et reconnaître les interfaces séries des matérielles.
  - Un **`0`** logique est reconnu pour une tension allant de **`+3`** à **`+40V`**.
  - Un **`1`** logique est reconnu pour une tension allant de **`-3`** à **`-40V`**. Généralement, les signaux envoyés sont compris entre **`-12`** et **`+12 V`**.
  - Sur une liaison série au repos on doit observer un **`1`** logique.
  - Pour faire un échange de données bidirectionnel sur une liaisons séries **`RS232C`** il faut au minimum **`3 fils`** : Un pour les données qui circulent dans un sens, un pour les données qui circulent dans l'autre sens et un pour la masse électrique des signaux. Cette liaison à 3 fils est une liaison minimum. Elle nécessite une collaboration logicielle active entre les 2 machines pour contrôler le transfert des informations. Un mécanisme souvent utilisé est le protocole **`XON XOFF`**.

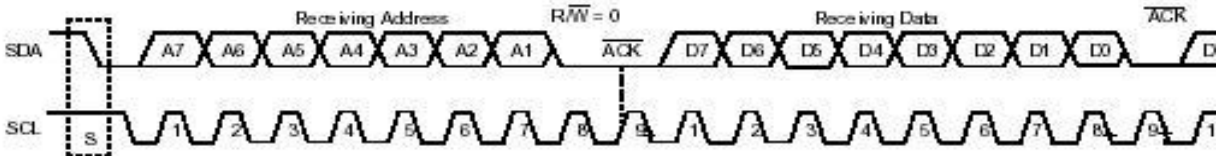


  - Le connecteur existe en version 25 broches (DB25) ou 9 broches (DB9).

- **Transmission série synchrone** : l'émetteur envoi en plus du message, l'horloge de synchronisation.

  Ce type de transmission est bien adapté aux données volumineuses et aux nécessités de transmission rapide. L'information est transmise sous la forme d'un flot continu de bits à une cadence définie par l'horloge d'émission. Le flot de bits est réparti cependant en trames qui peuvent être de longueur variable ou de longueur fixe. Les trames doivent être précédées d'un motif de bits annonçant un début de trame et, éventuellement se terminer par un motif analogue.

  Les liaisons **`I2C (Inter Integreted Circuit)`**, **`SPI (Serial Peripheral Interface)`**, **`PS/2 (Personal System/2)`** sont quelques exemples de liaisons séries synchrones.



Trame I2C

SDA : Adresse du destinataire et données à transmettre
SCL : Horloge de transmission

2.2.3 Codage des bits

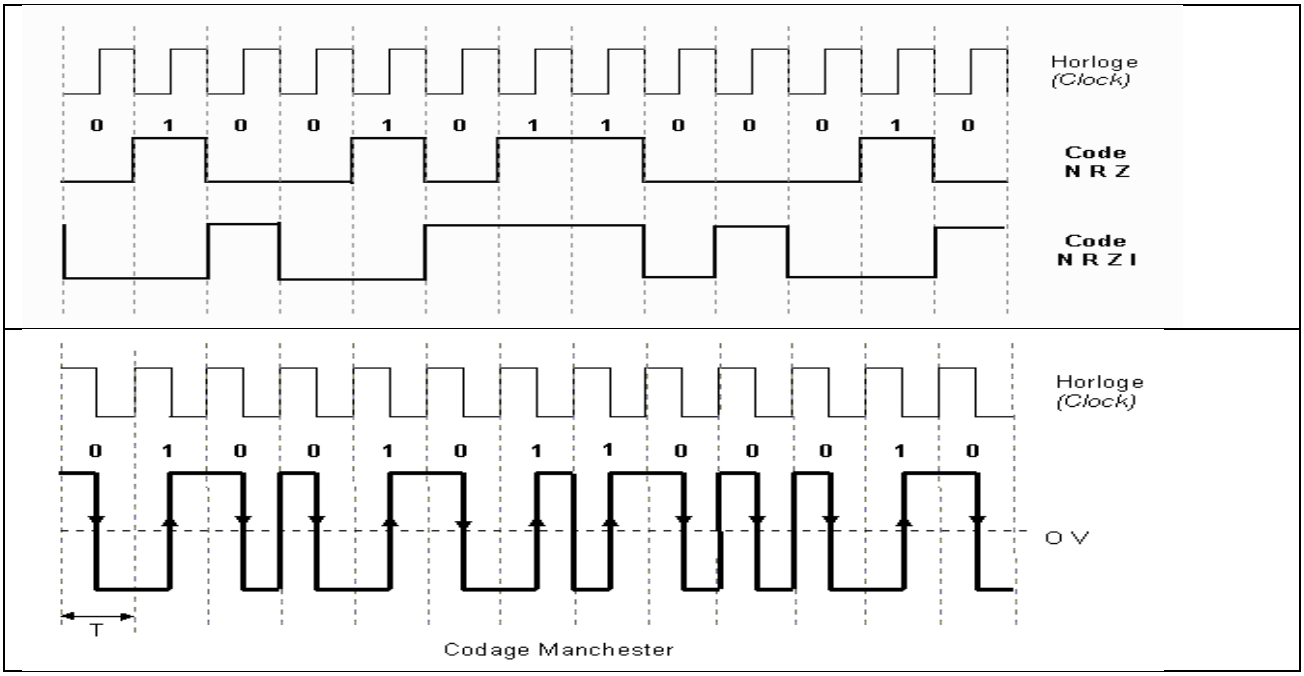
Toutes les communications provenant du réseau humain finissent sous la forme de chiffres binaires, qui sont transportés individuellement sur le support physique.

Les bits sont représentés sur le support en changeant une ou plusieurs des caractéristiques suivantes d'un signal :

- Amplitude
- Fréquence
- Phase

La nature des signaux réels représentant les bits sur le support dépend de la méthode de signalisation utilisée. Certaines méthodes peuvent utiliser un attribut de signal pour représenter un seul 0 et un autre pour représenter un seul 1.

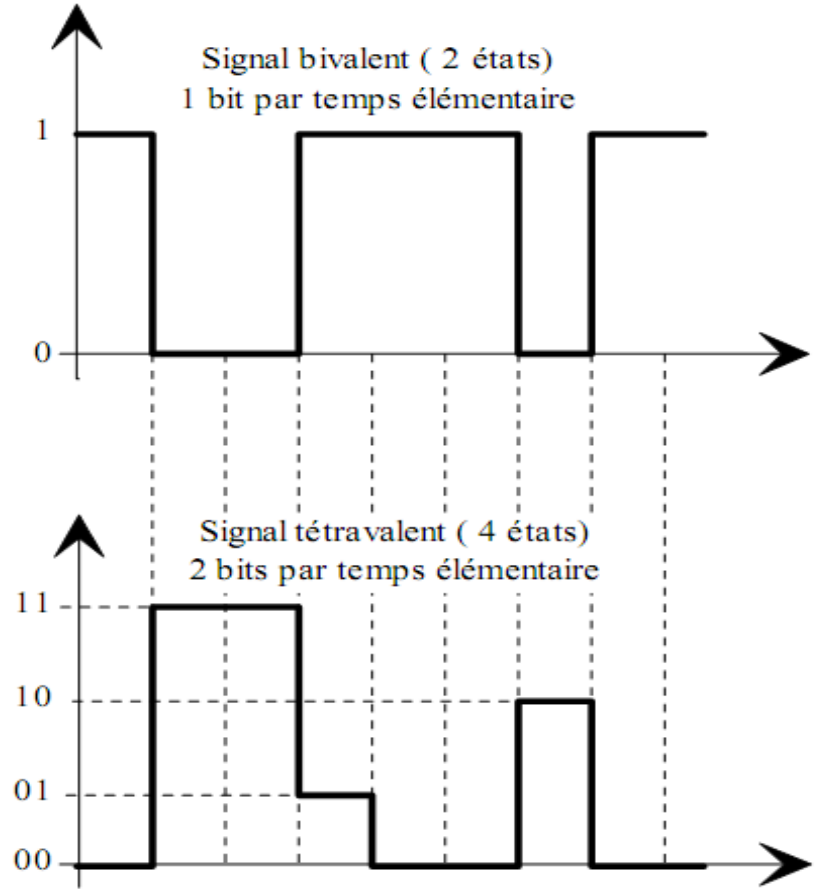
La transmission en bande de base consiste à envoyer directement les suites de bits sur le support à l'aide de signaux carrés constitués par un courant électrique pouvant prendre 2 valeurs (**`5 Volts`** ou **`0`** par exemple). Plusieurs type de codage des bits utilisent ce type de transmission :



Codage Manchester

La rapidité d'une liaison est définie comme le nombre d'états par unité de temps et est donnée en bauds alors que le débit de la liaison est défini comme la quantité d'informations binaires émises par unité de temps et est donnée en bits par seconde (bps).

Le nombre d'états utilisés pour représenter l'information s'appelle la valence. Cette valeur est une puissance de 2.



Pour un signal bivalent, le débit est égal à la rapidité :

1 bps = 1 baud

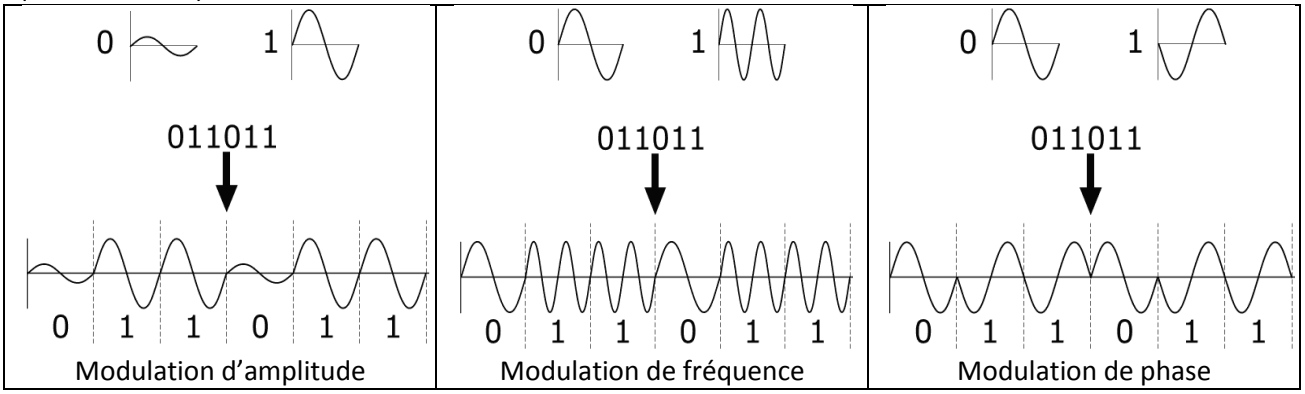
Pour un signal dont la valence est supérieure à 2 :

$$R_{max} = \frac{D_{max}}{\log_2 V}$$

Ici, R = D/2

Si D = 9600 bps, R = 4800 bauds

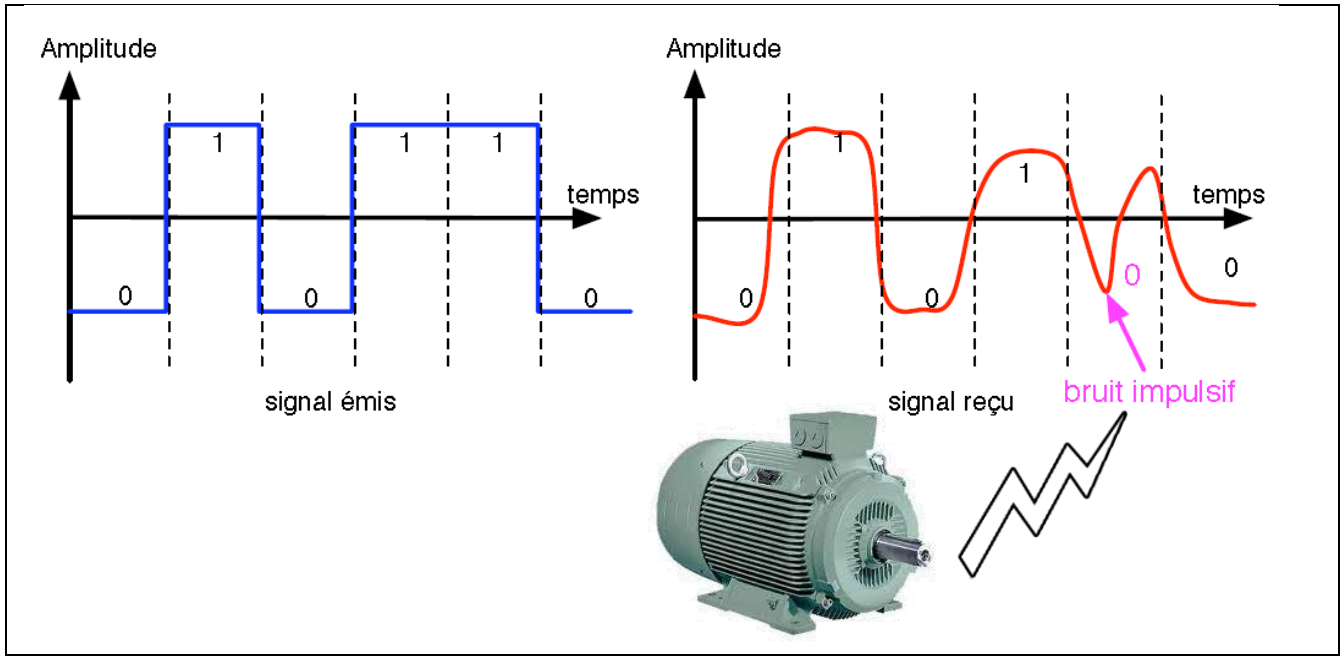
Le principal problème de la transmission en bande de base est la dégradation du signal très rapide en fonction de la distance parcourue, c'est pourquoi elle n'est utilisée qu'en réseau local (**<5km**). Il serait en effet trop coûteux de prévoir des **répéteurs** pour régénérer régulièrement le signal. C'est pourquoi sur les longues distances on émet un signal sinusoïdal qui, même s'il est affaibli, sera facilement décodable par le récepteur. Ce signal sinusoïdal est obtenu grâce à un **modem** (modulateur-démodulateur)qui est un équipement électronique capable de prendre en entrée un signal en bande de base pour en faire un signal sinusoïdal (modulation) et l'inverse à savoir restituer un signal carré à partir d'un signal sinusoïdal (démodulation).



2.3 Altération de la transmission

Avec la distance, le signal transmis se déforme. On appelle se phénomène la distorsion. Un signal transporté par un réseau est soumis à d'autres modifications : le réseau peut recevoir des perturbations provenant de l'environnement électromagnétique (exemple, passage d'un train électrique au voisinage d'une ligne téléphonique) et est perturbé par le bruit de fond provoqué par le mouvement brownien des électrons. Ce bruit de fond est un « bruit blanc » qu'il est impossible d'extraire du signal en raison de son caractère aléatoire.

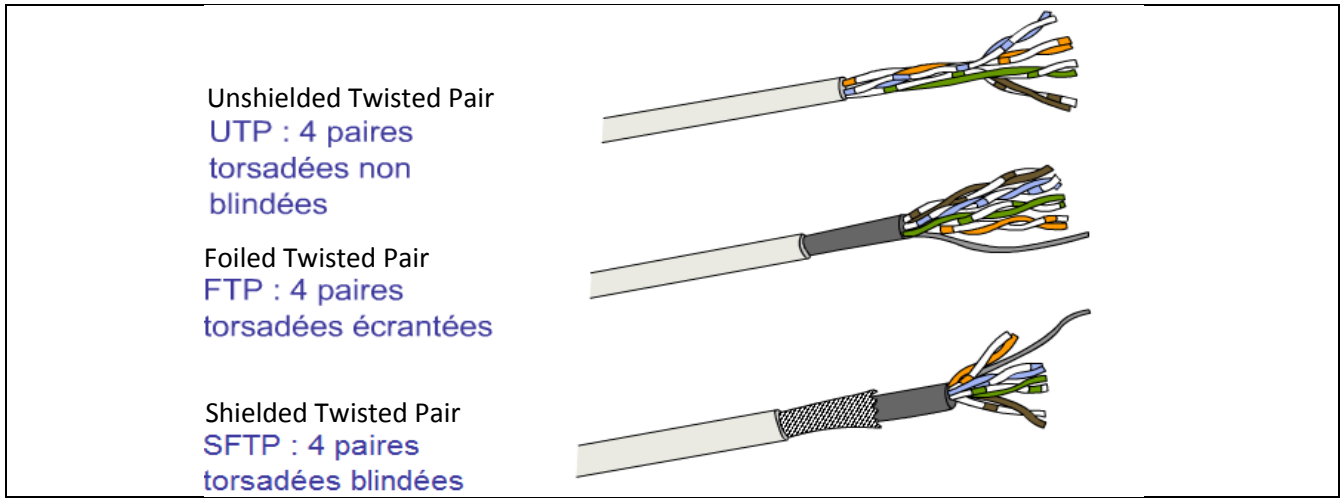
Ainsi le signal transporté par le réseau est après une certaine distance la somme du signal émis, des phénomènes d'affaiblissement et de distorsion qu'il a subis, et du bruit provoqué par les diverses perturbations.



2.4 Limitation des effets de l'altération

Les phénomènes d'altération du signal sur une ligne de transmission peuvent être limités par le choix du support.

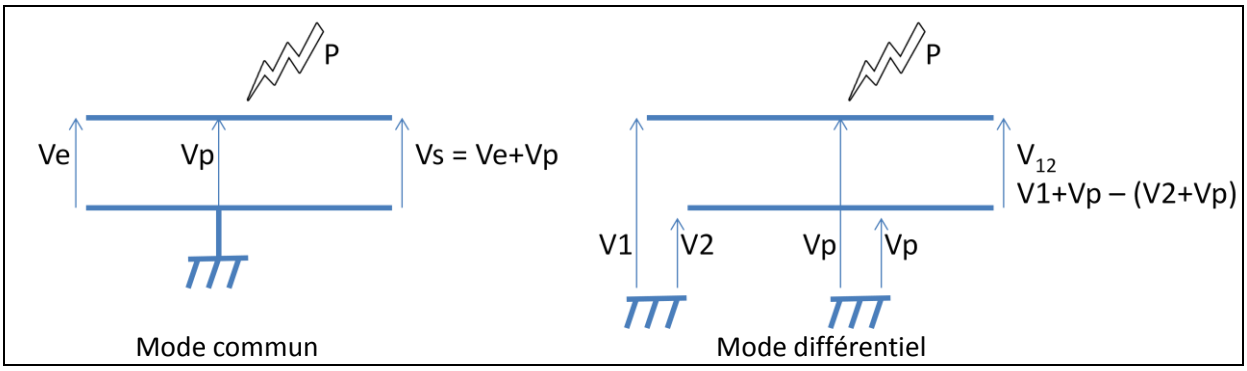
Le support le plus souvent utilisé est le câble à paires torsadées dont on distingue plusieurs types :



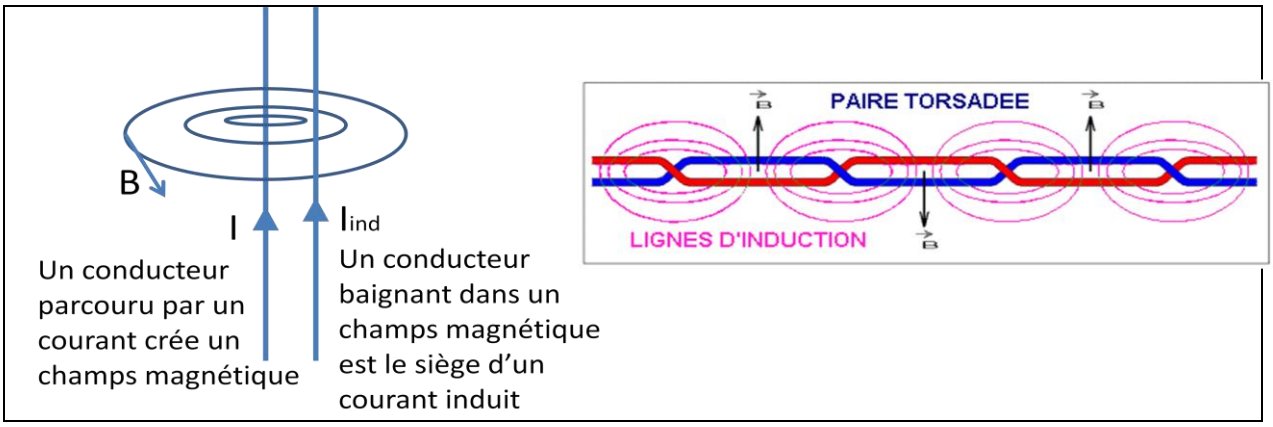
Ces câbles permettent la mise en place de plusieurs mécanismes de protections contres les interférences et les phénomènes de diaphonie qui se manifestent lorsque plusieurs conducteurs sont voisins.

- Le câble est blindé ou écranté : cet écran capte les parasites électromagnétiques et les draine vers la masse.

- La transmission s'effectue en mode différentiel : Ce mode de transmission permet d'annuler les tensions parasites produites.

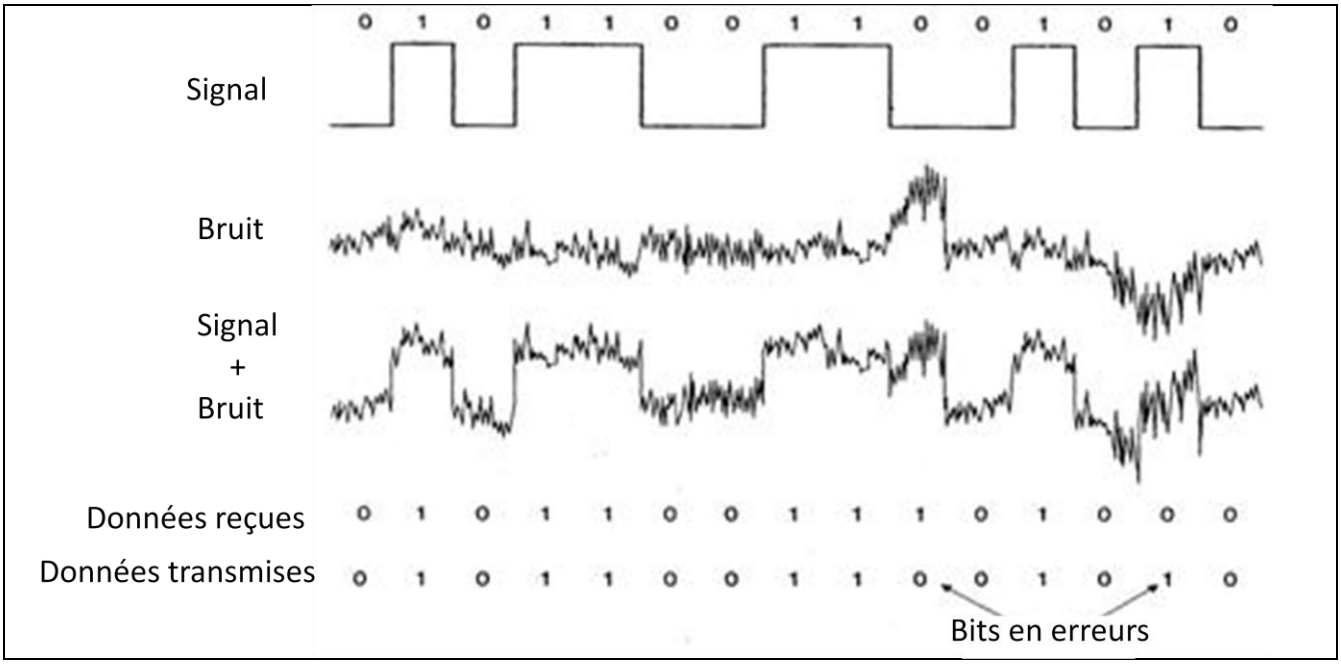


- Les paires sont torsadées : Le fait de torsader les paires diminue l'effet de diaphonie. Ce phénomène apparait lorsque deux conducteurs se trouvent au voisinage l'un de l'autre. Il est du à l'effet de mutuelle induction :



2.5 Détection d'erreur

Malgré le soin apporté à la qualité du support de transmission, le signal reste, dans une moindre mesure, bruité et parasité. Ces effets indésirables peuvent provoquer une modification de l'état d'un ou plusieurs bits lors d'une transmission.



Des mécanismes de détection ou de correction de ces erreurs sont alors mis en place.

2.5.1 Approche naïve : la répétition

Le caractère imprévisible du positionnement des bits en erreurs est mis à profit dans une approche naïve qui consiste à transmettre deux fois le même message successivement.

- Message à transmettre : **1001001**
- Message effectivement transmis : **1001001 1001001**

Si les deux messages arrivés sur le récepteur sont différents, il y a eu une erreur de transmission.

En envoyant un troisième message identique, il devient possible d'identifier le message correct et de procéder à une auto-correction.

- Message à transmettre : **1001001**
- Message effectivement transmis : **1001001 1001001 1001001**
- Message reçu : **1001001 1001011 1001001**
- Message correct : **1001001**

Caractère	ASCII	Nb de 1	Parité pair	Parité impair
A	0100 0001	2	0100 0001 **0**	0100 0001 **1**
L	0100 1100	3	0100 1100 **1**	0100 1100 **0**
z	0111 1010	5	0111 1010 **1**	0111 1010 **0**

Le message correct correspond aux 2 exemplaires identiques.

Quelques remarques :

- La **détection et la correction des erreurs** nécessitent d'introduire de la **redondance** dans les messages transmis, ce qui double ou triple la quantité de données à transmettre.
- **L'auto-correction** nécessite **plus de redondance** que la simple détection.
- **Certaines erreurs ne peuvent pas être détectées**
  Exemple : la même erreur sur les deux exemplaires
- **Certaines erreurs détectées ne peuvent pas être corrigées**
  Exemple : Une erreur différente sur au moins deux exemplaires.
- **Certaines erreurs sont mal corrigées**
  Exemple : une même erreur sur deux exemplaires simultanément

2.5.2 Utilisation du bit de parité

Un bit de parité permet d'assurer un contrôle sur le contenu d'un message. Un message même composé de plusieurs octets est vue comme une suite de bits. Selon que le nombre de bits à 1 soit pair ou impair, le bit de parité aura pour valeur 0 ou 1.

Dans un échange de message sur un réseau, l'expéditeur calcul le bit de parité et le joint au message. Le destinataire calcul le bit de parité sur le message reçu et le compare avec le bit de parité que l'expéditeur lui a envoyé. Si les deux bits de parités sont de valeurs différentes, alors c'est que le message a subit des dommages au cours de son transport puisque la série de bits a changé. Le destinataire va donc demander la réémission du message ou l'ignorer.

Dans la pratique, ce principe de détection d'erreur est appliqué à des messages constitués d'une suite d'octets transmis les uns après les autres. Le bit de parité est appliqué à chaque octet.

Le bit de parité détecte les erreurs en nombre impair dans le message et ne permet pas correction automatique.

2.5.3 Utilisation d'une somme de contrôle (Check Sum)

La somme de contrôle permet au récepteur d'un message de vérifier que les données transmises ne contiennent pas d'erreurs. Pour se faire, l'émetteur du message calcule une valeur « CheckSum » qui est fonction du contenu du message, puis l'ajoute à la fin du message. Le récepteur fait le même calcul, et contrôle que le « CheckSum » a la même valeur que celui de l'émetteur.

Exemple simple :

On calcul la somme des codes ASCII de chaque caractères d'une chaine constituant un message et lui applique un modulo 256 (reste de la division entière de la somme par 256).

Chaine	B	o	n	j	o	u	r		P	a	p	a	CheckSum
ASCII (hex)	42	6F	6E	6A	6F	75	72	20	50	61	70	61	481 % FF = 81

Si une erreur s'est produite sur un ou plusieurs caractères, la somme de contrôle change :

Chaine	B	o	n	j	o	u	r		P	a	p	a	CheckSum
ASCII (hex)	42	6F	6E	6A	6F	75	72	20	50	61	70	61	481 % FF = 81

Toutefois, il peut arriver que le message soit corrompu et que le résultat du calcul de contrôle soit correct :

Chaine	P	o	n	j	o	u	r		B	a	p	a	CheckSum
ASCII (hex)	50	6F	6E	6A	6F	75	72	20	42	61	70	61	481 % FF = 81

L'algorithme de calcul de la somme de contrôle est trop simple pour identifier ce genre d'erreur.

2.5.4 Utilisation du code CRC (Cyclic Redundancy Check – Contrôle de Redondance Cyclique)

Dans ce cas, la somme de contrôle est calculée à l'aide d'un algorithme plus complexe nommé CRC.

Cet algorithme est basé sur le principe de la division polynomiale. Le message à transmettre est traité comme un polynôme que l'on divise par un polynôme de référence appelé « polynôme générateur ». Le reste de la division constitue la somme de contrôle.

Mécanisme :

- **Une séquence de bits constitue un polynôme P(X) tel que :**

  ⇒ $\mathbf{a_{n-1}\ a_{n-2}\ \ldots\ a_2\ a_1\ a_0 \Leftrightarrow P(X) = a_{n-1}\ X^{n-1} + a_{n-2}\ X^{n-2} + \ldots + a_2\ X^2 + a_1\ X^1 + a_0\ X^0}$

  Exemple : 1110 0111 ⇔ $P(X) = X^7 + X^6 + X^5 + X^2 + X + 1$

- Utilisation d'un **polynôme de générateur g(X)** connu de l'émetteur et du récepteur

  Exemple : $g(X) = X^4 + X^2 + X$ ⇔ 10110

- **En émission :**

  ⇒ On ajoute au message à émettre un code de contrôle tel que le polynôme correspondant au message plus le code de contrôle soit divisible par le polynôme générateur choisi.

- **En réception :**

  ⇒ Le message reçu qui contient les données et le CRC doit être divisible par le polynôme générateur.

  ⇒ On vérifie donc par une division euclidienne en base 2 que le reste de la division est nul.

- **Procédure de codage :**

  ⇒ Séquence à transmettre : **1110 0111** ⇔ **$P(X) = X^7 + X^6 + X^5 + X^2 + X + 1$**

  ⇒ Polynôme générateur : **10110** ⇔ **$g(X) = X^4 + X^2 + X$**

  ⇒ On calcul $M(X)=P(X).X^k$ où k est le degré de g(X) : $M(X) = X^{11} + X^{10} + X^9 + X^6 + X^5 + X^4$

  ⇒ On calcul le reste de la division de M(X) / g(X) **: $M(X) = Q(X).g(X) + R(X)$**

  ⇒ **Le CRC est la séquence binaire correspondant à R(X)**

  ⇒ **On transmet la séquence binaire correspondant à la concaténation de P(X) et R(X)**

- **Exemple : Calcul du code CRC de la séquence 1110 0111 par le polynôme générateur 10110**

$X^{11} + X^{10} + X^9 + X^6 + X^5 + X^4$ | $X^4 + X^2 + X$

$X^{11} + X^9 + X^8$; $X^{10} + X^8 + X^6$; $X^{10} + X^8 + X^7$; $X^7 + X^6 + X^5$; $X^7 + X^5 + X^4$; $X^6 + X^4 + X^4$; $X^6 + X^4 + X^3$; $X^4 + X^3$; $X^4 + X^2 + X$

$X^7 + X^6 + X^3 + X^2 + 1$

$X^3 + X^2 + X$

CRC = $X^3 + X^2 + X$ ⇔ 1110

A transmettre : 1110 0111 1110

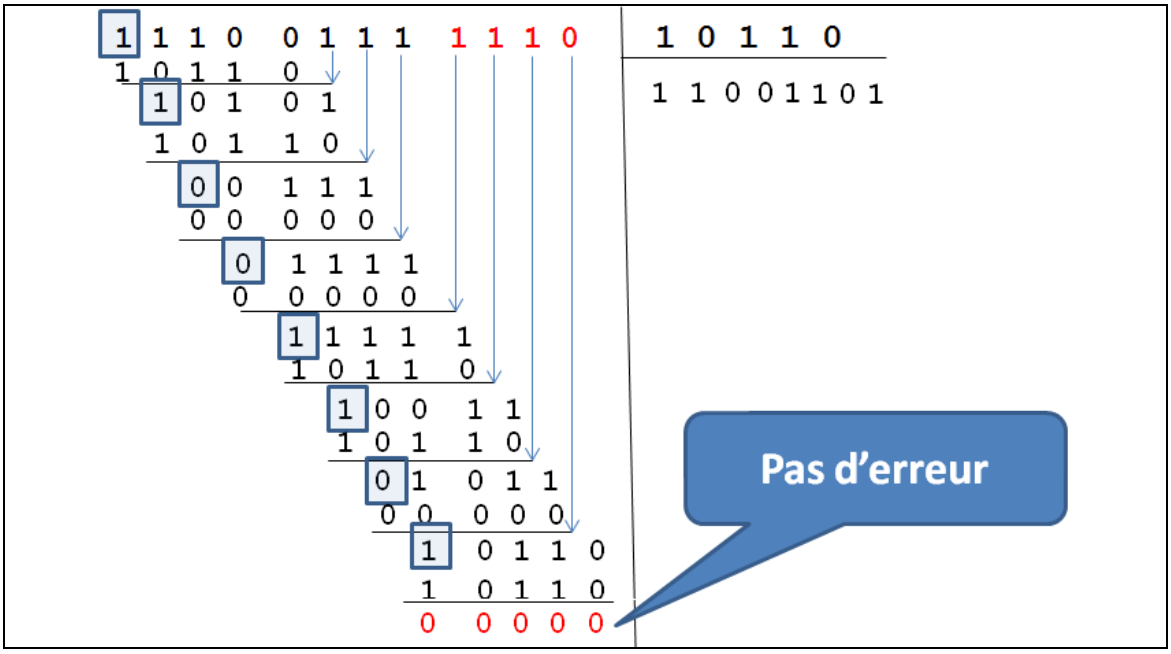
- **Vérification du CRC à la réception**

  Si M(X) est le message reçu, il doit vérifier : **$M(X) = Q(X).g(X)$**

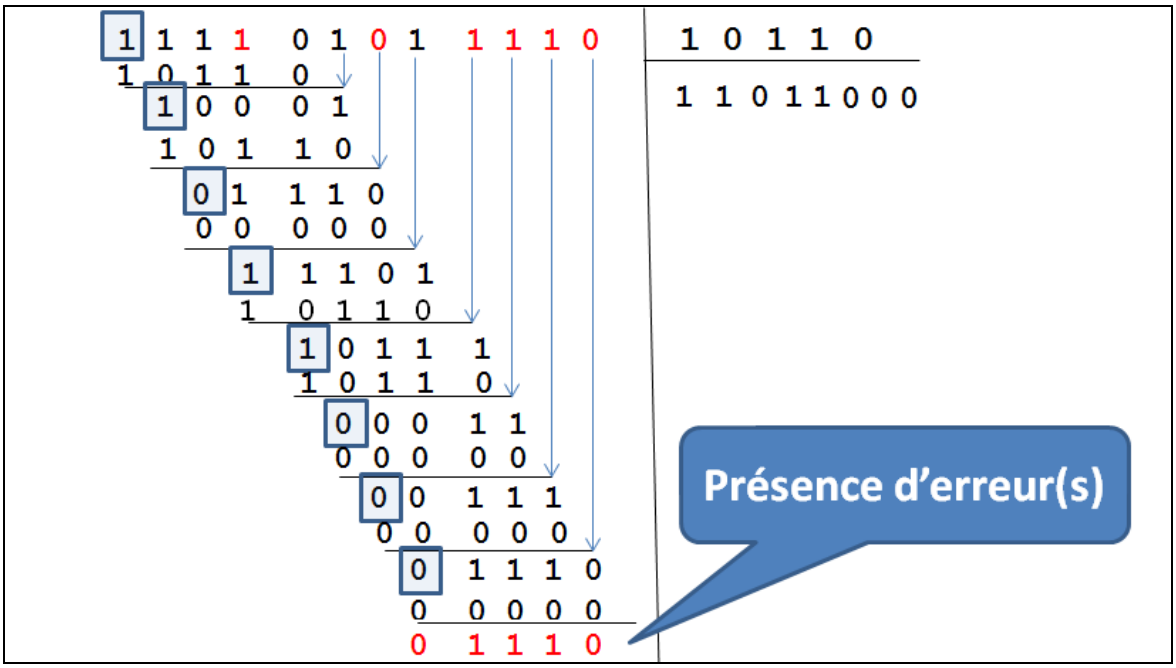
  Le reste de la division de la séquence reçue par le polynôme générateur est nulle s'il n'y a pas d'erreur

Les ordinateurs ne traitent évidemment pas des polynômes mais des données binaires. La division binaire utilise le principe du décalage des bits vers la droite (division par 2) et l'opérateur XOR pour le calcul du reste.

- **Vérification du CRC à la réception avec l'exemple précédent sans erreur de transmission**



- **Vérification du CRC à la réception avec l'exemple précédent avec une erreur de transmission**



Les polynômes générateurs sont standardisés :

- CRC-12 : $X^{12} + X^{11} + X^3 + X^2 + X + 1$
- CRC-16 : $X^{16} + X^{15} + X^2 + 1$
- CRC-32 (Ethernet) : = $X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

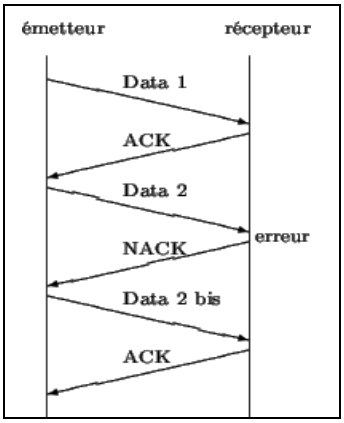
2.6 Correction d'erreur

2.6.1 Détection d'erreur et demande de retransmission

Les codes de détections d'erreurs utilisant une somme de contrôle ajouté à la fin des données transmises sont souvent utilisés avec un protocole basés sur un mécanisme d'accusé de réception.

Si le récepteur ne détecte pas d'erreur lors de la réception d'un message, il envoie un accusé de réception (ACK : Acknowledge receipt) à l'émetteur qui peut alors envoyer la suite du message.

Si le récepteur détecte une erreur lors de la réception d'un message, il envoie un accusé de non réception (NACK). L'émetteur sait alors qu'il doit renvoyer le message erroné.



2.6.2 Code de correction d'erreur : code de Hamming

Ce code permet de détecter et de corriger une seule erreur et seulement une dans un message. La correction proposée par le code est la plus probable selon certaines hypothèses statistiques. Il consiste à ajouter de l'information non plus à la fin du message comme pour une somme de contrôle, mais entrelacée dans l'information à transmettre.

On calcul t bits de contrôle tels que $\mathbf{2^t - 1 >= N + t}$ où N est le nombre de bits du message à transmettre. Ces bits de contrôle sont insérés dans le message aux positions correspondantes aux puissances de 2 (1, 2, 4, 8, …, 2^n).

- **Exemple** : transmission de **0101 0010** soit 8 bits donc **t = 4 bits** placés sur les bits **1, 2, 4** et **8**

Position des bits	12	11	10	9	8	7	6	5	4	3	2	1
bloc du message codé	0	1	0	1	**H**	0	0	1	**H**	0	**H**	**H**

Les bits de contrôle sont le résultat d'un ou-exclusif entre les positions des bits à 1 :

Position des bits	12	11	10	9	8	7	6	5	4	3	2	1
bloc du message codé	0	1	0	1	**H**	0	0	1	**H**	0	**H**	**H**

Bits à 1	binaire
11	1011
9	1001
5	0101
Ou-exclusif	0111

Les bits de contrôle sont insérés dans l'ordre dans le message à transmettre

Position des bits	12	11	10	9	8	7	6	5	4	3	2	1
bloc du message codé	0	1	0	1	**0**	0	0	1	**1**	0	**1**	**1**

Le résultat d'un ou-exclusif entre les positions des bits à 1 et les bits de contrôle permet de détecter la position d'une erreur. Il suffira alors de changer l'état du bit en erreur.

Position des bits	12	11	10	9	8	7	6	5	4	3	2	1
Message reçu	0	1	0	1	0	0	0	1	1	0	1	1

=> Pas d'erreur.

Bit erroné

Position des bits	12	11	10	9	8	7	6	5	4	3	2	1
Message reçu	0	1	0	**0**	0	0	0	1	1	0	1	1

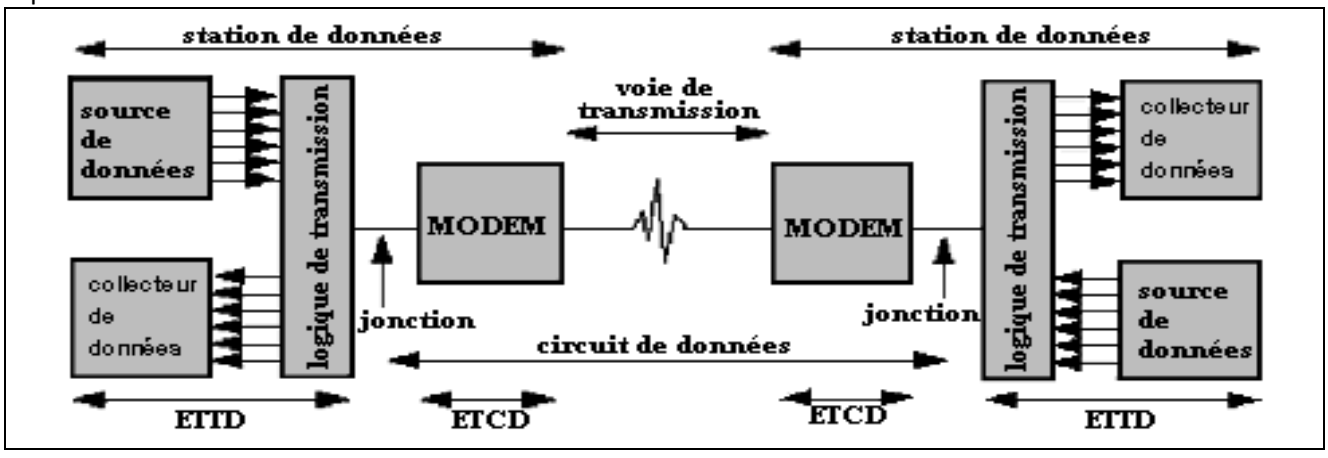
Bits de à 1	binaire
11	1011
5	0101
Contrôle	0111
Ou-exclusif	1001

Position du bit erroné : Inverser son état

2.7 Transmission longue distance sur cuivre

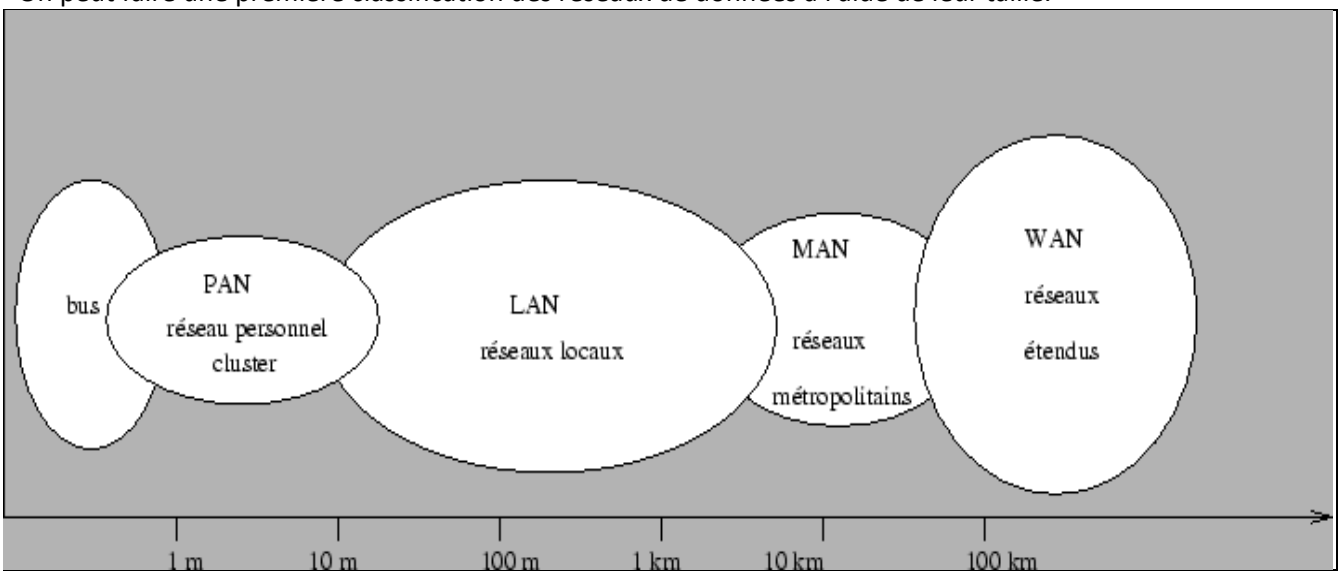
Un signal transmis en bande de base se dégrade rapidement à la distance. Ainsi les normes de câblage imposent une longueur maximale de 100 m pour une connexion directe sans amplification du signal.

Lorsque la longueur entre émetteur et récepteur devient trop importante, on utilise de manière quasi-générale la solution de la modulation. Une liaison télé-informatique classique (en modulation) est représentée ci-dessous :



2.8 Classification des réseaux de données

On peut faire une première classification des réseaux de données à l'aide de leur taille.



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.

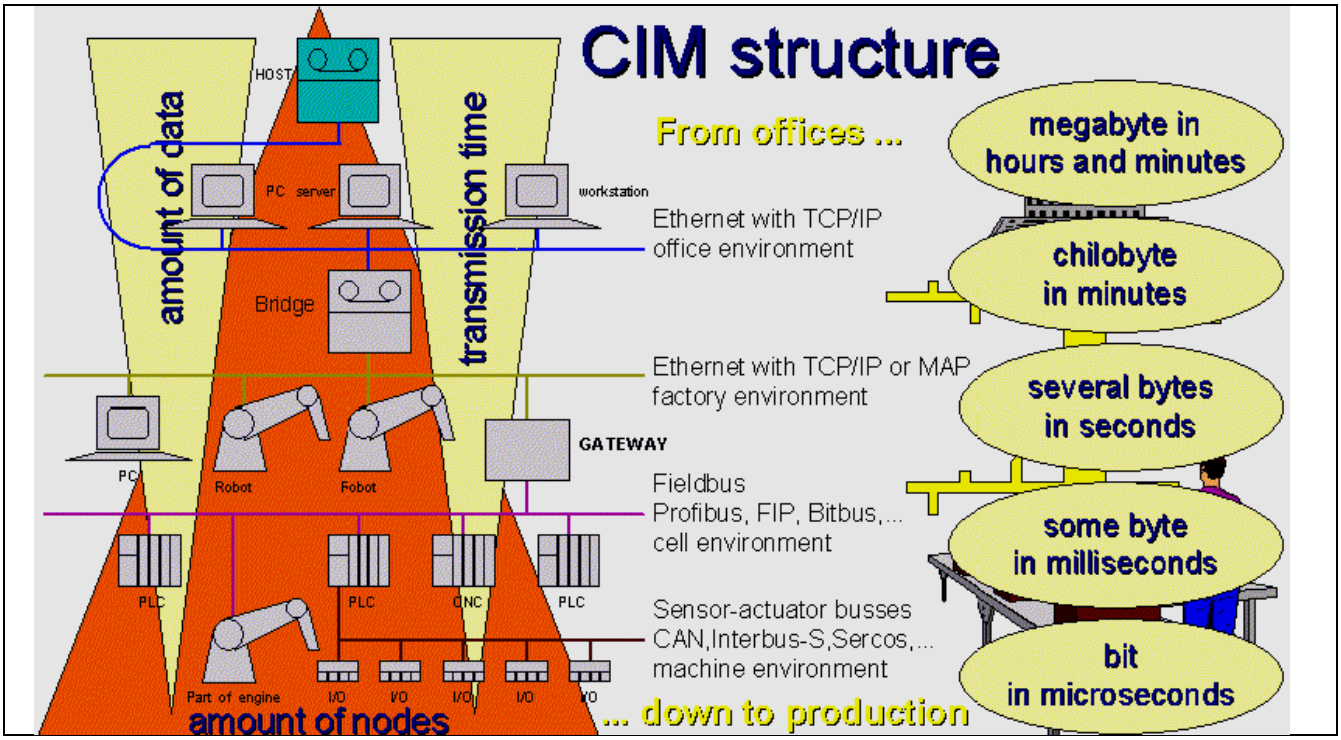
Un **réseau local** (**Local Area Network**) peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.

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**.

En milieux industriel, de nombreux type de réseaux de données sont mis en œuvre. On utilise le modèle de la pyramide CIM pour déterminer la meilleure stratégie d'implantation en fonction du volume et du type de données à traiter, du nombre de nœuds à interconnecter et du besoin de rapidité de transmission.

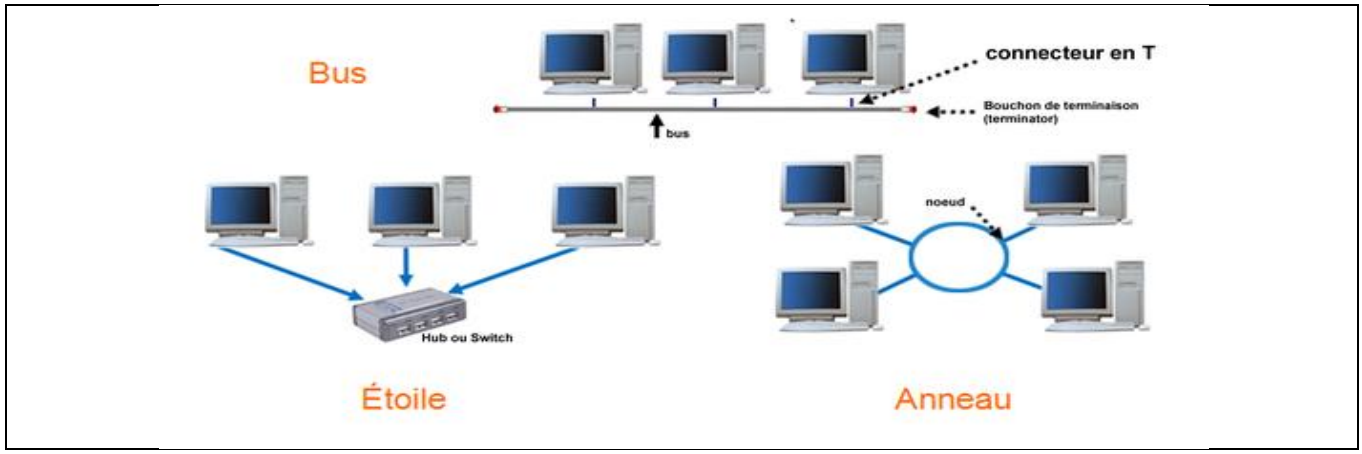

CIM structure
amount of data
transmission time
HOST
PC server
workstation
Bridge
PC
Robot
Robot
GATEWAY
PLC
PLC
CNC
PLC
Part of engine
I/O
I/O
I/O
I/O
I/O
amount of nodes
From offices ...
Ethernet with TCP/IP
office environment
Ethernet with TCP/IP or MAP
factory environment
Fieldbus
Profibus, FIP, Bitbus,...
cell environment
Sensor-actuator busses
CAN,Interbus-S,Sercos,...
machine environment
... down to production
megabyte in
hours and minutes
chilobyte
in minutes
several bytes
in seconds
some byte
in milliseconds
bit
in microseconds

2.9 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.

Aujourd'hui, la topologie logique la plus courante est **`Ethernet`**.

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



- **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.

  Cette topologie est obsolète dans les réseaux de données mais couramment utilisé dans les réseaux de terrain.

- **Topologie en étoile**

  Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé **`switch`** (**`commutateur`**). 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 commutateur sans pour autant paralyser le reste du réseau.

- **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.

Sur les réseaux de données, c'est la topologie en étoile qui la plus répandue.

3 Fonctionnement d'un réseau

3.1 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 (**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 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.

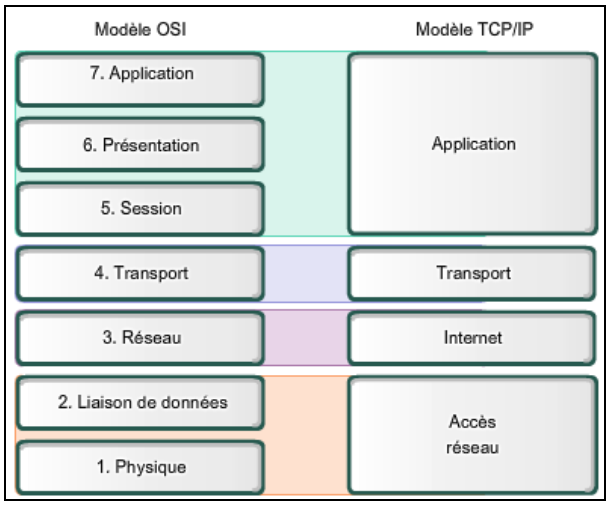
7- Application	La couche application permet d'obtenir une connectivité de bout en bout entre des individus dans le réseau humain à l'aide de réseau de données.
6- Présentation	La couche présentation fournit une représentation commune des données transférées entre des services de la couche application.
5- Session	La couche session fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.
4- Transport	La couche transport définit des services pour segmenter, transférer et rassembler les données de communications individuelles entre périphériques finaux.
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.

Malheureusement, du fait de la rapidité avec laquelle Internet basé sur TCP/IP a été adopté, ainsi que de la vitesse avec laquelle il s'est développé, le développement et l'acceptation de la suite de protocoles OSI sont restés à la traîne. Même si peu de protocoles développés à l'aide des spécifications OSI font l'objet d'une utilisation répandue aujourd'hui, le modèle OSI à sept couches a apporté des contributions essentielles au développement d'autres protocoles et produits pour tous les types de nouveaux réseaux.

3.2 Comparaison des modèles OSI et TSP/IP

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

Au niveau de la couche d'accès au réseau, la suite de protocoles TCP/IP ne spécifie pas quels protocoles utiliser lors de la transmission à travers un support physique ; elle décrit uniquement la remise depuis la couche Internet aux protocoles réseau physiques.



Les couches OSI 1 et 2 traitent des procédures nécessaires à l'accès aux supports et des moyens physiques pour envoyer des données à travers un réseau.

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

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

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

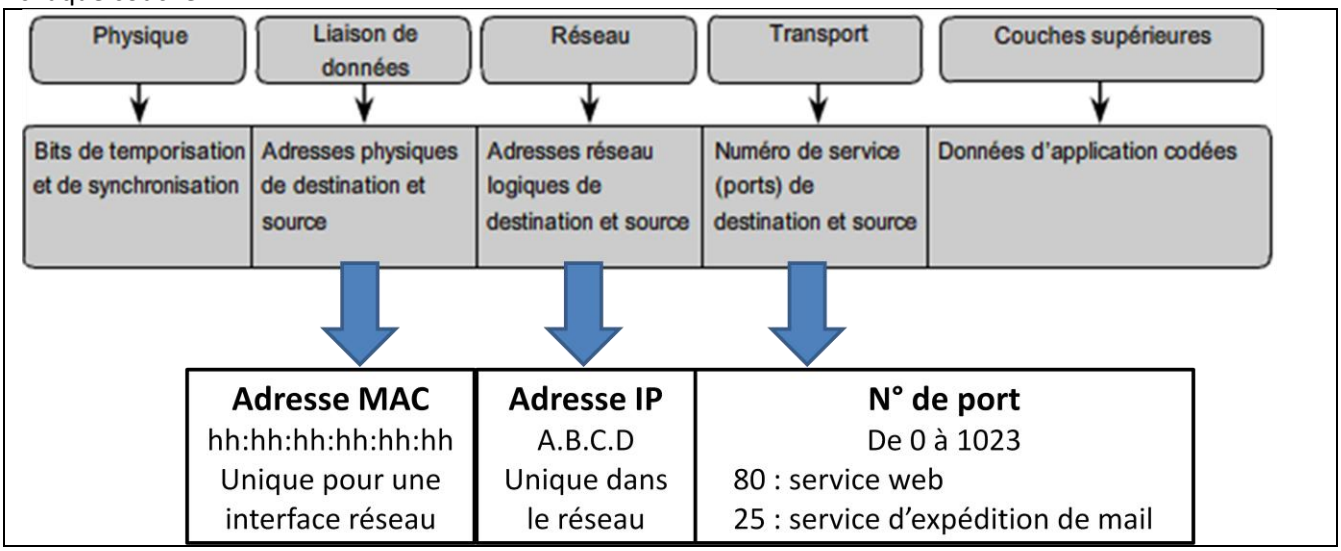
La couche 4, la couche transport du modèle OSI, sert souvent à décrire des services ou des fonctions générales qui gèrent des conversations individuelles entre des hôtes source et de destination. Ces fonctions incluent l'accusé de réception, la reprise sur erreur et le séquencement. À cette couche, les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

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

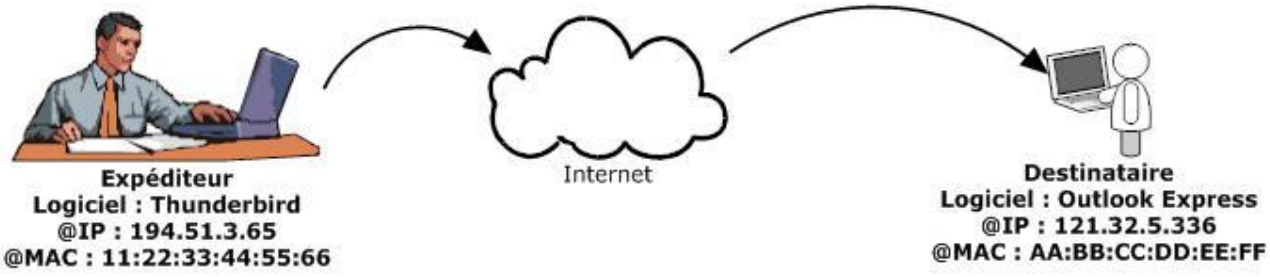
3.3 Principe de l'adressage et de l'encapsulation

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. En utilisant le modèle OSI comme guide, nous apercevons les différents identificateurs et adresses nécessaires à chaque couche.



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



Couche Application Repérage de l'application Codage du contenu	Données :
Couche Transport Découpage en segments Indication des ports sources et destination	Datagramme (UDP) : Segment (TCP) :
Couche Internet Découpage en paquets Indication des adresses IP sources et destination	Paquet :
Couche Accès Réseau Indication des adresses MAC sources et destination. Expédition des trames	Trame

3.4 Adressage IPv4

3.4.1 Nécessité

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

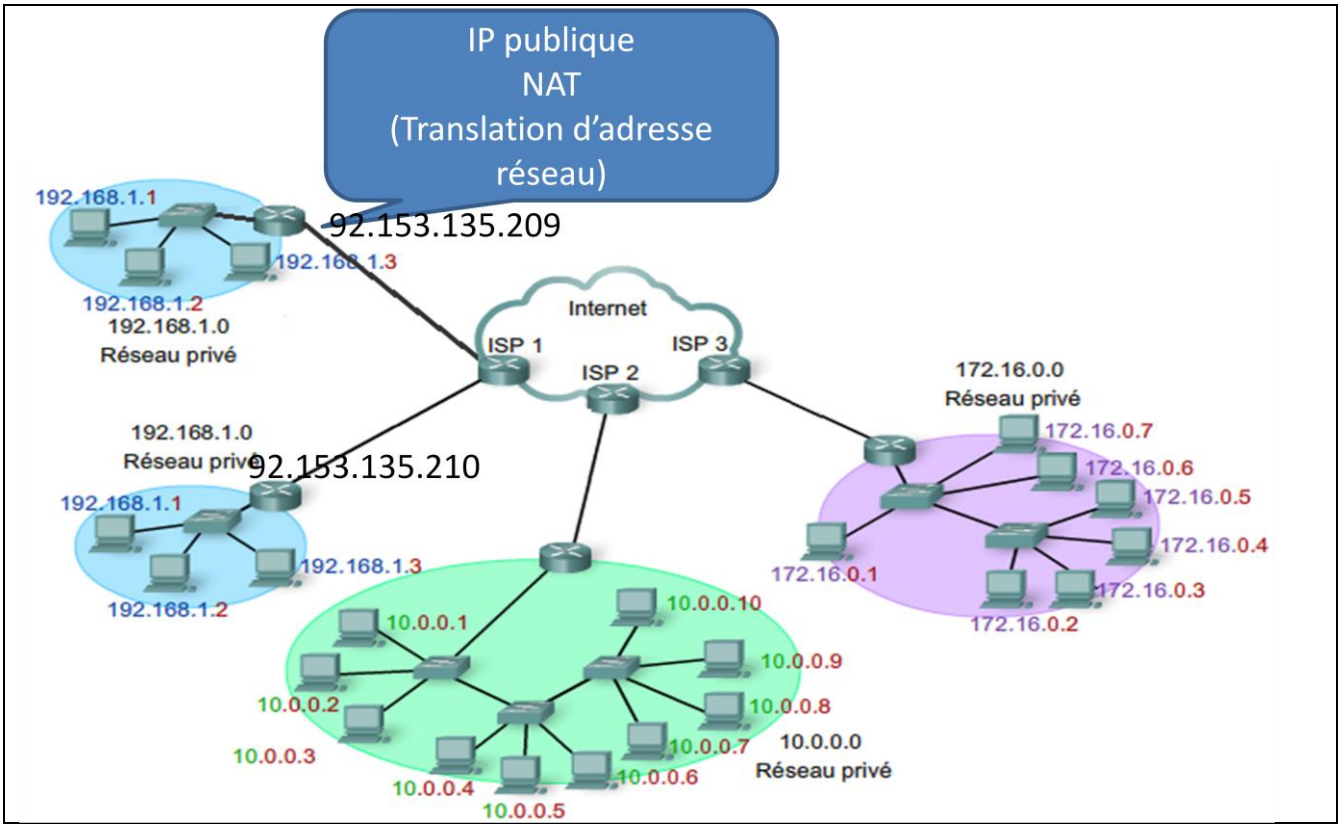
Bien que la majorité des adresses d'hôte IPv4 soient des adresses publiques utilisées dans les réseaux accessibles sur Internet, d'autres blocs d'adresses sont attribués à des réseaux qui ne nécessitent pas d'accès à Internet, ou uniquement un accès limité. Ces adresses sont appelées des adresses privées.

Les blocs d'adresses d'espace privé, comme illustrés, sont réservés aux réseaux privés. L'utilisation de ces adresses ne doit pas forcément être unique entre des réseaux externes. En règle générale, les hôtes qui ne nécessitent pas d'accès à Internet peuvent utiliser les adresses privées sans limitation. Toutefois, les réseaux internes doivent configurer des schémas d'adressage réseau pour garantir que les hôtes des réseaux privés utilisent des adresses IP qui sont uniques au sein de leur environnement de réseau.

Plusieurs hôtes de réseaux différents peuvent utiliser les mêmes adresses d'espace privé. Les paquets qui utilisent ces adresses comme source ou destination ne doivent pas être visibles sur Internet. Le routeur ou le périphérique pare-feu, en périphérie de ces réseaux privés, doivent bloquer ou traduire ces adresses. Même si ces paquets parvenaient sur Internet, les routeurs ne disposeraient pas de routes pour les acheminer vers le réseau privé en question.

Grâce à des services qui traduisent les adresses privées en adresses publiques, les hôtes d'un réseau privé peuvent accéder aux ressources présentes sur Internet. Appelés NAT (Network Address Translation), ces services peuvent être mis en œuvre sur un périphérique situé en périphérie du réseau privé.

Les services NAT permettent aux hôtes du réseau « d'emprunter » une adresse publique pour communiquer avec des réseaux externes. Bien que les services NAT soient associés à des limitations et à des problèmes de performances, ils permettent aux clients de nombreuses applications d'accéder à des services sur Internet, sans difficulté majeure.



Dans la plupart des réseaux de données, l'immense majorité des hôtes sont des périphériques finaux, tels que des ordinateurs, des téléphones IP, des imprimantes et des assistants numériques personnels. Dans la mesure où ces hôtes représentent le plus grand nombre de périphériques au sein d'un réseau, le plus grand nombre d'adresses doit leur être attribué.

3.4.2 Attribution

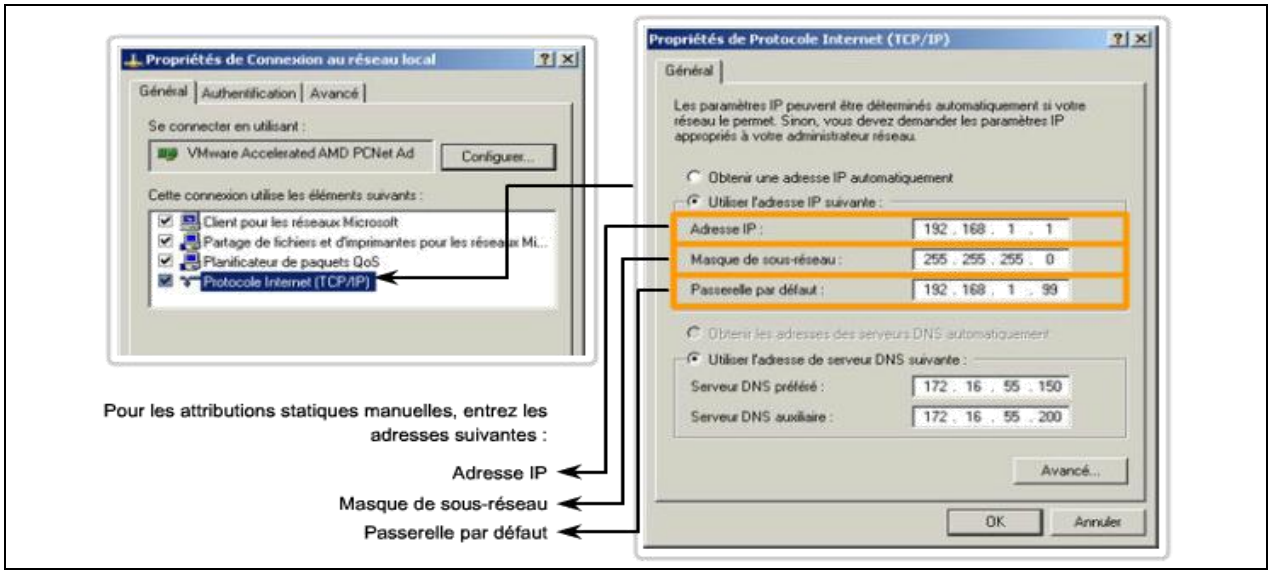
Les adresses IP peuvent être attribuées de manière statique ou de manière dynamique.

- **Attribution statique d'adresses**

  Avec ce type d'attribution, l'administrateur réseau doit configurer manuellement les informations de réseau pour un hôte, comme indiqué dans la figure. Ces informations comportent, au minimum, l'adresse IP, le masque de sous-réseau et la passerelle par défaut.

  Les adresses statiques présentent certains avantages sur les adresses dynamiques. Par exemple, elles conviennent pour les imprimantes, les serveurs et d'autres périphériques réseau, qui doivent être accessibles pour les clients d'un réseau. Si les hôtes ont l'habitude d'accéder à un serveur à une adresse IP particulière, cela peut poser des problèmes en cas de modification de cette adresse. De plus, l'attribution statique des informations d'adressage permet de mieux contrôler les ressources réseau. Toutefois, la configuration IP sur chaque hôte prend du temps.

  Lorsque l'adressage IP statique est utilisé, il convient de tenir à jour une liste exacte des adresses IP attribuées à chaque périphérique. Ces adresses étant permanentes, en principe, elles ne seront pas réutilisées.



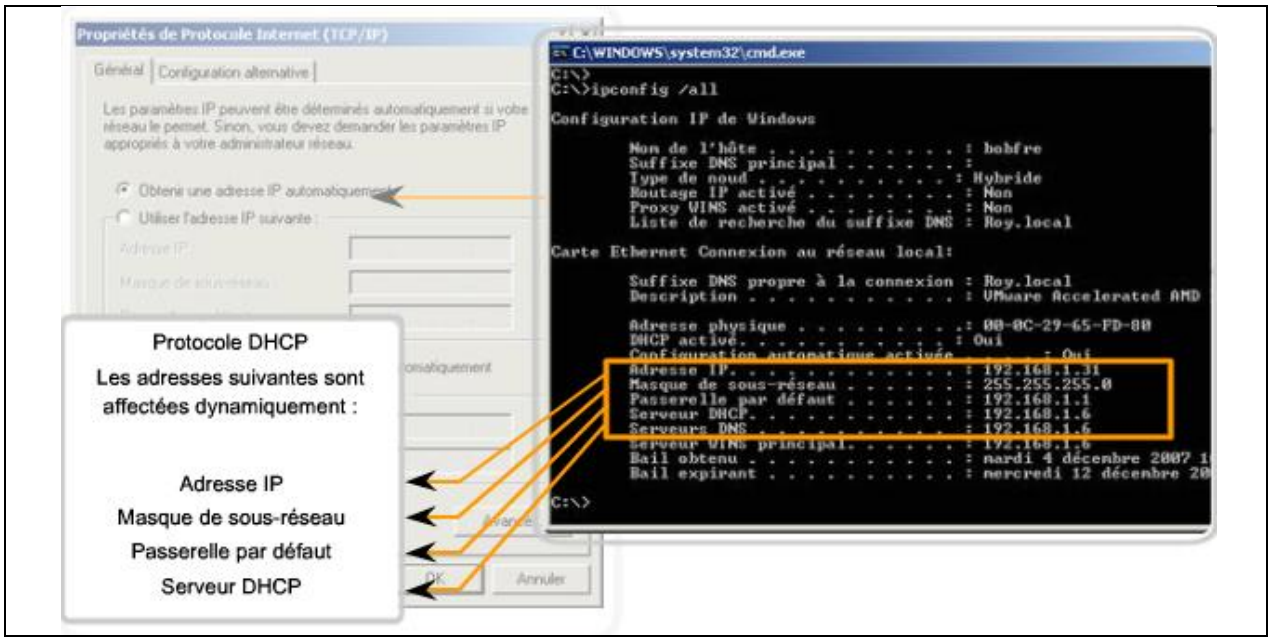
- **Attribution dynamique d'adresses**

  En raison des difficultés associées à la gestion des adresses statiques, les périphériques des utilisateurs se voient attribuer leur adresse de manière dynamique, à l'aide du protocole DCHP (Dynamic Host Configuration Protocol), comme indiqué dans la figure.

  Le protocole DHCP permet l'attribution automatique des informations d'adressage, telles que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et d'autres paramètres. La configuration du serveur DHCP nécessite qu'un bloc d'adresses appelé pool d'adresses soit défini de manière à être attribué aux clients DHCP d'un réseau. Les adresses attribuées à ce pool doivent être définies de manière à exclure toutes les adresses utilisées pour les autres types de périphérique.

  Le protocole DHCP est généralement la méthode d'attribution d'adresses IP privilégiée pour les réseaux de grande taille, car le personnel de support du réseau est dégagé de cette tâche et le risque d'erreur de saisie est quasiment éliminé.

  L'autre avantage de l'attribution dynamique réside dans le fait que les adresses ne sont pas permanentes pour les hôtes, elles sont uniquement « louées » pour une certaine durée. Si l'hôte est mis sous tension ou retiré du réseau, son adresse est renvoyée au pool et sera réutilisée. Cela est particulièrement intéressant pour les utilisateurs mobiles qui se connectent et se déconnectent d'un réseau.

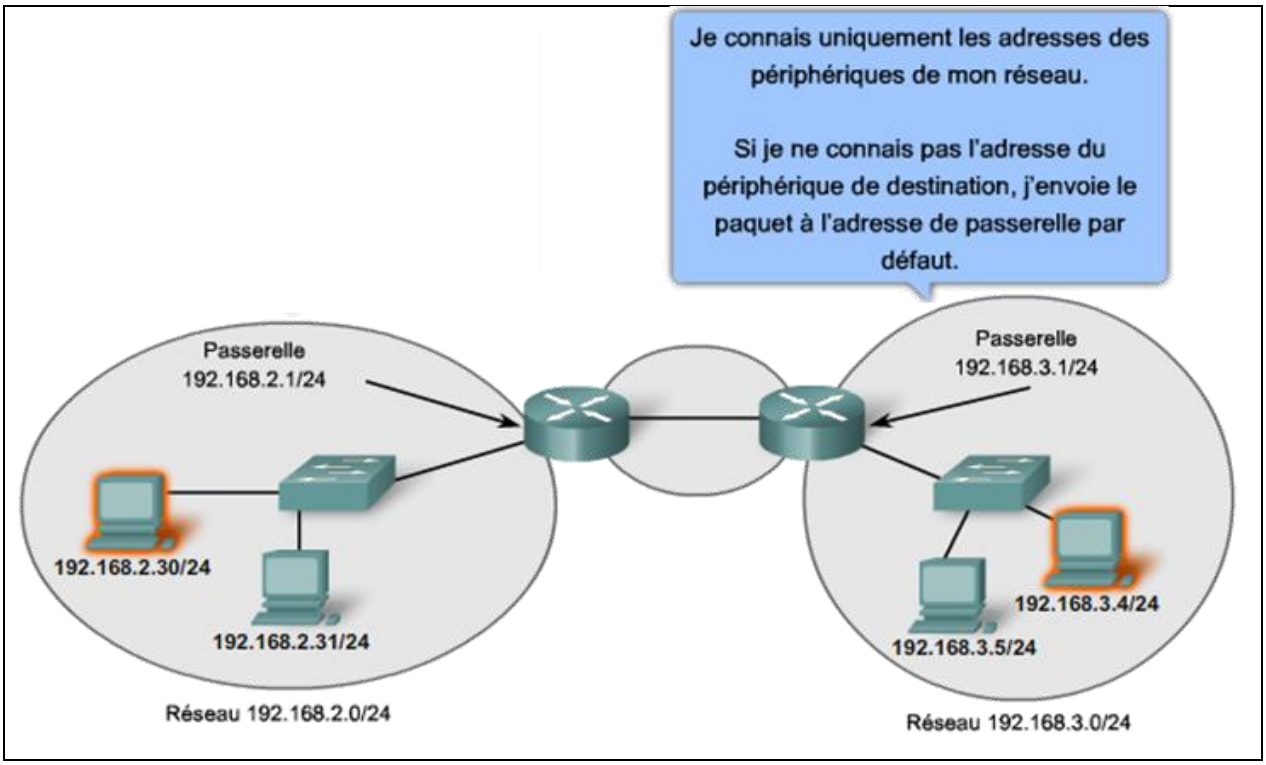


3.4.3 Passerelle par défaut

La passerelle, également appelée passerelle par défaut, est requise pour envoyer un paquet en dehors du réseau local.

Au sein d'un même réseau, les hôtes communiquent entre eux sans nécessiter de périphérique intermédiaire. Quand un hôte doit communiquer avec un autre réseau, un périphérique intermédiaire sert de passerelle avec l'autre réseau.

Cette passerelle est une interface de routeur connectée au réseau local. L'interface de la passerelle a une adresse IP appartenant au réseau auquel elle est connectée. Les hôtes sont configurés pour reconnaître cette adresse comme étant leur passerelle.



3.4.4 Constitution d'une adresse IPv4

Une adresse IPv4 est composée de 4 octets soit 32 bits. La notation couramment utilisée pour représenter ces adresses est notation « décimale pointée ».

Par exemple, l'adresse **10101100 00010000 00000100 00010100**

est exprimée en format décimal pointé de la manière suivante : **172.16.4.20**

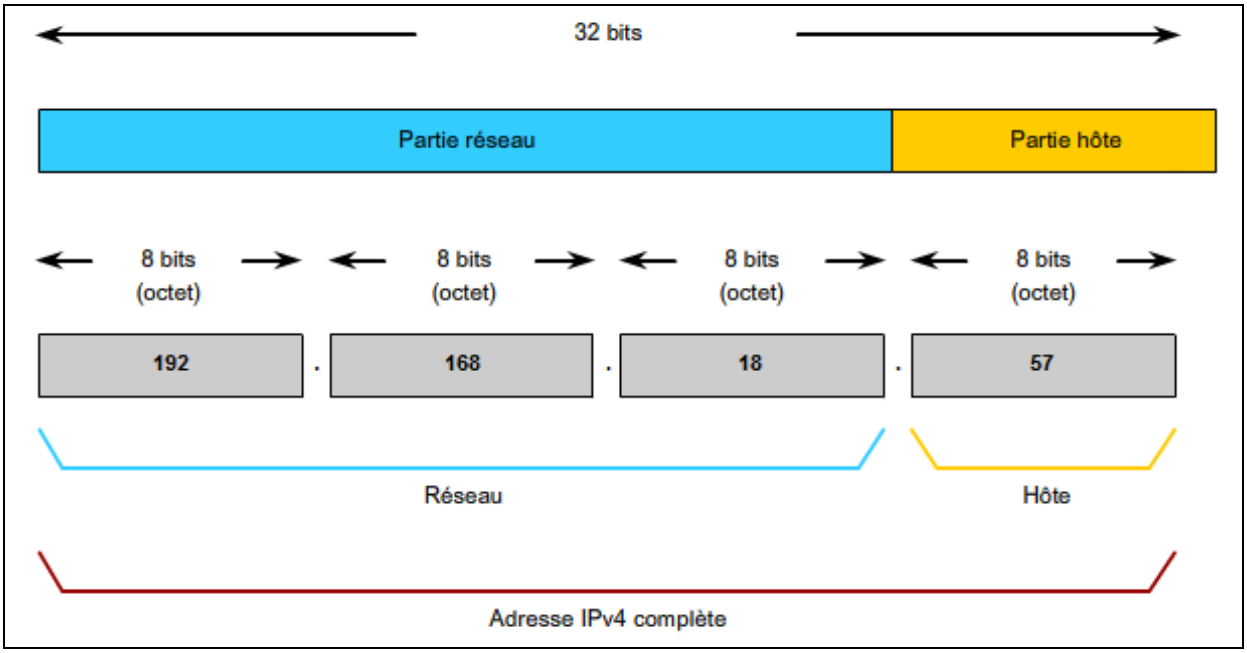
- **Parties réseau et hôte**

  Pour chaque adresse IPv4, une partie des bits d'ordre haut représente l'adresse réseau. Au niveau de la couche 3, un réseau se définit par un groupe d'hôtes dont la partie adresse réseau de l'adresse contient la même configuration binaire.

  Bien que l'ensemble des 32 bits définisse l'adresse IPv4 d'un hôte, un nombre variable de bits constitue la partie hôte de l'adresse. Le nombre de bits contenus dans la partie hôte détermine le nombre d'hôtes possible sur un réseau.

  Par exemple, si un réseau particulier doit contenir au minimum 200 hôtes, il faut utiliser suffisamment de bits dans la partie hôte pour pouvoir représenter au moins 200 configurations binaires différentes.

  Pour attribuer une adresse unique à 200 hôtes, il convient d'utiliser le dernier octet dans son intégralité. Avec 8 bits, nous pouvons obtenir un total de 256 configurations binaires différentes. Nous en déduisons que les bits des trois premiers octets représentent la partie réseau.

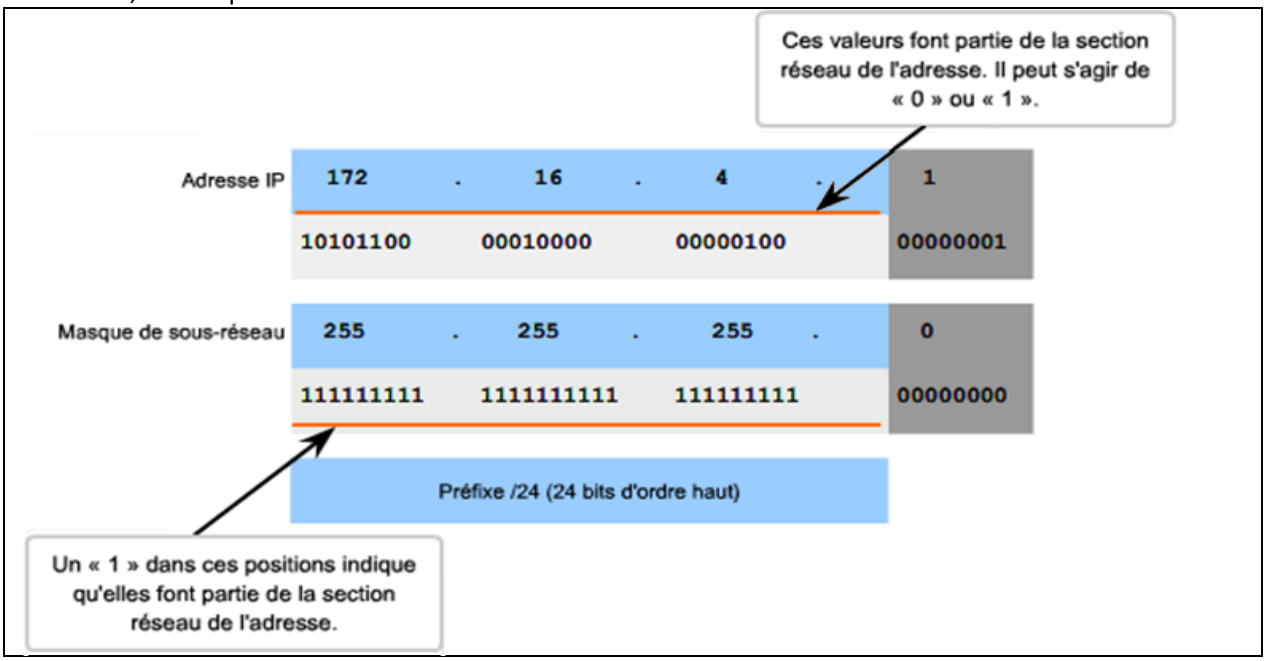


3.4.5 Masque de sous-réseau

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

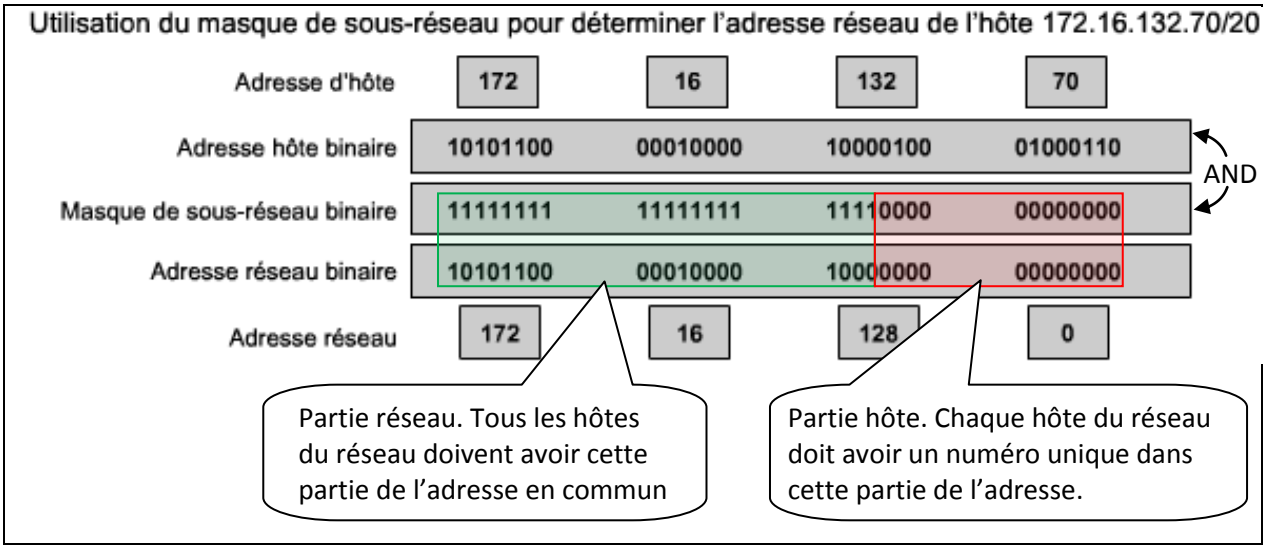
Le masque de sous-réseau est aussi appelé « préfixe ». Ce dernier un nombre de 0 à 32 qui représente le nombre de bits à 1 dans le masque de sous-réseau. Il représente la même chose : la partie réseau d'une adresse.

Par exemple, le préfixe /24, correspondant au masque de sous-réseau 255.255.255.0 (11111111.11111111.11111111.00000000). Les bits restants (à droite) du masque de sous-réseau sont des zéros, et indiquent l'adresse de l'hôte sur le réseau.



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

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



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

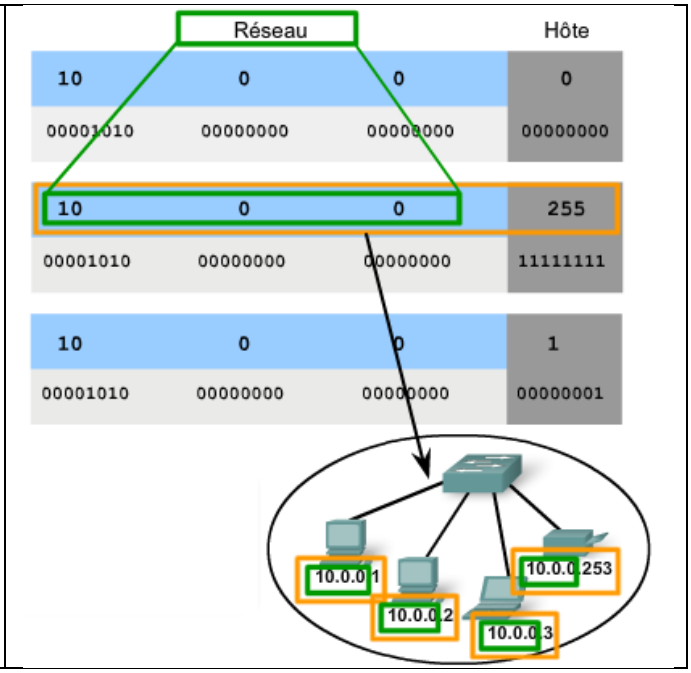
Ce réseau a les caractéristiques suivantes :

Adresse de réseau	172.16.128.0
Adresse du premier hôte	172.16.128.1
...	...
Adresse du dernier hôte	172.16.143.254
Dernière adresse dans le réseau	172.16.143.255

Dernière adresse de réseau = adresse de diffusion

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

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



3.4.6 Les anciennes classes réseau

À l'origine, la spécification RFC1700 regroupait les plages d'adresses en classes appelées classe A, B et C. Elle a également établi des adresses de classe D (multidiffusion) et de classe E (expérimentales).

Remarque : Un hôte peut établir une connexion de type :

- Monodiffusion (unicast) : « Je parle directement à quelqu'un ».
- Diffusion (broadcast) : « Je parle à tout le monde ».
- Multidiffusion (multicast) : « Je parle à un groupe restreint ».

Les classes d'adresse monodiffusion A, B et C définissaient des réseaux d'une certaine taille, ainsi que des blocs d'adresses particuliers pour ces réseaux. Une entreprise ou une administration se voyait attribuer un bloc d'adresses entier de classe A, B ou C. L'utilisation de l'espace d'adressage s'appelait adressage par classe.

- **Blocs d'adresses A**

  Un bloc d'adresses de classe A a été créé pour prendre en charge les réseaux de très grande taille, comportant plus de 16 millions d'adresses d'hôte. Les adresses IPv4 de classe A utilisaient un préfixe /8 invariable, le premier octet indiquant l'adresse réseau. Les trois octets restants correspondaient aux adresses d'hôte.

  Afin de réserver un espace d'adresses aux classes d'adresse restantes, le bit de poids fort de l'octet de valeur supérieure devait être un zéro dans toutes les adresses de classe A. De ce fait, seuls 128 réseaux de classe A, de 0.0.0.0 /8 à 127.0.0.0 /8, étaient possibles, avant de se servir des blocs d'adresses réservées. Bien que les adresses de classe A réservaient la moitié de l'espace d'adressage, elles ne pouvaient être attribuées qu'à 120 entreprises ou administrations, en raison de leur limite de 128 réseaux.

- **Blocs d'adresses B**

  L'espace d'adressage de classe B a été créé pour répondre aux besoins des réseaux de taille moyenne ou de grande taille, comportant plus de 65 000 hôtes. Les adresses IP de classe B utilisaient les deux premiers octets pour indiquer l'adresse réseau. Les deux octets suivants correspondaient aux adresses d'hôte. Comme avec la classe A, l'espace d'adressage pour les classes d'adresses restantes devait être réservé.

  Pour les adresses de classe B, les deux bits de poids fort du premier octet étaient 10. Cela limitait le bloc d'adresses de la classe B à 128.0.0.0 /16-191.255.0.0 /16. Les classes B étaient attribuées plus efficacement que les adresses de classe A, car elles répartissaient 25 % de l'espace d'adressage IPv4 total entre environ 16 000 réseaux.

- **Blocs d'adresses C**

  L'espace d'adressage de la classe C était le plus disponible des anciennes classes d'adresses. Cet espace d'adressage était réservé aux réseaux de petite taille, comportant 254 hôtes au maximum.

  Les blocs d'adresses de classe C utilisaient le préfixe /24. Ainsi, un réseau de classe C ne pouvait utiliser que le dernier octet pour les adresses d'hôte, les trois premiers octets correspondant à l'adresse réseau.

  Les blocs d'adresses de classe C réservaient l'espace d'adressage à la classe D (multidiffusion) et à la classe E (expérimentales) à l'aide d'une valeur fixe de 110 pour les trois bits les plus significatifs du premier octet. Cela limitait le bloc d'adresses de classe C à 192.0.0.0 /16-23.255.255.0 /16. Bien qu'il occupait seulement 12,5 % de l'espace d'adressage IPv4 total, il pouvait attribuer des adresses à 2 millions de réseaux.

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

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

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

  Quelques protocoles de routage font également ce type de supposition de masque. Lorsque ces protocoles de routage reçoivent une route annoncée, ils peuvent prévoir la longueur de préfixe en fonction de la classe de l'adresse.

Classe d'adresses	Plage du premier octet (décimal)	Bits du premier octet (les bits verts ne changent pas)	Parties réseau (N) et hôte (H) de l'adresse	Masque de sous-réseau par défaut (décimal et binaire)	Nombre de réseaux et d'hôtes possibles par réseau
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 réseaux (2^7) 16 777 214 hôtes par réseau (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16 384 réseaux (2^14) 65 534 hôtes par réseau (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2 097 150 réseaux (2^21) 254 hôtes par réseau (2^8-2)
D	224-239	11100000-11101111	S.O. (multidiffusion)		
E	240-255	11110000-11111111	S.O. (expérimental)		

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

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

- **Adresses réseau et de diffusion**

  La première et la dernière adresse ne peuvent pas être attribuées à des hôtes. Il s'agit respectivement de l'adresse réseau et de l'adresse de diffusion.

- **Route par défaut**

  La route IPv4 par défaut est représentée de la manière suivante : 0.0.0.0.

  La route par défaut est utilisée comme route « dernier recours » lorsqu'aucune route plus spécifique n'est disponible. L'utilisation de cette adresse réserve également toutes les adresses de la plage 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8).

- **Bouclage**

  L'adresse de bouclage IPv4 127.0.0.1 est une autre adresse réservée. Il s'agit d'une adresse spéciale que les hôtes utilisent pour diriger le trafic vers eux-mêmes. L'adresse de bouclage crée un moyen rapide, pour les applications et les services TCP/IP actifs sur le même périphérique, de communiquer entre eux. En utilisant l'adresse de bouclage à la place de l'adresse d'hôte IPv4 attribuée, deux services actifs sur le même hôte peuvent contourner les couches les plus basses de la pile TCP/IP. Vous pouvez également envoyer une requête ping à l'adresse de bouclage afin de tester la configuration TCP/IP de l'hôte local.

  Bien que seule l'adresse 127.0.0.1 soit utilisée, les adresses de la plage 127.0.0.0-127.255.255.255 sont réservées. Toutes les adresses de cette plage sont envoyées en boucle sur l'hôte local. Aucune des adresses de cette plage ne devrait jamais apparaître sur un réseau quel qu'il soit.

- **Adresses locales-liens**

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

- **Les adresses de multidiffusion**

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

- **Les adresses expérimentales**

  La plage d'adresses expérimentales IPv4 s'étend de 240.0.0.0 à 255.255.255.254. Actuellement, ces adresses sont répertoriées comme étant réservées pour une utilisation future (RFC 3330). Cela laisse à penser qu'elles pourraient être converties en adresses utilisables. Pour l'instant, leur utilisation dans des réseaux IPv4 n'est pas permise. Toutefois, ces adresses pourraient s'appliquer à la recherche.

- **Les adresses publiques**

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

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

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

3.5 Principe du routage

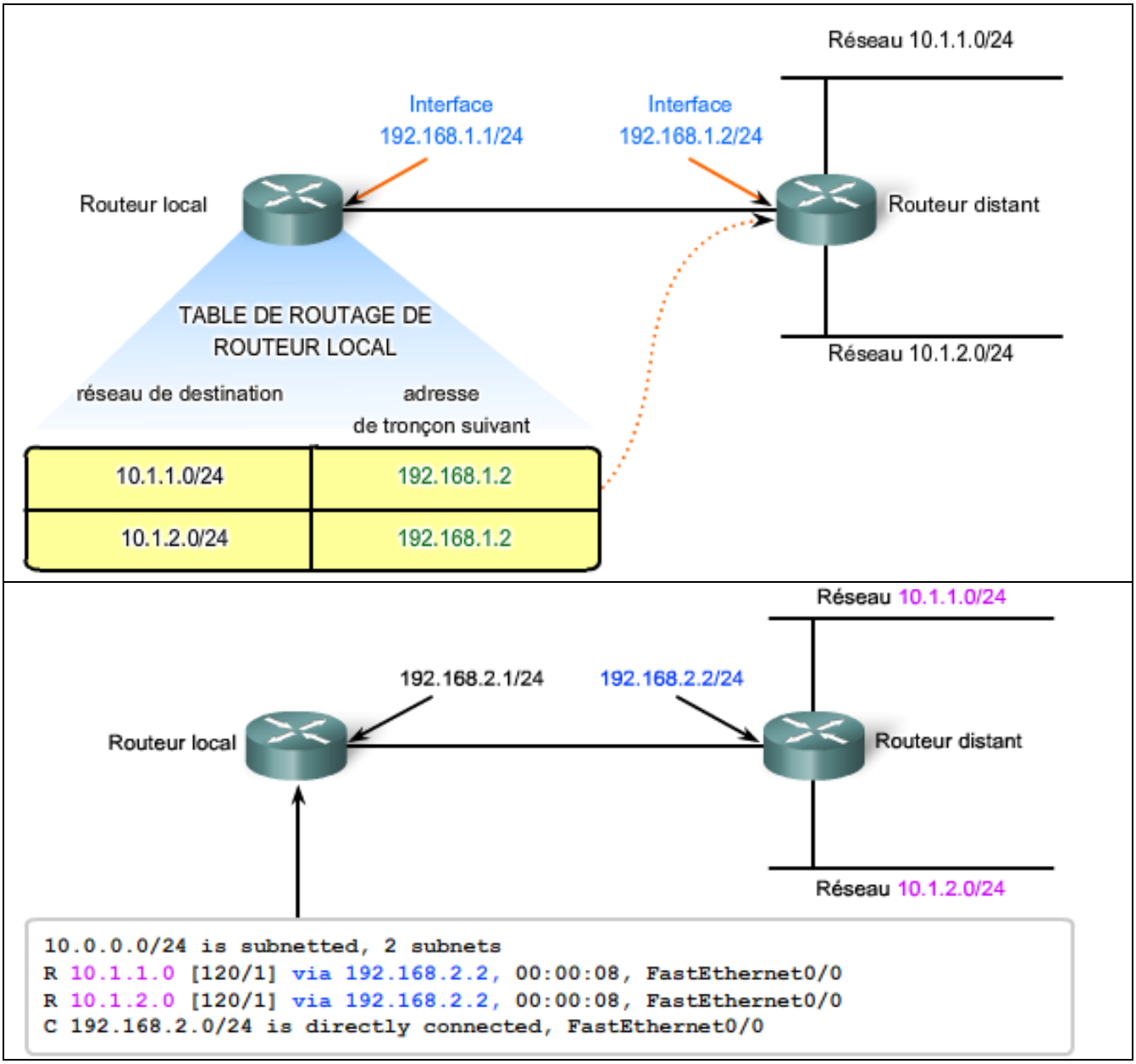
Si l'hôte de destination se trouve sur le même réseau que l'hôte source, le paquet est acheminé entre les deux hôtes sur le support local sans nécessiter de routeur.

Cependant, si l'hôte de destination et l'hôte source ne se trouvent pas sur le même réseau, le réseau local achemine le paquet de la source vers son routeur de passerelle. Le routeur examine la partie réseau de l'adresse de destination du paquet et achemine le paquet à l'interface appropriée. Si le réseau de destination est connecté directement à ce routeur, le paquet est transféré directement vers cet hôte. Si le réseau de destination n'est pas connecté directement, le paquet est acheminé vers un second routeur qui constitue le routeur de tronçon suivant.

Le transfert du paquet devient alors la responsabilité de ce second routeur. De nombreux routeurs ou sauts tout au long du chemin peuvent traiter le paquet avant qu'il n'atteigne sa destination.

Aucun paquet ne peut être acheminé sans route. Que le paquet provienne d'un hôte ou qu'il soit acheminé par un routeur intermédiaire, le routeur a besoin d'une route pour savoir où l'acheminer. S'il n'existe aucune route vers un réseau de destination, le paquet ne peut pas être transféré. Les routeurs utilisent des tables de routage qui contiennent les routes qu'ils connaissent. Ces tables peuvent être construites manuellement (routage statique) ou automatiquement (routage dynamique). Dans ce cas, les routeurs s'appuient sur des protocoles spécifiques comme le protocole RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), ….

Le réseau de destination peut être éloigné de la passerelle par un certain nombre de routeurs ou de sauts. La route vers ce réseau n'indique que le routeur de tronçon suivant vers lequel le paquet doit être transféré, et non le routeur final. Le processus de routage utilise une route de la table de routage pour mapper l'adresse du réseau de destination au tronçon suivant, puis transfère le paquet à cette adresse de tronçon suivant.

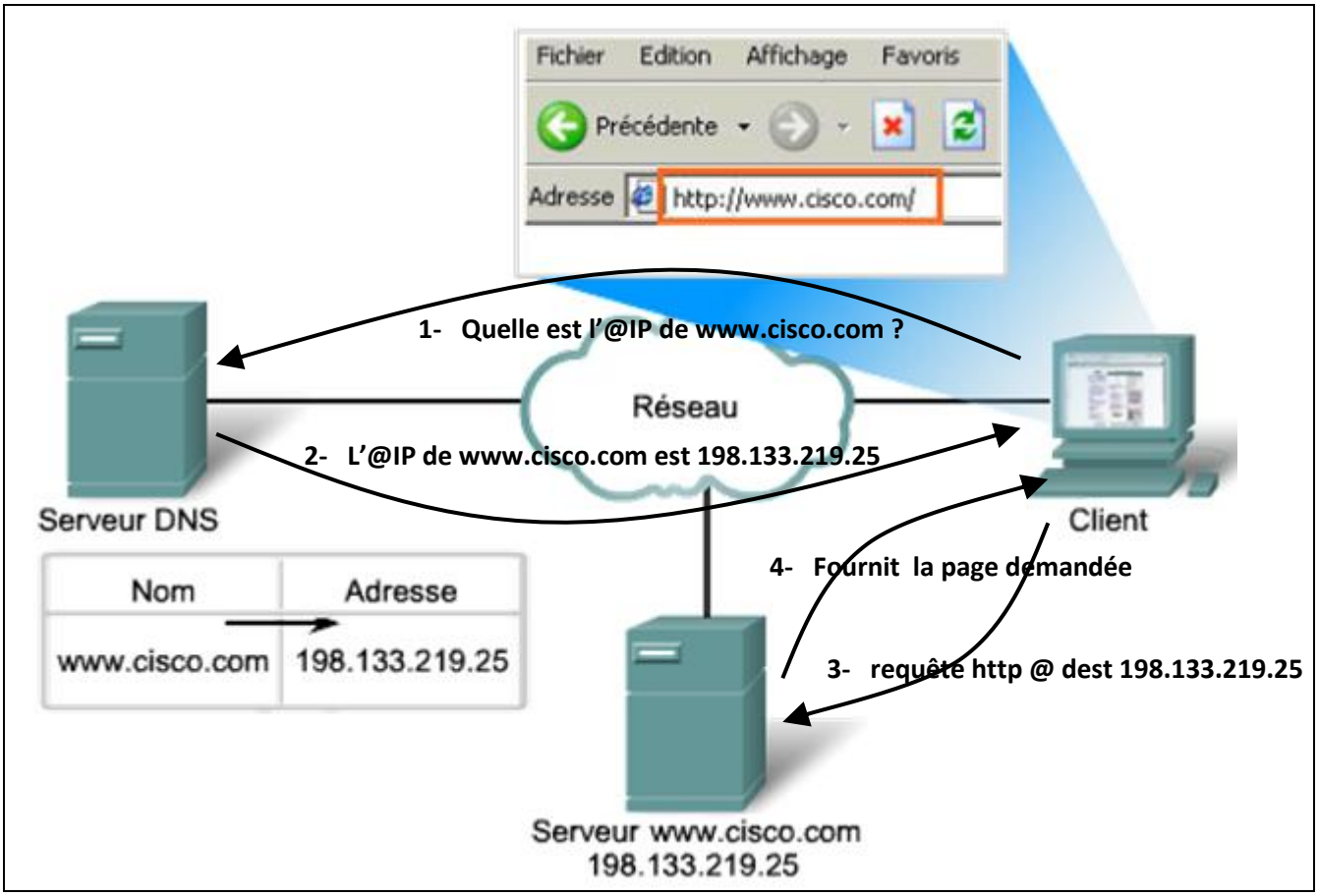


3.6 Principe du nommage – Service DNS (Domaine Name System)

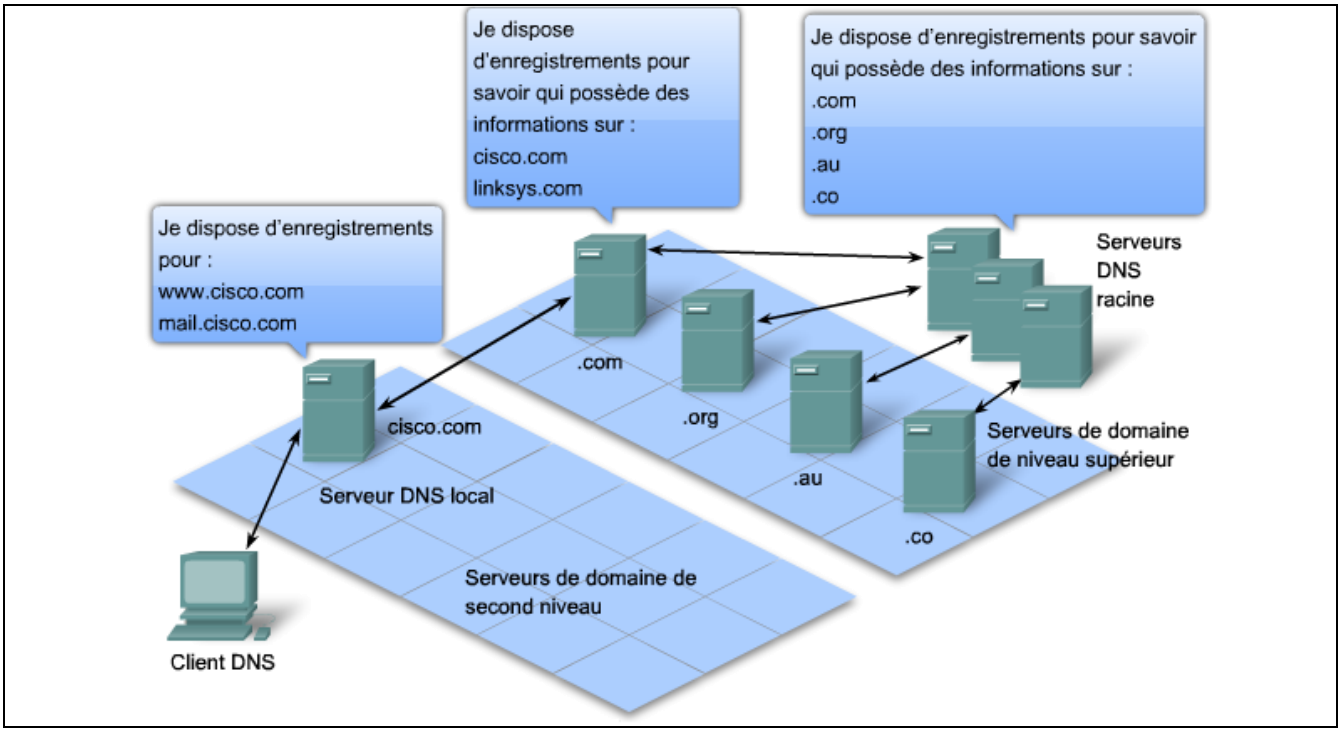
Sur les réseaux de données, les périphériques sont étiquetés par des adresses IP numériques, ce qui leur permet de participer à l'envoi et à la réception de messages via le réseau. Cependant, la plupart des utilisateurs mémorisent très difficilement ces adresses numériques. Pour cette raison, des noms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

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

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



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



3.7 Chemin suivit par l'information

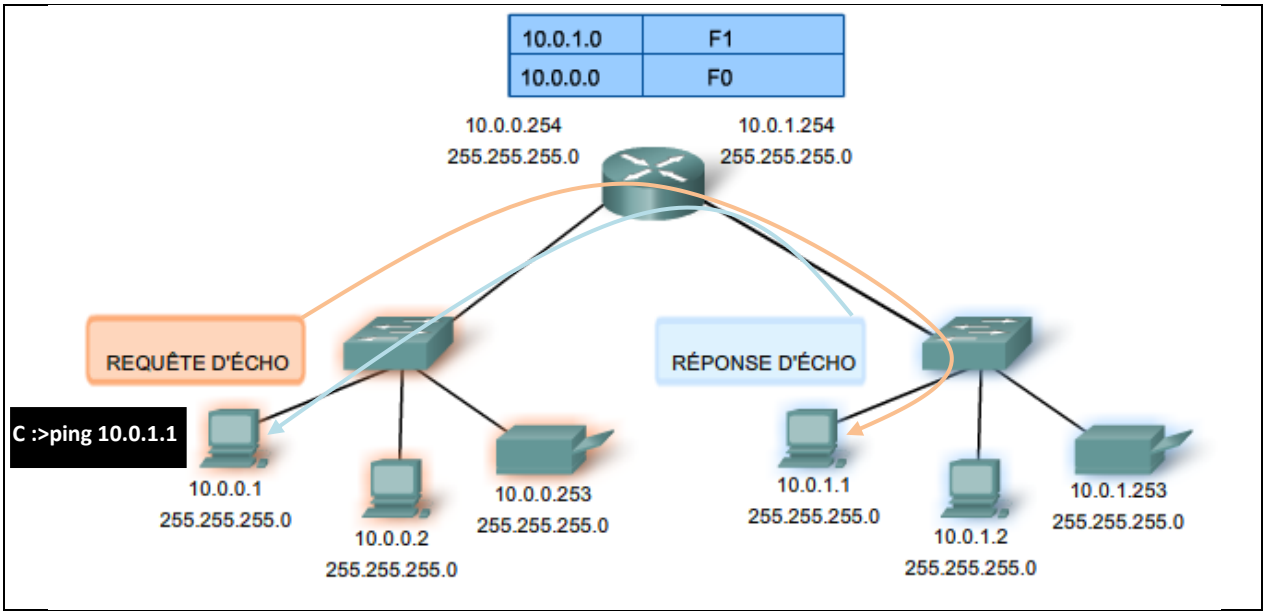
3.7.1 La commande ping

La commande ping est un utilitaire qui permet de tester une connectivité IP entre des hôtes. Elle envoie des demandes de réponse à une adresse hôte spécifiée. Elle utilise un protocole de couche 3 qui fait partie de la suite de protocoles TCP/IP appelée ICMP (Internet Control Message Protocol). Elle utilise un datagramme ICMP Echo Request.

Si l'hôte, à l'adresse spécifiée, reçoit une demande Echo, il répond par un datagramme ICMP Echo Reply. Pour chaque paquet envoyé, la commande ping mesure la durée de réception de la réponse.

Au fur et à mesure de la réception des réponses, la commande ping affiche l'intervalle de temps écoulé entre le moment où la requête ping a été envoyée et le moment de réception de la réponse. Cela permet de mesurer les performances du réseau. La commande ping a une valeur de délai d'attente pour la réponse. Si la réponse n'est pas reçue dans le délai imparti, la commande ping abandonne l'opération et affiche un message indiquant que la réponse n'a pas été reçue.

Une fois toutes les requêtes envoyées, l'utilitaire ping présente la sortie des résultats avec un récapitulatif des réponses. Cette sortie indique le taux de réussite et le délai moyen aller-retour, jusqu'à la destination.



3.7.2 La commande traceroute (tracert)

La commande traceroute (tracert) est un utilitaire qui permet d'identifier le chemin entre des hôtes. L'analyse du chemin génère une liste de sauts qui ont été traversés sur le trajet.

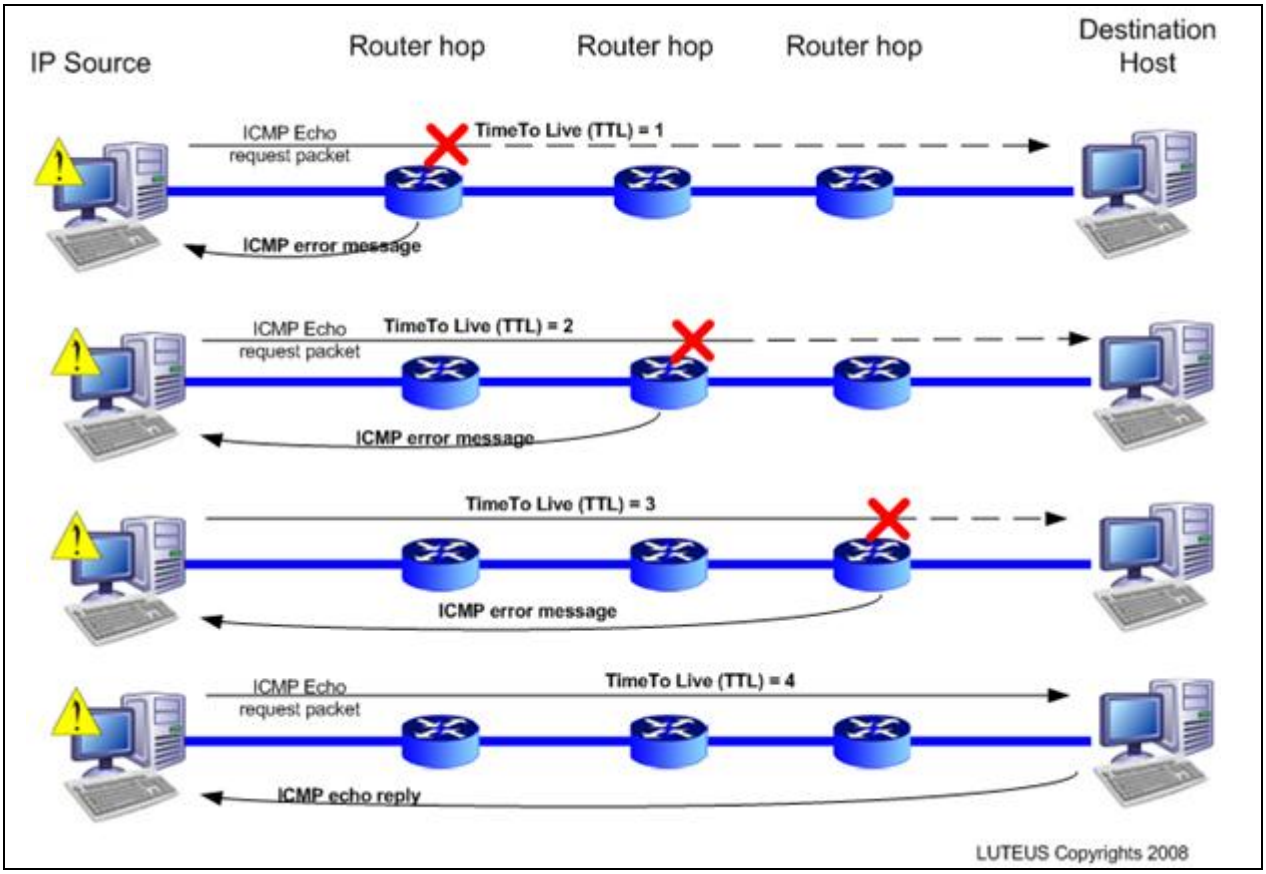
Cette liste peut fournir d'importantes informations pour la vérification et le dépannage. Si les données parviennent à destination, l'analyse du chemin répertorie tous les routeurs rencontrés sur le chemin.

Si les données n'atteignent pas un des sauts sur leur parcours, l'adresse du dernier routeur qui a répondu à l'analyse est renvoyée. Elle indique, soit l'endroit où le problème est survenu, soit l'endroit où des restrictions de sécurité s'appliquent.

La commande traceroute utilise une fonction de durée de vie dans l'en-tête de la couche 3 et le message ICMP Time Exceeded (Dépassement du délai). Le champ TTL permet de limiter le nombre de sauts qu'un paquet peut rencontrer. Lorsqu'un paquet traverse un routeur, le champ TTL est décrémenté de 1. Lorsque la durée de vie atteint zéro, le routeur ne transmet pas le paquet, et ce dernier est abandonné.

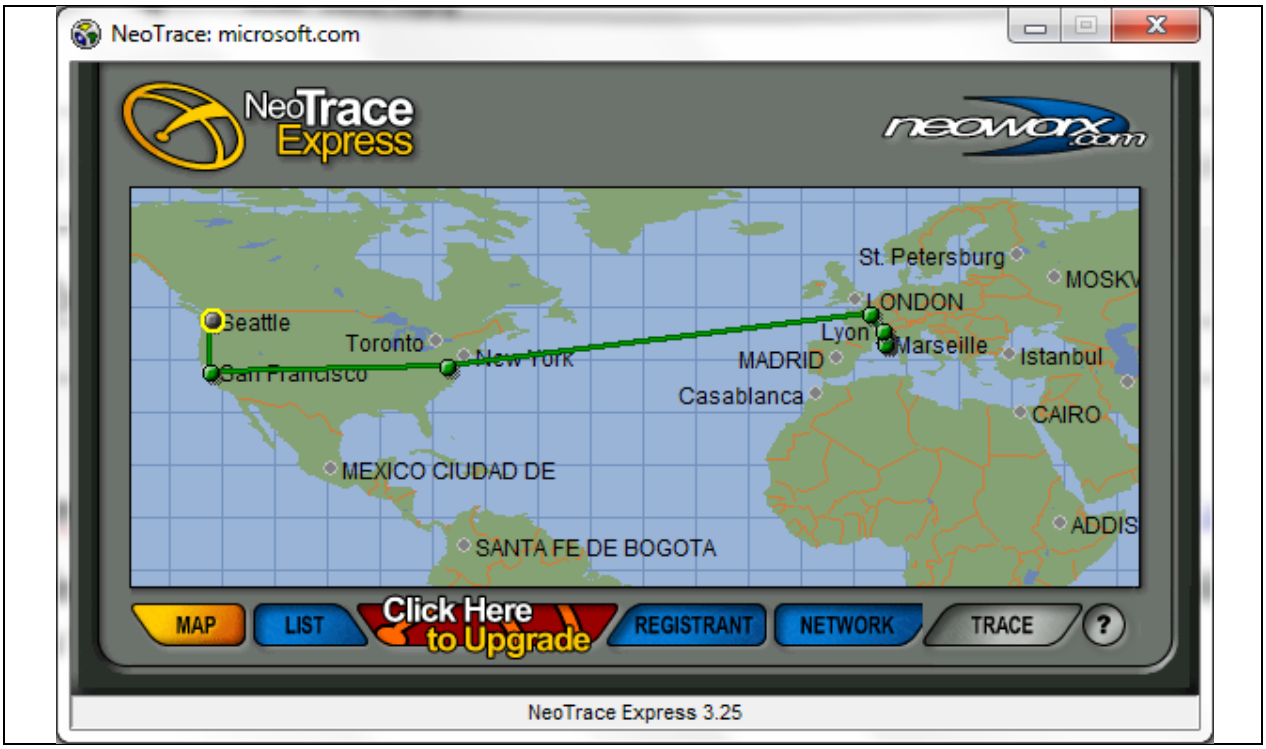
Outre abandonner le paquet, le routeur envoie en principe un message ICMP Time Exceeded (Délai dépassé) adressé à l'hôte source. Ce message contient l'adresse IP du routeur qui a répondu.

Le délai de TTL par défaut est fixé à 30.



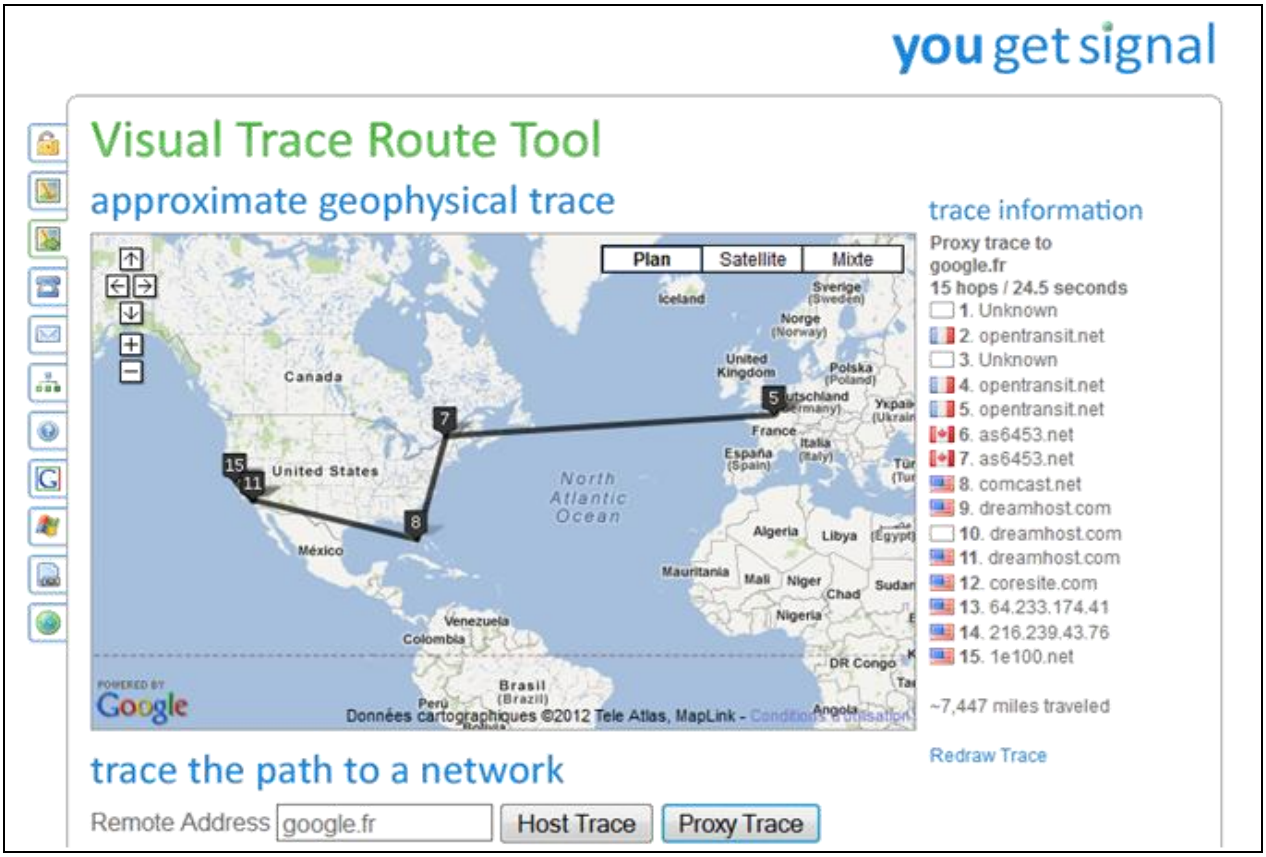
Il existe des logiciels qui fournissent une représentation graphique du chemin parcouru par l'information sur une carte du monde :

Neotrace (Express version gratuite, Pro évaluation pendant 30 jours)



Visual Traceroute : outil en ligne accessible à l'adresse http://www.yougetsignal.com/tools/visual-tracert/

Cet outil très simple à utilisé présente toutefois l'inconvénient de passer obligatoirement par les serveurs du fournisseur du service.



3.7.3 Analyse de l'entête d'un message électronique

Le courriel, le service réseau le plus répandu, par sa simplicité et sa vitesse d'exécution, a révolutionné la manière dont nous communiquons. Mais pour s'exécuter sur un ordinateur ou autre périphérique final, une messagerie nécessite plusieurs applications et services. Les protocoles POP (Post Office Protocol) et SMTP (Simple Mail Transfer Protocol), illustrés dans la figure, sont deux exemples de protocoles de couche application. Tout comme le protocole HTTP, ces protocoles définissent des processus client/serveur.

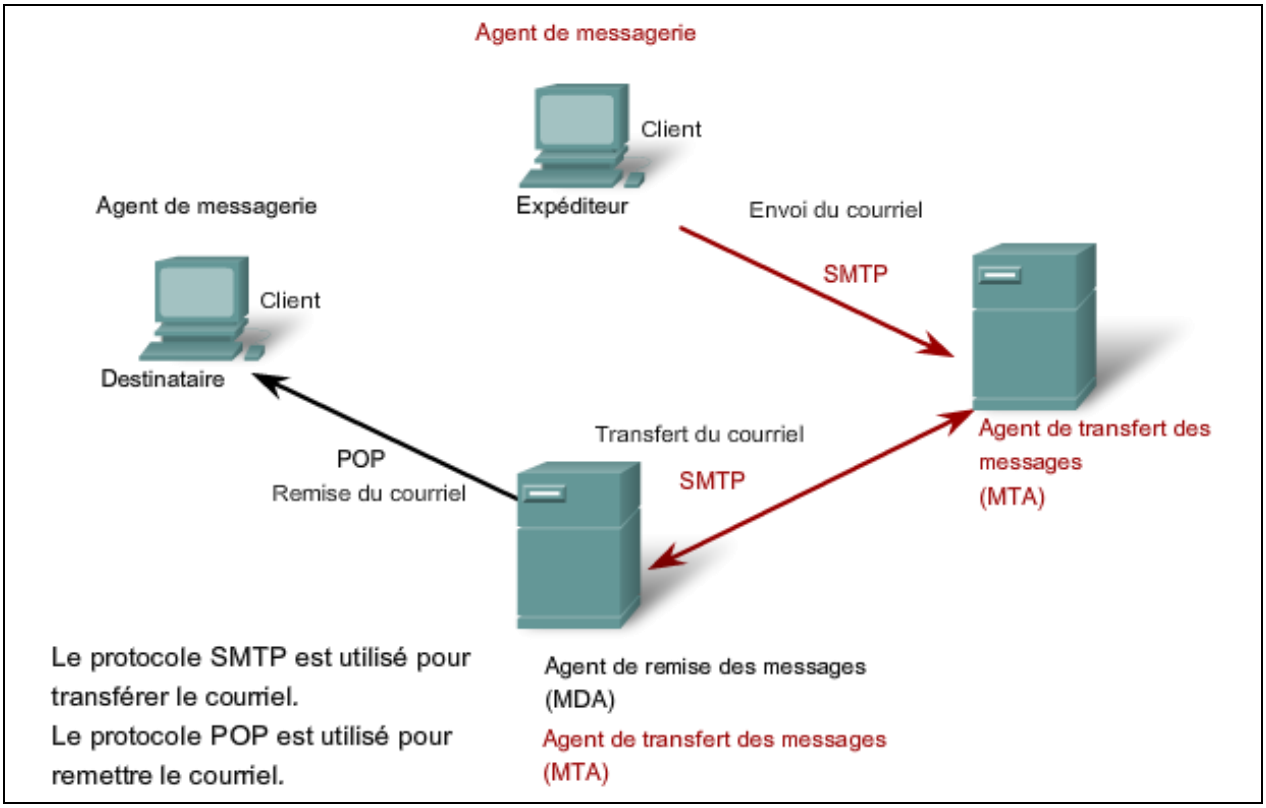
Lorsque l'utilisateur rédige un courriel, il fait généralement appel à une application connue sous le nom d'agent de messagerie ou de client de messagerie. L'agent de messagerie permet l'envoi des messages et place les messages reçus dans la boîte aux lettres du client, ces deux processus étant des processus distincts.

Pour recevoir le courriel d'un serveur de messagerie, le client de messagerie peut utiliser le protocole POP. L'envoi de courriel à partir d'un client ou d'un serveur implique l'utilisation de commandes et de formats de messages définis par le protocole SMTP. Un client de messagerie fournit généralement les fonctionnalités des deux protocoles au sein d'une application.

Le serveur de messagerie opère deux processus distincts :

- agent de transfert des messages (MTA) ;
- agent de remise des messages (MDA).

Le processus MTA est utilisé pour transférer le courriel. Le courriel peut traversé plusieurs serveurs intermédiaires MTA avant d'arriver sur le serveur MDA du destinataire.



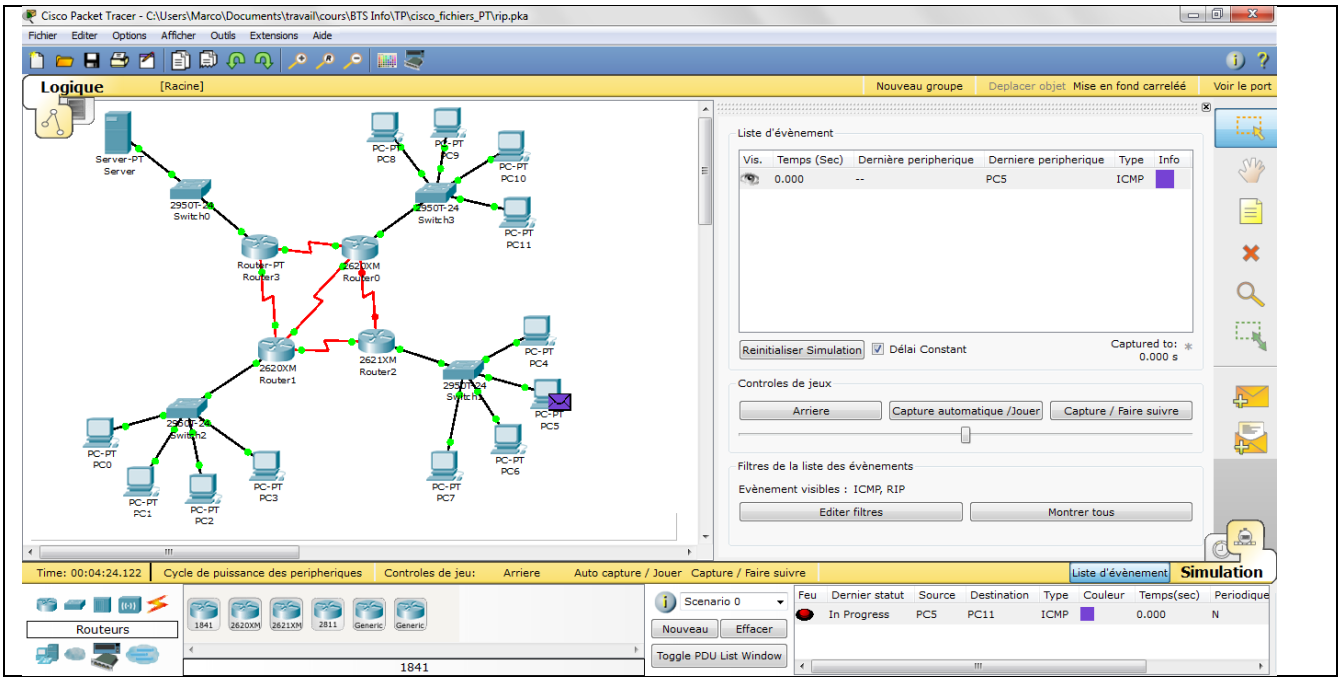
L'en-tête électronique d'un courriel renseigne sur l'expéditeur, le destinataire, la date, l'objet du courriel, le nom de chaque serveur de transmission impliqué, l'heure de l'envoi et l'adresse IP de l'expéditeur.

Détails :

```
Return-Path: <jkalsi@cisco.com>

Received: from mwinf5c51 (mwinf5c51.me-wanadoo.net [10.223.111.101])
by mwinb2603 with LMTPA;
Tue, 21 Feb 2012 02:03:46 +0100


Received: from rcdn-app-2.cisco.com ([173.37.86.82])
by mwinf5c51 with ME
id cR3l1i01L1mbFxZ01R3mKX; Tue, 21 Feb 2012 02:03:46 +0100


Received: from cna-prd-app35.cisco.com ([173.37.163.20])
 by rcdn-app-2.cisco.com with ESMTP; 21 Feb 2012 01:03:45 +0000

Received: from cna-prd-app35 (localhost.localdomain [127.0.0.1])
by cna-prd-app35.cisco.com (8.13.8/8.13.8) with ESMTP id q1L13jqY020728
for <marc.silanus@orange.fr>; Tue, 21 Feb 2012 01:03:45 GMT
```

4 Outils de simulation

4.1 Packet Tracer



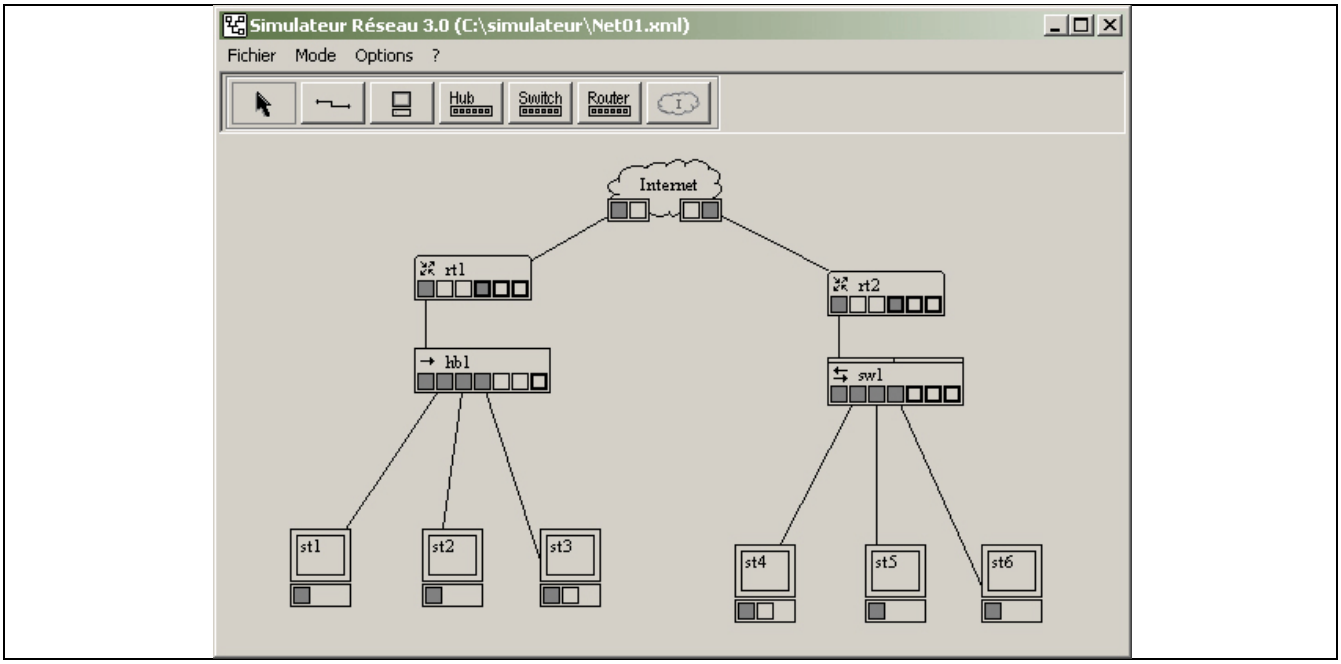
Packet Tracer est un programme puissant de simulation réseau qui permet aux élèves d'expérimenter le comportement du réseau et de répondre aux questions de type «et que ce pace-t-il si».

Il fournit la simulation, la visualisation, de création, d'évaluation et les capacités de collaboration et facilite l'enseignement et l'apprentissage des concepts technologiques complexes.

Il permet aux enseignants de démontrer des concepts techniques complexes liés au fonctionnement des réseaux de données.

Ce logiciel est disponible gratuitement UNIQUEMENT aux instructeurs, étudiants, diplômés, les administrateurs de l'Académie Cisco.

4.2 Le simulateur Réseau V3.0



Beaucoup plus basic que Packet Tracer et payant : http://www.sopireminfo.com/fr/simulateur/reseau/simulateur.html

Le simulateur réseau permet de créer des réseaux de manière graphique.

Un simple clic ajoute une station de travail, un hub, un switch, un routeur, ou encore le composant Internet.

Ces différents éléments peuvent être connectés à l'aide de câbles : droits, croisés, coaxiaux ou lignes télécom.

Chaque composant est configurable. Le fonctionnement du réseau peut être simulé au niveau ethernet, IP, transport ou application.

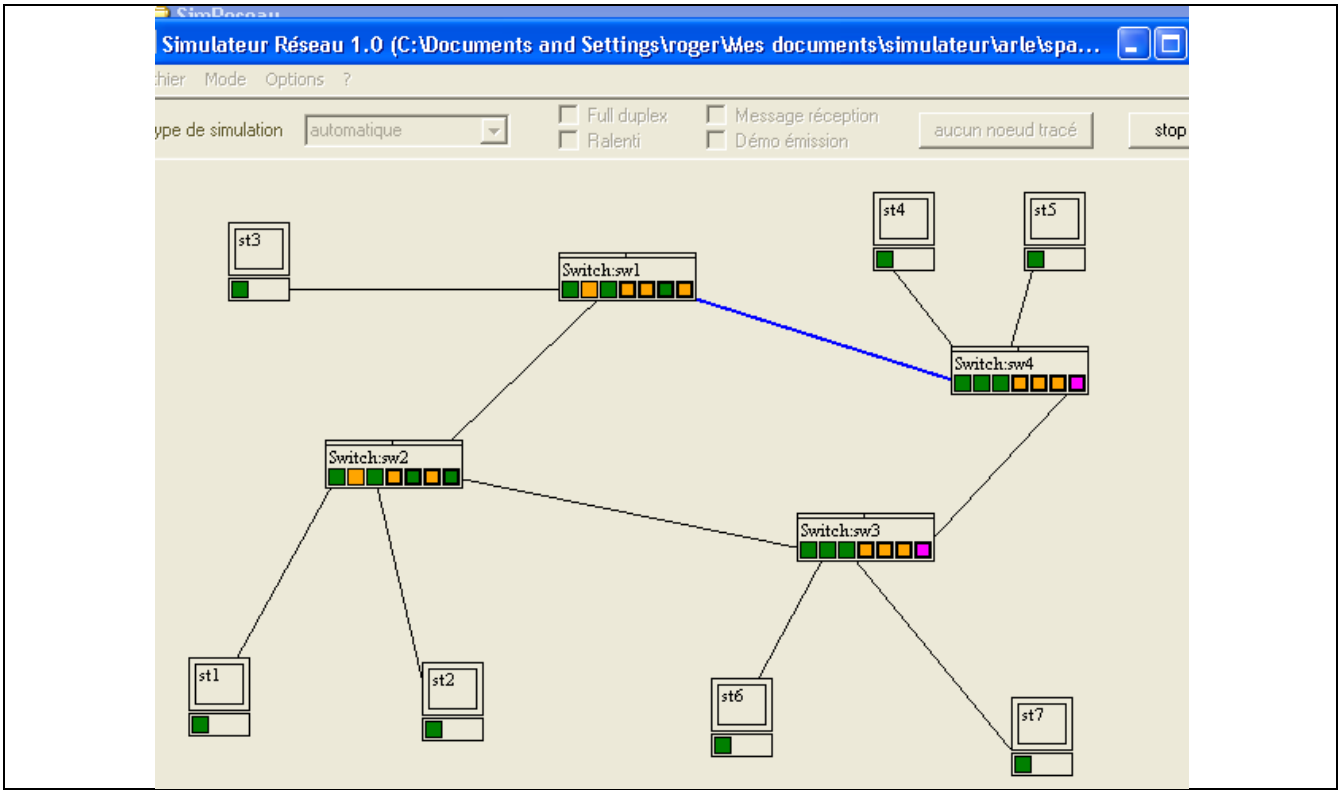
4.3 Le simulateur réseau de Pierre Loisel (Réseau Certa)

Le didacticiel simulateur de réseau local est un logiciel qui permet de construire un réseau virtuel de façon interactive sur écran puis d'observer son fonctionnement. Cet outil est développé par Pierre Loisel.

Ce simulateur réseau a été conçu pour rendre observable les principaux concepts associés aux réseaux locaux : topologie, adressage physique et logique, domaines de collision et de diffusion, commutation, routage, filtrage. Il peut être utilisé dans toutes les formations qui abordent les technologies réseau au niveau physique, liaison Ethernet, réseau IP et transport TCP ou UDP. L'accès au réseau Internet est également simulé. De nouvelles fonctionnalités sont en cours de développement.

De nombreuses ressources pédagogiques, basées sur l'utilisation du simulateur réseau, ont été rédigées. Elles permettent de bâtir un cours en utilisant le logiciel pour réaliser des démonstrations à l'aide d'un vidéo-projecteur ou encore pour faire des exercices.

http://www.reseaucerta.org/outils/simulateur/

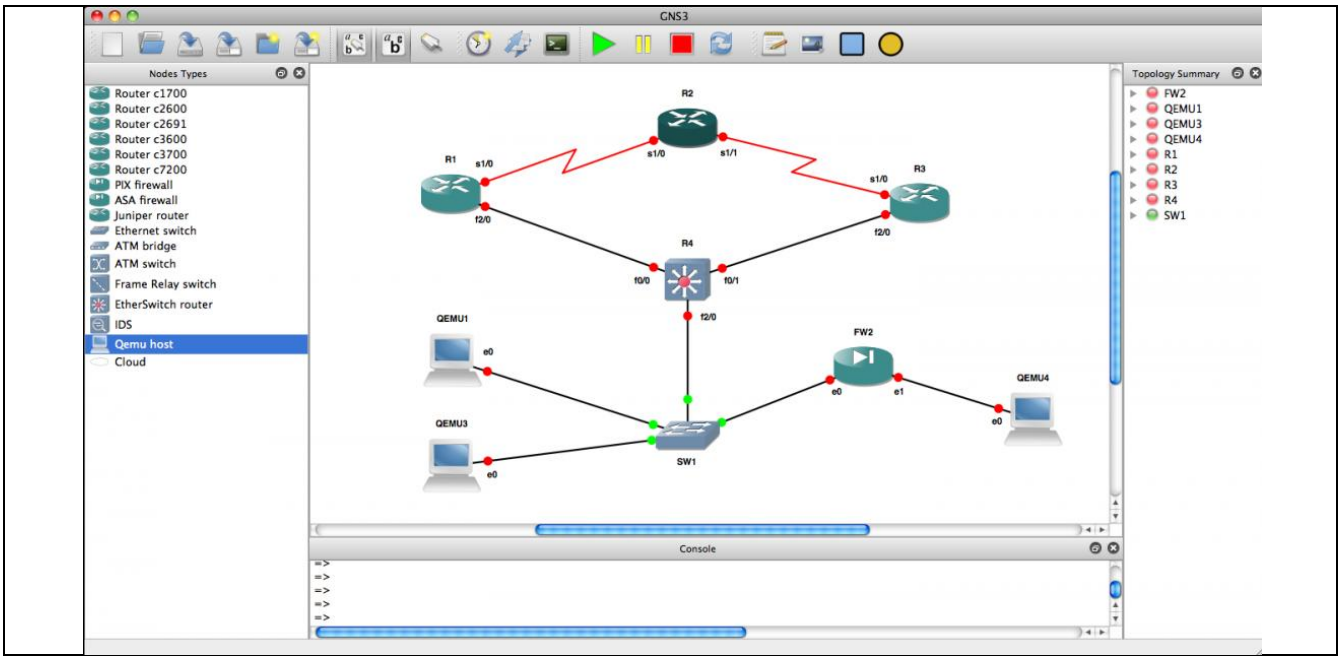


4.4 GNS3 (graphical network simulator)

GNS3 est un simulateur graphique de réseaux OpenSource et multi-plates-formes (Mac OS X, Windows et Linux) qui permet de créer des topologies de réseaux complexes et d'en établir des simulations.

Excellent outils même si la documentation n'existe qu'en anglais.

http://www.gns3.net/



5 Références

- Cours de l'Académie Cisco : CCNA Exploration – Notions de base sur les réseaux
- Cours de réseaux Master 1 d'informatique - Pascal Nicolas - Université d'Angers
  http://www.scribd.com/doc/2969777/Cours-de-reseaux-Maitrise-dinformatique-Universite-dAngers
- Did You Know 3.0 –
  http://www.youtube.com/watch?v=Gv8pmIr3a7k&feature=fvwrel
- L'influence croissante d'internet dans notre vie quotidienne
  http://www.fsa.ulaval.ca/personnel/vernag/eh/f/cons/internet.htm
- Centre pour l'Education et la Sensibilisation à la Coopération Internationale
  (dossier 11 : Internet, poste et télécommunications)
  http://www.genevedecouverte.ch/fr/internet_et_communication.html
- Réseaux locaux industriels et réseaux embarqués – Karen Godary
  http://www.polytech.univ-montp2.fr/~karen.godary/Info_Indus/