PRESENTATION GENERALE DES RESEAUX

Plan du chapitre :

1. Définitions
2. Objectifs d'un réseau
3. Composants physiques d'un réseau
4. Architectures des réseaux
5. Typologies et Topologies des réseaux

Objectifs du chapitre :

- Connaitre les objectifs d'un réseau.
- Connaitre les composants matériels et les architectures des réseau.
- Classifier les réseaux selon leurs tailles et leurs topologies.

1. Définitions :

1.1 Réseau :

Le terme générique « réseau » définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.

On distingue plusieurs catégories de réseaux :

- ✓ Les réseaux des opérateurs de télécommunications : ou RTC (Réseau Téléphonique Commuté) qui sert au transport de la voix.
- ✓ Les réseaux informatiques : Orientés vers le transfert de paquets de données (email, fichiers, etc).
- ✓ Les réseaux de canaux de télévision : Orientés vers la diffusion de canaux soit par des antennes soit par les réseaux câblés.

Pour ce cours, nous allons nous intéresser aux réseaux informatiques.

1.2 Réseau informatique :

C'est un ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques.

2. Objectifs d'un réseau :

Les objectifs d'un réseau sont classiquement les suivants :

- **Le partage de ressources** : Rendre accessible à une communauté d'utilisateurs des programmes, des données et des équipements informatiques (un ensemble de ressources) indépendamment de leur localisation.
- **La Fiabilité** : Permettre le fonctionnement même en cas de problèmes matériels (sauvegardes, duplication ...).
- **La réduction des coûts** : Les petits ordinateurs (PC par ex.) ont un meilleur rapport prix/performances que les gros. Un réseau est aussi une infrastructure de communication permettant le travail collaboratif et/ou les échanges (courrier électronique, discussion en direct, etc.) entre personnes géographiquement séparées.

3. Les composants physiques d'un réseau:

3.1 Périphériques finaux :

Les périphériques réseau auxquels les personnes sont le plus habituées sont appelés périphériques finaux. Ces périphériques forment l'interface entre le réseau humain et le réseau de communication sous-jacent. Comme exemple de ces périphériques, on peut citer :

- Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers, serveurs Web).
- Imprimantes réseau.
- Téléphones.
- Caméras de surveillance.
- Périphériques portables mobiles (par exemple, lecteurs de codes à barres sans fil ou assistants numériques personnels).

Dans le cas d'un réseau, les périphériques finaux sont appelés hôtes. Un périphérique hôte constitue soit la source, soit la destination d'un message transmis à travers le réseau.

3.2 Le support de transmission :

Par support de transmission ou support physique, il faut entendre tous les éléments permettant de transmettre les éléments binaires, suites de 0 et de 1, sur des supports câblés aussi bien que hertziens. Il existe de nombreux types de supports qui seront détaillés dans un autre chapitre, mais on distingue généralement :

- La paire de fils torsadés : C'est le même câble utilisé pour les téléphones.
- Le câble coaxial : Proche du câble qui relie le téléviseur à son antenne.
- La fibre optique : Elle permet de faire circuler l'information sous forme d'ondes lumineuses.
- Les supports hertziens : Elles supportent de grande distance et de grandes capacités.

Les différents types de supports réseau possèdent divers avantages et fonctionnalités. Tous ces supports ne possèdent pas les mêmes caractéristiques et ne conviennent pas pour les objectifs. Les critères de choix d'un support réseau sont :

• La distance sur laquelle les supports peuvent transporter correctement un signal,
• L'environnement dans lequel les supports doivent être installés,
• La quantité de données et le débit de la transmission,
• Le coût des supports et de l'installation.

3.3 Les équipements intermédiaires

Un réseau est composé par des supports de transmission et des machines terminales. Pour les relier, il faut des équipements intermédiaires.

3.3.1 Le connecteur

Le connecteur réalise la connexion mécanique. Il permet le branchement sur le support. Le type de connecteur utilisé dépend évidemment du support physique. Les figures suivantes illustrent deux types de connecteurs différents :

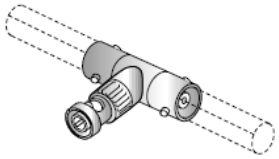


Figure 1: Un connecteur en T pour câble coaxial.

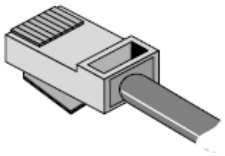


Figure 2: Fiche RJ 45

3.3.2 La carte réseau :

Pour relier un ordinateur à un réseau, il faut aussi disposer d'une carte réseau (coupleur). C'est une interface qui permet de connecter un ordinateur au support de transmission utilisé par le réseau. Elle contrôle le flux d'information qui circule entre l'ordinateur et le réseau. Chaque carte réseau possède une adresse matérielle exclusive. Cette adresse a été définie lors de la fabrication de la carte. Elle sert à identifier chaque carte réseau lorsque des informations sont envoyées ou reçu au sein du réseau.

Figure 3: Carte réseau

3.4 Les équipements d'interconnexion :

L'interconnexion de réseaux peut être locale: les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard (exp. répéteur, concentrateur) suffit à réaliser physiquement la liaison. L'interconnexion peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (exp. modems).

3.4.1 Le modem :

Les modems (modulateur/démodulateur) permettent aux ordinateurs d'échanger des données par l'intermédiaire des réseaux téléphoniques. Le modem émetteur a pour rôle de convertir les données de l'ordinateur (données numérique) pour les rendre transmissible à travers la ligne téléphonique (signaux analogiques). Le modem récepteur a pour rôle de convertir les signaux analogiques qu'il reçoit de la ligne téléphonique en information exploitable pour l'ordinateur (signaux numériques).

3.4.2 Le répéteur :

Un des problèmes les plus gênants lors de la construction d'un réseau est la limitation en termes de distance qui est introduite par les mediums de communication. En effet, plus un câble est long, plus l'atténuation du signal qui circule sur ce câble va être grande. Un des moyens de pallier cet inconvénient est l'utilisation de la fibre optique qui subit une atténuation moindre. Cependant elle reste financièrement un choix peu judicieux dans bien des cas.

La solution réside dans un appareil se nommant « répéteur ». Un répéteur a les caractéristiques suivantes :

- Amplification et régénération du signal origine pour lui permettre de voyager sur de plus longues distances dans le media.
- Possibilité de changer de média (passer d'un câble coaxial à une paire torsadée).

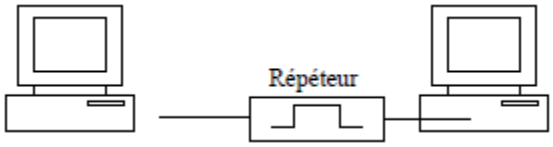


Figure 4: Le répéteur

3.4.3 Le pont (Bridge)

Un pont est un appareil qui permet aux ordinateurs d'un réseau d'échanger des informations :

- **Création d'inter réseaux :** Les ponts servent à relier les réseaux isolés pour leurs permettre de fonctionner ensemble sous la forme d'un même grand réseau.

- **Subdivision d'un réseau existant** : il est également possible de subdiviser un réseau surchargé en parties plus petites. Cette subdivision permet de réduire le volume des informations qui doivent circuler dans chaque partie du réseau.
- **Filtrage** : les ponts déterminent si les informations à transmettre doivent rester au sein du même réseau ou s'il faut les faire passer de l'autre coté du pont.

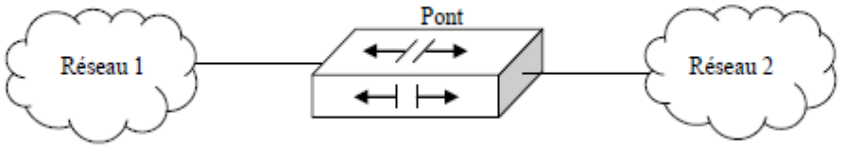


Figure 5: Le pont

3.4.4 Le concentrateur (hub) et le commutateur (switch) :

Les réseaux utilisent presque tous ce type d'équipement. Il possède généralement 4, 8, 16 ou 32 ports. Pour connecter un ordinateur au réseau, il suffit de connecter un câble qui part de la carte réseau à une prise murale qui est connecté au hub ou switch.

Le hub constitue un « répéteur multi_port » car tout signal reçu sur un port est répété (diffusé) sur tous les autres ports. Un message émis par un ordinateur est reçu par tous les autres ordinateurs, mais seul la destination tient compte du message en faisant une copie. Les autres ordinateurs ignorent le message.

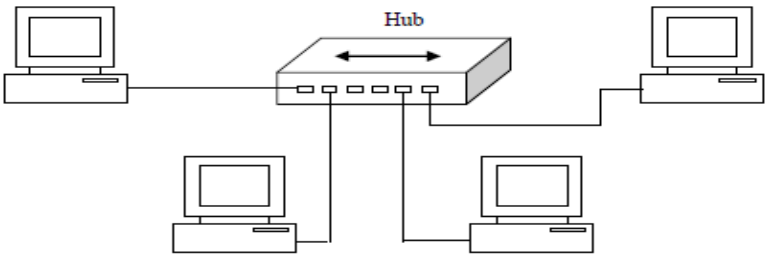


Figure 6: Le Hub

Un switch constitue un « pont multi-port » car il filtre le trafic pour l'acheminer uniquement vers son destinataire.

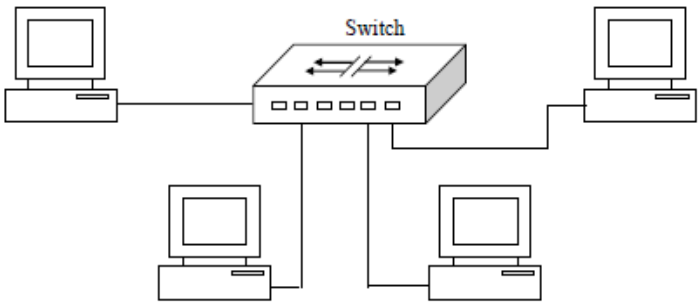


Figure 7: Le Switch

3.4.5 Routeur :

Un routeur permet de relier différents réseaux les uns aux autres. Il a pour rôle de diriger les informations dans la direction appropriée. Les informations peuvent souvent emprunter plusieurs chemins.

Pour fonctionner un routeur il faut lui communiquer un certain nombre d'informations tels que le type de chaque réseau connecté au routeur. Beaucoup de routeurs permettent de brancher directement un ordinateur pour entrer ses informations. Les routeurs réalisent une cartographie des réseaux et ils les subdivisent en segments. Chaque segment reçoit une adresse qui lui est propre. L'adresse du segment du réseau et celle de l'ordinateur destination aide le routeur à calculer le meilleur chemin pour acheminer les données.

4. Architectures des réseaux :

On distingue généralement deux modes de fonctionnement pour les réseaux qui dépendent de:

- Taille de l'entreprise,
- Niveau de sécurité nécessaire,
- Type d'activité,
- Niveau de compétence d'administration disponible,
- Volume du trafic sur le réseau,
- Besoins des utilisateurs du réseau,
- Budget alloué au fonctionnement du réseau (pas seulement l'achat mais aussi l'entretien et la maintenance).

4.1 Mode Client/Serveur :

Présentation :

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services.

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client (client FTP, client de messagerie, etc.) lorsque l'on désigne un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès d'un serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client de messagerie il s'agit de courrier électronique).

Un système client/serveur fonctionne selon le schéma suivant :

- Le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur.
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port.

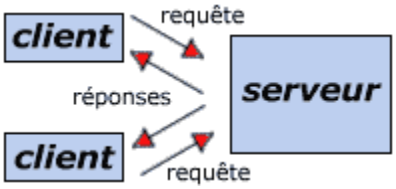


Figure 8: Système Client/Serveur

Avantages :

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- **Des ressources centralisées** : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction
- **Une meilleure sécurité** : car le nombre de points d'entrée permettant l'accès aux données est moins important.
- **Une administration au niveau serveur** : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.

- **Un réseau évolutif** : grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure.

Inconvénients :

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- Un coût élevé dû à la technicité du serveur.
- Un maillon faible : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID)

Architecture à plusieurs niveaux :

L'architecture à deux niveaux (aussi appelée architecture 2-tier) caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service.

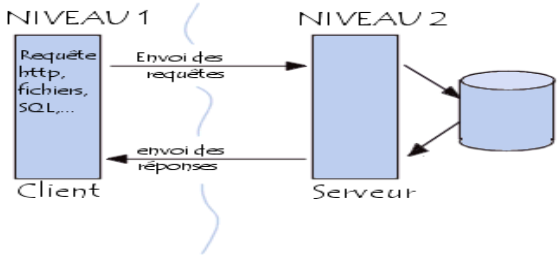


Figure 9: Architecture 2-tier

L'architecture à 3 niveaux (appelée architecture 3-tier), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre : un client (l'ordinateur demandeur de ressources), le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur et le serveur de données, fournissant au serveur d'application les données dont il a besoin. Il peut y avoir plusieurs serveurs de données :

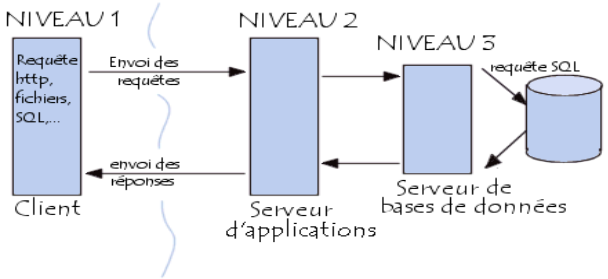


Figure 10: Architecture 3-tier

4.2 Mode poste à poste (Peer to Peer) :

Présentation:

Contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela signifie notamment que chacun des ordinateurs du réseau est libre de partager ses ressources.
Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés.
Tous les systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.
Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, cartes fax etc.)
Pour les connexions, on utilise un système de câblage simple et apparent. Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :

- ✓ Moins de 10-30 utilisateurs.
- ✓ Tous les utilisateurs sont situés dans une même zone géographique.
- ✓ La sécurité n'est pas un problème crucial.
- ✓ Ni l'entreprise ni le réseau ne sont susceptibles d'évoluer de manière significative dans un proche avenir.

Avantages:

- Un coût réduit (pas de matériel évolué et donc cher, pas de frais d'administration)
- Une grande simplicité (la gestion et la mise en place du réseau et des machines sont peu compliquées)

Note: L' « administration » d'un réseau ou de machines désigne :

- ✓ Gestion des utilisateurs et de la sécurité
- ✓ Mise à disposition des ressources
- ✓ Maintenance des applications et des données
- ✓ Installation et mise à niveau des logiciels utilisateurs

Inconvénients:

- Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer ;
- La sécurité est moins facile à assurer, compte tenu des échanges transversaux ;

- Aucun maillon du système ne peut être considéré comme fiable.

Ainsi, les réseaux d'égal à égal sont préférentiellement utilisés pour des applications ne nécessitant pas un haut niveau de sécurité ni une disponibilité maximale (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

5. Typologies et topologies des réseaux :

5.1 Typologies des réseaux :

On distingue différents types de réseaux (privés) selon leur taille (en terme de nombre de machine), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. Il existe généralement quatre catégories de réseaux :

- PAN (Private Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

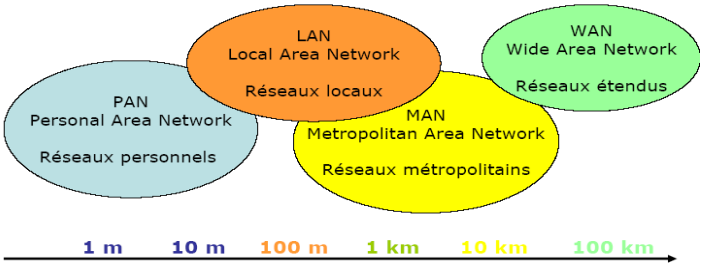


Figure 11: Classification des réseaux informatiques selon leur taille

5.1.1 Réseaux personnels PAN (Personnel Area Network) :

Un réseau personnel PAN (Personnal Area Network) s'étend sur quelque mètre et interconnecte (souvent par des liaisons sans fil) des équipements personnels comme un ordinateur portable, un agenda électronique...

5.1.2 Réseaux locaux LAN (Local Area Network)

Un réseau local LAN (Local Area Network) est un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique (quelques mètres à quelques kilomètres) par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet). La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10

Mbps (pour un réseau ethernet par exemple) et 1 Gbps (Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

5.1.3 Réseaux métropolitains MAN (Metropolitan Area Network)

Un réseau métropolitain MAN (Metropolitan Area Network) interconnecte plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

5.1.4 Réseaux distant WAN (Wide Area Network)

Ce type de réseau permet l'interconnexion de réseaux locaux et métropolitains à l'échelle de la planète, d'un pays, d'une région ou d'une ville. L'infrastructure est en général publique (Télécom par exemple) et l'utilisation est facturée en fonction du trafic et/ou en fonction de la bande passante réservée, pour les lignes louées (une ligne louée est réservée exclusivement au locataire, 24h sur 24, pour la durée du contrat).

Les modems sont un des éléments de base des WANs et la bande passante va de quelques kbits/s à quelques Mbit/s. Une valeur typique pour une ligne louée est de 64kbits/s (en fonction des services offerts).

5.2 Topologies des réseaux :

La topologie d'un réseau décrit la façon dont sont interconnectés les nœuds et les terminaux des utilisateurs. On distingue trois topologies, l'étoile, le bus et l'anneau, qui peuvent être combinées pour obtenir des topologies hybrides.

On distingue la topologie physique (la configuration spatiale, visible, du réseau) de la topologie logique. La topologie logique représente la façon de laquelle les données transitent dans les câbles : topologie en anneau, topologie point à point et topologie à accès multiple.

5.2.1 Topologie en étoile

Dans cette architecture, qui fut la première créée, chaque station est reliée à un nœud central.

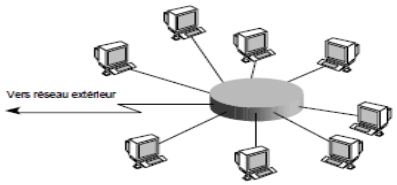


Figure 12: La topologie en étoile

Cette topologie présente les avantages suivants :

- Une étoile peut jouer le rôle d'un bus ou d'un anneau.
- Beaucoup moins vulnérables que les autres topologies car on peut aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau.
- Le fait que le logiciel soit centralisé présente néanmoins des avantages certains en matière de gestion du système, plus simple, et de coût, réparti entre les différents utilisateurs connectés.

Et elle présente toutefois les inconvénients suivants :

- Un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).
- Du fait de sa centralisation, la structure en étoile peut toutefois présenter une certaine fragilité.
- De plus, elle manque de souplesse, puisqu'il faut une liaison supplémentaire pour toute station rajoutée et que les extensions du réseau sont limitées par la capacité du nœud central. L'ensemble des prises et des câbles doit donc être prévu à l'origine de façon à ne pas avoir à entreprendre de travaux d'infrastructure, souvent coûteux.

5.2.2 Topologie en bus :

Sur un réseau en bus, les ordinateurs sont reliés par un câble interrompu. Un seul ordinateur peut transférer des informations à un instant donné. Lorsqu'un ordinateur envoie des informations, elles parcourent tout le câble dans les deux sens. L'ordinateur de destination doit ensuite récupérer les informations à partir du câble. Un bouchon de terminaison est un dispositif qui permet d'absorber les signaux transmit. Chaque extrémité du câble doit posséder un bouchon de terminaison.

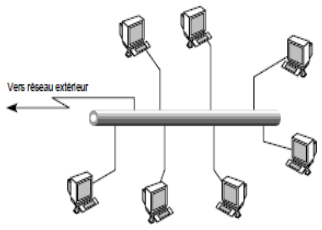


Figure 13: La topologie en bus

Cette topologie a pour avantages sa simplicité de mise en œuvre 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 sera affecté.

Une extension de la topologie en bus est la topologie en arbre, comme illustré à la figure14. Dans une structure en arbre, les équipements terminaux sont connectés sur des hubs qui sont reliés les uns aux autres jusqu'au hub racine.

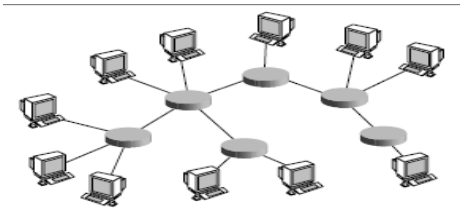


Figure 14: La topologie en arbre

5.2.3 Topologie en anneau :

Sur un réseau structuré en anneau, les ordinateurs sont disposés en anneau et reliés les uns aux autres par un câble circulaire interrompu. Les informations circulent dans un seul sens. Lorsqu'un ordinateur transfert une information, il envoie tout d'abord à l'ordinateur successeur au sein de l'anneau. Lorsque l'ordinateur reçoit des informations qui ne lui sont pas destiné, il les fait suivre automatiquement à l'ordinateur successeur. Les ordinateurs de l'anneau continuent à faire suivre les informations jusqu'à ce qu'elles parviennent à l'ordinateur destinataire.

Les réseaux en anneau utilisent des techniques de jeton, par lesquelles seul le coupleur qui possède le jeton a le droit de transmettre ; le jeton peut être une suite de bits ou parfois un seul bit. Pour qu'un coupleur capte le jeton au passage, il doit être capable de l'identifier et de l'arrêter. La médiocre fiabilité de ce type d'architecture lui a valu de nombreuses critiques, la rupture de l'anneau ou la défection d'un nœud actif paralysant le trafic du réseau. Divers mécanismes permettent de remédier à ce défaut. On peut notamment sécuriser la couche physique par redondance en doublant le support et les organes critiques et en utilisant des relais pour court-circuiter les nœuds défaillants.

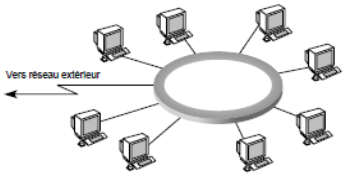


Figure 15: La topologie en anneau

.

Le tableau suivant résume les avantages et les inconvénients de chacune des topologies déjà vues :

Topologie	Avantages	Inconvénients
Bus	Economise la longueur de câble. Simple et facile à étendre	Ralentissement possible du réseau lorsque le trafic est important. Problèmes difficiles à isoler. La coupure du câble peut affecter de nombreuses stations.
Anneau	Accès égal pour tous les ordinateurs. Performances régulières même si les utilisateurs sont nombreux.	La panne d'un seul ordinateur peut affecter le reste du réseau. Problèmes difficiles à isoler.
Etoile	Il est facile d'ajouter de nouveaux ordinateurs et de procéder à des modifications. Contrôle et administration centralisés. La panne d'un seul ordinateur n'a pas d'incidence sur le reste du réseau	Si le point central tombe en panne, le réseau est mis hors service

NORMALISATION ET MODELES EN COUCHE

Plan du chapitre :

1. Introduction
2. Besoins de normalisation
3. Notion de modèle en couche
4. Le modèle OSI
5. Le modèle TCP/IP

Objectifs du chapitre :

- Montrer les besoins de normalisation pour les réseaux.
- Présenter les avantages d'un modèle en couche.
- Présenter le modèle OSI.
- Présenter le modèle TCP/IP.
- Comparer les deux modèles OSI et TCP/IP.

1. Introduction :

Au cours des dernières décennies, le nombre et la taille des réseaux ont augmenté considérablement. Cependant, bon nombre de réseaux ont été mis sur pied à l'aide de plates-formes matérielles et logicielles différentes. Il en a résulté une incompatibilité entre de nombreux réseaux et il est devenu difficile d'établir des communications entre des réseaux fondés sur des spécifications différentes. Pour ce raisons, il devient nécessaire de définir un modèle de communication ou architecture protocolaire réseau.

Historiquement, chaque grand constructeur avait définit la sienne : SNA(System Network Architecture) pour IBM , DSA(Distributed System Architecture) pour BULL… Ces architectures propriétaire incompatible entre elles ne permettaient pas l'interopérabilité des systèmes. D'où la nécessité de définir une architecture de communication normalisée. La normalisation désigne le procédé de standardisation d'un système. C'est l'activité qui a pour objet d'établir des documents de référence : les normes.

2. Besoins de normalisations :

Les normes établies par les organismes internationaux (et particulièrement américains) de normalisation ont contribué à :

- L'ouverture des architectures propriétaires.
- La convergence des efforts des petites sociétés.
- L'expansion de la micro-informatique dans le monde.
- …

Les besoins croissants des entreprises en matière d'interactivité, de partage de données, et de portage des applications dans différents environnements ont accéléré le développement des normes pour les réseaux. En général, les normes sont des spécifications techniques qui imposent certaines contraintes de fabrication aux constructeurs. Les fabricants adhèrent volontairement à ces directives, à ces recommandations, parce qu'elles leur assurent une large part de marché. Aujourd'hui, la conformité aux normes est presque un impératif. Les normes correspondent à la publication d'une certaine technologie par des organismes de normalisation.

Les principaux organismes de normalisation sont :

- **ISO (Organisation internationale de normalisation, International Organization for Standardization)**, c'est une organisation internationale qui regroupe les instituts nationaux de normalisation de plus de cent pays : AFNOR pour la France, BSI pour la

Grande-Bretagne, ANSI pour les Etats-Unis, DIN pour la République fédérale d'Allemagne, etc. Les travaux de l'ISO concernent tous les domaines industriels, à l'exception de l'électronique et de l'électricité qui sont du ressort de la Commission électrotechnique internationale(CEI). Pour l'informatique et les télécommunications, l'ISO et la CEI ont formé un Comité technique commun (ISO-IEC).

- **IUT-T (International Union of Telecommunication - section Télécommunication)** (qui a remplacé le CCITT : Comité Consultatif Internationnal Télégraphique et Téléphonique en 1993) est chargée par l'ONU des normes qui portent le nom de «recommandations », dans le domaine des télécommunications.
- **IEEE (Institute of Electrical and Electronic Engineers)** regroupe de nombreux chercheurs et ingénieurs en électronique et informatique.

3. Notion de modèle en couche :

3.1 Notion de couches :

Connecter en transparence des équipements provenant de constructeurs différents pour qu'ils s'échangent des informations nécessite que ceux-ci utilisent non seulement des techniques de connexion compatibles (raccordement , niveau électrique…), mais aussi des protocoles d'échange identiques et une sémantique de l'information compréhensible par les partenaires de la communication. Ces problèmes, de nature différente, peuvent être résolus chacun par une solution spécifique. Afin d'éviter une description trop complexe, le système a été découpé en entités fonctionnelles appelées couches. Une couche est donc un ensemble homogène destiné à accomplir une tâche ou à rendre un service. L'ensemble des couches mises en œuvre dans un système de communication constitue l'architecture protocolaire du système.

3.2 Avantages d'un modèle en couche :

Le but d'un système en couches est de séparer le problème en différentes parties (les couches) selon leurs niveaux d'abstraction. L'utilisation d'un modèle en couches présente certains avantages pour décrire des protocoles et des opérations sur un réseau. L'utilisation d'un modèle en couches :

- Encourage la concurrence, car les produits de différents fournisseurs peuvent fonctionner ensemble ; permet d'éviter que des changements technologiques ou fonctionnels dans une couche ne se répercutent sur d'autres couches, supérieures et inférieures ;
- Fournit un langage commun pour décrire des fonctions et des fonctionnalités réseau.

- L'approche en couche garantit une évolutivité facile du système : La prise en compte d'une nouvelle technologie ne remet en cause que la couche concernée.

3.3 Concepts de base pour les modèles d'architecture protocolaire :

Principe de fonctionnement:

Considérons le modèle simplifié à trois couches représenté dans la figure suivante. Pour communiquer l'application cliente remet à la couche supérieure ; ici la couche 3, des données à destination de l'application serveur, des instructions décrivant le service attendu et celles nécessaires à l'acheminement des données vers l'application serveur. La couche 3 interprète les instructions reçues et confectionne une structure de donnée à destination de la couche 3 distante, dite couche homologue. Cette structure de donnée est constituée d'une part des informations nécessaires à la couche 3 distante pour traiter ces données appelées en-tête de niveau 3(H3 pour Header de niveau 3) et des données elles-mêmes ; l'ensemble formant une unité de donnée de niveau N. les règles d'échange entre des données de même niveau constituent un protocole de niveau N.

Puis, la couche 3 remet cette unité de données et des instructions (I3) à la couche inférieure qui procède de même… enfin les données sont émises sur le support physique. En réception la couche la plus basse extrait l'en-tête protocolaire (H1), l'interprète, et remet les données à la couche supérieure qui procède de même jusqu'à remise des données à l'application distante.

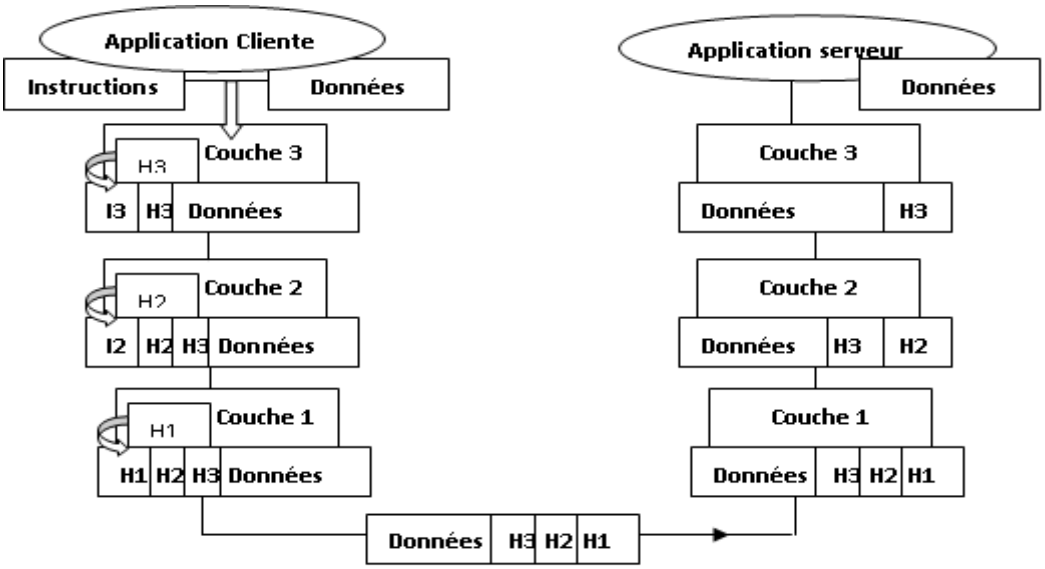


Figure 16: Principe de fonctionnement d'un modèle en couches

Terminologie

- ***Couche :*** Une couche correspond à un ensemble de **fonctions** ou de processus cohérents entre eux et assurant une **fonction précise globale.** Deux couches adjacentes sont indépendantes dans leurs fonctions mais elles s'interconnectent par ce qu'on appelle une **interface**. Chaque couche est caractérisée par un ensemble de fonctions et de messages de contrôle associés. Les messages de contrôle sont appelés Unités de Données de Protocole **PDU**.
- ***Protocole et service***

L'échange précédent, décrit deux types de dialogue :

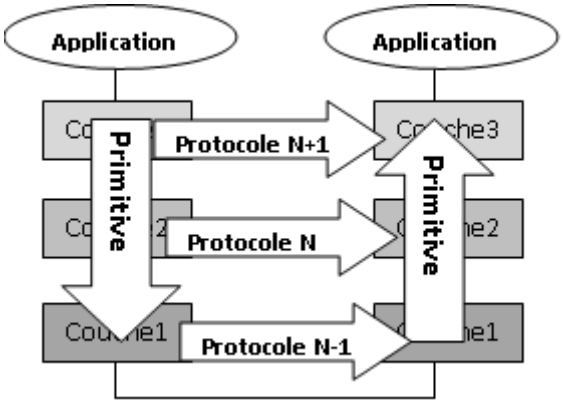


Figure 17: Les protocoles et les primitives de service

Protocole

Le protocole est défini comme l'ensemble des fonctions que la couche exécute avec l'aide d'autres entités, par le biais de l'échange des PDU. La spécification du protocole d'une couche définit de manière très précise les fonctions que la couche peut assurer, ainsi que les formats des paramètres des PDU associés.

Service

- ✓ Un service est un ensemble de primitives qu'une couche fournit à la couche supérieure.
- ✓ Les services d'une couche N sont accessibles par ce qu'on appelle des **points d'accès aux services**, ou **SAP** (Service Access Point).

- ***Entité :*** Une entité dans une couche **exécute** les fonctions de la couche dans un système.
  - ✓ Une entité constitue élément actif d'une couche.
  - ✓ Les entités de la même couche situées sur différentes machines sont appelées entités paires ou homologues.

- ✓ Dans une communication, les entités paires de la couche N communiquent entre elles en suivant un protocole de niveau N.

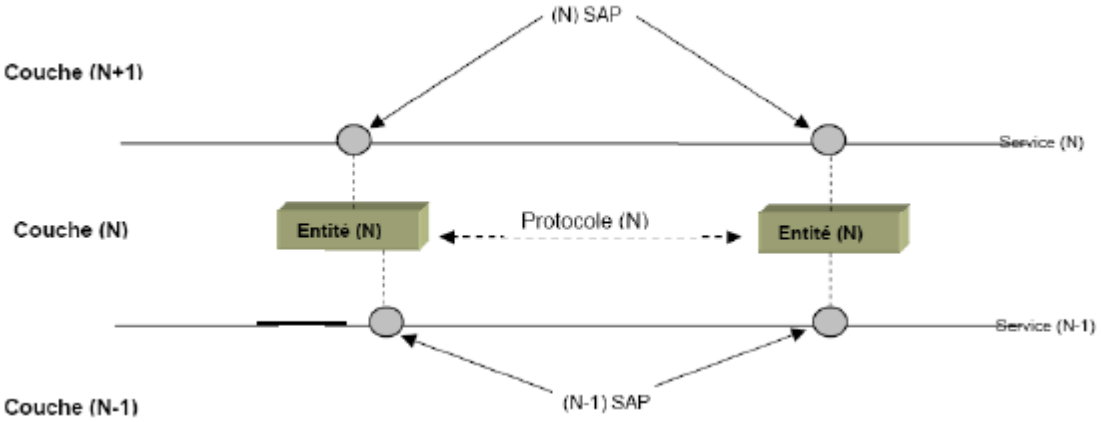


Figure 18: Dialogue entre deux entités homologues

L'encapsulation des données

En remettant les données à la couche n, la couche N+1 requiert, à l'aide d'une primitive de service de niveau N, les services de niveau N.peu importe à N+1 de savoir comment ces services sont rendus. L'unité de données protocolaire de niveau (N+1), données et en-tête, est transportée dans une unité de donnée de niveau N (protocole N). Les données de niveau (N+1) sont dites encapsulées dans le protocole N, on parle aussi de tunnel de niveau N.

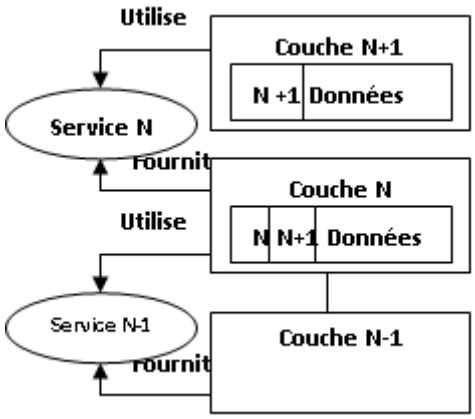


Figure 19: L'encapsulation de données

4 Le modèle OSI :

4.1 Présentation du modèle OSI :

Le modèle de référence OSI (Open System Interconnexion - interconnexion de systèmes ouverts), diffusé en 1984, a apporté aux fournisseurs un ensemble de normes assurant une compatibilité et une interopérabilité accrues entre les divers types de technologies de réseau produites par de nombreuses entreprises partout dans le monde.

Le modèle de référence OSI est le principal modèle des communications en réseau. Bien qu'il existe d'autres modèles, la majorité des fournisseurs de réseaux relient aujourd'hui leurs produits à ce modèle de référence.

Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau précise. Cette répartition des fonctions réseau est appelée organisation en couches.

4.2 Les 7 couches du modèle OSI :

Le problème consistant à déplacer de l'information entre des ordinateurs est divisé en sept problèmes plus petits et plus faciles à gérer dans le modèle de référence OSI. Chacun des sept petits problèmes est représenté par une couche particulière du modèle. Voici les sept couches du modèle de référence OSI :

- **Couche7 :** la couche application
- **Couche 6 :** la couche de présentation
- **Couche 5 :** la couche session
- **Couche 4 :** la couche de transport
- **Couche 3 :** la couche réseau
- **Couche 2 :** la couche liaison de données
- **Couche 1 :** la couche physique

Chaque couche du modèle OSI doit exécuter une série de fonctions pour que les paquets de données puissent circuler d'un ordinateur source à un ordinateur de destination sur un réseau :

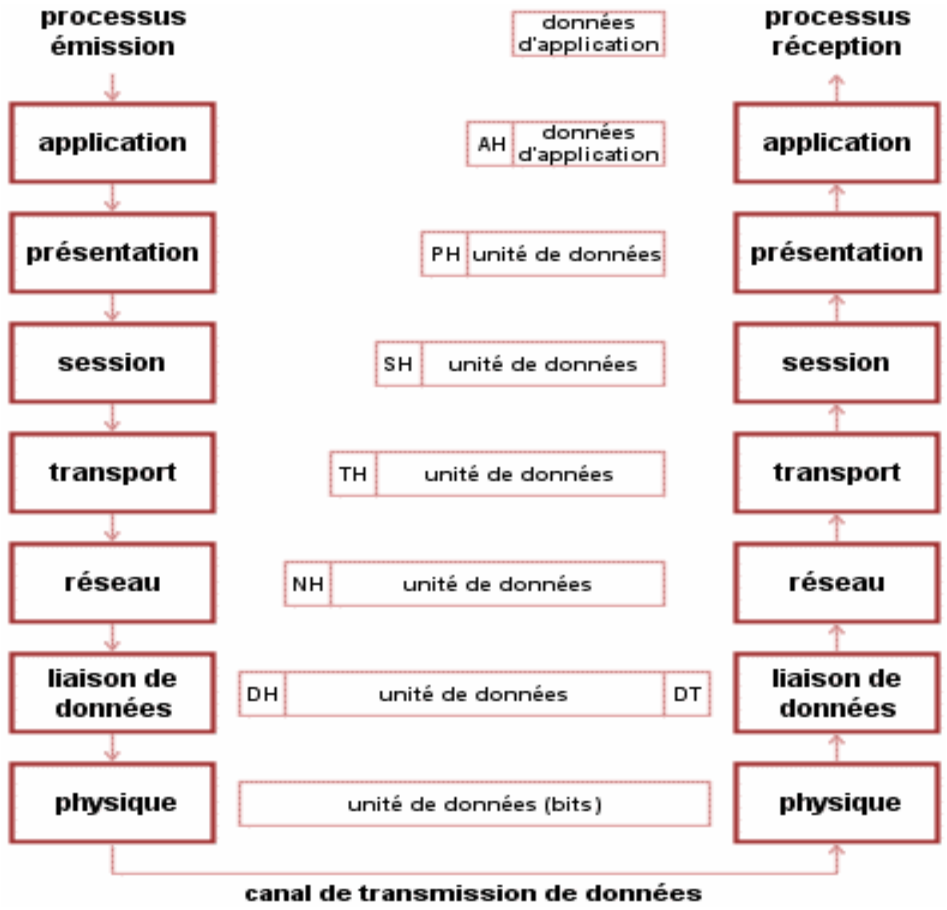
Couches	***Fonctions***
NIVEAU 1 ***Couche PHYSIQUE*** ***Physical Layer***	Elle assure un transfert de bits sur le canal physique (support). A cet effet, elle définit les supports et les moyens d'y accéder : spécifications mécaniques (connecteur), spécifications électriques (niveau de tension), spécifications fonctionnelles des

	éléments de raccordement nécessaires à l'établissement, au maintien et à la libération de la ligne.
NIVEAU 2 ***Couche LIAISON DE DONNEE*** ***Data link Layer***	Elle assure un transit fiable des données sur une liaison physique. Ainsi, la couche liaison de données s'occupe de l'adressage physique (adresse MAC), de la topologie du réseau, de l'accès au réseau, de la notification des erreurs (contrôle d'erreurs), de la livraison ordonnée des trames et du contrôle de flux (CSMA/CD :Carrier Sense with Multiple Access / Collision Detection).
NIVEAU 3 ***Couche RESEAU*** ***Ntework Layer***	La couche réseau est une couche complexe qui gère le routage. Elle assure la connectivité et la sélection du trajet entre deux systèmes hôte pouvant être situés sur des réseaux géographiquement éloignés. Cette couche travaille avec les adresses logiques (adresses IP) et le masque de réseau.
NIVEAU 4 ***Couche TRANSPORT*** ***Transport Layer***	La couche transport segmente les données au niveau de l'hôte émetteur et les rassemble en flot de données à l'hôte récepteur. Elle tente de fournir un service de transport des données qui protège les couches supérieures des détails d'implantation du transport. En fournissant un service de communication de bout en bout, la couche transport établit et raccorde les circuits virtuels, en plus d'en assurer la maintenance. Elle s'assure que les données sont échangées de manière fiable dans le bon ordre sans perte ni duplication. Elle fait appel à des contrôles de détection des erreurs de transport, de reprise sur incident et de flux d'information.
NIVEAU 5 ***Couche SESSION*** ***Session Layer***	Comme son nom l'indique, la couche session ouvre, gère et ferme les sessions entre deux systèmes hôtes en communication. Elle synchronise également le dialogue entre les couches présentation des deux hôtes et gère l'échange des données.
NIVEAU 6 ***Couche***	La couche présentation gère le format de la représentation des données. Elle s'assure que l'information envoyée par la couche application d'un système est lisible par la couche application d'un autre système. Au besoin, la couche présentation traduit

PRESENTATION ***Presentation Layer***	différents formats de représentation des données en utilisant un format commun. La couche présentation est également concernée par d'autres aspects de représentation de l'information (compression, cryptographie,…)
NIVEAU 7 ***Couche APPLICATION*** ***Application Layer***	La couche application est la couche OSI la plus près de l'utilisateur; elle fournit des services réseau aux applications de l'utilisateur par exemple, POP3, SMTP, FTP, Tel net et HTTP. Voici des exemples de ce type d'application : tableurs, traitement de texte et logiciels de terminaux bancaires.

4.3 Unité de données de protocole et encapsulation :

Lorsque les données d'application descendent la pile de protocoles en vue de leur transmission sur le support réseau, différents protocoles ajoutent des informations à chaque niveau. Il s'agit du processus d'encapsulation :



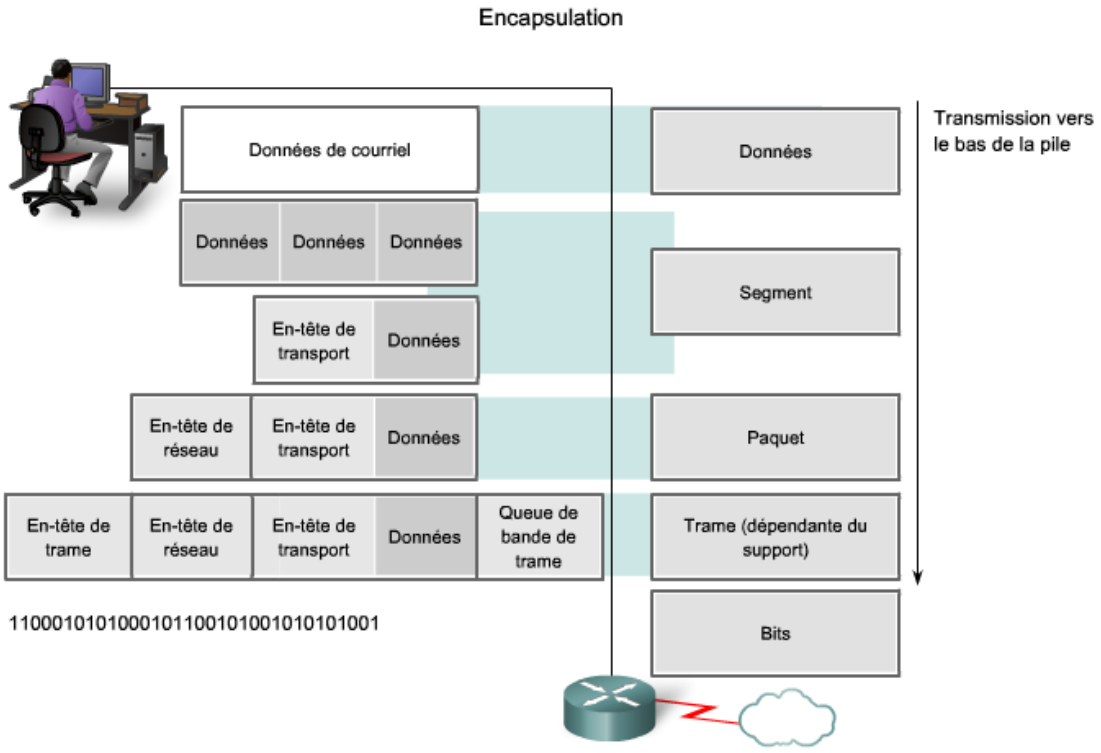


Figure 20: Processus d'encapsulation

Les réseaux doivent effectuer les cinq étapes de conversion ci-dessous afin d'encapsuler les données:

1. Construction des données – Lorsqu'un utilisateur envoie un message électronique, les caractères alphanumériques qu'il contient sont convertis en données pouvant circuler dans l'inter réseau.

2. Préparation des données pour le transport de bout en bout – Les données sont préparées pour le transport inter réseau. En utilisant des segments, la fonction de transport s'assure que les systèmes hôtes situés à chaque extrémité du système de messagerie peuvent communiquer de façon fiable.

3. Ajout de l'adresse IP du réseau à l'en-tête – Les données sont organisées en paquets, ou datagrammes, contenant un en-tête de paquet constitué des adresses logiques d'origine et de destination. Ces adresses aident les unités réseau à acheminer les paquets dans le réseau suivant un chemin déterminé.

4. Ajout de l'en-tête et de l'en-queue de la couche de liaison de données – Chaque unité réseau doit placer le paquet dans une trame. La trame permet d'établir la connexion avec la prochaine unité réseau directement connectée dans la liaison.

5. Conversion en bits pour la transmission – La trame doit être convertie en une série de uns et de zéros (bits) pour la transmission sur le média. Une fonction de synchronisation permet aux unités de distinguer ces bits lorsqu'ils circulent sur le média. Tout au long du trajet suivi dans l'inter réseau physique, le média peut varier.

La forme qu'emprunte une donnée sur n'importe quelle couche est appelée unité de données de protocole. À chaque étape du processus, une unité de données de protocole possède un nom différent qui reflète sa nouvelle apparence :

• **Données ou message** : terme générique pour l'unité de données de protocole utilisée à la couche application.

• **Segment** : unité de données de protocole de la couche transport.

• **Paquet** : unité de données de protocole de la couche réseau.

• **Trame** : unité de données de protocole de la liaison de données.

• **Bits** : unité de données de protocole utilisée lors de la transmission physique de données à travers le support.

5 Le modèle TCP/IP:

5.1 Présentation du modèle TCP/IP:

Le premier modèle de protocole en couches pour les communications inter réseau fut créé au début des années 70 et est appelé modèle Internet. Il définit quatre catégories de fonctions qui doivent s'exécuter pour que les communications réussissent. L'architecture de la suite de protocoles TCP/IP suit la structure de ce modèle. Pour cette raison, le modèle Internet est généralement appelé modèle TCP/IP.

TCP/IP désigne une architecture réseau en 4 couches. C'est en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol).

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

5.2 Présentation des couches et leurs rôles :

Le modèle TCP/IP **(*Transmission Control Protocol / Internet Protocol)*** est une architecture conçue dans le but de faire communiquer plusieurs machines différentes et incompatibles : hétérogènes.

L'architecture TCP/IP, comme le modèle OSI, est un modèle en couches. Il offre, néanmoins, quatre couches : Application, transport, Internet et accès réseaux

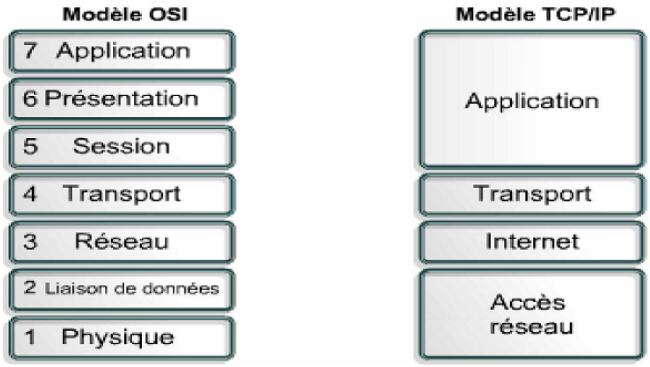


Figure 21: Modèle TCP/IP par rapport au modèle OSI

Les rôles des différentes couches sont les suivants:

- **La couche application**

La couche Application fournit les fonctionnalités et les moyens nécessaires pour accéder aux autres couches, et elle définit les protocoles pour que des applications échangent les données. Il existe plusieurs protocoles et les plus répandus sont les suivants :

- ✓ ***Le protocole HTTP (Hypertext Transport Protocol):*** ce protocole représente en quelque sorte le langage que les clients et les serveurs Web utilisent pour communiquer.
- ✓ ***Le protocole FTP (File Transfer Protocol):*** ce protocole est un service fiable pour transférer des fichiers. Il gère les transferts bidirectionnels des fichiers binaires et ASCII.
- ✓ ***Le protocole TFTP (Trivial File Transfer Protocol):*** ce protocole est utilisé pour transférer des fichiers de configuration. Il est utile dans certains LAN, car il s'exécute plus rapidement que le protocole FTP dans un environnement stable.
- ✓ ***Le protocole NFS (Network File System):*** ce protocole est un ensemble de protocoles pour systèmes de fichiers distribués, développé par Sun Microsystems, permettant un accès aux fichiers d'un équipement de stockage distant, tel qu'un disque dur, dans un réseau.
- ✓ ***Le protocole SMTP (Simple Mail Transfer Protocol):*** ce protocole régit la transmission du courrier électronique sur le réseau Internet. Il ne permet pas de transmettre des données autres que du texte en clair.

- ✓ ***Telnet:*** ce protocole permet d'accéder à distance à un autre ordinateur. Cela permet à un utilisateur d'ouvrir une session sur un hôte Internet et d'exécuter diverses commandes. Un client Telnet est qualifié d'hôte local. Un serveur Telnet est qualifié d'hôte distant.
- ✓ ***Le protocole SNMP (Simple Network Management Protocol):*** ce protocole permet de surveiller et de contrôler les équipements du réseau, ainsi que de gérer les configurations, les statistiques, les performances et la sécurité.
- ✓ ***Le protocole DNS (Domain Name System):*** ce protocole est utilisé par Internet pour convertir en adresses IP les noms de domaine et leurs nœuds de réseau annoncés publiquement.

- **La couche transport**

La couche transport présente deux protocoles de transport à savoir TCP qui est un protocole fiable fonctionnant en mode connecté et le protocole UDP, non fiable, fonctionnant en mode connecté. TCP permet de rectifier les erreurs du réseau (IP) à savoir la détection des erreurs, la retransmission sur perte de paquets, le contrôle de flux, le séquencement, etc.

- **La couche Internet**

Cette couche a pour fonction l'adressage des paquets et le routage. Les protocoles de cette couche sont les suivants :

- ✓ ***IP (Internet Protocol) :*** protocole responsable d'adressage, fragmentation et réassemblage des paquets.
- ✓ ***ARP (Address Resolution Protocol) :*** protocole chargé de la résolution de l'adresse de couche Internet en adresse physique.
- ✓ ***ICMP (Internet Control Message Protocol) :*** protocole de « gestion » de réseau. Son rôle est d'exécuter les fonctions de diagnostic et d'établir un rapport d'erreurs suite à la transmission des paquets IP.
- ✓ ***IGMP (Internet Group Management Protocol) :*** responsable de la gestion des groupes IP multicast ou multipoint.

- **Couche interface réseau (ou accès réseau)**

La couche interface réseau permet à un paquet IP d'établir une liaison physique avec un média réseau. Cela comprend les détails sur les technologies LAN et WAN, ainsi que toutes les informations contenues dans les couches physiques et liaison de données du modèle OSI. Les pilotes d'application, les cartes modem et les autres équipements s'exécutent au niveau de la

couche d'accès au réseau. Cette dernière définit les procédures utilisées pour communiquer avec le matériel réseau et accéder au média de transmission.

5.3 Comparaison des modèles OSI et TCP/IP :

En comparant le modèle OSI au modèle TCP/IP, on remarque des similitudes et des différences.

Les similitudes sont les suivantes:

• Tous deux comportent une couche application, bien que chacune fournisse des services très différents.

• Tous deux comportent des couches réseau et transport comparables.

• Les professionnels des réseaux doivent connaître ces deux modèles.

• Tous deux supposent que les paquets sont commutés. Cela signifie que chaque paquet peut prendre des chemins différents pour atteindre une même destination. Cela est différent des réseaux à commutation de circuits, où tous les paquets prennent le même chemin.

Les différences sont les suivantes:

• TCP/IP intègre la couche application, la couche présentation et la couche session dans sa couche application.

• TCP/IP regroupe la couche physique et la couche liaison de données du modèle OSI dans la couche d'accès réseau.

• TCP/IP paraît plus simple, car il comporte moins de couches.

• Les protocoles TCP/IP constituent la norme sur laquelle s'est développé Internet. Aussi, le modèle TCP/IP a bâti sa réputation sur ses protocoles. En revanche, les réseaux ne sont généralement pas architecturés autour du protocole OSI, même si le modèle OSI puisse être utilisé comme guide.

Les protocoles qui constituent la suite de protocoles TCP/IP peuvent être décrits selon les termes du modèle de référence OSI.

Chapitre 3

ADRESSAGE IP (COUCHE RESEAU)

Plan du chapitre :

1. Principe de l'adressage IP
2. Les techniques d'adressage dans un réseau IP

Objectifs du chapitre :

- Comprendre la notion d'adressage IP.
- Connaitre les classes d'adressage IP.
- Maitriser le découpage en sous réseaux.

1. Principe de l'adressage IP :

Chaque machine (Hôte, *Host*), raccordée au réseau logique IP, est indépendamment de l'adressage physique identifiée par un identifiant logique dénommé **adresse IP**. Pour assurer l'acheminement des données dans le réseau, il est nécessaire de définir des mécanismes de mise en relation de l'adresse logique seule connue des applications avec l'adresse physique correspondante.

Le protocole IP doit assurer le routage dans le réseau logique IP. A cet effet, il doit pouvoir identifier le réseau logique IP (Net_ID) et dans ce réseau la machine cible (Host_ID).

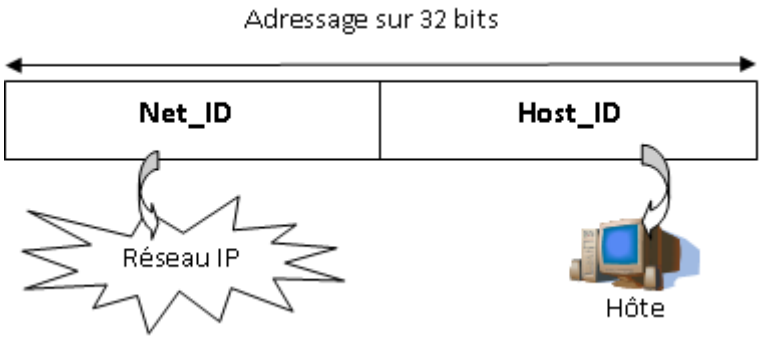


Figure 22: L'adressage IP

Un hôte est tout ce qui peut envoyer ou recevoir des trames IP sur le réseau, comme une station de travail ou un routeur. L'adresse IP de n'importe quel hôte est le rassemblement de deux choses : l'adresse du réseau où il se trouve et son adresse personnelle sur ce réseau.

Une adresse IP est une suite de 32 bits sous forme de 4 octets séparés par des points. On peut représenter une adresse IP de deux manières :

- Représentation binaire : une suite de 32 bits chaque 8 bits séparés par un point.
- Représentation décimale : cette représentation est plus simple et elle permet d'éviter un grand nombre d'erreurs de transposition liées à l'utilisation des nombres binaires et en plus on peut discerner plus facilement les relations entre les chiffres avec ce type de notation.

Application :

- ✓ Donner la représentation binaire correspondante à l'adresse : 192.168.1.8.
- ✓ Comparer entre 192.168.1.8 et 192.168.1.9 en binaire et en décimale.

Notes :

- ✓ Une adresse valide est dans la plage allant de 0.0.0.0 à 255.255.255.255, un total de 4.3 milliards d'adresses.
- ✓ Le nombre de bits dans une adresse IP réservé pour le réseau et celui pour l'hôte dépend selon le type du réseau.

2. Les techniques d'adressage dans un réseau IP:

2.1 Les classes d'adressages :

Afin d'assurer une meilleure utilisation de l'espace d'adressage et d'adapter celui-ci à la taille et au besoin de chaque organisation, il a été introduit une modularité dans la représentation des octets entre l'identifiant réseau (*Net_ID*) et l'identifiant machine (*Host_ID*). Ainsi, 5 classes d'adresses ont été définies. Les premiers bits du champ adresse réseau permettent de distinguer la classe d'adressage :

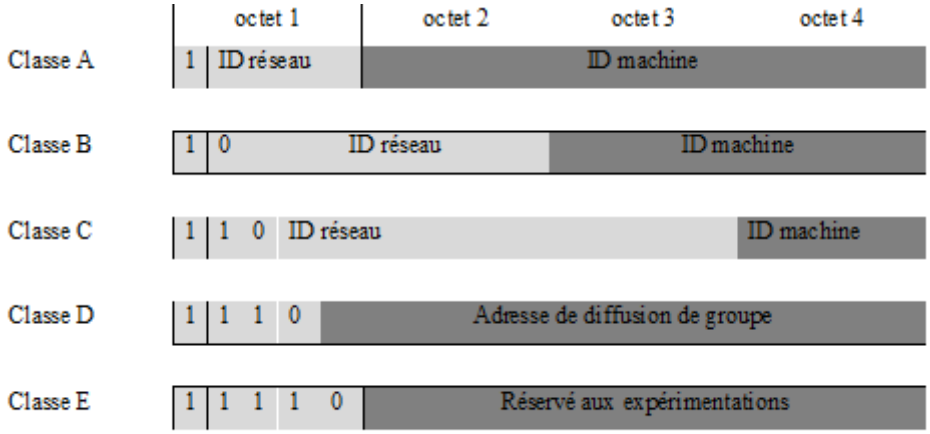


Figure 23: Les classes d'adresses IP

- ➢ **Classe A :**

L'adresse de classe A est réservée aux réseaux de très grande taille. Les adresses IP de classe A utilisent uniquement le premier octet pour indiquer l'adresse réseau. Les trois octets suivants sont utilisés pour définir les adresses hôte.

Les adresses de cette classe s'étendent de 1.0.0.1 à 126.255.255.254. Elles permettent d'adresser 126 réseaux (les valeurs 0 et 127 sont réservées) (2^7-2) et plus de 16 millions de machines (2^{24}-2) (Host_ID 0 et 255 ont une signification spécifique).

- **Classe B :**

L'adresse de classe B est réservée aux réseaux de taille moyenne ou grande. Les adresses IP de classe B utilisent les deux premiers octets (sur quatre) pour indiquer l'adresse réseau. Les deux octets suivants sont utilisés pour les adresses hôte.

Les deux premiers bits du premier octet d'une adresse de classe B sont toujours 10. Les adresses s'étendent alors de 128.0.0.1 à 191.255.255.254 ce qui correspond à 16384 réseaux de 65534 machines. Cette classe est la plus utilisée et les adresses sont pratiquement épuisées.

- **Classe C :**

Cet espace d'adressage est réservé aux réseaux de petite taille (254 hôtes maximum). Une adresse de classe C commence par la valeur binaire **110**. Par conséquent, le nombre le plus faible pouvant être représenté est 11000000 (192 en décimal) et le plus élevé est 11011111 (223 en décimal). Toute adresse contenant un nombre compris entre 192 et 223 dans le premier octet est une adresse de classe C.

- **Classe D :**

L'adresse de classe D est réservée à la diffusion multicast d'une adresse IP. Une adresse de multicast est une adresse réseau unique qui achemine les paquets associés à une adresse de destination vers des groupes prédéfinis d'adresses IP. Ainsi, une station peut transmettre simultanément un même flux de données vers plusieurs destinataires.

Les quatre premiers bits d'une adresse de classe D doivent correspondre à **1110**. Par conséquent, le premier octet d'une adresse de classe D est compris entre 11100000 et 11101111 (soit 224 et 239 en décimal). Toute adresse IP commençant par une valeur comprise entre 224 et 239 dans le premier octet est une adresse de classe D.

- **Classe E :**

Le groupe IETF (Internet Engineering Task Force) utilise ces adresses à des fins expérimentales. Aucune adresse de classe E n'est disponible sur Internet. Les quatre premiers bits d'une adresse de classe E sont toujours des **1**. Par conséquent, le premier octet d'une adresse de classe E est compris entre 11110000 et 11111111 (soit 240 et 255 en décimal).

2.2 Les adresses spéciales :

Toute machine d'un réseau IP est identifiée par le couple <Net_ID> <Host_ID> mais certaines valeurs de ces champs ont une signification particulière :

2.2.1 L'adresse réseau :

L'adresse <Net_ID><0> où tous les bits du champ *Host_ID* sont à 0 désigne le réseau lui-même.

Application : Donner l'adresse du réseau auquel appartiennent les machines suivantes :

PC1 :198.150.11.15

PC2 :198.150.11.19

2.2.2 L'adresse de route par défaut :

L'adresse 0.0.0.0 ne peut pas être affectée à une machine particulière. Dans les routeurs cette adresse désigne la route par défaut (route à prendre si aucune route ne correspond à l'adresse destination).

2.2.3 L'adresse de boucle locale :

La machine elle-même ou la machine locale peut être auto-adressée avec une adresse de la forme 127.x.x.x cette adresse dite de boucle locale (utilisée pour les tests ou les programmes applicatifs :

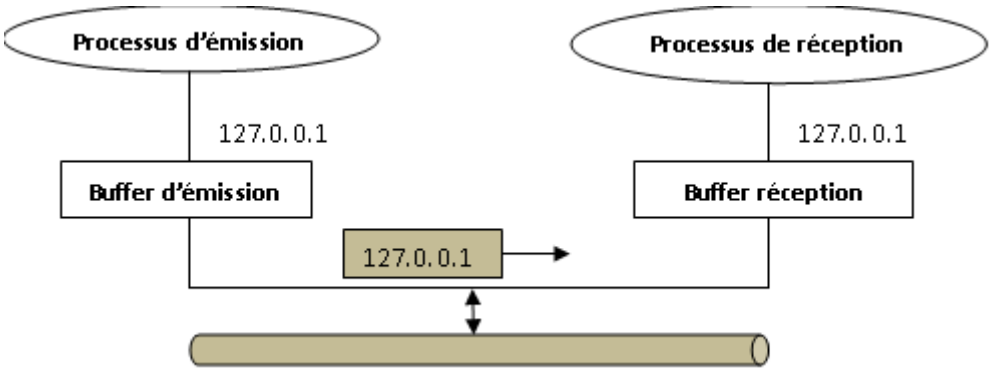


Figure24 : L'adresse de boucle locale

2.2.4 L'adresse de diffusion (*broadcast*):

Si une machine veut s'adresser à toutes les machines d'un autre réseau elle utilisera une adresse de type <Net_ID><1>, tous les bits à 1 du champs <Host_ID> identifient toutes les machines du réseau <Net_ID><0>.

Application : Donner la désignation de chacune des adresses suivantes :

- ✓ 123.0.0.0
- ✓ 123.0.0.18
- ✓ 123.255.255.255

2.3 Les adresses publiques et les adresses privées :

Pour permettre l'interconnexion des réseaux, il faut garantir l'unicité des adresses. C'est l'une des attributions de l'IANA qui attribue à chaque réseau un identifiant unique. Cependant, tous les réseaux n'ont pas nécessairement un besoin d'interconnexion au réseau public, dans ce cas le respect de l'unicité des adresses au plan mondial n'est pas nécessaire. Certaines entreprises (organisations) disposent de leur propre réseau (réseau privé) et n'ont aucun besoin d'interconnexion vers l'extérieur. Afin de prévenir dans les réseaux privés une éventuelle utilisation anarchique des adresses il a été envisagé de réserver des plages d'adresses à ces réseaux. Ces adresses ne sont pas routables sur Internet :

Classe	Début de la plage	Fin de la plage	Nombre de réseaux
A	10.0.0.0	10.255.255.255	1
B	172.16.0.0	172.31.255.255	16
C	192.168.0.0	192.168.255.255	256

Tableau 1: Les adresses privées

2.4 Notion de sous réseau (le subnetting) :

2.4.1 Nécessité de définir des sous-réseaux:

Dans ce qui suit nous allons expliquer la procédure de découpage en sous-réseaux afin de gérer les adresses IP. La décomposition en sous-réseaux (subnetting) est une méthode utilisée pour gérer les adresses IP.

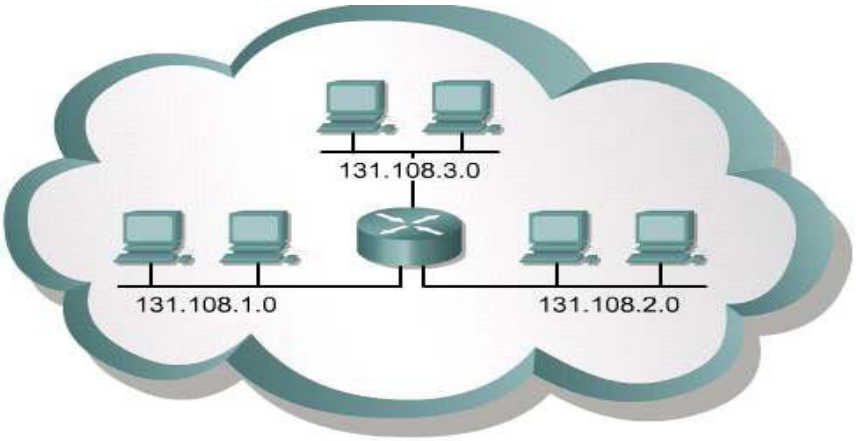


Figure25 : Notion de sous réseau

Comme le montre la figure, le réseau 131.108.0.0 est décomposé en trois sous-réseaux, le 131.108.1.0, le 131.108.2.0 et le 131.108.3.0.

Cette méthode, basée sur la fragmentation de classes d'adresses réseau entières en composants plus petits, a permis d'éviter la pénurie d'adresses IP. Il est impossible de traiter du protocole TCP/IP sans aborder la question des sous-réseaux. En tant qu'administrateur système, il est primordial d'appréhender la notion de découpage en sous-réseaux afin de pouvoir subdiviser un LAN et y identifier les différents réseaux. Dans le cas de réseaux de petite taille, il n'est pas toujours utile de créer des sous-réseaux.

Les avantages de la segmentation en sous-réseau sont les suivants :

- **Utilisation de plusieurs media** (câbles, supports physiques). La connexion de tous les nœuds à un seul support de réseau peut s'avérer impossible, difficile ou coûteuse lorsque les nœuds sont trop éloignés les uns des autres ou qu'ils sont déjà connectés à un autre media.
- **Réduction de l'encombrement**. Le trafic entre les nœuds répartis sur un réseau unique utilise la largeur de bande du réseau. Par conséquent, plus les nœuds sont nombreux, plus la largeur de bande requise est importante. La répartition des nœuds sur des réseaux séparés permet de réduire le nombre de nœuds par réseau. Si les nœuds d'un réseau de petite taille communiquent principalement avec d'autres nœuds du même réseau, l'encombrement global est réduit.
- **Economise les temps de calcul**. Les diffusions (paquet adressé à tous) sur un réseau obligent chacun des nœuds du réseau à réagir avant de l'accepter ou de la rejeter.
- **Isolation d'un réseau**. La division d'un grand réseau en plusieurs réseaux de taille inférieure permet de limiter l'impact d'éventuelles défaillances sur le réseau concerné Il peut s'agir d'une erreur matérielle du réseau.
- **Renforcement de la sécurité**. Sur un support de diffusion du réseau comme Ethernet, tous les nœuds ont accès aux paquets envoyés sur ce réseau. Si le trafic sensible n'est autorisé que sur un réseau, les autres hôtes du réseau n'y ont pas accès.

Les masques de sous-réseaux (*subnet mask*) permettent de segmenter un réseau en plusieurs sous-réseaux. On utilise alors une partie des bits de l'adresse d'hôte pour identifier des sous réseaux.

L'adressage de sous-réseau permet de définir des organisations internes de réseaux qui ne sont pas visibles à l'extérieur de l'organisation. Cet adressage permet par exemple l'utilisation d'un routeur externe qui fournit alors une seule connexion Internet.

Toutes les machines appartenant à un sous-réseau possèdent le même numéro de réseau.

On utilise le même principe que pour le masque par défaut sur l'octet de la partie hôte auquel on va prendre des bits. Ainsi, le masque de sous-réseau d'une adresse de classe B commencera toujours par 255.255.xx.xx

2.4.2 Utilisation du masque de sous-réseau :

Nous avons vu qu'une adresse IP était constituée d'un numéro de réseau et d'un numéro d'hôte. Cela dit, les masques de sous-réseaux permettent de diviser les réseaux de classe A, B ou C en sous-réseaux. En effet, en admettant que tous les hôtes d'un réseau de classe A soit sur le même sous-réseau, le réseau serait très rapidement saturé, ne serait-ce que par les broadcast qui sont destinés à tous les hôtes du même réseau. Les réseaux sont donc divisés en sous-réseaux et le masque permet de les déterminer. Par exemple, pour un réseau de classe C, on a coutume d'utiliser 255.255.255.0 comme masque de sous-réseau. Cela signifie que dans l'adresse IP, la partie numéro de réseau sera les trois premiers nombres et que la partie numéro d'hôte sera le quatrième.

En fait, pour savoir dans une adresse IP quelle est la partie numéro de réseau et numéro d'hôte, il suffit d'écrire l'adresse IP en binaire et d'écrire dessous le masque de sous-réseau, également en binaire. Soit l'adresse IP 192.168.2.53 et le masque 255.255.255.0…

On obtient, en binaire :

11000000.10101000.00000010.00110101

11111111.11111111.11111111.00000000

La partie correspondante aux 1 du masque de sous-réseau correspond au numéro de réseau et la partie correspondante au 0 correspond au numéro d'hôte. On fait un ET logique entre l'adresse IP et le masque, on obtient l'adresse réseau.

Ainsi, dans ce cas, avec un masque de 255.255.255.0, on peut avoir 254 hôtes différents sur le sous-réseau 192.168.2.0…

2.4.3 Détermination des caractéristiques de sous réseau :

- **Nombre de sous-réseaux :** Le nombre théorique de sous-réseaux est égal à 2^{n}, n étant le nombre de bits à 1 du masque qui ont été empruntés de la partie hôte, utilisés pour coder les sous-réseaux.

Exemple :

Adresse de réseau : 200.100.40.0

Masque : 255.255.255.224

224 = **111** 00000 donc **3 bits** pour le N° de **sous-réseau** et 5 bits pour l'hôte.

Autrement dit, dans notre exemple, on ne pouvait pas utiliser le sous-réseau 0 et le sous réseau 224. Le premier nous donnant une adresse de sous-réseau équivalente à l'adresse du réseau soit 200.100.40.0. Le deuxième nous donnant une adresse de sous-réseau dont l'adresse de diffusion se confondrait avec l'adresse de diffusion du réseau. Le nombre de sous-réseaux aurait alors été de seulement *: 2^3-2 =6.*

- **Adresse des sous-réseaux**

Il faut donc maintenant trouver les adresses des sous-réseaux valides en utilisant les bits à 1 du masque.

Pour l'exemple précédent, il faut utiliser les 3 premiers bits:

000 00000 = 0

001 00000 = 32

010 00000 = 64

011 00000 = 96

100 00000 = 128

101 00000 = 160

110 00000 = 192

111 00000 = 224

On constate que le pas entre 2 adresses de sous-réseau est de *32 = 2^5* correspondant au nombre théorique d'hôtes par sous-réseau.

- **Adresse de diffusion d'un sous-réseau**

Il faut mettre **tous les bits de la partie hôte à 1**. Cherchons l'adresse de diffusion des sous réseaux précédents.

Exemple 1

• Avec le masque 255.255.255.224

- Pour le sous-réseau 200.100.40.32 :

32 = **001** 00000 donc l'adresse de diffusion est ***001*** *11111 = 63.*

L'adresse de diffusion complète est donc *200.100.40.63.*

L'adresse de la première machine est *200.100.40.33* avec 33 = **001** 00001.

L'adresse de la dernière machine est *200.100.40.62* avec 62 = **001** 11110.

- Pour le sous-réseau 200.100.40.64 :

64 = **010** 00000 donc l'adresse de diffusion est ***010*** *11111 = 95.*

L'adresse de diffusion complète est donc *200.100.40.95.*

L'adresse de la première machine est *200.100.40.65* avec 65 = **010** 00001.

L'adresse de la dernière machine est *200.100.40.94* avec 94 = **010** 11110.

Exemple 2

• Avec le masque 255.255.255.129

129 = **1**0000000**1** donc **2 bits** pour le N° de **sous-réseau** et 6 bits pour l'hôte, d'où le nombre de sous-réseaux théorique est 22=4.

- Pour le sous-réseau 200.100.40.1 :

1 = **0**0000000**1** donc l'adresse de diffusion est ***0***1111111***1*** *= 127.*

L'adresse de diffusion complète est donc 200.100.40.127.

L'adresse de la première machine est *200.100.40.3* avec 3 = **0**0000001**1**.

L'adresse de la dernière machine est *200.100.40.125* avec 125 = **0**1111110**1**.

- Pour le sous-réseau 200.100.40.128 :

128 = **1**0000000**0** donc l'adresse de diffusion est **1**1111111**0** = 254.

L'adresse de diffusion complète est donc 200.100.40.254.

L'adresse de la première machine est 200.100.40.130 avec 130 = **1**0000010**0**.

L'adresse de la dernière machine est 200.100.40.252 avec 252 = **1**1111100**0**.

- **Nombre de postes d'un sous-réseau**

Le nombre de postes est égal à $\mathbf{2^n}$, **n** étant le nombre de **bits à 0** du masque permettant de coder l'hôte. A ce chiffre il faut enlever 2 numéros réservés :

• tous les bits hôtes à zéro qui identifient le sous-réseau lui-même.

• tous les bits hôtes à 1 qui est l'adresse de diffusion pour le sous-réseau.

Exemples :

Soit le masque 255.255.255.224

*224 = **111**00000 donc 3 bits pour le N° de sous-réseau et 5 bits pour l'hôte*

Le nombre de postes est donc de : 2^5 -2 =30 postes.

De même, avec le masque non contigu 255.255.255.129 le nombre de postes sera de

2^6-2 = 62 postes

Lorsque l'@ IP et le masque de sous-réseau sont exprimés en notation décimale :

• Convertir l'@IP au format binaire.

• Utiliser le masque de sous-réseau au format binaire.

• Pour connaître l'adresse du sous-réseau auquel une machine appartient, on effectue en réalité un **ET logique** entre l'adresse de la machine et le masque.

Exemple 1 :

Adresse : 200.100.40.33 11001000.01100100.00101000.00100001

Masque : 255.255.255.224 11111111.11111111.11111111.11100000

Opération ET 11001000.01100100.00101000.00100000

La machine appartient au sous-réseau : 200.100.40.32

Exemple 2 :

Adresse : 192.0.0.131

Masque : 255.255.255.192

Conversion de l'adresse en binaire : 11000000 00000000 00000000 10000011

Conversion du masque en binaire : 11111111 11111111 11111111 11000000

Décomposition de l'adresse (R, H) : **11000000 00000000 00000000 10**000011

La machine appartient au sous-réseau *192.0.0.128* et dont l'identifiant hôte est *3 (11 en binaire).*

Exemple 3:

Soit l'@ IP 10.217.123.7 et le masque de S/R 255.248.0.0 qui lui est associé. Calculer l'identificateur de réseau

Notation binaire

Adresse IP 00001010 11011001 01111011 00000111

Masque de S/R 11111111 11111000 00000000 00000000

Identificateur de Réseau 00001010 11011000 00000000 00000000

Identificateur de réseau en notation décimale: 10.216.0.0

DETECTION ET CORRECTION D'ERREURS (COUCHE LIAISON DE DONNEES)

Plan du chapitre :

1. Introduction
2. Notion de trame
3. Notion d'erreur
4. Détection d'erreur
5. Correction d'erreur

Objectifs du chapitre :

- Comprendre la notion de détection d'erreur.
- Maitriser quelques codes détecteurs d'erreurs.
- Maitriser quelques codes correcteurs d'erreurs.

1. Introduction :

La couche liaison de données est responsable du transfert de datagrammes, sur un lien, d'un nœud vers son adjacent. Le datagramme est encapsulé dans une trame par l'ajout d'entête.

Au niveau de la couche liaison de données, les adresses physiques (adresses MAC) sont utilisées dans les en-têtes des trames pour identifier la source et la destination. La couche liaison de données offre plusieurs services:

- Contrôle de flux : entre les nœuds d'envoi et réception adjacents.
- Détection d'erreurs : erreurs causées par l'atténuation du signal, par le bruit. Le récepteur détecte la présence d'erreurs : il demande une retransmission ou destruction de la trame.
- Correction d'erreurs : le récepteur identifie et corrige les erreurs de bits sans donner lieu à une retransmission.

La couche liaison est implémentée dans un "adaptateur" (carte Ethernet par exemple). Lors de l'émission, l'émetteur encapsule le datagramme dans une trame en ajoutant les bits de contrôle d'erreurs, de fiabilité, de contrôle de flux, etc. Lors de la réception, le récepteur vérifie les erreurs, la fiabilité, contrôle le flux, etc et extrait ensuite le datagramme.

2. Notion de trame :

Le but de cette notion est de Fixer une unité de données pour le contrôle d'erreur. Dans ce cas, le récepteur doit savoir quand commence une trame et quand elle finit. Pour cela, il existe différentes techniques de découpage en trame. On peut citer comme exemple :

- **Compter les caractères :** comme dans l'exemple suivant, on trouve le nombre d'octet avant le début de chaque trame :

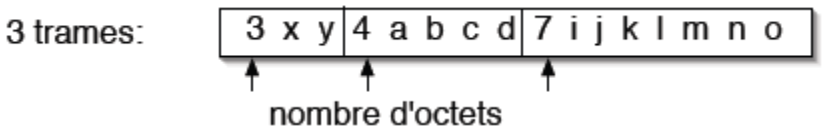


Figure 26: technique de comptage de caractère

- **Utiliser la notion de fanion :** un caractère spécial ou une combinaison de bits particulière appelée fanion, permet de récupérer le début et la fin des données transmises :

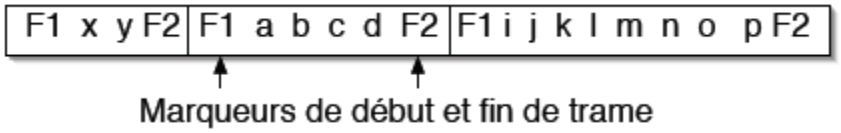


Figure 27: technique de fanion

3. Notion d'erreurs :

3.1 Taux d'erreur binaire :

On appelle taux d'erreur binaire ou BER(Bit Error Rate) le rapport entre le nombre d'information (bits) erronées reçues et le nombre d'information (bits) transmises :

$$Teb = \frac{\text{Nombre de bits erronés}}{\text{Nombre de bits transmis}}$$

Exemple :

Les données transmises : 01100 10011 00100 10100 1010

Les données reçues : 01100 11011 00101 10100 0010

- Teb= 3/24= 0,125

Remarques :

- Le taux d'erreur binaire varie entre 10^{-4} (RTC) et 10^{-9} (Réseaux locaux).
- Dans les réseaux les erreurs se produisent généralement par rafale(l'erreur affecte aléatoirement n bits consécutifs et non 1 bit tous les x bits).
- Si Te est la probabilité pour qu'un bit soit, la probabilité de recevoir un bit correcte est de (1-Te) pour un bloc de N bits la probabilité de recevoir ce bloc correcte est : $(1\text{-}Te)^N$. On peut alors déduire que le probabilité d'une réception correcte est plus faible que la longueur du bloc est plus grande.

Exercice d'application :

Supposons une transmission de 100 caractères émis sur une liaison de 4800 bit/s avec un Te= 10^{-4}. Quelle est la probabilité de recevoir un message erroné ?

Correction :

Un message de 100 caractère correspond à un bloc de : 100*8=800 bits.

La probabilité de réception d'un bloc correcte est de : $(1\text{-}0{,}0001)^{800}$=0,923.

La probabilité de réception d'un message erroné est de : 1-0,923=0,077.

3.2 La détection d'erreur :

C'est le mécanisme mis en œuvre par le système destinataire pour vérifier la validité des données reçues. La détection d'erreur repose sur l'introduction d'une certaine redondance dans l'information transmise.

Quatre techniques peuvent être mises en œuvre pour détecter et éventuellement corriger les erreurs :

- **La détection par écho :** Le récepteur renvoie en écho, à l'émetteur, le message reçu. Si le message est différent à celui qu'il a émis, l'émetteur annule sa précédente transmission et retransmet le message.
- **La détection par répétition :** Chaque message émis est suivi de sa réplique. Si les deux messages sont différents, le récepteur demande une retransmission.
- **La détection d'erreur par clé calculé :** une information supplémentaire (clé) déduite des informations transmises est ajoutée à celle-ci. En réception, le récepteur recalcule la clé, si le résultat obtenu correspond à la clé reçue, les données sont réputées exactes, sinon le récepteur ignore les données reçues et éventuellement en demande la retransmission. Dans ce cas, on a : Bloc émis= Message+clé.
- **Détection et correction d'erreur par code :** cette technique consiste à ajouter aux caractères à transmettre, une combinaison binaire différente du codage de base tels qu'en cas d'erreur sur un nombre limité de bits, on puisse toujours déduire du code reçue la valeur binaire envoyée.

4 Détection d'erreurs:

4.1 Technique de bit de parité :

Consiste à ajouter, à la séquence binaire à protéger, un bit à 1 ou à 0 suivant la parité du nombre de bits à dans les données. Le récepteur vérifie la valeur de ce bit de parité.

- Si la parité est paire et le nombre de bits égaux à 1 est pair, on ajoute le bit de parité 0, sinon on ajoute le bit 1.
- Si la parité est impaire, on inverse.

Exemple :

- Parité paire :

Données : 100011 ➡ bit de parité =1

Données : 100111011 ➡ bit de parité =0

- Parité impaire :

Données : 100011 ➡ bit de parité =0

Données : 100111011 ➡ bit de parité =1

4.2 Les codes cycliques ou détection par clé calculée :

Dans la détection par clé calculée, l'information redondante, la clé CRC(Cyclic Redundancy Check) est déterminé par une opération mathématique complexe appliquée au bloc de donnée à transmettre et transmise avec celui-ci.

Cette méthode est appelée aussi méthode de contrôle polynomial, elle est très utilisé dans les protocoles modernes car elle permet de détecter des erreurs sur plusieurs bits.

Cette méthode utilise les polynômes suivants :

- *P(x) :* Polynôme associé à l'information à transmettre.
- *Q(x) :* Polynôme générateur caractérisant le contrôle.
- *R(x)* : Polynôme reste correspond à l'information redondante ajoutée en fin de trame.

✓ Si r est le degré de *Q(x)* alors *R(x)* est le reste de la division euclidienne de $x^r \times P(x)$ par *Q(x)* :

$$R(x) = (x^r \times P(x)) \bmod Q(x)$$

✓ En réception, pour vérifier la validité des données, il suffit d'effectuer le quotient suivant :

$$(x^r \times P'(x) + R'(x)) / Q(x)$$

Si le reste est nul alors on suppose qu'il n'y a pas eu d'erreur de transmission.

Si le reste n'est pas nul, alors il y a eu une erreur de transmission et il faut demander la réémission de la trame.

Exemple :

Soit 1000001110000100 l'information à transmettre. Alors le polynôme correspondant est :

$$P(x) = x^{15} + x^9 + x^8 + x^7 + x^2$$

Soit le polynôme de contrôle de degrés 12 suivant :

$$Q(x) = x12 + x11 + x3 + x2 + x + 1$$

La division de $x12 \times P(x)$ par *Q(x)* donne le polynôme reste :

$R(x) = (x^{12} \times P(x)) \bmod Q(x) = x^{11} + x^9 + x^8 + x^7 + x^6 + x^4 + 1$

L'information redondante à ajouter en fin de trame est donc : 101111010001.

La trame envoyée contient donc : 1000001110000100 101111010001.

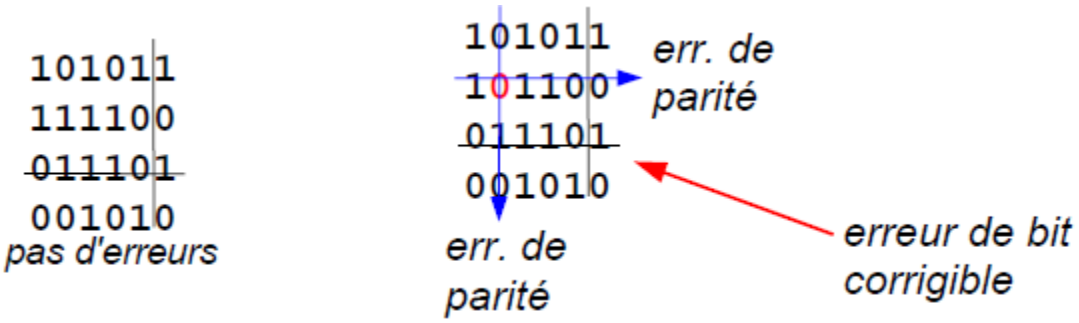
CRC

5 Correction d'erreurs:

5.1 Parité matricielle :

Le bit de parité bidimensionnel permet de détecter et corriger l'erreur sur un seul bit. Dans ce cas les trames sont considérées comme des matrices n x n (généralement n = 8 bits). On ajoute alors un bit de parité par colonne (LRC : Longitudinal Redundancy Check) et par ligne (VRC : vertical Redundancy Check).

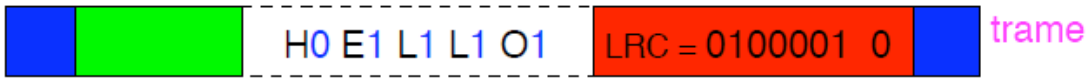
Soient les deux trames reçues suivantes :



Exemple 1 **: VRC + LRC**

Le mot **HELLO** va être envoyé dans le réseau, déterminons alors la trame émise :

lettre	lettre codée	VRC
H	0001001	0
E	1010001	1
L	0011001	1
L	0011001	1
O	1111001	1
LRC	0100001	0



***Exemple 2*:**

Un émetteur va envoyer la séquence de bits suivantes: D = 1101101 1111110 1111111

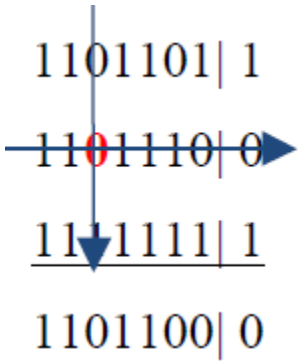
1101101| 1
1111110| 0
1111111| 1
1101100| 0

En effectuant la méthode de parité matricielle les données à transmettre seront :

D' = 11011011 11111100 11111111 11011000

Supposons que les données reçues sont: D'' = 11011011 11011100 11111111 11011000

D''≠ D', pour corriger procède de la manière suivante :



Il y a une erreur, il suffit de remplacer le bit 0 par 1.

5.2 Code de Hamming :

5.2.1 Définitions :

- **Mot du code :** Si une trame contient m bits de données et r bits de contrôle, on appelle mot du code le mot formé par les m + r bits. On pose n = m + r.

- **Distance de Hamming :** Étant donné deux mots de n bits m1 et m2, le nombre de bits dont ils diffèrent est appelé leur distance de Hamming (notée Disth).

Soient 2 mots de code (100001001 et 100110001), il est possible de déterminer combien de bits diffèrent (ex. 3 bits).

La distance de Hamming est le nombre de bits pour lesquels 2 mots de code diffèrent. Si 2 mots de code sont distants de d il faudra d bits en erreur pour passer de l'un à l'autre.

Remarque :

- ✓ Pour détecter x erreurs on a besoin d'une distance de x+1
- ✓ Pour corriger x erreurs on a besoin d'une distance 2x+1

Exemple :

Soient 4 mots de code 0000000000, 0000011111, 1111100000, 1111111111. La distance de Hamming est 5, d'où on peut corriger 2 erreurs.

Si 0000000111 arrive, le récepteur saura que le mot de code était 0000011111. Mais si une triple erreur se produit, il ne pourra pas la corriger.

5.2.2 Détection et correction d'erreurs:

Considérons un émetteur qui veut transmettre : D = 110101110111, on a alors 12 bits de données, $2^0 < 12 < 2^4$, donc il y a 5 bits de contrôle, ainsi le mot de code est formé par 17 bits = 12+5

	2^4									2^3				2^2		2^1	2^0
1		1	0	1	0	1	1	1		0	1	1		1			
17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	

- Remplissage des bits de contrôle

a) Ecrire les positions de données comme une somme des positions de contrôle (sans répétition)

3 = 2 + 1

5 = 4 + 1

6 = 4 + 2

7 = 4 + 2 + 1

9 = 8 + 1

10 = 8 + 2

11 = 8 + 2 + 1

12 = 8 + 4

13 = 8 + 4 + 1

14 = 8 + 4 + 2

15 = 8 + 4 + 2 + 1

17 = 16 + 1

b) Associer aux bits de contrôle les bits de données correspondants et calculer la parité de ces bits :

$1 \leftarrow 3^1\ 5^1\ 7^0\ 9^1\ 11^1\ 13^1\ 15^1\ 17^1$ 1

$2 \leftarrow 3^1\ 6^1\ 7^0\ 10^1\ 11^1\ 14^0\ 15^1$ 1

$4 \leftarrow 5^1\ 6^1\ 7^0\ 12^0\ 13^1\ 14^0\ 15^1$ 0

$8 \leftarrow 9^1\ 10^1\ 11^1\ 12^0\ 13^1\ 14^0\ 15^1$ 1

$16 \leftarrow 17^1$ 1

c) Remplir les bits de contrôle en utilisant la parité

	2^4								2^3				2^2		2^1	2^0
1	1	1	0	1	0	1	1	1	1	0	1	1	0	1	1	1
17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

On obtient alors : D' = 11101011110110111

Considérons que le récepteur a reçu la séquence suivante: D'' = 11001011110110111

Si D''≠ D', on peut corriger en suivant la méthode suivante :

	2^4								2^3				2^2		2^1	2^0
1	1	0	0	1	0	1	1	1	1	0	1	1	0	1	1	1
17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

a) De même que pour l'émetteur

b)

$1 \leftarrow 3^1\ 5^1\ 7^0\ 9^1\ 11^1\ 13^1\ 15^0\ 17^1$ 0 x

$2 \leftarrow 3^1\ 6^1\ 7^0\ 10^1\ 11^1\ 14^0\ 15^0$ 0 x

$4 \leftarrow 5^1\ 6^1\ 7^0\ 12^0\ 13^1\ 14^0\ 15^0$ 1 x

$8 \leftarrow 9^1\ 10^1\ 11^1\ 12^0\ 13^1\ 14^0\ 15^0$ 0 x

$16 \leftarrow 17^1$ 1 γ

Pour chercher l'erreur, il faut appliquer la formule suivante :

∩ {positions de données associées aux bits de contrôle erronés} – U {positions de données associées aux bits de contrôle corrects}. Si on trouve Ø, l'erreur est dans le bit de contrôle où se trouve l'erreur.

D'où : on obtient le bit erroné n°15 ainsi on remplace 0 par 1.

TRANSMISSION DES DONNEES (COUCHE PHYSIQUE)

Plan du chapitre :

1. Représentation des données
2. Principaux éléments intervenants dans la transmission
3. Supports physiques
4. Caractéristiques d'une transmission

Objectifs du chapitre :

- Définir les différents élements d'une transmission.
- Comparer les différents supports physiques.
- Distinguer entre les différents types de transmission.

1. Représentation des données :

Le but d'un réseau est de transmettre des informations d'un ordinateur à un autre. Pour cela, il faut dans un premier temps décider du type de codage de la donnée à envoyer, c'est-à-dire sa représentation informatique. Celle-ci sera différente selon le type de données, car il peut s'agir de:

- données sonores
- données textuelles
- données graphiques
- données vidéo
- ...

La représentation de ces données peut se diviser en deux catégories:

• Une représentation numérique: c'est-à-dire le codage de l'information en un ensemble de valeurs binaires, soit une suite de 0 et de 1.

• Une représentation analogique: c'est-à-dire que la donnée sera représentée par la variation d'une grandeur physique continue.

2. Principaux éléments intervenants dans la transmission :

Les principaux éléments intervenants dans la transmission sont les suivants :

- **L'ETTD : E**quipement **T**erminal de **T**raitement de **D**onnées : C'est l'ordinateur.
- **L'ETCD : E**quipement **T**erminal de **C**ommunication (ou circuit) de **D**onnées : C'est un équipement spécifique chargé d'adapter les données à transmettre au support de communication : C'est le MODEM.
- Le support de transmission.

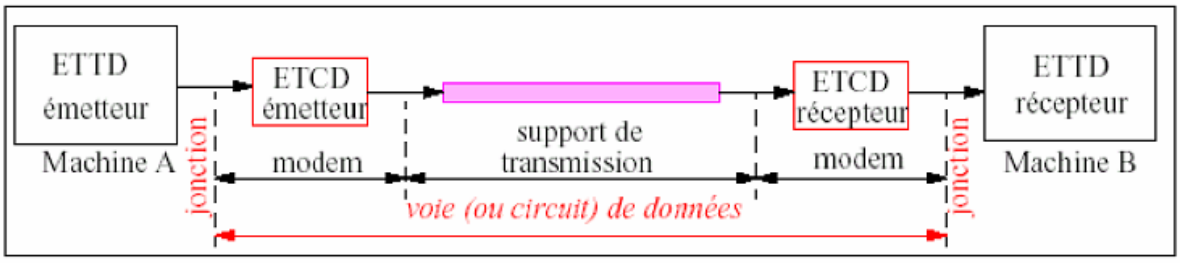


Figure 28: Les principaux éléments d'une transmission

Le **MODEM** est un **Mo**dulateur-**DEM**odulateur. Il permet la communication entre ordinateurs par le réseau téléphonique.

Figure 29: Communication entre deux ordinateurs par le réseau téléphonique à travers le modem

La modulation est la conversion du signal numérique en signal analogique. La démodulation est la conversion du signal analogique en signal numérique.

A l'émission l'ETCD émetteur a pour rôle la modulation. Et à la réception le rôle de l'ETCD récepteur est inversement la démodulation :

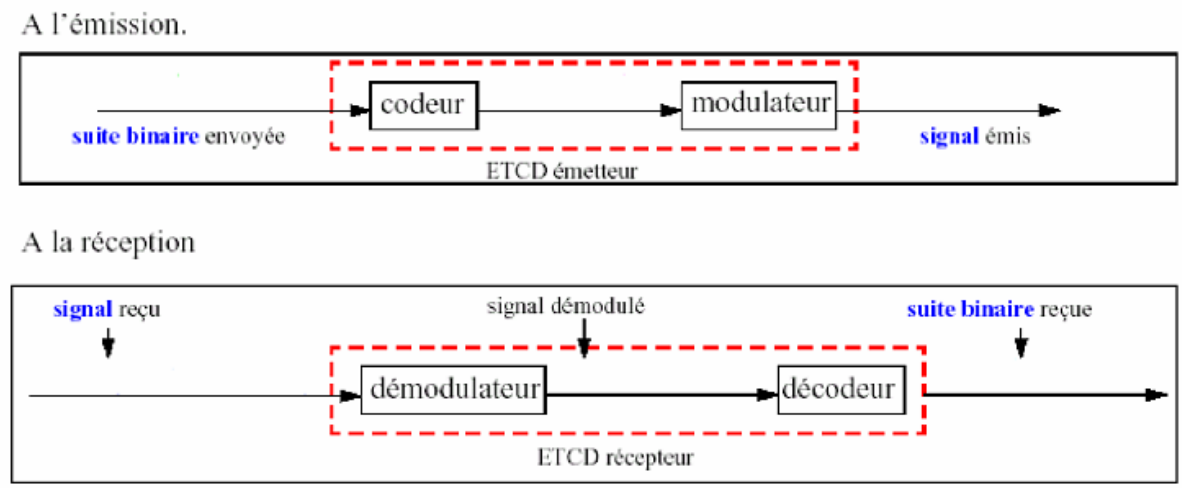


Figure 30: Rôles ETCD émetteur et ETCD récepteur

3. Supports physiques :

Les supports physiques de transmissions sont les éléments permettant de faire circuler les informations entre les équipements de transmission. On classe généralement ces supports en trois catégories, selon le type de grandeur physique qu'ils permettent de faire circuler, donc suivant leur constitution physique:

- Les supports filaires permettent de faire circuler une grandeur électrique sur un câble généralement métallique.

- Les supports aériens désignent l'air ou le vide, ils permettent la circulation d'ondes électromagnétiques ou radioélectriques diverses.
- Les supports optiques permettent d'acheminer des informations sous forme lumineuse.

Il existe de nombreux types de câbles, mais on distingue généralement:

- Le câble coaxial
- Les paires torsadées
- Les fibres optiques

3.1 Câble coaxial :

Le câble coaxial est une ligne de transmission utilisée en hautes fréquences. Il est peu coûteux et facilement manipulable (poids, flexibilité, …) et composée d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure.

Figure 31: Câble coaxial

• La **gaine** permet de protéger le câble de l'environnement extérieur. Elle est habituellement en caoutchouc.

• Le **blindage** (enveloppe métallique) entourant les câbles, permet de protéger les données transmises sur le support des parasites (autrement appelé bruit) pouvant causer une distorsion des données.

• L'**isolant** entourant la partie centrale, est constitué d'un matériau diélectrique permettant d'éviter tout contact avec le blindage, provoquant des interactions électriques (court-circuit).

• L'**âme**, accomplissant la tâche de transport des données, est généralement composée d'un seul brin en cuivre ou de plusieurs brins torsadés.

Grâce à son blindage, le câble coaxial peut être utilisé sur des longues distances et à haut débit (contrairement à un câble de type paire torsadée), on le réserve toutefois pour des installations de base. On distingue habituellement deux types de câble coaxiaux:

- Le câble coaxial **fin** (appelé Thinnet) Il s'agit d'un câble de diamètre 6mm. Très flexible il peut être utilisé dans la majorité des réseaux, en le connectant directement sur la carte réseau. Il permet de transporter un signal sur une distance d'environ 185 mètres sans affaiblissement.

- Le câble coaxial **épais** (Thicknet) est un câble de plus gros diamètre (12 mm). Il a longtemps été utilisé dans les réseaux, ce qui lui a valu l'appellation de « Câble Ethernet Standard ». Etant donné que son âme a un plus gros diamètre, la distance susceptible d'être parcourue par les signaux est grande, cela lui permet de transmettre sans affaiblissement des signaux sur une distance atteignant 500 mètres.

Usage :

- ✓ Entre une antenne TV et une télévision.
- ✓ Dans le réseau câblé urbain de télévision.
- ✓ Entre un émetteur et l'antenne d'émission.
- ✓ Dans les réseaux de transmission de données tels qu'Ethernet dans ses anciennes versions 10 Base 2, 10 Base 5.
- ✓ Pour les liaisons interurbaines téléphoniques et dans les câbles sous marins.

Le câble coaxial est maintenant remplacé par la Fibre Optique sur les longues distances (> à quelques Km).

3.2 Paires torsadées :

Le câble à paire torsadée (TWISTED-PAIR CABLE) est composé de deux brins de cuivre entrelacés (torsadés) et recouverts d'une enveloppe isolante. L'entrelacement des brins de cuivre permet de limiter les interférences extérieures (moteur, relais, transformateur, …), toutefois la protection d'un blindage est bien plus efficace pour diminuer les risques d'interférences.

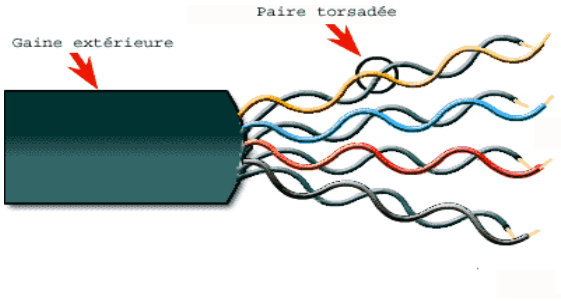


Figure 32: Câble Paires torsadées

On distingue généralement deux types de paires torsadées :

- Le câble à paire torsadée non blindée (UTP pour UNSHIELDED TWISTED-PAIR) : est composé de deux ou quatre brins de cuivre entrelacés (torsadés) et recouverts d'une enveloppe isolante. Les caractéristiques du câble à paire torsadée non blindée (UTP) :
  - Utilisé à l'origine pour les lignes téléphoniques.
  - Répond aux spécifications de la norme « 10 base T » des réseaux ETHERNET.

- Le câble à paire torsadée blindée (STP pour SHIELDED TWISTED-PAIR) : est composé de quatre brins de cuivre entrelacés deux par deux, deux blindages autour de chaque couple de brins et d'une enveloppe isolante. Le blindage (STP) permet des transferts de données à des débits plus importants et sur des distances plus grandes que l'UTP. Le câble à paire torsadée a été largement diffusé parce qu'il est à l'origine utilisé pour les lignes téléphoniques et qu'il était jusqu'en 1983 systématiquement pré installé dans tous les nouveaux bâtiments américains. Le câble à paire torsadée est le support (le média) le plus utilisé à l'intérieur d'un bâtiment. Il est donc adapté à la mise en réseau local d'un faible parc (longueur maximale de 100 m) avec un budget limité et une connectique simple. Toutefois sur de longues distances avec des débits élevés, elle ne permet pas de garantir l'intégrité des données.

3.3 Fibres Optiques :

Une fibre optique peut être schématisée par la figure suivante :

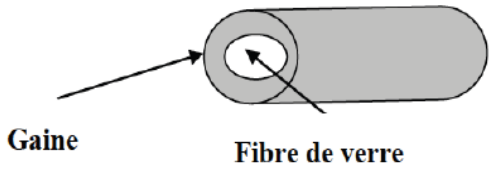


Figure 33: Fibre Optique

La transmission dans ce type de support est basée sur l'émission de la lumière laser ou infrarouge modulé par le signal d'information dans cette fibre. La conversion du signal électrique en signal lumineux est assurée par des émetteurs lasers ou des diodes électroluminescentes.

Avantages : Légèreté, immunité au bruit, faible atténuation, débit très élevé, communication sur de très longues distances.

Inconvénients : Coût élevé, installation difficile.

Usage : adapté à la liaison entre répartiteurs (liaison centrale entre plusieurs bâtiments) car elle permet des connexions sur de longues distances.

4. Caractéristiques d'une transmission

Pour une transmission de données sur une voie de transmission entre deux machines, la communication peut s'effectuer de différentes manières. La transmission est caractérisée par :

- ✓ Le mode de transmission selon le sens des échanges.
- ✓ Le mode de transmission selon le nombre de bits envoyés simultanément.

- ✓ La synchronisation entre émetteur et récepteur.

4.1 Modes de transmission selon le sens des échanges

Selon le sens des échanges, on distingue 3 modes de transmission:

- **La liaison simplex** caractérise une liaison dans laquelle les données circulent dans un seul sens, c'est-à-dire de l'émetteur vers le récepteur. Ce genre de liaison est utile lorsque les données n'ont pas besoin de circuler dans les deux sens (par exemple de votre ordinateur vers l'imprimante ou de la souris vers l'ordinateur...).

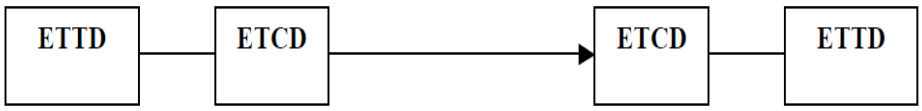


Figure 34: Transmission simplex

- **La liaison half-duplex** (parfois appelée liaison à l'alternat ou semi-duplex) : caractérise une liaison dans laquelle les données circulent dans un sens ou l'autre, mais pas les deux simultanément. Ainsi, avec ce genre de liaison chaque extrémité de la liaison émet à son tour. Ce type de liaison permet d'avoir une liaison bidirectionnelle utilisant la capacité totale de la ligne.

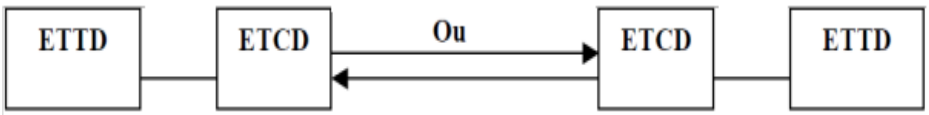


Figure 35: Transmission half-duplex

- **La liaison full-duplex** (appelée aussi duplex intégral) : caractérise une liaison dans laquelle les données circulent de façon bidirectionnelle et simultanée. Ainsi, chaque extrémité de la ligne peut émettre et recevoir en même temps, ce qui signifie que la bande passante est divisée par deux pour chaque sens d'émission des données si un même support de transmission est utilisé pour les deux transmissions.

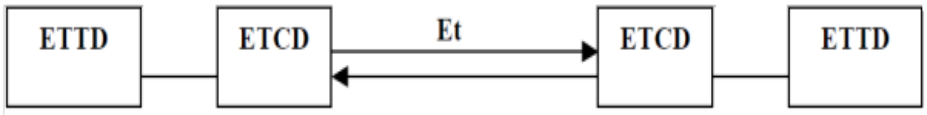


Figure 36: Transmission full-duplex

4.2 Mode de transmission selon le nombre de bits envoyés simultanément:

Désigne le mode de transmission selon le nombre de bits pouvant être simultanément transmis par le canal de communication. En effet, un processeur (donc l'ordinateur en général) ne traite jamais (dans le cas des processeurs récents) un seul bit à la fois, il permet généralement d'en traiter plusieurs (la plupart du temps 8, soit un octet), c'est la raison pour laquelle la liaison de base sur un ordinateur est une liaison parallèle.

- **Transmission parallèle :** On désigne par liaison parallèle la transmission simultanée de N bits. Ces bits sont envoyés simultanément sur N voies différentes. Exemple : Imprimante.

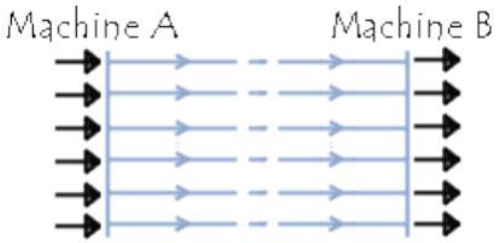


Figure 37: Transmission parallèle

- **Transmission série :** Dans une liaison en série, les données sont envoyées bit par bit sur la voie de transmission. Toutefois, étant donné que la plupart des processeurs traitent les informations de façon parallèle, il s'agit de transformer des données arrivant de façon parallèle en données en série au niveau de l'émetteur, et inversement au niveau du récepteur. Exemple : Souris, Clavier.

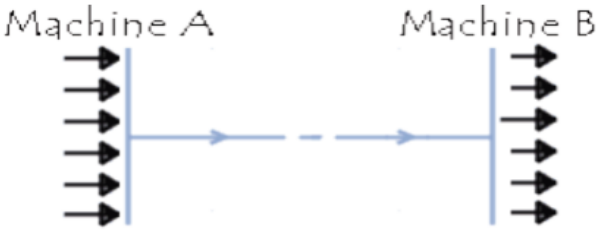


Figure 38: Transmission Série

4.3 Transmission synchrone et asynchrone :

Dans la liaison série, puisqu'un seul fil transporte l'information, il existe un problème de synchronisation entre l'émetteur et le récepteur, c'est-à-dire que le récepteur ne peut pas à priori distinguer les caractères (ou même de manière plus générale les séquences de bits) car les bits

sont envoyés successivement. Il existe donc deux types de transmission permettant de remédier à ce problème:

- **Transmission asynchrone :** Chaque caractère est émis de façon irrégulière dans le temps (par exemple un utilisateur envoyant en temps réel des caractères saisis au clavier). Ainsi, imaginons qu'un seul bit soit transmis pendant une longue période de silence, le récepteur ne pourrait savoir s'il s'agit de 00010000, ou 10000000 ou encore 00000100... Afin de remédier à ce problème, chaque caractère est précédé d'une information indiquant le début de la transmission du caractère (l'information de début d'émission est appelée bit START); et terminé par l'envoi d'une information de fin de transmission (appelée bit STOP).
- **Transmission synchrone :** L'émetteur et le récepteur sont cadencés à la même horloge. Le récepteur reçoit de façon continue (même lorsqu'aucun bit n'est transmis) les informations au rythme ou l'émetteur les envoie. C'est pourquoi il est nécessaire qu'émetteur et récepteur soient cadencés à la même vitesse.

4.4 Transmission analogique et numérique :

- **Transmission analogique :** La transmission analogique de données consiste à faire circuler des informations sur un support physique de transmission sous la forme d'une onde. La transmission des données se fait par l'intermédiaire d'une *onde porteuse*, une onde simple dont le seul but est de transporter les données par modification de l'une de ces caractéristiques (amplitude, fréquence ou phase), c'est la raison pour laquelle la transmission analogique est généralement appelée transmission par modulation d'onde porteuse. Selon le paramètre de l'onde porteuse que l'on fait varier.
  - ✓ **Transmission analogique des données analogiques :** Ce type de transmission désigne un schéma dans lequel les données à transmettre sont directement sous forme analogique. Ainsi, pour transmettre ce signal, l'ETCD doit effectuer une convolution continue du signal à transmettre et de l'onde porteuse, c'est-à-dire que l'onde qu'il va transmettre va être une association de l'onde porteuse et du signal à transmettre.
  - ✓ **Transmission analogique des données numériques :** Lorsque les données numériques ont fait leur apparition, les systèmes de transmissions étaient encore analogiques, il a donc fallu trouver un moyen de transmettre des données numériques de façon analogique. La solution à ce problème était le modem.

Transmission numérique

Définition

La transmission numérique consiste à faire transiter les informations sur le support physique de communication sous forme de signaux numériques. Ainsi, des données analogiques devront préalablement être numérisées avant d'être transmises. Toutefois, les informations numériques ne peuvent pas circuler sous forme de 0 et de 1 directement, il s'agit donc de les coder sous forme d'un signal possédant deux états. Cette transformation de l'information binaire sous forme d'un signal à deux états est réalisée par l'ETCD, appelé aussi codeur bande de base, d'où l'appellation de transmission en bande de base pour désigner la transmission numérique.

Codage des signaux

Pour que la transmission soit optimale, il est nécessaire que le signal soit codé de façon à faciliter sa transmission sur le support physique. Il existe pour cela différents systèmes de codage on peut citer comme exemples:

- ✓ **Codage NRZ** (signifiant No Return to Zero, soit Non Retour à Zéro) est le premier système de codage, car il est le plus simple. Il consiste tout simplement à transformer les 0 en -X et les 1 en +X.

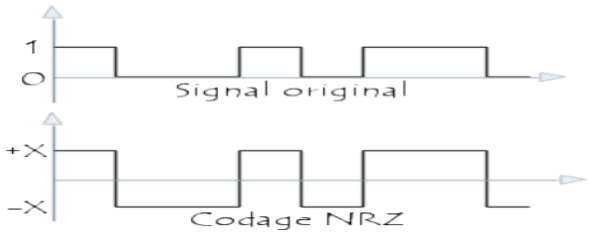


Figure 39: Codage NRZ

- ✓ **Codage Manchester**, également appelé codage biphase ou PE (pour Phase Encode), introduit une transition au milieu de chaque intervalle. Il consiste en fait à faire un OU exclusif (XOR) entre le signal et le signal d'horloge, ce qui se traduit par un front montant lorsque le bit est à zéro, un front descendant dans le cas contraire.

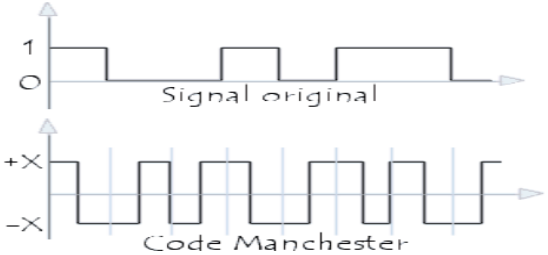


Figure 40: Codage Manchester

- ✓ **Codage Delay Mode**, aussi appelé code de Miller, est proche du codage de Manchester. Le codage peut être réalisé de la manière suivante :
  - transition (front montant ou descendant) au milieu du bit "1"
  - pas de transition au milieu du bit "0"
  - une transition en fin de bit "0" si celui-ci est suivi d'un autre "0"

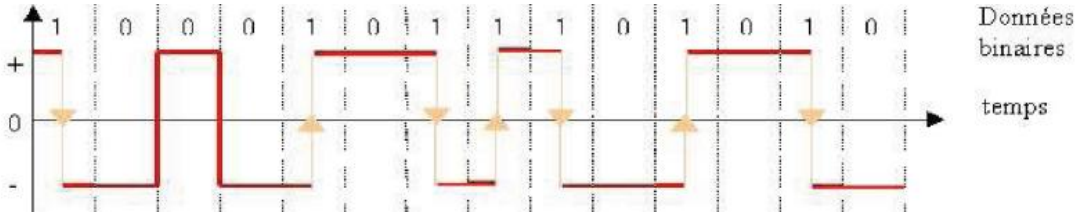


Figure 41: Codage de Miller

- ✓ **Codage bipolaire simple** est un codage sur trois niveaux. Il propose donc trois états de la grandeur transportée sur le support physique:
  - La valeur *0* lorsque le bit est à 0
  - Alternativement +X et -X lorsque le bit est à 1

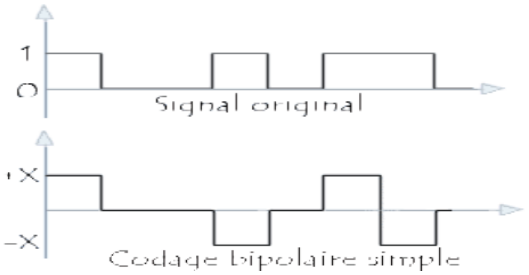


Figure 42: Codage Bipolaire Simple

COMMUTATION ET ROUTAGE

Plan du chapitre :

Objectifs du chapitre :

- Introduire les deux notions de commutation et de routage.

1. Introduction

On a vu que les commutateurs permettent de raccorder plusieurs périphériques à un réseau (le réseau local), tandis que les routeurs assurent l'interconnexion de plusieurs réseaux (sur le réseau étendu). D'où vient la différence entre la commutation et le routage.

2. La commutation

2.1 Principe :

La commutation est la fonctionnalité qui permet d'acheminer les données d'un point A vers un point B dans un même réseau local. La commutation, effectuée par les commutateurs ou switchs, se base sur l'adresse niveau 2 de destination contenu dans la trame paquet reçue (par exemple, c'est une adresse MAC pour le protocole Ethernet).

2.2 Techniques :

La commutation rassemble toutes les techniques qui réalisent la mise en relation de 2 abonnés quelconques. Il existe 4 techniques de commutation :

- Commutation de circuit
- Commutation de messages
- Commutation de paquets
- Commutation de cellules

2.2.1 Commutation de circuit (ex : téléphone)

Un chemin physique est établi à l'initialisation de la communication entre l'émetteur et le récepteur et reste le même pendant toute la durée de la communication. Si les deux correspondants n'ont pas de données à transmettre pendant un certain temps, la liaison restera inutilisée. L'idée est de concentrer plusieurs correspondants sur une même liaison. Dans le cas où les communications seraient nombreuses, il faut prévoir des mémoires pour stocker des informations en attendant que la liaison soit disponible.

2.2.2 Commutation de messages

Un message est un ensemble d'informations logiques formant un tout (fichier, mail) qui est envoyé de l'émetteur vers le récepteur en transitant nœud à nœud à travers le réseau. On a un

chemin logique par message envoyé. Le message ne peut être envoyé au nœud suivant tant qu'il n'est pas reçu complètement et sans erreur par le nœud actuel.

2.2.3 Commutation de paquets

C'est une optimisation de la commutation de message qui consiste à découper les messages en plusieurs paquets pouvant être acheminés plus vite et indépendamment les uns des autres. Cette technique nécessite la mise en place de la numérotation des paquets.

2.2.4 Commutation de cellule

Commutation de paquets particulière. Tous les paquets ont une longueur fixe de 53 octets (1 paquet = 1 cellule de 53 octets). C'est la technique utilisée dans les réseaux ATM où un chemin est déterminé pour la transmission des cellules. Commutation de cellule = superposition de 2 types de commutation : commutation de circuit et la commutation de paquets.

- Mode connecté : Demande explicite de connexion et de déconnexion.
- Mode non connecté : Pas de demande de connexion.

3. Le routage :

3.1 Principe :

Le routage est la fonctionnalité qui permet d'acheminer les données d'un point A vers un point B situé dans un réseau distant. Le routage, effectué par les routeurs, se base sur l'adresse IP de destination contenu dans le paquet reçu.

3.2 Table de routage :

La table de routage est une table de correspondance entre l'adresse de la machine visée et le nœud suivant auquel le routeur doit délivrer le message. En réalité il suffit que le message soit délivré sur le réseau qui contient la machine, il n'est donc pas nécessaire de stocker l'adresse IP complète de la machine: seul l'identificateur du réseau de l'adresse IP (c'est-à-dire l'ID réseau) a besoin d'être stocké.

La table de routage est donc un tableau contenant des paires d'adresses :

Adresse de destination	Adresse du prochain routeur directement accessible	Interface

3.3 Modes de routage :

Il existe deux modes de routages bien distincts le routage statique et le routage dynamique.

3.3.1 Routage statique :

Dans le routage statique, l'administrateur configure les routeurs un à un au sein du réseau afin d'y saisir les routes à emprunter pour aller sur tel ou tel réseau.

Le routage statique présente plusieurs avantages :

- **Économie de bande passante** : Étant donné qu'aucune information ne transite entre les routeurs pour qu'ils se tiennent à jour, la bande passante n'est pas encombrée avec des messages d'information et de routage.
- **Sécurité** : Contrairement aux protocoles de routage dynamique, le routage statique ne diffuse pas d'information sur le réseau puisque les informations de routage sont directement saisies de manière définitive dans la configuration par l'administrateur.
- **Connaissance du chemin à l'avance** : L'administrateur ayant configuré l'ensemble de la topologie saura exactement par où passent les paquets pour aller d'un réseau à un autre, cela peut donc faciliter la compréhension d'un incident sur le réseau lors des transmissions de paquets.

Mais aussi des désavantages :

- La configuration de réseaux de taille importante peut devenir assez longue et complexe.
- A chaque fois que le réseau évolue, il faut que chaque routeur soit au courant de l'évolution par une mise à jour manuelle de la par de l'administrateur qui doit modifier les routes selon l'évolution.

3.3.2 Routage dynamique :

Le routage dynamique permet quant à lui de se mettre à jour de façon automatique. La définition d'un protocole de routage va permettre au routeur de se comprendre et d'échanger des informations de façon périodique ou événementielle afin que chaque routeur soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau. Concrètement, le protocole de routage fixe la façon dont les routeurs vont communiquer mais également la façon dont ils vont calculer les meilleures routes à emprunter.

Le routage dynamique présente les avantages suivants:

- Une **maintenance réduite** par l'automatisation des échanges et des décisions de routage
- Une **modularité** et une **flexibilité** accrue, il est plus facile de faire évoluer le réseau avec un réseau qui se met à jour automatiquement.
- Sa **performance** et sa mise en place ne dépendent pas de la taille du réseau

Mais aussi des désavantages :

- Il peut être plus compliqué à mettre en place lors de son initialisation
- Il consomme de la bande passante de par les messages que les routeurs s'envoient périodiquement sur le réseau
- La diffusion automatique de message sur le réseau peut constituer un problème de sécurité car un attaquant peut obtenir des informations sur la topologie du réseau simplement en écoutant et en lisant ces messages d'information du protocole de routage et même en créer afin de se faire passer pour un membre du réseau.