République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de L'**E**nseignement **S**upérieur et de la A **R**echerche **S**cientifique
UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DE **G**ENIE **E**LECTRIQUE ET D' **I**NFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etude
de MASTER ACADEMIQUE

Spécialité : **Réseaux et Télécommunications**

Filière : **Electronique**

Présenté par
BEN AISSA Tarik
RAAB Ali

Thème

Mesure de la qualité d'une liaison physique point à point dans un réseau informatique

Mémoire soutenu publiquement le 24 septembre 2017 devant le jury composé de :

Président :	**Mr Lazri Mourad**	**MCA,**	**UMMTO**
Encadreur :	**Mr Ouallouche Fethi**	**MCB,**	**UMMTO**
Examinateur :	**Mr Hameg Slimane**	**MAA,**	**UMMTO**

REMERCIMENTS

Avant tout je tiens à présenter mes remerciements à dieu tout puissant, de m'avoir donner la force et le courage.

Je saisis cette occasion pour adresser mes remerciements les plus profonds à :
Mes parents, mon promoteur Mr. OUALLOUCHE Fethi, les ingénieurs travaillaient au centre de réseaux Hassnaoua, pour leurs conseils et leurs encouragements, et qui ont fourni des efforts énormes dans ce sens.

Mes plus chaleureux remerciements pour tous ceux qui de prés et de loin ont contribué à la réalisation de ce projet.

RAAB Ali

Remerciements

Avant tout, je remercie DIEU, le tout puissant, pour la force, la volonté, la santé et la patience qu'il ma donné pour accomplir ce travail.

Je profite de cette opportunité pour adresser mes plus vifs et profonds remerciements à mes très chers parents, à mon promoteur Mr. OUALLOUCHE Fethi pour nous avoir honoré en acceptant de diriger nôtre mémoire et pour son encadrement de qualité tout au long de ce travail, ainsi qu'à l'équipe d'ingénieurs travaillant au centre réseau Hasnaoua pour leurs conseils et leurs encouragements, et qui n'ont ménagé aucun efforts pour nous aider, notamment dans la partie pratique du présent travail

Et enfin, je tiens à remercier toutes personnes ayant participées de prée ou de loin à ce projet.

BEN AISSA Tarik

DEDICACES

Je rends grâce à Dieu de m'avoir donner le courage et la volonté. Ainsi que la conscience d'avoir pu terminer mes études.

Je dédie ce modeste travail :
A mes très chères : A celui qui m'a toujours appris comment réfléchir avant d'agir, à Celui qui m'a soutenu tout au long de ma vie scolaire, à Celui qui n'a jamais épargner un effort pour mon bien, Mon cher père .A celle qui est toujours à coté de mon cœur, à celle qui n'a hésité aucun moment à m'encouragé, Ma Chère mère.

A mes frères et sœur , et les petits malak ,wissam, amine ,asma pour leurs soutiens morale . A toute ma famille grande et petite.

A touts mes amis les plus sincères qui m'ont beaucoup aider a réaliser ce travaille

A tous les enseignants et étudiants de la faculté génie électrique et informatique, à tout mes collègues, et bien sure a toute la famille "RAAB " et à tous ceux que me connaîssent.

RAAB Ali

Dédicaces

Avant tout, je remercie DIEU, le tout puissant, pour la force, la volonté, la santé et la patience qu'il ma donné pour accomplir ce mémoire.

C'est avec profonde gratitude, sincères mot, amour et fierté, que je dédie cet humble et modeste travail de fin d'études à mes chers parents, source de tendresse, d'inspiration, de noblesse et d'affection, et qui ont sacrifié leur vie pour ma réussite et m'ont éclairé le chemin par leurs conseils judicieux.

J'espère qu'un jour, je pourrais leurs rendre un peu de ce qu'ils ont fait pour moi, que dieu leurs prête bonheur et longue vie.

Je dédie aussi ce travail à mon petit frère et ma petite sœur, ma famille et mes amis.

Je le dédie aussi à tous mes enseignants du département électronique.

BEN AISSA Tarik

SOMMAIRE

Sommaire

Introduction générale.....1

Chapitre I : Généralités sur les réseaux informatiques

I.1- Introduction 3

I.2- Définition.....3

I.3- Les types de réseaux informatiques 4

I.3.1- Les réseaux PAN.....4

I.3.2- Les réseaux LAN (Local Area Network).....5

I.3.2.1- Les architectures des réseaux LAN 6

I.3.2.1.1- L'architecture poste à poste 6

I.3.2.1.2- L'architecture client/serveur 7

I.3.2.2- Les réseaux VLANs (Réseaux locaux virtuels) 7

I.3.2.3- Les topologies des réseaux LAN 9

I.3.2.3.1- La topologie physique 9

I.3.2.3.2- La topologie logique 11

I.3.2.4- Les constituants matériels d'un réseau LAN 12

I.3.2.4.1- La carte réseau (parfois appelé coupleur).....12

I.3.2.4.2- Les supports physiques d'interconnexion 14

I.3.2.4.2.1- Le câble coaxial 14

I.3.2.4.2.2- La paire torsadée 16

I.3.2.4.2.2- La fibre optique 19

I.3.3- Les réseaux MAN (Metropolitan Area Network) 25

I.3.4- Les réseaux WAN (Wide Area Network) 26

I.4- Conclusion 26

Chapitre II: La transmission des données

II.1- Introduction 27

II.2- Les architectures de réseaux 27

II.2.1- Le modèle de référence OSI 27

II.2.1.1- Les couches du modèle de référence 28

II.2.1.1.1- La couche 1 Physique (niveau physique).....28

II.2.1.1.2- La couche 2 liaison (niveau trame).....28

II.2.1.1.3- La couche 3 réseaux (niveau paquet).....28

II.2.1.1.4- La couche 4 transports (niveau message).....28

II.2.1.1.5- La couche 5 sessions (niveau session).....29

II.2.1.1.6- La couche 6 présentations (niveau présentation).....29

. II.2.1.1.7- La couche 7 applications (niveau application) 29

II.2.2- Le modèle TCP/IP.....29

II.2.2.1- Encapsulation des données 30

II.2.2.2- Protocole (c'est quoi un protocole).....30

SOMMAIRE

II.2.2.3- Protocoles orientés et non orientés connexion.....31
II.2.2.4- La couche Accès réseau.....31
II.2.2.5- La couche Internet 32
II.2.2.5.1- Le protocole IP 32
II.2.2.5.2- Le protocole ARP 33
II.2.2.5.3- Le protocole ICMP 33
II.2.2.5.4- Le protocole RARP 34
II.2.2.5.5- Le protocole IGMP 34
II.2.2.6- La couche transport 35
II.2.2.6.1- Port 35
II.2.2.6.2- Le protocole TCP 36
II.2.2.6.3- Le protocole UDP 37
II.2.2.7- La couche application 37
II.3- Les équipements d'interconnexion réseaux 38
II.3.1- Les répéteurs 38
II.3.2- Les concentrateurs (Hub) 38
II.3.3- Les ponts (bridge) 39
II.3.4- Les commutateurs (switch) 40
II.3.5- Les passerelles (gateway) 41
II.3.6- Les routeurs 42
II.4- Les modes de transmission 43
II.4.1- Liaison simplex 44
II.4.2- Liaison half-duplex 44
II.4.3- Liaison full-duplex 44
II.4.4- Transmission série et parallèle 44
II.4.4.1- Liaison parallèle 45
II.4.4.2- Liaison série 45
II.4.5- Transmission synchrone et asynchrone 46
II.4.5.1- Liaison asynchrone 46
II.4.5.2- Liaison synchrone 46
II.5- Les techniques de commutation 47
II.5.1- Commutation de circuits 47
II.5.2- Commutation de messages 48
II.5.3- Commutation par paquets 49
II.6- Les réseaux IP 50
II.6.1- L'adressage IP 50
II.6.1.1- Les adresses IPv4 51
II.6.1.2- Le masque réseau 51
II.6.1.3-Adresses particulières 52
II.6.1.4-Notation CIDR 53
II.6.1.5- Délivrance des adresses 53

SOMMAIRE

II.6.1.6-Les classes d'adresses 53
II.7- Quelques protocoles utilisées sur internet 54
II.7.1-le protocole NAT (Network Address Translation) 54
II.7.2-Le DHCP (Dynamic Host Configuration Protocol) 55
II.7.3-Le DNS (Domain Name System) 55
II.8- Conclusion 56

Chapitre III : Application

III.1- Introduction 57
III.2- Le logiciel IPerf3 57
III.2.1- Principe de fonctionnement 58
III.2.2- Interface graphique jperf 58
III.2.3- Téléchargement et Installation sous Windows ... .63
III.3- Matériel utilisé 66
III.4- Méthode de travail et but des tests 66
III.4.1- Méthode de travail 66
III.4.2- Buts des tests 66
III-5- Tests 66
III.5.1- Test 1 66
III.5.2- Test 2 68
III.5.3- Test 3 69
III.6- Conclusion 71
Conclusion générale et perspectives..... 72
Bibliographie

Introduction Générale

Introduction générale

Un ensemble de terminaux informatiques reliés entre eux afin d'échanger des donnés, communiquer, partager des ressources et des applications (messagerie électronique, les agendas de groupe,…etc.) forment un réseau informatique.[1]

Dans un réseau filaire, ses échanges et partages s'effectuent avec des débits plus au moins optimaux et des pertes de transmission plus au moins importantes selon plusieurs critères, parmi lesquels figure la qualité des liaisons physiques reliant ses différents équipements.[2]

Vu l'importance de cette qualité et son impact sur le réseau, différents moyens matériels et logiciels ont été mis au point afin de la mesurer.

Matériels allant du testeur de câbles le plus rudimentaire servant juste à tester la continuité d'une liaison jusqu'aux testeurs les plus sophistiqués permettant une mesure en temps réel de cette dernière, en prenant en compte plusieurs paramètres, tel que : la continuité, le débit, les pertes de transmission,… etc.

Cependant cette solution, est relativement onéreuse, ce qui a motivé le présent travail, qui est de proposer une solution logiciel et qui ne coûte pratiquement pas chère dans le but d'effectuer cette mesure, celle-ci étant l'utilisation du logiciel **iperf-3.1.3,** qui est un outil open-source permettant la mesure des performances d'un réseau informatique.

Pour cela, notre présent travail est diviser en trois chapitres, dans le premier nous avons donné des définitions et généralités sur les réseaux informatiques, les différentes classifications selon leurs étendues géographiques y seront abordées, notamment les réseaux LAN, leurs architectures (client/serveur et poste à poste), leurs topologies et leurs constituants matériels ainsi que la notion de VLANs (Réseaux locaux virtuels).

Dans le second chapitre, nous avons donné une présentation de la transmission dans un réseau, une description précise du **modèle de référence OSI**, une définition des concepts généraux du modèle TCP/IP et des protocoles

qui y sont utilisés, des équipements d'interconnexion utilisés pour relier des réseaux locaux et on terminera par une présentation des caractéristiques et des techniques de commutation et les modes de transmissions de données.

Dans le troisième chapitre et le dernier, premièrement on donner une présentation du logiciel IPerf, son principe de fonctionnement, de l'interface graphique jPerf ainsi que ses différentes fonctionnalités. En suite, nous donnons les étapes à suivre, afin de les installer sous Windows. Puis nous citons le matériel utilisé, nous donnons la méthode de travail ainsi que le but des tests à effectuer.

Nous terminons par donner les résultats obtenues testons en trois liaisons physiques (tronçons de câbles réseaux au sein de l'UMMTO), avec le logiciel IPerf et son interface graphique JPerf.

Et enfin à la lumière des résultats ainsi obtenus, on conclut par donner une appréciation de la qualité de chaque liaison testée.

Chapitre I : Généralités sur les réseaux informatiques

I-1-Introduction :

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que des stations de travail ou des serveurs.

Etant devenus incontournables aujourd'hui, ils sont employés dans toutes les entreprises et même chez les particuliers, permettant ainsi la mise en œuvre d'applications très diverses, des plus simples aux plus sophistiquées. La plus connue est le partage d'informations grâce à Internet.

Dans ce chapitre, nous allons poser le fondement en ce qui concerne les réseaux informatiques, les différentes classifications selon l'étendue géographique y seront abordé, notamment les réseaux LAN, leurs architectures (client/serveur et poste à poste), leurs topologies et leurs constituants matériels ainsi que la notion de VLANs (Réseaux locaux virtuels).

I-2-Définition :

Un réseau est tout ensemble d'entités (objets ou personnes), reliées entre elles.

Selon le type de ces entités, on peut distinguer :

- ✓ réseau de transport
- ✓ réseau téléphonique
- ✓ réseaux de neurones
- ✓ réseaux de personnes
- ✓ réseaux informatique

  .
  .
  .
- ✓ etc

Le réseau informatique est un ensemble d'équipements informatiques reliés entre eux, pour s'échanger des donnés, de communiquer, de partager des ressources et des applications (messagerie électronique, les agendas de groupe,…etc.).

- ✓ Si les liens sont assurés par des câbles, on parle de réseau câblé ou filaire.

- ✓ Si les liens sont sous forme d'ondes radios, on parle de réseau sans fil.

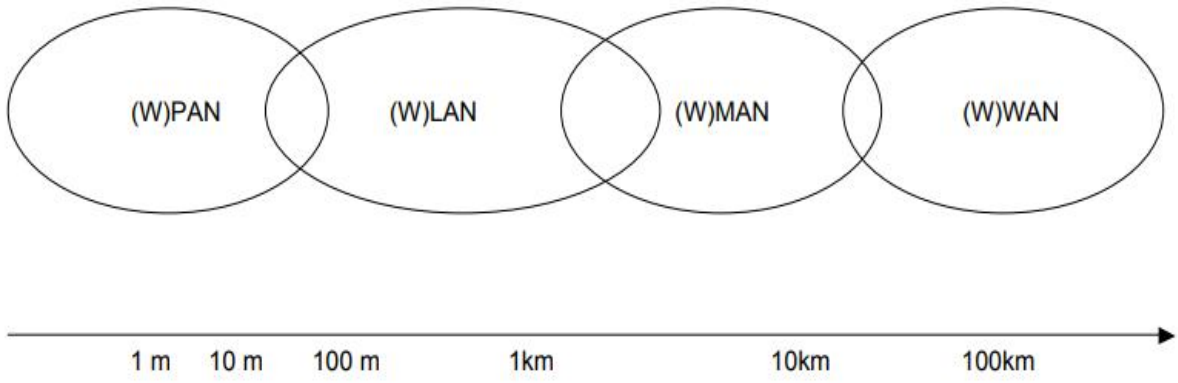
I-3-Les types de réseaux informatiques

On peut différencier les types de réseaux informatiques selon plusieurs critères, tel que :

- Leurs tailles en termes de nombre de machines ;
- Leurs vitesses de transfert des données ;
- Leurs étendues.

On distingue généralement les catégories de réseaux suivantes :

- **Réseaux personnels ou PAN** (*Personal Area Network*).
- **Réseaux locaux ou LAN** (*Local Area Network*).
- **Réseaux métropolitains ou MAN** (*Metropolitan Area Network*).
- **Réseaux étendus ou WAN** (*Wide Area Network*).



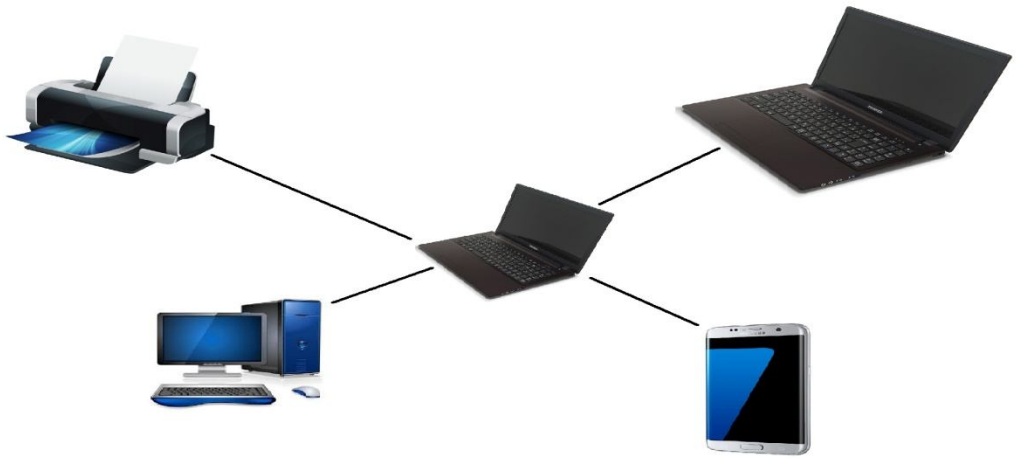
FigI.1-Types réseaux informatiques

I-3-1-Les réseaux PAN (*Personal Area Network)* :

Ce sont des réseaux qui interconnectent sur quelques mètres des équipements personnels d'un même utilisateur, tel que :

- Ordinateur personnel(PC) ;
- Téléphone portable ;
- Imprimantes ;
- Scanner ;

- ...etc.

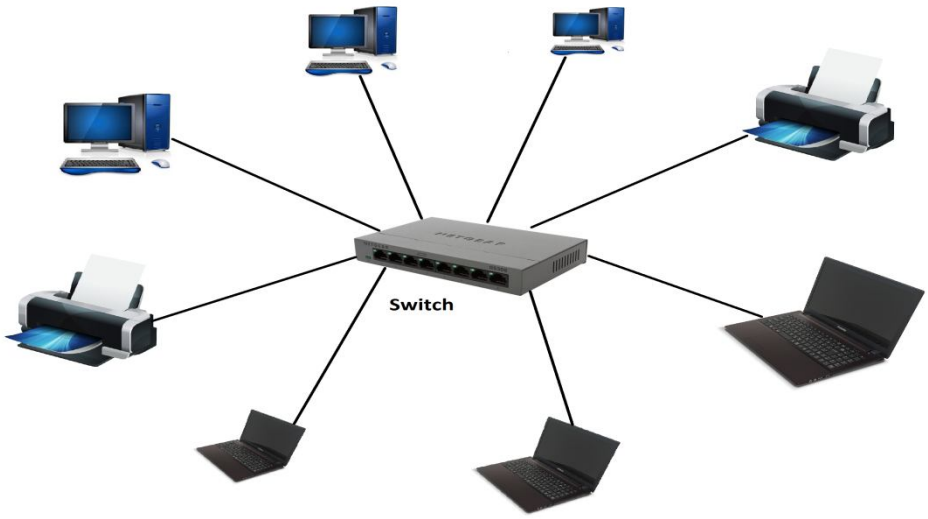


FigI.2-Réseau PAN

I-3-2-Les réseaux LAN (*Local Area Network)* :

Un réseau local (LAN) désigne un ensemble d'ordinateurs reliés entre eux, appartenant à une même organisation et contenus dans une petite surface géographique, utilisant souvent une même technologie (Ethernet ou WIFI).

Ce type de réseau possède une vitesse de transfert de données qui varie entre 10 Mb/s (pour un réseau Ethernet standard) à 1 Gb/s (pour un réseau Gigabit Ethernet). Sa taille peut atteindre jusqu'à 100 voire 1000 machines.



FigI.3-Réseau LAN

I-3-2-1-Les architectures des réseaux LAN :

On distingue généralement deux types d'architectures :

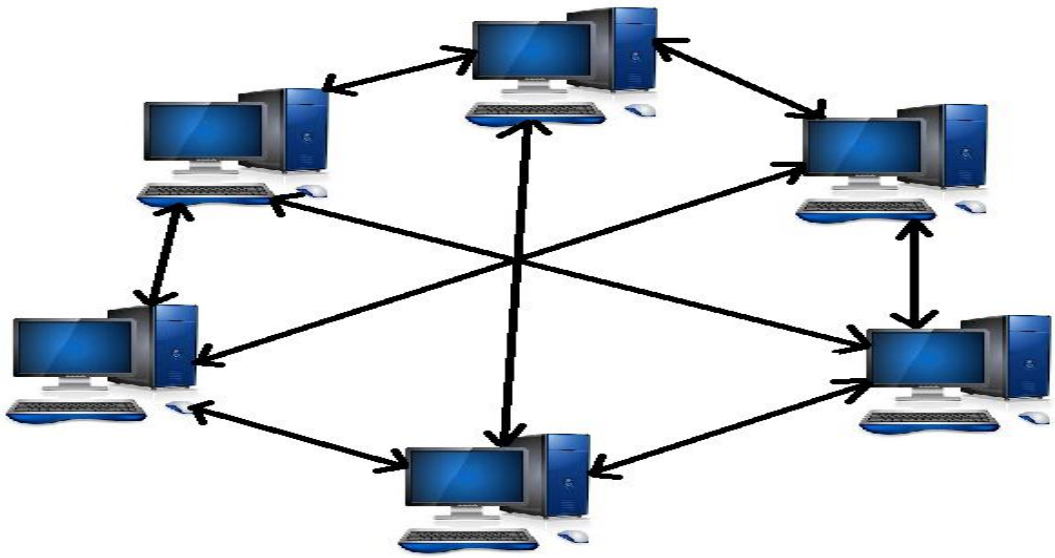
- ✓ Architecture poste à poste (peer to peer ou égal à égal)
- ✓ Architecture client/serveur

I-3-2-1-1- L'architecture poste à poste :

Chaque poste connecté est à la fois client et serveur et peut mettre ses ressources à disposition du réseau (et bénéficie également des ressources des autres postes).

- ❖ Cette solution n'est pas simple à mettre en œuvre au sein de grandes structures.
  - *<u>Exemple</u> : Si on a 4 postes et 10 utilisateurs, chaque poste doit contenir les 10 mots de passe afin que les utilisateurs puissent travailler sur n'importe lequel des postes. Mais si maintenant il y a 60 postes et 300 utilisateurs, la gestion des mots dépasse devient périlleuse et assez compliqué !*

- Les profils des utilisateurs sont généralement stockés sur un seul poste. Donc les utilisateurs ne peuvent pas changer aisément de machine.
- La définition de ressources multiples disséminées sur des postes de travail divers et éloignés pose des problèmes d'organisation (versions multiples de fichier) et d'administration de ces ressources.



FigI.4-Architecture poste à poste

I-3-2-1-2- L'architecture client/serveur:

Dans cette architecture, un ordinateur est dédié au rôle de serveur, machine généralement très puissante, des machines clientes (des PC sur le réseau) le contactent afin qu'il leurs fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, l'accès à une base de données, …etc.

Remarque : Plusieurs machines peuvent être dédiées au rôle de serveur.

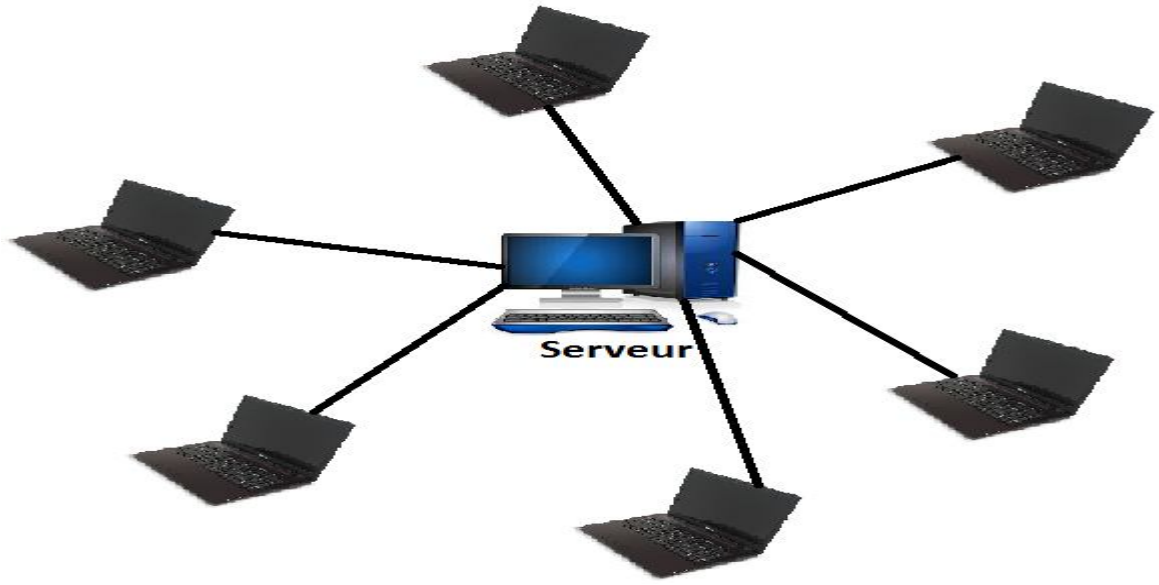
Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client FTP, client

de messagerie, … lorsqu'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client de messagerie il s'agit de courrier électronique).

Ce modèle d'architecture est surtout recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- Des ressources centralisées, communes à tous les utilisateurs (évite la redondance et la contradiction) ;
- Une meilleure sécurité ;
- Une administration serveur en lieu et place d'une administration de n clients ;
- Facilité d'ajout et de suppression des clients.

Cependant une telle architecture est assez onéreuse, ce qui est du à la technicité du serveur, ce dernier étant aussi le maillon faible de celle-ci.



FigI.5-Architecture client/serveur

I-3-2-2-Les réseaux VLANs *(Réseaux locaux virtuels)* :

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).[1]

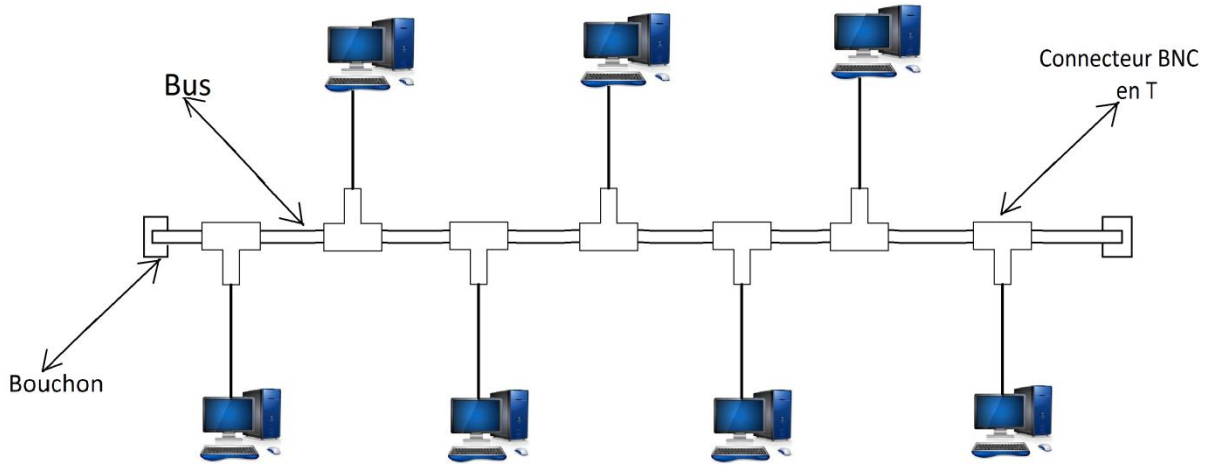
I-3-2-3-Les topologies des réseaux LAN:

I-3-2-3-1-La topologie physique:

L'arrangement physique, c'est-a-dire la configuration spatiale du réseau est appelée topologie physique [1], autrement dit c'est la façon dont les composants physiques sont connectés dans ce dernier, on distingue géneralement les topologies suivantes :

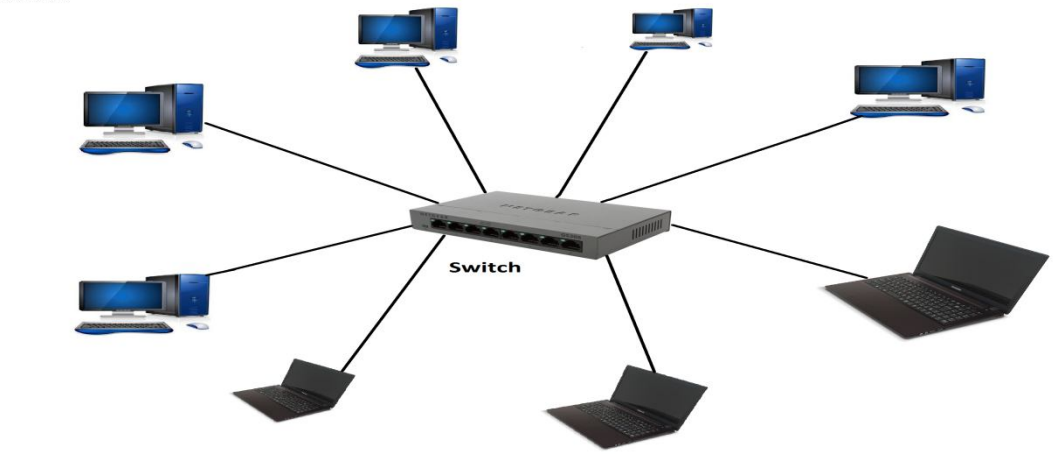
- ✓ La toplologie en bus ;
- ✓ La toplologie en étoile ;
- ✓ La toplologie en anneaux ;

- ❖ **La topologie en bus:** Tous les ordinateurs sont reliés via un connecteur en T à une même ligne de transmission centrale, désignée par le mot bus, qui est un câble coaxial terminé par des bouchons en ses deux extrémités.



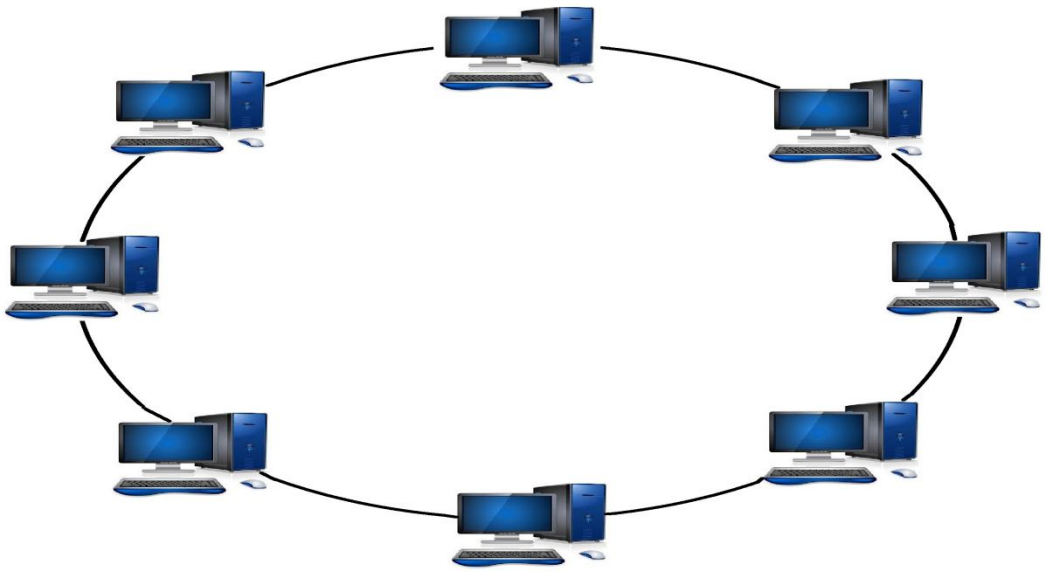
FigI.6-Topologie en bus

- **La topologie en étoile:** Dans une topologie en étoile, les ordinateurs du réseau sont tous reliés à un point central qui est un système matériel : switch ou routeur, on utilisant géneralement un câblage en cuivre paire torsadé (RJ45). La communication entre deux machines ne peut se faire que par un seul chemin possible.



FigI.7-Topologie en étoile

- **La topologie en anneau:** Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour(le principe du jeton), on a donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va "avoir la parole" successivement. Un message envoyé par une machine passe par toutes les autres .



FigI.8-Topologie en anneau

I-3-2-3-2-La topologie logique:

La topologie logique, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet et Token Ring [1].

❖ La topologie Ethernet :

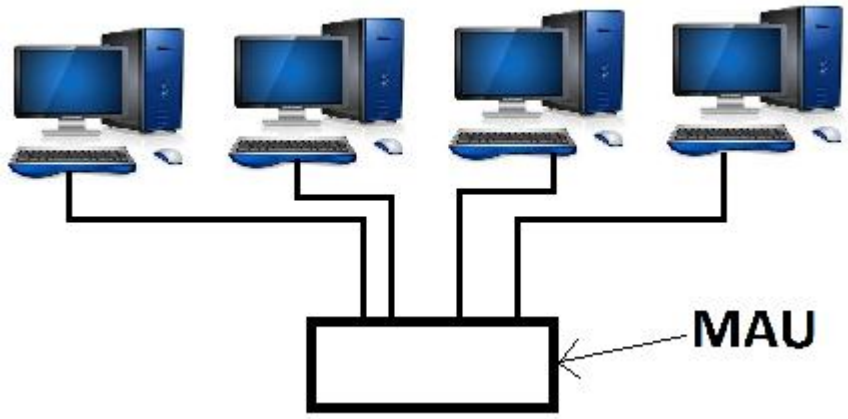
Dans la topologie Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detect), qui permet la surveillance des données à transmettre pour éviter toute sorte de collision. Elle consiste pour une station, au moment où elle émet, à écouter si une autre station n'est pas aussi en train d'émettre. Si c'est le cas, la station cesse d'émettre et réémet son message au bout d'un

délai fixe. Cette méthode est aléatoire, en ce sens on ne peut prévoir le temps nécessaire à un message pour être émis, transmis et reçu.

❖ La topologie Token Ring :

Dans cette topologie, une structure permet de faire tourner un jeton unique en anneau, donnant le droit d'émettre à au plus une station. Une station pour émettre, doit attendre de capturer le jeton et le remplace par sa (ses) trame(s) de données. La trame de données qui est munie de l'adresse d'émission et celle de destination, lors de sa rotation est copiée par le(s) récepteur(s), lorsque la rotation est complète elle revient à l'émetteur, qui est ensuite détruite et remplacée par le jeton, qui est à nouveau relâché et permettra à d'autres stations d'émettre.

En réalité dans cette topologie, les ordinateurs ne sont pas disposés en boucle, mais sont reliés à un répartiteur (appelé MAU, *Multistation Access Unit*) qui va donner successivement "la parole" à chacun d'entre-eux.



FigI.9-Topologie Token Ring

I-3-2-4-Les constituants matériels d'un réseau LAN:

Un réseau local est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels. Les éléments matériels permettant d'interconnecter les ordinateurs sont les suivants :

I-3-2-4-1-*La carte réseau (parfois appelé coupleur):*

La carte réseau (appelée Network Interface Card en anglais et notée NIC) constitue l'interface entre l'ordinateur et le câble du réseau. La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau.

La carte réseau possède généralement deux témoins lumineux (LEDs) :

- La LED verte correspond à l'alimentation de la carte ;
- La LED orange (10 Mb/s) ou rouge (100 Mb/s) indique une activité du réseau (envoi ou réception de données).

Ainsi une carte réseau prépare pour le câble réseau les données émises par l'ordinateur, les transfère vers un autre ordinateur et contrôle le flux de données entre l'ordinateur et le câble. Elle traduit aussi les données venant du câble et les traduit en octets afin que l'Unité Centrale de l'ordinateur les comprenne.

La plupart des cartes réseau destinées au grand public sont des cartes Ethernet. Elles utilisent comme support de communication des paires torsadées (8 fils en cuivre), disposant à chaque extrémité de prises RJ45.

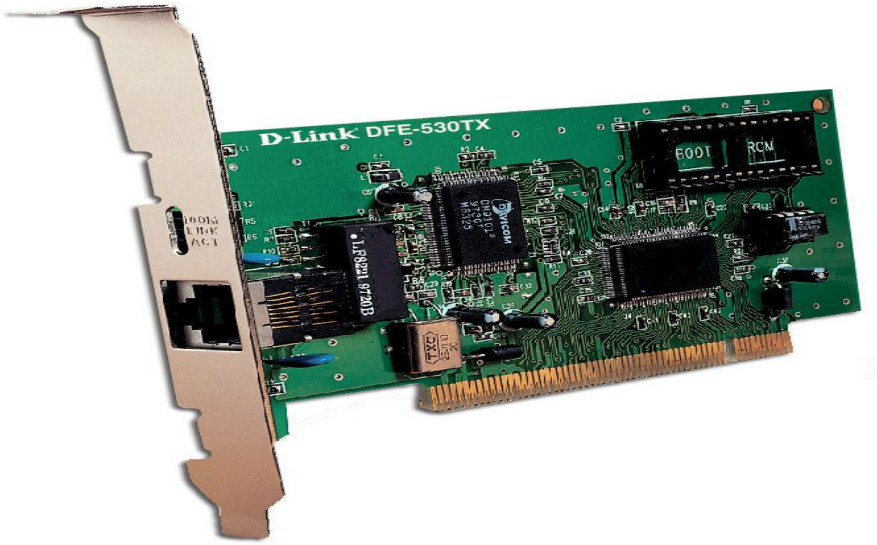
Les trois standards Ethernet (norme 802.3) les plus courants correspondent aux trois débits les plus fréquemment rencontrés :

- Le 10Base-T permet un débit maximal de 10 Mbit/s. Le câble RJ45 peut alors mesurer jusqu'à une centaine de mètres et seuls 4 des 8 fils sont utilisés.

- Le 100Base-TX permet un débit maximal de 100 Mbit/s. Il est également appelé Fast Ethernet et est désormais supporté par la quasi-totalité des cartes réseau. Comme pour le 10Base-T, le câble RJ45 peut alors mesurer jusqu'à une centaine de mètres et seuls 4 des 8 fils sont utilisés.

- Le 1000Base-T permet un débit maximal de 1 000 Mbit/s. Il est également appelé Gigabit Ethernet et se démocratise rapidement. Pour que le réseau fonctionne correctement, le câble RJ45 peut toujours mesurer jusqu'à 100 m, mais doit être de bonne qualité. Cette fois, les 8 fils sont utilisés.

Remarque : *Pour relier plus de deux machines, on utilise un matériel nommé hub ou switch : une extrémité du câble sera alors branchée sur l'ordinateur alors que l'autre sera relié au switch. Les deux caractéristiques fondamentales d'un switch sont sa vitesse (compatibilité 10Base-T, 100Base-TX et/ou 1000Base-T) et son nombre de ports (nombre de prises RJ45).*



FigI.10-Carte réseau Fast Ethernet D-LINK DFE-530TX – PCI/100Mbps

I-3-2-4-2-*Les supports physiques d'interconnexion:*

I-3-2-4-2-1-Le câble coaxial :

Le câble coaxial (en anglais coaxial câble) a longtemps été le câblage de prédilection, pour la simple raison qu'il est peu coûteux et facilement manipulable (poids, flexibilité, ...).

Un câble coaxial est constitué d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure.

FigI.11-Câble coaxial

- ***La gaine*** permet de protéger le câble de l'environnement extérieur. Elle est habituellement en caoutchouc (parfois en Chlorure de polyvinyle (PVC), éventuellement en téflon).
- ***Le blindage*** (enveloppe métallique) entourant les câbles permet de protéger les données transmises sur le support des parasites (autrement appelés bruit) pouvant causer une distorsion des données.
- ***L'isolant*** entourant la partie centrale est constitué d'un matériau diélectrique permettant d'éviter tout contact avec le blindage, provoquant des interactions électriques (court-circuit).
- ***L'âme***, accomplissant la tâche de transport des données, est généralement composée d'un seul brin en cuivre ou de plusieurs brins torsadés.

Remarque *il existe des câbles coaxiaux possédant un blindage double (une couche isolante, une couche de blindage) ainsi que des câbles coaxiaux à quadruple blindage (deux couches isolantes, deux couches de blindage).*

-On distingue habituellement deux types de câbles coaxiaux :

- ***Le 10Base2 - câble coaxial fin*** (appelé Thinnet : réseau fin ou encore CheaperNet : plus économique) est un câble de diamètre (6 mm), de couleur blanche (ou grisâtre) par convention. Très flexible il peut être utilisé dans la majorité des réseaux, en le connectant directement sur la carte réseau. Il permet de transporter un signal sur une distance d'environ 185 mètres sans affaiblissement.

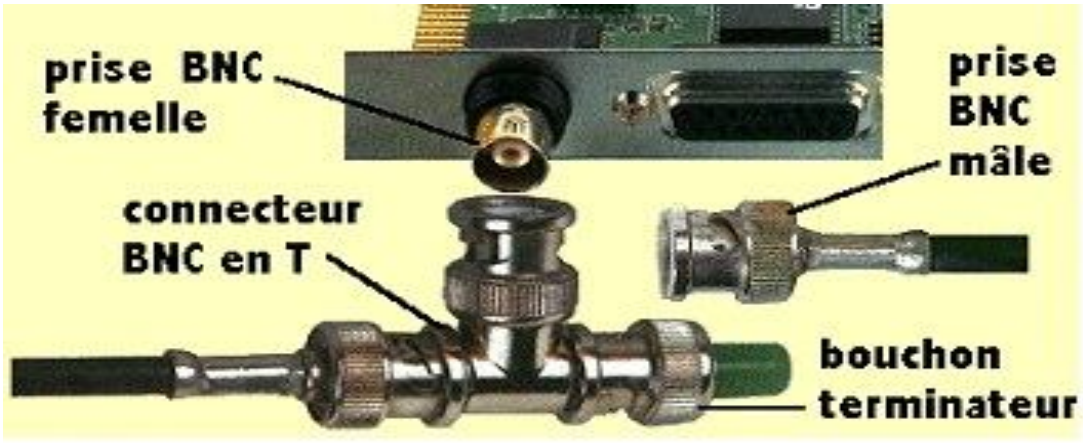
- ***Le 10Base5 - câble coaxial épais*** (en anglais Thicknet ou Thick Ethernet et également appelé Yellow Cable, en raison de sa couleur jaune conventionnelle) est un câble blindé de plus gros diamètre (12 mm) et de 50 ohms d'impédance. Il a longtemps été utilisé dans les réseaux Ethernet, ce qui lui a valu l'appellation de « Câble Ethernet Standard ». Etant donné que son âme a un plus gros diamètre, la distance susceptible d'être parcourue par les signaux est grande, cela lui permet de transmettre sans affaiblissement des signaux sur une distance atteignant 500 mètres (sans réamplification du signal). Sa bande passante est de 10 Mbps Il est donc employé très souvent comme câble principal (backbone) pour relier des petits réseaux dont les ordinateurs sont connectés avec du Thinnet. Toutefois, étant donné son diamètre il est moins flexible que le Thinnet.

- **Les connecteurs pour câble coaxial :**

Thinnet et Thicknet utilisent tous deux des connecteurs BNC (Bayonet-Neill-Concelman ou British Naval Connector) servant à relier les câbles aux ordinateurs.

Dans la famille BNC, on trouve :

- **Connecteur de câble BNC** : il est soudé ou serti à l'extrémité du câble.
- **Connecteur BNC en T** : il relie la carte réseau des ordinateurs au câble du réseau.
- **Prolongateur BNC** : il relie deux segments de câble coaxial afin d'obtenir un câble plus long.
- **Bouchon de terminaison BNC** : il est placé à chaque extrémité du câble d'un réseau en Bus pour absorber les signaux parasites. Il est relié à la masse. Un réseau bus ne peut pas fonctionner sans. Il serait mis hors service.



FigI.12-Connecteurs pour câble coaxial

I-3-2-4-2-2-La paire torsadée :

Dans sa forme la plus simple, le câble à paire torsadée (en anglais Twisted-pair cable) est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants.

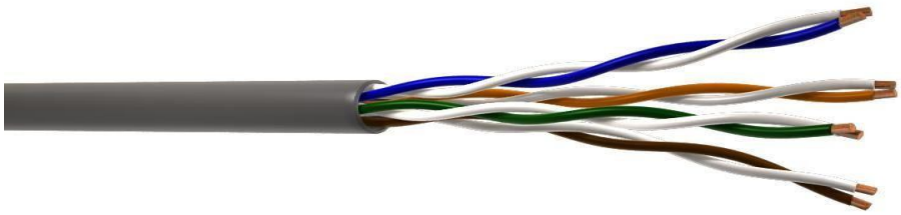
On distingue généralement deux types de paires torsadées :

- **Les paires blindées** (STP : Shielded Twisted-Pair) ;
- **Les paires non blindées** (UTP : Unshielded Twisted-Pair).

Un câble est souvent fabriqué à partir de plusieurs paires torsadées regroupées et placées à l'intérieur de la gaine protectrice. L'entrelacement permet de supprimer les bruits (interférences électriques) dus aux paires adjacentes ou autres sources (moteurs, relais, transformateur).

La paire torsadée est donc adaptée à la mise en réseau local d'un faible parc avec un budget limité, et une connectique simple. Toutefois, sur de longues distances avec des débits élevés elle ne permet pas de garantir l'intégrité des données (c'est-à-dire la transmission sans perte de données).

- **La paire torsadée non blindée (UTP)**



FigI.13-Câble UTP

Le câble UTP obéit à la spécification 10BaseT. C'est le type de paire torsadée le plus utilisé et le plus répandu pour les réseaux locaux. Voici quelques caractéristiques :

- **Longueur maximale d'un segment :** 100 mètres
- **Composition :** 2 fils de cuivre recouverts d'isolant
- **Normes UTP :** conditionnent le nombre de torsions par pied (33 cm) de câble en fonction de l'utilisation prévue
- **UTP :** répertorié dans la norme Commercial Building Wiring Standard 568 de l'EIA/TIA (Electronic Industries Association / Telecommunication Industries Association). La norme EIA/TIA 568 a utilisé UTP pour créer des normes applicables à toutes sortes de locaux et de contextes de câblage qui garantissent au public l'homogénéité des produits. *Ces normes incluent cinq catégories de câbles UTP :*

- ✓ **Catégorie 1 :** Câble téléphonique traditionnel (transfert de voix mais pas de données)
- ✓ **Catégorie 2 :** Transmission des données à 4 Mbit/s maximum (RNIS). Ce type de câble est composé de 4 paires torsadées
- ✓ **Catégorie 3 :** 10 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées et de 3 torsions par pied
- ✓ **Catégorie 4 :** 16 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre
- ✓ **Catégorie 5 :** 100 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre

- ✓ **Catégorie 5e :** 1000 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre

La plupart des installations téléphoniques utilisent un câble UTP. Beaucoup de locaux sont pré-câblés pour ce genre d'installation (souvent en nombre suffisant pour satisfaire les futurs besoins). Si la paire torsadée pré-installée est de bonne qualité, il est possible de transférer des données et donc l'utiliser en réseau informatique. Il faut faire attention cependant aux nombres de torsades et aux autres caractéristiques électriques requises pour une transmissions de données de qualité.

Le majeur problème provient du fait que le câble UTP est particulièrement sujet aux interférences (signaux d'une ligne se mélangeant à ceux d'une autre ligne). La seule solution réside dans le blindage.

- ➢ **La paire torsadée blindée (STP)**

FigI.14-Câble STP

Le câble STP (Shielded Twisted Pair) utilise une gaine de cuivre de meilleure qualité et plus protectrice que la gaine utilisée par le câble UTP. Il contient une enveloppe de protection entre les paires et autour des paires. Dans le câble STP, les fils de cuivre d'une paire sont eux-mêmes torsadés, ce qui fournit au câble STP un excellent blindage, c'est-à-dire une meilleure protection contre les interférences). D'autre part il permet une transmission plus rapide et sur une plus longue distance.

- **Les connecteurs pour paire torsadée**

FigI.15-Connecteur RG-45

La paire torsadée se branche à l'aide d'un connecteur RJ-45(RJ signifiant Registered Jack), aussi appelé 8P8C (8 positions 8 connexions) constitue un des principaux connecteurs de carte réseau pour les réseaux Ethernet utilisant des paires torsadées pour la transmission d'information. Ainsi, il est parfois appelé port Ethernet.

I-3-2-4-2-3-La fibre optique :

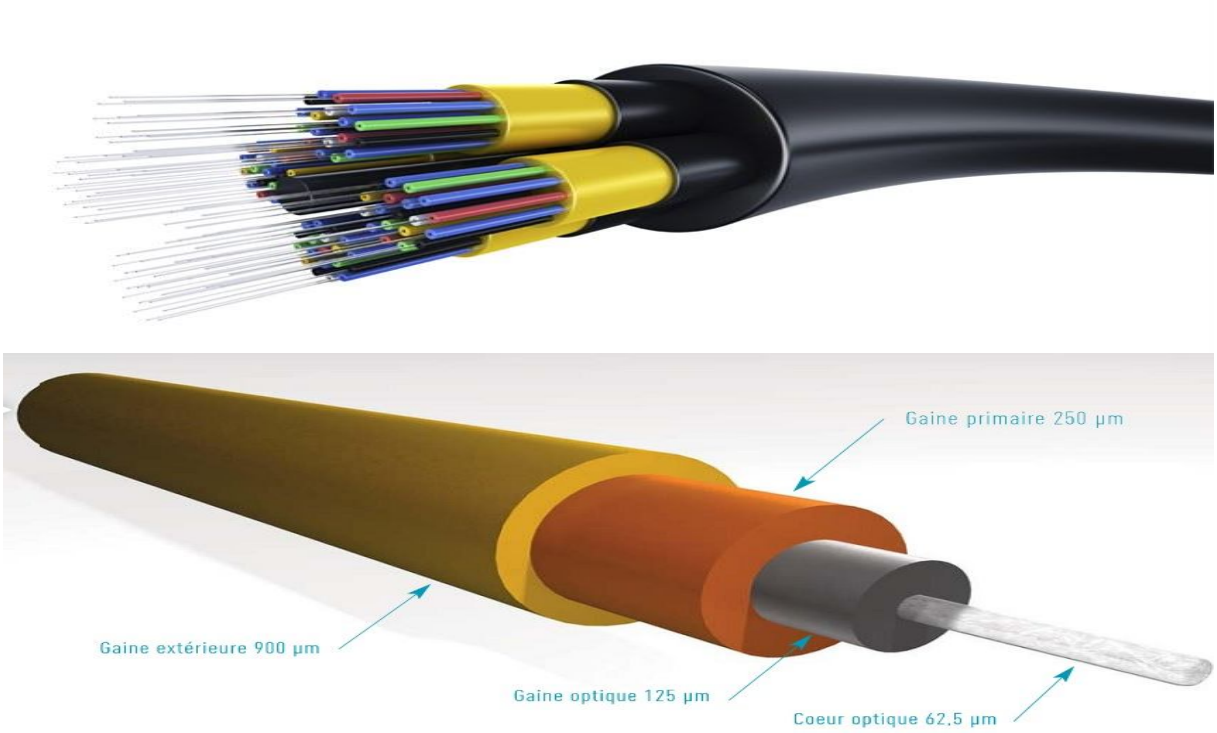
La fibre optique est un conducteur d'ondes lumineuses, constituée d'un fil de verre très fin. Elle comprend un cœur, dans lequel se propage la lumière émise par une diode électroluminescente ou une source laser et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre.

Chaque fibre de verre transmet les signaux dans un seul sens. De ce fait, un câble est constitué de deux fibres. Une pour l'émission et l'autre pour la réception.

Le principe d'isolation totale de la fibre optique permet une réflexion totale des ondes lumineuses entre cœur et gaine.

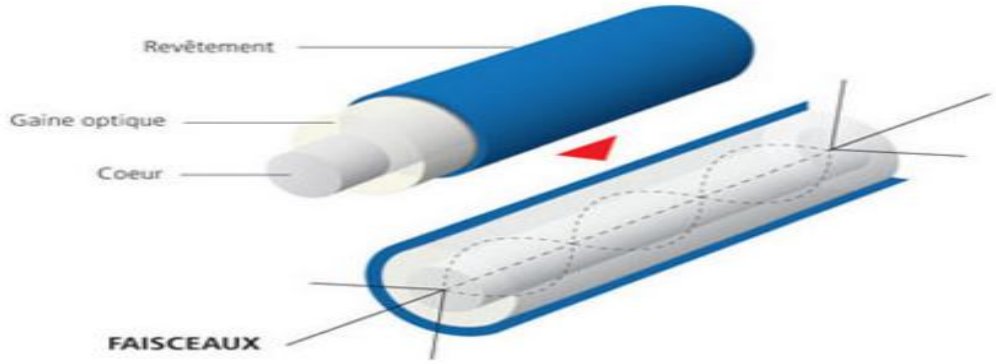
Les avantages de la fibre optique sont nombreux : le diamètre extérieur est de l'ordre de 0,1 mm, son poids est de quelques grammes au kilomètre. Cette réduction de taille et de poids la rend facilement utilisable. En outre, sa très grande capacité permet la transmission simultanée de très nombreux canaux de télévision, de téléphone… Les points de régénération des signaux transmis sont plus éloignés, du fait de l'atténuation plus faible de la lumière. Enfin, l'insensibilité des fibres aux parasites électromagnétiques constitue un avantage très apprécié, puisqu'une fibre optique supporte sans difficulté la proximité d'émetteurs radioélectriques. On peut donc les utiliser dans des environnements très perturbés (avec de puissants champs électromagnétiques, par exemple).

Les fibres optiques peuvent être classées en deux catégories selon le diamètre de leur cœur et la longueur d'onde utilisée : les fibres monomodes et multimodes.



FigI.16-Fibre optique

- **Fibre multimodes :**



FigI.17-Fibre optique multimodes

A saut d'indice :

La fibre multimode à saut d'indice est la fibre la plus ordinaire. C'est ce type de fibre qui est utilisé dans les réseaux locaux de type LAN.

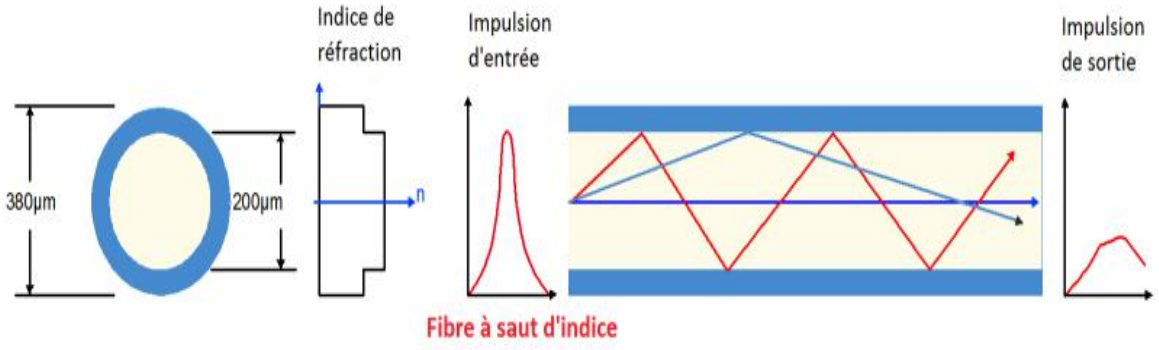
Etant donné que la fibre à saut d'indice est multimode, il existe plusieurs modes de propagation de la lumière au sein de son coeur de silice.

Il existe dans cette fibre une très grande variation entre l'indice de réfraction du coeur et de la gaine optique.

C'est pour cela que les rayons lumineux se propagent par réflexion totale interne en "dent de scie".

La fibre à saut d'indice possède un cœur très large. L'atténuation sur ce type de fibre est très importante comme on peut le voir sur la différence des impulsions d'entrée et de sortie.

- ✓ **Débit:** environ 100 Mbit/s
- ✓ **Portée maximale:** environ 2 Km
- ✓ **Affaiblissement:** 10 dB/Km



FigI.18-Propagation dans la fibre optique à saut d'indice

A gradient d'indice

La fibre multimode à gradient d'indice est elle aussi utilisée dans les réseaux locaux. C'est une fibre multimode, donc plusieurs modes de propagation coexistent. A la différence de la

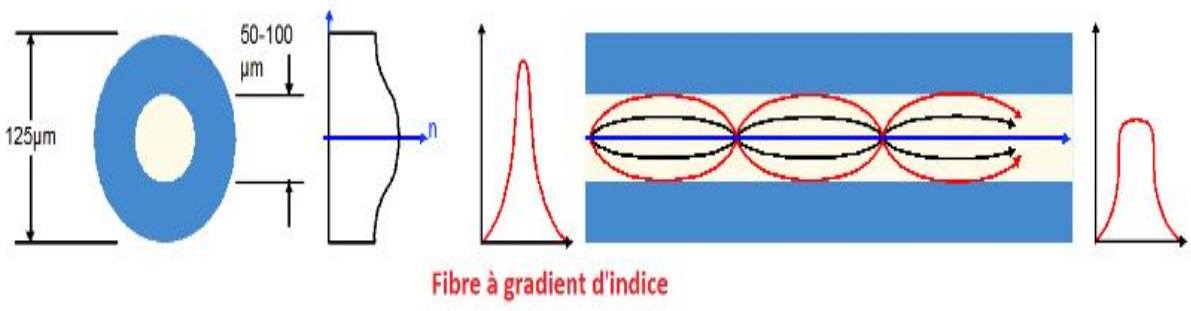
fibre à saut d'indice, il n'y a pas de grande différence d'indice de réfraction entre cœur et gaine.

Cependant, le cœur des fibres à gradient d'indice est constitué de plusieurs couches de matière ayant un indice de réfraction de plus en plus élevé.

Ces différentes couches de silice de densités multiples influent sur la direction des rayons lumineux, qui ont une forme elliptique.

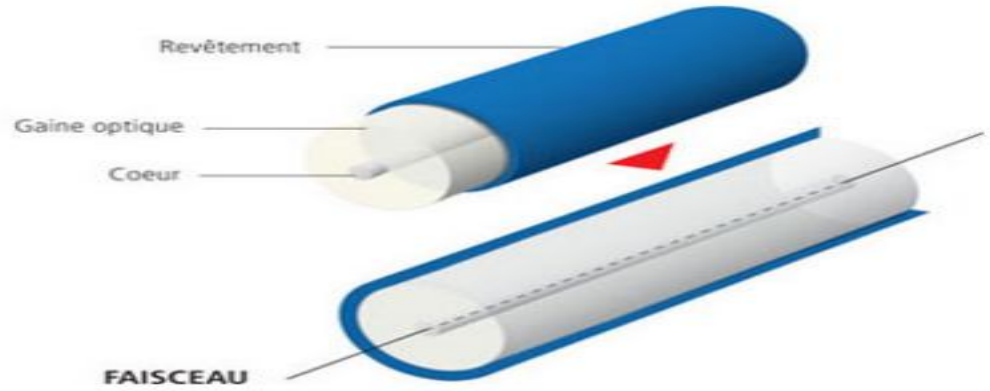
La fibre à gradient d'indice possède un coeur de taille intermédiaire. L'atténuation sur ce type de fibre est moins importante que sur les fibres à saut d'indice.

- ✓ **Débit:** environ 1 Gbit/s
- ✓ **Portée maximale:** environ 2 Km
- ✓ **Affaiblissement:** 10 dB/Km



FigI.19- Propagation dans la fibre optique à gradient d'indice

- ➢ **Fibre monomode :**

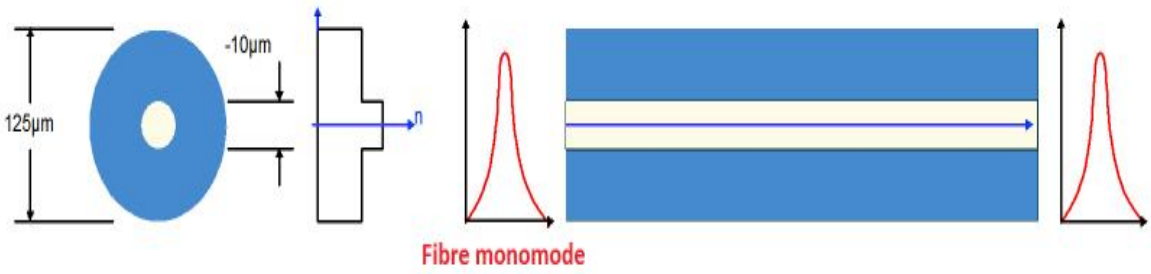


FigI.20-Fibre optique monomode

La fibre monomode est la meilleure fibre existante à l'heure actuelle. C'est ce type de fibre qui est utilisé dans les cœurs de réseaux mondiaux.

Un seul mode de propagation de la lumière existe : c'est le mode en ligne droite. La fibre monomode possède un coeur très fin, de la taille d'un cheveu. L'atténuation sur ce type de fibre est quasi nulle, c'est ce qui en fait sa force.

- ✓ **Débit:** environ 100 Gbit/s
- ✓ **Portée maximale:** environ 100 Km
- ✓ **Affaiblissement:** 0,5 dB/Km



FigI.21-Propagation dans la fibre optique monomode

➢ Les principaux connecteurs de la fibre optique :

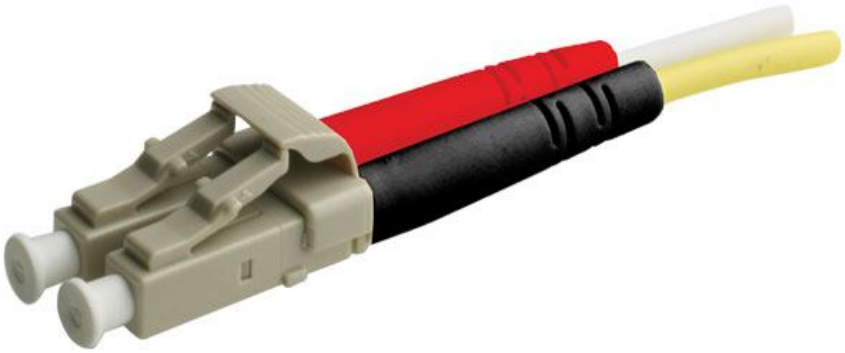
- ❖ ***Le connecteur ST*** *: //* rappelle les fiches BNC ; le verrouillage s'effectue par quart de tour de la bague externe. Proposé par tous, le connecteur ST est devenu un standard. Il porte la dénomination BFOC 2.5.

FigI.22-Connecteur ST

- ***Le connecteur SC*** : Il est le plus employé actuellement. On le retrouve sur un grand nombre d'équipements actifs quelle que soit l'application (Ethernet par exemple). Il présente de nombreux avantages par rapport aux connecteurs ST: il possède une conception "pull-proof" donc pas de risque de déconnexion lors d'une traction sur le câble, une section rectangulaire pour une meilleure prise en main et un guidage amélioré à l'intérieur du raccord. Il porte la dénomination SC ("Subscriber connector").

FigI.23-Connecteur SC

- ***Le connecteur bi-fibre LC*** : Il dispose d'embouts céramiques 1,25 mm et corps plastique. Les fibres sont espacées de 6,25 mm. Développé par AVAYA, il permet de réduire de moitié la taille des connecteurs existants, tout en conservant des technologies éprouvées. Il porte la dénomination LC.



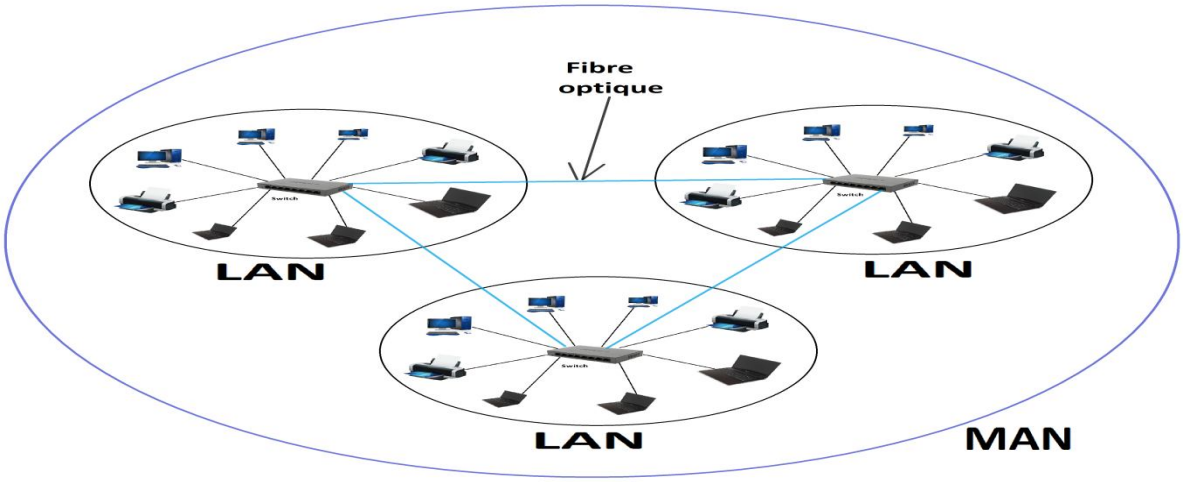
FigI.24-Connecteur LC

- ***Le connecteur MT-RJ :*** IL est réalisé autour d'un embout rectangulaire à 2 positions en polymère chargé. C'est un connecteur bivoie où les 2 fibres dans l'embout sont espacées de 750 µm. Il porte la dénomination MT-RJ.

FigI.25-Connecteur MT-RJ

I-3-3-Les réseaux MAN (*Metropolitan Area Network)* :

Les réseaux métropolitains (MAN, Metropolitan Area Network) interconnectent plusieurs réseaux locaux géographiquement proches (au maximum quelques dizaines de kilomètres] avec un débit important. Ainsi, un réseau métropolitain permet a deux machines distantes de communiquer comme si elles faisaient partie d'un même réseau local. Un MAN est forme d'équipements réseau interconnectes par des liens hauts débits (en général en fibre optique) [1].



FigI.26-Réseau MAN

I-3-4-Les réseaux WAN (*Wide Area Network)*:

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

I-4-Conclusion:

Dans ce chapitre nous avons vu les concepts généraux liées aux réseaux informatiques. Parmi ces concepts, nous avons abordé la classification de ces derniers selon leurs étendus géographique.

Les topologies et leurs constituants matériels des réseaux LAN, ainsi que la notion de VLANs ont été aussi abordés.

La compréhension de ces concepts est une étape nécessaire pour acquérir la maitrise globale d'un environnement réseau.

Chapitre II: La transmission des données

II.1- Introduction :

Réseaux locaux, réseaux sans fil, réseaux d'opérateurs ou petits réseaux privés, ils obéissent tous à des principes de structuration, utilisant une architecture en couches, dans laquelle la communication entre ordinateurs obéit à des règles précises définies par des protocoles de communication, les plus connus étant TCP et IP, ils ont donné leur nom à l'architecture TCP/IP.

Dans ce chapitre on débutera par donner une description précise du **modèle de référence OSI**, définir les concepts généraux du modèle TCP/IP et les protocoles qui y sont utilisés puis on parlera sur les équipements d'interconnexion utilise pour relier des réseaux locaux et on terminera par une présentation des caractéristiques et des techniques de commutation et les modes de transmissions de données.

II.2-Les architectures de réseaux :

II.2.1-Le modèle de référence OSI :

Le modèle de référence OSI comporte sept niveaux, ou couches, plus un médium physique. Le médium physique, que l'on appelle parfois couche 0, correspond au support physique de communication chargé d'acheminer les éléments binaires d'un point à un autre jusqu'au récepteur final. Ce médium physique peut prendre diverses formes, allant du câble métallique aux signaux hertziens, en passant par la fibre optique. [1]

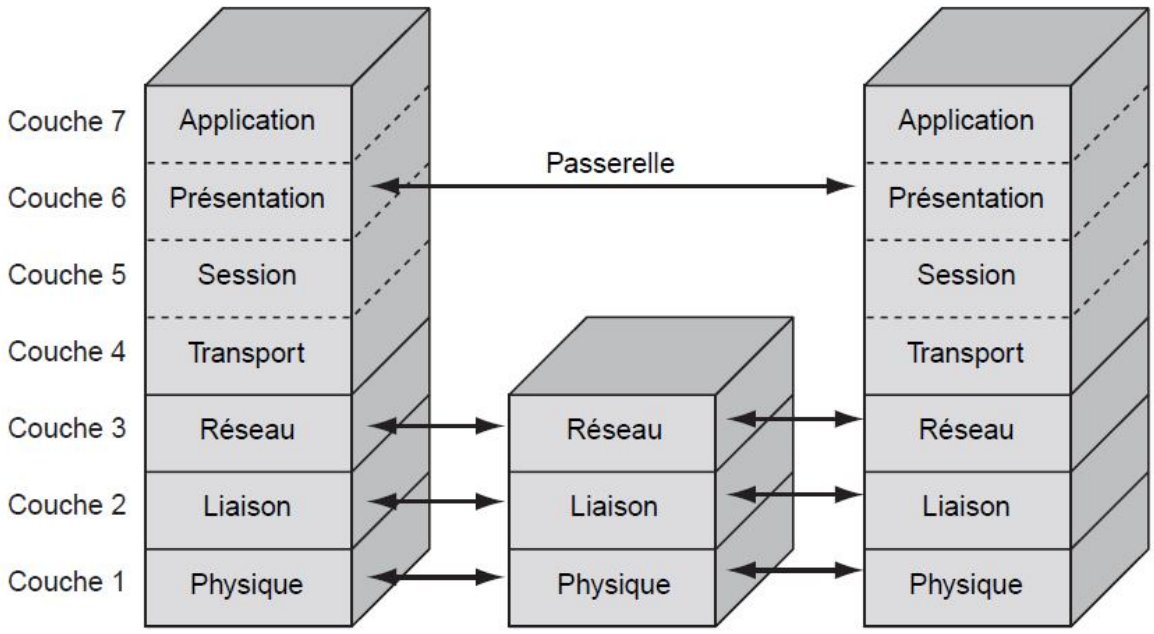


Fig.II.1-L'architecture OSI

II.2.1.1- Les couches du modèle de référence

II.2.1.1.1- La couche 1 Physique (niveau physique)

Le niveau physique correspond aux règles et procédures à mettre en œuvre pour acheminer les éléments binaires sur le médium physique. On trouve dans le niveau physique les équipements réseau qui traitent l'élément binaire, comme les modems, concentrateurs, ponts, hubs, etc.
Les différentes topologies de support physique affectent le comportement du niveau physique.

II.2.1.1.2- La couche 2 liaison (niveau trame)

La trame est l'entité transportée sur les lignes physiques. Elle contient un certain nombre d'octets transportés simultanément. Le rôle du niveau trame consiste à envoyer un ensemble d'éléments binaires sur une ligne physique de telle façon qu'ils puissent être récupérés correctement par le récepteur. Sa première fonction est de reconnaître, lors de l'arrivée des éléments binaires, les débuts et fins de trame. C'est là, aujourd'hui, le rôle principal de cette couche, qui a été fortement modifiée depuis son introduction dans le modèle de référence. Au départ, elle avait pour fonction de corriger les erreurs susceptibles de se produire sur le support physique, de sorte que le taux d'erreur résiduelle reste négligeable. En effet, s'il est impossible de corriger toutes les erreurs, le taux d'erreur non détectée doit rester négligeable. Le seuil à partir duquel on peut considérer le taux d'erreur comme négligeable est dépendant de l'application et ne constitue pas une valeur intrinsèque.[8]

II.2.1.1.3- La couche 3 réseau (niveau paquet)

Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

II.2.1.1.4- La couche 4 transport (niveau message)

La couche transport doit normalement permettre à la machine source de communiquer directement avec la machine destinatrice. On parle de communication de bout en bout (end to end). Son rôle est d'optimiser l'utilisation des services de réseau

disponibles afin d'assurer à moindre coût les performances requise par la couche session.

II.2.1.1.5- La couche 5 session (niveau session)

Définit l'ouverture et la destruction des sessions de communication entre les machines du réseau. Il s'agit de la gestion d'accès, de sécurité et d'identification. Son rôle est de transmettre les informations de programmes à programmes.

II.2.1.16- La couche 6 présentation (niveau présentation)

La couche présentation définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.

II.2.1.1.7- La couche 7 application (niveau application)

Dans la couche 7 on trouve normalement les applications qui communiquent ensemble. (Courrier électronique, transfert de fichiers,...) et son rôle assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tout les services directement utilisables par l'application (transfert de données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications). [1]

II.2.2- Le modèle TCP/IP :

Le modèle TCP/IP, inspiré du modèle OSI, reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre :

Modèle TCP/IP	Modèle OSI
Couche Application	Couche Application
	Couche Présentation
	Couche Session
Couche Transport (TCP)	Couche Transport
Couche Internet (IP)	Couche Réseau
Couche Accès réseau	Couche Liaison données
	Couche Physique

Tableau II.1. Couches du modèle TCP/IP

Comme on peut le remarquer, les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI. [1]

II.2.2.1- Encapsulation des données :

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un **en-tête**, ensemble d'informations qui garantit la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état originel.

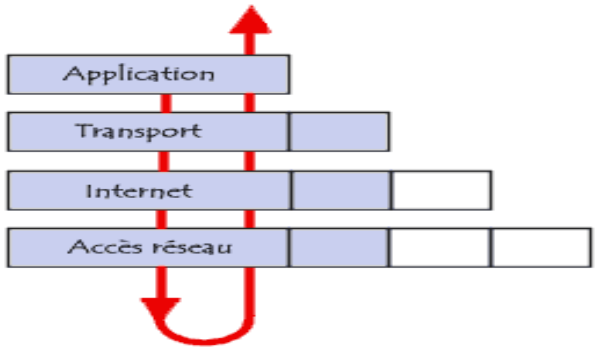


Fig.II.2- Encapsulation des données

A chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé **message** au niveau de la couche Application
- Le message est ensuite encapsulé sous forme de **segment** dans la couche Transport
- Le segment une fois encapsulé dans la couche Internet prend le nom de **datagramme**
- Enfin, on parle de **trame** au niveau de la couche Accès réseau.[8]

II.2.2.2- Protocole (c'est quoi un protocole) :

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (le FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP), ...etc

II.2.2.3- Protocoles orientés et non orientés connexion :

On classe généralement les protocoles en deux catégories selon le niveau de contrôle des données que l'on désire :[3]

- **Les protocoles orientés connexion** : Il s'agit des protocoles opérant un contrôle de transmission des données pendant une communication établie entre deux machines. Dans un tel schéma, la machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données qu'elle envoie. Les données sont ainsi envoyées sous forme de flot. TCP est un protocole orienté connexion. [2]

- **Les protocoles non orientés connexion** : Il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première. Les données sont ainsi envoyées sous forme de blocs (datagrammes). UDP est un protocole non orienté connexion

II.2.2.4- La couche Accès réseau :

La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.

Ainsi, la couche accès réseau contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local, de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau. Elle prend en charge les notions suivantes :

- ✓ Acheminement des données sur la liaison
- ✓ Coordination de la transmission de données (synchronisation)
- ✓ Format des données
- ✓ Conversion des signaux (analogique/numérique)
- ✓ Contrôle des erreurs à l'arrivée
- ✓ ...

Heureusement toutes ces spécifications sont transparentes aux yeux de l'utilisateur, car l'ensemble de ces tâches est en fait réalisé par le système d'exploitation, ainsi que les drivers du matériel permettant la connexion au réseau (ex : driver de carte réseau).[1]

II.2.2.5- La couche Internet :

La couche Internet est c'est elle qui définit les datagrammes, et qui gère les notions d'adressage IP. Elle permet l'acheminement des datagrammes (paquets de données) vers des machines distantes ainsi que de la gestion de leur fragmentation et de leur assemblage à réception.

La couche Internet contient 5 protocoles : [3]

- ✓ Le protocole IP
- ✓ Le protocole ARP
- ✓ Le protocole ICMP
- ✓ Le protocole RARP
- ✓ Le protocole IGMP

II.2.2.5.1- Le protocole IP :

Le **protocole IP** fait partie de la couche Internet de la suite de protocoles TCP/IP. C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (des données encapsulées), sans toutefois en assurer la « livraison ». En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

Le protocole IP détermine le destinataire du message grâce à 3 champs : [6]

- ✓ ***Le champ adresse IP :*** adresse de la machine
- ✓ ***Le champ masque de sous-réseau :*** un masque de sous-réseau permet au protocole IP de déterminer la partie de l'adresse IP qui concerne le réseau
- ✓ **Le champ passerelle par défaut :** Permet au protocole Internet de savoir à quelle machine remettre le datagramme si jamais la machine de destination n'est pas sur le réseau local.

Remarque : Le routage IP fait partie intégrante de la couche IP de la suite TCP/IP. Le routage consiste à assurer l'acheminement d'un datagramme IP à travers un réseau en empruntant le chemin le plus court. Ce rôle est assuré par des machines appelées routeurs, c'est-à-dire des machines reliées (reliant) au moins deux réseaux.

II.2.2.5.2- Le protocole ARP :

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse (en anglais ARP signifie Address Resolution Protocol). [6]

Chaque machine connectée au réseau possède un numéro d'identification de 48 bits (***adresse MAC***). Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte en usine. Toutefois la communication sur Internet ne se fait pas directement à partir de ce numéro (car il faudrait modifier l'adressage des ordinateurs à chaque fois que l'on change une carte réseau) mais à partir d'une adresse dite logique attribuée par un organisme : l'adresse IP.

Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance. Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête sur le réseau. L'ensemble des machines du réseau vont comparer cette adresse logique à la leur. Si l'une d'entre-elles s'identifie à cette adresse, la machine va répondre à ARP qui va stocker le couple d'adresses dans la table de correspondance et la communication va alors pouvoir avoir lieu. [6]

II.2.2.5.3- Le protocole ICMP :

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé Delivery Problem).

Les messages ICMP sont encapsulés, ils sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi, les messages d'erreur peuvent eux-mêmes être sujet d'erreurs. Toutefois en cas d'erreur sur un datagramme transportant un message ICMP, aucun message d'erreur n'est délivré pour éviter un effet « boule de neige » en cas d'incident sur le réseau. [6]

II.2.2.5.4- Le protocole RARP :

Le protocole RARP (Reverse Address Resolution Protocol) est beaucoup moins utilisé, il signifie Protocole ARP inversé, il s'agit donc d'une sorte d'annuaire inversé des adresses logiques et physiques.

Le protocole RARP permet à une station de connaître son adresse IP à partir d'une table de correspondance entre adresse MAC (adresse physique) et adresses IP hébergée par une passerelle (gateway) située sur le même réseau local (LAN).

Pour cela il faut que l'administrateur paramètre le gateway (routeur) avec la table de correspondance des adresses MAC/IP. En effet, à la différence de ARP ce protocole est statique. Il faut donc que la table de correspondance soit toujours à jour pour permettre la connexion de nouvelles cartes réseau.

RARP souffre de nombreuses limitations. Il nécessite beaucoup de temps d'administration pour maintenir des tables importantes dans les serveurs. Cela est d'autant plus vrai que le réseau est grand. Cela pose les problèmes de la ressource humaine, nécessaire au maintien des tables de correspondance et des capacités des matériels hébergeant la partie serveur du protocole RARP. En effet, RARP permet à plusieurs serveurs de répondre à des requêtes, bien qu'il ne prévoit pas de mécanismes garantissant que tous les serveurs soient capables de répondre, ni même qu'ils répondent de manière identique.

Ainsi, dans ce type d'architecture on ne peut avoir confiance en un serveur RARP pour savoir si à une adresse MAC peut être liée à une adresse IP parce que d'autres serveurs RARP peuvent avoir une réponse différente. Une autre limitation de RARP est qu'un serveur ne peut servir qu'un LAN.

Pour pallier les deux premiers problèmes d'administration, le protocole RARP peut être remplacé par le protocole DRARP, qui en est une version dynamique. Une autre approche, consiste à utiliser un serveur DHCP, qui lui, permet une résolution dynamique des adresses. [2]

II.2.2.5.5- Le protocole IGMP :

Le protocole IGMP (Internet Group Management Protocol) est un protocole Internet de Gestion de groupes entre les machines et les routeurs de groupe. Il permet d'échanger des informations d'appartenance aux groupes. Il est utilisé pour accéder à un groupe de multidiffusion IP.[3]

Remarque : *La multidiffusion (multicast) est une technique intégrée au protocole IP qui permet à plusieurs machines destinataires de recevoir une même trame. Par rapport à du broadcast, qui s'adresse à toutes les machines du réseau, le muticast ne s'adresse qu'à un groupe de machines ciblées au sein du réseau.*

II.2.2.6- La couche transport :

Les protocoles des couches précédentes permettaient d'envoyer des informations d'une machine à une autre. La couche transport permet à des applications tournant sur des machines distantes de communiquer. Le problème consiste à identifier ces applications.

En effet, suivant la machine et son système d'exploitation, l'application pourra être un programme ou une tâche.

De plus, la dénomination de l'application peut varier d'un système à un autre, c'est la raison pour laquelle un système de numéro a été mis en place afin de pouvoir associer un type d'application à un type de données, ces identifiants sont appelés ports.

La couche transport contient deux protocoles permettant à deux applications d'échanger des données indépendamment du type de réseau emprunté (c'est-à-dire indépendamment des couches inférieures…), il s'agit des protocoles suivants :[6]

- ***TCP***, un protocole orienté connexion qui assure le contrôle des erreurs
- ***UDP***, un protocole non orienté connexion dont le contrôle d'erreur est archaïque

II.2.2.6.1- Port :

De nombreux programmes TCP/IP peuvent être exécutés simultanément sur Internet (on peut par exemple ouvrir plusieurs navigateurs simultanément ou bien naviguer sur des pages HTML tout en téléchargeant un fichier). Chacun de ces programmes travaille avec un protocole, toutefois l'ordinateur doit pouvoir distinguer les différentes sources de données.

Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits : un port (la combinaison adresse IP + port est alors une adresse unique au monde, elle est appelée **socket**).

L'adresse IP sert donc à identifier de façon unique un ordinateur sur le réseau tandis que le numéro de port indique l'application à laquelle les données sont destinées. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers l'application correspondante. S'il s'agit d'une requête à

destination de l'application, l'application est appelée application serveur. S'il s'agit d'une réponse, on parle alors d'application cliente.[3]

II.2.2.6.2- Le protocole TCP :

TCP (qui signifie Transmission Control Protocol, soit en français : Protocole de Contrôle de Transmission) est un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP). Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP. TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission. Les caractéristiques principales du protocole TCP sont les suivantes

Grâce au protocole TCP, les applications peuvent communiquer de façon sûre (grâce au système d'accusés de réception du protocole TCP), indépendamment des couches inférieures. Cela signifie que les routeurs (qui travaillent dans la couche Internet) ont pour seul rôle l'acheminement des données sous forme de datagrammes, sans se préoccuper du contrôle des données, car celui-ci est réalisé par la couche transport (plus particulièrement par le protocole TCP).

Lors d'une communication à travers le protocole TCP, les deux machines doivent établir une connexion. La machine émettrice (celle qui demande la connexion) est appelée client, tandis que la machine réceptrice est appelée serveur. On dit qu'on est alors dans un environnement Client/serveur .

Pour permettre le bon déroulement de la communication et de tous les contrôles qui l'accompagnent, les données sont encapsulées, c'est-à-dire qu'on ajoute aux paquets de données un en-tête qui va permettre de synchroniser les transmissions et d'assurer leur réception.

Une autre particularité de TCP est de pouvoir réguler le débit des données grâce à sa capacité à émettre des messages de taille variable, ces messages sont appelés segments. [2]

II.2.2.6.3- Le protocole UDP :

Le protocole UDP (User Datagram Protocol) est un protocole orienté « non connexion ». Pour faire simple, lorsqu'une machine A envoie des paquets à destination d'une machine B, ce flux est unidirectionnel. En effet, la transmission des données se fait sans prévenir le destinataire (la machine B), et le destinataire reçoit les données sans effectuer d'accusé de réception vers l'émetteur (la machine A). Ceci est dû au fait que l'encapsulation des données envoyées par le protocole UDP ne permet pas de transmettre les informations concernant l'émetteur. De ce fait, le destinataire ne connait pas l'émetteur des données hormis son IP.[2]

II.2.2.7- La couche application :

La couche application est la couche située au sommet des couches de protocoles TCP/IP. Celle-ci contient les applications réseaux permettant de communiquer grâce aux couches inférieures.

Les logiciels de cette couche communiquent donc grâce à un des deux protocoles de la couche inférieure (la couche transport) c'est-à-dire TCP ou UDP.

Les applications de cette couche sont de différents types, mais la plupart sont des services réseau, c'est-à-dire des applications fournies à l'utilisateur pour assurer l'interface avec le système d'exploitation. On peut les classer selon les services qu'ils rendent :[3]

- Les services de gestion (transfert) de fichier et d'impression ;
- Les services de connexion au réseau ;
- Les services de connexion à distance ;
- Les utilitaires Internet divers.

II.3- Les équipements d'interconnexion réseaux :

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

Lorsqu'il s'agit de deux réseaux de même type, il suffit de faire passer les trames de l'un sur l'autre. Dans le cas contraire, c'est-à-dire lorsque les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à une conversion de protocole avant de transférer les trames. Ainsi, les équipements à mettre en œuvre sont différents selon la configuration face à laquelle on se trouve.

II.3.1- Les répéteurs :

Sur une ligne de transmission, le signal subit des distorsions et un affaiblissement d'autant plus importants que la distance qui sépare deux éléments actifs est longue. Généralement, deux nœuds d'un réseau local ne peuvent pas être distants de plus de quelques centaines de mètres, c'est la raison pour laquelle un équipement supplémentaire est nécessaire au-delà de cette distance.

Un répéteur (en anglais repeater) est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.

D'autre part, un répéteur peut permettre de constituer une interface entre deux supports physiques de types différents, c'est-à-dire qu'il peut par exemple permettre de relier un segment de paire torsadée à un brin de fibre optique.[6]

II.3.2- Les concentrateurs (Hub) :

Un concentrateur est un élément matériel permettant de concentrer le traffic réseau provenant de plusieurs hôtes, et de régénérer le signal. Le concentrateur est ainsi une entité possédant un certain nombre de ports (il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4, 8, 16 ou 32). Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports. Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé répéteur multiports.[6]

Fig.II.3-Le concentrateur(Hub)

On distingue plusieurs catégories de concentrateurs :

- ***Les concentrateurs dits "actifs" :*** ils sont alimentés électriquement et permettent de régénérer le signal sur les différents ports.
- ***Les concentrateurs dits "passifs" :*** ils ne permettent que de diffuser le signal à tous les hôtes connectés sans amplification.

II.3.3-Les ponts (bridge) :

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique (au niveau de la couche 2 du modèle OSI), c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont.

Ainsi, le pont permet de segmenter un réseau en conservant au niveau du réseau local les trames destinées au niveau local et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic (notamment les collisions) sur chacun des réseaux et d'augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être écoutées sur l'autre brin.

En contrepartie, l'opération de filtrage réalisée par le pont peut conduire à un léger ralentissement lors du passage d'un réseau à l'autre, c'est la raison pour laquelle les ponts doivent être judicieusement placés dans un réseau.[6]

- ***Principe de fonctionnement :***

Un pont fonctionne selon la couche Liaison données du modèle OSI, c'est-à-dire qu'il opère au niveau des adresses physiques des machines. En réalité le pont est relié à plusieurs réseaux locaux, appelés segments. Le pont élabore une table de correspondance entre les adresses des machines et le segment auquel elles appartiennent et "écoute" les données circulant sur les segments.

Lors d'une transmission de données, le pont vérifie sur la table de correspondance le segment auquel appartiennent les ordinateurs émetteurs et récepteurs (grâce à leur adresse physique, appelée adresse MAC, et non leur adresse IP. Si ceux-ci appartiennent au même segment, le pont ne fait rien, dans le cas contraire il va faire basculer les données vers le segment auquel appartient le destinataire.[]

Fig.II.4-Le pont (Cisco-Linksys HomeLink Broadband Network Bridge)

II.3.4-Les commutateurs (switch) :

Un commutateur (en anglais switch) est un pont multiports, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI. Le commutateur analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (on parle de commutation ou de réseaux commutés). Si bien que le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

Le commutateur utilise un mécanisme de filtrage et de commutation consistant à diriger les flux de données vers les machines les plus appropriées, en fonction de certains éléments présents dans les paquets de données.[6]

Fig.II.5-Le commutateur (switch)

Un commutateur de niveau 4, agissant au niveau de la couche transport du modèle OSI, inspecte les adresses de source et de destination des messages, dresse une table qui lui permet alors de savoir quelle machine est connectée sur quel port du switch (en général ce processus se fait par auto-apprentissage, c'est-à-dire automatiquement, mais le gestionnaire du switch peut procéder à des réglages complémentaires).

Connaissant le port du destinataire, le commutateur ne transmettra le message que sur le port adéquat, les autres ports restants dès lors libres pour d'autres transmissions pouvant se produire simultanément. Il en résulte que chaque échange peut s'effectuer sans collisions, avec pour conséquence une augmentation très sensible de la bande passante du réseau.[3]

II.3.5-Les passerelles (gateway) :

Une passerelle (en anglais « gateway ») est un système matériel et logiciel permettant de faire la liaison entre deux réseaux, afin de faire l'interface entre des protocoles réseau différents.

Fig.II.6-La passerelle (gateway)

Lorsqu'un utilisateur distant contacte un tel dispositif, ce dernier examine sa requête et, si jamais celle-ci correspond aux règles que l'administrateur réseau a définies, la passerelle crée une liaison entre les deux réseaux. Les informations ne sont donc pas directement transmises, mais traduites afin d'assurer la continuité des deux protocoles.

Ce système offre, outre l'interface entre deux réseaux hétérogènes, une sécurité supplémentaire car chaque information est passée à la loupe (pouvant causer un ralentissement) et parfois ajoutée dans un journal qui retrace l'historique des événements. [2]

II.3.6-Les routeurs :

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

Un routeur possède plusieurs interfaces réseau, chacune connectée sur un réseau différent. Il possède ainsi autant d'adresses IP que de réseaux différents sur lesquels il est connecté.[6]

Fig.II.7-Le routeur

On distingue généralement deux types d'algorithme de routage :

- ***Les routeurs de type vecteur de distance (distance vector)*** : ils établissent une table de routage recensant en calculant le « coût » (en termes de nombre de sauts) de chacune des routes puis transmettent cette table aux routeurs voisins. A chaque demande de connexion le routeur choisit la route la moins coûteuse.
- ***Les routeurs de type link state (link state routing) :*** ils écoutent le réseau en continu afin de recenser les différents éléments qui l'entourent. A partir de ces informations chaque routeur calcule le plus court chemin (en temps) vers les routeurs voisins et diffuse cette information sous forme de paquets de mise à jour.

II.4-Les modes de transmission :

Pour une transmission 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 du nombre de bits envoyés simultanément ;
- **La synchronisation:** il s'agit de la synchronisation entre émetteur et récepteur.

II.4.1-Liaison simplex :

Elle caractérise une liaison dans laquelle les données circulent dans un seul sens, c'est-à-dire de l'émetteur vers le récepteur. Ce genre de liaison est utile lorsque les données n'ont pas besoin de circuler dans les deux sens (par exemple d'un ordinateur vers l'imprimante ou de la souris vers l'ordinateur...).[3]

II.4.2- Liaison half-duplex :

Parfois appelée liaison à l'alternat ou semi-duplex, Elle 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.[3]

II.4.3- Liaison full-duplex:

Appelée aussi duplex intégral, elle 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 divisée par deux pour chaque sens d'émission des données si un même support de transmission est utilisé pour les deux transmissions.[3]

II.4.4- Transmission série et parallèle :

Une transmission est série ou parallèle selon le nombre d'unités élémentaires d'informations (bits) pouvant être simultanément transmises par le canal de communication.

Un processeur (l'ordinateur en général) ne traite jamais (dans le cas des processeurs récents) un seul bit à la fois, il permet généralement d'en traiter plusieurs (la plupart du temps 8, soit un octet), c'est la raison pour laquelle la liaison de base sur un ordinateur est une liaison parallèle.[3]

II.4.4.1- Liaison 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). La liaison parallèle des ordinateurs de type PC nécessite généralement 10 fils.[3]

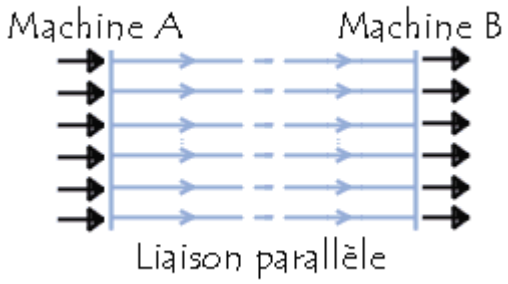


Fig.II.8-Liaison parallèle

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), étant donné que les fils conducteurs sont proches sur une nappe, il existe des perturbations (notamment à haut débit) dégradant la qualité du signal...
- **Une ligne physique** divisée en plusieurs sous-canaux par division de la bande passante. Ainsi chaque bit est transmis sur une fréquence différente...

II.4.4.2- Liaison série :

Dans une liaison en série, les données sont envoyées bit par bit sur la voie de transmission. Toutefois, étant donné que la plupart des processeurs traitent les informations de façon parallèle, il s'agit de transformer des données arrivant de façon parallèle en données en série au niveau de l'émetteur, et inversement au niveau du récepteur.[3]

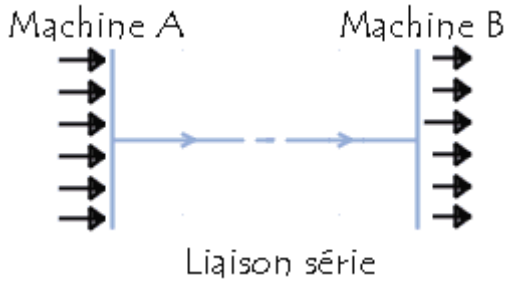


Fig.II.9-Liaison série

II.4.5- Transmission synchrone et asynchrone:

Etant donné les problèmes que pose la liaison de type parallèle, c'est la liaison série qui est la plus utilisée. 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 envoyés successivement. Il existe donc deux types de transmission permettant de remédier à ce problème :[8]

II.4.5.1- Liaison asynchrone :

Dans cette liaison chaque caractère est émis de façon irrégulière dans le temps (par exemple un utilisateur envoyant en temps réel des caractères saisis au clavier). Ainsi, imaginons qu'un seul bit soit transmis pendant une longue période de silence... le récepteur ne pourrait savoir s'il s'agit de 00010000, ou 10000000 ou encore 00000100...

Afin de remédier à ce problème, chaque caractère est précédé d'une information indiquant le début de la transmission du caractère (l'information de début d'émission est appelée bit START) et terminé par l'envoi d'une information de fin de transmission (appelée bit STOP, il peut éventuellement y avoir plusieurs bits STOP).[8]

II.4.5.2- Liaison synchrone :

Dans cette liaison, 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 est donc 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 envoi 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. [8]

II.5- Les techniques de commutation:

II.5.1- Commutation de circuits :

Dans les réseaux à commutation de circuits, de multiples supports de transmission sont installés entre les différents commutateurs. Pour échanger des informations entre deux équipements terminaux, il est nécessaire de déterminer un chemin à travers le réseau et de réserver un support de transmission entre chaque paire de commutateurs situés sur ce chemin. Chaque commutateur ré-émet les signaux qu'il reçoit suivant ce chemin. Le réseau fournit donc l'équivalent d'un support de transmission point à point entre les équipements terminaux. Le réseau téléphonique est un exemple classique de réseau à commutation de circuits. Dans le contexte de la téléphonie, le mot circuit désigne une liaison entre 2 commutateurs.

Tout dialogue se décompose en 3 phases : une première phase d'établissement du circuit entre les équipements terminaux par réservation de l'ensemble des circuits nécessaires à l'intérieur du réseau, la phase classique de transfert des informations puis une phase de libération pour permettre la réutilisation des différents circuits par d'autres équipements terminaux. La libération se fait à la demande d'un des équipements terminaux (ou si le réseau détecte qu'un équipement est en panne).

Tant qu'elle n'a pas eu lieu, les circuits restent réservés à l'intérieur du réseau, même s'il n'y a aucun transfert d'information. Ce type de commutation présente l'inconvénient de

monopoliser les circuits entre commutateurs pendant la durée entière du dialogue. Il est donc nécessaire de multiplier les circuits entre commutateurs, on parlera dans ce cas de

faisceaux (ou trunks). Il nécessite, de plus, la disponibilité simultanée des deux équipements terminaux pour tout dialogue.

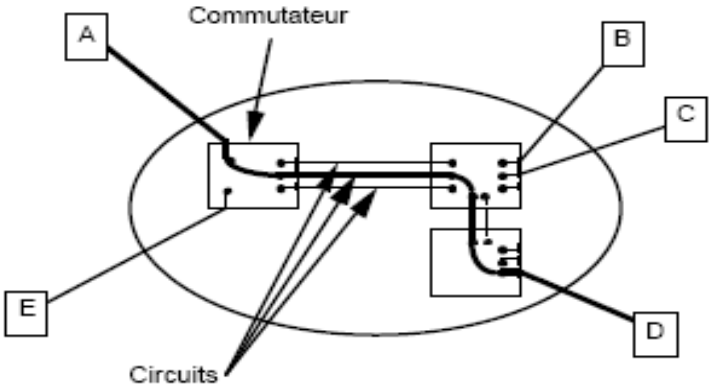


Fig.II.10-Principe de la commutation de circuits

En revanche, il présente l'avantage d'être assez simple : la commutation de circuits peut s'appliquer sur un réseau analogique ou bien numérique. Dans le cas d'un réseau numérique, la mémoire nécessaire dans les commutateurs est réduite et il n'y a aucun traitement à faire sur l'information transmise.

Un faisceau peut correspondre à plusieurs supports physiques différents (par exemple une paire torsadée par circuit) ou bien à un seul support physique sur lequel les circuits sont multiplexés en temps ou en fréquence mais la philosophie reste la même : il y a toujours réservation d'une partie de la capacité de transmission pendant tout le dialogue.[7]

II.5.2- Commutation de messages :

La commutation de messages s'applique aux seuls réseaux numériques. Un message est défini comme une suite de données binaires formant un tout logique pour les équipements terminaux. C'est, par exemple, un fichier complet, un courrier électronique ou une page d'écran. Lorsqu'un équipement veut transmettre un message, il lui ajoute l'adresse du destinataire et le transmet au commutateur. Celui-ci attend la réception complète du message, le stocke, analyse son adresse et le réémet alors vers le commutateur voisin adéquat. Le message transite ainsi à travers le réseau par réémissions successives entre les commutateurs (on utilise quelquefois le terme anglais store-and-forward).

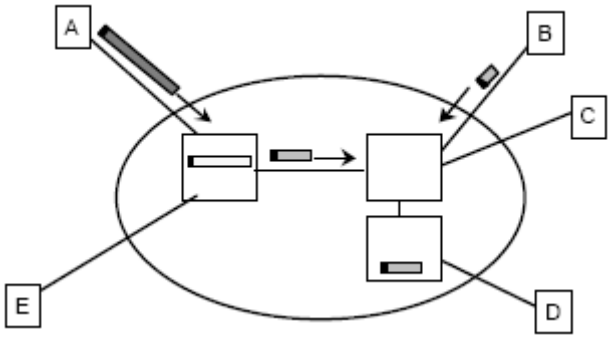


Fig.II.11-Principe de la commutation de messages

Les commutateurs sont reliés deux à deux par une liaison de données. Celle-ci est occupée uniquement pendant la durée de transmission du message mais elle n'est jamais monopolisée par un équipement indépendamment de toute transmission. De plus, si un équipement terminal est temporairement indisponible, le réseau peut stocker le message jusqu'au rétablissement de l'équipement.

Dans un tel réseau, chaque commutateur doit être capable de stocker le message en entier. Comme un commutateur supporte simultanément plusieurs dialogues et que la taille d'un message est déterminée par les équipements, la mémoire nécessaire peut être importante. De plus, le délai de transmission à travers le réseau est fonction du nombre de commutateurs traversés et de la taille du message. Il peut donc être assez important. Enfin, pour un taux d'erreur donné par bit transmis, la probabilité d'une erreur sur un message augmente avec la taille du message. La transmission de longs messages dans le réseau est donc très pénalisante.[7]

II.5.3- Commutation par paquets :

Les inconvénients de la commutation de messages sont liés à la taille des messages. La commutation par paquets consiste à découper les messages en morceaux appelés segments. Ce découpage est la segmentation. Il est fait par l'expéditeur. A chaque segment sont ajoutées des informations permettant d'identifier l'expéditeur et le destinataire : l'ensemble forme un paquet.

La taille maximale d'un paquet est fonction du réseau. Les paquets sont acheminés par le réseau comme dans un réseau à commutation de messages jusqu'au destinataire. Celui-ci attend la réception de tous les paquets pour reconstituer le message et le traiter. Cette opération est le réassemblage.

Un paquet ne forme pas un tout logique pour l'équipement terminal. Il n'a de sens que comme " atome d'information " acheminé par le réseau par réémissions successives entre les commutateurs. Sa petite taille permet de réduire le délai global d'acheminement des messages à travers le réseau. Une liaison entre commutateurs n'est pas monopolisée par un équipement mais supporte la transmission de paquets de multiples utilisateurs.

Dans la fig.II-11 le message émis par A est segmenté en 5 paquets, qui sont acheminés un par un par le réseau.[7]

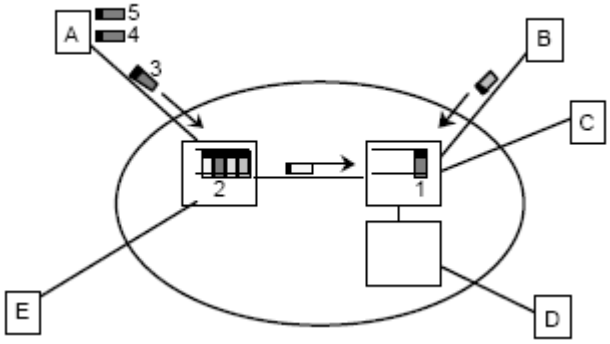


Fig.II.12-Principe de la commutation par paquets

II.6- Les réseaux IP:

Les réseaux IP (Internet) devient nom seulement un moyen de communication mais aussi un moyen de commerce globale de développement et distribution. Utilisant l'architecture TCP/IP, qui ne correspond pas à un seul protocole mais à un ensemble de petits protocoles spécialisée appelés sous protocoles (TCP, IP, UDP, ARP ICMP……).[6]

II.6.1- L'adressage IP :

Sur internet, les ordinateurs communiquent entre eux grâce au protocole IP (internet Protocol), qui utilise des adresses numériques, appelées adresses IP. C'est l'ICANN (internet Corporation for Assigned Names and Numbers, remplaçant l'IANA, internet Assigned Numbers Agency, depuis 1998) qui est chargée d'attribuer des adresses IP publiques, c.à.d les adresses IP des ordinateurs directement connectés sur le réseau public internet.

Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.

II.6.1.1- Les adresses IPv4:

L'adresse IP identifie l'emplacement d'un hôte sur le réseau. Une adresse IP doit être unique et présenter un format normalisé. Chaque adresse IP comporte deux parties :

- ✓ ***Un ID de réseau (Net ID)***
- ✓ ***Un ID d'hôte (Host ID)***

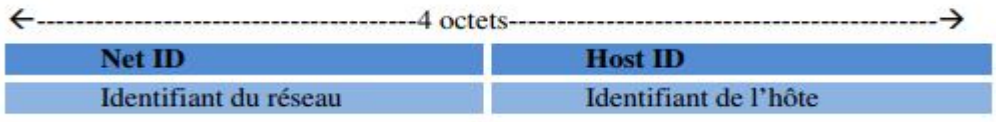


Fig.II.13-Les différentes parties d'une adresse IP

Tous les hôtes d'un même réseau doivent avoir le même **ID réseau**, unique dans l'inter-réseau. L'**ID d'hôte** identifie une station de travail, un serveur, un routeur ou tout autre hôte TCP/IP du réseau. L'ID d'hôte doit être unique pour chaque ID de réseau. Chaque hôte TCP/IP est identifié par une adresse IP logique. Tous les hôtes et les composants du réseau qui communiquent à l'aide de TCP/IP doivent posséder une adresse IP unique.

Deux formats permettent de faire référence à une adresse IP le format binaire et la notation décimale pointée.

Chaque adresse IP a une longueur de 32 bits et est composée de quatre champs de 8 bits (1 octet). Les octets sont séparés par des points et représentent un nombre décimal compris entre 0 et 255. Les 32 bits de l'adresse IP sont alloués à l'ID de réseau et à l'ID d'hôte.

II.6.1.2- Le masque réseau:

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

Le masque de réseau, ou **Netmask**, est constitué de 32 bits. Les bits à « 1 » sont tous à gauche alors que les « 0 » sont tous à droite. On dit que les bits à « 1 » sont contigus (c'est-

à-dire collés).

- ***Exemples de masques :*** 11111111.00000000.00000000.00000000 = 255.0.0.0

  11111111.11111111.11111111.00000000=255.255.255.0

  11110000.00000000.00000000.00000000 = 240.0.0.0

- **Exemple de masque invalide** : 11111111.**0**1111111.00000000.00000000

Pour calculer l'adresse réseau, il suffit d'appliquer un « ET » logique entre le masque de réseau et l'adresse IP.

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

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

II.6.1.3-Adresses particulières:

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

  Ex : 192.168.10.0/ 255.255.255.0 = 192.168.10.00000000

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

  Ex : 172.27.255.255 / 255.255.0.0 = 172.27.11111111.11111111

- ✓ ***L'adresse de rebouclage (loopback)*** **:** l'adresse 127.0.0.1 (127.X.X.X) est appelée ainsi car elle désigne la machine (local/host).

II.6.1.4-Notation CIDR:

On a vu que pour connaitre l'adresse d'un réseau, il fallait également connaitre le masque. Une forme plus courte est connue sous le nom de « notation CIDR ». Elle donne le numéro du réseau suivi par un slash ("/") et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.0.0, équivalent en binaire à 11111111.11111111.00000000.00000000, sera donc représenté par /16 (16 bits à la valeur 1, par exemple **:** 186.15.0.0 /16). [1]

II.6.1.5- Délivrance des adresses:

On distingue deux types d'adresses IP :

- ***Les adresses privées*** **:** que tout administrateur de réseau peut s'attribuer librement pourvu qu'il ne cherche pas à les router sur l'Internet.
- ***les adresses publiques*** **:** délivrées par une structure mondiale (*l'ICANN : internet Corporation for Assigned Names and Numbers*) qui en assurent l'unicité. Ce dernier point est capital pour assurer l'efficience du routage. [1]

II.6.1.6-Les classes d'adresses:

Selon la longueur de l'ID Host et de l'ID Net, on peut distinguer 5 classes d'adresses(FigII.13), le nombre d'hôtes (machines) et de sous-réseaux diffère d'une classe à l'autre(FigII.14) :

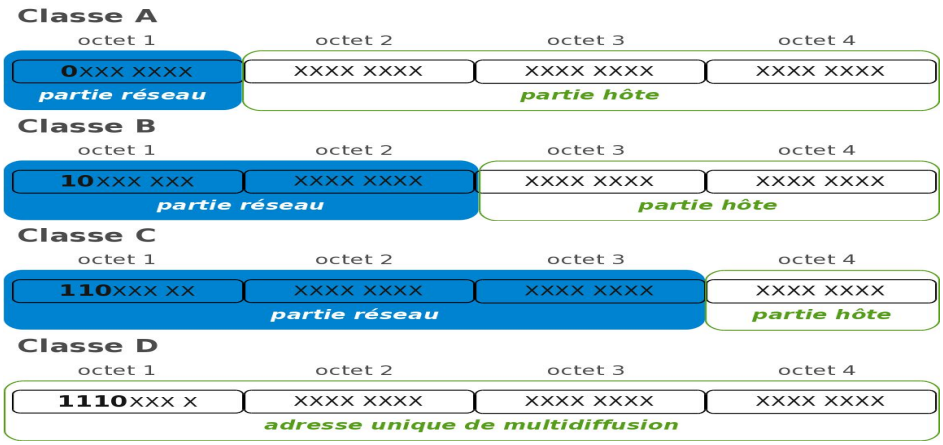


Fig.II.14-Les classes d'adresses

Classe	Nombre de réseaux/machines
A	1.x.y.z à 127.x.y.z 127 réseaux 16 777 216 machines (2^24)
B	128.0.x.y à 191.255.x.y 16 384 réseaux (2^14) 65536 machines (2^16)
C	192.0.0.z à 223.255.255.z 2 097 152 réseaux (2^21) 256 machines (2^8)
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Tableau II.2. Nombres de machines/sous-réseaux dans chaque classe

II.7- Quelques protocoles utilisées sur internet

II.7.1-Le NAT (Network Address Translation):

Le mécanisme de translation d'adresses (en **anglais Network Address Translation** noté **NAT**) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4.

En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.

Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement une « traduction ») entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle. [6]

II.7.2-Le DHCP (Dynamic Host Configuration Protocol):

DHCP utilise un modèle client/serveur dans lequel le serveur DHCP assure la gestion centralisée des adresses IP utilisées sur le réseau. Les clients qui prennent en charge DHCP peuvent ensuite demander et obtenir automatiquement la location d'une adresse IP auprès d'un serveur DHCP dans le cadre de leur procédure d'amorçage réseau. [6]

II.7.3-Le DNS (Domain Name System):

Chaque ordinateur directement connecté à internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 194.153.205.26 mais avec un nom de domaine ou des adresses plus explicites (appelées adresses FQDN : Fully Qualified Domain Name) du type [www.google.com].

Ainsi, il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name System), qui est utilisé en zone Internet (zone public) et en zone Intranet (zone privée de l'entreprise), Il s'agit d'un système standardisé et indépendant de la plate-forme qui lui fait appel malgré que les implémentations de celui-ci et les fonctionnalités offertes par ces dernières, diffèrent d'une plate-forme à une autre.

L'objectif du DNS est la résolution de noms de domaines (ou résolution d'adresses) et cela en faisant la corrélation entre les adresses IP et le nom de domaine associé, c.à.d : trouver l'adresse IP à partir du nom d'un domaine ou inversement, trouver le nom d'un domaine à partir d'une adresse IP.[6]

II.8- Conclusion

Dans ce chapitre on a abordé des notions de structuration réseau utilisant l'architecture en couche TCP/IP, obéissant a des protocoles de communications, qui sont TCP et IP, et leurs sous protocoles, comme on a aussi vu le modèle de référence OSI des architecture en couche.

Comme on a présenté aussi, les notions d'adressage IP, les différents équipements d'interconnexion réseaux, les modes de transmission, les techniques de commutation ainsi que quelques protocoles utilisées sur internet.

Chapitre III : Utilisation du logiciel IPerf 3 pour la mesure de la qualité de 3 liaisons physiques point à point au sein du réseau informatique de l'UMMTO

III.1- Introduction :

Dans ce chapitre, nous débutons par donner une présentation du logiciel IPerf, son principe de fonctionnement, puis nous donnons une présentation de l'interface graphique jPerf ainsi que ses différentes fonctionnalités. En suite, nous donnons les étapes à suivre, afin de les installer sous Windows.

Par la suite, nous citons le matériel utilisé, nous donnons la méthode de travail ainsi que le but des tests à effectuer.

Et enfin nous terminons par donner les résultats obtenues en testons 3 liaisons physiques, en tirons à chaque fois une conclusion du résultat obtenu pour chaque ligne de transmission par rapport à sa qualité.

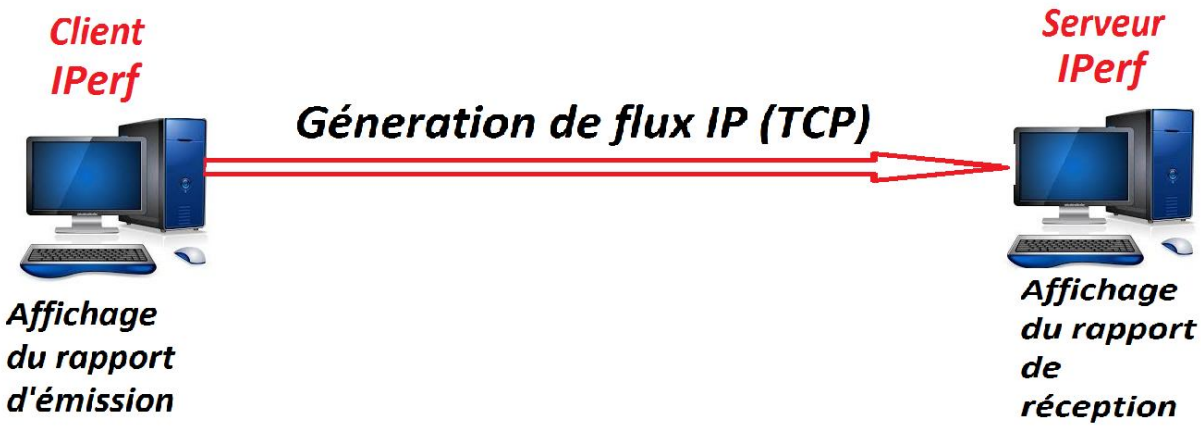
III.2- Le logiciel IPerf3 :

IPerf3 est un outil open-source pour la mesure des performances d'un réseau. Conçu pour des architectures client-serveur, Il supporte l'accord de différents paramètres liés au timing, aux tampons et aux protocoles TCP et UDP, entre autres. Pour chaque test, il indique la bande passante, la perte et d'autres paramètres.

Il se présente sous la forme d'une ligne de commande à exécuter sur deux machines disposées aux extrémités du réseau à tester. IPerf3 est principalement développé par ESnet / Lawrence Berkeley National Laboratory. Il est disponible sur de nombreuses plateformes (Linux, BSD, Mac, Windows…).

III.2.1- Principe de fonctionnement:

Iperf fonctionne suivant l'architecture client-serveur selon le diagramme suivant :



FigIII.1-Fonctionnement d'**Iperf**

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 l'option -s), la seconde en « mode client » (option -c). Par défaut le test réseau se fait en utilisant le protocole TCP (mais il est également possible d'utiliser le mode UDP avec l'option -u).

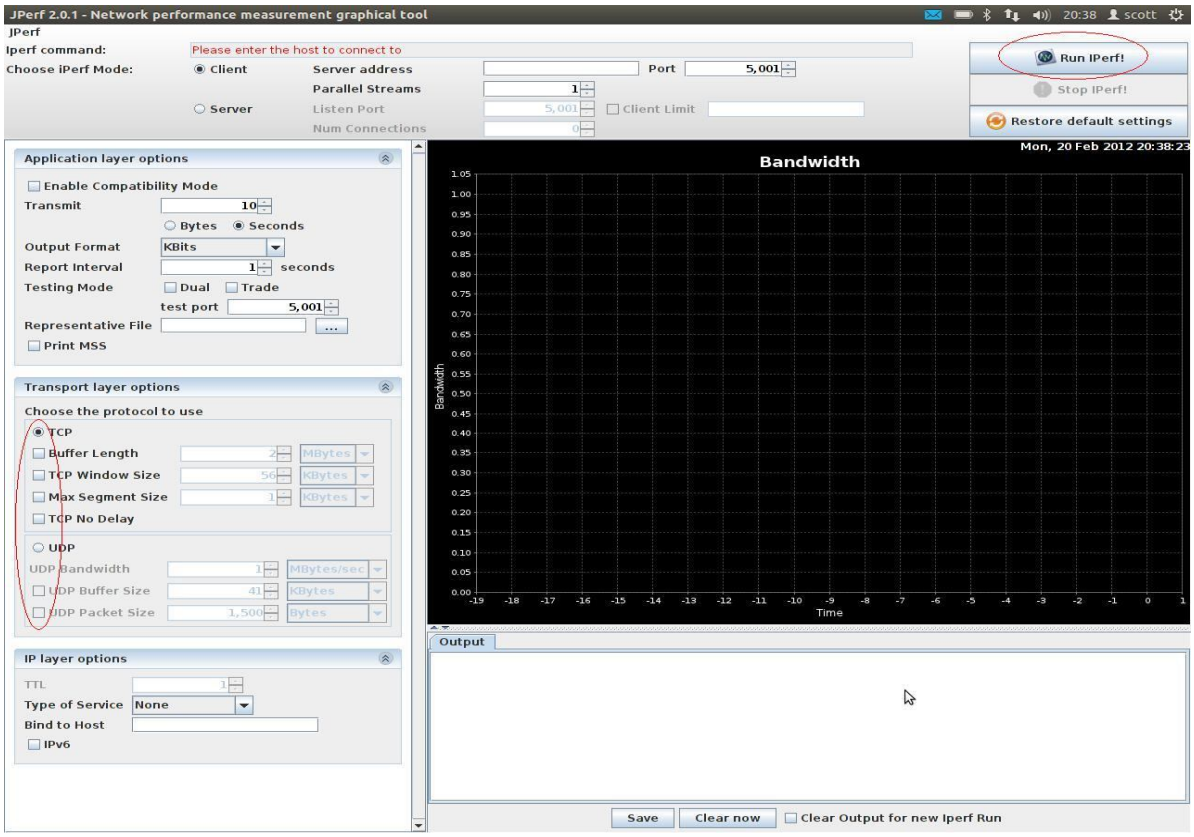
III.2.2- Interface graphique jperf:

Iperf étant un logiciel fonctionnant sous MS-DOS dans le cas de la version Windows, ce qui implique de ce fait pour pouvoir utiliser ses différentes fonctions, afin de tester les performances d'un réseau :

- On doit utiliser des commandes MS-DOS dédiées pour cela, ce qui peut s'avérer des fois compliqué à manipuler ;
- On n'obtient aucun résultat graphique des tests effectués, ce qui diminue considérablement nôtres appréciation de ces derniers.

Afin de remédier à cela, une interface graphique Java à été mise au point : **JPerf,** qui permet d'assurer toutes les fonctions d'**Iperf,** sans les deux inconvénients précédents.

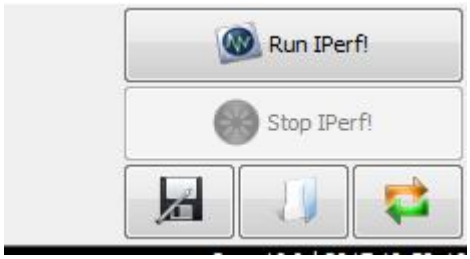
Elle se présente sous la forme suivante voir la figure ci-dessous (figIII.1) :



FigIII.1-Interface graphique JPerf

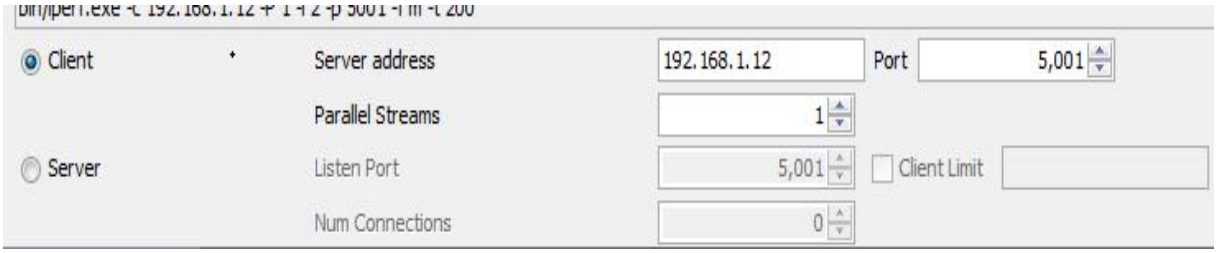
A partir de la figure ci-dessus (figIII.1), on peut voir que cette interface graphique peut être décomposée en 3 parties :

- ✓ ***La 1ière partie (haute) :***
  - ➢ Permet de lancer l'interface ou de la réinitialiser :



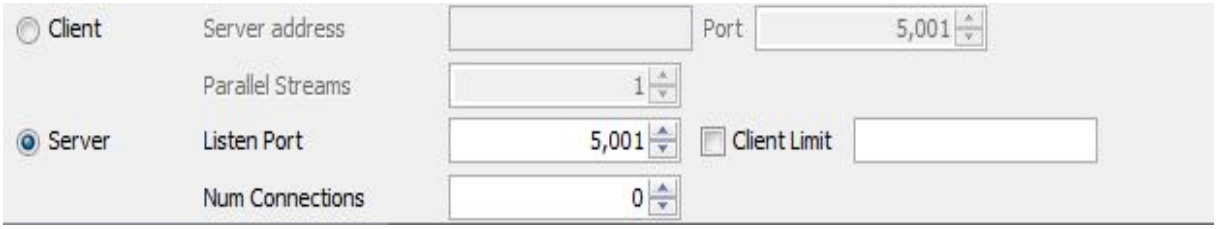
FigIII.2-Marche /arrêt de JPerf

- Permet de choisir soit le mode **client** (dans une machine parmi les deux utilisé**,** et dans ce cas la, on doit définir l'adresse du serveur (adresse de la machine configurée en mode serveur) et enfin, on peut aussi spécifier le numéro du port, celui par défaut étant 5001.



FigIII.3-Sélection du mode client et le numéro du port

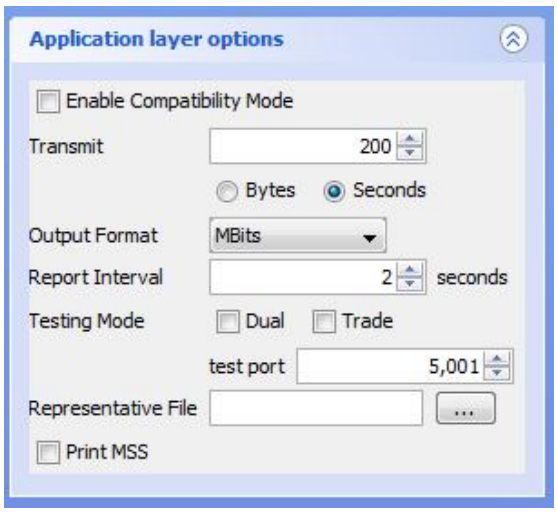
Ou le mode **serveur,** alors on doit rentrer le numéro du port écouté (Listen port) de la machine configurée en mode **client**, par défaut c'est 5001.



FigIII.4-Sélection du mode serveur et le numéro du port

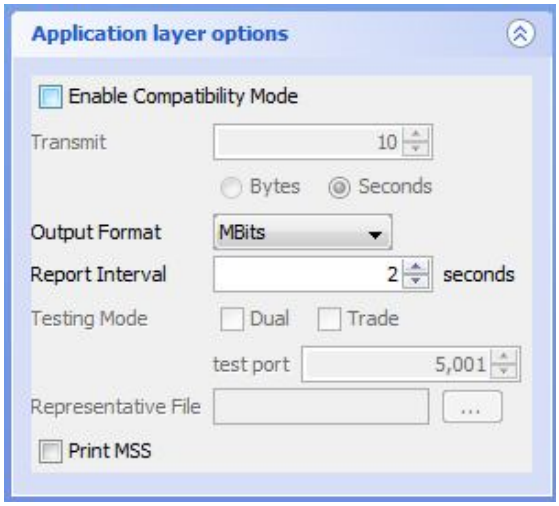
- ✓ ***La 2ième partie (à gauche) :***
  - Permet de définir, en mode **client** le temps total du test à effectuer (Transmit), le format de sortie des résultats du test (Output Format) : Kbits ou

Mbits, ainsi que l'intervalle de prise des échantillons des résultats qui seront obtenus (Report Interval).



FigIII.5-Sélection du : temps total d'un test, output format et du report interval

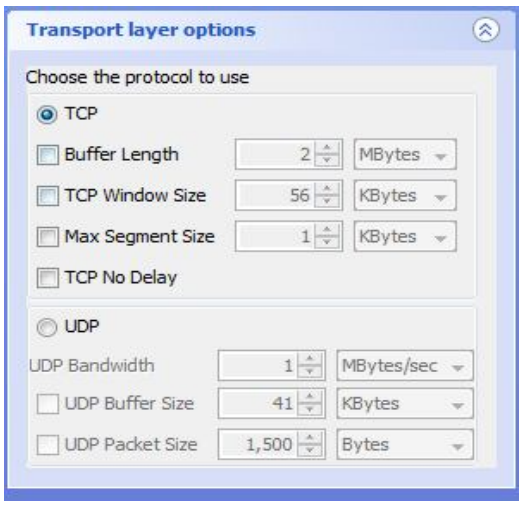
Et en mode **serveur,** on doit aussi l'*Output Format* et le *Report Interval*.



FigIII.6-Sélection du : output format et du report interval

- Cette partie permet également de choisir le protocole de communication pour la transmission de données qui sera utilisé pour effectuer le test, soit

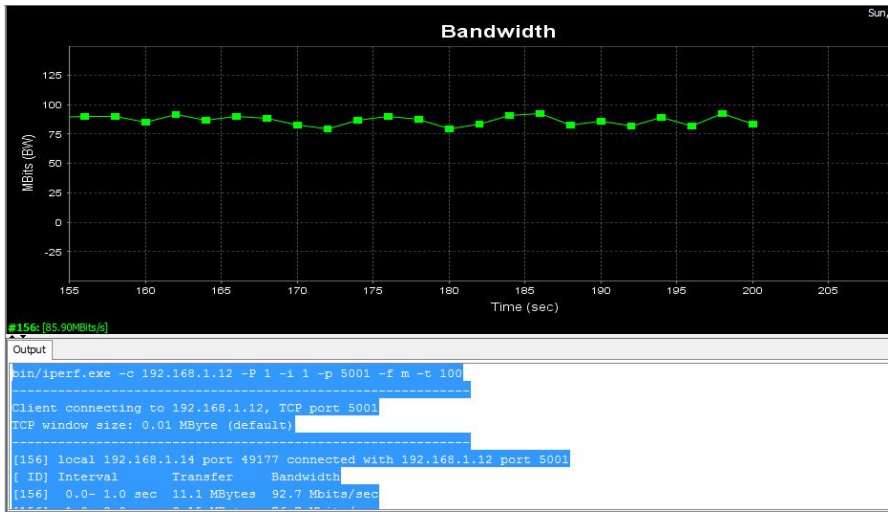
TCP ou **UDP** et cela doit être homogène dans les 2 machines, celle en mode **serveur** et celle en mode **client**.



FigIII.7-Sélection du mode TCP/UDP

✓ ***La 3ième partie (à droite) :***

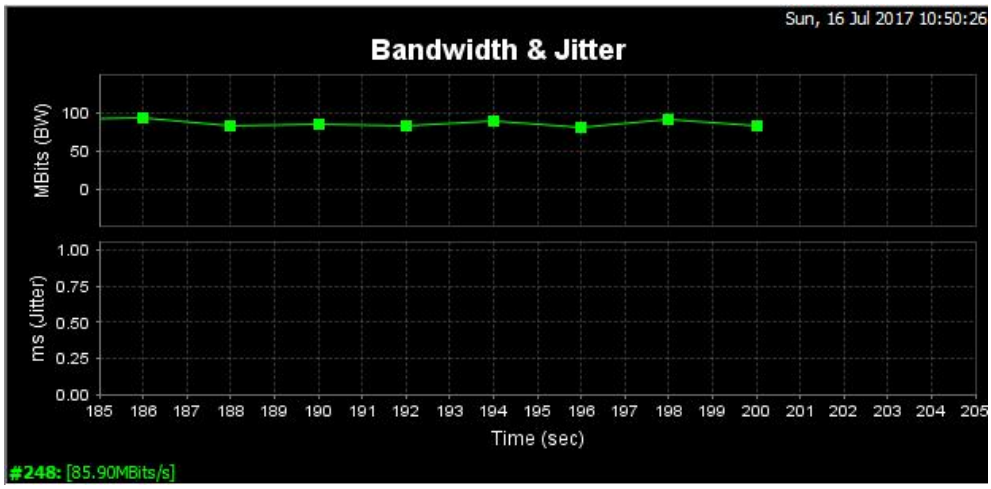
- En mode **client,** cette partie de l'interface permet de visualiser la bande passante (débit maximum) en fonction du temps du résultat du test, comme elle permet de voir sous format **texte**, pour chaque intervalle de temps de la duré total du test :
  - La bande passante en Mbits/s
  - La quantité de donnée transférée en Mbits



FigIII.8- Fenêtre graphique de JPerf

- En mode **serveur,** on à accès aux mêmes visualisations qu'en mode **client** à une différence près, c'est que dans ce cas-ci en peut aussi visualiser l'évolution de la gigue dans chaque intervalle de temps de la duré total du test.

Remarque : *La gigue est la variation de la latence, qui est quand à elle le temps que met un paquet pour arriver d'un point A à un point B dans un réseau, Il est tout à fait possible d'avoir une latence élevée, par exemple de 200ms, et d'avoir une gigue très faible. Cela veut dire que la latence est toujours la même.*



FigIII.9- Fenêtre graphique de JPerf : gigue et bande passante

III.2.3- Téléchargement et Installation sous Windows :

- ***Téléchargement :***

  - **iPerf :**

Iperf étant un logiciel open-source, on peut le télécharger gratuitement depuis le site officiel(***www.iperf.fr***), nous dans nôtre travail, on

a téléchargé la dernière version : **iPerf 3.1.3** *(du 8 juin 2016)* , pour **Windows 64bits.**

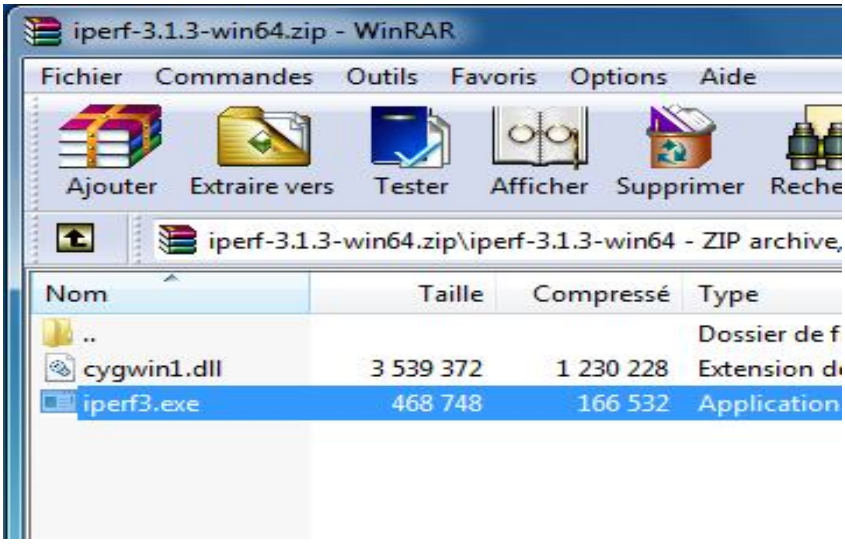
- **Jperf :**

Jperf étant lui aussi un logiciel open-source et on peut aussi de ce fait le télécharger gratuitement depuis de nombreux sites, nous dans le présent travail, nous l'avons fait depuis *« http://www.softpedia.com/get/Network-Tools/Network-Testing/JPerf.shtml#download »* et la version qu'on a téléchargé est la suivante : **jperf-2.0.2** .

Remarque : **Jperf** étant une interface graphique Java, de ce fait pour qu'il fonctionne sous Windows, on doit télécharger aussi une machine virtuelle Java(JRE : Java SE Runtime Environment) et l'installer, dans le présent travail nous avons téléchargé la version java JRE 8(le minimum conseillé étant la version 1.5 et plus), du site officiel(**www.java.com**).

- ***Installation :***
  - **iPerf :**

Le fichier téléchargé étant un archive (*format : .zip*), il suffit de décompresser le dossier qui y est contenu, de l'ouvrir et de cliquer sur **iperf3.exe**, l'installation s'effectuera instantanément.



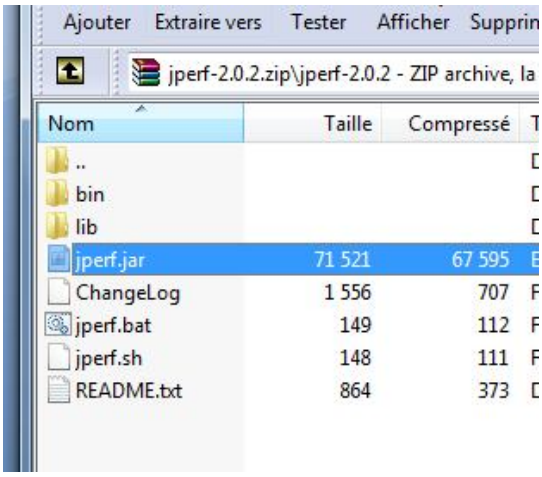
FigIII.10- Décompression/installation de IPerf

- **Jperf :**

Avant d'installer Jperf, on doit d'abord installer java JRE, téléchargée précédemment, ce qui ce fait de la même façon que pour installer n'importe quel logiciel sous Windows.

L'étape suivante consiste à décompresser le dossier Jperf téléchargé précédemment (une archive au format : .zip) et de le placer sur le bureau.

Pour lancer **jperf,** il suffit d'ouvrir ce dossier et de cliquer sur **jperf.jar** .



FigIII.11- Décompression/installation de JPerf

III.3- Matériel utilisé :

Dans le présent test, nous avons utilisé 2 PC sous Windows 7, dans lesquels sont installés : **iPerf 3.1.3** et **jperf-2.0.2** .

III.4- Méthode de travail et but des tests:

III.4- 1-Méthode de travail :

Pour effectuer nos tests :

- On a placé les deux machines utilisées, sur les 2 extrémités de chaque ligne ou liaison physique à tester ;
- On a lancé **jPerf** au début de chaque test et on a paramétré à chaque fois :
  - ✓ Le mode client sur une des 2 machines et le mode serveur sur l'autre ;
  - ✓ Le protocole TCP sur les 2 machines client et serveur ;
  - ✓ Le temps total de chaque test à 100 secondes ;
  - ✓ L'intervalle de prise des échantillons à 1 seconde.

III.4.2- Buts des tests :

C'est d'effectuer des comparaisons à chaque fois entre la quantité de donné (paquets de données) émise par le client IPerf pendant chaque seconde et le débit d'émission avec la quantité de donné qui a été reçue par le serveur IPerf pendant chaque seconde aussi et le débit de réception, et cela pendant une durée totale de 100 secondes pour chaque test.

Ainsi, les résultats obtenus détermineront la qualité des liaisons physiques (lignes) testées.

III.5- Tests :

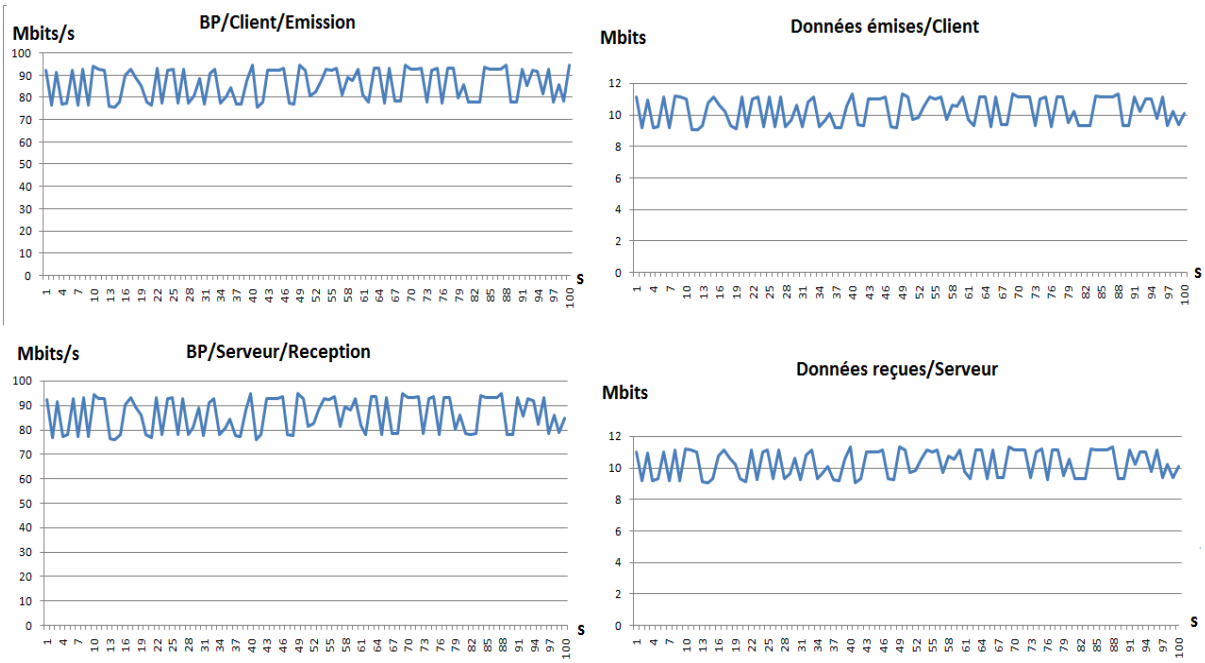
III.5.1- Test 1 :

- **Caractéristiques de la liaison physique (ligne) à tester :**
  - **Extrémités :** Bibliothèque centrale Campus de Bastos/ centre réseaux campus Hasnaoua.
  - **Type :** Fibre optique monomode.

➢ Résultats du test :

- ✓ **Données totales émise :** 1026Mbits
- ✓ **Données totales reçue :** 1026Mbits
- ✓ **Débit moyen d'émission :** 86.1 Mbits/s
- ✓ **Débit moyen de réception :** 86.1Mbits/s

Graphes :



➢ Interprétation :

- ✓ Les courbes des débits d'émission et de réception sont quasi égales, et celles des données transmises et reçues le sont également.
- ✓ La quantité de données totales émise est égale à celle reçue.
- ✓ Le débit moyen d'émission est égal à celui de réception.

➔D'après cela, on en conclu que cette liaison est bonne.

III.5.2- Test 2 :

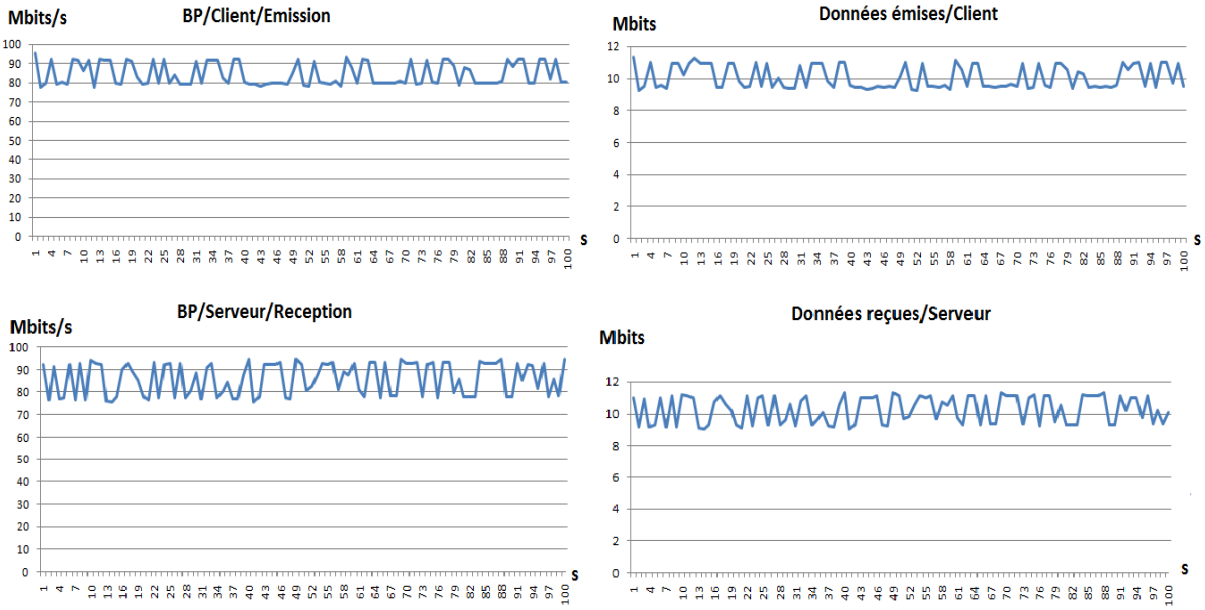
➢ Caractéristiques de la liaison physique (ligne) à tester :

- **Extrémités :** Bloc B campus Hasnaoua/Centre réseau campus Hasnaoua.
- **Type :** Fibre optique monomode.

➢ Résultats du test :

- ✓ **Données totales émise :** 1006Mbits.
- ✓ **Données totales reçue :** 1006Mbits.
- ✓ **Débit moyen d'émission :** 83.7Mbits/s.
- ✓ **Débit moyen de réception :** 83.7 Mbits/s.

Graphes :



- **Interprétation :**

✓ Les courbes des débits d'émission et de réception sont quasi égales, et celles des données transmises et reçues le sont également.
✓ La quantité de données totales émise est égale à celle reçue.
✓ Le débit moyen d'émission est égal à celui de réception.

➔D'après cela, on en conclu que cette liaison est bonne.

III.5.3- Test 3 :

- **Caractéristiques de la liaison physique (ligne) à tester :**

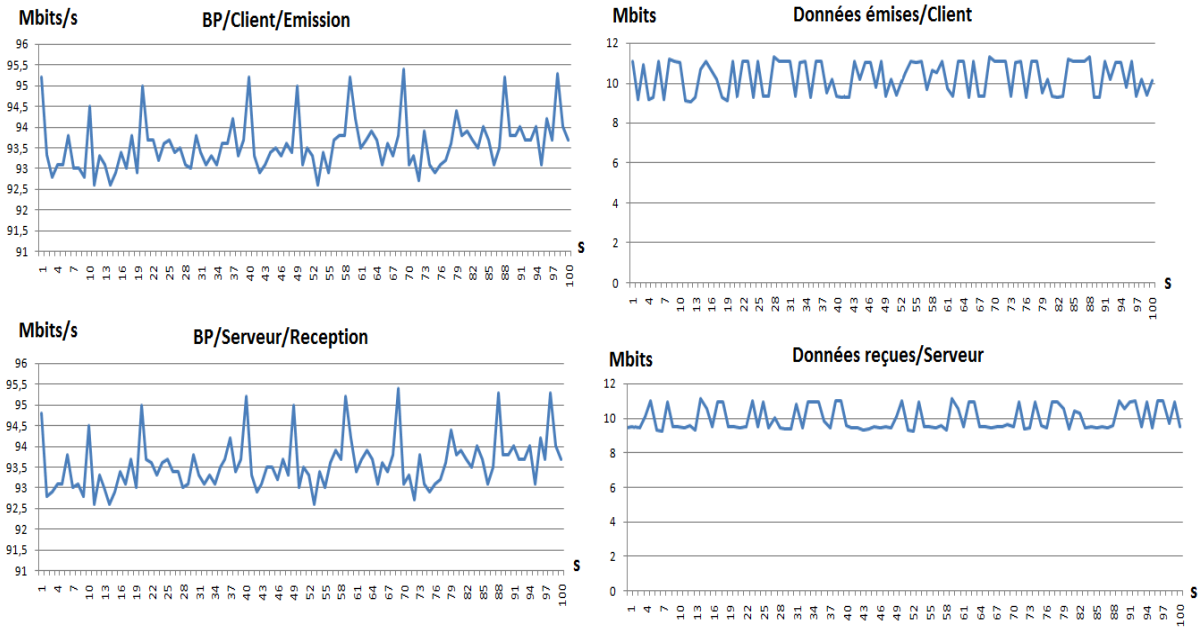
  - **Extrémités :** Les 2 extrémités au sein du département d'Arabe campus Hasnaoua.

  - **Type :** Paire torsadée cat 6 e.

- **Résultats du test :**

  ✓ **Données totales émise :** 1133 Mbits.
  ✓ **Données totales reçue :** 1133Mbits.
  ✓ **Débit moyen d'émission :** 93.7 Mbits/s.
  ✓ **Débit moyen de réception :** 93.7Mbits/s.

Graphes :



➢ Interprétation :

- ✓ Les courbes des débits d'émission et de réception sont quasi égales, et celles des données transmises et reçues le sont également.
- ✓ La quantité de données totales émise est égale à celle reçue.
- ✓ Le débit moyen d'émission est égal à celui de réception.

➔D'après cela, on en conclu que cette liaison est bonne.

III.6- Conclusion :

Dans ce chapitre, on a pu déterminer la qualité de trois liaisons physiques, deux liaisons fibres optiques monomodes et une liaison paire torsadé, et cela en utilisant le logiciel **IPerf** et son interface graphique java **JPerf**, qui se résume concrètement à faire une comparaison entre la quantité de données envoyées depuis la machine configurée en mode client et celle reçu par la machine configuré en mode serveur et entre le débit d'émission et de réception de cette quantité de donné, toute les secondes et cela pendant la durée totale de chaque test qui est de 100 secondes.

Conclusion générale et perspectives

Dans ce projet, on a pu déterminer la qualité de trois liaisons physiques, deux liaisons fibres optiques monomodes et une liaison paire torsadé, et cela en utilisant le logiciel **IPerf** et son interface graphique java **JPerf**, et on se basant sur l'architecture client/serveur et le protocole TCP, qui se résume concrètement à faire une comparaison entre la quantité de données envoyées depuis la machine configurée en mode client et celle reçu par la machine configuré en mode serveur et entre le débit d'émission et de réception de cette quantité de donné, toute les secondes et cela pendant la durée totale de chaque test qui est de 100 secondes.

Au cours de ce travail qui a commencé par une étude bibliographique, nous avons découvert un champ de recherche très intéressant qui touche presque tous les aspects des réseaux informatiques, et notamment celui de la transmission dans ses derniers. Cela nous a permis de nous initier à la recherche, et nous espérons avoir apporté une contribution, aussi petite qu'elle soit, à ce domaine qui est en pleine évolution.

Comme perspectives, nous pouvons continuer à amélioré ce travail, et cela en apportant des modifications au code source de l'interface graphique JPerf, celle-ci étant un logiciel libre (open source), afin de l'adapter mieux aux besoins des tests de liaisons physiques, on y ajoutant de nouvelles fonctionnalités ou en améliorant celles déjà existantes, entre autres, celle permettant l'affichage des graphes des résultats obtenues en temps réel et celle permettant le stockage des résultats de chaque tests, ce qui permettra une meilleur appréciation de ses derniers, et ainsi en faire un outil logiciel dédié à cet effet, qui pourra peut être par la suite concurrencée les solutions matérielles déjà existantes. Nous pourrons envisagez tout cela dans nos futures travaux de recherche qu'ils soient d'ordre individuels, professionnels ou académiques.

Résumé :

Un ensemble de terminaux informatiques reliés entre eux afin d'échanger des donnés, communiquer, partager des ressources et des applications, forment un réseau informatique

Dans un réseau filaire, ses échanges et partages s'effectuent avec des débits plus au moins optimaux et des pertes de transmission plus au moins importantes selon plusieurs critères, parmi lesquels figure la qualité des liaisons physiques reliant ses différents équipements.

Vu l'importance de cette qualité et son impact sur le réseau, différents moyens matériels et logiciels ont été mis au point afin de la mesurer.

Matériels allant du testeur de câbles le plus rudimentaire servant juste à tester la continuité d'une liaison jusqu'aux testeurs les plus sophistiqués permettant une mesure en temps réel de cette dernière, en prenant en compte plusieurs paramètres, tel que : la continuité, le débit, les pertes de transmission,… etc.

Cependant cette solution, est relativement onéreuse, ce qui a motivé le présent travail, qui est de proposer une solution logiciel et qui ne coûte pratiquement pas chère dans le but d'effectuer cette mesure, celle-ci étant l'utilisation du logiciel **iperf-3.1.3,** qui est un outil open-source permettant la mesure des performances d'un réseau informatique.

Mots clés : Types de réseaux informatiques, les architectures des réseaux LAN, les topologies des réseaux LAN, le modèle de référence OSI, le modèle TCP/IP, les modes de transmission, les équipements d'interconnexion réseaux, les techniques de commutation , les réseaux IP, les adresses IPv4, notation CIDR, le masque réseau, délivrance des adresses, le protocole NAT, le DHCP, le DNS, le logiciel IPerf3, Interface graphique jperf .