République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET D' INFORMATIQUE
DEPARTEMENT D' ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Télécommunication et réseaux**

Présenté par
TITOUCHE Ali

SMAANI Aghilas

Thème

Mise au point d'une application d'analyse et de mesure de flux

Mémoire soutenu publiquement le 06/07/ 2017 devant le jury composé de :

M F. OUALLOUCHE
Maitre assistant A, UMMTO, Président

M M. LAZRI
Maitre de conférence B, UMMTO, Encadreur

M D. ALOUACHE
Maitre assistant A, UMMTO, Examinateur

1République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET D' INFORMATIQUE
DEPARTEMENT D' ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Télécommunication et réseaux**

Présenté par
TITOUCHE Ali

SMAANI Aghilas

Thème

Mise au point d'une application d'analyse et de mesure de flux

Mémoire soutenu publiquement le 06/07/ 2017 devant le jury composé de :

M F. OUALLOUCHE
Maitre assistant A, UMMTO, Président

M M. LAZRI
Maitre de conférence B, UMMTO, Encadreur

M D. ALOUACHE
Maitre assistant A, UMMTO, Examinateur

Remerciements

On tient à remercier tout d'abord notre Promoteur, Mr M.LAZRI, pour sa patience, et surtout pour sa confiance, ses remarques et ses conseils, sa disponibilité et sa bienveillance.

Qu'il trouve ici le témoignage de notre profonde gratitude.

On voudrait également remercier les membres du jury pour avoir accepter d'évaluer ce travail et pour toutes leurs remarques et critiques.

On tient aussi à remercier le personnel du Centre des systèmes et réseaux d'informations, de communication, de Télé-enseignement et Enseignement a distance (EX CENTRE DE CALCULE) de l'Université Mouloud Mammeri Tizi-Ouzou qui nous a aidés dans nos recherches et leurs dispositions

Enfin, nous tenons à exprimer notre profonde gratitude à nos familles qui nous ont toujours soutenues et à tout ce qui participe de réaliser ce mémoire. Ainsi que l'ensemble des enseignants qui ont contribué à notre formation.

Dédicace

Je dédie ce modeste travail :

A la mémoire de mon défunt père,

A ma chère mère pour son soutien inestimable,

A mon cher frère **Arezki.**

A mes chères sœurs **Lila, Siham.**

A mes cousins et cousines.

A mes petites cousines **Massilia, Inas, Lina.**

A tous mes ami(e)s ainsi qu'à tous ceux qui me sont chers

Et qui m'ont connu et aidé de prés ou de loin

SMAANI Aghilas

Dédicace

Je dédie ce modeste travail :

A Mes très chers parents à qui je doits tout, je profite de les remercier pour leur encouragement, leur aide, le soutien qu'ils m'ont apporté et le sacrifice qu'ils ont fait pour moi, que dieu les protège et les entoure de sa bénédiction.

A mes chères frères : Lounes, yaçine, Kamel, Hamid, Karim.

A mes chères sœurs : Malika, Saliha, Dalila.

A mes cousins et cousines.

A tous mes ami(e)s qu'à tous ce qui me sont chers

Et a tous ceux qui m'ont aidé et tous ceux qui m'ont connu de près et de loin.

TITOUCHE Ali

Liste des figures

Liste des tableaux :

Sommaire

Chapitre II : Transmission et supports

Chapitre III : Méthode d'évaluation de la transmission de flux d'information

Introduction générale

Introduction générale :

L'histoire des réseaux et des télécommunications pourrait se résumer à une perpétuelle course au débit ou à ce que l'on appelle aussi largeur de bande. Pour supprimer la distance, il faut transporter une quantité toujours plus grande d'information sur des distances de plus en plus importante.Or, on constate que plus les distances sont grandes plus les débits disponible sont faible.

Abolir les distances, c'est lutter contre ces lois et pénaliser le moins possible le débit, et réaliser le vieux rêve des réseaux : transférer aussi vite des informations entre deux ordinateurs situées a 200 km l'un de l'autre qu'à l'intérieure d'un ordinateur.

Empruntant d'abord des lignes terrestres de télécommunication, essentiellement composées de fils de cuivre, l'information s'est ensuite également propagée par le biais des ondes hertziennes et de la fibre optique. Il convient d'ajouter a ces lignes de communication le réseau d'accès, aussi appelé la boucle locale, permettant d'atteindre l'ensemble des utilisateurs potentiels.

Actuellement, tout le monde veut y partager des informations, s'informer et télécharger, sans forcément se soucier de ce que cela implique au niveau de leur réseau. Souvent, les personnes dépassent leur capacité de bande passante ce qui implique un ralentissement de leur ordinateur. [1]

Tout d'abord, il faut savoir que la bande passante est la taille du canal dans lequel vont transiter les informations, plus la bande passante est grande, plus le débit qui y transite peut être élevé. On dit en général que le débit maximum est égal à la taille de la bande passante.
Une diminution du débit maximum est provoquée par la bande passante. En effet, on ne peut pas transmettre les données à une vitesse supérieure à celle de la bande passante. A tout cela s'ajoute la latence (temps nécessaire pour véhiculer un paquet au travers d'un réseau). Si la bande passante de notre réseau est saturée, une congestion à de fortes chances de se produire et la latence va alors augmenter. Cependant, si la bande passante n'est pas submergée, la latence restera alors la même. [1]

Il faut aussi tenir compte de la gigue (jitter en anglais) qui va nous indiquer la variation du délai de transmission des paquets et permettre de savoir si la latence est stable.

Notre travail consistera donc à bien comprendre comment détecter une augmentation du trafic(flux) qui provoque un ralentissement global de réseau. Pour ce faire, nous allons utiliser l'outil de mesure de la bande passante Iperf qui nous permettra à nous fournir des résultats sur le débit qui transite entre deux extrémités. Et aussi, mesurer la gigue et s'informer sur la perte des datagrammes lors d'une transmission.

Notre mémoire est organisé en quatre chapitres :

Dans le premier chapitre, nous avons donné des généralités sur les réseaux informatiques, leur classement selon l'étendu géographique, selon leur topologie physique et logique et selon l'architecture.

Dans le deuxième chapitre, nous avons présenté les éléments de base de la transmission, et les différentes caractéristiques des supports de transmissions tels que les supports métalliques (câbles coaxiaux, paire torsadées), et non métalliques (fibre optiques), qui permette ainsi la communication entre l'équipement informatique a distance les uns des autres.

Dans le troisième chapitre, nous sommes intéressés à les méthodes d'évaluations de la transmission, en présentant les différentes étapes d'acheminement d'un flux d'information en utilisant les différentes technologies tels que : la commutation circuit et paquet, commutation par cellule et le routage.

Enfin, dans le dernier chapitre, nous avons simulé avec le logiciel Iperf, et nous avons aussi effectué des différents tests entre le centre du réseau informatique de Hasnoua et les différents départements. Donc l'objectif de notre étude est de vérifier la quantité d'information qui transite dans un canal et de s'informer sur la bande passante disponible lors d'une transmission.

Chapitre I : Généralités sur les réseaux

1.1. Préambule :

Dans ce chapitre nous allons présenter les éléments de base d'un réseau informatique, ensuite nous allons montrer comment on peut classer ses différents réseaux selon leur étendue géographique, topologie et architecture.

Selon l'entendue on trouve les réseaux PAN, LAN, MAN et WAN. Selon l'architecture on trouve principalement deux architecture : architecture client/serveur et l'architecture poste a poste. Après nous allons interpréter et analysé ces différentes topologies tel que la topologie physique et la topologie logique.

1.2. Généralitéssur les réseaux :

Un ordinateur est une machine permettant de manipuler des données. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations.

La nécessité de communication et de partage des informations en temps réel, impose aujourd'hui aux entreprises la mise en réseau de leurs équipements informatique en vue d'améliorer leurs rendements.

1.2.1. Définition d'un réseau informatique :

Un réseau informatique est un ensemble d'équipement matérielles et logiciels interconnectés les un avec les autres dans le but de partager des ressources (donné).ces équipements peuvent êtres éloigner ou rapprochés.

Suivant l'éloignement (la taille du réseau) entre ces équipements, on distingue les réseaux suivant :

- **Les réseaux personnels**
- **Les réseaux locaux**
- **Les réseaux métropolitains**
- **Les réseaux étendus**

1.2.2. Classement selon l'étendu géographique :

En fonction de leur étendue géographique et de leur taille (en termes de nombre de machines), on distingue plusieurs types de réseaux :

1.2.2.1. Les réseaux personnels (Personal Area Network) :

Egalement appelé réseau domestique, un réseau personnel désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètre autour d'un utilisateur. Ce type de réseau sert généralement à relier des périphériques tels qu'imprimante, téléphone portable, appareils domestique à un ordinateur personnel. La liaison avec ces périphériques peuvent être câblées ou sans fil (par Bluetooth).

Figure 1 : réseau personnel PAN

1.2.2.2. Les réseaux locaux (Local Area Network) :

De taille supérieure, s'étendant sur quelque dizaines à certaine de mètres, un réseau local relie entre eux des ordinateurs appartenant à une même organisation et situé dans une même salle, un même bâtiment ou un même terrain. Un tel réseau peut reposersur différentes technologies (câblés ou wifi) la plus répondue étant **Ethernet**.

Du fait de la faible dimension de ce type de réseau, les délais de transmission sont courts avec peu d'erreurs, ce qui a l'avantage d'en simplifier l'administration. Couramment utilisé pour le partage de ressources communes, comme des périphériques, des données ou des applications, un réseau local bénéficie d'une vitesse de transfert de données entre 10 Mbit/s et 1 Gbit/s. La taille d'un tel réseau peut atteindre jusqu'à 100 voire 1000 utilisateurs.

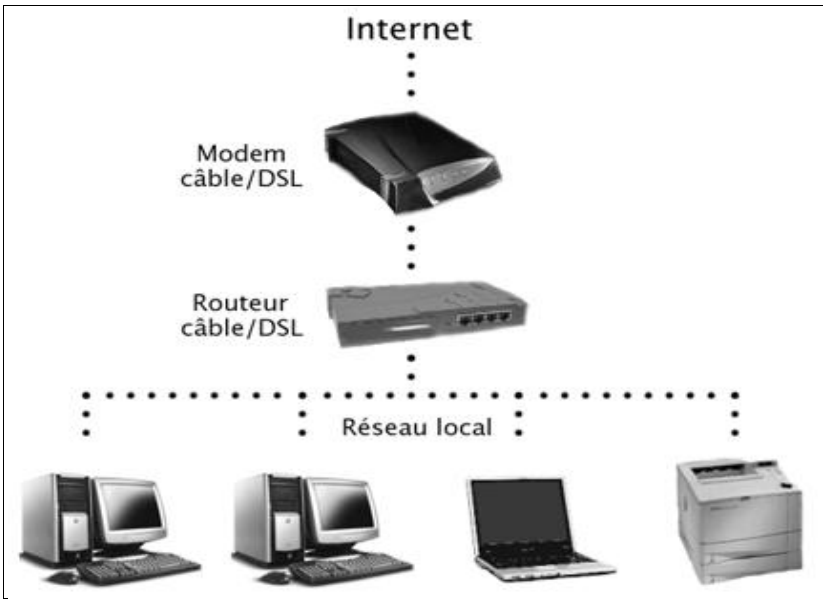


Figure 2 : réseau local LAN

1.2.2.3. Les réseaux métropolitains (Metropolitan Area Network):

Un réseau métropolitain, également nommé réseau fédérateur, assure des communications sur de plus long distances, interconnectant souvent plusieurs réseaux LAN avec des débits plus importants. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments, distants de quelques dizaines de kilomètres. Ainsi, un MAN permet à deux nœuds distants de communiquer comme s'il faisait partie d'un même réseau local. Un MAN est formé de commutateurs et de routeurs interconnectés par des liens à haut débit généralement en fibre optique.

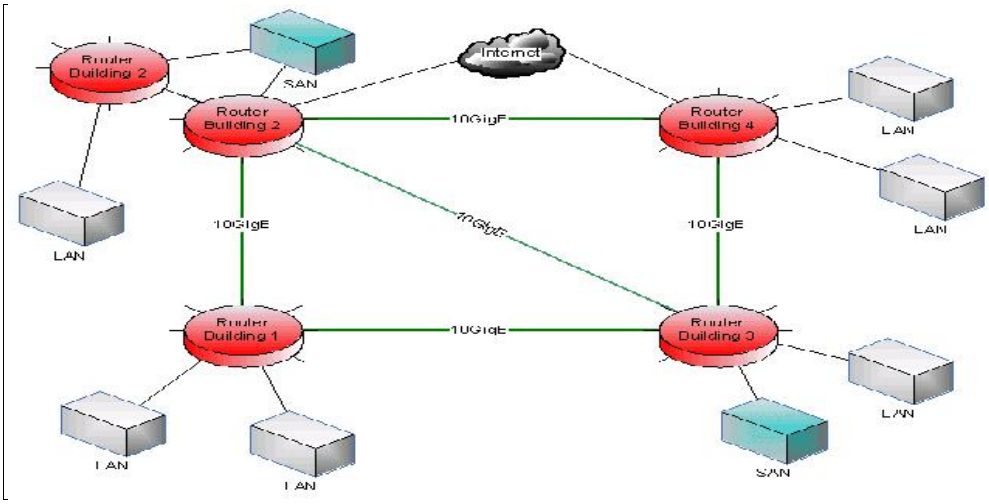


Figure 3 : réseau métropolitain MAN

1.2.2.4. Les réseaux étendu (Wide Area Network) :

Constitués d'interconnexions de LAN, voire de MAN, les réseaux étendues sont capables de transmettre des informations sur des milliers de kilomètres à travers le monde entier par le biais de routeurs et de liaisons nationales ou internationales à très haut débit, appelées épines dorsale (backbon). Puisque la majeure partie du trafic d'un WAN se situe dans les LAN qui le constituent, les routeurs sont investis d'une mission importante : contrôler le trafic. Ils doivent être paramétrés avec des informations appelées routes qui leur indiquent comment acheminer des données entre réseaux. En outre, l'épine dorsale est un ensemble de lignes téléphoniques très rapides utilisées par les opérateurs de télécommunications pour transmettre de gros volumes de trafic.

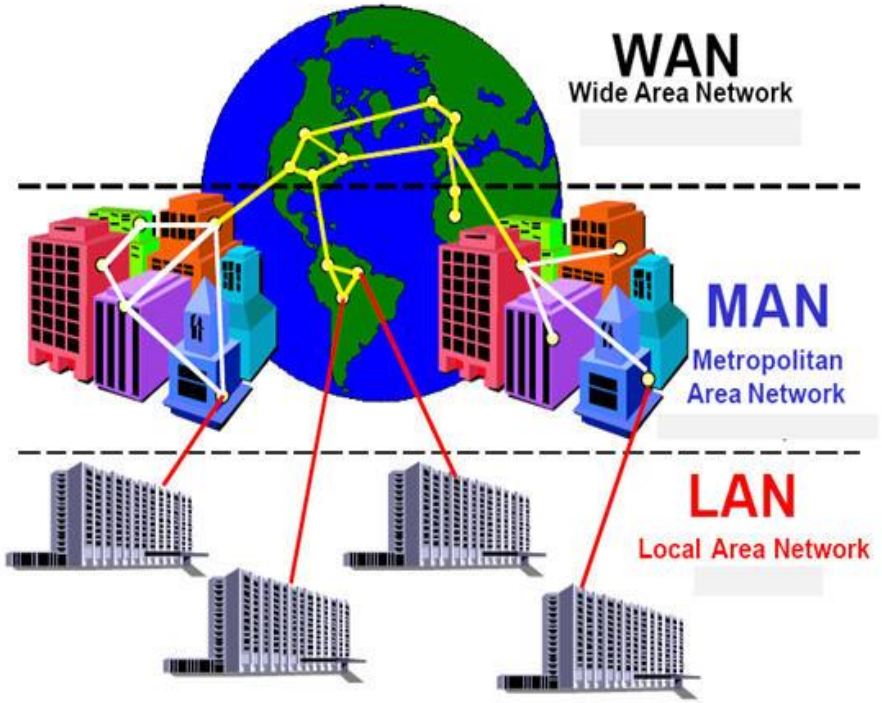


Figure 4 : réseau étendu WAN

1.2.3. **Classement selon la topologie :**

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles, fibre optique, ondes hertzien…) et des éléments matériels (cartes réseaux ainsi que d'autre équipements permettant d'assurer la bonne circulation des données).

La topologie du réseau décrit la manière dont les éléments d'un réseau sont disposés les uns par rapport aux autres. Celle-ci habituellement décomposée en topologie physique et topologie logique.

La topologie physique d'un réseau décrit la configuration spatiale ainsi que l'organisation des connexions physiques entre les éléments du réseau. Bien que tous les réseaux installés de nos jours soient à topologie en étoile ou en anneau, le nombre de réseaux existant qui s'appuient sur l'ancienne topologie en bus n'est pas négligeable. Une topologie logique est la structure logique d'une topologie physique, c'est-à-dire que la topologie logique définit comment se passe la communication dans la topologie physique.

1.2.3.1. **Topologie en bus :**

Une topologie en bus est l'organisation la plus simple d'un réseau. En, effet dans une telle topologie, tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble. Le mot « bus » désigne la ligne physique qui relie les machines du réseau. Une trame envoyé par l'ordinateur « A » prend le bus et part en direction des deux arrêts terminus de la ligne. Une copie de la trame descend à chaque arrêt de bus, les ordinateurs à qui la trame n'est pas destinée l'ignorant. Si la trame arrive à l'arrêt terminal, celle-ci est terminée.

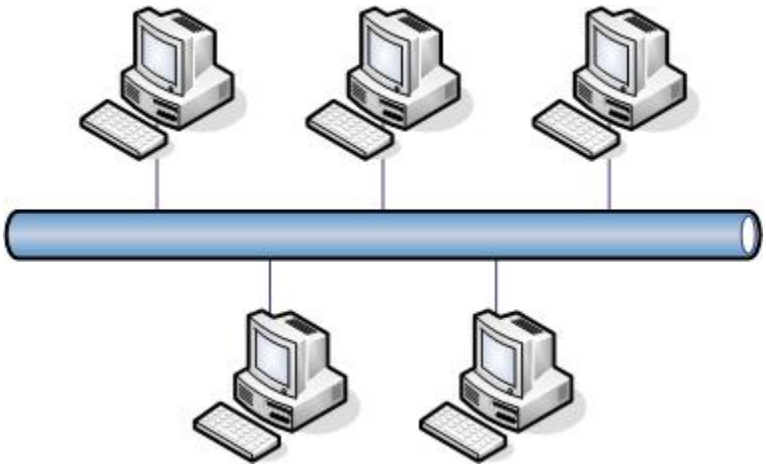


Figure 5 : Topologie en bus

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau est affecté. En outre, deux

trames expédiées simultanément par deux ordinateurs différents peuvent entrer en collision et être supprimées, les ordinateurs les ayant expédiés devant les réexpédiés. Dés lors, plus il y a d'ordinateurs connectés et donc de trafic, plus le nombre de collisions augmente, ralentissant par conséquent la vitesse du trafic.

Cette topologie adopte les règles de communications basées sur la norme CSMA/CD. Quand un ordinateur décide de transmettre un paquet d'information, il écoute sur le bus. Si le bus est déjà utilisé, il attend qu'il devienne disponible ; en revanche, s'il est libre, l'ordinateur transmet immédiatement. Si deux ou plusieurs stations de travails transmettent simultanément sur le bus, qui leur paraissait disponible, il y a collision. Toutes les stations victimes d'une collision arrêtent immédiatement, observent un délai d'attente de durée aléatoire et renouvèlement leur tentative de transmission ultérieurement.

1.2.3.2. Topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central qui est le plus souvent un concentrateur (Hub) ou un commutateur (Switch). Il s'agit d'une boite comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions. La plupart des réseaux actuels sont fondés sur une variante ou un autre de cette topologie.

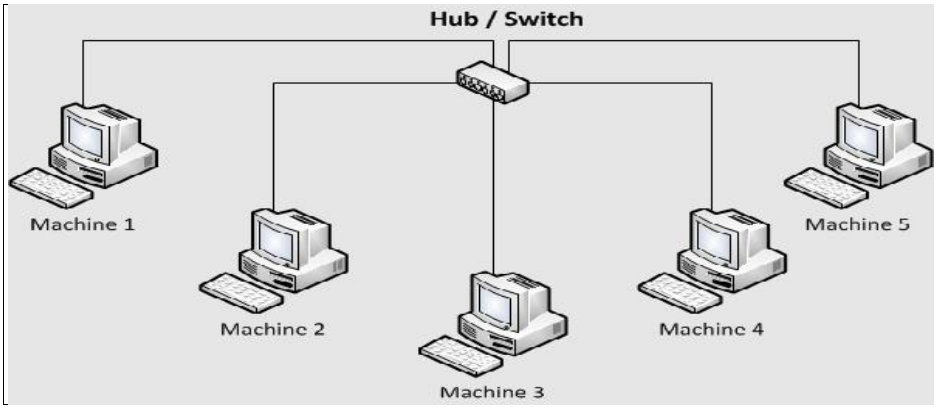


Figure 6 : Topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseauest le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est

possible. En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire : le concentrateur.

1.2.3.3. Topologie en anneau :

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent à tour de roule. Chaque nœud fait office de récepteur dans la circulation des informations : un ordinateur reçoit un paquet d'informations et le relaie à son voisin direct, les informations ne circulant dans l'anneau que dans un sens.

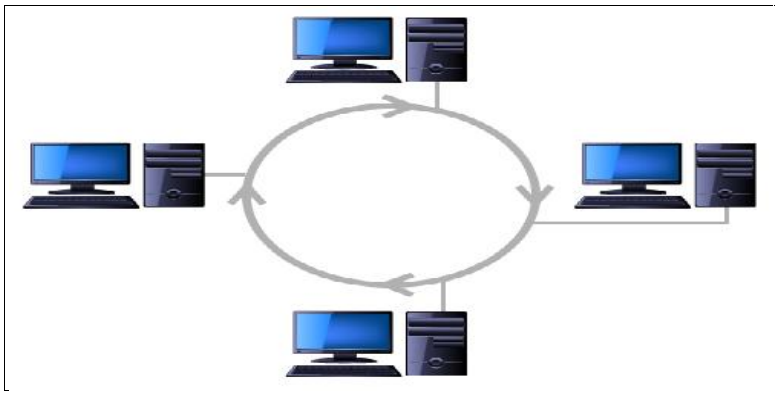


Figure 7: Topologie en anneau

Dans la topologie en anneau à jeton, une trame contenant un jeton circule en permanence dans l'anneau. Un ordinateur désirant envoyer une information retire le jeton de la trame et y place l'information à envoyer. Lorsque la trame arrive à l'ordinateur de destination, celui-ci extrait de la trame l'information lui étant adressé et place dans la trame en circulation un accusé de réception à l'intention de l'expéditeur. Une fois que l'expéditeur reçoit l'accusé de réception, il replace le jeton sur l'anneau qui passe à l'ordinateur suivant. En cas de trafic important, la topologie en anneau est plus efficace qu'une topologie en bus dans la mesure où elle présente une absence de collision de trames. Par contre, une telle topologie est plus vulnérable à une panne généralisée en cas de panne d'un des ordinateurs et doit être interrompu complètement en cas de reconfiguration du réseau par l'ajout ou la suppression d'un ordinateur.

1.2.3.4. Topologie maillée :

Une topologie maillée est une évolution de la topologie en étiole puisqu'elle correspond à plusieurs liaison point à point mais décentralisé. Une unité réseau peut avoir (1, N)

connexion point à point vers plusieurs unités. Chaque terminal est relié à tous les autres de manière indirect si le maillage est complet et de manière indirecte si le maillage est partiel, engendrant dans les deux cas un nombre élevé de liaisons. Dans le cas d'un maillage partiel, un ordinateur recevant un paquet d'information ne lui étant pas destiné joue le rôle d'intermédiaire et l'expédié plus loin.

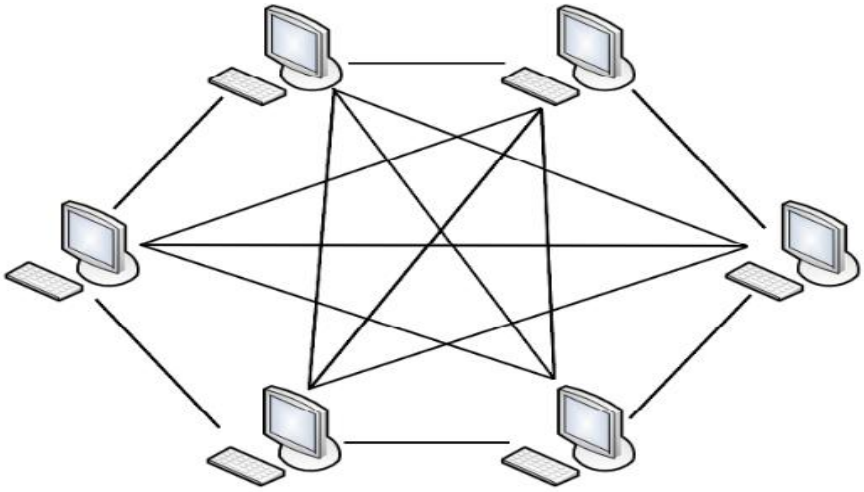


Figure 8: Topologie maillée

Cette topologie se rencontre dans les grands réseaux de distribution. L'information peut parcourir le réseau suivant des itinéraires divers grâces à des méthodes de routage reparties. L'armée utilise également cette topologie dont l'organisation décentralisée assure qu'en cas de rupture d'un lien, l'information soit tout de même acheminée.

1.2.4. Classement selon l'architecture :

L'architecture d'un réseau peut être construite sur le paradigme client-serveur ou poste à poste (peer to peer).

1.2.4.1. Architecture client-serveur :

Selon le paradigme, un ordinateur connecté à un réseau peut jouer deux rôles différents et complémentaires : le client ou le serveur.

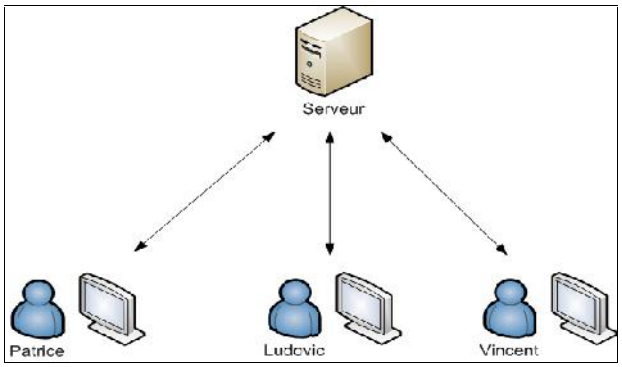


Figure 9 : Architecture client-serveur

Les machines clientes d'un réseau contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée- sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion… etc. Les services sont exploités par des programmes, appelées programmes clientss'exécutent sur les machines clientes et capables de traiter des informations récupérées auprès d'un serveur (client FTP, client de messagerie). Le schéma de fonctionnement de l'architecture client-serveur est le suivant : le client émit une requête vers le serveur grâce à son adresse IP et le numéro du port du service à contacter. Le serveur reçoit la demande, la traite et répond au client à l'aide de son adresse IP et le numéro de port du programme client.

Ainsi, un serveur web héberge des ressources du Web accessible à l'aide d'un navigateur client alors qu'un serveur d'impression permet de partager une ou plusieurs imprimantes entre plusieurs clients situés sur un même réseau les en placent dans des filles d'attentes puis en les envoyant petit à petit à l'imprimante.

Les avantages du modèle client-serveur :

Les atouts principaux du modèle client-serveur sont les suivants :

- **Des ressources centralisées :** étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tout les utilisateurs, comme par exemple une base de données centralisé, afin d'éviter les problèmes de redondances et de contradiction.
- **Une meilleure sécurité :** le nombre de points d'entrée permettant l'accès aux données est moins important.

- **Une administration au niveau serveur :** les clients ayant peu dans ce modèle ont moins besoins d'être administré.
- **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 majeur.

L'approche client-serveur est donc prépondérante dans les réseaux de grandes et moyennes entreprises non seulement pour des raisons de fiabilités et de capacité de montée en charge mais également pour répondre à deux autres critères qui ont un impact financier important : la sécurité des données et la centralisations de l'administration.

1.2.4.2. Architecture poste à poste :

A l'autre bout du spectre des possibilités, l'architecture poste à poste permet à toutes les stations de travail clientes de jouer le rôle de serveur. Par exemple une machine qui dispose d'un gros disque dur peut le partager avec les autres stations.

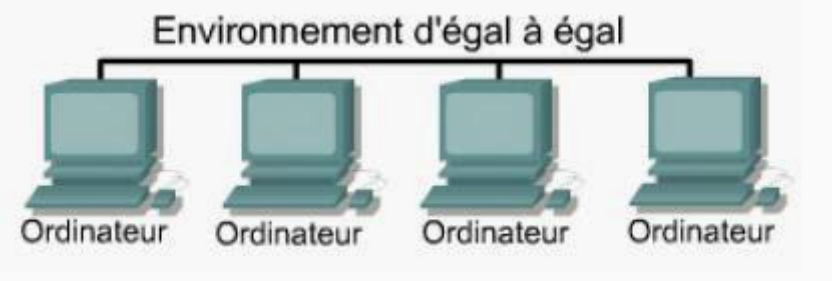


Figure 10 : architecture poste à poste

Dans un tel réseau, il n'y a pas de serveur dédié et tous les ordinateurs peuvent être utilisés en tant que stations de travail. Ainsi un ordinateur relié à une imprimante pourra la partager afin que tous les autres ordinateurs puissent y accéder via le réseau. Parmi les services poste à poste traditionnels, nous relèverons le partage de fichier (bit torrent), la communication(Skype).

Les avantages du modèle posteà poste :

Les atouts principaux du modèle poste à poste sont les suivants :

- La panne d'un ordinateur du réseau n'entraine pas la paralysie de tout le réseau de par la décentralisation de l'architecture.

- Un tel réseau est facile à installer et à configurer.
- Il est moins cher qu'un réseau client-serveur.

Cependant, un réseau poste à poste présente plus d'inconvénients que d'avantages :

- Il manque complètement de contrôle centralisé, ce qui le rend ingérable.
- Il est particulièrement non sécurisé : la sécurité est quasi inexistante.
- Le stockage de fichiers illégaux sur les clients et leur diffusion sur internet engendre des risques de sanctions pénales et civiles.

Ainsi les réseaux poste à poste ne sont valables que pour un petit nombre d'ordinateurs et pour des applications ne nécessitant pas une grande sécurité.

1.2.5. Classement selon la topologie logique :

La topologie logique, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Il s'agit de l'ensemble des règles qui décrivent l'organisation des chemins suivis par l'information passant d'un composant du réseau à un autre. Les topologies les plus courantes sont Ethernet, Token Ring et FDDI.

1.3. Réseaux locaux : (Ethernet et Token Ring)

1.3.1. Réseau Ethernet :

Ethernet est une technologie universelle qui dominait déjà les réseaux locaux bien avant ledéveloppement de l'internet. La clé de la longévité de cette technologie, c'est sa simplicité.

Le réseau Ethernet est basé sur le principe que l'émission d'une trame se fait dans les deux sens sur le bus afin que toutes les stations connectées au réseau puissent la recevoir. Il est basé sur le mode d'accès CSMA/CD, ce qui signifié détection de porteuse et accès multiple avec détection de collision.

Les fonctions principales réalisées de CSMA/CD sont :

- Que l'ensemble des stations on les même droit d'accès au réseau.
- Que chaque station écoute le réseau avant d'émettre, en détectant la présence d'une porteuse et donc d'une autre émission.

- Que chaque station après avoir émit vérifié que le signal généré n'est pas entrés en collision avec un autre. Ceci est réalisé, par le transceiver en vérifiant que le signal, présent sur le média, n'a pas une trop grande amplitude.

1.3.1.1. Fonctionnement et normalisation du mode d'accès CSMA/CD :

Le réseau Ethernet a une topologie en bus et donc toutes les stations sont connectées en parallèle sur le même support. Une trame émise de façon bidirectionnelle, par une station est donc reçu par l'ensemble des postes du réseau.

1.3.1.2. Délai inter trame :

Ce délai est respecté lorsque que la même station émet consécutivement deux trames.

Elle permet la réinitialisation des processus des couches 1et 2, et la stabilisation des signaux électrique sur le média. Ce délai selon la norme 802.3 est de 96 bit-times, le bit-times est l'unité du temps utilisés par la norme 802.3. Cette unités représente le temps nécessaire que met une station pour emmètre un bit, par exemple pour un débit de 10 Mb/s, ce temps est de 0.1 micro second.(durée d'un bit)

1.3.1.3. Détection de collision :

La détection d'une porteuse était simple, la détection d'une collision l'est moins.

On considère que nous avons la topologie de réseau suivant :

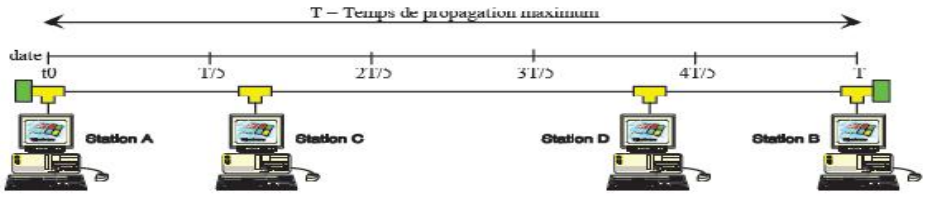


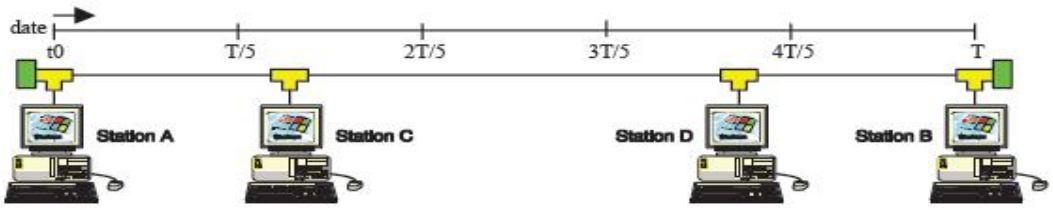
Figure 11 : L'émission avec le mode CSMA/ CD

Les deux stations A et B étant les stations d'extrémité du réseau.

Figure 12 : les différents états utilisés avec le mode CSMA/CD

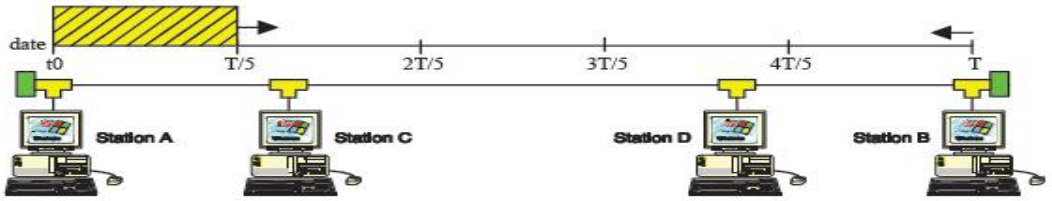
1er étape :

La station A veut émettre une trame vers la station D. Elle commence par vérifier que le média est libre, c'est le cas. Elle commence à émettre sa trame.



2éme étape :

A la date T/5, la station B veut émettre une trame vers la station A. Elle commence par vérifier que le média est libre, ce qui est le cas puisque la trame provenant de la station A n'est pas encore arrivé à son niveau.

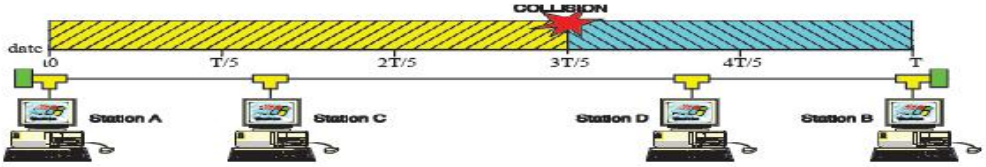


3éme étape :

A la date 2T/5 A et B émettent simultanément.

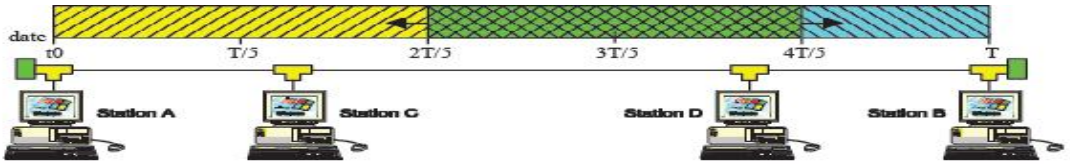
4éme étape :

A la date 3T/5, les deux trames se rencontrent, il y a collision.



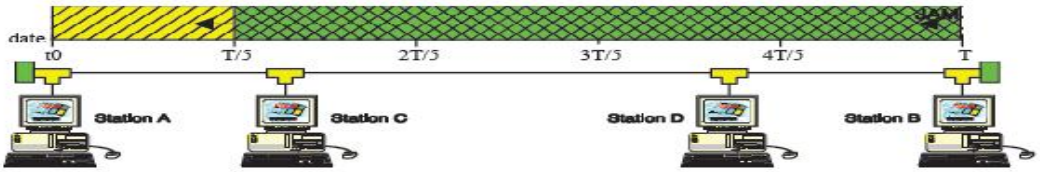
5éme étape :

A la date 4T/5, malgré la collision les trames, qui sont maintenant altérés, continuent à se propager sur le média. Les stations continuent à émettre, car elles n'ont toujours pas détecté la collision, puisque les trames altérées ne leur sont pas encore parvenues.



6éme étape :

A la date 5T/5, la station B détecte la collision. Alors elle annule son émission d'une trame, puis elle met un JAM. Le JAM est un ensemble de 32 bits de renforcement de collision afin d'informer l'ensemble des stations présentes sur le réseau qu'il y à une collision.



7éme étape :

A la date 6T/5, la station A détecte la collision, alors elle aussi annule son émission et émit un JAM.

8éme étape :

A la date 7T/5 la station D est informée de la présence d'une collision. Elle déduit que la trame qu'elle était entrain de traiter n'est plus exploitable, et donc elle arrête ce traitement.

9éme étape :

Après que toutes les stations soit informer (il faut que le JAM circule sur l'ensemble du réseau), toutes les stations arrêtent leurs émissions pendant une durée aléatoire. Après cette attente les stations se remettent en position d'émission. [2]

1.3.1.4. Différentes normes du réseau Ethernet :

Norme	Débit	Type de transmission	Média
10 base T	10Mbits/s	Bande de base	Paire torsadé
10 base 5	10Mbits/s	Bande de base	Câble coaxial de longueur max 500m
100 base-fx	100Mbits/s	Bande de base	Fibre optique multi mode de longueur max 2 km
1000 base Lx	1000 Mbit/s	Bande de base	Fibre optique monomode de longueur max 3km

Tableau 1 : différentes normes du réseau Ethernet

1.3.2. Réseau Token Ring :

Les réseaux Token Ring sont implémentés dans une topologie en anneau. La topologie physique Token Ring est la topologie en étoile, dans laquelle tous les ordinateurs du réseau sont physiquement connectés a un concentrateur appelé MSAU (MultisationAcces Unit).

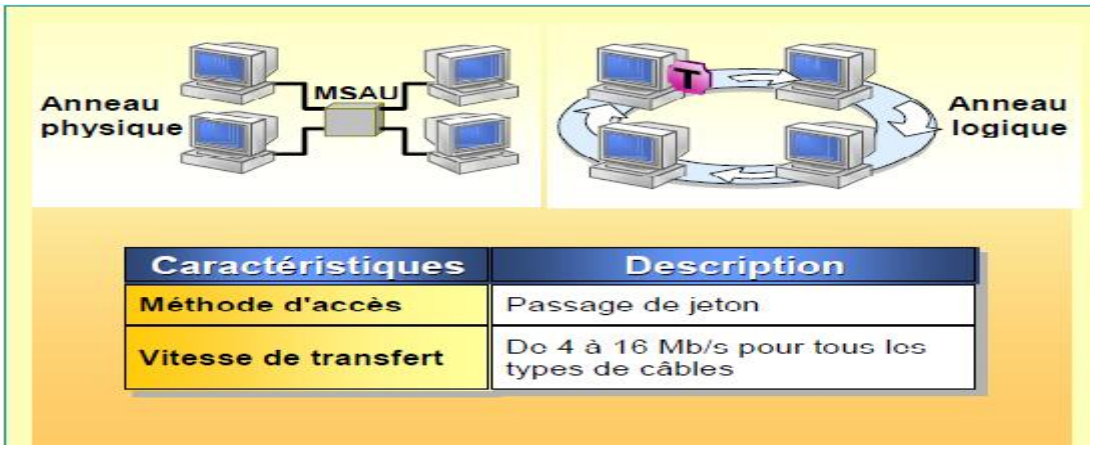


Figure 13 : réseau Token Ring

1.3.2.1. Méthode d'accès :

La méthode d'accès utilisé dans un réseau Token Ring est le passage du jeton. Un jeton est une séquence spéciale des bits qui transite sur l'anneau.

Un ordinateur ne peut pas transmettre des donnés tant qu'il n'a pas en possession du jeton, tant que se jeton est utilisé par un ordinateur, les autre ordinateur ne peuvent pas transmettre.

Lorsque le premier ordinateur de l'anneau se retrouve en ligne, le réseau génère un jeton. Ce jeton transite sur l'anneau jusqu'à ce que l'un de ces ordinateurs prenne le contrôle du jeton.

Cet ordinateur envoie alors une trame de données sur le réseau. Cette trame parcoure l'anneau jusqu'à ce qu'il atteigne l'ordinateur dont l'adresse correspond à l'adresse de destination de la trame. L'ordinateur destinataire copie la trame en mémoire et la marque pour indiquer que les informations ont été reçues.

La trame continue à parcourir l'anneau jusqu'à l'ordinateur expéditeur, sur laquelle la transmission est réussie. L'ordinateur qui a transmis les données retire alors la trame de l'anneau, et envoie sur celui-ci un nouveau jeton.

1.3.2.2. Vitesse de transfert :

La vitesse de transfert d'un réseau Token Ring est comprise entre 4 et 16 Mbit/s.

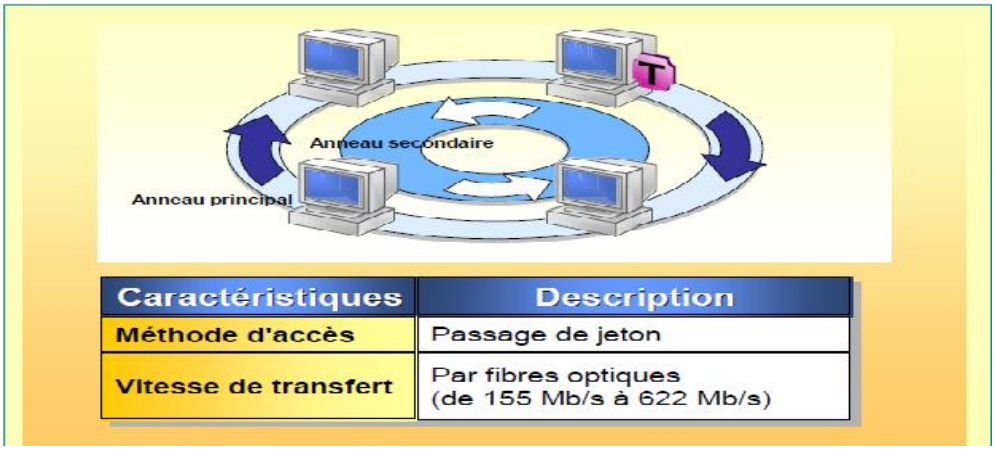
1.4. Réseaux métropolitains :

1.4.1. Réseau FDDI :

Le réseau FDDI (FiberDistributed Data Interface) est un réseau MAN il permet l'interconnexion de réseaux locaux. Un réseau FDDI peut prendre en charge plusieurs réseaux locaux de faible capacité nécessitant une dorsale rapide.

Ce type de réseaux est composé de deux flux de données similaire, transitant dans des directions opposés sur deux anneaux. L'un de ces anneau est appelé anneau principal et l'autre anneau secondaire. En cas de problème avec l'anneau principal, par exemple une

défaillance de l'anneau ou rupture de câble, l'anneau se reconfigure en transférant les données sur l'anneau secondaire, qui continue à transmettre.



Caractéristiques	Description
Méthode d'accès	Passage de jeton
Vitesse de transfert	Par fibres optiques (de 155 Mb/s à 622 Mb/s)

Figure 14 : réseau FDDI

Le réseau FDDI permet l'interconnexion jusqu'à 1000 station de travail formant ainsi un réseau étendu sur 100 Km dont le support physique est la fibre optique le plus souvent la multimode, mais aussi monomode. Les stations doivent être éloignées les unes des autres au maximum de 2Km.une version du FDDI en paire torsadées existe, il est nommée TPDDI, et elle autorise un débit 100 Mbit/s sur un anneau de 100m.

1.4.1.1. Méthode d'accès :

La méthode d'accès utilisée dans un réseau FDDI est le passage de jeton. Sur un réseau FDDI, un ordinateur peut transmettre autant de paquets qu'il peut en générer dans un délai prédéfini avant de restituer le jeton. Dés qu'il a fini de transmettre, ou dés que son délai de transmission est écoulé, il restitue le jeton.

Comme l'ordinateur restitue le jeton dés qu'il a fini de transmettre, plusieurs paquets peuvent circuler sur l'anneau en même temps. Cette méthode de passage de jeton est plus efficace que celle d'un réseau TOKEN RING traditionnelle, qui ne permet de faire circuler qu'une seul trame à la fois. Elle autorise également un débit de données plus élevé pour une même vitesse de transfert.

1.4.1.2. Vitesse de transfert :

La vitesse de transfert d'un réseau FDDI est comprise entre 155 et 622 Mbit/s.

1.5. Conclusion :

Ce chapitre présente les éléments de base du réseau informatique, et montre comment on peut classer les différents types de réseaux selon leur étendue, topologie et l'architecture.

Selon l'étendue on trouve les réseaux PAN qui sont limités à une distance de 10 mètres et les réseaux LAN qui peuvent atteindre les centaines de mètres.

Pour le réseau MAN il peut regrouper plusieurs réseaux LAN avec des débits plus importants et enfin les réseaux WAN qui sont capable de transmettre des informations sur des milliers de kilomètres à travers le monde entier.

Selon l'architecture on trouve l'architecture client server et poste à poste. L'architecture client serveur est utilisée dans des réseaux grands et moyens entreprise pour des raisons de fiabilité. Ainsi les réseaux poste à poste ne sont valable que pour un petit nombre d'ordinateurs et pour des applications qui ne nécessitant pas une grande sécurité.

Selon la topologie on distingue deux catégories : la topologie physique et logique. La topologie physique qui désigne l'organisation des connexions physique entre les éléments du réseau. La topologie logique représente la façon dont les données transitent dans les lignes de communication.

Chapitre II : transmission et supports

2.1. Préambule :

Dans ce chapitre nous allons présenter les éléments de base d'une transmission et nous allons aussi montrer comment les signaux électriques ou liminaux se propagent dans des supports comme les câbles ou les fibres optique afin d'assurer une communication entre les équipements informatiques.

En suite, nous allons présenter les différentes caractéristiques de ces supports de transmission et les technique utilisé lors d'une transmission de donné tel que la transmission en bande de base.

2.2. Transmission de données :

2.2.1. Généralité sur la transmission de données :

Les réseaux sont nés du besoin de transporter une information d'une personne à une autre. Pendant longtemps, cette communication s'est faite directement par l'homme, comme dans le réseau postal ou par des moyens sonores ou audiovisuels. Il y a un peut plus d'un siècle, la première révolution des réseaux consisté à automatiser le transport des données.

Empruntant d'abord des lignes terrestres de télécommunications, essentiellement composées des files de cuivre, l'information s'est ensuite également propagée par le biais des ondes hertziennes et de la fibre optique.

Aujourd'hui, on peut dire qu'un réseau est un ensemble d'équipements et de liaisons de télécommunications autorisant le transport d'une information quelle qu'elle soit, d'un point à un autre, où qu'il soit.

2.2.2. Rappels de théorie du signal :

Un signal est une information qui transite à travers un canal de communication. Il permet de transmettre une donnée brute entre deux machines de manière adaptée au support de transmission.

Un signal s(t) peut se présenter sous différentes formes : analogique ou numérique.

2.2.2.1. Signal analogique :

Dans un signal analogique, tel que celui en usage pour la diffusion radio et TV, les informations voyage sous forme d'onde continûment variable .Comme le montre l'illustration suivante.

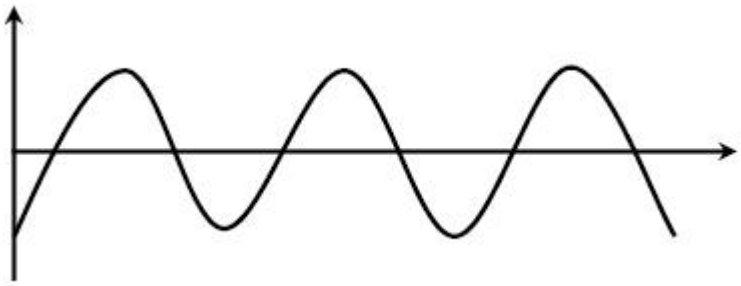


Figure 15 : Exemple de signal analogique

2.2.2.2. Signal numérique :

Lorsque on a faire a des signaux numériques, on est en face des signaux plus simples, dans la mesure où les informations circulent au moyens d'impulsions discrète (Active/désactive) sur un medium de communication. Par exemple, du courant peut être envoyé sur le fil électrique pour transmettre un ''1'' binaire, et l'absence du courant est équivalent à un ''0'' binaire. Un signal numérique rassemble à l'illustration suivante :

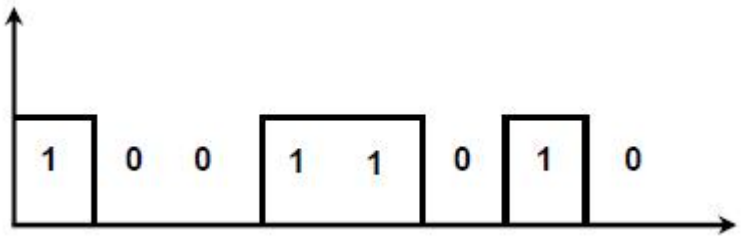


Figure 16 : Exemple de signal numérique

2.2.3. Caractéristiques des réseaux de transmission :

2.2.3.1. Notion de débit binaire :

Les systèmes de traitement de l'information emploient une logique à deux états ou binaire. L'information traitée par ceux-ci doit être traduite en symboles compréhensibles et manipulables par ces systèmes. L'opération qui consiste à transformer les données en éléments binaire s'appelle codage selon le type d'information à transformé.

On appelle débit binaire (**D**) le nombre d'éléments binaires, ou nombre de bits, émis sur le support de transmission pendant une unité de temps. C'est l'une des caractéristiques essentielles d'un système de transmission.

Le débit binaire s'exprime par la relation : **D = v/t.**

Avec **D** (débit) en bit par second (bit/s), V le volume à transmettre exprimé en bits et t la durée de la transmission en seconde.

Le débit binaire mesure le nombre d'éléments binaires transitant sur le canal de transmission pendant l'unité de temps (figure17).

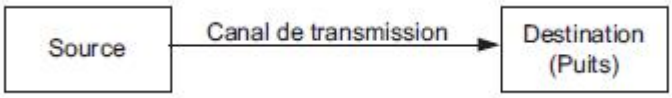


Figure 17: schématisation d'un système de transmission

2.2.3.2. Notion de rapport signal sur bruit :

Les signaux transmis sur un canal peuvent être perturbés par des phénomènes électriques ou électromagnétiques désignés sous le terme générique de **bruit**. Le bruit est un phénomène qui dénature le signal et introduit des erreurs.

Le rapport entre la puissance du signal transmis et celle du signal de bruit qualifié le canal vis-à-vis du bruit. Ce rapport est appelé rapport signal sur bruit (S/N) s'exprime en

dB (décibel).

$$S/N\ dB = 10 \log_{10} S/N(\text{en puissance})$$

2.2.3.3. Notion de taux d'erreur :

Les phénomènesparasites (bruit) perturbent le canal de transmission et peuvent affecter les informations en modifiant un ou plusieurs bits du message transmis, introduisant ainsi des erreurs dans le message. On appelle **Taux d'erreur binaire**(Te ou **BER**, Bit Error Rate) le rapport du nombre de bits reçus en erreur au nombre de bits total transmis. [3]

Te = nombre de bits en erreur / nombre de bits transmis

2.2.4. Classification en fonction du mode de contrôle de l'échange :

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

- Le sens des échanges.
- Le mode de transmission : il s'agit de nombre de bit envoyés simultanément.
- La synchronisation : il s'agit de la synchronisation entre l'émetteur et le récepteur.

2.2.4.1. Selon l'organisation des échanges :

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

a. La liaison simplex :

Caractérise une liaison dans laquelle les données circulent dans un 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 l'ordinateur vers l'imprimante ou de la souris vers l'ordinateur.

b.La liaison half –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.

c. La liaison full-duplex :

Caractérise une liaison dans laquelle les données circulent de façon bidirectionnelle et simultanément.

Ainsi, chaque extrémité de la ligne peut émettre et recevoir en même temps, ce qui signifie que la bande passante est devisée par deux pour chaque sens d'émission des données si un même support de transmission est utilisé pour les deux transmissions.

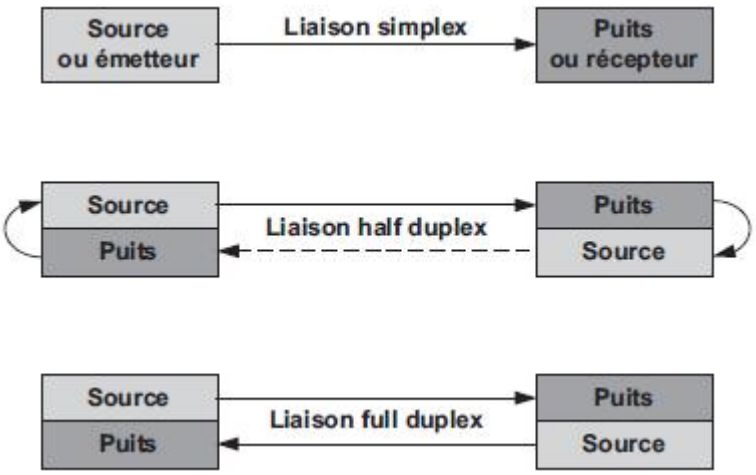


Figure 18: organisation des échanges

2.2.4.2. Selon le mode de liaison :

a. La liaison point à point :

Dans ce mode de liaison chaque correspondant est relié par un lien dédié à un seul autre correspondant. C'est le cas par exemple d'une liaison entre nœuds d'un même réseau ou entre un ordinateur et un terminal.

Figure 19 : La relation point à point

b. Les liaisons multipoints :

Une liaison est dite **multipoint** lorsqu'un même support est partagé par plusieurs nœuds. Dans ce cas, des conflits d'accès sont inévitables, il est nécessaire d'instaurer une politique d'accès au support. L'ensemble des mécanismes particuliers mis en œuvre, pour assurer le partage de l'accès au support, porte le nom de politique d'accès au canal on distingue deux modes de contrôle de l'accès selon la manière dont est gérée la politique d'accès : le mode centralisé ou maitre/esclave et le mode décentralisé ou d'égale à égale.

c. Le mode maitre/esclave :

Dans le mode de relation dit maitre esclave (figure 20) le primaire, généralement un ordinateur multiposte (mini ordinateur) est responsable de l'initialisation du dialogue, de la

récupération des erreurs et de l'organisation des échanges. Le transfert des données s'effectue selon la technique dite du **« polling /selecting »** (figure 21). Le maitre invite le terminal (secondaire) à émettre (polling) ou lui demande de passer en mode réception (selecting).

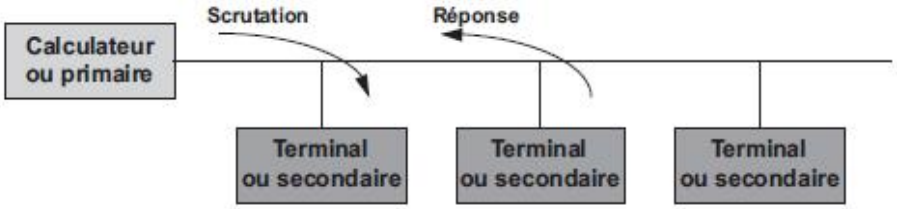


Figure 20 : la relation maitre/esclave

Dans de grandes configurations, le polling de toutes les stations peut demander beaucoup de temps. Pour améliorer le temps de réponse, on utilise la technique dite du polling lent et polling rapide. A l'initialisation, toutes les stations sont interrogées, ensuite uniquement celles qui ont répondu (polling rapide) ; périodiquement, toutes les stations sont de nouveau interrogé (polling lent).

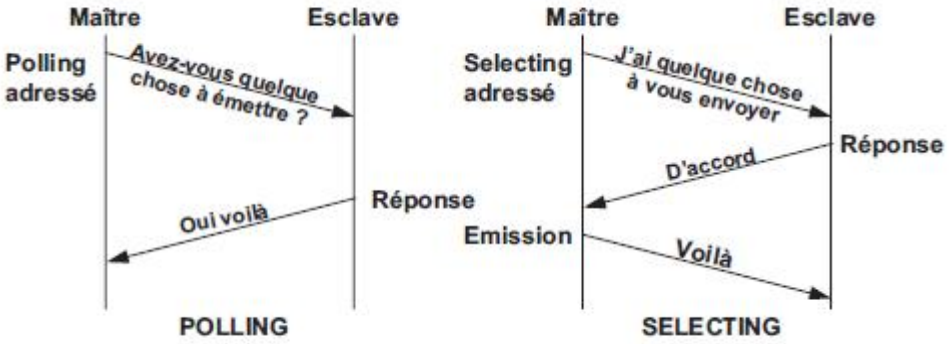


Figure 21 : polling /selecting

d. Le mode d'égale à égale :

Dans ce type de configuration, tous le calculateurs sont autorisés à émettre vers n'importe quelle autre calculateur et ce, à tout moment. Cet accès partagé peut donner lieu à des collisions ou contentions de messages (deux stations transmettent en même temps). Mais contrairement à la relation maitre/esclave, ici, chaque calculateur déroule un algorithme pour assurer le partage du support. [4]

2.2.5. Classification en fonction des paramètres physique :

2.2.5.1. Transmission série et parallèle :

Le mode de transmission désigne le nombre d'unités élémentaires d'informations (bits) pouvant être simultanément transmises par le canal de communication. En effet un processeur (donc l'ordinateur on générale) ne traite jamais (dans le cas des processeurs récents) un seul bit à la fois, il permet généralement d'en traiter plusieurs (8octet), c'est la raison pour laquelle la liaison de base sur un ordinateur est une liaison parallèle.

a. Transmission parallèle :

On désigne par liaison parallèle la transmission simultanée de N bits. Ces bits sont envoyés simultanément sur N voies différentes (une voie étant par exemple un fil, un câble ou tout autre support physique).

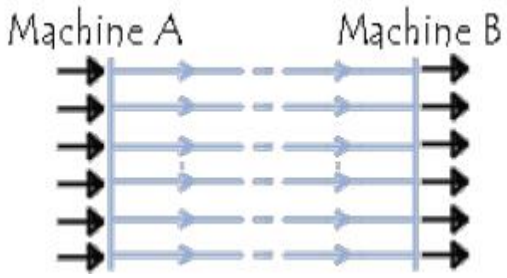


Figure 22 : liaison parallèle

Ces voies peuvent être :

- N lignes physiques : auquel cas chaque bit est envoyé sur une ligne physique, c'est la raison pour laquelle les câbles parallèles sont composés de plusieurs fils en nappe.
- Une ligne physique divisée en plusieurs sous-canaux par division de la bande passante, ainsi chaque bit est transmis sur une fréquence différente.

La transmission parallèle pose de nombreuses difficultés dont les principales sont le rayonnement des conducteur l'un sur l'autres (diaphonie) et la différence de vitesse de propagation entre les différents conducteurs (Delay skew) qui nécessitent la réalisation d'une électronique couteuse.

b. Transmission série :

En transmission série, tous les bits d'un mot ou d'un message sont transmis successivement sur une même ligne. 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 de récepteur.

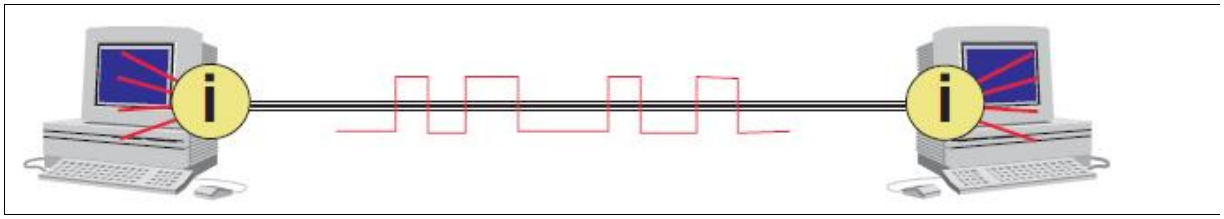


Figure 23 : transmission série

2.2.6Transmission synchrone et asynchrone :

Etant donné les problèmes que pose la liaison de type parallèle, c'est la liaison série qui est la plus utilisées. Toutefois, 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 a priori distinguer les caractères (ou même de manière plus générale les séquences de bits) car les bits sont envoyé successivement. Il existe donc deux types de transmission permettant de remédier à ce problème :

2.2.6.1. Transmission asynchrone :

La liaison asynchrone, dans laquelle 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'envoie d'une information de fin de transmission (appelée bit STOP, il peut éventuellement y avoir plusieurs bits STOP).

2.2.6.2. Transmission synchrone :

La liaison synchrone, dans laquelle émetteur et récepteur sont cadencés à la même horloge. Le récepteur reçoit de façon continue (même lorsque aucun bit n'est transmis) les informations

au rythme où l'émetteur les envoie. C'est pourquoi il est nécessaire qu'émetteur et récepteur soient cadencés à la même vitesse. De plus, des informations supplémentaires sont insérées afin de garantir l'absence d'erreurs lors de la transmission.

Lors d'une transmission synchrone les bits sont envoyés de façon successive sans séparation entre chaque caractère, il estdonc nécessaire d'insérer des éléments de synchronisation, on parle alors de synchronisation au niveau caractère.

Le principal inconvénient de la transmission synchrone est la reconnaissance des informations au niveau du récepteur, car il peut exister des différences entre les horloges de l'émetteur et du récepteur. C'est pourquoi chaque envoie de données doit se faire sur une période assez longue pour que le récepteur la distingue. Ainsi la vitesse de transmission ne peut pas être très élevée dans une liaison synchrone.

2.2.7. Principe d'une liaison de données :

Une transmission de données met en œuvre des calculateurs d'extrémité et des éléments d'interconnexion dont les appellations et fonctions sont codifiés (figure 24) :

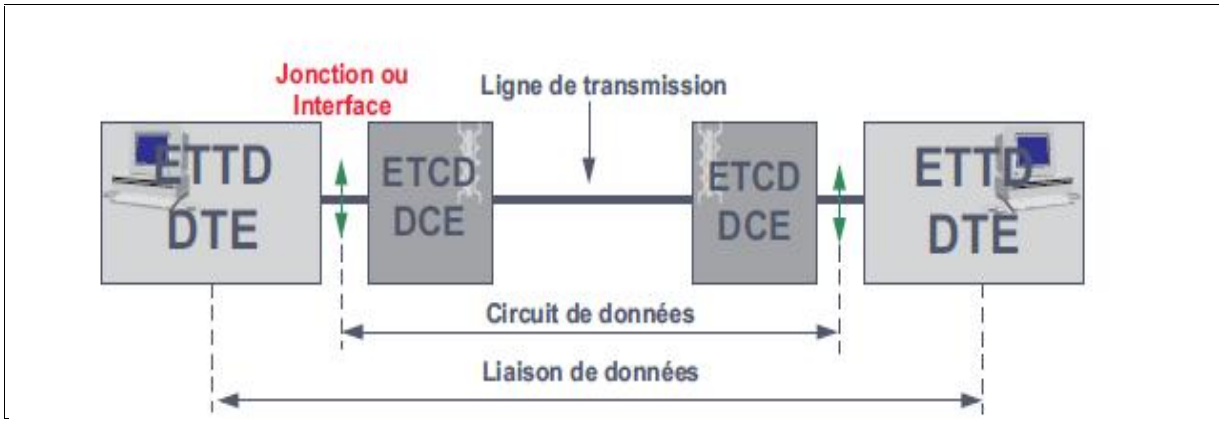


Figure 24 : constituant de base d'une liaison de données

On distingue :

Les équipements terminaux (end système) ou ETTD, Equipement Terminal de Traitement de Données, appelé aussi DTE (Data Terminal Equipement) représentant les calculateurs d'extrémité. Ces calculateurs sont dotés de circuits particuliers pour contrôler les communications. L'ETTD réalise la fonction de contrôle de dialogue.

Des équipements d'adaptation ou ETCD, Equipement Terminal de circuit de Données ou DCE (Data communication Equipement) réalisent l'adaptation entre les calculateurs d'extrémité et le support de transmission. Cet élémentremplit essentiellement des fonctions électroniques, il assure un meilleur transport sur la ligne de transmission. Il modifie la nature du signal, mais pas sa signification.

La jonction constitue l'interface entre ETTD (DTE) et ETCD (DCE), elle permet à l'ETTD de gérer l'ETCD pour assurer le déroulement des communications (établissement du circuit, initialisation de la transmission, échange de données et libérations de circuit).

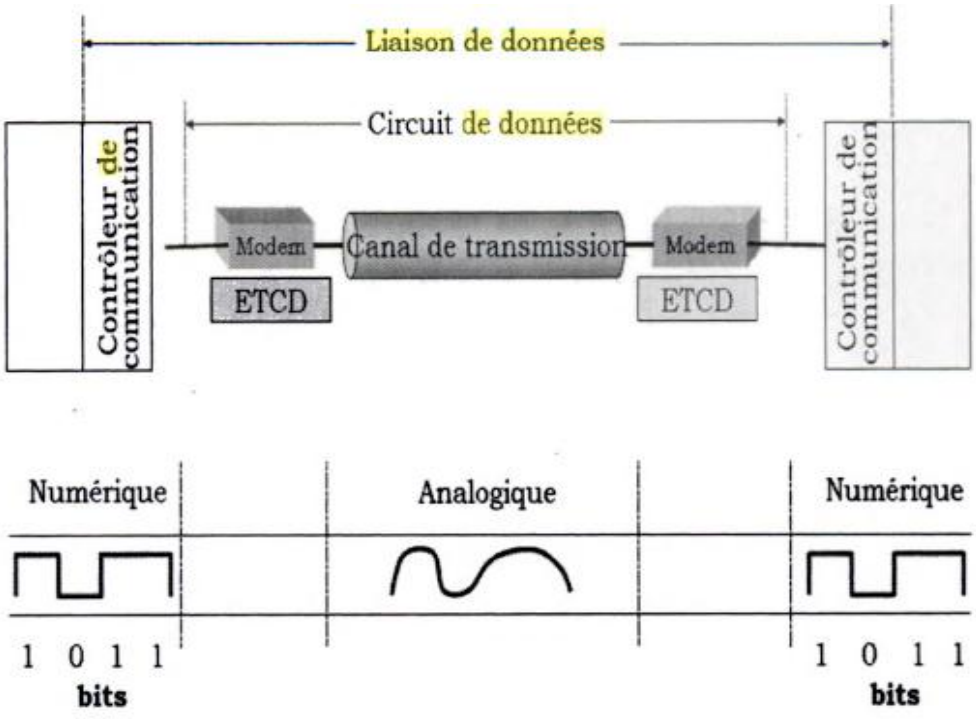


Figure 25 : circuit de donnée et transmission de donnée

Le support ou ligne de transmission est un élément essentiel de la liaison. Les possibilités de transmission (débit, taux d'erreur…) dépendent essentiellement des caractéristiques physiques et de l'environnement de celui-ci. [4]

2.3.Supports de transmission :

Un réseau suppose plusieurs équipements informatiques (ordinateurs fixes ou portable, divers équipements électronique…) situés à distance les uns des autres. La première chose à mettre

en œuvre pour constitués le réseau est la transmission des informations d'un équipement à l'autre : on utilise des supports de transmission.

Nous appelons support de transmission tout moyen permettant de transporter des données sous forme de signaux de leur source vers leur destination.

Les supports de transmission sont nombreux .Parmi ceux-ci, on distingue : les supports métalliques, non métalliques et immatériels. Les supports métalliques, comme les paires torsadées et les câbles coaxiaux, sont les plus enceint et les plus largement utilisés ;ils transportent des courants électriques.les supports du verre ou de plastique, comme les fibres optique, transmettent la lumière, tandis que les supports immatériels des communications sans fil propagent des ondes électromagnétique et sont en plein essor.

2.3.1. Paires torsadées :

Une paire torsadée non blindé (UTP, UnshieldedTwisted Pair) se compose de deux conducteurs en cuivre, isolés l'un de l'autre et enroulés de façon hélicoïdale autour de l'axe de symétrie longitudinale (voire figure 26).

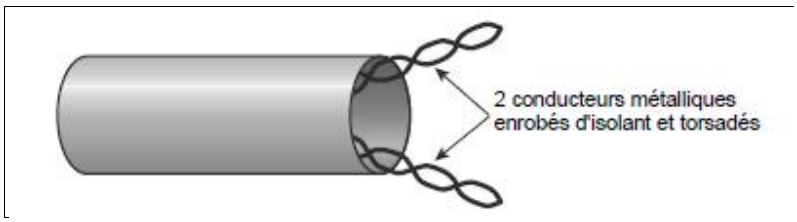


Figure 26 : paire torsadée

L'enroulement réduit les conséquences des inductions électromagnétiques parasites dues à l'environnement. L'utilisation courante de la paire torsadée est le raccordement des usagers au centrale téléphonique (la boucle locale) ou la déserte des usagers de réseaux privés. Son principal inconvénient est l'affaiblissement des courants, d'autant plus important que le diamètredes conducteurs est faible. Les paires torsadées contiennent, à intervalles régulier, des répéteurs qui régénèrent les signaux .Quand plusieurs paires sont rassemblées dans un même câble, les courants transportés interférents les uns avec les autres .Ce phénomène est appelé diaphonie.

La paire torsadée suffit pour les réseaux locaux d'entreprise ou les distance se limitent à quelque kilomètre. Ses avantages sont nombreux : technique maitrisée, facilité de connexion

et d'ajout de nouveaux équipements, faible coût .Certains constructeurs proposent des paires torsadées blindées (STP, SheildedTwisted Pair) .Enrobées d'un conducteur cylindrique, elles sont mieux protégées des rayonnements électromagnétiques parasites. Une meilleure protection prévoit un blindage par paire.

2.3.2. Câbles coaxiaux :

Pour éviter les perturbations dues aux bruits externes, on utilise deux conducteurs métalliques cylindriques de même axe séparés par un isolant. Le tout forme un câble coaxiale (voire figure 27). Ce câble présente de meilleures performances que la paire torsadée : affaiblissement moindre, transmission de signaux de fréquence plus élevé,…etc.

La capacité de transmission d'un câble coaxiale dépend de sa longueur et des caractéristiques physiques des conducteurs et de l'isolant .Sur 1 KM, un débit de plusieurs centaines de Mbit/s peut être attient .Sur des distances supérieurs à 10 KM, l'atténuation des signaux réduit considérablement les débits possibles .C'est la raison pour laquelle on utilise désormais les fibres optiques sur les liaisons grandes distances.[5]

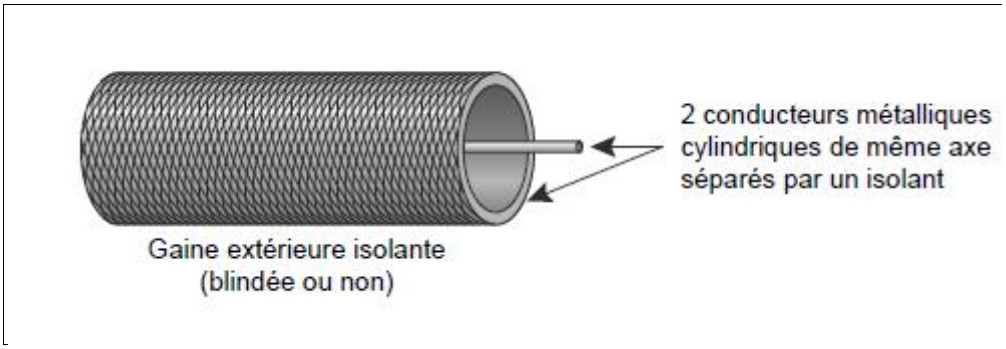


Figure 27: câble coaxial

La constitution :

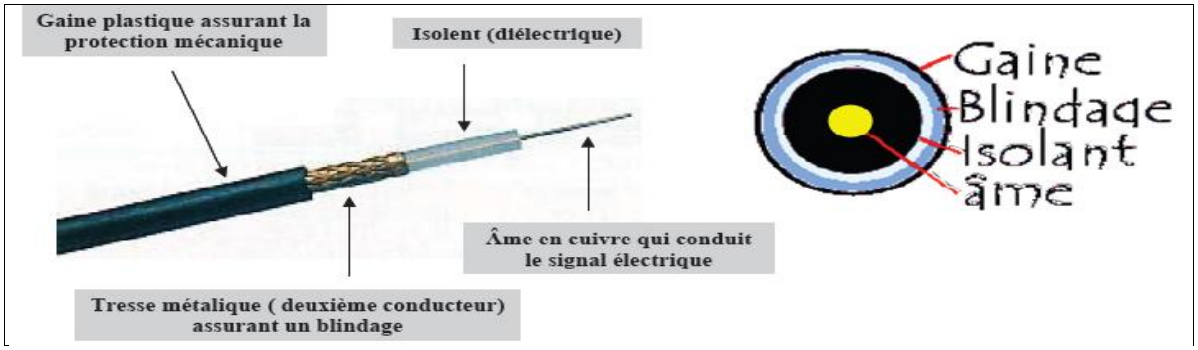


Figure 28 : constitution d'un câble coaxial

La gaine : permet de protéger le câble de l'environnement extérieur. Elle est habituellement en caoutchouc (PVC).

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 tache de transport des données, est généralement composée d'un seul brin en cuivre ou de plusieurs brins torsadés.

2.3.3. Fibre optique :

Une fibre optique est constituée d'un fil de verre très fin. Elle comprend un cœur, dans laquelle se propage la lumière émise par une diode électroluminescente ou une source laser (voire figure 29) et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre. [5]

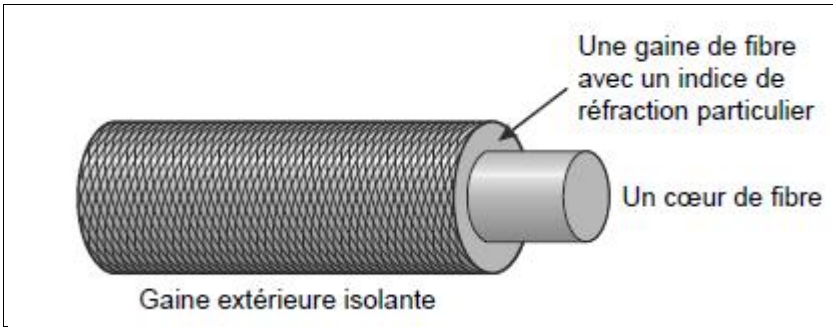


Figure 29 : fibre optique

2.3.3.1. Différents types de fibre :

a. Fibremulti-mode :

Ce type de fibre est dit multi-mode car la lumière se propage suivant plusieurs modes, c'est-à-dire qu'elle peut suivre plusieurs trajets a l'intérieur du cœur.

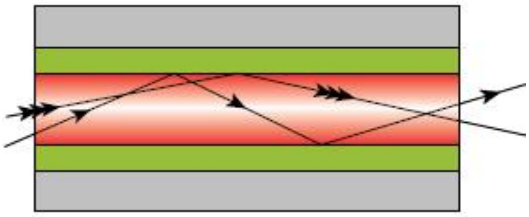


Figure 30 : fibre multi-mode

b. Fibre monomode :

Dans ce cas, la fibre est dite monomode car, en raison de la très petite taille du cœur (9 micro mètre), il n'y a qu'un seul mode de propagation de la lumière.

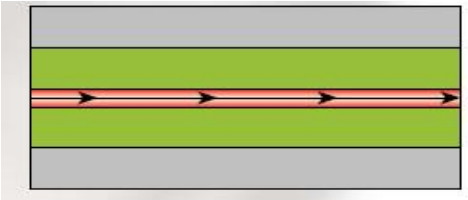


Figure 31 : fibre monomode

Les avantages de la fibre optique sont nombreux : diamètre extérieure de l'ordre de 0.1 mm, poids de quelques grammes au Kilomètre. Cette réduction de taille et de poids la rend facile à utiliser. En outre, sa très grande capacité permet la transmission simultanée de nombreux canaux de télévision, de téléphone… Les points de régénérations de signaux sont plus éloignés (jusque à 200KM), du fait de l'atténuation moindre de la lumière. Enfin, l'insensibilité des fibres au parasite électromagnétique est un avantage très apprécié, puisque une fibre supporte sans difficulté la proximité d'émetteurs radioélectriques. On peut l'utiliser dans des environnements perturbés (avec de puissants champs électromagnétiques, par exemple).

Par ailleurs, elle résiste bien aux écarts de température.la fibre optique la plupart des artères des réseaux de télécommunications et des réseaux locaux à très haut débit.

2.4. Caractéristiques des supports de transmission :

2.4.1. Bande passante :

La bande passante B d'une voie est la plage de fréquence sur laquelle la voie est capable de transmettre des signaux sans que leur affaiblissement soit trop important. Elle s'exprime en hertz.

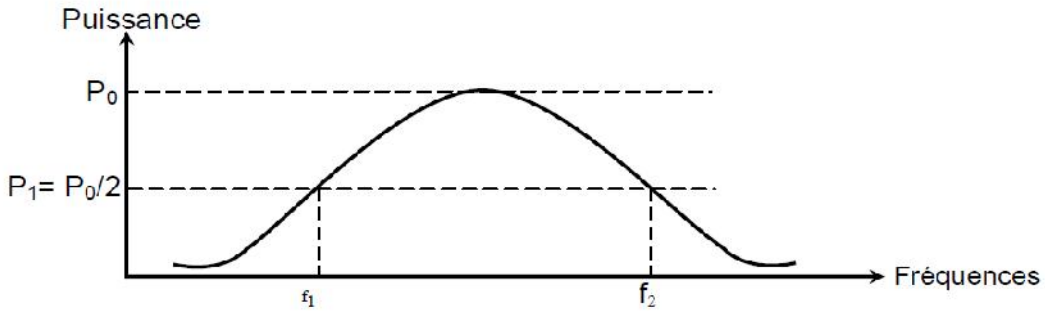


Figure 32 : bande passante

2.4.2. Capacité :

La capacité d'un support de transmission mesure la quantité d'information transportée par unité de temps. Les caractéristiques que nous venons de voir fait que la capacité d'un support est limitée. Un théorème dû à**Shanon**exprime, en bits par second, la borne maximale de la capacité Cap max d'un support de transmission :

$Capmax = W \log2 (1 + S/B)$

Dans cette formule, W est la largeur de la bande passante du support exprimé en hertz, s/b représente la valeur du rapport entre la puissance du signal (notée s) et la puissance du bruit (notée b) ; la base 2 du logarithme sert à exprimer la quantité d'information en bits. [5]

2.4.3. Transmission en bande de base :

Lorsque la longueur de liaison ne dépasse pas quelques certaines de mètre, les informations peuvent être transmises sur le support de liaison sans transformation du signal numérique en un signal analogique.

Ce type de transmission sans transposition de fréquence par modulation est appelé transmission en bande de base.

Cette transmission est rencontrée principalement dans les réseaux locaux. Elle permet d'obtenir des transmissions à grand débit mais à faible portée. Elle utilise des medias de type métallique (paires torsadées, câble coaxiale).

Les signaux bande de base sont sujets à une atténuation et doivent donc être régénérés périodiquement sur une longue distance.

Le signal binaire n'est généralement pas transmis directement sur la ligne, différents codages numérique sont utilisés pour différentes raisons :

La récupération de l'horloge nécessaire en transmission synchrone et facilitée par des séquences qui présentent des changements d'états fréquents et évitent ainsi les longues suites de ''1'' ou de ''0''.

Le spectre d'un signal binaire est concentré sur les fréquences basses qui sont les plus affaiblies sur la ligne.

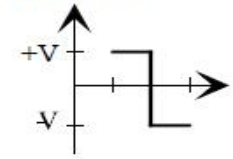
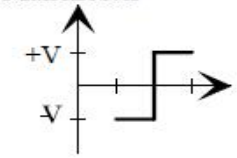
Les perturbations subies par un signal sont proportionnelles à la largeur de sa bande de fréquence.

2.5. Codage bande de base :

2.5.1. Codes à deux niveaux :

2.5.1.1. Codage Manchester (Biphasé) :

Avec une transition au milieu de chaque temps bit, le codage Manchester remédie à l'absence d'information de synchronisation. La transition est décroissante pour les **« 0 »**,croissante pour les **« 1 »**. Les sens des transitions est significatif, ce qui pose des problèmes en cas d'inversions des fils de liaison. Multipliant les transitions, le codage Manchester à un spectre très large, il est utilisé dans les réseaux locaux de type Ethernet sur câble coaxial. La bande passante du support y est importante.

Niveau logique	codage Manchester
Niveau bas	codage Manchester 
Niveau haut	codage Manchester 

Exemple :

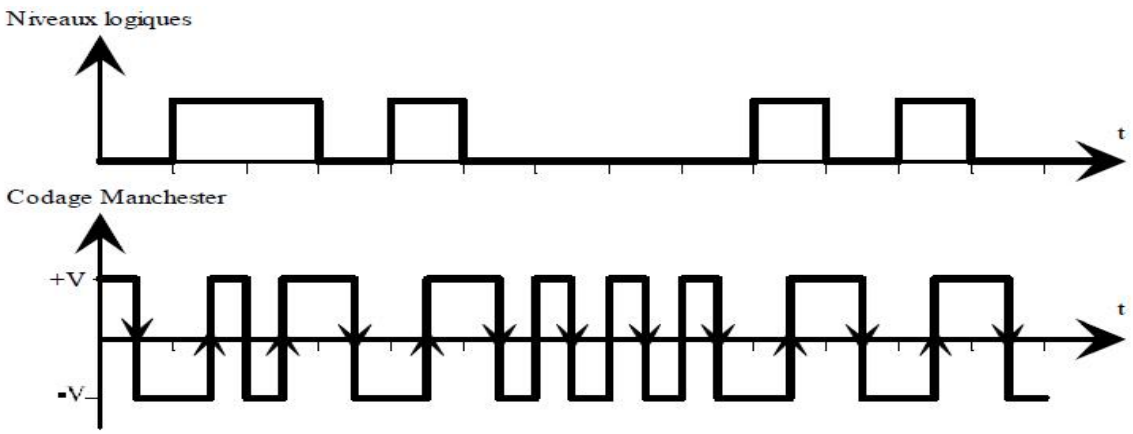


Figure 33 : code Manchester

2.5.1.2. Codage Manchester différentiel :

Le codage Manchester différentiel résout le problème d'inversion des conducteurs. Chaque transition, au milieu du temps bit, est codée par apport à la précédente. Si le bit à coder vaut zéro la transition est de même sens que la précédente, si le bit est à 1 on inverse le sens de la transmission de la transmission par apport à celui de la précédente.

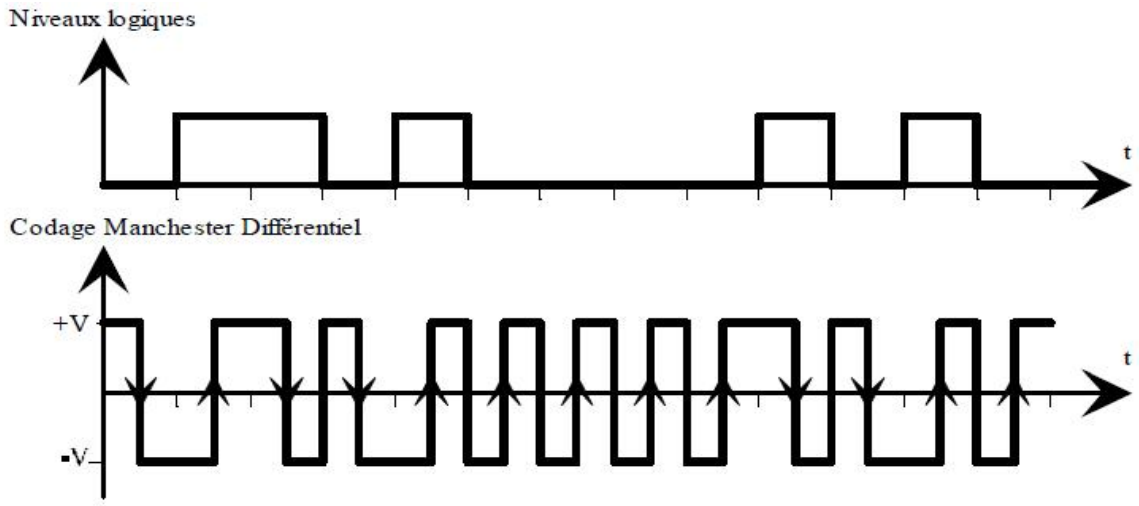


Figure 34 : code Manchester différentiel

Ce codage résout la plupart des problèmes posés, mais son spectre est relativement large.il est utilisé dans les réseaux locaux de type Token Ring.

2.5.2. Codes à trois niveaux :

2.5.2.1. Codage MLT3 :

Afin d'augmenter les possibilités de codage et de diminuer les erreurs de transmission, les codages à niveaux multiples furent imaginés.

Très utilisés dans Fast Ethernet (100base TX) et en réseau ATM, le codage en MLT3 est un codage dont les 1 font changer l'état du signal. D'abord le signal passe de l'état 1 à l'état 0, puis de l'état 0 à l'état -1.

Avec le bit 0, le signal reste sans transition.

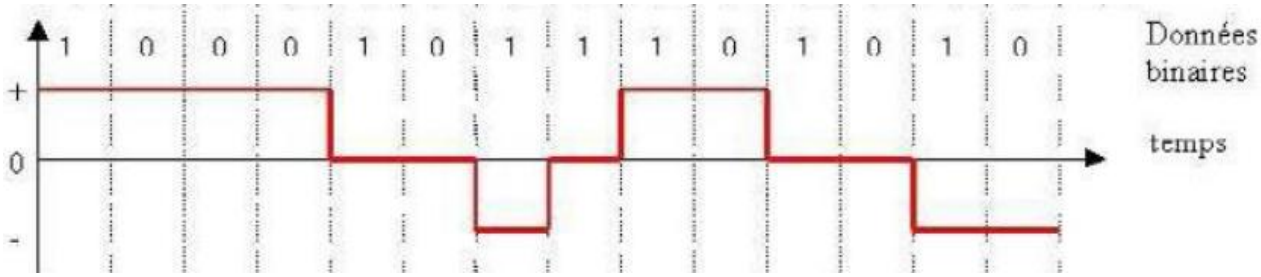


Figure 35 : code MLT3

Ce codage permet d'utiliser une cadence d'émission- réception deux fois plus élevé qu'avec NRZ.

Cependant, le code MLT3 ne résout pas le problème de perte de synchronisation des horloges lors d'une longue suite de 0, ce qui contraint donc à utilisé une horloge indépendante. [2]

2.5.2.2. Codage HDB3 :

Très utilisésdans les réseaux Transfix, HDB3 (High DensityBipolar) est un code bipolaire d'ordre 3. Le principe de fonctionnement est identique au codage bipolaire, sauf que si on a une succession de quatre 0 ou plus, le quatrième **« 0 »** est considéré comme viol.

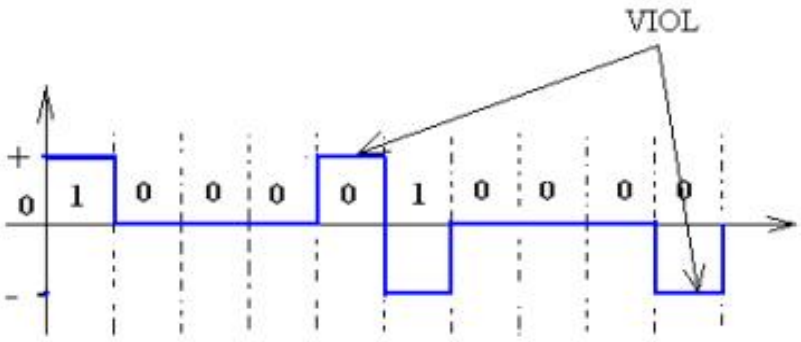


Figure 36 : code HDB3

2.5.3. Codes à multiples niveaux :

2.5.3.1. Codage nB/mB :

Le codage **nB/mB** ou **nBmB** (**4B/5B** ou **4B5B** ou **8B/10B**) s'agit d'un codage par bloc. Le principe est de coder un group de n bit, avec **m> n**.

Quand nous disons par exemple **4B/5B** ou **4B5B**, cela dit que 4 bits de données déterminant 5 bits transmis. De même si nous disons**8B/10B**, cela signifié 8 bits de données déterminant 10 bits transmis.

Il faut porter que le codage 8B10B s'agit d'un codage utilisé dans la transmission de données sur les réseaux locaux LAN.

Ci- dessous, nous dressons le tableau de transcodage 4B5B :

Code 4 bits	Code 5 bits
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Tableau 2 : transcodage 4B5B

2.6. Conclusion :

Ce chapitre présente les éléments de base de la transmission et montrent comment les signaux électriques, lumineux, se propagent dans des supports comme les câbles ou les fibres optiques et permettent ainsi la communication entre équipements informatiques à distance les uns des autres.

La bande passante et le taux d'erreur sont les principales caractéristiques d'un support. À chaque extrémité, des modems ou des codecs (codeurs et décodeurs des signaux numériques) transmettent des signaux adaptés à la nature du support. Les techniques de transmission de données (en bande de base) adaptent au mieux les signaux aux caractéristiques des supports.

La transmission directe du message n'est généralement possible que sur de très courtes distances. Un signal à transmettre subira donc un codage plus ou moins élaboré afin d'adapter son spectre au support utilisé : réduction ou suppression de la composante continue, transmission de l'horloge en synchrone…etc.

Les codages utilisés peuvent être classés selon le nombre de niveaux électriques :

- 2 niveaux : Manchester, Manchester différentiel …etc.
- 3 niveaux : MLT3, HDB3…etc.
- Multi- niveaux : nB/mB…etc.

Chapitre III : Méthodes d’évaluation de la transmission de flux d’information

3.1. Préambule :

Dans ce chapitre on va présenter les différentes étapes d'acheminement d'un flux d'information en utilisant les différentes technologies tels que : la commutation circuit et paquet, commutation par cellules, routage.

Les réseaux a grande distance, appelé aussi WAN, relient plusieurs centaines de milliers, voire des millions d'équipements terminaux sur un territoire national ou international. Il n'est donc pas possible de partager le même support de transmission, ni de raccorder directement deux abonnés désirant communiquer. On crée une structure de communication qui, en mettant bout à bout des tronçons de lignes raccordés par un ensemble de commutateurs, réalise une connexion entre deux abonnés d'un réseau ; on parle alors de réseau a commutation.

Ce chapitre montre aussi les problèmes spécifiques de recherche d'un chemin à travers un réseau et explique comment les routeurs communiquent entre eux pour partager les informations sur l'état des liaisons du réseau.

3.2. Réseaux à commutation :

L'operateur d'un réseau comptant un grand nombre d'abonnés doit offrir une garantie de bon fonctionnement, tout en optimisant les coûts d'évolutions et de maintenance de réseau. Il lui faut donc exploiter une infrastructure de réseau pour optimiser les ressources mises en œuvre. Pour cela, on utilise principalement deux techniques de commutations ; la commutation de circuit et la commutation de paquet. La première, utilisée pour les communications téléphoniques, réserve des ressources physiques pour chaque couple d'équipements désirant communiquer. La seconde est plus utilisée pour les échanges de données informatiques. Pour assurer le transfert des données, deux services réseau sont possible : l'un, évolué, en mode connexion et l'autre de plus simple, sans connexion. Le premier, normalisé sur le plan international, est baptisé circuit virtuel. Il transporte des unités de données appelées paquets.

Le second, transportant des datagrammes, sert à l'échelle mondiale dans internet. Des fonctions de contrôle interne du réseau assurent la meilleure gestion des ressources disponibles, pour en garantir le meilleur usage possible aux utilisateurs.

Un réseau à commutation fournit l'équivalent d'une liaison de données point à point entre deux équipements terminaux quelconques abonnés au réseau.

Des commutateurs, qui ont pour fonction de concentrer, d'éclater et de rédiger les informations, relient les équipements terminaux. Ils communiquent entre eux par des circuits

point à point, qui constituent les artères de communication du réseau. On considère un réseau de commutation comme un graphe, où les nœuds représentent les commutateurs et les arcs figurent les circuits (quelques fois appelés canaux, lignes de transmission, ou même liaison, selon le cas). La figure 37 montre la structure d'un réseau à commutation. [5]

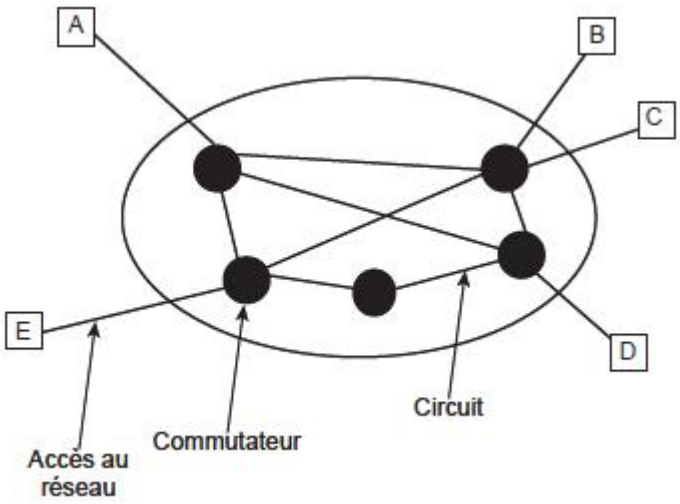


Figure 37 : structure générale d'un réseau à commutation : commutateurs et circuit.

3.2.1. Commutation de circuit :

3.2.1.1. Introduction :

Pour transmettre des informations au-delà d'un réseau local, il est nécessaire d'utilisé un réseau commuté qui est un réseau partiellement maillé, comportant des nœuds de commutation. Les stations qui échangent des informations doivent être reliées chacune à un nœud de commutation.

Le maillage d'un réseau commuté n'est pas total ce qui serait irréaliste (chaque nœuds n'est pas reliés directement à tous les autre nœuds). Il existe donc pour chaque nœud quelque liaison directe avec l'autre nœud, appelés nœud voisins. Le choix des liaisons résulte d'une analyse en coût, en charge et en sécurité.

Les nœuds ont pour vocation essentielle de recevoir des informations par une liaison et de les diriger vers un autre nœud par une autre liaison de manière à les acheminer au destinataire (fonction routage). Les informations vont donc passer de nœud en nœud pour arriver à destination. Certain nœuds sont des nœuds d'entrée-sortie du réseau : des stations leur sont attachées. Ces nœuds ont donc une fonction supplémentaire de réception/ délivrance de données.

3.2.1.2. Commutation de circuit :

Dans les réseaux à commutation de circuits, de multiples supports de transmission relient les différents commutateurs. Echanger des informations entre deux équipements terminaux nécessite de déterminer un chemin dans le réseau et de réserver un support de transmission entre chaque paire de commutateurs situés sur ce chemin.

Chaque commutateur reçoit les signaux d'une liaison et les retransmet sur la liaison vers le commutateur suivant. Le réseau téléphonique est l'exemple le plus connue de réseau à commutation de circuits. En téléphonie, le mot circuit désigne une liaison entre deux commutateurs.

Tout dialogue entre équipements terminaux se décompose en trios phase :

a. L'établissement du circuit :

Il faut au préalable construire un circuit entre les deux stations à faire communiquer. La station émettrice envoie une demande de connexion au nœud le plus proche. Celui-ci réception cette demande, l'analyse et suivant les règle de routage choisit un canal (et le réserve) vers le nœud voisin le plus adéquat vers lequel la demande de connexion est transmise. Le processus de poursuit ainsi jusqu' au nœud de rattachement de la station réceptrice, et donc jusqu' a cette station (on vérifie aussi que cette station est prête à accepter la connexion).

b. Transfert des données :

Le circuit de bout en bout étant défini et construit, les données peuvent être échangées entre les deux stations (le circuit est généralement full duplex) comme si ces stations étaient reliées directement.

c. Déconnexion :

Enfin, la phase de libération rend les différents circuits utilisés disponibles pour les communications ultérieures. La libération se fait à la demande de l'un des équipements terminaux (ou par le réseau s'il détecte qu'un des équipements du chemin est en pane). Tant que la libération n'a pas eu lieu, les circuits restent attribués au même correspondant, même s'ils n'effectuent aucun transfert d'information sur une longue durée.

Ce type de commutation présente l'inconvénient de monopoliser les circuits entre commutateurs pendant toute la durée du dialogue, même pendant les périodes de silence. Il est donc nécessaire de multiplier les circuits entre commutateurs ; on parle dans ce cas de faisceaux. De plus, la commutation de circuits requiert la disponibilité simultanée des deux équipements terminaux pour tout dialogue. En revanche, elle présente l'avantage d'être assez simple et peut s'employer sur un réseau analogique ou numérique. Dans le cas d'un réseau numérique, la mémoire nécessaire dans les commutateurs est réduite. La figure 38 décrit le principe de fonctionnement d'un réseau à commutation de circuits. Nous voyons que la communications entre A et D traverse différents commutateurs et emprunte plusieurs circuits. Les deux équipements terminaux disposent de l'ensemble de ces sources pour la durée de leur communication.

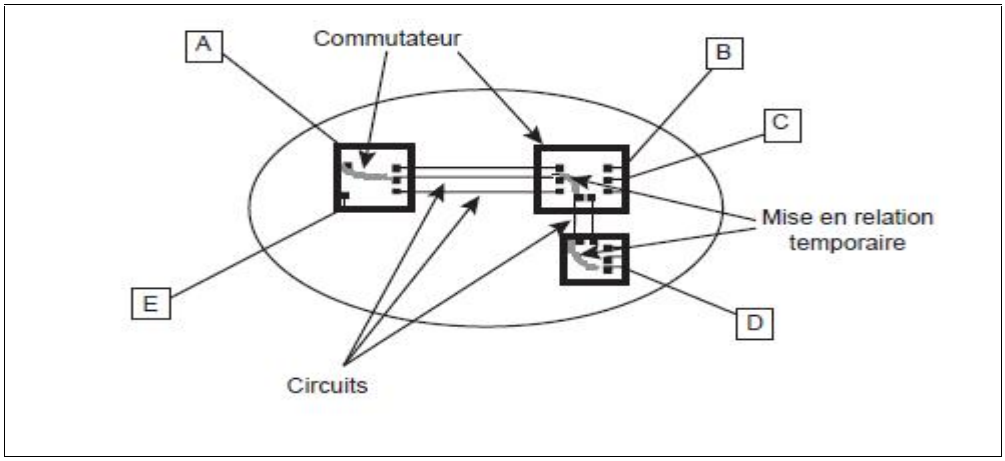


Figure 38 : Principe de la commutation de circuit

3.2.2. Commutation de message :

La commutation de messages est la première technique imaginée pour les réseaux transportant des données informatiques. Un message se définit comme une suite de données binaires formants un tout cohérent pour les utilisateurs (une page de texte, un fichier son, une image fixe ou animée…).

Un utilisateur qui veut émettre un message l'envoie au commutateur en précisant l'adresse du destinataire. Le commutateur attend la réception complète du message, le stocke, analyse l'adresse du destinataire puis émet le message vers le commutateur voisin adéquat ou, le cas échéant, vers l'équipement terminal (technique store and forward). L'aiguillage du message s'effectue en fonction des informations de contrôle. Le commutateur conserve le message si la liaison est occupée : chaque commutateur se comporte donc comme une mémoire tampon.

Le message transite ainsi à travers le réseau par émissions successives entre les commutateurs jusqu'au destinataire. La figure 39 montre l'infrastructure d'un réseau à commutation de message : A, B, C, D et E sont des abonnées au réseau qui échangent des messages et les carrés représentent les commutateurs. Dans la commutation de message, les liaisons ne sont utilisées que pour la durée de transmission entre les deux équipements adjacents. Chaque commutateur doit être capable de stocker le message entier.

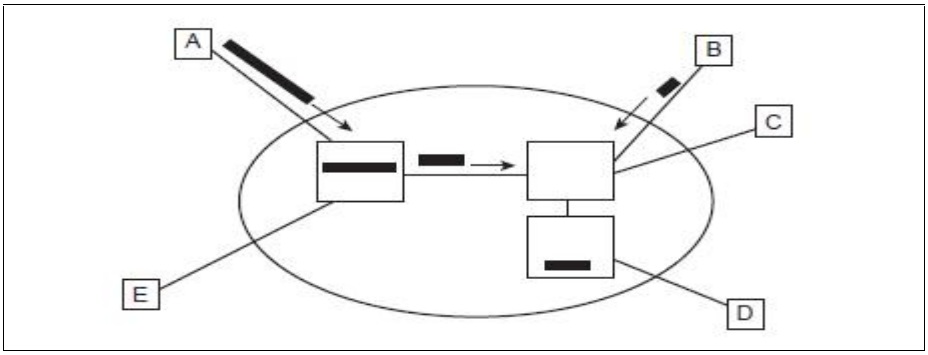


Figure 39 : Réseau à commutation de message

Comme un commutateur gère simultanément plusieurs échanges, la taille de la mémoire nécessaire à la gestion des messages est importante et entraine des problèmes d'allocation complexes. De plus, les liaisons entre commutateurs ne sont pas d'une fiabilité totale. Des Protocol de liaison de données sont nécessaires entre chaque paire d'équipements. Les commutateurs gèrent autant de liaisons de données que d'équipements auxquels ils sont reliés. La commutation de messages ne permet qu'un échange simplex et asynchrone, elle est plus un service qu'un technique réseau. La commutation de messages est aujourd'hui le support logique des réseaux de télex et des systèmes de messagerie modernes.

Le délai de transmission dans le réseau est fonction du nombre de commutateurs traversés et de la longueur du message. Remarquons que la probabilité d'une erreur sur un message augmente avec sa longueur : la transmission du message long dans le réseau est très pénalisante. Une amélioration de cette technique réduit la taille des messages envoyés et conduit à la commutation de paquets. [5]

3.2.3. Commutation de paquets :

La commutation de paquets est apparue vers 1970 pour résoudre le problème de la transmission de données numériques sur longues distances. La commutation de circuit était en effet relativement inadapté (mais parfaitement adaptée pour la voie) à la transmission de

données numériques ; d'une part, la communication entre systèmes informatiques comporte de nombreux « silence » et la voie de transmission, si elle est réservée en totalité à cette communication, n'est donc pas utilisée à 100% ; par ailleurs, la commutation de circuits s'effectue à débit constant ce qui contraint énormément les équipements (serveurs, stations) qui possèdent des possibilités différentes en débit.

Dans la commutation de paquets, on découpe d'abord le message en plusieurs morceaux, appelés paquets avant de l'envoyer dans le réseau : cela s'appelle la fragmentation. Comme dans un réseau à commutation de messages, les commutateurs utilisent des informations de contrôle pour acheminer correctement les paquets depuis l'expéditeur jusqu' au destinataire.

L'opérateur du réseau (ou des normes internationales) définit le format de l'en-tête et la taille maximale d'un paquet. Le destinataire doit attendre la réception de tous les paquets pour reconstituer le message et le traiter : cette opération est le réassemblage.

Un paquet ne forme donc pas un tout logique pour l'équipement terminal : ce n'est qu'un ''élément d'information'', acheminé dans le réseau par les réémission successives entre commutateurs. Sa petite taille réduit le délai global d'acheminement des messages. Cependant, elle accroît la complexité de sa gestion dans les commutateurs : le dimensionnement de la mémoire des commutateurs est un élément important dans la détermination de la capacité et les performances d'un réseau à commutation de paquets.

Si la mémoire d'un commutateur est entièrement utilisée, celui-ci n'est plus en mesure de recevoir de nouveaux paquets. Il peut dans certains cas, détruire des paquets et dégager les performances du réseau. L'ensemble des techniques mises en œuvre pour éviter la saturation de la mémoire des commutateurs s'appel le contrôle de congestion.

Comme pour la commutation de messages, une paire d'équipement ne monopolise plus une liaison entre commutateurs : celle-ci supporte la transmission de paquets de multiples utilisateurs. Si le débit de la liaison est supérieur au flux transmis par l'ensemble des utilisateurs, elle peut supporter de plusieurs dialogues simultanés tout en donnant à chaque utilisateur l'impression d'être seul sur le réseau. Ainsi, même si le flux générer par un utilisateur donné augmente subitement, l'impact sera fiable sur le flux global dans le réseau.

La figure 40 montre comment un message constitué de cinq paquets est transmis d'un utilisateur à l'autre.

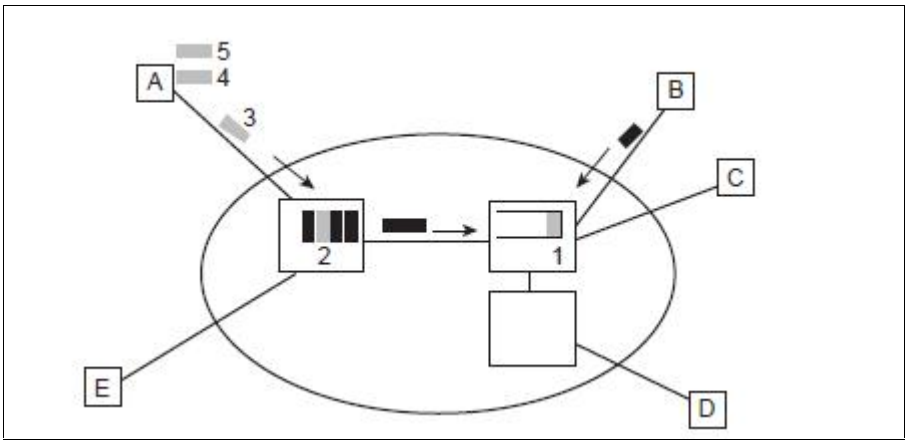


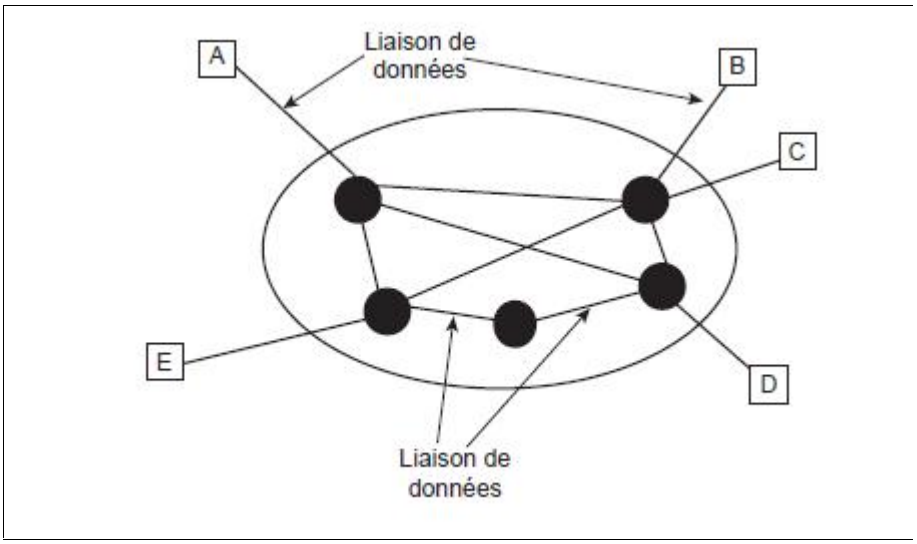
Figure 40 : Réseau à commutation de paquets : il peut y avoir simultanément transmission de plusieurs paquets d'un même message sur différentes liaisons du réseau.

Le message émis par A est découpé en cinq paquets, acheminé un par un par le réseau.

La méthode pour structurer les équipements et les services est hiérarchique : à chaque extrémité d'un circuit on trouve une succession d'entités assurant un service donné pour une entité de niveau supérieure.

A une extrémité de la liaison de données, l'entité de liaison assure un dialogue fiable avec l'entité de même type situé à l'autre extrémité. Une entité de niveau supérieur, l'entité de réseau, assure le routage des paquets à travers le réseau. Elle utilise pour cela l'entité de liaison comme une boite noire lui fournissant un service. Elle est le seul à interpréter et exploiter l'en-tête pour acheminer les paquets jusqu'à leur destination. L'entité de liaison de données considère le paquet comme l'élément à transmettre : par exemple, elle l'insère dans le champ d'information de la trame gérée selon le Protocol HDLC. [5]

La figure 41 montre la mise en œuvre d'une succession de liaison de données, et la figure 42, le découpage d'un message en paquets et leur intégration dans plusieurs trames.



Figue 41 : mise en œuvre des liaisons de données dans un réseau à commutation : des successions de liaison de données relient toutes les paires d'équipements.

Une succession de liaisons de données est mise en œuvre entre toutes les paires d'équipements pour acheminer les données de l'expéditeur jusqu'au destinataire.

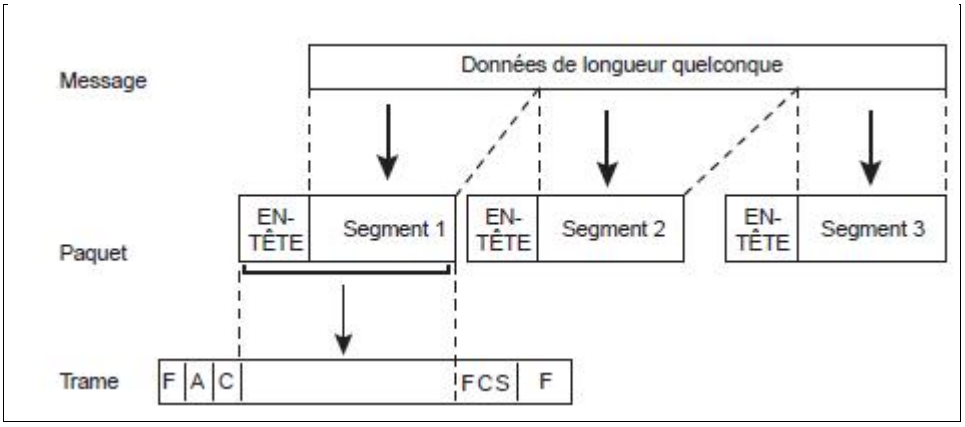


Figure 42 : découpage d'un message en trois paquets insérés dans trios trames successives.

Le message est coupé en trois morceaux : un en-tête s'ajoute chacun pour constituer un paquet, transmis dans le champ information d'une trame.

La commutation de paquet décline deux modes de mise en relation (figure 43). Le premier, le mode datagramme ou non connecté est le mode naturel de la commutation de paquets. Le second met en œuvre un mécanisme de stabilité de route qui consiste à « baliser » un chemin qui suivra ensuite tous les paquets émulant ainsi un circuit sur un réseau en mode paquet. Ce

second mode de fonctionnement est dit mode orienté connexion ou plus simplement mode connecté. Le circuit émulé porte le nom de circuit virtuel.

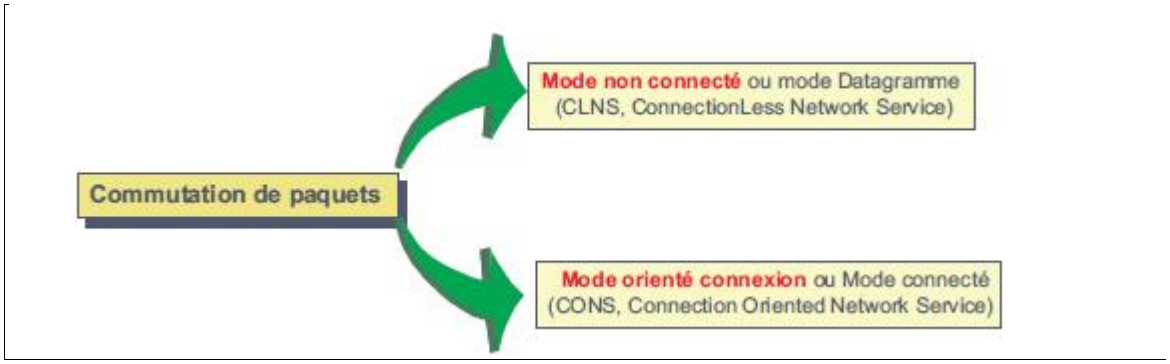


Figure 43 : les modes de mise en relation

3.2.3.1. Mode non connecté :

En mode non connecté (CLNS : Connection Less Network Service), les informations transitent dans le réseau indépendamment les unes des autres. Le destinataire n'est pas nécessairement à l'écoute, les informations sont dans ce cas, perdues. Dans tell mode de fonctionnement, les routes empruntées par les différents blocs d'informations peuvent être différentes, le séquencement des informations ne peut être garantie (figure 44).

Les mécanismes réseaux sont allégés au détriment d'une complexité dans les organes d'extrémités qui doivent être capables de réordonnancer les différents blocs d'information.

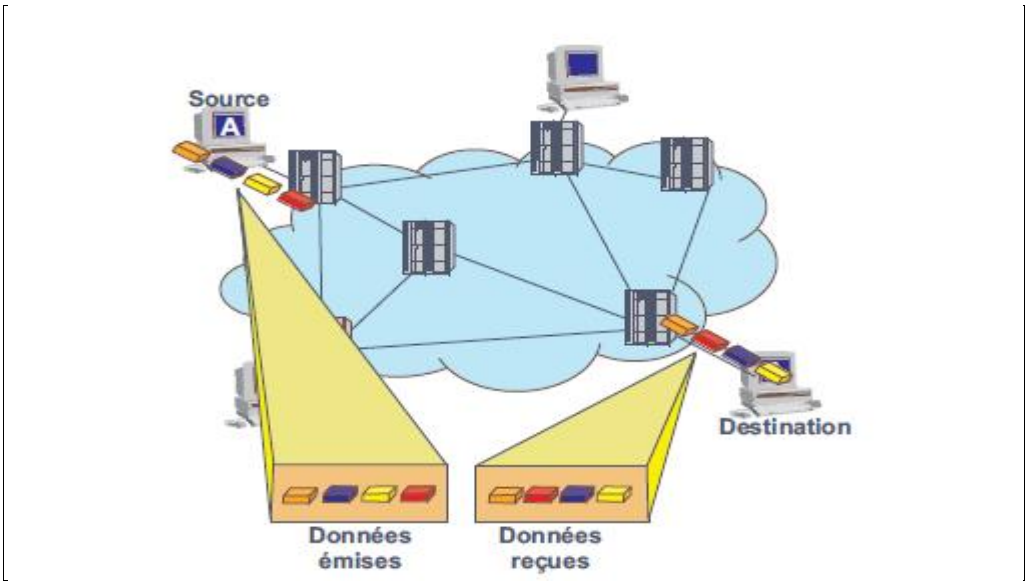


Figure 44 : réseau en mode datagramme

La possibilité d'un routage différent pour chaque bloc d'information (paquet) d'un même utilisateur permet de répartir la charge du réseau (routage adaptif). Chaque bloc est acheminé indépendamment du précédent, il doit par conséquent, contenir l'adresse du destinataire.

Aucune réservation de ressources n'est effectuée préalablement à tout envoie de données. De ce fait, en cas de surcharge du réseau, des blocs d'informations peuvent être perdues. [4]

3.2.3.2. Mode orienté connexion :

Un chemin entre le nœud entrant et le nœud destination est construit (établissement du circuit virtuel, puis tous les paquets d'un même message suivent ce chemin, ils arrivent donc dans l'ordre où ils ont été émis (acheminement en séquence).

3.3. Commutation de cellules (ATM) :

3.3.1. Présentation générale :

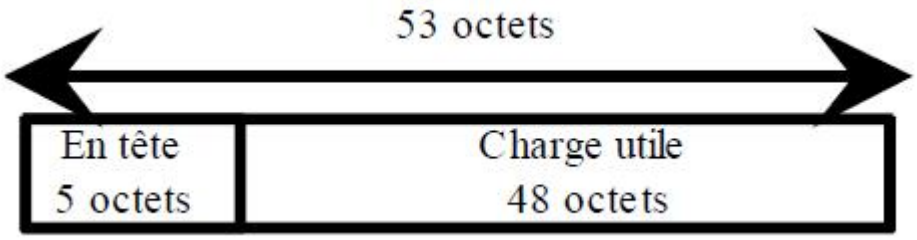
La technologie ATM fut développée par le CENT, centre d'étude de France télécom afin d'améliorer le transport des données sur le réseau public, mais en plus des organes tel que ATM Forum a fait que cette technologie puisse s'appliquer aussi LAN, WAN, public ou privé.

ATM permet donc une exploitation plus efficace des liaisons WAN des opérateurs, en raison d'un véritable multiplexage dynamique lors de la transmission ce qui évite de laisser le support inoccupé pendant un certain lapse de temps et donc d'engendré un coup supplémentaire des transmissions.

Avec ATM il est donc possible de transporter tous les trafics, et cela sur toutes les distances envisageables, de quelque dizaines de mettre à plusieurs dizaines de milliers de kilomètres et quel que soit le type de média (paire torsadé, fibre optique, et le sans fil). En plus le débit peut être complètement variable.

3.3.2. Cellules ATM :

Les cellules ATM sont de longueurs fixes ce qui facilite le multiplexage, où autrement dit la commutation de celle-ci. Grace à cette longueur fixe les Systèmes de commutation ne sont plus logiciel mais matériel, ce qui permet d'obtenir des vitesses de commutation de plusieurs centaines de Méga bite.



La taille d'une cellule ATM à été fixée à 53 octets ce qui permet d'améliorer le multiplexage des données sur la voix (qui fut le critère déterminant pour la taille) tout en n'en minimisant les conséquences. En réduisant la taille des cellules on réduit aussi le temps de traitement de celle-ci.

Cette taille ne devait pas être inférieure afin que le rapport entre la charge utile et l'en-tête soit suffisant.

C'est ainsi qu'en limitant les longueurs des filles d'attente sur les éléments de commutation que l'on va pouvoir obtenir un débit pratiquement constant avec une gigue (décalage temporel entre des cellules de même source) pratiquement nulle.

3.3.3. Liaisons ATM:

Les liaisons gérable par la technologie ATM sont de deux types, les liaisons point à point et les liaisons point à multipoint. A la différence des réseaux locaux tel que Ethernet ou Token-Ring, le réseau ATM est dit orienté connexion, a chaque demande de transmission un circuit virtuel est établit répondant a la qualité de service souhaité, ce circuit peut être permanant ou pas.

3.3.4. Couches ATM :

Les couches ATM sont au nombre de trois :

a. Couche physique :

Qui permet l'adaptation des cellules au système de transport physique utilisé.

b. Couche ATM :

Qui permet d'effectuer la commutation et le multiplexage des cellules.

c. Couche AAL (ATM adaptation layer) :

Qui permet d'adapter les unités de données des protocoles supérieurs a la couche ATM. [15]

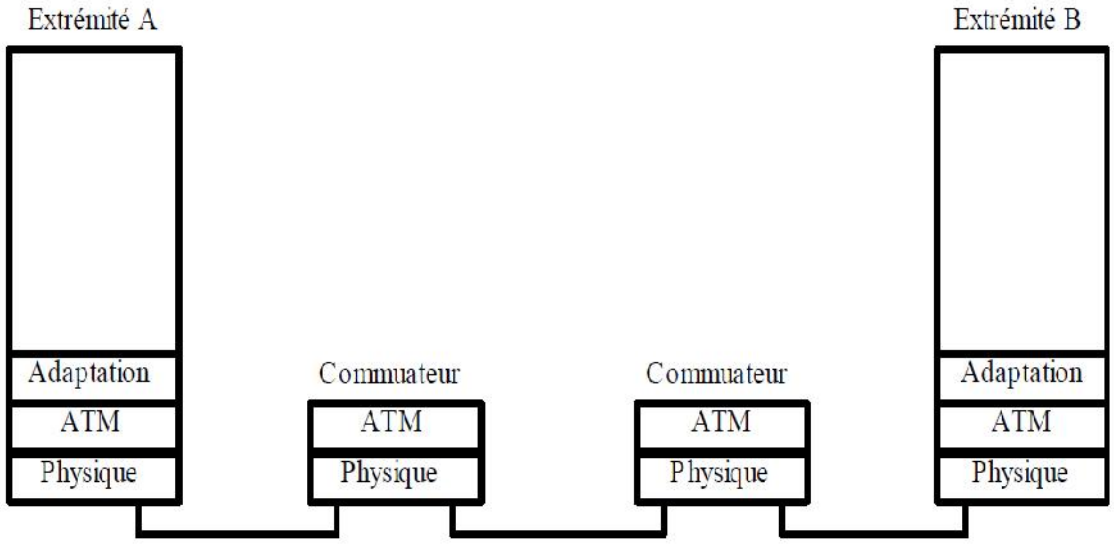


Figure 45 : les couches ATM

3.4. Notion d'adressage dans le réseau :

Si deux équipements reliés directement l'un à l'autre par une liaison de données n'ont pas de problème d'identification du correspondant, il n'en va pas de même pour les abonnées des grands réseaux : chacun d'eux doit posséder une identité unique, afin que les commutateurs acheminent les données au bon destinataire. Nous avons remarqué précédemment qu'il existait une structure hiérarchique des équipements : la communication utilise un circuit de données, contrôlé par le Protocol de liaison, sur lequel sont véhiculés les messages découpés en paquets.

Une entité distincte gère chaque niveau. Il faut pour chaque niveau, une identification unique de la ressource gérée : on utilise donc plusieurs nivaux d'adressage. Selon ses besoins, chaque niveau d'adressage doit faire la correspondance entre l'adresse qu'il utilise et les adresses manipulées par les niveaux qui lui sont immédiatement inférieurs ou supérieur. On distingue principalement trois types d'adresse : physique, logique et symbolique présentons les successivement.

3.4.1. Adresse physique :

L'adresse physique est l'adresse de l'équipement situé au plus prés du support de transmission. Elle identifie l'interface série utilisée pour l'émission et la réception des données. Elle distingue, parmi plusieurs interface série disponibles, celle vers laquelle émettre ou depuis laquelle sont reçues des données. Elle a une signification purement locale à l'équipement.

En général, les abonnées d'un réseau à commutation n'utilisent guère l'adresse physique, puis qu'une seule liaison point à point les relie au commutateur d'entrée dans le réseau. En revanche l'adresse physique est indispensable aux commutateurs qui doivent décider sur quelle liaison acheminé les données d'un abonnées – ou un commutateur – à l'autre.

L'adresse physique est utile dans les réseaux locaux. Par exemple on identifié avec elle la carte Ethernet qui sert d'accès au support commun du réseau local.

3.4.2. Adresse logique :

Pour atteindre un utilisateur quelconque depuis n'importe quel point du réseau, il ne suffit pas de distinguer localement les différentes liaisons disponibles. Il faut que les commutateurs puisent ébouter les liaisons à emprunter pour relié la source à la destination.

Pour cela ils doivent identifier un utilisateur parmi tous les usagers du réseau : chaque utilisateur doit donc posséder une adresse unique, connue de tous les commutateurs traversés, à partir de laquelle les points d'accès au réseau organisent le routage pour acheminer les données le plus efficacement possible. L'adresse utilisée doit être unique et dépond de la nature du réseau de transport et du mode d'acheminement des données : c'est l'adresse logique. Elle est déterminée par l'operateur du réseau ou par un organisme international.

L'adresse IP utilisé dans internet en est l'exemple le plus connue.

3.4.3. Adresse symbolique :

L'adresse logique identifier tous les équipements du réseau. Un utilisateur peut familier des contrainte imposée par la structure du réseau peut avoir des difficultés à mémorisé cette information. Pour faciliter sont accès au réseau, il se choisit (ou l'administrateur du réseau choisit pour lui) une adresse symbolique plus facilement compréhensible et mémorisable qu'une adresse logique. Ainsi par exemple, plutôt que de se souvenir de l'adresse IP :

192.122.1.25 il retiendra plus facilement l'adresse symbolique : prénom.nom@mon_ fournisseur.mon_ pays… tout comme l'adresse logique, elle doit être unique pour le réseau.

Des organismes internationaux ont proposé une structuration des adresses symboliques, pour garantir leur l'unicité. Le logiciel gérant la connexion réseau de l'ordinateur au fournisseur d'accès a internet doit apparier adresse logique et adresse symbolique et mémoriser ces informations.

3.5. Notion de service dans un réseau à commutation :

On distingue deux types de service réseau : le service sans connexion et le service en mode connecté, encore appelé service orienté connexion. Le premier type est utilisé dans internet, le second est proposé dans les réseaux publics de données respectant les normes X.25 de l'ITU.

Ces services correspondent à deux façons d'exploiter la commutation de paquet.

Dans un service sans connexion, l'expéditeur traite chaque paquet comme une unité de données totalement indépendante des autres. Un paquet doit donc inclure l'adresse complète du destinataire, éventuellement celle de l'expéditeur. A tous moments l'équipement terminal peut fournir au réseau un paquet à transmettre sans procédures préalable. Un tel service est par exemple celui fourni par le réseau postal : une lettre peut être postée à tout moment. La figure 52 donne un exemple de service réseau sans connexion.

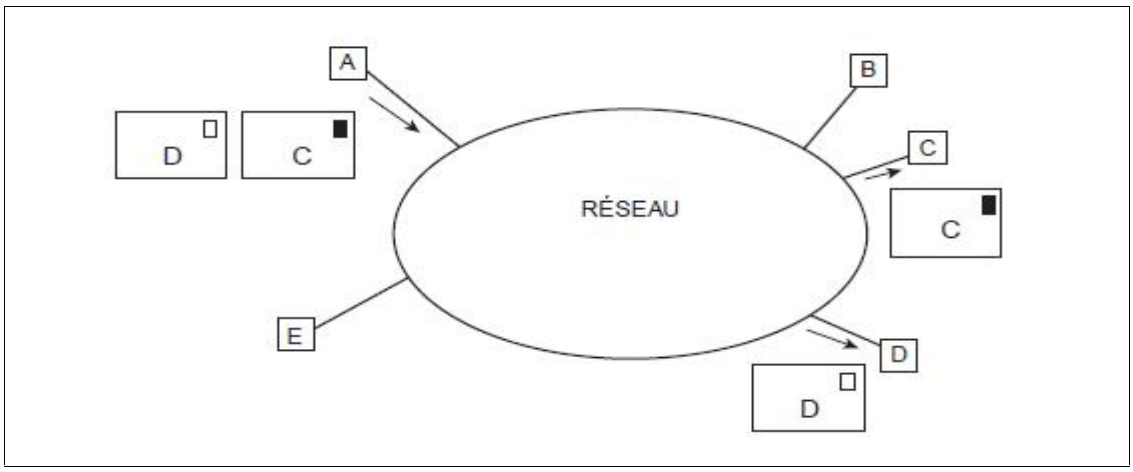


Figure 46 : service réseau sans connexion : un paquet peut être émis à tout moments, indépendamment des autres paquets et sans soucier de l'état du destinataire.

Dans un service en mode connecté ou orienté connexion, l'utilisateur doit d'abord indiquer avec qu'il veut dialoguer. Pour cela, une procédure, appelé ouverture de connexion établit un lien logique entre deux équipements terminaux et constitue un « tube » de dialogue, appelé circuit virtuel. La connexion criée n'est active que si le destinataire accepte la communication. Ensuite, le réseau transmets tous les paquets de données jusqu'au destinataire, en se référent au circuit virtuel précédemment établi (l'émetteur n'a plus besoin de préciser l'adresse du destinataire dans chaque paquet). Lorsque le dialogue se termine, un des utilisateurs indique au réseau qu'il souhaite libérer la connexion.

Pour dialoguer avec un autre équipement(ou le même), il faut déclencher une nouvelle ouverture de connexion. Le réseau téléphonique illustre un tel service : il faut décrocher le téléphone, composer le numéro de son correspondant, attendre qu'il réponde avant pouvoir dialoguer avec lui. Après, avoir raccroché, il faut répéter les opérations précédentes si on veut communiquer à nouveau. La figure 47 montre une connexion établie entre les équipements terminaux A et C.

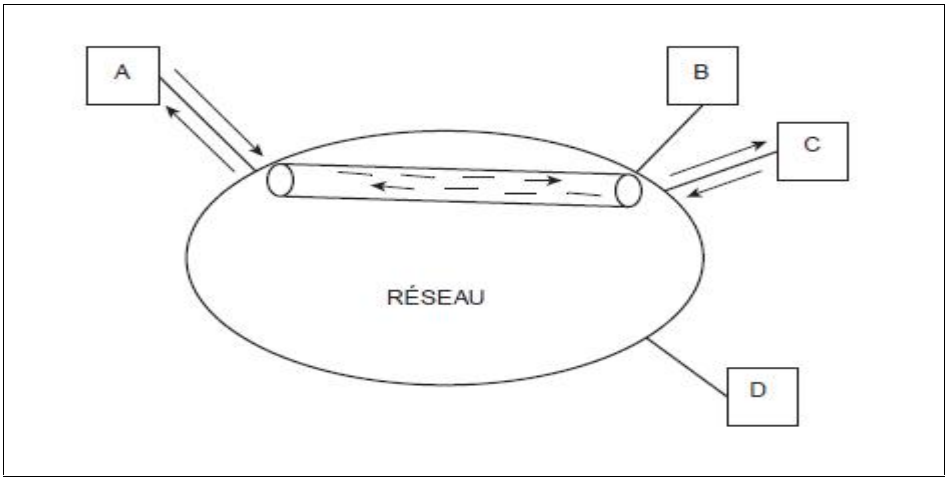


Figure 47 : service réseau en mode connecté entre les équipements A et C

Un lien logique entre émetteur et récepteur est maintenu pendant toute la communication, mais les ressources physiques sont partagées.

3.5.1. Service sans connexion :

Un réseau à commutation de paquets qui offre un service sans connexion s'appelle couramment réseau à datagrammes, du nom des unités de données transportées. Un service sans connexion considère les différents datagrammes comme totalement indépendants les uns

des autres. Chacun transite à travers le réseau avec l'ensemble des informations nécessaire à son acheminement. Il comprend notamment les adresses complète de l'expéditeur et du destinataire. La fonction de routage s'exécute pour chaque datagramme. Ainsi plusieurs datagrammes échangés entre les mêmes équipements terminaux peuvent suivre des chemins différents dans le réseau et le destinataire les recevoir dans un ordre différent de l'ordre d'émission. De plus en cas de problème (rupture de liaison, manque de mémoire dans un commutateur), des datagrammes peuvent se perdre. L'équipement terminal doit non seulement reconstituer l'ordre des datagrammes reçus pour en exploiter correctement le contenu, mais aussi vérifier qu'aucun ne s'est égaré.

L'avantage d'un tell réseau est sa simplicité de réalisation interne : ce sont les équipements terminaux qui mettent en œuvre les fonctions de contrôle. La figure 48 montrent l'acheminement des datagrammes entre les équipements A et D.

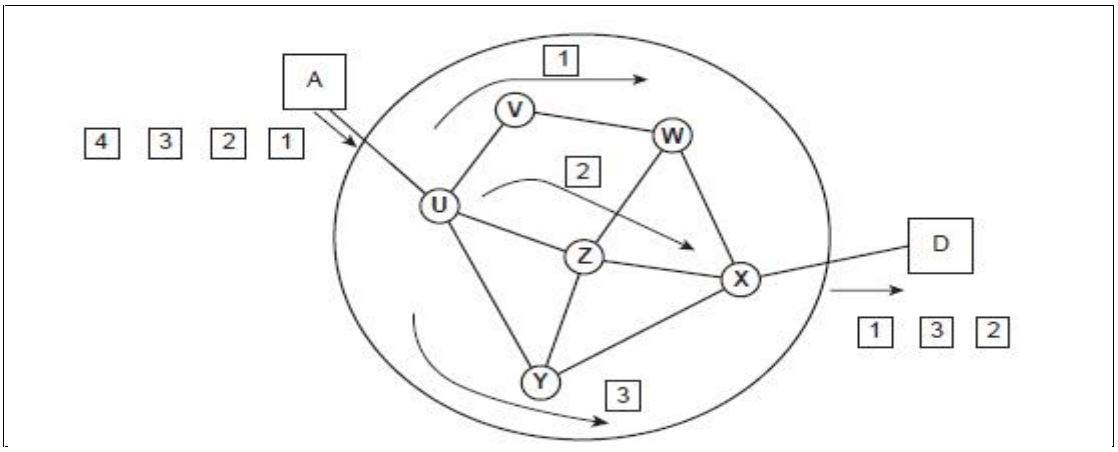


Figure 48 : acheminement des datagrammes entre les équipements A et D : l'ordre n'est pas garanti et il ya des pertes.

A envoie successivement les paquets 1, 2, 3,4.

Le paquet 1 empreinte le chemin passant par les commutateurs U, V, W, X.

Les paquets 2 et 3 empruntent respectivement U, Z, X et U, Y, X le paquet 4 se perd.

D reçois dans l'ordre 2, 3 puis 1 et ne reçois pas 4.

3.5.2. Service avec connexion :

Le service avec connexion est couplé avec la notion de circuit virtuel. A l'ouverture de la connexion, le réseau détermine le chemin que tous les paquets emprunteront par la suite.

Ce chemin s'appelle « circuit virtuel » .Il s'agit d'un circuit car on utilise les mêmes principes que dans la commutation de circuit ; il est virtuel puisqu'une connexion ne monopolise une liaison entre commutateurs que pendant le temps de transfert d'un paquet. Une fois le paquet transmis, la liaison est utilisable par un autre circuit virtuel. La liaison entre deux commutateurs transporte donc plusieurs circuits virtuels entre des équipements terminaux totalement différents. De ce fait, l'utilisation du support de transmission est beaucoup plus efficace que dans le cas de la commutation de circuit.

Un équipement terminal peut gérer plusieurs connexions en parallèle. Un identifiant, souvent appelé numéro de voie logique, les distingues. L'équipement émetteur précise l'adresse logique du destinataire à l'établissement d'une connexion. Il lui associer un numéro de voie logique. Le commutateur relié au récepteur attribue de son coté un numéro de voie logique à la future connexion. Les deux numéros de voie logique identifiant la connexion sont choisis indépendamment l'un de l'autre, pour la duré de la connexion. Ils constituent un adressage abrégé : les correspondants n'ont pas besoins de transporter dans leur paquet les adresses complètes de l'émetteur et du destinataire. A titre de comparaison, lorsqu'un usager du téléphone affecte une touche du clavier à un numéro de téléphone particulier, il n'a pas tapé les 10 chiffres avant chaque appel.

L'équipement terminal place le numéro de la voie logique approprié dans l'en-tête du paquet qu'il transmit. Celui-ci parvient au point d'accès du réseau et les commutateurs le propagent jusqu' au destinataire. Tous les paquets reçus et émis sur cette connexion portent donc le même numéro de voie logique, la figure 49 montre un exemple de connexions multiples entre plusieurs équipements terminaux.

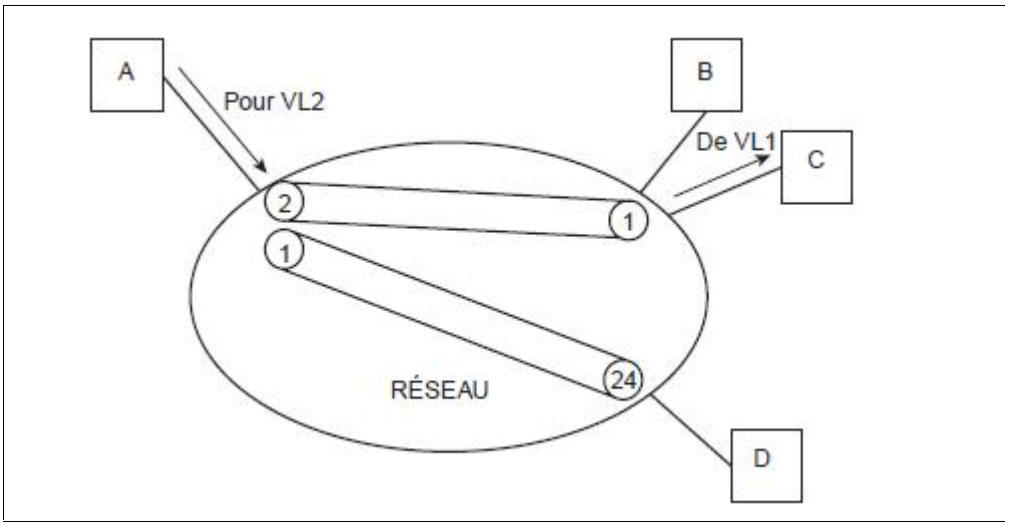


Figure 49 : exemple de connexions dans un réseau à commutation fonctionnant en mode connecté : signification local des numéros de voie logique.

La voie logique 2 référence pour A sa connexion avec C, la voie logique 1 référence pour C sa connexion avec A. la voie logique 1 référence pour A sa connexion avec D, la voie logique 24 référence pour D sa connexion avec A.

L'équipement A dispose de deux voies logiques 1 et 2 multiplexées sur la liaison avec le commutateur d'accès.

La correspondance entre l'adresse logique du destinataire (l'adresse complète de l'abonné) et le raccourci d'adressage qui l'identifier localement(le numéro de voie logique utilisé) est bijective (un numéro de voie logique n'identifier qu'un seul circuit virtuel, pour un échange de données bidirectionnel). [5]

L'avantage d'un réseau à circuit virtuel (voir figure 50) est sa fiabilité : comme les paquets d'un même circuit virtuel suivent le même chemin, il suffit de conserver l'ordre des paquets sur chaque tronçon du chemin pour conserver globalement l'ordre des paquets sur le circuit virtuel. L'opérateur du réseau peut donc garantir une certaine qualité de service (taux d'erreur, contrôle de séquence et de flux…), au prix d'une plus grande complexité de réalisation et de gestion du réseau.

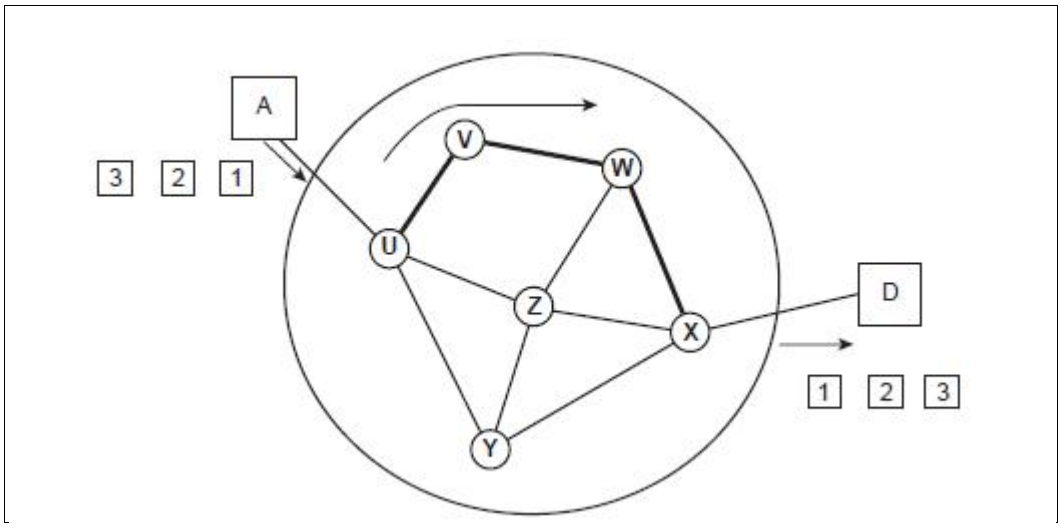


Figure 50 : exemple de réseau à circuit virtuel

Tous les paquets empruntent le chemin défini par les commutateurs U, V, W, X.

3.6. Contrôle interne dans un réseau :

Pour assurer le bon fonctionnement du réseau, l'opérateur ou l'administrateur de réseau exerce des fonctions de contrôle interne au réseau, principalement les fonctions de routage, de contrôle de congestion et d'administration.

3.6.1. Présentation :

Nous allons ici aborder les termes de routage statique et de routage dynamique. Ce sont tous les deux des modes de routage qu'il est important de connaitre pour bien choisir le Protocol de routage que nous souhaitons mettre en place au sein d'un réseau.

3.6.2. Pourquoi-a-t-on besoin du routage ?

Internet n'est rien d'autre qu'un immense de lien et d'interconnexion entre plusieurs réseaux. Pour savoir le chemin à emprunter parmi tous ces liens pour aller d'un réseau A à un réseau B, il faut qu'un Protocol de routage ait été mise en place. Le but de routage est définir une route ou un chemin à un paquet celui-ci arrive sur un routeur. Le but du routage est donc d'assurer qu'il existe toujours un chemin pour aller d'un réseau à un autre.

Figure 51 : routage à travers 3 réseaux

On voit ici trois réseau séparés chacun par un routeur. Chaque poste de chaque réseau contient dans sa configuration l'IP d'une passerelle qui constitue l'élément vers lequel les postes vont envoyer des paquets. Le rôle de la passerelle est donc de transmettre ce ou ces paquets à leurs destinataires. Le routeur 2 connait ici le réseau C et B mais ne connait pas le réseau A. C'est ici que le routage intervient, le routage sert en effet à indiquer au routeur 2 par quel chemin doit passer pour joindre un réseau auquel il n'est pas directement connecté.

On peut imaginer une seconde topologie (infrastructure réseaux) :

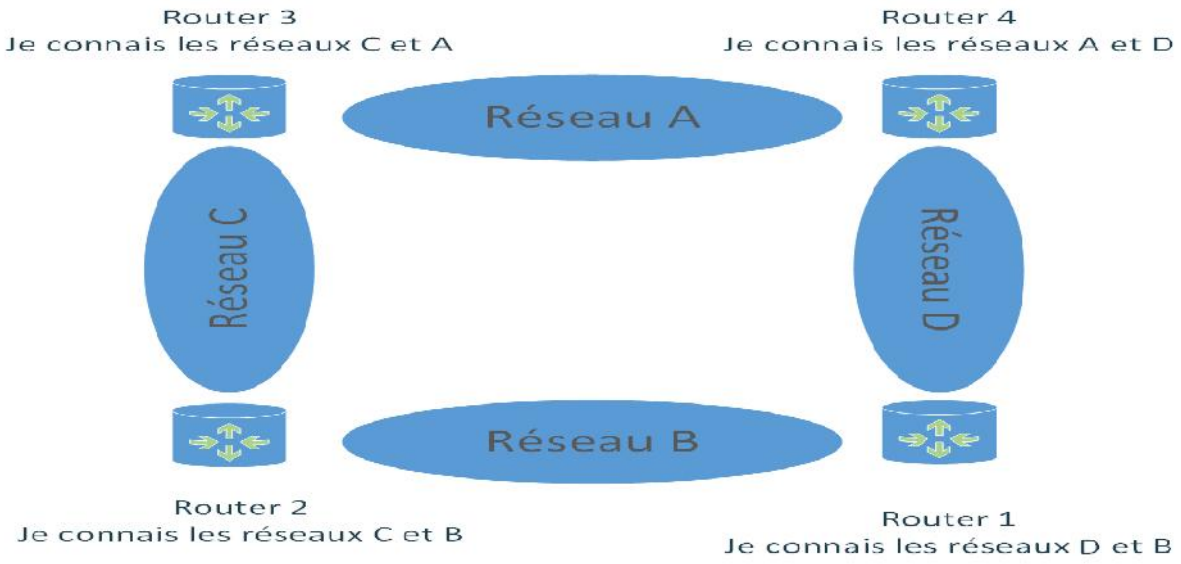


Figure 52 : l'utilité de la fonction routage

On voit ici pour aller du B au réseau A, il existe deux chemin possible. Le rôle du routage va ici être de déterminer une route (la plus prête) pour communiquer d'un réseau vers un autre quand il en existe plusieurs possibles.

3.6.3. Deux modes de routages :

Il existe deux modes de routages bien distincts lorsque nous souhaitons aborder la mise en place d'un Protocol de routage. Il s'agit du routage statique et du routage dynamique.

3.6.3.1. Routage statique :

Dans le routage statique, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes (par l'intermédiaire de port de sortie ou d'IP de destination) à emprunter pour aller sur tel ou tel réseau.

Concrètement, un routeur sera un pont entre deux réseaux et le routeur d'après sera un autre pont entre deux autres réseaux :

Figure 53 : routage statique

Ici, l'administrateur a indiqué au routeur 2 que le réseau A pouvait être joint à travers le routeur 1 qu'il connait puisque il se situe sur le même réseau B que lui. Le routage statique permet donc à l'administrateur de saisir manuellement les routes sur les routeurs et ainsi de choisir lui-même le chemin qui lui semble le meilleur pour aller d'un réseau A à un réseau B. Si un nouveau réseau vient à se crier sur le routeur 1 par exemple, il faudra indiquer au routeur 2 qu'il faut a nouveau passer par le routeur 1 pour aller sur le réseau D.
Le routage statique présente plusieurs avantages :

Economie de la bande passante c.à.d. 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 que nous allons voir plus bas, 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 a 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, il faut en effet connaitre l'intégralité de la topologie pour saisir les informations de manière exhaustive et correcte pour que les réseaux communiquent entre eux. Cela peut devenir une source d'erreur et de complexité supplémentaire quand la taille du réseau grandit.

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 part de l'administrateur qui doit modifier les routes selon l'évolution.

On voit donc que le routage statique peut être intéressant pour de petits réseaux de quelques routeurs n'évoluant pas souvent. En revanche pour des réseaux à forte évolution ou pour les réseaux de grande taille, le routage statique peut devenir complexe et long à maintenir.

3.6.3.2. Routage dynamique :

Le routage dynamique permet quand à lui de se mettre à jour de façon automatique. La définition d'un Protocol 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 Protocol de routage fixe la façon dont les routeurs vont communiquer mais également la façon dont ils vont calculer les meilleures routes à emprunter. Nous verrons un peu plus bas qu'il existe pour cela deux méthodes mais avant voici un schéma qui illustre le routage dynamique :

Figure 54 : routage dynamique

On voit ici que dans un premier temps, on ajoute le réseau C au routeur 2 (on le connecte à l'interface du routeur 2). Une annonce va ensuite suivre pour que les autres routeurs sachent que le réseau C est joignable via le routeur 2. Par la suite, les routeurs continueront à

communiquer périodiquement pour voir si chacun des routeurs est toujours joignable. Si un routeur vient à tomber et qu'une autre route existe pour accéder à un réseau, les tables de routages des routeurs vont se modifier dynamiquement via des communications faites entre les routeurs et le calcul de la meilleure route possible à emprunter. Cela facilite la transmission des informations entre les routeurs et la mise à jour des topologies réseaux. On doit bien sur pour cela définir la façon dont ils vont communiquer et calculer les routes (le Protocol de routage qu'ils doivent utiliser). Ils pourront ensuite se comprendre par l'échange de message de mise à jour, des messages '' Hello'' (indiquant que l'hôte est toujours joignable), des requêtes et des réponses diverses et différente selon le Protocol de routage.
Il est important de savoir que certains Protocoles de routage calculent les routes en fonction de la vitesse des liens, d'autre en fonction du nombre de routeurs à passer avant d'atteindre notre destination (saut).

Le routage dynamique présente les avantages suivant :

Une maintenance réduite par l'automatisation des échangent et des décisions de routage.

Une modularité et une flexibilité accrue, il est plus facile de faire évaluer 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 peur être plus compliqué à mettre en place lors de son initialisation.

Il consomme la bande passante par ce que les routeurs envoient périodiquement des messages 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 Protocol de routage et même en créer afin de se faire passer pour un membre du réseau.

Le traitement des messages réseau et le calcul de meilleures routes à emprunter représentent une consommation de CPU et de RAM supplémentaire qui peut encombrer certains éléments du réseau.

3.7. **Conclusion :**

Une infrastructure de communication optimise les coûts de fonctionnement et de maintenance d’un réseau reliant un grand nombre d’équipement informatique. Elle utilise différentes techniques de commutation pour organiser le partage des ressources. La commutation de circuits est la technique employée dans le réseau téléphonique alors que la commutation de paquets sert dans les échanges de données informatique.

Deux services réseau peuvent s’utiliser pour transférer les données. Le premier service est évolué, il est normalisé sur le plan international et fonctionne en mode connecté.

Il est couramment appelé circuit virtuel et transporte des paquets en garantissant leur séquence et leur intégrité. L’autre, plus simple, s’utilise à l’échelle mondiale dans internet. Il fonctionne en mode non connecté et transfère des datagrammes indépendants les uns des autres sans leur apporter de contrôle. Enfin des fonctions de contrôle interne-routage, contrôle de congestion et administration- assurent la bonne marche d’un réseau.

Chapitre IV : Méthodologie adoptée pour la mesure et l’analyse de flux d’information

4.1. Préambule :

Dans ce chapitre, nous allons effectuer des mesures et des analyses de flux d'informations afin d'évaluer l'évolution de la quantité d'informations transitées à l'intérieur du canal de transmission en fonction de temps. Aussi, cette application permet d'estimer les pertes dues à l'utilisation protocole UDP. Pour ce faire, nous avons utilisé les différentes commandes du système d'exploitation Linux et le logiciel Iperf. A cet effet, dans un premier temps, nous donnons ces différentes commandes et dans un second temps nous définissons les différentes caractéristiques du logiciel Iperf. Enfin, les résultats et les tests obtenus par notre application sont exposés dans ce chapitre.

4.2. Linux :

Linux est un système d'exploitation complet et libre, qui peut être utilisés en lieu et place de système d'exploitation commercialisé, tels que Windows, de Microsoft. Il est accompagné de nombreux logiciels libres complémentaires, offrant un système complet aux utilisateurs. Linux étant gratuit, différente sociétés l'on reprit et complété afin de distribuer un système d'exploitation à leur gout.

4.2.1. Les avantages de Linux par apport à Windows :

- Open source (libre) : le code source du noyau système et des programmes sont accessibles à tous (majoritairement sous la licence GPL ''licence de public général''). Cela veut dire qu'un utilisateur ou un programmeur peut modifier, ajouter ou corriger un logiciel via son code source et ce, librement, sans aucune limite dans le temps. Par conséquent, un développeur est plus en mesure de comprendre le fonctionnement du système car rien n'est caché. Cependant, sous licence GPL ou ses dérivés, certaines clauses exigent que tous utilisateurs ayant fait des ajouts ou des modifications d'un programme, ce dernier doit envoyer le code source modifiés aux concepteurs. Attention, contrairement a ce que la plupart des gens pensent, un programme peut être libre et payant a la fois.
- Gratuit (aucune licence a payé) : donc des économies pour les entreprises. Ils peuvent alors faire de bénéfices sur certains services comme l'installation et le support linux. Certaines distributions Linux sont payantes mais la plupart d'entre eux sont moins chère que Windows.

- Compatibilité multi-architecturales : Linux s'installe sur toute sorte de machine : Intel (x86),powerpc, sparc, alpha, arm…

En comparaison, à ce jour, Windows n'est compatible qu'avec les processeurs Intel (x 86) et AMD 32 bits et 64 bits (mais très peu d'applications 64 bits).

Il est logique de penser que plus un système est compatible avec plusieurs architectures informatiques, et plus cela touchera un plus grand nombre d'utilisateurs dans le monde.

- Aucun virus et spyware (fichier espion) : n'affectent les fichiers ou programmes systèmes de manières critiques ou dangereuses. Dans Linux, on n'a pas besoins ni d'anti-virus ni d'anti spyware sauf si c'est pour scanner des fichiers sur une partition dans un réseau partagé avec d'autres systèmes d'exploitations Windows.

Si les virus et les spyware sont si efficaces contre Windows, c'est que ce dernier contient d'énormes trous de sécurité et de faiblesses dans le système qui n'ont jamais été corrigés par Microsoft. Et les virus où plutôt les crackers informatiques (ceux qui conçoivent les virus et spyware) savent comment exploiter ces failles du système. Il existe quelque virus contre Linux (on peut les compter sur les doigts de la main) mais ce si ne sont pas considéré comme dangereux.

- Plus de choix de logiciels libre et gratuits : sous linux que sous Windows. Le choix des logiciels sous Linux est très impressionnant. La meilleure preuve est de vérifier le nombre total de logiciels libre pour Windows et Linux sur un serveur de programmes comme par exemple Sourceforge.net, l'un des plus gros serveurs mondiaux de logiciels multiplateformes. Plusieurs de ces logiciels deviennent vite à l'état de maturité (stabilité, performance, sécurité et professionnalisme) comme par exemple le logiciel Open office, Blender, Firefox , Mplayer…etc.

4.2.2. Les inconvénients de Linux par apport à Windows :

- Plus complexe que Windows : en effet, Linux possédant une structure plus complexe demande de la part d'utilisateur débutant une plus grande recherche et de bidouillages dans ce dernier pour s'y retrouver et ce, même s'il ya beaucoup de documentations conçues pour lui. Cela demande bien sûr, de nouvelles habitudes d'utilisation et aussi beaucoup de temps d'apprentissages.

- Pas assez de publicité : pour mieux faire connaitre Linux dans le monde. A part internet ; il n'y a que très peu de publicité faites par des entreprises, mêmes par ceux utilisant régulièrement Linux.
- Un manque de pilotes ou de drivers propriétaire pour Linux : le fait que la plupart des constructeurs de matériels informatiques ne puissent écrire des fichiers pilotes pour Linux n'aident pas beaucoup aux concepteur de noyau à mieux détecter et exploiter au maximum toutes les fonctions de certaines périphérique comme les imprimantes, scanneurs, routeurs Wifi, Webcam…etc.

Plusieurs systèmes d'exploitation pour linux sont utilisés, entre autre, a debian.

4.3. Introduction a debian :

Debian GNU/ Linux est une distribution non commerciale. Debian est une organisation à but non lucratif constituée d'un millier de développeurs bénévoles non pas par une société comme Red-Hat. Debian se distingue aussi par son système attachement très fort à la philosophie du logiciel libre. Debian se distingue aussi par son système de gestion des packages très performant et très facile à utilisé qui vous permet d'installer des logiciels, de les retirés et de les mettre à jour très facilement. D'un autre coté Debian GNU/Linux est réputé pour être un système d'exploitation très stable. Avant chaque nouvelle version, le système est longuement testé et il ne sort qu'une fois que tous les bugs connus ont été corrigés. Debian GNU/Linux est disponible sous 11 architectures dont Intel, Power PC,Sparc (Sun).

4.3.1. Installation de logiciel sous Linux (debian):

L'installation classique d'un système Debian propose une sécurité plus élevée que celle de la plupart des autres distributions. Debian contient un paquetage nommé **apt** qui automatise le téléchargement et l'installation de paquetages. Il suffit d'exécuter le programme d'installation **apt-get insatll** pour que apt télécharge le programme ainsi que tous les paquetages dont il dépend, les installe dans l'ordre adéquat et fasse appel à l'utilisateur pour toute information ou réglage nécessaire.

Trois programmes s'occupent de la gestion des paquetages Debian :**dpkg, apt-get et dselect** :

couche	programme	Fonction
Supérieur	Apt-get ou dselect	Gestion intelligente des packages : source, versions, dépendance et conflit
Inferieur	Dpkg	Installation et retrait de packages

Tableau 3 : les programmes de la gestion des paquetages Debian

Utilité « Dpkg » : Il faut éviter de l'utiliser en temps normal pour installer et désinstaller des packages, puisque qu'il ne gère pas les dépendances entre packages. Par contre, c'est souvent le seul moyen d'installer des packages qui ne sont pas présents dans la distribution. Il faut alors télécharger les fichiers correspondant aux packages et les installer avec la commande **dpkg**.

4.3.2. Utilisation de dpkg :

 # dpkg -i nom_ du_ package1.deb nom_ du_ package2.deb ou dpkg --install nom_ du_ package.deb : installe les packages package 1 et package2 (il faut installer en même temps les packages qui dépend l'un de l'autre)

 # dpkg –r package 1 : désinstalle le package 1 mais ne supprime pas ses fichiers de configuration.

#dpkg –r -- purge package1 : désinstalle le package 1 et supprime ses fichiers de configuration.

 # dpkg- reconfigure package 1 : reconfigure le package 1 qui est déjà installé.

 # dpkg –l : affiche la liste des packages installés.

Pour avoir la liste complète des options disponibles, on consulte le manuel de dpkg : **man dpkg.**

4.3.3. Utilité Apt-get :

Apt –get est la couche qui apporte une grande facilité d'utilisation au système de gestion des packages debian. On définit les sources des packages dans le fichier de configuration /etc/apt/sources.list. La gestion de l'installation et du retrait des packages tient compte des dépendances. Apt-get supporte le téléchargement des packages s'ils sont sur une source réseau. Apt-get est donc utilisé pour installer et retirer les packages inclus dans la distribution ainsi que des packages qui peuvent être inclus dans les sources.

4.3.4. Différentes commandes d'Apt-get :

 # Apt-get update : Met à jour la liste des packages disponibles.

 # Apt-get update –u upgrade : Met à jour les packages eux-mêmes à la dernière version disponibles dans les sources.

 # apt-get install package1 package2 : installe les packages package 1 et 2 et les packages dont il dépend.

 # apt-get install –f nom_du_package : forcer l'installation en cas de problème de dépendance.

 # apt-get remove package1 : désinstalle le package 1 sans effacer ses fichiers de configuration.

 # Apt-cahe search liste_de_mots_clés : Chercher un package dans la base des packages disponible.

#Apt-file search nom_du_fichier : connaitre le paquetage auquel un fichier appartient.

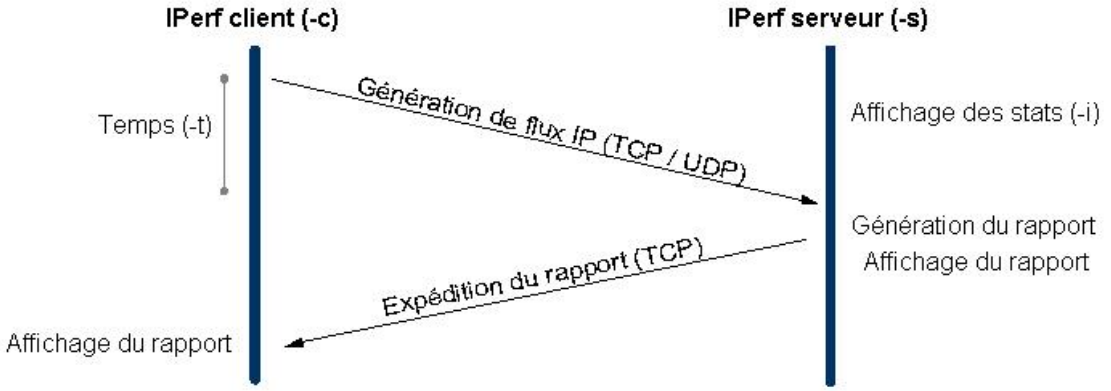
 # Apt-cache show package 1 : affiche les caractéristiques et la description du package1.

4.4. Présentation de l'outil iperf :

Iperf est un outil de réseau simple et très puissant qui a été développé pour mesurer la performance de la bande passante TCP et UDP.

Iperf est une application qui fonctionne avec un client et un serveur, il faut donc deux machines positionner aux deux extrémités du réseau à tester pour fonctionner .Cette application est disponible sur de nombreuses plateformes (Linux, BSD, Mac, Windows…), se présente sous la forme d'une ligne de commande à exécuter sur deux machines disposées aux extrémités du réseau à tester.

Iperf fonctionne comme un client/serveur selon le diagramme suivant :



[6]

Figure 55 : diagramme de fonctionnement d'iperf

Ce dernier permet d'apprécier la qualité d'un réseau que l'on peut définir par 4 valeurs :

- La bande passante en TCP.
- La latence.
- La gigue (jitter).
- Le taux de perte en UDP.

La latence : défini les délais d'aller retour d'une information transmise sur le réseau. On comprend bien que plus la latence (le temps) est faible, la connexion est meilleur.

La gigue : c'est la variation de latence, les paquets arrivent de manière irrégulière en fonction du trafic réseau.

Le taux de perte : oblige à la retransmission des données, elle affecte considérablement donc la qualité du lien réseau.

Pour démarrer un test Iperf, il faut tout d'abord l'installer sur les deux machines (client et serveur).

4.4.1. Mesure de la bande passante :

4.4.1.1. Mesure de la bande passante unidirectionnelle :

Iperf doit être lancé sur deux machines se trouvant de part et d'autre du réseau à tester. La première machine lance Iperf en « mode serveur » avec la commande suivante :

```
iperf3 –s
```

« -s » pour spécifier que ce PC est le serveur.

Ensuite, il faut se connecter au serveur depuis la machine client :

```
Iperf3 –c <ip_de_mon_serveur>
```

« -c » pour spécifier que Pc est le client

Ces deux lignes sont le moyen le plus basique d'établir une connexion entre les deux PC avec Iperf et va, par défaut, afficher du trafic TCP uniquement (mais il est également possible d'utiliser le mode UDP avec l'option -u).

La différence entre TCP et UDP :

Le TCP (transmission control Protocol) utilise des processus pour vérifier que les paquets sont correctement envoyés au receveur. Ceci n'est pas le cas pour UDP ou les paquets sont envoyés sans aucune vérification mais avec l'avantage d'être plus rapide que TCP.

Après le lancement de connexion entre les deux machines on y voit :

- les informations sur la connexion établie (IP des PCs client et serveur, ports utilisés).
- rapports intermédiaires (par exemple toutes les secondes), et le rapport qui s'affiche après dix seconde de test.
- Un résumé qui nous montre le transfert et la bande passante utilisée pour le transfert des données dans un intervalle de dix secondes.

```
------------------------------------------------------------
Accepted connection from 192.168.1.4, port 43249
[  5] local 192.168.1.7 port 5201 connected to 192.168.1.4 port 43250
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-1.00   sec  7.25 MBytes  60.7 Mbits/sec
[  5]   1.00-2.00   sec  8.39 MBytes  70.4 Mbits/sec
[  5]   2.00-3.00   sec  6.59 MBytes  55.3 Mbits/sec
[  5]   3.00-4.00   sec  6.05 MBytes  50.5 Mbits/sec
[  5]   4.00-5.00   sec  6.85 MBytes  57.7 Mbits/sec
[  5]   5.00-6.01   sec  6.91 MBytes  57.6 Mbits/sec
[  5]   6.01-7.00   sec  8.63 MBytes  72.8 Mbits/sec
[  5]   7.00-8.00   sec  10.1 MBytes  85.1 Mbits/sec
[  5]   8.00-9.00   sec  10.1 MBytes  84.5 Mbits/sec
[  5]   9.00-10.01  sec  9.35 MBytes  77.5 Mbits/sec
[  5]  10.01-10.03  sec   112 KBytes  44.8 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[  5]   0.00-10.03  sec  81.0 MBytes  67.8 Mbits/sec   13             sender
[  5]   0.00-10.03  sec  80.3 MBytes  67.2 Mbits/sec                  receiver
------------------------------------------------------------
```

Figure 56 : exemple des résultats obtenus après le lancement de connexion entre deux machines

Avec les options par défaut, le test est fait en TCP sur une durée de dix secondes.

4.4.1.2. Mesure de la bande passante bidirectionnelle :

La commande « - r » mesure la bande passante dans le sens client/serveur puis serveur/client.

```
------------------------------------------------------------
Client connecting to 192.168.1.7, TCP port 5001
TCP window size: 43.8 KByte (default)
------------------------------------------------------------
[  5] local 192.168.1.8 port 33429 connected with 192.168.1.7 port 5001
[  5]  0.0-10.1 sec  84.1 MBytes  69.5 Mbits/sec
[  4] local 192.168.1.8 port 5001 connected with 192.168.1.7 port 56796
[  4]  0.0-10.2 sec  70.4 MBytes  57.7 Mbits/sec
------------------------------------------------------------
Client connecting to 192.168.1.7, TCP port 5001
TCP window size: 43.8 KByte (default)
------------------------------------------------------------
[  4] local 192.168.1.8 port 33430 connected with 192.168.1.7 port 5001
[  4]  0.0-10.1 sec  38.4 MBytes  31.9 Mbits/sec
```

Figure 57 : exemple de mesure de la bande passante bidirectionnelle

Donc 57.7 Mbits/sec dans le sens client/serveur et 31.9 Mbits/sec dans l'autre sens.

4.4.1.3. Mesure de la bande passante bidirectionnelle simultanée (-r –d) :

```
^Croot@debian:/home/debian# iperf -c 192.168.1.7 -p 5001 -r -d
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
------------------------------------------------------------
Client connecting to 192.168.1.7, TCP port 5001
TCP window size: 43.8 KByte (default)
------------------------------------------------------------
[  5] local 192.168.1.8 port 33431 connected with 192.168.1.7 port 5001
[  4] local 192.168.1.8 port 5001 connected with 192.168.1.7 port 56797
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-10.1 sec  24.5 MBytes  20.4 Mbits/sec
[  4]  0.0-10.2 sec  45.8 MBytes  37.5 Mbits/sec
```

Figure 58 : exemple de mesure de la bande passante bidirectionnelle simultanée.

20.4 Mbits/sec dans le sens client serveur et 37.5 Mbits/sec dans l'autre sens.

Lors de tests dans les deux sens, il vaut mieux utiliser l'option « -r » plutôt que « -d ». en effet, lors d'un test full duplex a de hauts débits, Le CPU des machines aux deux extrémités est très sollicitée et fausse largement la mesure. Avec l'option « -r », le test est d'abord fait dans un sens, puis il est lancé dans l'autre sens. Le résultat est plus pertinent.

4.5. Mesure de la gigue et perte de paquet :

Pour évaluer la gigue nous allons transmettre les paquets en UDP et en bidirectionnelle simultanée de manière à saturer notre lien réseau.

```
root@debian:/home/debian# iperf -c 192.168.1.7 -p 5001 -d -u -b 10m
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  160 KByte (default)
------------------------------------------------------------
------------------------------------------------------------
Client connecting to 192.168.1.7, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  160 KByte (default)
------------------------------------------------------------
[  4] local 192.168.1.8 port 57270 connected with 192.168.1.7 port 5001
[  3] local 192.168.1.8 port 5001 connected with 192.168.1.7 port 53195
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec  3.42 MBytes  2.86 Mbits/sec
[  4] Sent 2440 datagrams
[  3]  0.0-10.0 sec  11.3 MBytes  9.51 Mbits/sec  1.841 ms  414/ 8504 (4.9%)
[  3]  0.0-10.0 sec  1 datagrams received out-of-order
```

Figure 59 : exemple de mesure de la gigue et la perte de paquet.

On remarque que le résultat de la gigue est de 1.841 ms, donc nous avons des pertes de datagrammes qu'est de 414 paquets perdus. Alors à chaque fois la gigue augmente, le nombre de datagrammes perdus sera plus important.

4.6. Affichage de la taille de segment maximale (-m) :

La taille de segment maximale(ou en anglais, Maximum Segment Size, MSS) est la plus grande quantité de données, en octets (bytes) qu'un ordinateur peut supporter. Le MTU définit la taille maximale (en octet) du paquet pouvant être transmis en une seule fois. Pour l'Ethernet, cette valeur doit être de 1500 octets. Elle peut être calculée de la manière suivante :

MSS = MTU – en-têtes TCP & IP

Les en-têtes TCP & IP occupent 40 octets. La MTU (Maximum Transmission Unit, unité de transmission maximale) est la plus grande quantité de données qui peut être transférée dans une trame. La découverte de cette valeur peut être utile à l'optimisation de votre réseau et des applications qui tournent dessus.

Généralement, une MTU (et une MSS) élevée permet une plus grande bande passante.

```
Sur la machine S: # iperf -s -m
Sur la machine C: # iperf -c IPS
Résultat (à lire sur la machine S):
------------------------------------------------------------
Client connecting to 192.168.29.1, TCP port 5001
TCP window size: 56.0 KByte (default)
------------------------------------------------------------
[ 3] local 192.168.29.157 port 65066 connected with 192.168.29.1 port 5001
[ 3] 0.0-10.0 sec 112 MBytes 93.5 Mbits/sec[ 3] MSS size 1448 bytes (MTU
1500 bytes, ethernet)
```

Figure 60 : exemple de l'affichage de la taille de segment maximale.

4.7. Pour générer deux flux réseau entre S et C :

Il est parfois utile de générer plusieurs flux simultanément pour simuler une application. Iperf permet cela grâce a l'option –P et en donnant le nombre de flux à générer. L'exemple suivant génère deux flux TCP entre S et C.

Coté client :

```
c:\iperf>iperf -c 10.90.90.10 -P 2
------------------------------------------------------------
Client connecting to 10.90.90.10, TCP port 5001
TCP window size: 63.0 KByte (default)
------------------------------------------------------------
[  4] local 10.90.90.9 port 49301 connected with 10.90.90.10 port 5001
[  3] local 10.90.90.9 port 49300 connected with 10.90.90.10 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 7.0 sec   388 MBytes   464 Mbits/sec
[  4]  0.0-10.0 sec   591 MBytes   495 Mbits/sec
[SUM]  0.0-10.0 sec   979 MBytes   821 Mbits/sec
```

Coté serveur :

```
[  4] local 10.90.90.10 port 5001 connected with 10.90.90.9 port 49300
[  5] local 10.90.90.10 port 5001 connected with 10.90.90.9 port 49301
[  4]  0.0-10.0 sec   388 MBytes   325 Mbits/sec
[  5]  0.0-13.0 sec   591 MBytes   381 Mbits/sec
[SUM]  0.0-13.0 sec   979 MBytes   632 Mbits/sec
```

4.8. Exemple pour tester un flux de type VOIP :

Les paquets de type voix sur IP ont les caractéristiques suivantes : protocole UDP et taille des paquets petites (bien inférieur au MTU). Le meilleur moyen de tester un flux de type VOIP avec iperf est d'utiliser les options –l (taille du datagramme) et –w (taille maximale du buffer recevant les datagrammes) en fixant une valeur de datagramme inférieure a celle du buffer.

La taille du datagramme est fixée par défaut à 8K pour TCP et 1470 pour UDP.

Testons avec un buffer de 40 en UDP, ce qui correspond a la taille des paquets de VOIP.

```
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 40 byte datagrams
UDP buffer size:   108 KByte (default)
------------------------------------------------------------
[  3] local 10.33.100.1 port 5001 connected with 10.33.102.12 port 32790
[  3]  0.0-10.0 sec  1.24 MBytes  1.04 Mbits/sec  0.003 ms  178/32772 (0.54%)
[  3]  0.0-10.0 sec  1 datagrams received out-of-order
```

```
# iperf -c 10.33.100.1 -u -l 40
------------------------------------------------------------
Client connecting to 10.33.100.1, UDP port 5001
Sending 40 byte datagrams
UDP buffer size:   107 KByte (default)
------------------------------------------------------------
[  5] local 10.33.102.12 port 32790 connected with 10.33.100.1 port 5001
[  5]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  5] Sent 32773 datagrams
```

Remarque : L'option –l ne fonctionne pas toujours quand vous utilisez des OS différents entre le client et le serveur

4.9. Pour générer le format du débit réseau :

En utilisant la commande « -f » et en rajoutant une lettre spécifiant le format pour afficher la bande passante.

Les formats supportés sont :

' k ' = Kbits/sec ' K '= Koctets/sec

' m'= Mbits/sec ' M'= Moctets/sec

```
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[  5]   0.00-10.25  sec   113 MBytes  11.0 MBytes/sec    0             sender
[  5]   0.00-10.25  sec   111 MBytes  10.9 MBytes/sec                  receiver
------------------------------------------------------------
```

Figure 61 : format de débit en Moctets/sec

4.10. Pour définir les tailles de tampon (-w):

La taille de la fenêtre TCP correspond aux données qui peuvent être mise en tampon pendant une connexion sans la validation du receveur. On parle aussi de fenêtre glissante car cette fenêtre peut varier en fonction de la qualité du réseau.

Sur les systèmes Linux, quand on spécifie une taille de fenêtre TCP avec l'argument –w, le noyau alloue le double de la valeur indiquée.

4.11. Pour fixer la durée du test :

Il peut être utile de générer un flux réseau plus long pour tester par exemple une liaison Internet pendant les heures d'utilisation.

Alors la commande « -t » spécifie la durée du test en seconde.

4.12. D'autres commandes d'iperf :

Le tableau suivant nous montre d'autres options d'Iperf :

Options de la ligne de commande	**Options générales Clients/serveurs**
-F	Coté client : lire le fichier et écrire sur le réseau, au lieu d'utiliser des données aléatoires. Coté serveur : lire a partir du réseau et écrire dans le fichier au lieu de jeter les données.
-o	Afficher le rapport ou le message d'erreur à cette durée spécifiée.
-B	Lier à l'hôte, une interface ou une adresse de multidiffusion.
-C	Pour une utilisation avec les anciennes versions ne provoque pas de messages supplémentaires.
-M	Définir la taille maximale du segment.
-V	Définir le domaine vers IPv6.

Options de la ligne de commande	**Options spécifiques au client**
-n	Nombre d'octets a transmettre (au lieu de –t).
-I	Saisir les données à transmettre a partir de stdin.
-L	Pour lancer des tests parallèles.
-T	Préfixer chaque ligne de sortie avec cette chaine de caractères.
-4	Réaliser le test en IPv4 uniquement.
-6	Réaliser le test en IPv6 uniquement.

Tableau 4 : d'autres commandes d'iperf.

4.13. Tests et résultats

Pour tous les tests que nous avons réalisés, la bande passante du canal est de 100 Mbits/s

4.13.1. Test entre deux postes :

Avant de lancer le test entre deux machines reliées par un Switch, la première étape consiste à définir un client et un serveur avec les différentes commandes.

La figure suivante montre les résultats obtenus :

```
root@debian:/home/debian# iperf -s -t 1800 -i 300
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 10.2.64.200 port 5001 connected with 10.2.100.50 port 49465
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-300.0 sec  3.24 GBytes  92.7 Mbits/sec
[  4] 300.0-600.0 sec  3.25 GBytes  92.9 Mbits/sec
[  4] 600.0-900.0 sec  3.21 GBytes  92.0 Mbits/sec
[  4] 900.0-1200.0 sec  3.25 GBytes  92.9 Mbits/sec
[  4] 1200.0-1500.0 sec  3.27 GBytes  93.5 Mbits/sec
[  4] 1500.0-1800.0 sec  3.25 GBytes  93.0 Mbits/sec
[  4]  0.0-1800.3 sec  19.5 GBytes  92.9 Mbits/sec
```

Figure 62 : les résultats du test entre deux postes.

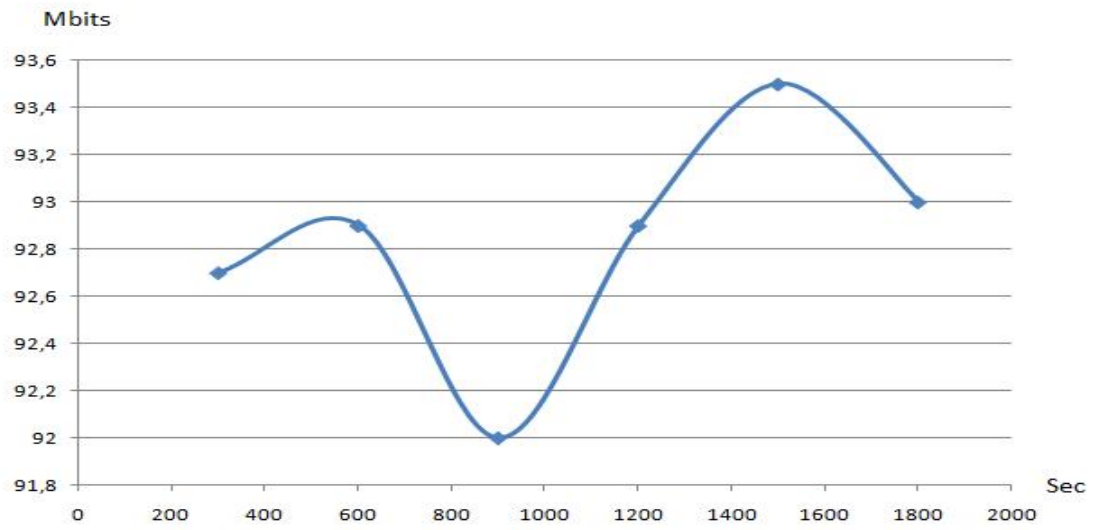


Figure 63 : les résultats graphiques entre deux postes.

Nous remarquons que les valeurs de la bande passante se varient entre 92 Mbits/s et 94Mbits/s.

Dans cette durée du test nous constatons que le nombre d'utilisateurs sur ce réseau est très élevé, on conclue alors que les valeurs mesurées sont très proches de la capacité du canal (100Mbits/s), ce qu'implique que la bande passante restante est insuffisante pour effectuer une transmission rapide.

4.13.2. Test entre CSRI et réseau informatique de bastos :

Nous lançons un test entre le CSRI et le réseau informatique de bastos pendant 15 minutes avec un intervalle de 3 minutes. Nous avons déclaré le CSRI comme serveur et on a reçu les résultats tels que la figure (64) le montre :

```
iperf -s -P 0 -i 180 -p 5001 -f m
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 0.08 MByte (default)
------------------------------------------------------------
[  4] local 10.2.95.175 port 5001 connected with 10.5.1.5 port 54202
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-180.0 sec  1950 MBytes  90.9 Mbits/sec
[  4] 180.0-360.0 sec  1952 MBytes  91.0 Mbits/sec
[  4] 360.0-540.0 sec  1947 MBytes  90.7 Mbits/sec
[  4] 540.0-720.0 sec  1937 MBytes  90.3 Mbits/sec
[  4] 720.0-900.0 sec  1919 MBytes  89.4 Mbits/sec
[  4]  0.0-900.0 sec  9705 MBytes  90.5 Mbits/sec
```

Figure 64 : Les résultats du test entre CSRI et réseau informatique de bastos.

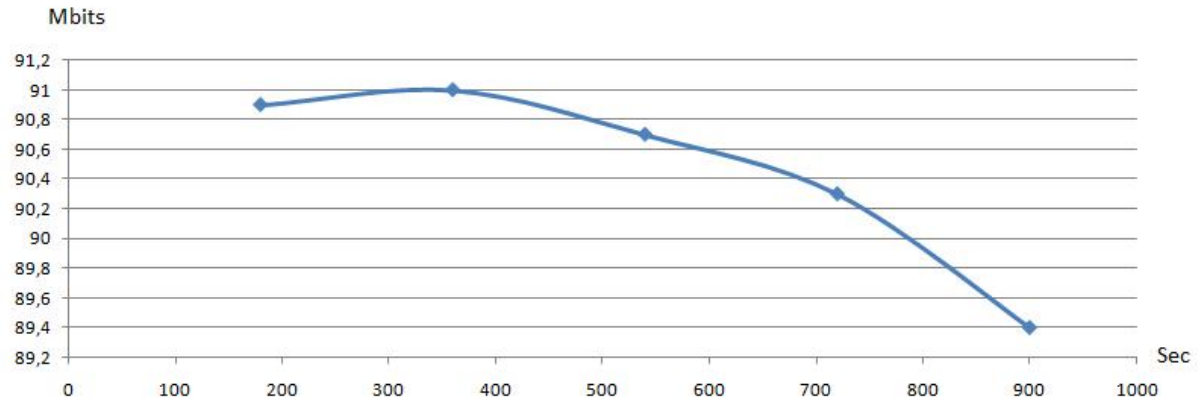


Figure 65 : les résultats graphiques du test entre CSRI et réseau informatique du bastos.

Nous constatons que les résultats obtenus de la bande passante varient entre 89 Mbits/s et 91 Mbits/s, cela signifie une grande exploitation de la bande passante du canal par les utilisateurs.

4.13.3. Test entre le CSRI et le département anglais.

Nous définissions le CSRI en tant que serveur et le département anglais en tant que client sur une durée du temps de 30 minutes avec un intervalle de 5 minutes.

la figure (66) nous montre les résultats de ce test .

```
root@debian:/home/debian# iperf -c 10.2.0.20 -p 5001 -t 1800 -i 300
------------------------------------------------------------
Client connecting to 10.2.0.20, TCP port 5001
TCP window size: 43.8 KByte (default)
------------------------------------------------------------
[  3] local 10.8.54.236 port 56817 connected with 10.2.0.20 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-300.0 sec   589 MBytes  16.5 Mbits/sec
[  3] 300.0-600.0 sec  2.36 GBytes  67.6 Mbits/sec
[  3] 600.0-900.0 sec  2.46 GBytes  70.3 Mbits/sec
[  3] 900.0-1200.0 sec  1.46 GBytes  41.8 Mbits/sec
[  3] 1200.0-1500.0 sec  1.26 GBytes  36.0 Mbits/sec
[  3] 1500.0-1800.0 sec  1.15 GBytes  33.0 Mbits/sec
[  3]  0.0-1800.1 sec  9.27 GBytes  44.2 Mbits/sec
```

Figure 66 : les résultats du test entre le CSRI et le département anglais.

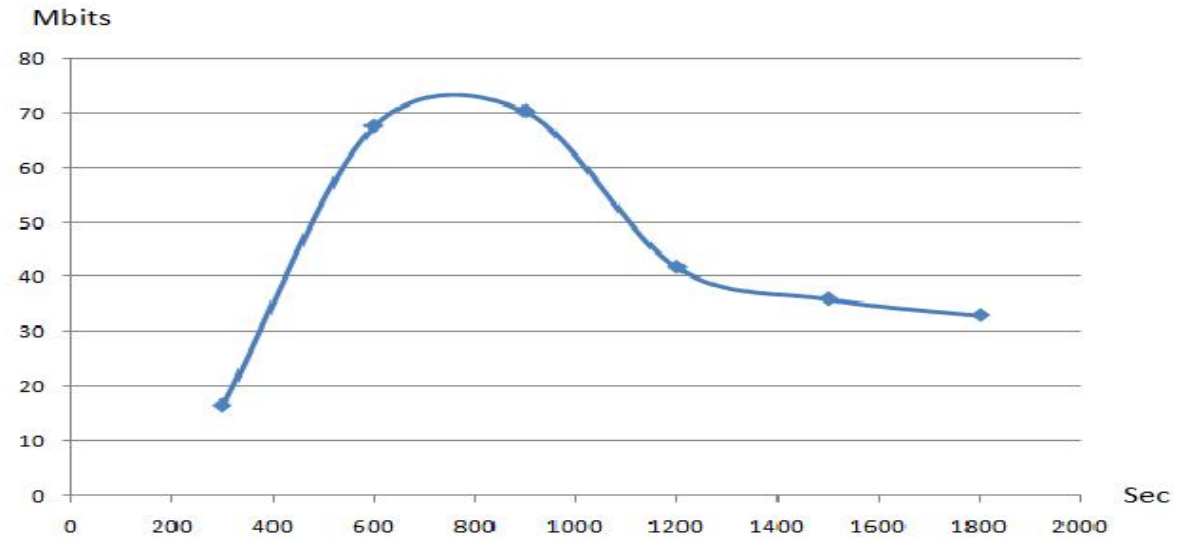


Figure 67 : représentation graphiques des résultats du test entre le CSRI et le département anglais.

Les valeurs de la bande passante varient entre 16Mbits/s et 71Mbits/s, ce qui veut dire qu'elle a été moins utilisée par les utilisateurs, de ce fait la transmission des données sera plus fiable entre les équipements interconnectés au réseau.

4.13.4. Test entre le CSRI et bastos pendant 24h :

Nous avons effectués un test entre le CSRI et le réseau informatique de bastos en fixant la durée du test a 24h et un intervalle de temps de 30 minutes pour nous fournir des résultats de la bande passante maximale atteignable entre ces deux stations.

La figure (68) nous montre les résultats de ce test :

```
[  3] local 10.5.1.5 port 41235 connected with 10.2.0.20 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-1800.0 sec  19.1 GBytes  91.1 Mbits/sec
[  3] 1800.0-3600.0 sec  17.2 GBytes  82.2 Mbits/sec
[  3] 3600.0-5400.0 sec  5.56 GBytes  26.5 Mbits/sec
[  3] 5400.0-7200.0 sec  15.6 GBytes  74.4 Mbits/sec
[  3] 7200.0-9000.0 sec  18.8 GBytes  89.7 Mbits/sec
[  3] 9000.0-10800.0 sec  18.8 GBytes  89.7 Mbits/sec
[  3] 10800.0-12600.0 sec  19.0 GBytes  90.8 Mbits/sec
[  3] 12600.0-14400.0 sec  19.0 GBytes  90.5 Mbits/sec
[  3] 14400.0-16200.0 sec  18.9 GBytes  90.2 Mbits/sec
[  3] 16200.0-18000.0 sec  19.2 GBytes  91.5 Mbits/sec
[  3] 18000.0-19800.0 sec  10.3 GBytes  49.2 Mbits/sec
[  3] 19800.0-21600.0 sec  19.1 GBytes  91.2 Mbits/sec
[  3] 21600.0-23400.0 sec  19.2 GBytes  91.4 Mbits/sec
[  3] 23400.0-25200.0 sec  19.0 GBytes  90.5 Mbits/sec
[  3] 25200.0-27000.0 sec  19.2 GBytes  91.7 Mbits/sec
[  3] 27000.0-28800.0 sec  19.6 GBytes  93.7 Mbits/sec
[  3] 28800.0-30600.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 30600.0-32400.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 32400.0-34200.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 34200.0-36000.0 sec  19.7 GBytes  94.0 Mbits/sec
[  3] 36000.0-37800.0 sec  19.7 GBytes  93.9 Mbits/sec
[  3] 37800.0-39600.0 sec  19.7 GBytes  93.9 Mbits/sec
[  3] 39600.0-41400.0 sec  19.7 GBytes  93.8 Mbits/sec
[  3] 41400.0-43200.0 sec  19.7 GBytes  93.8 Mbits/sec
[  3] 43200.0-45000.0 sec  19.7 GBytes  93.9 Mbits/sec
[  3] 45000.0-46800.0 sec  19.7 GBytes  94.0 Mbits/sec
[  3] 46800.0-48600.0 sec  19.7 GBytes  93.9 Mbits/sec
[  3] 48600.0-50400.0 sec  19.7 GBytes  94.0 Mbits/sec
[  3] 50400.0-52200.0 sec  19.7 GBytes  93.9 Mbits/sec
[  3] 52200.0-54000.0 sec  19.7 GBytes  93.9 Mbits/sec
[  3] 54000.0-55800.0 sec  19.7 GBytes  93.9 Mbits/sec
[  3] 55800.0-57600.0 sec  19.7 GBytes  93.8 Mbits/sec
[  3] 57600.0-59400.0 sec  19.7 GBytes  93.8 Mbits/sec
[  3] 59400.0-61200.0 sec  19.6 GBytes  93.8 Mbits/sec
[  3] 61200.0-63000.0 sec  19.6 GBytes  93.7 Mbits/sec
[  3] 63000.0-64800.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 64800.0-66600.0 sec  19.7 GBytes  93.8 Mbits/sec
[  3] 66600.0-68400.0 sec  19.7 GBytes  93.9 Mbits/sec
[  3] 68400.0-70200.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 70200.0-72000.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 72000.0-73800.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 73800.0-75600.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 75600.0-77400.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 77400.0-79200.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 79200.0-81000.0 sec  19.7 GBytes  94.1 Mbits/sec
[  3] 81000.0-82800.0 sec  19.6 GBytes  93.6 Mbits/sec
[  3] 82800.0-84600.0 sec  19.3 GBytes  91.9 Mbits/sec
[  3] 84600.0-86400.0 sec  19.2 GBytes  91.5 Mbits/sec
[  3]  0.0-86400.0 sec   907 GBytes  90.1 Mbits/sec
univ-tizi2:~#
```

Figure 68 : résultats du test entre le CSRI et le réseau informatique de bastos.

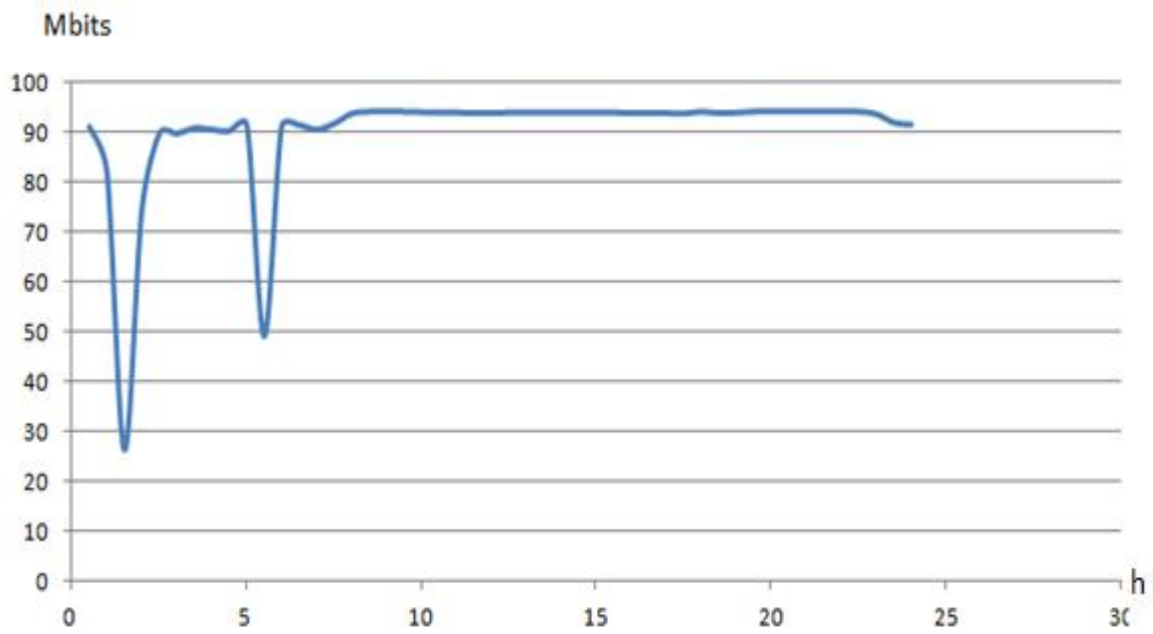


Figure 69 : représentation graphique des résultats du test entre le CSRI et le réseau informatique de bastos.

Nous remarquons pendant les deux premières heures, que la bande passante de notre réseau varie entre 26 Mbits/s à 92Mbits/s, Ce qui explique que le nombre d'utilisateurs a cette heure-ci exploitent une bande passante moyenne du canal.

Pour les trois prochaines heures nous remarquons que la bande passante atteint 92 Mbits/s, ce que signifie que le nombre d'utilisateurs a augmenté et cela influe sur la quantité de la bande passante disponible sur le canal.

Ensuite, pour la prochaine heure nous constatons que la bande passante du canal se libère jusqu'à 49 Mbits/s, donc nous avons moins d'utilisateurs qui consomment le débit de ce canal.

Enfin, pour les heures restantes on remarque une stabilité de la bande passante à 94 Mbits/s, ce qui signifie que la consommation de la bande passante par les utilisateurs est presque la même sur cette durée.

4.12.5. Tests de la gigue et la perte des datagrammes entre le CSRI et bastos :

En utilisant le protocole UDP pour mesurer la gigue et la perte des datagrammes lors d'une transmissions, nous allons effectuer un test entre le CSRI et le réseau informatique de bastos en fixant la durée du test a 1h et un intervalle de temps de 5 minutes,

La figure (70) montre les résultats du test :

```
^Croot@debian:/home/debian# iperf -c 10.5.1.5 -p 5001 -u -t 3600 -i 300
------------------------------------------------------------
Client connecting to 10.5.1.5, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  160 KByte (default)
------------------------------------------------------------
[  3] local 10.2.117.131 port 47026 connected with 10.5.1.5 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-300.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 300.0-600.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 600.0-900.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 900.0-1200.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 1200.0-1500.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 1500.0-1800.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 1800.0-2100.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 2100.0-2400.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 2400.0-2700.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 2700.0-3000.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 3000.0-3300.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3] 3300.0-3600.0 sec  37.5 MBytes  1.05 Mbits/sec
[  3]  0.0-3600.0 sec   450 MBytes  1.05 Mbits/sec
[  3] Sent 321000 datagrams
[  3] Server Report:
[  3]  0.0-3600.1 sec   450 MBytes  1.05 Mbits/sec   0.044 ms    0/321000 (0%)
```

Figure 70 : les résultats du test entre le CSRI et le réseau informatique de bastos avec le protocole UDP

D'après les résultats qu'on a obtenus, nous remarquons que la gigue est de 0.044 ms sans perte de paquets.

On constate que les différents datagrammes ont suivi un chemin correct vers le destinataire, ce qui résulte un bon acheminement d'information, donc pas de perte de datagrammes

Il est tout à fait possible d'avoir une latence élevée, par exemple de 200ms, et d'avoir une gigue très faible 0.044 ms. Cella veut dire que la latence est toujours la même. Le problème d'une gigue élevée (donc une latence qui n'arrête pas de varier), c'est que par moment les paquets vont arriver tous d'un coup, et par moment aucun paquet n'arrivera.

4.14. Discussion :

Dans ce chapitre, nous avons effectué des tests avec le logiciel iperf qui permet de faire des différentes fonctionnalités tels que la mesure de la bande passante maximale atteignable sur le réseau, la gigue et la perte de datagramme. Ce logiciel se présente sous la forme d'une ligne de commande à exécuter sur deux machines disposées à l'extrémité du réseau à tester.

Nous avons lancé des tests entre les différents départements tels que : réseau informatique de bastos, département d'anglais… etc. Après l'interprétation des résultats nous avons déduit que la consommation de la bande passante est relative au nombre d'utilisateurs, plus le nombre d'utilisateurs augmente, plus la consommation de la bande passante sera élevée ; ce qui provoque une transmission lente entre les équipements interconnectés aux réseaux et peut même engendrer une saturation temporaire du canal, donc ce logiciel nous permet de vérifier toute ses fonctionnalités. Et nous permet aussi si un utilisateur se plaint d'une lenteur généralisée des accès de sa machine, des tests Iperf mettront en évidence des éventuels problèmes réseaux. Si les résultats de tests effectués dans les deux sens montrent une forte asymétrie en termes de performances ou de pertes avec plusieurs machines, c'est souvent le signe d'un câble réseau défectueux.

Conclusion générale

5. Conclusion générale :

Durant ce travail, nous nous sommes intéressés à la mesure de la bande passante disponible dans un chemin entre deux extrémités. En utilisant l'outil de mesure et d'analyse de flux (trafic) Iperf pour objectif d'avoir les différentes valeurs de la bande passante.

Dans notre projet, nous avons effectué des différents tests entre le centre des systèmes et réseaux d'informations et les différents départements, et nous avons obtenu des résultats qui sont exposé dans le quatrième chapitre. D'après tout ses tests on a conclue que plus le nombre des utilisateurs augmente, plus l'occupation de la bande passante dans le canal sera plus élevée, cela influencera sur la transmission des données entre les équipements. Ce qui provoque une connexion lente entre les départements (encombrement du canal) et des fois même une saturation temporaire.

La gigue et la latence joue un rôle très important lors d'une transmission. La latence nous permet de nous informer sur les délais d'aller retour d'une information transmise sur le réseau. Pour ce qui concerne la gigue c'est la variation de la latence. On a conclue alors plus la gigue augmente, les valeurs de la latence sont pas stable, ce qui perturbera le transfert des datagrammes d'un réseau a un autre.

Il devrait être relativement aisé de produire une solution plus poussée avec des logiciels payants, disposant d'outils plus avancés et de plus de fonctionnalités. La perspective de ce travail peut être envisagée dans ce sens.

Bibliographie :

[1] Lorenzo cortes, détection et analyse d'un problème de congestion réseau, informatique de gestion, Haute école de gestion de Genève, 2015,82.

[2] https://www.bestcours.com

[3] Nicolas baudru, réseau 1, transmission de données, 2010-2011.

[4] Claude Servin, Jean-Pierre Arnaud, Réseau et Télécoms, Edition Dunod (2003).

[5] Danièle Dromard, Dominique Seret, Architecture des réseaux, Edition Collection Synthex (2009).

[6] Nicolas Hennion, Tester la performance de votre réseau avec Iperf, 9 mars 2007-mise a jour le 3 octobre 2013

Site WEB :

http://ofppt.info/wp-content/uploads/2014/07/C-005.pdf

http://www.commentcamarche.net/contents/1113-ethernet

http://hautrive.free.fr/reseaux/supports/methodes-acces-au-reseau.html

http://csud.educanet2.ch/3oc-info/3_Internet/3_Reseaux/page2.html

http://xcotton.pagespersoorange.fr/electron/generalites_sur_la_transmission_des_donnees.pdf

http://www.commentcamarche.net/contents/1131-transmission-de-donnees-les-modes-de-transmission

http://www.amphenol-socapex.com/wp-content/themes/amphenol_socapex_theme /downloads/pdf/Comprendre_la_Fibre_Optique_DOC-000537-FRA-A.pdf

http://www.samomoi.com/teleinformatique/le_codage_numerique_fin.php

http://liris.cnrs.fr/amille/enseignements/emiage/emiage%20-%20ModuleC214/ GMC/214_5_1.htm

https://repo.zenk-security.com/Protocoles_reseaux_securisation/Les_reseaux_ATM.pdf

https://www.it-connect.fr/routage-statique-et-routage-dynamique/

Annexe :

Topologie en arbre :

Dans une topologie en arbre, le réseau est divisé en niveaux. Le sommet est connecté à plusieurs nœuds de niveau inférieur dans la hiérarchie. Ces nœuds peuvent eux-mêmes être connectés à plusieurs nœuds de niveau inférieur.

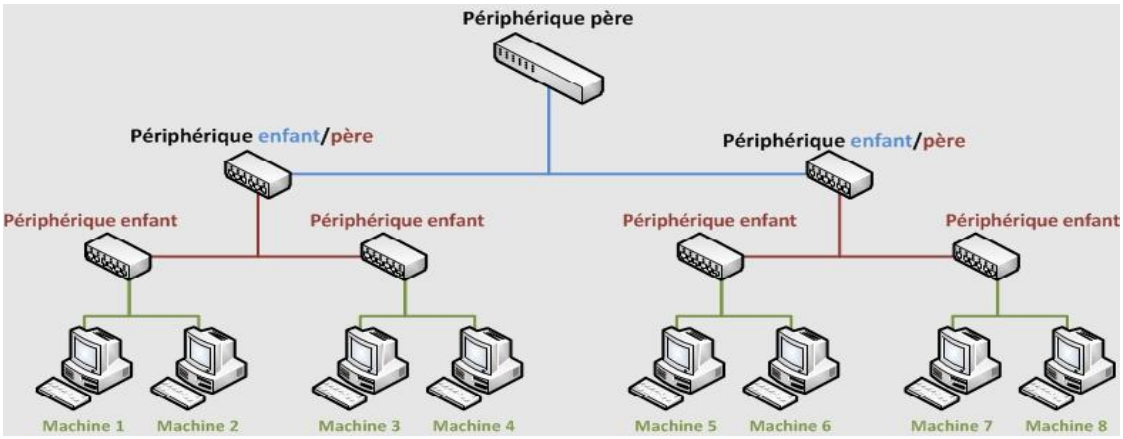


Figure : Topologie en arbre

Cette topologie permet de compartimenter un réseau en sous-réseaux hiérarchisé et de séparer certains composants d'autres composants tout comme d'isoler une pane, une pane d'un nœud n'affectant que ses sous-nœuds et pas le reste du réseau. Une telle topologie réduit également la longueur totale des câbles et leurs coûts par rapport à un réseau en étoile et simplifie la recherche d'un ordinateur dans le réseau par rapport à une topologie maillé. Néanmoins, dans cette topologie, une panne d'un nœud empêche tous les nœuds de chaque branche en étant issue d'échanger des informations avec les nœuds des autres branches partant de ce même nœud. De plus une panne du nœud racine empêche à touts les réseaux d'accéder à des services externes comme Internet.[1]

Structure générale d'une Chaine de transmission :

La chaine de transmission de l'information, dans sa structure fonctionnelle la plus simple est constituée :

- D'un émetteur.
- D'un canal de transmission.
- D'un récepteur.

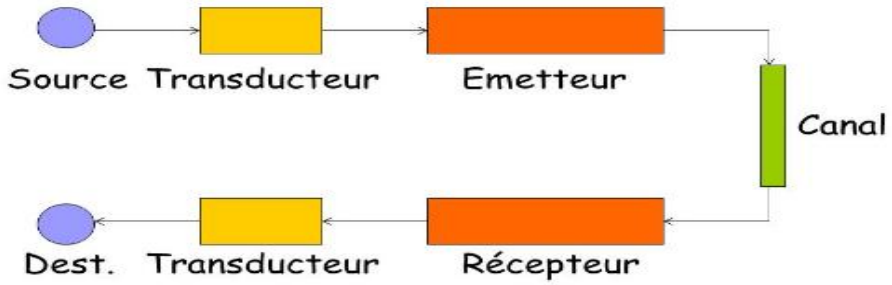


Figure : chaine de transmission

Transducteur à l'émission :

Transducteur à l'émission permet de convertir le signal original (voix, image …) en un signal électrique utile pour l'émetteur.

L'émetteur :

L'émetteur a pour fonction d'adapter le signal issu du transducteur en vue de le transmettre au canal de transmission. Il peut simultanément remplir plusieurs fonctions :

Coder le signal issu du transducteur (tension) en nombre.

Moduler, amplifier.

Le canal de transmission :

Le canal de transmission permet au récepteur de recevoir l'information émise par l'émetteur.

Le récepteur :

Son rôle est àla fois de recevoir le signal émis ainsi que de le rendre compatible avec le transducteur (exemple haut parleur) servant à la réception. Les actions réalisées par le récepteur sont alors les suivantes :

- Filtrer le signal reçu.
- Décoder.
- Amplifier le signal pour le rendre utilisable par le transducteur de sortie.

Transducteur à la sortie :

Son rôle est de fournir une information exploitable par le destinataire sous forme d'un signal.

Notion de spectre du signal :

Le mathématicien français Joseph Fourier a montré que tous signal périodique de forme quelconque pouvaient être décomposés en une somme des signaux élémentaires sinusoïdaux (fondamentale et harmonique) autour d'une valeur moyenne (composante continue) qui pouvait être nulle. L'ensemble de ces composantes forme le spectre du signal ou bande de fréquence occupé par le signal (largeur de bande).

Temps de propagation :

Le temps de propagation **TP** est le temps nécessaire à un signal pour parcourir un support d'un point à un autre, ce temps dépend donc de la nature du support, de la distance et également de la fréquence du signal.

Temps de transmission :

Le Temps de transmission (ou de traitement) Tt est le délai qui s'écoule entre le début et la fin de la transmission d'un message sur une ligne, ce temps est donc égale au rapport entre la longueur du message et le débit de la ligne.

Tt= L/D

Temps de traversée :

Le temps de traversée ou délai d'acheminement sur une voie est égale au temps totale mis par un message pour parvenir d'un point à un autre, c'est donc la somme des temps TP et Tt.

Le temps de traversée = TP+ Tt

Bruit et distorsion :

Les supports de transmission déforment les signaux qu'ils transportent, même lorsque leurs fréquences sont adaptées, comme l'illustre la figure 20.Diverses sources de bruit perturbent les signaux : parasites, phénomène de diaphonie…Certaines perturbation de l'environnement introduisent également des bruits (foudre, champ électromagnétiques dans des ateliers…).

Par ailleurs, les supports affaiblissent et retardent les signaux. La distance est un facteur d'affaiblissement .Ces déformations appelées distorsions, sont gênantes pour la bonne reconnaissance des signaux en sortie, d'autant qu'elles varient avec la fréquence et la phase.

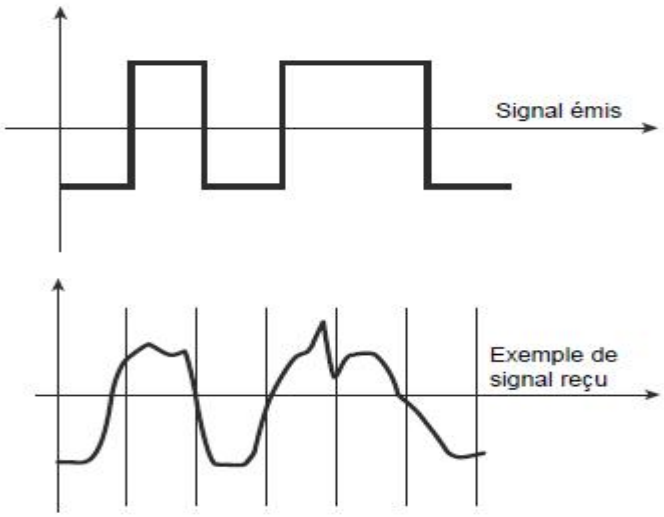


Figure : signal émis et exemple de signal reçu

Même lorsque les signaux sont adaptés aux supports, on ne peut pas garantir leur réception correcte à 100% .Le récepteur d'un signal doit prendre une décision dans un laps de temps très court. De ce fait, cette décision peut être mauvaise. Par exemple, un symbole 1 émis donne une décision «symbole0 reçu », ce qui constitue une erreur de transmission. Les fibres optiques sont les meilleurs supports, car le taux d'erreur y est très faible. Les câbles et les supports métalliques présentent des taux d'erreur moyens.

Code bipolaire simple AMI :

Utilisation : ligne DS1/T1 (utilisé par le système de téléphonie numérique PCM sur la ligne de transmission T1).

Principe : Les 0 sont représentés par des potentiels nuls, les 1 par +V et –V en alternance.

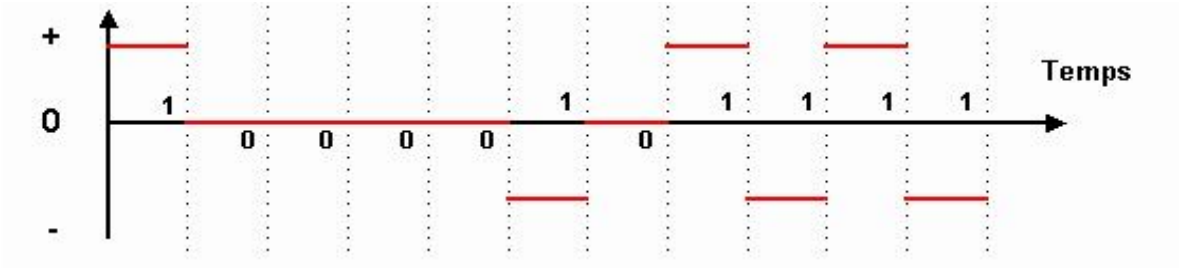


Figure : codage AMI

Il peut y avoir de longues séquences sans potentiel et donc perte de synchronisation.

Codage NRZ (No Return to Zero):

Le codage NRZ permet une symétrie de la valeur des niveaux logiques hauts et des niveaux logiques bas par apports à un niveau de potentiel nul, ce qui nous donne :

Niveau logique	codage NRZ
BAS	- V
HAUT	+ V

Ce codage permet la diminution de la valeur de la composante continue.

Exemple :

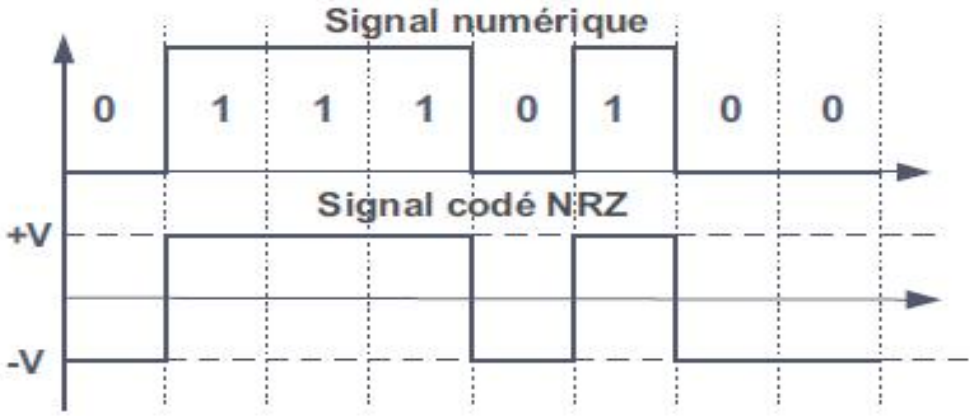


Figure 35: le signal NRZ

Ce codage ne permet pas la création de transition lors de longues séquences de 0 ou de 1 d'où un risque de perte de synchronisation.

Technologie de l'ATM :

Modèle de l'ATM :

La technologie ATM est décrite à l'aide d'un modèle relativement élaboré, qui comprend trois couches horizontal correspondant aux trois premiers niveaux OSI, et trois plans verticaux successifs qui traitent des différents aspect ATM.

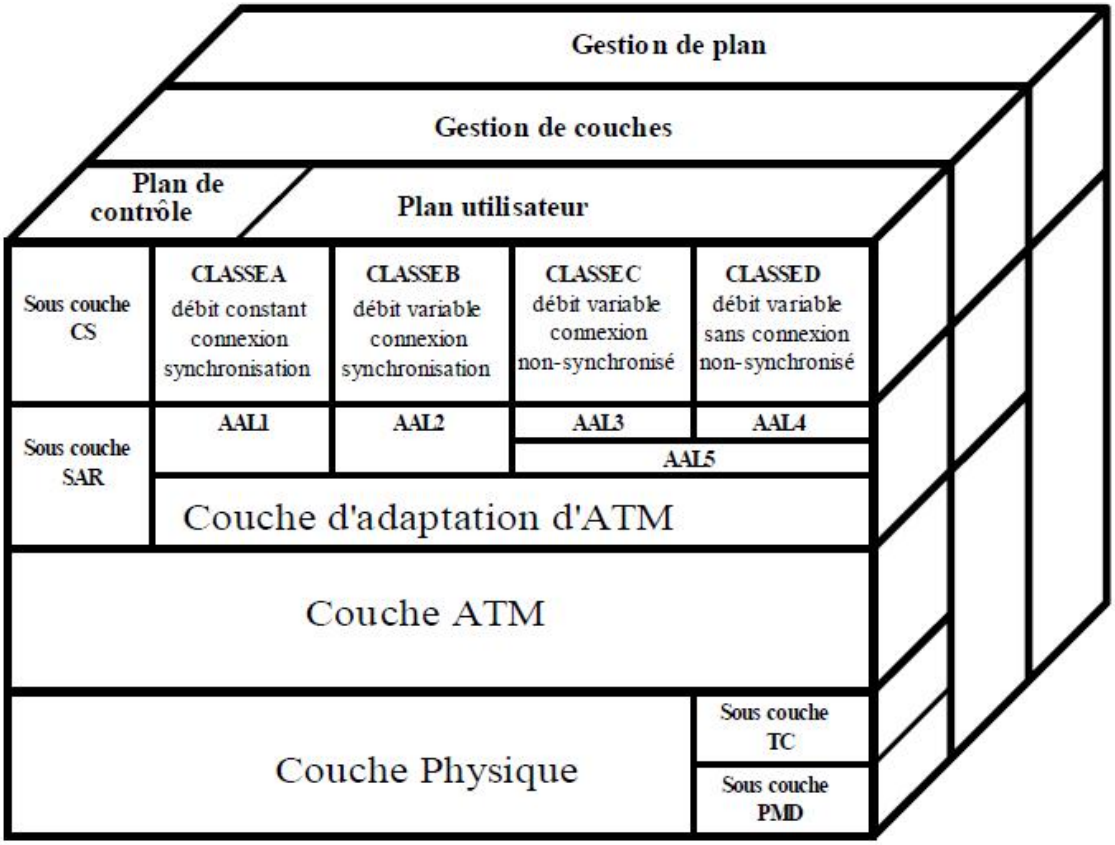


Figure : le modèle d'ATM

Différents plans du modèle :

Le plan utilisateur correspond a la fonction d'acheminement offert par ATM à un Protocol ou applicatifs au niveau supérieur.

Le plan contrôle ou de commande correspond au mécanisme interne à ATM. Tel que la signalisation nécessaire à l'établissement, au maintien, et à la libération de la connexion.

Les plans gestion permettent la gestion des performances, qui permet au plan utilisateur d'offrir les différents services requis. Il utilise des cellules spécifiques.

Différentes couches :

La couche physique est chargée à la couche ATM un service de transport des cellules, elle est décomposée en deux sous couches :

- La sous-couche TC (Transmission convergence) : assure l'adaptation des débits, le contrôle des données, et la délimitation des cellules.

- La sous-couche PM (physical medium) : fournis l'accès au support physique et gère les mécanismes de synchronisation.

La couche ATM assure les fonctions de multiplexage et de démultiplexage des cellules, la génération est l'extraction des en-têtes, l'acheminement (la commutation) des cellules.

La couche AAL garantit aux applications utilisateurs la qualité de service requise par l'application. Cinq type d'AAL ont été définit, ils sont devisé en deux sous-couche :

- La sous-couche SAR (Segmentation And Reasembly sublayer) : elle segmente et rassemble les cellules pour les couches supérieures.
- La sous-couche CS (Convergence Sublayer) : elle assure la synchronisation des horloges entre l'application et le système de transmission.

Composants constituant ATM :

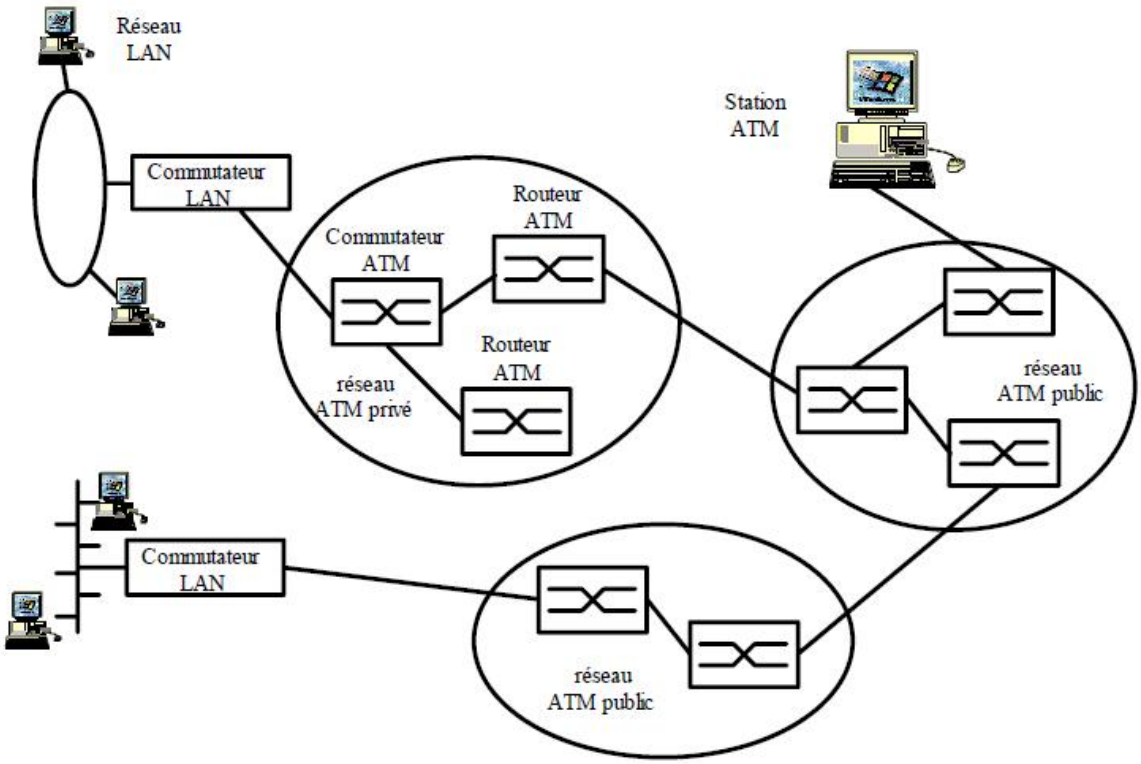


Figure : les composants constituants ATM

Carte d'interface de réseau ATM :

Une carte d'interface de réseau ATM relie une station LAN à un commutateur ATM. L'interface ATM converti les données générer par la station en cellules qui sont transmises à

un commutateur ATM LAN et convertit les cellules reçues de ce commutateur en un format de données manipulable par la station.

Commutateur LAN :

Un commutateur LAN assure l'interconnexion entre les réseaux locaux classiques tels qu'Ethernet ou Token-Ring et le réseau ATM. Il supporte au moins deux types d'interfaces, une interface ATM et une interface LAN.

Le commutateur LAN fonction à la fois comme un commutateur et comme un convertisseur de protocole.

Commutateur ATM :

Un commutateur ATM est un commutateur multiport où chaque port est connecté à un équipement ATM. Il constitue l'infrastructure de base d'un réseau ATM.

L'interconnexion des commutateurs ATM permet de constituer le réseau ATM. Il permet de router les cellules d'un port d'entrer vers un port de sortie.

Contrôle de congestion :

Le contrôle de congestion est l'ensemble des opérations qu'il faut effectuer pour éviter que les ressources des commutateurs soient saturées. L'efficacité de la fonction de routage est, à ce titre, fondamentale car elle doit répartir le trafic entre les commutateurs.

On peut mentionner plusieurs méthodes : perte délibérer de paquets, limitation du nombre de connexions et le contrôle isorythmique. Perdre des paquets est une méthode radicale qui vide la mémoire d'un commutateur, celui-ci récupère des ressources pour la suite En général, on compte sur le fait que tous les paquets jetés et qui vont être retransmis par les utilisateurs ne le seront pas tous en même temps .La limitation du nombre des connexions consiste à refuser de nouvelles connexions si le niveau de disponibilité des ressources dépasse un certains seuil. Le contrôle isorythmique peut se substituer au contrôle du nombre des connexions ou s'y ajouter : il consiste à maitriser le nombre de paquets entrants dans le réseau : chaque commutateur d'accès dispose d'un certain nombre de crédit, tout paquet entrant consomme un crédit et tout paquet sortant du réseau libère un crédit. Lorsque le commutateur n'a plus de crédit, il bloque les paquets à l'entrée. La description présidente n'et pas exhaustive car il existe de nombreuses méthodes de contrôle de congestion, qui peuvent être combinées. [11]

Administration des réseaux :

Administrer un réseau revient à gérer au mieux sa mise en œuvre opérationnelle. Or, les architectures actuelles ne sont pas homogènes car il n'existe pas de système permettant de répondre à l'ensemble des besoins d'un utilisateur.

De plus, la gestion du réseau ne se limite pas à la bonne gestion du service de transport de l'information. Elle implique également la gestion correcte de son traitement. L'utilisateur a donc besoin d'une gestion puissante, qui tienne compte de l'hétérogénéité de l'architecture du réseau et lui fournisse un véritable « système d'exploitation réseau » prenant en charge les aspects distribués du système.

Glossaire :

A :

AAL: ATM adaptation layer

ATM: Asynchrone Transfert Mode

B :

B : bande passante

C :

CLNS: Connection Less Network Service

CONS: Connection Oriented Network Service

CPU: Central Processing Unit

CSMA/CD: carrier sense Multiple access/collision detection (accès multiple avec écoute de la porteuse)

CSRI: Centre des Systèmes et Réseaux D'informations

E :

ETCD : équipement terminal de traitement de données

ETTD: équipement terminal de traitement de données

F :

FDDI : Fiber Distributed Data interface

FTP : File Transfer Protocol

G :

Gbps: Gigabits

H:

HDB3: high-density bipolar 3

I:

ITU: International Telecommunication Union

L:

LAN: local area network

M:

MAN: Metropolitan area network

Mbps: Megabits

MLT3: Multi Level Transmit 3

MSUA : Multistation acces unit

O:

OS : Operating system= SE = système d'exploitation

P:

PAN : Personal area network

S:

STP : Sheilded Twisted Pair

T:

TCP: Transmission Control Protocol

TPDDI: Twisted Pair Distributed Data Interface

U:

UDP: User Datagram Protocol

UTP : Unshielded Twisted Pair

W:

W : largueur de la bande passante

WAN: Wide area network

Résumé

Durant ce travail, nous nous sommes intéressés à la mesure de la bande passante disponible dans un chemin entre deux extrémités. En utilisant l'outil de mesure et d'analyse de flux (trafic) Iperf pour objectif d'avoir les différentes valeurs de la bande passante.

Tout d'abord, il faut savoir que l'outil qu'on a utilisé dans ce travail est gratuit, et par fois open source. Il devrait être relativement aisé de produire une solution plus poussée avec des logiciels payants, disposant d'outils plus avancés et de plus de fonctionnalités. L'idée générale de ce travail est surtout de voir l'approche à adopter pour la mesure et l'analyse de flux d'information.

Dans notre projet, nous avons effectué des différents tests entre le centre des systèmes et réseaux d'informations et les différents départements, et nous avons obtenu des résultats qui sont exposé dans le quatrième chapitre.

Dans le Protocol UDP la gigue et la latence joue un rôle très important lors d'une transmission. La latence nous permet de nous informer sur les délais d'aller retour d'une information transmise sur le réseau. Pour ce qui concerne la gigue c'est la variation de la latence. Donc notre étude consistera à étudier ces deux phénomènes et de les analysé.

Mots clés : transmission, flux d'information, réseau, bande passante, commutation.