RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ IBN-KHALDOUN DE TIARET

FACULTÉ DES SCIENCES APPLIQUEES

DÉPARTEMENT DE GENIE ELECTRIQUE

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du diplôme de Master

Domaine : Sciences et Technologie

Filière : Génie Electrique

Spécialité : Electronique des Systèmes Embarqués

THÈME

Migration IPv4 vers IPv6

Préparé par : Mr BENZIANE Mohamed Djamel

Devant le Jury :

Nom et prénoms	Grade	Qualité
Mr GOISMI Mohamed	MAA	Président
Mr MAASKRI Mustapha	MAA	Examinateur
Mr BENABID Houari	MAA	Encadreur

PROMOTION 2019 /2020

Dédicace

Je dédie ce modeste travail :

À ceux que personne ne peut compenser les sacrifices qu'ils ont consentis pour notre éducation et notre bien-être :

Mes très chers parents.

Que Dieu les protèges

À mes chers frères et sœurs.

A toutes la famille.

À Tous ceux que j'aime et ceux qui m'aime

Djamel

Remerciements

Je tiens à remercier tout d'abord DIEU le tout puissant qui m'a donné, durant toutes ces années, la santé, le courage pour arriver à ce jour et de préparer un deuxième diplôme de Master.

Aux termes de ce travail, je tiens à exprimer mes sentiments envers tous ceux et toutes celles qui ont contribué de loin ou de près dans ce travail;

Je tiens à exprimer ma profonde gratitude à mon Encadreur Monsieur BENABID Houari, que je les remercie considérablement de m'avoir fait confiance et bien accepté de m'encadrer, je tians à remercier toutes personnes qui m'aidées de loin ou de près: prof. DAHMANI Youcef, Prof. MOSTEFAOUI Kada, Prof. BEKKAR Mohamed.

Djamel

Sommaire

Chapitre II: Les différents types de services réseaux

Chapitre III: L'Adressage et Le Routage

Chapitre IV: Simulation d'immigration IPv4 vers IPv6

SIGLES ET ABREVIATIONS

PAN : Personal Area Network

LAN : Local Area Network

MAN: Métropolitain Area Network

WAN : Wide Area Network

GSM : Global System for Mobile Communication

PDA: Personal Digital Assistant

GPRS: General Packet Radio Service

UMTS: Universal Mobile Telecommunication System

Wimax: Worldwide Interoperability for Microwave Accessstandard

MAU : Multistation Access Unit

FDDI: Fiber Distributed Data Interface

OSI: Open System Interconnection

TCP/IP : Transfert Control Protocol/ Internet Protocol

WIFI : Wireless Fidelity

IP: Internet Protocol

IRC : Internet Relay Chat

HTTP : Hypertext Transfer Protocol

FTP: File Transfert Protocol

Telnet : télécommunication network

SMTP : Simple Mail Transfer Protocol

POP : Post Office Protocol

IMAP : Internet Mail Access Protocol

HTML : Hyper Text Markup Language

URL : Uniform Ressource Locator

DHCP : Dynamic Host Configuration Protocol

DNS : Domain Name System

TLD : Top Level Demain

WWW: World Wide Web

FQDN : Fully Qualified Domain Name

ICANN: L'Internet Corporation for Assigned Names and Numbers

RIPE: Réseaux IP Européens

AFNIC: Association française pour le nommage Internet en coopération

BAL : Boite aux lettres

ODBC : Open Data Base Connectivity

RTC : Réseau Téléphonique Commuté

ADSL: *Asymmetric Digital Subscriber Line*

RNIS : *Réseau numérique à intégration de services*

MTA : Message Transfer Agent

IMAP : *Interactive Mail Access Protocol*

MIME : *Multipurpose Internet Mail Extension*

netID : Network Identity

hostID : host Identity

CIDR : *Classless Interdomain Routing*

IPv4 : Internet Protocol version 4

IPv6 : Internet Protocol version 6

RIP : Routing Information Protocol

SPF : Shortest Path First

SPA: Shortest Path Algorithm

AS : Autonomous System

IGP: Interior Gateway Protocols

EGP: Exterior Gareway Protocol

OSPF : Open Shortest Path First

BGP : Border Gateway Protocol

FAI: Fournisseur d'accès d'Internet

EIGRP : Enhanced Interior Gateway Routing Protocol

IGRP : Interior Gateway Routing Protocol

NAT : Network address Translation

ISATAP : Intra-Site Automatic Tunnel Addressing Protocol

MPLS : Multi Protocole Label Switching

6PE : IPv6 on Provider Edge routers

NAPT-PT : Network Address Port Translation-Protocol Translation

Dual Stack ALG : Dual Stack Application Level Gateway

TRT : Transport Relay Translator

NDP : Neighbor Discovery Protocol

iBGP : internal BGP

Liste des figures

Liste des Tableaux

Introduction générale

Vue l'augmentation du nombre de machines le protocole IPv4 sera victime de son succès et ne permettra plus de répondre à la demande de connexion de milliards de machines informatisées et d'autres équipements dont disposeront les internautes de demain.

En raison de la limitation des adresses IPv4, une autre technologie a surgi: le protocole Internet version 6 (IPv6). La version 6 d'IP a été introduite en 1998 par l'IETF (Internet Engineering Task Force) pour non seulement conserver les principes qui ont fait le succès d'IP mais aussi pour corriger les défauts de la version courante et anticiper les besoins futurs des utilisateurs.

L'IPv6 a été conçu pour un espace d'adressage suffisant pour la demande actuelle et future pour la croissance accrue d'Internet. IPv6 augmente la taille du schéma d'adresse IP d'IPv4-32 bits à 128 bits. L'adresse IPv6 coopère avec l'adresse IPv4; cela signifie que les réseaux IPv6 sont capables de fusionner avec les réseaux IPv4 pour les futurs réseaux. Mais, de toute façon, IPv4 ne prend pas en charge les nouveaux critères de réseau à venir. Le réseau IPv4 actuel est énorme et complexe, donc IPv4 ne pouvait pas être remplacé soudainement par IPv6. La migration d'une technologie à une autre technologie est absolument difficile, car IPv4 et IPv6 ne sont pas le même assemblage pour la communication.

Le protocole IPv4 n'est pas compatible avec son successeur IPv6. Un nœud implémentant uniquement la version 4 du protocole IP ne peut pas échanger avec un nœud utilisant seulement la version 6. Et pour faire communiquer les deux versions, il faut suivre quelques méthodes de migration.

Les trois principaux mécanismes de transition sont largement connus sous le nom de Dual Stack, Tunneling et Network address translation.

Afin d'atteindre ces objectifs notre étude s'articulera autour de quatre chapitres essentiels :

- Généralités sur les réseaux (chapitre I)
- Les différents types de services réseaux (chapitre II)
- L'Adressage et Le Routage (chapitre III)
- Une simulation de migration IPv4 vers IPv6 (chapitre IV).

Dans notre travail, nous nous sommes intéressés à la migration IPv4 vers IPv6 avec la méthode du tunneling, nous allons utiliser le logiciel Packet tracer pour la simulation.

Chapitre I

Généralité sur les réseaux

I.1 Introduction

Le terme générique « réseau » définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres.

La mise en réseau consiste à relier plusieurs ordinateurs en vue de partager des ressources logicielles, des ressources matérielles ou des données. Selon le nombre de systèmes interconnectés et les partages demandés, les techniques de raccordement seront différentes et la transmission et la réception des données sont avec des protocoles bien spécifiés

I.2 Définition

Un réseau informatique est un ensemble d'ordinateurs reliés entre eux grâce à des lignes de communication et échangeant des informations sous forme de données numériques.

Un réseau peut aussi contenir des équipements spécialisés, comme des hubs, des routeurs, et bien d'autres équipements.

I.3 Intérêt des réseaux informatiques

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct, etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau)
- Le jeu vidéo multijoueurs

Les réseaux permettent aussi de standardiser les applications, on parle généralement de groupware[1] pour qualifier les outils permettant à plusieurs personnes de travailler en réseau. Par exemple la messagerie électronique et les agendas de groupe permettent de communiquer plus efficacement et plus rapidement. Voici un aperçu des avantages qu'offrent de tels systèmes :

- Diminution des coûts grâce aux partages des données et des périphériques,
- Standardisation des applications,
- Accès aux données en temps utile,
- Communication et organisation plus efficace.

I.4 Types des réseaux informatiques (la typologie)

I.4.1 Le réseau personnel (PAN) Personal Area Network

Est un réseau d'étendue limitée à quelques mètres pour l'interconnexion des équipements personnels (GSM[2], PDA[3], PC et PC portable) d'un seul utilisateur.

[1] Un **groupware** est un logiciel de groupe qui permet à un groupe de personnes de partager des documents à distance.
[2] Global System for Mobile Communication.
[3] Personal Digital Assistant

I.4.2 Le réseau local (LAN)

LAN (Local Area Network) il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

En élargissant le contexte de la définition aux services qu'apporte le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement d'égal à égal" (en anglais peer to peer), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire

- dans un environnement "client/serveur", dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

I.4.3 Le réseau métropolitain (MAN)

Les MAN (Métropolitain Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.
Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique). **[9]**

I.4.4 Le réseau étendu (WAN)

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. **[9]**

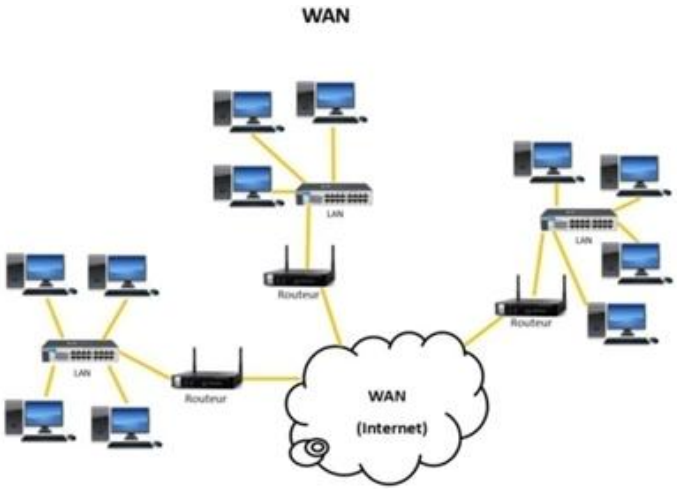


Figure 1.1 réseau WAN

I.4.5 Réseaux sans fil (Wireless networks)

Un réseau sans fil (en anglais wireless network) est un réseau dans lequel au moins deux équipements peuvent communiquer sans liaison filaire.

- **Un réseau personnel sans fil (WPAN : Wireless Personal Area Network)** concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...). Il existe plusieurs technologies utilisées pour les WPAN :

- La principale technologie WPAN est la technologie Bluetooth

- Home RF (pour Home Radio Frequency)

- les liaisons infrarouges

- **Un réseau local sans fil (WLAN : Wireless Local Area Network)** est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il existe plusieurs technologies concurrentes :

- Le Wifi soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance)

- hiperLAN2 (HIgh Performance Radio LAN 2.0),

- **Un réseaux métropolitains sans fils (WMAN : Wireless Metropolitan Area Network)** est un réseau métropolitain sans fils (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR), ce qui destine principalement cette technologie aux opérateurs de télécommunication.
- **Un réseau étendu sans fil (WWAN : Wireless Wide Area Network)** est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes :
  - GSM (Global System for Mobile Communication ou en français Groupe Spécial Mobile)
  - GPRS(General Packet Radio Service)
  - UMTS (Universal Mobile Telecommunication System).
  - Wimax (Worldwide Interoperability for Microwave Accessstandard).

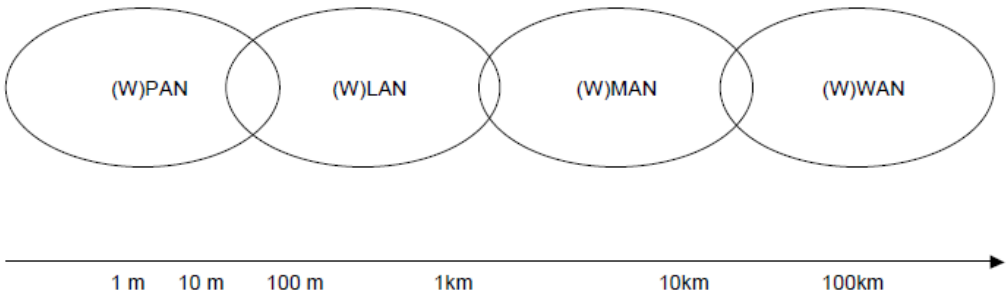


Figure 1.2 : les différents types des réseaux

I.5 Topologie physique des réseaux

Le terme topologie physique désigne l'organisation ou la disposition physique des nœuds du réseau. Un nœud de réseau représente un ordinateur, une imprimante, un équipement d'interconnexion.
La topologie physique détermine non seulement le type de câble utilisé, mais également la façon dont le câblage doit être effectué.
La configuration spatiale du réseau est appelé topologie physique. On distingue généralement les topologies suivantes : **[4]**

- Topologie en bus
- Topologie en étoile
- Topologie en anneau
- Topologie en arbre
- Topologie maillée

I.5.1 La topologie en bus (le support linéaire)

Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

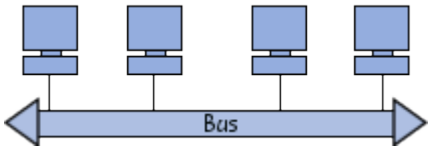


Figure 1.3 : Topologie en bus

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté. **[4]**

I.5.2 La topologie en étoile

Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un système matériel central appelé **concentrateur** (en anglais *hub*, littéralement *moyen de roue*). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions. **[4]**

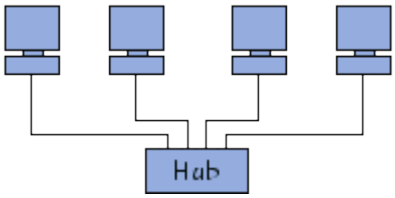


Figure 1.4 : Topologie en étoile

I.5.3 La topologie en anneau

Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

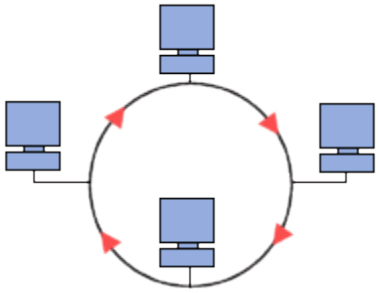


Figure 1.5 : Topologie en anneau

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (appelé *MAU*, *Multistation Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un « temps de parole ».

Les deux principales topologies logiques utilisant cette topologie physique sont Token ring (anneau à jeton) et FDDI. **[4]**

I.5.4 La topologie en arbre

Aussi connu sous le nom de *topologie hiérarchique*, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence. **[4]**

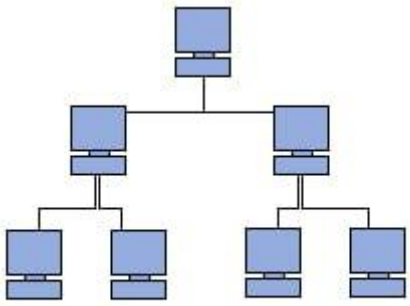


Figure 1.6 : Topologie en arbre

I.5.5 La topologie en maillage

Une topologie maillée ou en maillage, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1,N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple: Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties. **[4]**

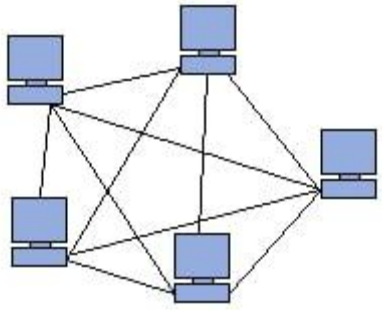


Figure 1.7 : Topologie en maillage

I.6 Architectures des réseaux informatiques (rôle)

I.6.1 L'architecture client/serveur

Les réseaux Client/Serveur comportent en général plus de dix postes. La plupart des machines sont des « postes clients », c'est à dire des ordinateurs ou des terminaux connectés (tablettes, smartphones) utilisés par les utilisateurs. Ces machines vont communiquer avec une ou plusieurs machines dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveurs.

Les « postes serveurs » sont en général de puissants ordinateurs fonctionnant en continu. Il existe plusieurs types de serveurs (serveur de fichiers et d'impression, serveur d'application, serveur de messagerie,…).

Dans une organisation Clients/Serveurs, les clients n'ont accès qu'au(x) serveur(s).

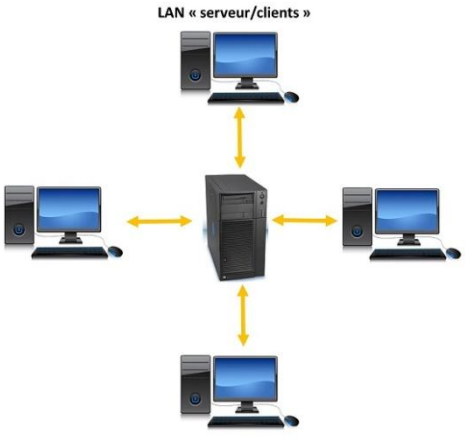


Figure 1.8 : réseau Client/Serveur

I.6.1.1 L'architecture à deux (02) niveaux

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

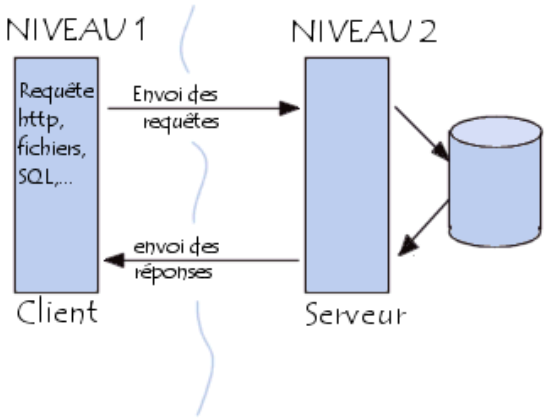


Figure 1.9 : réseau Client/Serveur à deux (02) niveaux

I.6.1.2 L'architecture client-serveur à trois (3) niveaux

Dans l'architecture à 3 niveaux (appelée architecture 3-tier), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :

Un client, c'est-à-dire l'ordinateur demandeur de ressources, équipée d'une interface utilisateur (généralement un navigateur web) chargée de la présentation ;

Le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur

Le serveur de données, fournissant au serveur d'application les données dont il a besoin.

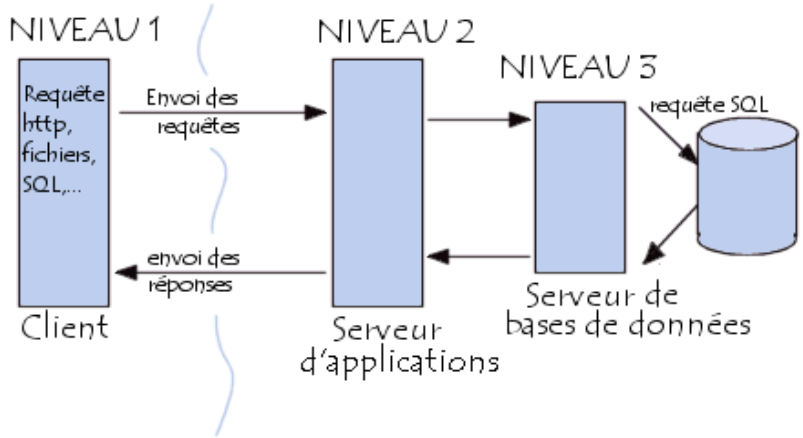


Figure 1.10 : réseau Client/Serveur à trois (03) niveaux

Etant donné l'emploi massif du terme d'architecture à 3 niveaux, celui-ci peut parfois désigner aussi les architectures suivantes :

Partage d'application entre client, serveur intermédiaire, et serveur d'entreprise ;

Partage d'application entre client, serveur d'application, et serveur de base de données d'entreprise.

I.6.2 L'architecture poste à poste ou pair-à-pair (peer-to-peer)

Les réseaux « postes à postes » également appelés réseaux « Peer to Peer » en anglais, ne comportent en général que peu de postes, moins d'une dizaine de postes. Chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central et aucune hiérarchie entre les postes et les utilisateurs.

Dans un réseau « Peer to Peer » chaque poste est à la fois client et serveur.

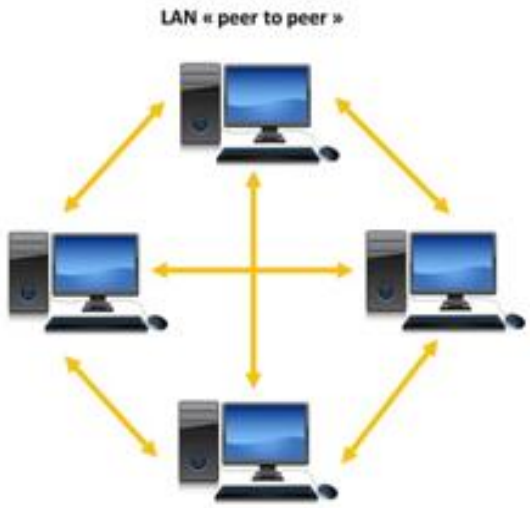


Figure 1.11 réseau peer to peer

I.7 Le modèle de référence OSI ou Open Systems Interconnexion:

Il est créé en 1978 par l'organisation internationale de normalisation (ISO), a pour objectif de constituer un modèle de référence d'un réseau informatique et ceci dans le but de permettre la connexion entre les architectures propriétaires hétérogènes qui existaient. Ce modèle est constitué de sept couches dont chacune correspond à une fonctionnalité particulière d'un réseau. Les quatre premières couches dites basses, assurent l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les trois autres couches, dites hautes, sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. **[14]**

Les 7 couches du modèle OSI sont les suivantes :

I.7.1 Couche 1 : La couche physique

Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédure les nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entres deux entités de la couche liaisons de données. **[8]**

I.7.2 Couche 2 : La Couche liaison de donnée

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de donnes entre les entités du réseau.
Cette couche détecte et corrige, quand cela est possible, les erreurs de la coche physique et signale à la couche réseau les erreurs irrécupérables. **[8]**

I.7.3 Couche 3 : La couche réseaux

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 le correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport. **[8]**

I.7.4 Couche 4 : La couche transport

Cette douche définit un transfert de données entre les entités en les déchargeant des détails d'exécution (contrôle entre l'OSI et le support de transmission).
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. **[8]**

I.7.5 Couche 5 : La couche session

Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données.
Il s'agit de la gestion d'accès, de sécurité et d'identification des services. **[8]**

I.7.6 Couche 6 : La couche présentation

Cette couche assure la transparence du format des données à la couche application. **[8]**

I.7.7 Couche 7 : La couche application

Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tout les services directement utilisables par l'application (transfert e données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications). **[8]**

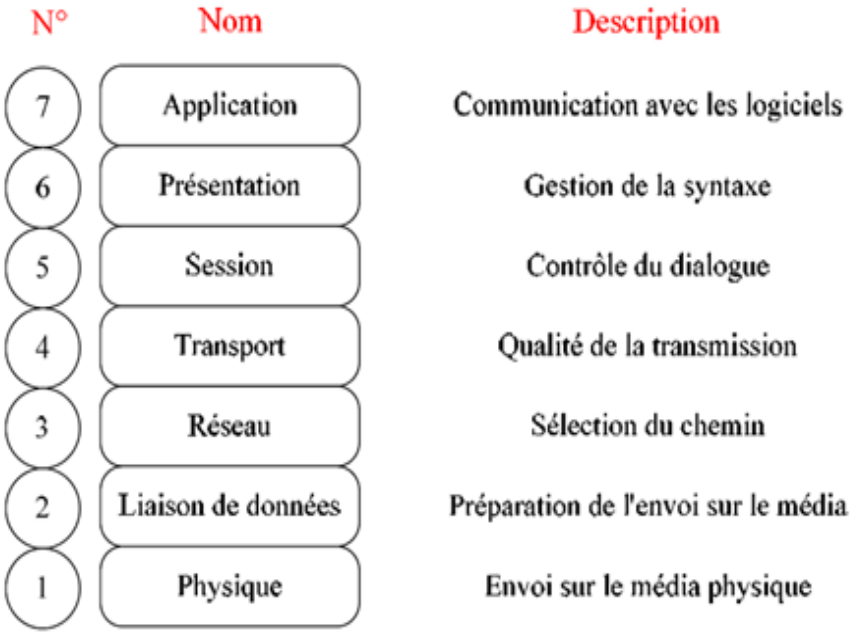


Figure 1.12 les 7 couches du model OSI

I.8 Le modèle TCP/IP

La forme actuelle de TCP/IP résulte du rôle historique que ce système de protocoles a joué dans le parachèvement de ce qui allait devenir Internet. À l'instar des nombreux développements de ces dernières années, Internet est issu des recherches lancées par le DOD (Department Of Defense), département de la défense américaine.

À la fin des années 60, les officiels du DOD se rendirent compte que les militaires du département de la défense possédaient une grande quantité de matériel informatique très divers, mais ces machines travaillaient pour la plupart de manière isolée ou encore en réseaux de taille très modeste avec des protocoles incompatibles entre eux, ceci rendant une interconnexion impossible.

Les autorités militaires se sont alors demandées s'il était possible, pour ces machines aux profils très différents, de traiter des informations mises en commun. Habitués aux problèmes de sécurité, les responsables de la défense ont immédiatement réalisés qu'un réseau de grande ampleur deviendrait une cible idéale en cas de conflit. La caractéristique principale de ce réseau, s'il devait exister, était d'être non centralisée.

Ses fonctions essentielles ne devaient en aucun cas se trouver en un seul point, ce qui le rendrait trop vulnérable. C'est alors que fut mis en place le projet ARPANet (Advanced Research Projects Agency Network du DOD), qui allait devenir par la suite le système d'interconnexion de réseau qui régit ce que l'on appelle aujourd'hui Internet : TCP/IP. **[13]**

TCP/IP est un modèle comprenant 4 couches :

1.8.1 La couche hôte réseau

Cette couche est assez « étrange ». En effet, elle semble « regrouper » les couches physiques et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau. **[6]**

1.8.2 La couche internet

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures. **[6]**

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI. **[6]**

1.8.3 La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. **[6]**

1.8.4 La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP. **[6]**

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par

exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs. **[6]**

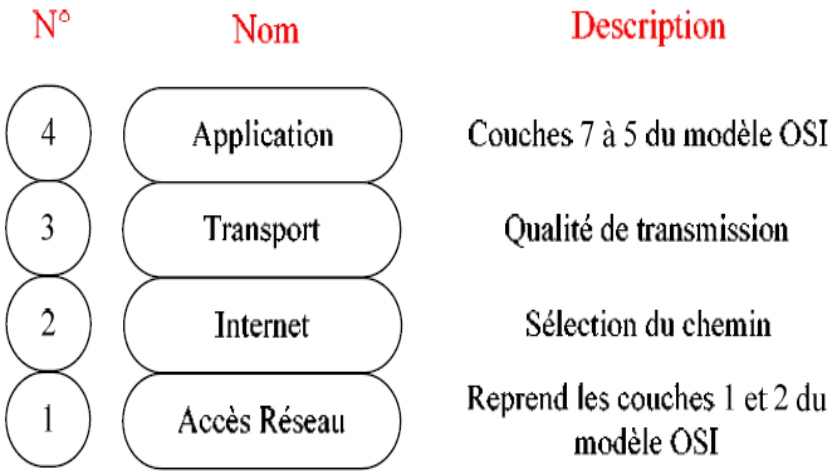


Figure 1.13 les 4 couches du model TCP/IP

I.9 L'Internet

Internet est un ensemble de réseaux interconnectés utilisant une suite protocolaire appelée TCP/IP (Transmission Control Protocol/Internet Protocol) pour échanger des informations à travers le monde. En termes simples : Internet est un immense réseau d'ordinateurs qui peuvent communiquer entre eux en utilisant TCP/IP.

1.9.1 Les services offerts par l'internet

Sur le plan pratique, Internet est un outil capable de nous rendre un certain nombre de services. Ces services sont réalisables à travers les différents protocoles de l'Internet (Les protocoles de la couche application TCP/IP).

- **IRC** (Internet Relay Chat) : pour discuter en direct (chat) avec des gens du monde entier. Le dialogue s'effectue par échange de texte, mais il est possible de dialoguer aussi en temps réel avec la voix et la vidéo (vidéoconférence).
- **http** (ou *World Wide Web* ou *www* ou tout simplement le *web*) pour accéder à des pages web. Le web est l'application Internet la plus populaire. Grace à un navigateur web (browser), un utilisateur (internaute) peut lire des pages web stockées sur un ordinateur serveur situé n'importe où dans le monde.
- **ftp** (File Transfert Protocol) pour le transfert électronique de fichiers entre des machines distantes. Avec FTP on peut charger des fichiers sur des ordinateurs serveurs connectés à Internet, ou télécharger des fichiers sur le poste client.
- **telnet** (Connexion à un ordinateur distant) : tout utilisateur d'Internet peut travailler à distance sur une machine, sur laquelle il dispose d'un compte utilisateur et dont il a accès. Il peut utiliser Telnet ou d'autres programmes de contrôle à distance (*rlogin,rsh*…)
- **SMTP , POP** et **IMAP**: pour la messagerie électronique (ou mail)
  - **SMTP** (Simple Mail Transfer Protocol) pour l'envoi du courrier.

- **POP** (Post Office Protocol) permet à l'utilisateur de récupérer les messages qu'il a reçu sur le serveur de messagerie hébergeant sa boite aux lettres en les déplaçant sur son ordinateur local.
- **IMPAP** (Internet Mail Access Protocol) un autre protocole qui permet aussi de consulter notre boite aux lettres sur le serveur de messagerie.
- La boite aux lettres est aussi un moyen de stockage de courrier et les pièces jointes (les fichiers joints aux différents mails).

1.9.2 Avantages de l'internet

- Accès à l'information d'une manière continue et à partir de n'importe quel point du monde et ce pour un coût d'accès limité.
- Communication sous toutes formes (d'une personne à une autre, d'une personne à un groupe, d'un groupe à un autre, d'un groupe à une personne) à partir d'un même outil.
- Échanger tous types de données numérisées (documents, dessins, photos, son, vidéo, logiciels, etc.).
- Permettre le commerce électronique grâce à des échanges sécurisés.
- Permettre l'enseignement/apprentissage à distance en synchrone ou en asynchrone.

1.9.3 Fonctionnement de l'internet

Internet est un réseau basé sur le modèle client / serveur :

- L'ordinateur client, utilise un logiciel spécifique (**le navigateur** : par exemple Google Chrome, Mozilla Firefox ou Microsoft Internet explorer) pour aller chercher l'information numérique auprès d'un autre ordinateur distant : **le serveur**.
- Le serveur, ou hôte, stocke les données numériques sur des disques durs et les envoie, à la demande, sur l'ordinateur client.

1.9.3.1 Consultation d'une page Web

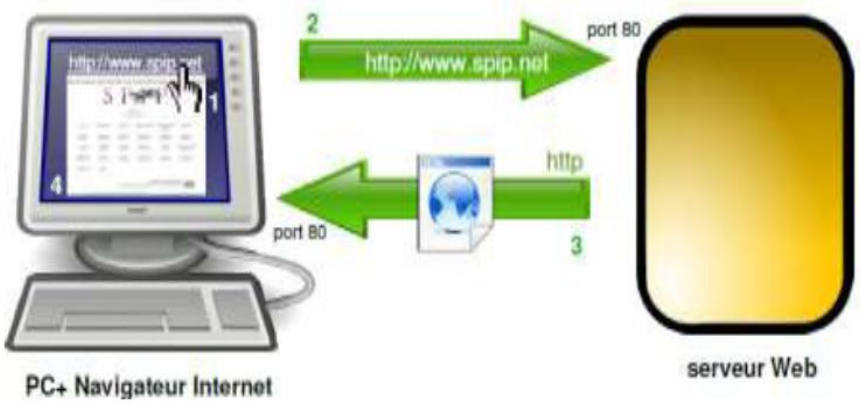


Figure 1.14 *Consultation d'une page Web*

1. Action de l'utilisateur dans le navigateur (clic lien)
2. Requête HTTP du navigateur avec adresse
3. Réponse HTTP du serveur avec document HTML
4. Interprétation et affichage du navigateur

I.10 Les protocoles de communication (la topologie logique)

I.10.1 Le protocole TCP/IP

Le sigle TCP/IP est formé sur les noms des deux protocoles majeurs utilisés sur Internet: le protocole TCP pour "Transmission Control Protocol" et le protocole IP pour "Internet Protocol".
Ce sigle désigne une suite de protocoles, c'est-à-dire de règles de communication que les ordinateurs doivent respecter pour communiquer entre eux via Internet.
IP: signifie Internet Protocol : littéralement "le protocole d'Internet". C'est le principal protocole utilisé sur Internet.
Le protocole IP permet aux ordinateurs reliés à ces réseaux de dialoguer entre eux.
L'adresse IP est une adresse unique attribuée à chaque ordinateur sur Internet (c'est-à-dire qu'il n'existe pas sur Internet deux ordinateurs ayant la même adresse IP).

I.10.2 Le protocole IP (Internet Protocol)

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 (les paquets de données), 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.

Les données circulent sur internet sous forme de **datagrammes** (on parle aussi de paquets). Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP destination).

Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit.

Les choses sont toutefois différentes selon qu'il s'agit d'un datagramme IPv4 ou IPv6. **[5]**

I.10.3 Le protocole UDP

User Datagram Protocol – Protocole de datagramme utilisateur. Paquet dont le destinataire n'accuse pas la réception; il est purement et simplement supprimé si le destinataire n'est pas joint. Ce protocole est de type non connecté, c'est-à-dire qu'expéditeur et destinataire ne sont pas reliés ensemble. Cela signifie qu'un problème de transmission n'est pas détecté au niveau du protocole. Cette détection et la solution sont à la charge de l'application exploitant le protocole. Ainsi, TFTP (Trivial File Transfer Protocol), NFS (Network File System sous UNIX) ou SNMP sont des exemples de telles applications.

I.10.4 Le protocole BOOTP

Bootstrap Protocol (BOOTP) est un protocole réseau d'amorçage, qui permet à une machine cliente sans disque dur de découvrir sa propre adresse IP, l'adresse d'un hôte serveur, et le nom d'un fichier à charger en mémoire pour exécution. On peut représenter l'amorçage comme une opération se produisant en deux phases :

- Détermination d'adresses et sélection du fichier de démarrage, c'est ici qu'intervient BOOTP.

- Transfert du fichier de démarrage, le transfert utilisera typiquement le protocole TFTP, SFTP ou encore FTP. **[7]**

I.10.5 Le protocole DHCP

DHCP (Dynamic Host Configuration Protocol) est un protocole de configuration dynamique d'hôte qui permet d'allouer à la demande des adresses IP aux machines se connectant au réseau.

I.10.6 Le protocole http

Le protocole HTTP (HyperText Transfer Protocol) est le protocole le plus utilisé sur Internet depuis 1990.

Le but du protocole HTTP est de permettre un transfert de fichiers (essentiellement au format HTML) localisés grâce à une chaîne de caractères appelée URL entre un navigateur (le client) et un serveur Web.

Lorsque le navigateur du client veut accéder à une ressource vers un serveur, l'adresse IP correspondant au nom indiqué dans l'URL est récupérée grâce au protocole DNS. Une connexion TCP vers le serveur est ensuite établie sur le port 80 par défaut. Pour utiliser un port non standard, il faut le préciser dans l'URL (ex. : http://www.babao- rum.arn1or.fr:l224). Une fois la connexion TCP établie, le navigateur envoie sa demande de ressource par l'intermédiaire du protocole HTTP. La requête contient la méthode à utiliser pour récupérer la ressource (GET par exemple), l'URL de la ressource demandée et la version du protocole HTTP invoqué (figure 1.15). Le protocole HTTP communique ses informations au format texte afin de ne pas être gêné par les différences d'implémentation des jeux de caractères d'une plate-forme à l'autre. **[3]**

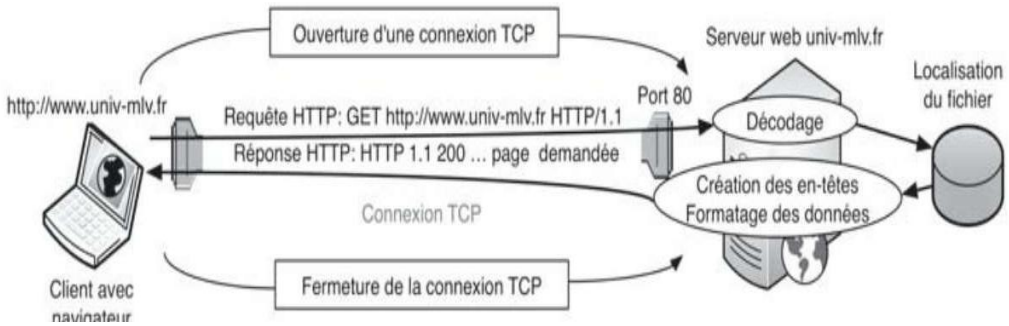


Figure 1.15 fonctionnement du HTTP

I.11 Gestion de la communication

La circulation des informations sur le réseau, le type de transmission et le partage du média sont des aspects importants de l'architecture.

I.11.1 Sens de transmission

Différentes directions du flot de données sont possibles, particulièrement dépendant du support de transmission et des techniques utilisées.

I.11.1.1 Le mode simplex :

Ce mode n'exploite qu'un seul sens de transfert de l'information. Il correspond généralement à l'usage d'un seul émetteur pour n récepteur. Ces derniers sont peu coûteux.

L'émission de programmes radio est un exemple d'utilisation de communication en mode simplex.

Une fibre optique n'offre qu'un sens de connexion, ne permettant que le mode simplex. Ainsi, au moins deux fibres sont utilisées, en multimode, pour permettre une communication bidirectionnelle.

I.11.1.2 Le mode half-duplex :

Ici, les deux sens de communication sont alternés, chaque interface étant successivement émettrice et réceptrice.

Les radios amateurs (CB- Citizen Band) sont basées sur ce principe.

Le câble coaxial représente un bon exemple de support half-duplex.

I.11.1.3 Le mode full-duplex

Dans ce mode, les deux extrémités peuvent transmettre simultanément. C'est la solution la plus couteuse, mais également la plus efficaces.

Les communications téléphoniques sont de type full-duplex.

Le support filaire paire torsadée est un média de transmission full-duplex. Une carte réseau connectée à l'équipement adéquat peut utiliser simultanément une paire de fils pour l'émission et une autre pour la réception.

1.11.2 Les types de transmission

Les données transmises doivent être synchronisées par le récepteur afin d'être lues.

Pour cela, plusieurs types de transmission peuvent être utilisés. Les principaux sont :

I.11.2.1 Le type synchrone

Synchrone, utilisant une horloge pour transmettre à flots continus ;

I.11.2.2 Le type asynchrone

Asynchrone, permettant de gérer un échange imprévisible ou occasionnel, débutant par un bit de démarrage (start) et terminant par un bit de stop.

Dans les réseaux locaux, les deux premiers types sont particulièrement utilisés. Le tableau suivant les caractérise plus précisément.

	Synchrone	**Asynchrone**
Avantage	Plus efficace. Vitesse rapide Meilleure détection des erreurs	Peu compliqué. Matériel peu cher.
Inconvénients	Les circuits des émetteurs et des récepteurs sont plus complexe et plus chers.	La mise en trame de chaque caractère et la détection des erreurs correspond à 20 à 30 % du débit utile. Le bit de parité détecte une seule erreur. Transfert lent.

Tableau 1.1 les types de transmission

I.13 Conclusion

Dans ce chapitre, nous avons fait une présentation générale sur les réseaux informatique, nous avons décrit les différents types et les topologies des réseaux informatiques, nous avons explicité les deux grandes modèles de référence OSI et TCP/IP et le réseau mondial Internet. L'objectif était double, d'une part pour rappeler des notions de base sur les réseaux et d'autre part pour déterminer la portée des futures notions qui seront présentées dans les chapitres suivants.

Chapitre II

Les différents types de services réseaux

II.1-Introduction

Nous connaissons, utilisons, « surfons » régulièrement sur Internet, nous savons comment envoyer des fichiers, Nous maîtrisons plus ou moins le navigateur, connaissons les adresses de nos sites préférés. Nous savons chercher, trouver le « meilleur » abonnement au prestataire de service. Ce qui est moins connu, moins visible, ce sont les métiers et techniques qui permettent à nos messages d'arriver à leur destinataire, et nous permettent d'interroger et naviguer sur les serveurs web.
Cette interrogation nous amène à présenter les différents services réseaux.

II.2 Définition

Un service réseau est une application exécutée depuis la couche d'application réseau et au-dessus. Il fournit des capacités de stockage, de manipulation, de présentation, de communication ou d'autres services qui sont souvent mises en œuvre en utilisant une architecture client-serveur ou pair à pair basée sur un protocole de communication de la couche « application » du modèle OSI.

Chaque service est habituellement fourni par un composant de serveur fonctionnant sur un ou plusieurs ordinateurs (souvent un ordinateur serveur dédié offrant plusieurs services) et accessible *via* un réseau par des composants client exécutés sur d'autres périphériques. Toutefois, les composants client et serveur peuvent être exécutés sur la même machine.

Les clients et les serveurs ont souvent une interface utilisateur, et parfois d'autres matériels qui leur sont associés.

II.3 Le service WEB

II.3.1 Définition

Le service Web est le service d'Internet. C'est lui qui permet d'héberger des serveurs web, et donc de proposer des pages à lire comme OpenClassrooms ou Facebook.

II.3.2 URL et protocole HTTP

II.3.2.1 Service web et hypertexte

Il permet d'accéder à des documents au format HTML (*Hyper Text Markup Language*) stockés sur un serveur, en utilisant pour la connexion et les échanges le protocole HTTP (*Hyper Text Transfer Protocol*). Les documents sont accessibles par un URL (*Uniform Ressource Locator*) comportant le nom du serveur http contenant le document, le chemin d'accès au document et le nom de celui-ci.

Les serveurs HTTP les plus courants sont Netscape Entreprise Server, Apache HTTP Server, Microsoft Internet Information Server et NetWare Web Server de Novell.

Pour accéder aux serveurs web, les stations doivent être équipées de navigateurs Internet. On trouve Internet Explorer de Microsoft, Netscape Navigator ou Google chrome de Google.

Le protocole de communication HTTP (HyperText Transfer Protocol) utilisé entre le navigateur du client et les serveurs web est basé sur le principe des liens hypertextes. Ces liens sont repérés par des mots de couleur différente (bleu en général) ou des images qui servent de liens entre les documents. Il suffit de cliquer sur un lien pour accéder à un autre document localisé sur le même

serveur ou sur un autre, pouvant être situé n'importe où sur le réseau Internet. Ces liens hypertextes rendent la lecture dynamique et permettent de «naviguer» sur une bibliothèque à l'échelle planétaire.

Les URL (Uniform Resource Locators) sont les noms donnés aux liens hypertextes.
Un URL peut relier à un fichier sur un serveur ftp, une image, une adresse courrier, un serveur de News, un serveur telnet et bien sûr un serveur http, c'est-à-dire un serveur web. La figure 2.1 donne des exemples de fichiers accessibles par URL à partir d'une page HTML : l'image (fichier gif ou jpeg par exemple) se trouve sur un serveur accessible par le réseau Internet, alors que le fichier son (fichier wav par exemple) et le fichier texte (fichier html par exemple) sont localisés sur le serveur http du réseau de l'entreprise.
Exemple de syntaxes d'URL :
– http://www.babaorum.armor.fr donne accès à la page par défaut du serveur web babaorum.armor.fr ;

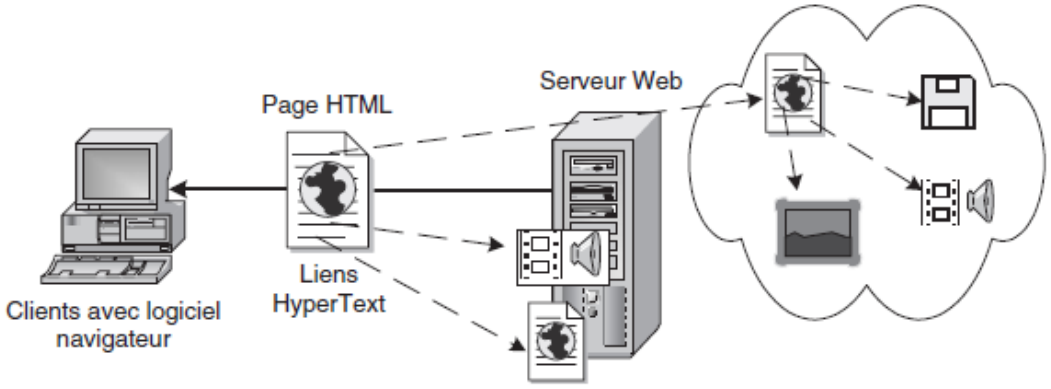


Figure 2.1 Localisation de fichiers par URL.

II.3.2.2 Dialogues du protocole HTTP

Le navigateur web du client utilise le port TCP 80 (par défaut) pour établir une connexion avec le serveur web. Un port non standard peut être utilisé. Il doit être précisé dans l'URL exemple :
http:// www.someorg.com:8080 **[2]**

II.4 Le service DHCP (Dynamic Host Configuration Protocol)

II.4.1 Définition

Un service DHCP est un service qui délivre des adresses IP aux équipements qui se connectent sur le réseau.

Nous allons nous intéresser ici à la manière dont cette adresse peut être obtenue. On distinguera deux méthodes :

- une méthode manuelle où vous choisirez vous-même l'adresse IP de votre machine ;

- une méthode dynamique où l'adresse IP de votre machine sera fournie par un serveur, le serveur DHCP. Nous verrons que ce dernier a d'autres utilités que la simple distribution d'adresses IP. **[1]**

II.4.2 Principe du DHCP

La méthode manuelle pose quelques problèmes de prime abord. En effet, vous avez vu que pour qu'une machine puisse communiquer avec ses voisines, son adresse IP devait se trouver dans le même réseau que les autres machines. Pour sortir du réseau local, il faut que notre machine connaisse l'adresse de la passerelle. Cela fait déjà quelques informations dont il faut avoir connaissance quand vous branchez votre ordinateur à un réseau local.

- Un autre problème se pose : même si l'on possède ces informations, comment s'assurer que l'adresse IP que l'on choisit n'est pas déjà utilisée par une autre machine sur le réseau?

Il serait bien d'avoir un mécanisme rapide et fiable pour adresser les machines d'un réseau. C'est là qu'entre en jeu le protocole DHCP. **[1]**

II.4.2.1 Un protocole pour distribuer des adresses IP

La première fonction d'un serveur DHCP est de fournir des adresses IP (associées à un masque, bien évidemment) aux machines en faisant la demande.

Si vous avez configuré votre carte réseau pour récupérer son adresse IP automatiquement, votre machine va chercher à contacter un serveur DHCP susceptible d'être présent sur votre réseau local. **[1]**

II-5 Le service DNS (Demain Nome System)

II.5.1 Définition

Le DNS (Domain Name System) est un service permettant d'établir une correspondance entre un nom de domaine et une adresse IP. Il s'agit donc d'un système essentiel à Internet afin de ne pas avoir à saisir des adresses IP à longueur de temps. **[1]**

II.5.2 Un arbre avec des branches

Une arborescence ordonnée

Vous utilisez tous les jours le système DNS lorsque vous naviguez sur Internet. Pour accéder OpenClassrooms.com, le système DNS se charge de convertir (on parle de résolution) le nom du site Web demandé en adresse IP.

Un nom de domaine se décompose en plusieurs parties. Prenons un exemple simple: www.google.fr

Chaque partie est séparée par un point. Nous allons les détailler de droite à gauche. On trouve tout

d'abord **l'extension**; on parle de TLD (Top Level Domain). Il existe des TLD nationaux (fr, it, de, es, etc.) et les TLD génériques (com, org, net, biz, etc).

Il existe une infinité de possibilités pour la deuxième partie. Cela correspond à tous les sites qui existent: google.fr, openclassrooms.com, ovh.net, twitter.com, etc.

Comme vous le voyez, google.fr est un sous-domaine de **fr**. Le domaine **fr** englobe tous les sous-domaines finissant par **fr**.

La troisième partie est exactement comme la deuxième. On y retrouve généralement le fameux www, ce qui nous donne des noms de domaine comme www.google.fr. **www** peut soit être un **sous-domaine** de google.fr, mais dans ce cas il pourrait y avoir encore des machines ou des sous-domaines à ce domaine, soit être directement le **nom d'une machine**.

Ici, www est le nom d'une machine dans le domaine google.fr.

On peut bien entendu ajouter autant de troisièmes parties que nécessaire, ce qui peut vous conduire à avoir un nom de domaine comme : http://www. fr.1.new.super.google.fr/.

Voici une toute petite partie de l'arborescence des noms Internet :

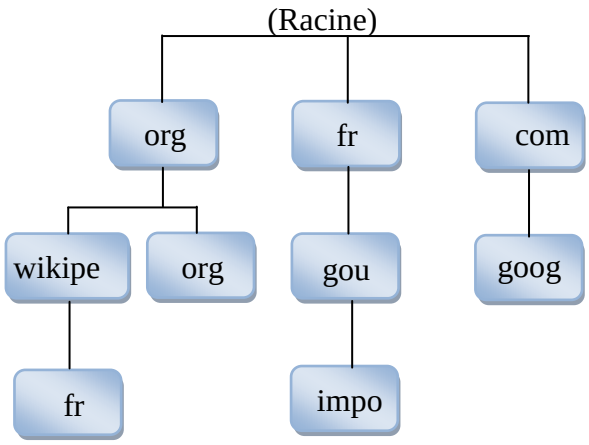


Figure 2.2 Une partie de l'arborescence des noms de domaine

Chaque « partie » est appelée label et l'ensemble des labels constitue un **FQDN** (Fully Qualified Domain Name). Ce FQDN est unique. Par convention, un FQDN se termine par un point, car au-dessus des TLD il y a la racine du DNS, tout en haut de l'arbre. Ce point disparaît lorsque vous utilisez les noms de domaines avec votre navigateur, mais vous verrez qu'il deviendra très important lorsque nous configurerons notre propre serveur DNS.

Au niveau DNS, http://www.google.fr/ n'est pas un FQDN, car il manque le point à la fin.

Tout FQDN sur Internet doit obligatoirement se finir par un point, comme :
www. Openclassrooms.com. qui est alors bien un FQDN, car on est sûr qu'il n'y a pas de domaine au-dessus.
Dans l'architecture du service DNS, chaque label est responsable du niveau directement en dessous et uniquement de celui-ci. La racine est responsable du domaine **.com**, le **.com** de google.com de http://www.google.com/, etc. Bien entendu, Google veut gérer lui- même le domaine google.com. L'organisme qui gère le domaine **.com** délègue donc la gestion de ce nom de domaine à Google.

Ainsi, chaque personne qui veut posséder un domaine sur Internet peut l'acheter, mais devra ensuite gérer un serveur DNS pour publier ses adresses.

Cependant, la plupart des entreprises qui vendent des noms de domaines (qu'on appelle des registrars) proposent de gérer elles-mêmes vos enregistrements DNS, mais c'est moins intéressant.

Nous savons donc que le DNS est organisé sous forme d'une grande arborescence, et que chaque partie de cette dernière peut être gérée par la personne qui la possède.

Comment faire pour savoir qui possède telle ou telle partie et où sont stockées les informations que l'on recherche ? **[1]**

II.5.3 La gestion internationale des noms de domaines

Même si le système DNS n'est pas indispensable au fonctionnement d'1nternet, il en est un élément incontournable.

Le système de noms de domaines est géré par un organisme américain appelé l'ICANN, qui dépend directement du Département du Commerce des États-Unis. L'ICANN est responsable de la gestion des 13 serveurs DNS qui gèrent la racine du DNS. Ces 13 serveurs connaissent les adresses IP des serveurs DNS gérant les TLD (les .fr, .com, .org, etc.)

En fait, après plusieurs attaques sur les serveurs racines, on s'est rendu compte de la faiblesse de n'avoir que 13 serveurs et de la menace que cela pouvait représenter pour le fonctionnement d'Internet.

On a donc mis en place un système qui dupliqué les 13 serveurs en différents endroits d'Internet. Il y a donc réellement aujourd'hui plusieurs centaines de serveurs racines qui dupliquent les informations des 13 serveurs d'origine.

Le mécanisme qui permet cette duplication de serveurs, et notamment d'adresses IP, s'appelle fanycast.

C'est l'ICANN[1] qui autorise la création d'une nouvelle extension, comme le **.xxx** il y a plusieurs mois, ou l'utilisation de caractères non latins (arabes, chinois, japonais, etc.) il y a quelques années.

L'ICANN délègue ensuite les domaines de premier niveau à divers organismes. Pour l'Europe, c'est le RIPE[2] qui délègue lui-même à L'AFNIC[3] qui est responsable du domaine **.fr** (ainsi que des extensions correspondantes à la France d'outremer) ; pour le domaine **.com**, c'est Verisign[4] qui s'en occupe. Les labels inférieurs correspondent généralement à des sites ou à des entreprises, et la gestion du nom de domaine leur revient. **[1]**

II.6 Le service de messagerie

II.6.1 Définition

Plus connus sous le nom de courrier électronique ou e-mail, ces services permettent d'échanger des messages et des fichiers. La taille des fichiers (pièces jointes) est limitée par les serveurs de messagerie (limitation d'environ 1 Mo) pour restreindre le stockage et préserver la bande passante. Au-delà, il faudra utiliser un service spécialisé dans le transfert de fichier utilisant un protocole adapté tel que FTP (File Transfer Protocol).

Il faut différencier la messagerie interne et la messagerie externe. La messagerie interne est installée à l'intérieur d'un intranet (réseau informatique interne: une entreprise, un organisme…), la messagerie externe (avec Internet) permettant la communication avec l'extérieur de l'intranet, le service de messagerie (souvent constitué d'une passerelle qui convertit les protocoles) est géré par un fournisseur extérieur.

L'architecture de la première étant la plus simple, elle sera étudiée en premier, même s'il est rare qu'elle soit dissociée de la seconde, sauf pour des raisons de sécurité. Dans ce cas, deux services distincts coexisteront, les postes permettant la messagerie interne étant dissociés de ceux autorisant l'échange de messages avec le monde Internet. **[2]**

II.6.2 Architecture d'une messagerie interne

L'architecture de base tourne autour d'un serveur de messagerie disposant de boîtes aux lettres (BAL). Chaque utilisateur dispose d'une BAL à laquelle il peut accéder en lecture par un « nom utilisateur » et un « mot de passe » (figure 2.3). La liste des BAL est stockée dans une base de données de comptes. Cette base de données est le plus souvent compatible avec ODBC (Open Data Base Connectivity).

[1] ICANN: L'Internet Corporation for Assigned Names and Numbers.
[2] RIPE: Réseaux IP Européens.
3 AFNIC: Association française pour le nommage Internet en coopération.
[4] Verisign : est une société américaine établie à Reston (virginie).

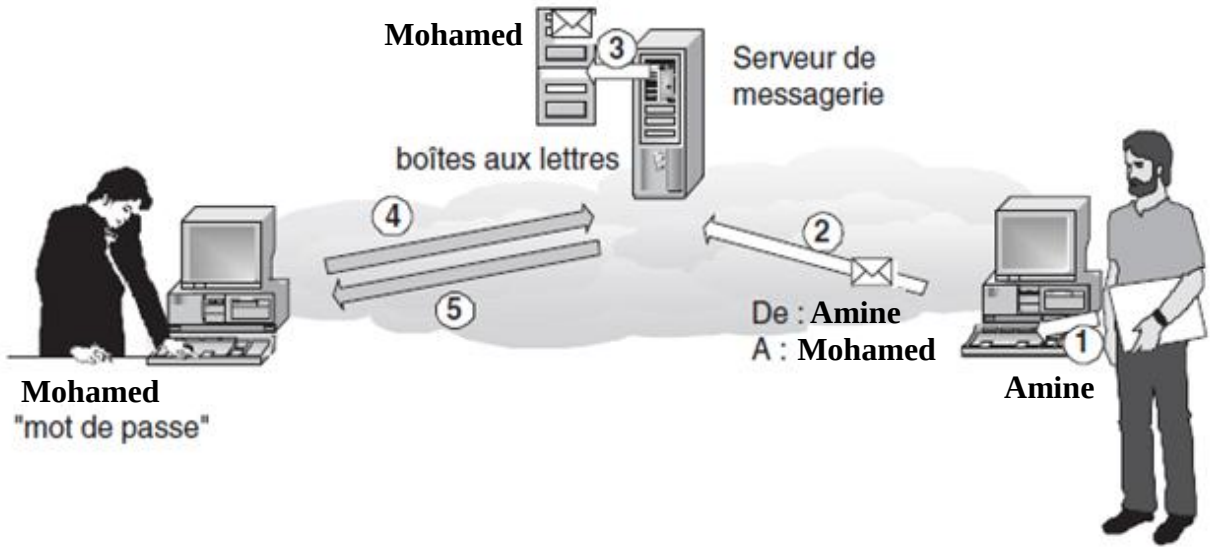


Figure 2.3 Architecture et fonctionnement d'une messagerie interne.

Le fonctionnement comprend deux phases distinctes : l'envoi du message d'une part, la lecture du message d'autre part. Ces deux phases sont indépendantes et décorrélées dans le temps.

– Phases d'envoi :

1. L'expéditeur (Amine) rédige le message (texte + destinataire). Le poste peut être déconnecté du réseau.

2. L'expéditeur envoie le message au serveur de messagerie. Le poste doit être connecté au réseau. L'expéditeur n'a pas besoin de disposer d'une BAL sur le serveur, mais le poste doit connaître le nom du serveur (il doit posséder un compte si l'accès au réseau est contrôlé par un serveur de comptes).

3. Le serveur de messagerie vérifie l'existence d'une BAL au nom du destinataire (Mohamed) et y stocke le message.

– Phases de réception :

4. Le destinataire (Mohamed) interroge sa BAL. Le poste doit connaître le nom du serveur de messagerie (il doit d'abord ouvrir une session dans le cas d'un serveur de comptes).

5. Après vérification de son nom et de son mot de passe par le serveur, Mohamed peut lire ou transférer les messages situés dans sa BAL. Dans le cas où le message est transféré vers l'outil de messagerie du poste client, la lecture du message peut se faire en différé (hors connexion au réseau).

Les protocoles utilisés par le serveur pour traiter le message et par le destinataire pour interroger sa Boîte aux lettres sont différents. Le plus souvent, le traitement des messages se fait avec SMTP (Simple Mail Transfer Protocol), alors que l'interrogation de la BAL utilise POP3 (Post Office Protocol). **[2]**

II.6.3 Architecture d'une messagerie externe

La particularité d'une messagerie externe est que la boîte aux lettres du destinataire ne se trouve pas sur le serveur de messagerie auquel est connecté l'expéditeur du message. Pour atteindre la BAL du destinataire, les deux serveurs doivent s'échanger le message à travers un ou plusieurs réseaux d'opérateurs. Ces réseaux peuvent être de type Internet, mais également de type RTC[5], ADSL[6] ou RNIS[7]. Les deux serveurs vont devoir utiliser un protocole d'adressage compatible avec celui utilisé par les équipements de l'opérateur auquel ils sont raccordés. La figure 2.4 donne l'exemple le plus simple de l'architecture d'une messagerie externe.

Dans ce cas, la transmission du message va faire intervenir les agents de transfert MTA (Message Transfer Agent) de chaque serveur de messagerie. La succession des phases se présente ainsi (figure 2.4) :

1. Transfert du message du poste de l'expéditeur (Amine) vers le serveur du réseau local A (réseau d'Amine) où il est stocké en attente d'émission par le MTA.

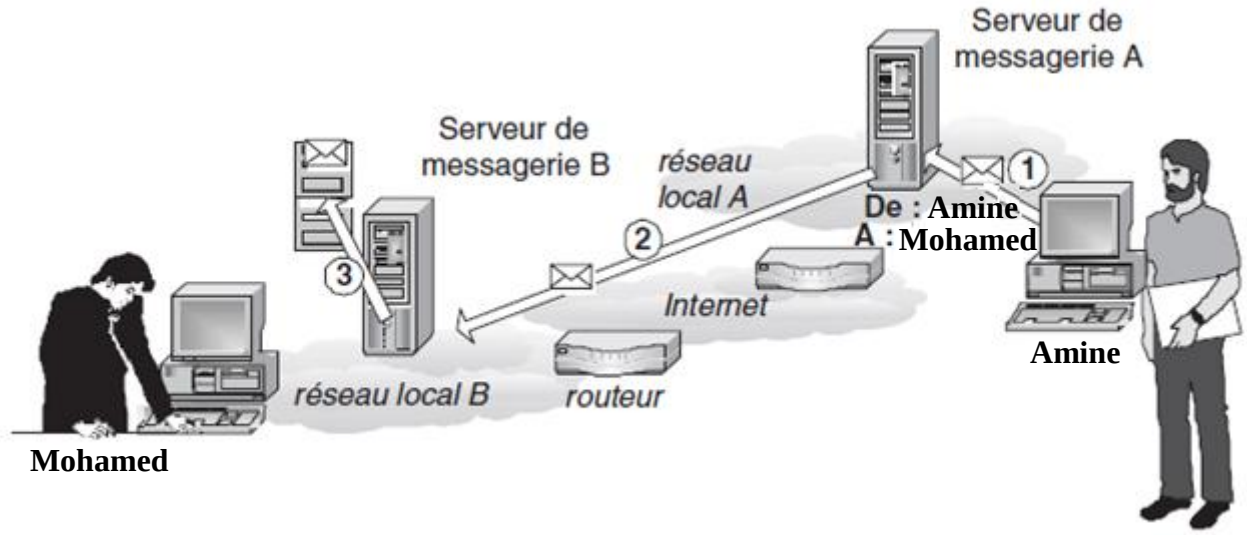


Figure 2.4 Architecture d'une messagerie externe.

2. Le serveur de messagerie A se connecte au serveur de messagerie B à travers le réseau de l'opérateur Internet. L'agent de transfert du serveur A transmet le message à l'agent de transfert du serveur B.

3. Le service de traitement du serveur de messagerie B stocke le message dans la BAL du destinataire (Mohamed).

L'agent de transfert du serveur de messagerie B devra vérifier l'existence de la BAL du destinataire (Mohamed). Si la BAL n'est pas trouvée, un message d'erreur est transmis par l'agent de transfert du serveur B vers l'agent de transfert du serveur A.

Celui-ci peut adresser à l'expéditeur un message d'erreur de transmission indiquant que le destinataire n'a pas été trouvé. Sur Internet, les agents de transfert utilisent le protocole SMTP (*Simple Mail Transfer Protocol*).

Lorsque le nombre de comptes de messagerie à gérer et que le volume de messages traités sont importants, le serveur d'émission des messages est physiquement séparé du serveur de réception.**[2]**

5 Le réseau téléphonique commuté

6 Asymmetric Digital Subscriber Line: est une technique de communication numérique

7 *Réseau numérique à intégration de services*

II.6.4 Les protocoles de messagerie

II.6.4.1 SMTP pour la gestion du courrier

Le protocole SMTP (*Simple Mail Transfer Protocol*) est le plus couramment utilisé pour la gestion du courrier entre serveurs sur Internet, reliés en permanence. Un utilisateur connecté de façon intermittente (*Dial up*) à travers le RTC ou RNIS utilisera également SMTP pour l'expédition de son courrier (courrier sortant) et un protocole tel que POP3 (*Post Office Protocol*) pour lire son courrier (courrier entrant).
Le format des messages SMTP utilise le caractère « @ » comme séparateur du nom de la BAL de celui du serveur de messagerie. Ce dernier utilise le format commun des serveurs sur Internet tel que « mail.babaorum.fr » pour le serveur « mail » du domaine « babaorum.fr ». Ainsi l'adresse de Bernard sur ce serveur aura la syntaxe *bernard@mail.babaorum.fr*. Cette adresse devra apparaître dans le champ « destinataire » de l'éditeur de messages. **[2]**

II.6.4.2 POP3 et IMAP pour interroger la BAL

Ce protocole POP3 (*Post Office Protocol*) est destiné à récupérer le courrier sur un serveur pour un utilisateur non connecté en permanence à Internet, mais se connectant à travers un réseau d'opérateur de télécommunication tel que le RTC ou le RNIS. Il gère :
– l'authentification du client (vérification du nom et du mot de passe) ;
– la réception des courriers et fichiers attachés à partir du serveur de messagerie ;
– la réception de messages d'erreur ou d'acquittement.

Ce protocole ne permet pas l'envoi de messages. Il ne permet pas non plus la lecture des messages « en ligne ». Il est nécessaire de télécharger l'intégralité du message et des pièces jointes avant sa lecture. Il ne permet donc pas de manipuler les messages sur le serveur.

Pour lire le courrier « en ligne », il faut utiliser un protocole comme IMAP (*Interactive Mail Access Protocol*). Il permet également la manipulation sur les messages tels que les recherches selon critères, le tri, l'effacement, ainsi que la création sur le serveur de dossiers publics et privés pour le classement des messages. Les dossiers privés ne sont accessibles qu'à leur créateur; les dossiers publics sont accessibles à tous ou à un groupe de clients. **[2]**

II.6.4.3 *MIME pour la mise en forme des messages*

Pendant longtemps, le codage des caractères était laissé au libre choix des éditeurs de logiciels de messagerie. Il s'ensuivait des affichages peu fiables lorsque le message était lu sur un logiciel d'un éditeur différent de celui utilisé pour la création du message. Aujourd'hui, les éditeurs proposent aux utilisateurs plusieurs choix de protocoles.
Le plus utilisé actuellement est le protocole MIME (*Multipurpose Internet Mail Extension*). Ce protocole assure le codage du texte et l'insertion de fichiers joints, qu'ils soient de texte formaté, d'image ou de son. **[2]**

II.7 Le service de transfert de fichiers

II.7.1 Définition

Le service de transfert de fichiers c'est un service qui va permettre l'échange de fichiers entre 2 ordinateurs, et plus exactement entre un serveur et un client.
On parle alors de :

- serveur FTP
- client FTP **[2]**

II.7.2 Architecture et fonctionnement d'un serveur de fichiers

Il permet à un client d'échanger des fichiers avec un serveur de fichiers en accédant directement et de manière sécurisée (sauf connexion « anonymous ») à l'arborescence des répertoires de ce dernier. C'est un outil très utile pour le travail coopératif (*groupware*). Il permet à un groupe (équipe de projet par exemple) de travailler et de s'échanger des documents de travail sans multiplier les copies, comme cela se passe dans le cas d'un échange par messagerie (sauf avec le Webmail). Son utilisation permet également la mise à jour à distance de pages d'un serveur web.

La procédure commence par l'établissement d'une connexion (niveau TCP) entre un client et le serveur. Une fois la connexion établie, le client dialogue avec le serveur en lui envoyant des « commandes » à exécuter. La connexion et le dialogue entre la station du client et le serveur utilisent le protocole FTP (*File Transfer Protocol*).

Le serveur FTP dispose de deux types de répertoires : les répertoires « privés » accessibles uniquement aux clients possédant un compte sur le serveur, compte auquel sont associés des droits d'accès sur certains répertoires « privés », et les répertoires « publics » accessibles aux autres clients (comptes « anonymous »).

Après qu'un client se soit connecté au serveur, celui-ci demande un nom de compte et un mot de passe (figure 2.5). Le compte *anonymous* permet au client d'accéder aux fichiers des répertoires « public ». Dans ce cas, le mot de passe demandé est généralement l'adresse e-mail du demandeur.

Les logiciels sur la station du client disposent des commandes permettant de se déplacer dans l'arborescence du disque du serveur, de définir le type des données transférées (binaire ou ASCII), de manipuler des fichiers (écrire, lire, effacer, renommer, transférer…). Le protocole FTP fonctionne, côté serveur, avec deux canaux distincts. Par défaut, ces canaux sont ouverts sur les ports TCP (figure 2.5) :

– 20 pour le canal de données ;

– 21 pour le canal de commande. **[2]**

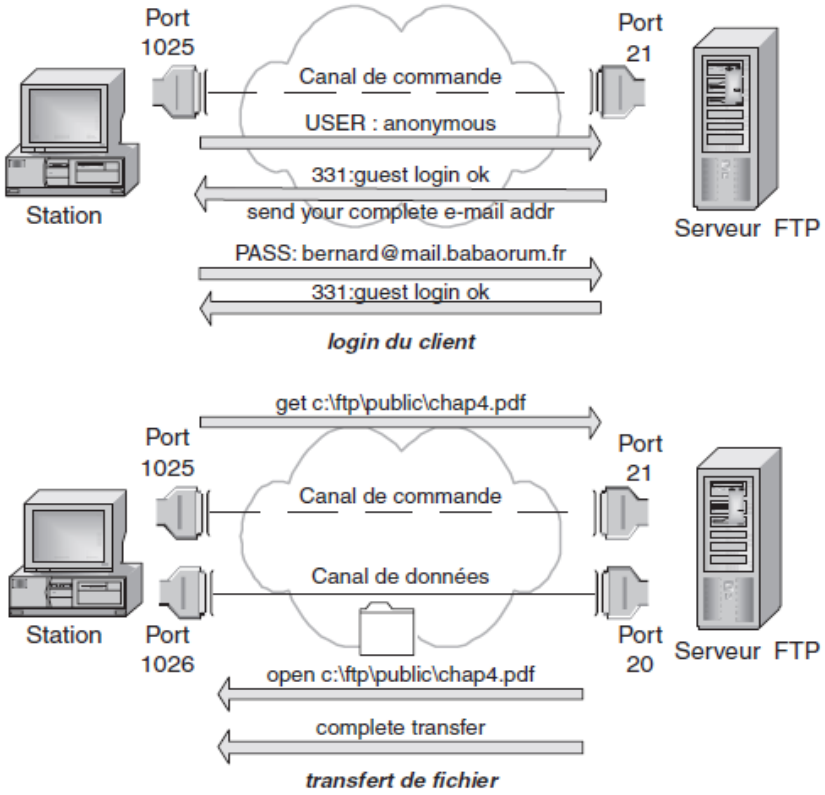


Figure 2.5 Connexion FTP.

II.8 Conclusion

Dans ce chapitre nous avons présenté les différents types de services réseaux qui sont des applications fournis par des serveurs pour les clients.

Chapitre III

L'Adressage et Le Routage

III.1 Introduction

L'adressage est une représentation numérique qui identifie de façon unique une interface donnée sur le réseau.
Le routage est la fonctionnalité qui permet d'acheminer les données d'un point A vers un point B situé dans un réseau distant. Le routage, effectué par les routeurs, se base sur l'adresse IP de destination contenu dans le paquet reçu.

III.2 L'adressage IP

À la différence des adresses physiques, les adresses réseaux ou adresse IP sont attribuées par les administrateurs réseau et sont configurées logiquement.
L'adresse IP comporte pour commencer deux parties principales :
- Une ID (Network Identity) de réseau (netID) qui est l'adresse réseau logique du sous réseau auquel l'ordinateur se rattache,
- Une ID d'hôte (hostID) qui est l'adresse logique du périphérique logique identifiant chaque ordinateur sur un sous réseau.

Il y'a deux version d'adresse IP :
- IPv4 utilises des adresses uniques de 32 bits

- IPv6 utilises des adresses uniques de 128 bits

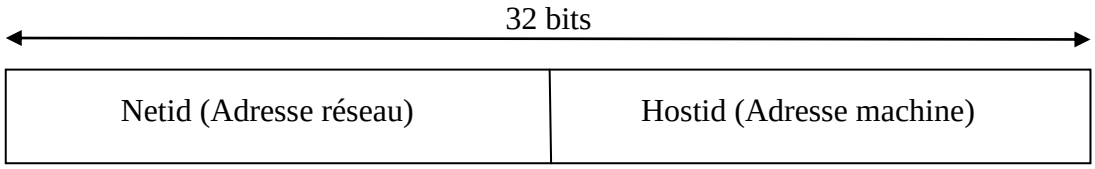
III.2.1 Adressage IPv4 (IP version 4.0)

III.2.1.1 Introduction aux adresses IPv4

Une adresse IPv4 est un nombre d'une valeur de 32 bits représentée par 4 valeurs décimales pointées ; chacune a un poids de 8 bits (1 octet) prenant des valeurs décimales de 0 à 255 séparées par des points. La notation est aussi connue sous le nom de "décimale pointée".

Le masque de réseau lui aussi noté en décimal pointé indique avec les bits à 1 la partie réseau partagée par toutes les adresses d'un bloc et avec les bits à 0 la partie unique qui identifie les interfaces sur la liaison.

On les note donc sous la forme xxx.xxx.xxx.xxx.



Par exemple, `192.168.1.25 255.255.255.0` indique un numéro de réseau (première adresse) `192.168.1.0` et un numéro de Broadcast `192.168.1.255`. Toutes les adresses comprises entre ces valeurs peuvent être utilisées par les interfaces attachées à une même liaison (un même switch).

À cause du manque d'espace IPv4 disponible, on trouve souvent des masques qui chevauchent les octets, ce qui nécessite de passer par des calculs binaires.

III.2.1.2 Les classes d'adresse

À l'origine d'IPv4, on distingue une organisation en classes d'adresses dont les quatre premiers bits indiquent la classe. **[10]**

- La classe A
Cette classe est faite pour les très grands réseaux. Seul le premier octet est utilisé pour la partie réseau, ce qui laisse donc trois octets pour la partie hôte. Ce premier octet est compris entre 1 et 126. Cette classe peut accueillir plusieurs millions d'hôtes. **[10]**

- La classe B

Cette classe est faite pour les moyens et grands réseaux. Les deux premiers octets sont utilisés pour la partie réseau et les deux suivants pour la partie hôte. Le premier octet est compris entre 128 et 191. Cette classe peut accueillir plusieurs dizaines de milliers d'hôtes. **[10]**

- La classe C

Cette classe est faite pour les petits réseaux puisqu'elle ne peut accueillir que 256 hôtes. Les trois premiers octets étant employés pour la partie réseau, il n'en reste qu'un seul pour la partie hôte. Le premier octet est compris entre 192 et 223. **[10]**

- La classe D

C'est une classe utilisée pour le multicasting. Le premier octet de cette classe est compris entre 224 et 239. **[10]**

- La classe E
Cette classe a été définie comme étant une classe pour les ordinateurs de recherche. Le premier octet de cette classe est compris entre 240 et 255. **[10]**

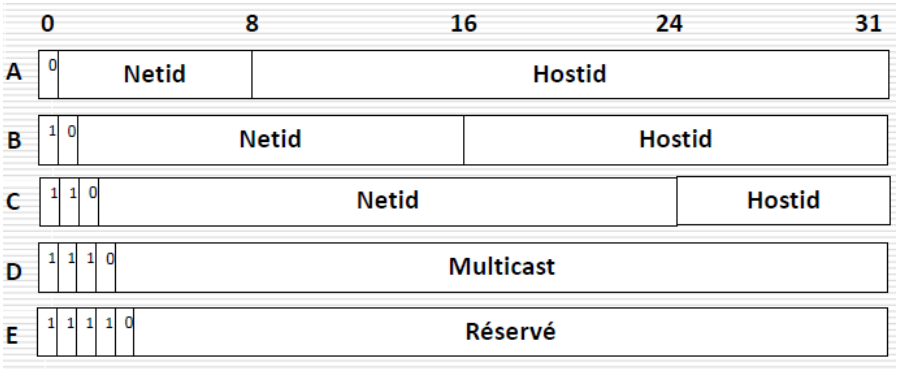


Figure 3.1 Les classes d'adressages

III.2.1.2.1 Notes sur les Classes d'adresses

- Seules les adresses de Classes A, B et C sont assignables à des interfaces (**adresse d'Unicast**)
- La classe D est utilisée pour des **adresses de Multicast** (adresse unique identifiant de nombreuses destinations)
- La classe E est utilisée pour des besoins futurs ou des objectifs scientifiques

Adresses spécifiques :

- Les adresses commençant de `127.0.0.0` à `127.255.255.255` sont réservées pour le bouclage (loopback)
- Adresses privées non routables vers l'Internet sont :
  - Pour la classe A : de `10.0.0.0` à `10.255.255.255`
  - Pour la classe B : de `172.16.0.0` à `172.31.255.255`
  - Pour la classe C : de `192.168.0.0` à `192.168.255.255`

III.2.1.3 Le Masque de réseaux

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse. On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque de réseau.

Un masque va préciser de manière certaine dans quel réseau se trouve une adresse IP et en conséquence :

1. L'**adresse du réseau** (appelée aussi numéro de réseau, non assignable)
2. L'**adresse de Broadcast** (adresse visant toutes les destinations, non assignable)
3. La plage d'adresses utilisables (de la première à la dernière en dehors des adresses précitées)

Un masque sera une suite de 32 bits divisée en 4 octets pointés composée uniquement d'abord d'une suite de 1 et, après, d'une suite de 0. La notation est aussi décimale pointée. Toutefois, on trouvera une autre notation dite CIDR (*Classless Interdomain Routing*) qui représente le nombre de bits pris par la partie réseau du masque.

III.2.1.3.1 Masque par défaut

Le nombre d'hôtes possibles obtenus ci-dessus correspond à l'application d'un masque par défaut sur un type de classe d'adresse :

- Le masque par défaut des adresses de Classe A est `255.0.0.0` ou /8
- Le masque par défaut des adresses de Classe B est `255.255.0.0` ou /16
- Le masque par défaut des adresses de Classe C est `255.255.255.0` ou /24

III.2.1.4 Communication IPv4

Un hôte connecté à un réseau peut communiquer avec les autres périphériques de trois façons :

III.2.1.4.1 Transmission monodiffusion

La monodiffusion est utilisée dans les communications normales d'hôte à hôte tant entre client et serveur que dans un réseau peer-to-peer. Les paquets de type monodiffusion utilisent l'adresse du périphérique de destination comme adresse de destination et peuvent être acheminés sur un inter-réseau.

Dans un réseau IPv4, l'adresse monodiffusion appliquée à un périphérique final est désignée sous le nom d'adresse d'hôte. Dans une monodiffusion, les adresses attribuées aux deux périphériques finaux sont utilisées comme adresses IPv4 source et de destination. Durant l'encapsulation, l'hôte source utilise son adresse IPv4 comme adresse source et l'adresse IPv4 de l'hôte de destination comme adresse de destination. Même si la destination est spécifiée dans un paquet comme une monodiffusion, une diffusion ou une multidiffusion, l'adresse source d'un paquet est toujours l'adresse de monodiffusion de l'hôte d'origine. **[11]**

III.2.1.4.2 Transmission de diffusion

Le trafic de diffusion est utilisé pour envoyer des paquets à tous les hôtes du réseau grâce à l'adresse de diffusion du réseau. En diffusion, le paquet contient une adresse IPv4 de destination avec uniquement des un (1) dans la partie hôte. Cela signifie que tous les hôtes se trouvant sur ce réseau local (domaine de diffusion) recevront le paquet et le regarderont. De nombreux protocoles réseau, tels que DHCP, utilisent les diffusions. Lorsqu'un hôte reçoit un paquet envoyé à l'adresse de diffusion du réseau, il traite le paquet comme s'il s'agissait d'un paquet adressé à son adresse de monodiffusion.

La diffusion peut être dirigée ou limitée. Une diffusion dirigée est envoyée à tous les hôtes d'un réseau particulier. Par exemple, un hôte sur le réseau 172.16.4.0/24 envoie un paquet à 172.16.4.255. Une diffusion limitée est envoyée à 255.255.255.255. Par défaut, les routeurs ne transfèrent pas les diffusions.

Par exemple, un hôte du réseau 172.16.4.0/24 envoie une diffusion à tous les hôtes de son réseau à l'aide d'un paquet dont l'adresse de destination est 255.255.255.255.

Lorsqu'un paquet est diffusé, il utilise les ressources du réseau et est traité par chaque hôte destinataire sur le réseau. Ainsi, le trafic de diffusion devrait être limité de sorte qu'il ne réduise pas les performances du réseau ou des périphériques. Dans la mesure où les routeurs séparent les domaines de diffusion, la création de sous-réseaux peut améliorer les performances du réseau en éliminant le trafic de diffusion excessif. **[11]**

III.2.1.4.3 Transmission multidiffusion

La transmission multidiffusion réduit le volume du trafic en permettant à un hôte d'envoyer un seul paquet à un groupe d'hôtes désigné inscrits à un groupe de multidiffusion.

IPv4 a réservé les adresses 224.0.0.0 à 239.255.255.255 comme plage de multidiffusion. Les adresses de multidiffusion IPv4 du bloc 224.0.0.0 à 224.0.0.255 sont réservées à la multidiffusion

sur le réseau local uniquement. Ces adresses s'appliquent aux groupes de multidiffusion d'un réseau local. Un routeur connecté au réseau local sait reconnaître que ces paquets sont adressés à un groupe de multidiffusion d'un réseau local et ne les transmet jamais. Les adresses de multidiffusion de réseau local réservées s'appliquent principalement aux protocoles de routage qui utilisent la transmission multidiffusion pour échanger des informations de routage. Par exemple, 224.0.0.9 est l'adresse de multidiffusion utilisée par le protocole RIP (Routing Information Protocol) version 2 pour communiquer avec d'autres routeurs RIPv2.

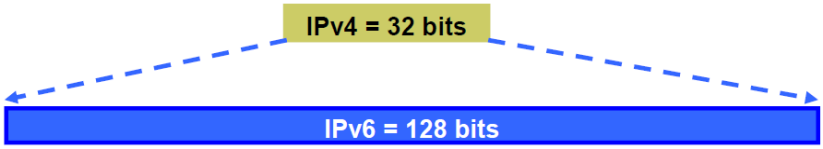
Les hôtes qui reçoivent des données multidiffusion spécifiques sont appelés des « clients multidiffusion ». Ces derniers font appel à des services demandés par un programme client pour s'abonner au groupe de multidiffusion.

Chaque groupe de multidiffusion est représenté par une seule adresse de destination multidiffusion IPv4. Lorsqu'un hôte IPv4 s'abonne à un groupe de multidiffusion, il traite les paquets envoyés à cette adresse de multidiffusion, ainsi que ceux destinés à son adresse de monodiffusion, qui a été attribuée à lui seul. **[11]**

III.2.2 Adressage IPV6 (IP version 6.0)

III.2.2.1 Introduction d'IPv6

Les ID de réseaux disponibles dans IPv4 sont de plus en plus rares. Une nouvelle version a donc été mise au point IPv6.
IPv6 utilise **16 octets**. Il comporte 8 paires d'octets séparées par des virgules. Les octets sont représentés en notation hexadécimale.
IPv6 est une nouvelle structure de paquets incompatible avec les systèmes IPv4, mais offrant plusieurs avantages tels qu'un espace d'adressage étendu, un format d'en-tête simplifié, la prise en charge d'un trafic dépendant du temps, ainsi que la possibilité d'ajouter de nouvelles fonctionnalités.



23

- IPv4
  - 32 bits
  - = 4,294,967,296 dispositifs adressables
- IPv6
  - 128bits: 4 fois la taille en bit
  - =3.4 x 10^{38} dispositifs adressables
  - = 340,282,366,920,938,463,463,374,607,431,768,211,456
  - ~ 5 x 1028 adresses par personne sur la planète

III.2.2.2 Les nouveautés d'IPV6

- L'espace d'adressage étendu constitue l'une des principales caractéristiques d'IPv6.
IPv6 utilise des adresses source et de destination à 128 bits (4 fois plus grandes qu'avec IPv4). Exemple d'adresse IP valide avec IPv6 : 4A3F :AE67 :F240 :56C4 :3409 :AE52 :440F :1403

- Les en-têtes Ipv6 sont conçus pour minimiser le traitement de l'en-tête IP en déplaçant les champs non essentiels et les champs d'option dans des en-têtes d'extension placés après l'en-tête IP.

- Un nouveau champ dans l'en-tête IPv6 permet la pré-allocation de ressources réseau sur le chemin afin que les services à dépendance temporelle tels que les services vocaux et vidéo bénéficient d'une bande passante garantie avec des retards fixes.

- IPv6 peut facilement être étendu pour incorporer de nouvelles fonctionnalités par l'ajout d'en-têtes d'extension après l'en-tête IPv6 de base. La prise en charge de nouveaux matériels ou de nouvelles technologies d'application est ainsi incorporée.

III.2.2.3 Types d'adresses d'IPv6

- **Unicast :** une adresse pour chaque interface (équipement).

Un paquet envoyé à une adresse unicast est délivre à une seule interface.

- **Anycast :** une adresse désigne un groupe d'interfaces. Un paquet envoyé à une adresse anycast est délivre à une des interfaces identifiées par l'adresse anycast.
- **Multicast :** une adresse désigne un groupe d'interfaces. Un paquet envoyé à une adresse multicast est délivré à toutes les interfaces identifiées par l'adresse multicast.

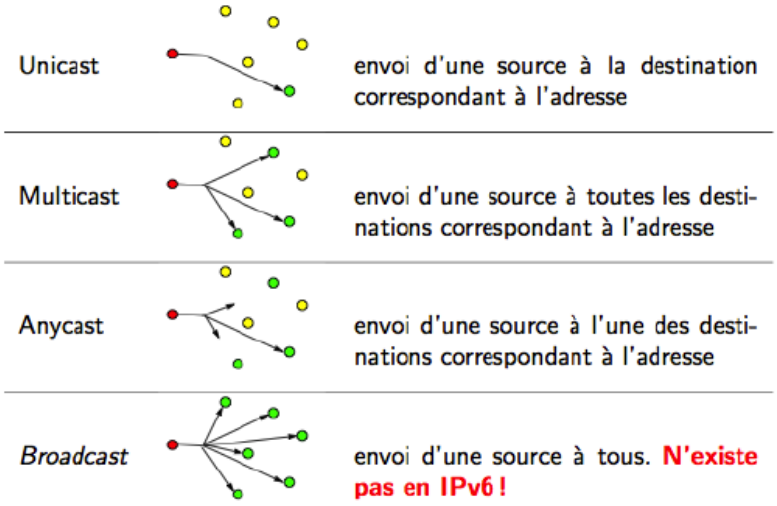


Figure 3.2 Types d'adresses d'IPv6

III.2.2.4 Notation D'IPv6

Les adresses IP peuvent être écrites de trois manières :

- une forme hexadécimale complète : X :X :X :X :X :X :X :X
  ou chaque X représente une valeur sur 16 bits ;
- une forme hexadécimale abrégée qui ressemble à la forme précédente mais dans laquelle les valeurs X égales à 0 sont condensées comme dans l'exemple suivant (attention l'abréviation: « : » ne peut apparaitre qu'une seule fois dans une adresse) :
  1 :0 :0 :0 :0 :0 :0 :15 s'écrit en forme condensée 1 : :15 ;

- une forme permettant le rapprochement entre adresses IPv4 et adresses IPv6 qui s'écrit sous la forme : X :X :X :X :X :d.d.d.d ou chaque X représente une valeur sur 16 bits et chaque d représente une valeur sur 8 bits. Par exemple au lieu d'écrire l'adresse IPv4 0 :0 :0 :0 :0 :0 :194.12.5.01 avec des zéros on l'écrit de la manière suivante: :194.12.5.01

III.3 LE ROUTAGE

III.3.1 Principe

Le routage d'un paquet consiste à trouver le chemin de la station destinatrice à partir de son adresse IP. Si le paquet émis par une machine ne trouve pas sa destination dans le réseau ou sous-réseau local, il doit être dirigé vers un routeur qui rapproche le paquet de son objectif. Il faut par conséquent que toutes les stations du réseau possèdent l'adresse du routeur par défaut. La machine source applique le masque de sous-réseau (netmask) pour savoir si le routage est nécessaire.

Chaque routeur doit donc connaître l'adresse du routeur suivant lorsque la machine de destination n'est pas sur les réseaux ou sous-réseaux qui lui sont raccordés. Le routeur intègre au moins deux interfaces réseau avec une adresse IP dans chaque réseau connecté. Il doit gérer une table de routage de manière statique ou dynamique. **[3]**

III.3.2 Routages statiques

Le routeur apprend ces routes quand l'administrateur les entre manuellement. Cela peut prendre un temps considérable si l'entreprise possède beaucoup de routeurs et en cas de modification d'un réseau, il va falloir passer sur tous les routeurs pour faire la modification. **[3]**

III.3.3 Routages dynamiques

Le routeur apprend ces routes de manière automatique. Pour cela, on utilise un protocole de routage, qui va s'occuper de remplir la table de routage selon ses propres critères. Dès qu'il y a un changement sur le réseau, le routeur va l'apprendre automatiquement et il n'y aura pas besoin d'une intervention manuelle sur le routeur pour changer quelque chose puisque le protocole va s'en charger. Il faut bien entendu plusieurs routeurs pour que cela serve à quelque chose. **[3]**

III.3.4 Table de routage

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

Adresse de destination	Adresse du prochain routeur directement accessible	Interface

Ainsi grâce à cette table, le routeur, connaissant l'adresse du destinataire encapsulée dans le message, va être capable de savoir sur quelle interface envoyer le message (cela revient à savoir quelle carte réseau utiliser), et à quel routeur, directement accessible sur le réseau auquel cette carte est connectée, remettre le datagramme.
Ce mécanisme consistant à ne connaître que l'adresse du prochain maillon menant à la destination est appelé *routage par sauts successifs* (en anglais *next-hop routing*).

Cependant, il se peut que le destinataire appartienne à un réseau non référencé dans la table de routage. Dans ce cas, le routeur utilise un **routeur par défaut** (appelé aussi *passerelle par défaut*). **[3]**

Voici, de façon simplifiée, c'est à quoi pourrait ressembler une table de routage :

Adresse de destination	Adresse du prochain routeur directement accessible	Interface
194.56.32.124	131.124.51.108	2
110.78.202.15	131.124.51.108	2
53.114.24.239	194.8.212.6	3
187.218.176.54	129.15.64.87	1

Tableau 3.1 Exemple de table de routage

Le message est ainsi remis de routeur en routeur par sauts successifs, jusqu'à ce que le destinataire appartienne à un réseau directement connecté à un routeur. Celui-ci remet alors directement le message à la machine visée...

Dans le cas du routage statique, c'est l'administrateur qui met à jour la table de routage. Dans le cas du routage dynamique, par contre, un protocole appelé protocole de routage permet la mise à jour automatique de la table afin qu'elle contienne à tout moment la route optimale. **[3]**

III.3.5 Les algorithmes de routage

Dans le cas du routage statique, la table est établie et modifiée manuellement. Ce type de routage simple peut être utilisé pour un petit réseau local avec une connexion externe.

Pour le routage dynamique, la table est mise à jour périodiquement et automatiquement à l'aide de protocoles spécifiques. Les routeurs envoient régulièrement la liste des réseaux ou des sous-réseaux que l'on peut atteindre par eux. Ce qui permet aux autres routeurs de mettre à jour leurs tables de routage. Pour les réseaux mailles, ils évaluent dynamiquement la meilleure route vers chaque réseau ou sous-réseaux. **[3]**

Deux types d'algorithmes de routage dynamique existent :

III.3.5.1 Algorithmes à vecteur de distance

Les algorithmes à vecteurs de distance (Vector-Distance) pour lesquels les informations échangées permettent pour chaque routeur de retenir la plus courte distance (le plus petit nombre de sauts) pour atteindre une destination ;

Ils sont basés sur l'algorithme de Belman-Ford :

- un routeur diffuse régulièrement à ses voisins les routes qu'il connaît ;

- une route est composée d'une adresse destination, d'une adresse de routeur et d'une métrique indiquant le nombre de sauts nécessaires (la distance) pour atteindre la destination ;

- un routeur qui reçoit ces informations compare les routes reçues avec ses propres routes connues et met à jour sa table de routage :

<> si une route reçue comprend un plus court chemin (nombre de sauts +1 inférieur),

<> si une route reçue est inconnue.

Dans l'exemple donné Figure 3.3, le routeur A reçoit à un instant donné le vecteur contenant les routes connues par le routeur voisin J. Le routeur A examine chaque route transmise et effectue si nécessaire une mise à jour de sa table de routage. Ainsi, rentrée pour atteindre le réseau 4 est modifiée car le routeur J connaît une route plus courte. Le nombre de sauts transmis est de 3, le routeur A ajoute 1 saut pour aller jusqu'à J. Une nouvelle entrée pour atteindre le réseau 21 est également ajoutée.

Ce type d'algorithme que l'on retrouve dans le protocole RIP à l'avantage de la simplicité pour des réseaux limités mais présente plusieurs inconvénients parmi lesquels:

- la taille des informations de routage est proportionnelle au nombre de routeurs interconnectés ;

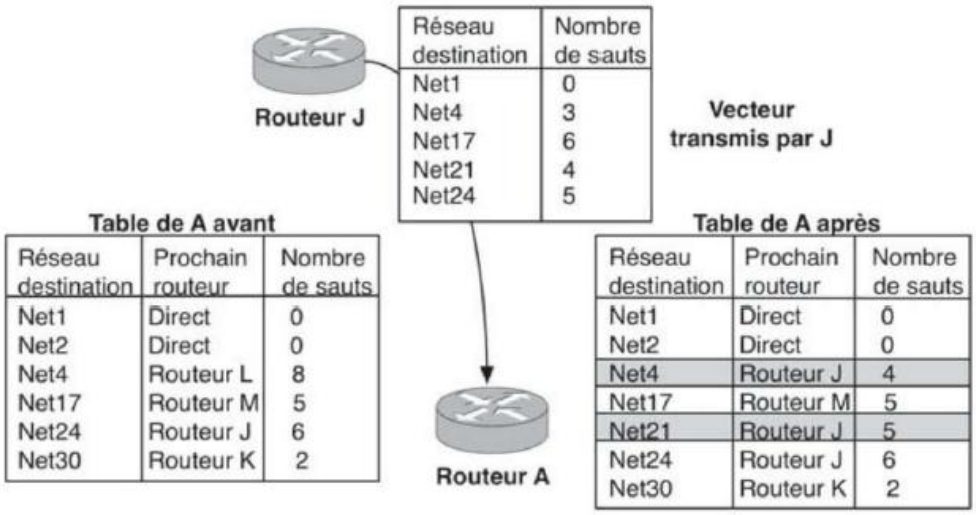


Figure 3.3: exemple d'application de l'algorithme vector-distance.

- La métrique de distance est difficilement utilisable sur des réseaux étendus car elle présente une grande lenteur de convergence (beaucoup l'échanges sont nécessaires avant d'obtenir des valeurs de distance optimisées et stables) ;

- Des bouclages peuvent exister, éventuellement à l'infini (le routeur A transmet une route erronée au routeur B qui la retransmet à A avec un coût augmenté de 1...) ;

- il ne peut y avoir de chemins multiples. **[3]**

III.3.5.2 Algorithmes à état des liens

Les algorithmes à état de lien (Link-State) basés sur la transmission d'une carte complète des liens possibles entre les routeurs, ceux-ci doivent ensuite localement calculer les meilleures routes pour une destination.

Ils sont basés sur la technique du plus court chemin (SPF, Shortest Path First) :

- Les routeurs maintiennent une carte complète du réseau et calculent les meilleurs chemins localement en utilisant cette topologie ;

- Les routeurs ne communiquent pas la liste de toutes les destinations connues (contrairement aux algorithmes Vector-Distance) ;

- Un routeur basé sur l'algorithme SPF teste périodiquement l'état des liens qui la relient à ses voisins, puis diffuse périodiquement ces états (Link-State) à tous les autres routeurs du domaine ;

- Les messages diffusés ne spécifient pas des routes mais simplement l'état (up, down) entre deux

routeurs ;

- Lorsqu'un message parvient à un routeur, celui-ci met à jour la carte de liens et recalcule localement, pour chaque lien modifié, 1a nouvelle route selon l'algorithme de Dijkstra (Shortest Path Algorithm) qui détermine le plus court chemin pour toutes les destinations à partir d'une même source.

La Figure 3.4 montre un exemple d'application de cet algorithme. Tous les routeurs possèdent à un instant donné la même table des liens. Si le routeur A veut envoyer un paquet vers le routeur C, il calcule le plus court chemin vers C et sélectionne en conséquence le routeur B pour lui envoyer le paquet ; B trouve à son tour le plus court chemin vers C qui est direct.

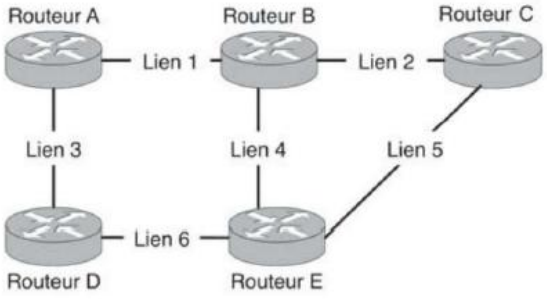


Table des liens

De	à	Lien	Distance
A	B	1	1
A	D	3	1
B	A	1	1
B	C	2	1
B	E	4	1
C	B	2	1
C	E	1	1
D	A	3	1
D	E	6	1
E	B	4	1
E	C	5	1
E	D	6	1

Figure 3.4 Exemple d'application de l'algorithme Link-State.

Ce type d'algorithme présente plusieurs avantages :

- la convergence est rapide et sans boucle ;
- les chemins multiples sont possibles ;
- les métriques ne sont pas limitées à la distance (par exemple, la distance peut être remplacée par le débit et la meilleure route calculée sera celle présentant le meilleur débit) ;
- chaque routeur calcule ses routes indépendamment des autres ;
- les messages diffusés sont inchangés d'un routeur à l'autre et permettent un contrôle aisé en cas de dysfonctionnement ;
- les messages ne concernent que les liens directs entre routeurs et ne sont donc pas proportionnels au nombre de réseaux dans le domaine. **[3]**

III.3.6 Le routage sur Internet

Pour l'Internet, qui est constitué par l'interconnexion d'une grande quantité de réseaux, une organisation hiérarchique est établie pour séparer des domaines de routage (Figure 3.5) :

- le routage à l'intérieur de systèmes autonomes (AS, Autonomous System) qui correspondent à un domaine de routage lié à un découpage de l'Internet et sous la responsabilité d'une autorité unique.

- le routage d'interconnexion entre les AS. Ces deux niveaux de routage font appel à des protocoles spécifiques :

- les protocoles de routage interne IGP (Interior Gateway Protocols) tels que RIP et OSPF qui concernent les routeurs internes ;

- les protocoles de routage externe comme EGP (Exterior Gareway Protocol) ou BGP (Border Gateway Protocol) utilisés par les routeurs externes ou routeurs de bord (border routers). **[3]**

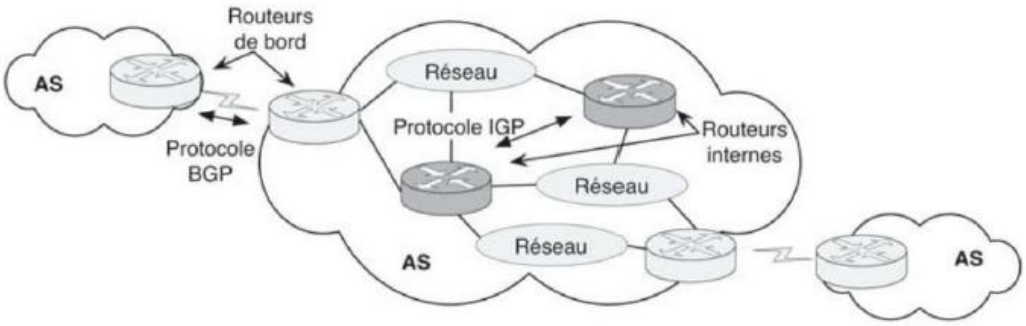


Figure 3.5 : Organisation hiérarchique du routage.

III.3.7 Les Protocoles de routage

Les protocoles de routage sont des opérations sur un routeur qui va diriger les paquets du réseau des directions différentes. Cela dépendra de l'éloignement de la destination est pour le paquet, la quantité de trafic qu'il ya sur les routes et la vitesse du trafic peut se déplacer.

Les principaux protocoles de routages dynamiques sont : **[3]**

III.3.7.1 Le protocole RIP

RIP (Routing Information Protocol) est un protocole à vecteur de distance qui utilise une technique de diffusion (broadcast) périodique. Les transferts se font à l'aide de datagrammes UDP émis toutes les 30 secondes. La distance évaluée (la métrique) est le nombre de sauts, exprimée comme un nombre entier variant de l à 15; la valeur l6 correspond à l'infini. Si une route n'est pas annoncée au moins une fois en 3 minutes, la distance correspondante devient « infinie ».

Les messages au format RIP Figure 3.6 commencent par un mot de 32 bits comportant le code de la commande et un numéro de version, suivi par un ensemble de couples adresse/métrique occupant 5 mots de 32 bits.

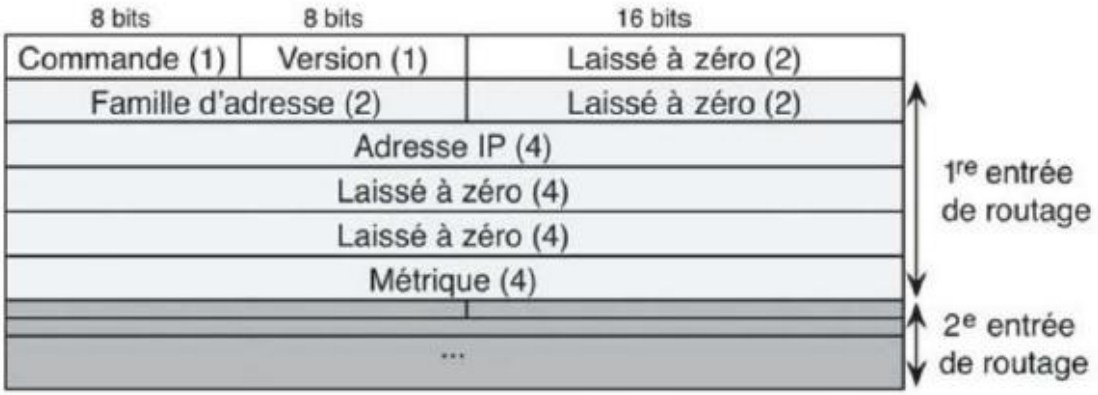


Figure 3.6 Format des messages RIP.

Les messages peuvent être de deux types :

- une requête (champ commande à 1) permet de demander à l'autre routeur d'envoyer tout ou partie de sa table de routage ;

- une réponse (champ commande à 2) contient tout ou partie de la table de routage de la machine émettrice.

Chacun des couples adresse/métrique permet la mise à jour des tables de routage du routeur recevant le message suivant l'algorithme de Belman-Ford décrit précédemment; le champ « famille d'adresse » est par défaut à 2 pour les adresses IP. Le message RIP peut comporter jusqu'à 25 entrées de routage de 20 octets chacune (la taille totale du message reste inférieure à 512 octets). **[3]**

III.3.7.2 Le protocole OSPF (Open Shortest Path First)

OSPF est un protocole à état des liens globalement plus efficace que RIP et qui tend à remplacer ce dernier pour le routage interne. En revanche, les calculs locaux peuvent être assez lourds et les formats des messages ainsi que les échanges sont relativement complexes.

OSPF utilise l'algorithme SPF (Shortest Path First) afin d'élire la meilleure route, celle présentant le coût cumulé le plus faible sur l'ensemble de ses liens, vers une destination donnée. Dans l'exemple décrit à la Figure 3.7, il s'agit d'atteindre le réseau local 192.168.10.0 à partir du routeur Rl. Avec le protocole RIP, la route 1a plus courte en nombre de sauts passe par R5. Si certains liens présentent un débit plus élevé que d'autres, le choix de RIP n'est pas forcément pertinent. Le protocole OSPF attribue un coût à chaque lien afin de privilégier 1'élection de certaines routes. Dans l'exemple, la métrique choisie est le débit. Suivant la table des liens et les coûts associés, la route OSPF passera par R2, R3 et R4 avec un coût total de l3 (l+1+l+10) et un débit minimum de l0 Mbit/s sur toute la route.

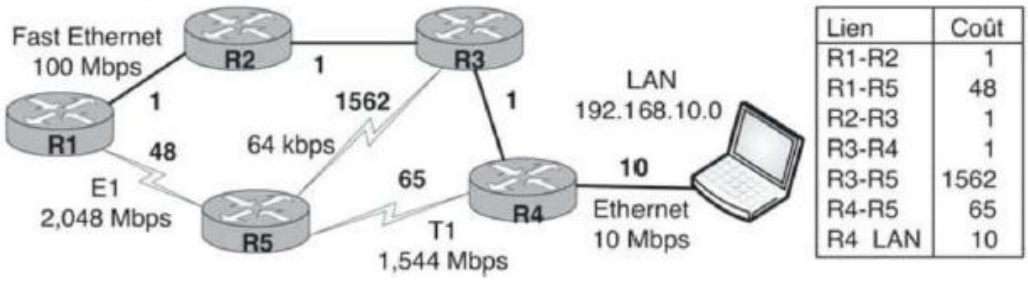


Figure 3.7 : Exemple de coût sur les liens OSPF.

Un réseau OSPF est divisé en plusieurs zones (Areas) qui se connectent à une zone centrale de distribution, Area 0, appelée aussi le backbone. À terme, tous les routeurs auront la même base de données sur l'état des liens de tous les autres routeurs appartenant à la même zone. Avant de pouvoir effectuer leur travail de routage à l'intérieur de cette même zone. **[3]**

III.3.7.3 Le protocole BGP

BGP (Border Gateway Protocol) est utilisé par les routeurs de bord des AS pour échanger de grandes quantités d'informations sur les réseaux qu'ils connaissent et pour lesquels ils proposent du transit (Figure 3.8). Des attributs associés à ces réseaux internes sont également échangés pour permettre par exemple d'éviter les boucles ou d'élire la meilleure route. Contrairement aux protocoles de routage interne, BGP n'utilise pas de métrique classique mais base les décisions de routage sur la succession d'AS et de réseaux internes du chemin, sur les attributs de ces réseaux internes et sur un ensemble de règles de sélection définies par l'administrateur de l'AS. BGP est un protocole à vecteur de chemin (path vector).

Pour échanger les données de routage entre AS, deux types de partage (peering) entre deux routeurs voisins BGP (peers) existent (Figure 3.8) :

- customer-provider peering : il s'agit d'une relation asymétrique dans laquelle un client (un domaine de routage) achète une connectivité à 1'Internet auprès d'un FAI[1] (un autre domaine de routage). Dans ce cas, le client envoie ses routes internes et les routes apprises de ses propres clients au fournisseur. Ce dernier annoncera ces routes sur tout l'Internet. Le fournisseur annonce à son client toutes les routes qu'il connaît et le client est capable en principe d'atteindre n'importe quelle adresse sur 1'Internet ;
- shared-cost peering : il s'agit d'une relation symétrique où deux domaines de routage acceptent d'échanger gratuitement leurs paquets à travers un point d'interconnexion. Chaque peer BGP envoie à l'autre ses propres routes et celles de ses clients. Le point d'interconnexion sera utilisé par chaque peer BGP pour atteindre les destinations des clients de l'autre. **[3]**

[1] Fournisseur d'accès d'Internet

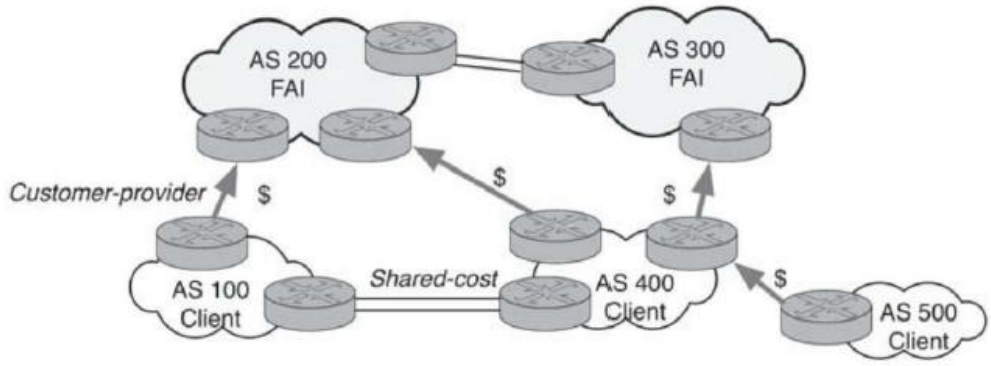


Figure 3.8 : Les deux types de partage BGP.

III.3.7.4 Le protocole EIGRP

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage propriétaire développé par Cisco à partir de leur protocole original IGRP. De ce fait, EIGRP ne pouvait être utilisé que sur des équipements Cisco, mais il est devenu un protocole partiellement ouvert en 2013, permettant aux fabricants de routeurs de l'utiliser.

EIGRP est un protocole de routage à vecteur de distance IP, avec une optimisation permettant de minimiser l'instabilité de routage due aussi bien au changement de topologie qu'à l'utilisation de la bande passante et la puissance du processeur du routeur. **[15]**

III.3.7.4.1 Les caractéristiques d'EIGRP

- EIGRP résout un des problèmes majeurs des protocoles de routage à vecteur de distance, celui des boucles (comme pour les switchs). S'il peut le faire, c'est qu'il a connaissance du réseau et non pas seulement de ses voisins directs (comme un protocole à état de lien).
- La convergence des informations est relativement rapide comparé à d'autres protocoles de la même famille (RIP, Routing Information Protocol).
- Il utilise la métrique, en prenant en compte la bande passante et le délai, et non pas les sauts (d'où le nom d'hybride).
- Il possède, en plus d'une route vers le plus court chemin, une seconde route de secours. Ce qui est très efficace lors de panne. Notez qu'il est le seul à avoir cette route de secours.
- Il peut faire du *load-balancing* sur des bandes passantes égales ou inégales (que deux câbles n'est pas la même capacité), ce qu'il est le seul à faire.
- Il a une distance administrative de 90.

III.4 Conclusion

Dans ce chapitre nous avons décrit d'une part la définition de l'adressage et la différence d'adressage entre IPv4 et IPv6 (L'espace d'adressage d'IPv6 à 128 bits par contre l'adressage IPv4 à 32 bits), d'autre part nous avons présenté le routage et ces différents protocoles qui nous aide à achevé le quatrième chapitre.

Chapitre IV

Simulation d’immigration IPv4 vers IPv6

IV.1 Introduction

Le passage d'un réseau IPv4 à un réseau IPv6 est prévu pour durer très longtemps. Il est donc nécessaire pendant cette période de transition de permettre aux machines IPv4 et IPv6 de cohabiter et de communiquer entre elles.

Pour faire communiquer des machines IPv4 avec des machines IPv6, il est nécessaire d'implémenter des mécanismes de traduction ou de conversion de paquets.

IV.2 Les techniques de migration de réseaux IPv4 vers IPv6

Pour faciliter cette transition différents mécanismes de transition peuvent être utilisés pendant la phase de la transition: Double pile (dual stack), tunnel IPv4/IPv6 configuré, tunnel IPv6 automatique IPv4-compatible, 6to4, Broker, NATPT/ DNS-PT, BIS,…etc. Parmi ces mécanismes il y'a ceux qui font l'encapsulation de l'IPv6 dans IPv4 ou inversement s'appellent les mécanismes de tunneling, ceux qui font la conversion des paquets ou de la traduction des en-têtes (IPv6 en IPv4 ou inversement) s'appellent les mécanismes de translation et un seul mécanisme qui ne fait intervenir ni l'encapsulation ni la traduction d'en-têtes se nomme double pile. Par conséquent ces mécanismes peuvent être classés en 3 familles: Double pile, Tunneling et Translation comme le montre la Figure 4.1 ci-dessous : **[12]**

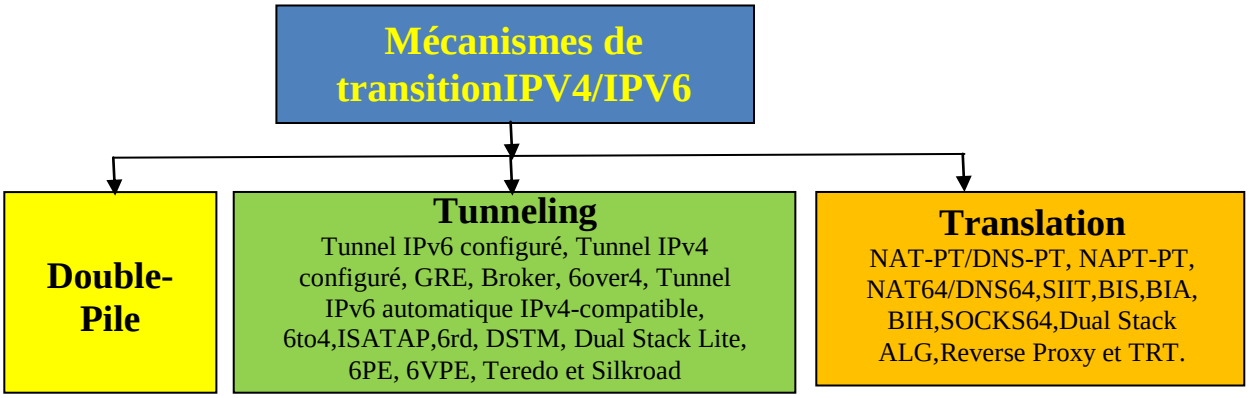


Figure 4.1 Classification des mécanismes de transition IPv4/IPv6

IV.2.1 Famille 1 : Double pile (dual stack)

Double pile est un mécanisme simple à mettre en place et se considère comme la préférée des techniques de transition, car elle ne fait intervenir aucun mécanisme de tunneling ou de translation d'adresse. Il comprend deux piles de protocoles IPv4 et IPv6 fonctionnant en parallèles et côte-à-côte sur la même infrastructure et sur tous les équipements connectés au réseau: ordinateur, routeur, serveur,...etc, comme on peut le voir à la Figure 4.2 ci dessous. Les applications communiquent avec IPv4 et IPv6. Cela signifie qu'on est sur un réseau IPv4/IPv6 et par conséquent on n'a pas besoin de mécanismes supplémentaires pour accéder à la fois à des machines IPv4 et à des machines IPv6. Dans ce cas, les communications sont transmises par les couches IP correspondantes aux adresses utilisées et il n'y a aucun problème de conversion.
Le choix de la version IP est basé sur le résultat de la requête DNS ou de la préférence de l'application.

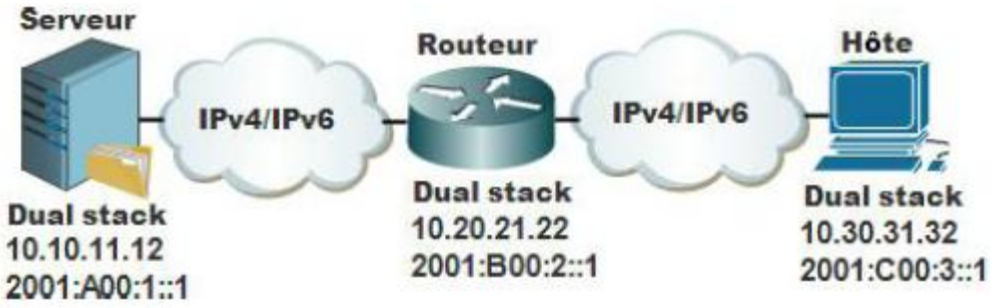


Figure 4.2 : Réseau double pile

Avantages :

- Mécanisme de transition le plus simple à mettre en place en termes d'implémentation et configuration
- Pas besoin de conversion des paquets
- Pas besoin de mécanismes supplémentaires pour accéder à la fois à des machines IPv4 et à des machines IPv6
- Se connecté aux applications IPv4 existantes via IPv4 et accès aux applications IPv6 via IPv6

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP
- Augmente les coûts en termes de performance et d'utilisation CPU du fait que les deux protocoles IPv4 et IPv6 fonctionnent simultanément sur tous les équipements connectés au réseau
- Augmente la complexité :
    - Des politiques de sécurité pour IPv4 et IPv6
    - Certaines applications fonctionnent différemment dans chacun des deux protocoles **[12]**

IV.2.2 Famille 2 : Tunneling

Les mécanismes de tunneling sont des techniques dans lesquelles un protocole est encapsulé dans un autre protocole, selon le réseau où le paquet doit être acheminé.

Plusieurs mécanismes de tunneling peuvent être utilisés pour cette raison: tunnel IPv4/IPv6 configuré, 6to4, Broker, ISATAP, Silkroad, Teredo,…etc. Parmi ces tunnels il y'a ceux qui font l'encapsulation de l'IPv6 dans IPv4 appelés les tunnels IPv6 over IPv4, ceux qui font l'encapsulation de l'IPv4 dans IPv6 appelés les tunnels IPv4 over IPv6, ceux qui font la transmission de l'IPv6 sur un réseau IPv4/MPLS appelés les tunnels IPv6 over MPLS et ceux qui traversent les NATs (traduction d'adresse réseau) en faisant l'encapsulation de l'IPv6 dans UDP sur IPv4 s'appellent les tunnels traversant les NATs. Par conséquent ces mécanismes peuvent être divisés en 4 catégories: tunnels IPv6 over IPv4, tunnels IPv4 over IPv6, tunnels IPv6 over MPLS et tunnels traversant les NATs comme le montre la Figure 4.3 ci-dessous : **[12]**

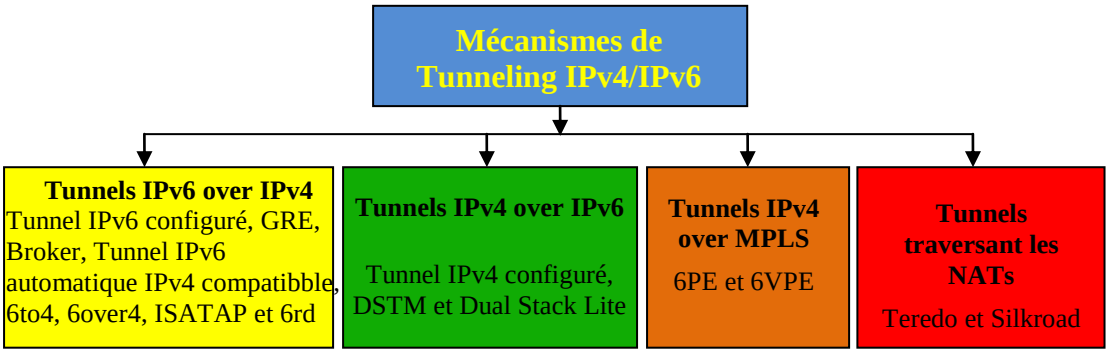


Figure 4.3 Classification des mécanismes de transition IPv4/IPv6 de la famille de Tunneling

IV.2.2.1 Catégorie 1 : Tunnels IPv6 over IPv4

Les tunnels IPv6 over IPv4 sont utilisés pour permettre à des hôtes/sites IPv6 de communiquer entre eux en traversant une infrastructure IPv4. Différents mécanismes de tunneling peuvent être utilisés pour cette raison: tunnel IPv6 configuré, GRE, Broker, tunnel IPv6 automatique IPv4-compatible, 6to4, 6over4, ISATAP et 6rd. **[12]**

IV.2.2.1.1 Tunnel Broker

Le Tunnel Broker est une société tierce fournissant un service de tunnel après une simple demande aux serveurs dédiés appelés « Tunnels Brokers » qui gèrent les demandes de tunnel des utilisateurs. Pour ce faire, il faut généralement s'inscrire chez le tunnel broker, puis demander l'ouverture du tunnel. Alors, le tunnel broker va configurer un de ses routeurs afin de mettre en place le tunnel. Enfin, il enverra un script à exécuter sur la machine souhaitant utiliser le tunnel, pour configurer correctement les paramètres réseaux. La machine est alors connectée à l'IPv6 via le service du tunnel broker. Les étapes énumérées ci-avant sont illustrées à la Figure 4.4 ci dessous :

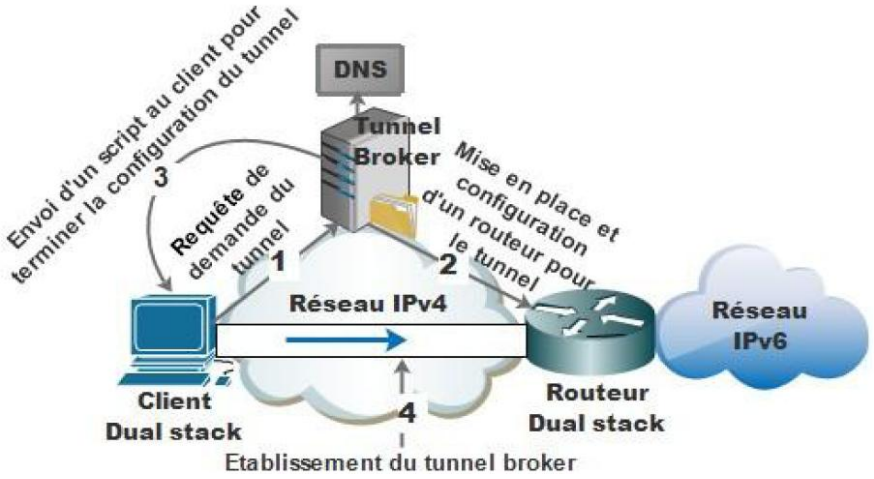


Figure 4.4 Tunnel Broker

Avantages :

- Bien adapté pour les petits sites IPv6 isolés et les machines IPv6 isolées sur l'internet IPv4, qui veulent se connecter à un réseau IPv6 existant
- Mise en place semi-automatique du tunnel après une inscription et demande du tunnel depuis le client
- Permet a des FAI (Fournisseurs d'Accès a Internet) IPv6 de gérer facilement les contrôles d'accès des utilisateurs, renforçant ainsi leur politique d'utilisation des ressources réseau.

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP
- Les performances dépendent de l'emplacement géographique du routeur du tunnel broker
- La sécurité car le routeur du tunnel broker doit accepter des modifications de configuration depuis un serveur distant. **[12]**

IV.2.2.1.2 6over4

Le mécanisme 6over4 permet à des machines IPv6 isolées, qui ne sont pas directement connectées à un routeur IPv6 mais connectées par un réseau IPv4 supportant le multicast, de communiquer entre elles en créant un réseau IPv6 local, comme si elles étaient situées sur le même lien (voir à la Figure 4.5 ci-dessous). Contrairement au tunnel configuré/tunnel automatique, 6over4 ne nécessite ni une configuration d'adresse, ni une adresse IPv6 IPv4- compatible. L'adresse IPv6 lien local d'une

machine utilisant le protocole 6over4 est créée automatiquement à partir de l'adresse IPv4 comme suivant: FE80::X.Y.Z.W ou l'adresse X.Y.Z.W est son adresse IPv4. L'adresse IPv4 du point final du tunnel est déterminée en utilisant le Neighbor Discovery.

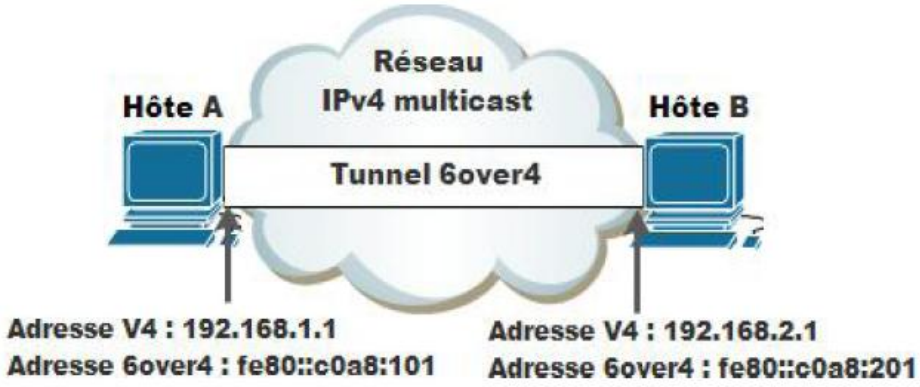


Figure 4.5 6over4

Avantages :

- Bien adapté pour les hôtes IPv6 isolés sur l'internet IPv4 qui ne sont pas directement connectés à des routeurs IPv6 et qui veulent se connecter entre eux à travers un réseau IPv4/multicast
- Ne nécessite ni configuration d'adresse, ni adresse IPv6 IPv4-compatible
- Base sur l'adresse lien local

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP
- Repose sur la disponibilité d'un réseau IPv4multicast
- Utilité pratique limitée (n'est pas pris en charge par les systèmes d'exploitation les plus courants) **[12]**

IV.2.2.1.3 ISATAP

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) est une autre technique de tunneling, conçue, pour une portée Intra-Site (Intranet), permettant à des nœuds IPv6 isolés dans des sites IPv4 d'obtenir une connectivité IPv6 via des tunnels automatiques IPv6 in IPv4 en utilisant l'infrastructure IPv4 existante, comme le montre la Figure 4.6 ci-dessous. Un hôte ISATAP obtient un préfixe de 64 bits depuis le serveur ISATAP, puis l'adresse ISATAP est formée de son propre identifiant d'interface comme suite: PrefixISATAPServer::5EFE:@IPv4(Hexa). Après cela les hôtes ISATAP peuvent se connecter les uns avec les autres via le tunnel IPv6 in IPv4 avec des adresses ISATAP.

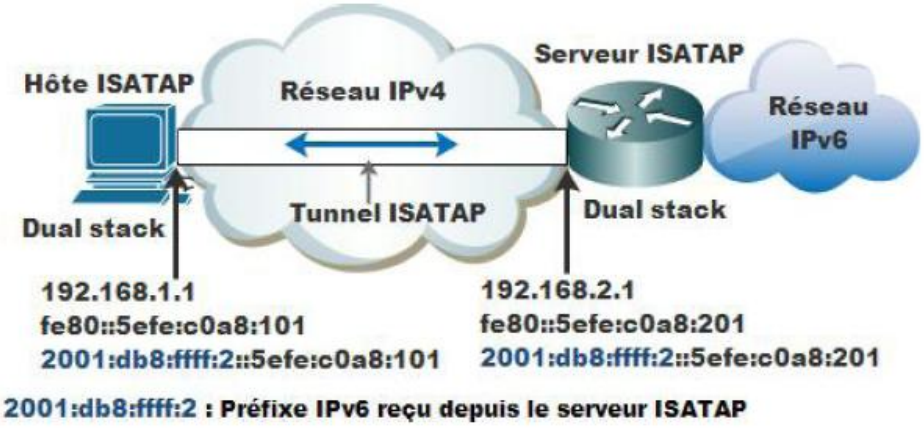


Figure 4.6 ISATAP

Avantages :

- Permettre à des machines IPv6 isolées dans des sites IPv4 Intranet de se connecter et d'échanger des contenus entre elles.
- Utile quand on a des machines/routeurs de notre réseau Intranet qui ne supportent pas IPv6
- Le routeur ISATAP peut faire le travail du serveur ISATAP si la fonctionnalité est intégrée de dedans (l'inverse du Teredo)

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP
- Utilité géographique limitée (portée Intra-Site)
- Ne supporte ni du NAT, ni du multicast **[12]**

IV.2.2.2 Catégorie 2 : Tunnels IPv4 over IPv6

Les tunnels IPv4 over IPv6 sont utilisés pour permettre à des hôtes/sites IPv4 de communiquer entre eux en traversant une infrastructure IPv6. Différents mécanismes de tunneling peuvent être utilisés pour cette raison: tunnel IPv4 configuré, DSTM et Dual stack Lite. **[12]**

IV.2.2.2.1 Tunnel IPv4 configuré

Le tunnel IPv4 configuré est assez similaire au tunnel IPv6 configuré. Il est utilisé pour la communication entre des hôtes/sites IPv4 à travers des réseaux IPv6 en encapsulant les paquets IPv4 dans des en-têtes IPv6, comme le montre la Figure 4.7 ci-après.

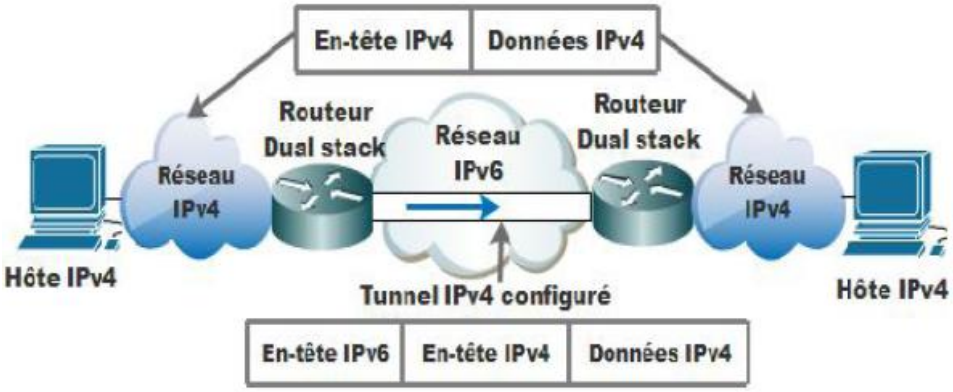


Figure 4.7 Tunnel IPv4 configuré

Avantages :

- Permettre à des machines IPv4 distantes et isolées sur l'internet IPv6 d'échanger des contenus entre elles.
- Simple à mettre en place en terme de configuration
- L'infrastructure centrale apporte les avantages d'IPv6 (efficacité, simplicité, sécurité)
- Idéal pour les petits réseaux

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP
- Nécessite une configuration manuelle aux deux extrémités du tunnel
- Ne supporte pas les grands réseaux (Solution n'est pas scalable). **[12]**

IV.2.2.3 Catégorie 3 : Tunnels IPv6 over MPLS

Les tunnels IPv6 over MPLS (Multi Protocole Label Switching) sont utilisés pour permettre à des hôtes/sites IPv6 de se connecter entre eux au travers d'un cœur de réseau IPv4/MPLS. La transmission de l'IPv6 over MPLS est basée sur des labelles au lieu des en-têtes IP. Deux mécanismes peuvent être utilisés pour cette raison : 6PE et 6VPE. **[12]**

IV.2.2.3 .1 6PE

Dans le mécanisme de transition 6PE (IPv6 on Provider Edge routers), l'infrastructure de base MPLS est IPv4 et les routeurs PE sont mis à jour pour supporter le dual stack et le 6PE. La transmission 6PE utilise des étiquettes ou lieu des entêtes IP. Elle a deux étiquettes: l'étiquette intérieure est limitée à l'annonce du préfixe IPv6 de destination, et l'étiquette extérieure est liée à l'adresse IPv4 de sortie du routeur 6PE, comme le montre la Figure 4.8 ci-dessous. L'accessibilité IPv6 est entre les dispositifs 6PE utilisant le Multi Protocol-iBGP (MP-iBGP). Ceci est une solution très rentable pour le déploiement de l'IPv6 avec des changements minimes sur le réseau IPv4/MPLS existant.

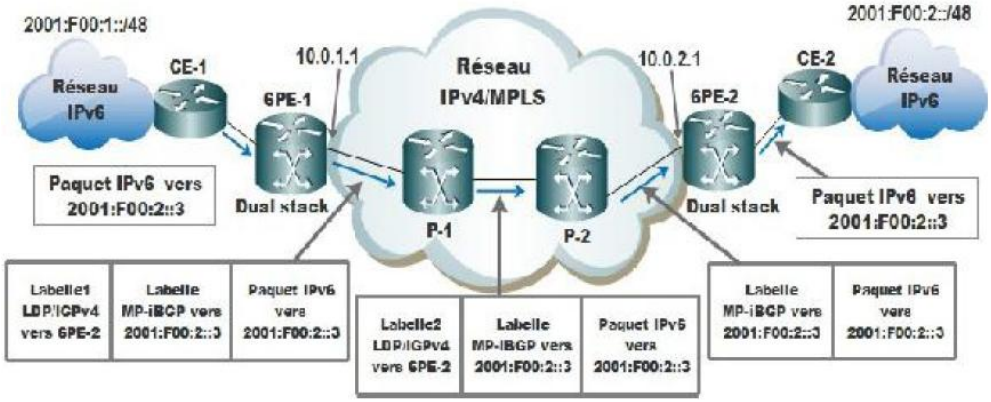


Figure 4.8 6PE

Avantages :

- Permettre à des hôtes/sites IPv6 distants et isolés sur l'internet IPv4 de communiquer et échanger des contenus entre eux
- Ne nécessite pas un upgrade du cœur (aucun impact sur les routeurs du cœur)
- Seuls les routeurs PE doivent être mis à jour et supporter 6PE
- Aucun tunnel n'est à configurer manuellement, ils sont établis automatiquement et re-routés dynamiquement en cas de panne.

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP
- Les paquets IPv6 ne sont pas transportés nativement par le réseau (cela peut être une exigence du client)
- Certaines fonctions peuvent ne pas être disponibles une fois le trafic encapsulé dans MPLS **[12]**

IV.2.2.4 Catégorie 4 : Tunnels traversant les NATs

Ce sont des tunnels permettant de fournir une connectivité IPv6 pour des nœuds résidant derrière un ou plusieurs NATs IPv4 en utilisant des mécanismes de tunneling IPv6 over IPv4 dans lesquels les paquets IPv6 sont encapsulés dans des paquets UDP puis dans IPv4. Différents mécanismes peuvent être utilisés pour cette raison : Teredo et Silkroad. **[12]**

IV.2.2.4.1 Teredo

Ce mécanisme permet aux nœuds situes derrière un ou plusieurs NATs IPv4 d'obtenir une connectivité IPv6 en encapsulant les paquets IPv6 dans des paquets UDP puis dans IPv4, comme illustré à la Figure 4.9 ci-dessous. L'hôte Teredo obtient d'abord un préfixe IPv6 à partir du Teredo Server, puis l'adresse IPv6 est formée comme suite: PrefixTeredoServer:Server IPv4:Flags:Port:client IPv4. La communication entre les clients Teredo peut être faite directement avec le tunnel IPv6 in UDP in IPv4. La connectivité vers le réseau IPv6 sera atteinte par le Teredo

Relay Gateway. Les tunnels automatiques entre les hôtes Teredo distribuent le trafic entre eux et partagent le Teredo Relay Gateway.

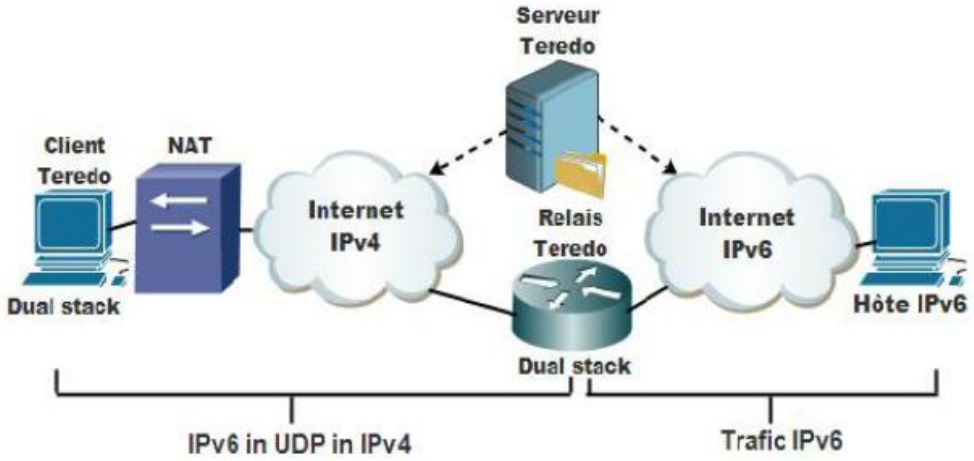


Figure 4.9 Teredo

Avantages :

- Permettre à des clients IPv4 (d'adresses IPv4 privées) résidant derrière un ou plusieurs NATs IPv4 d'obtenir une connectivité IPv6
- La capacité de traverser la plupart des NATs sur un ou plusieurs niveaux, en encapsulant les paquets IPv6 dans des paquets UDP puis dans IPv4

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP
- Le client Teredo ne peut faire le travail du serveur Teredo, ils doivent être séparés (l'inverse de l'ISATAP)
- Ne traverse pas les NATs symétriques **[12]**

IV.2.3 Famille 3 : Translation

Les mécanismes de translation ont été développés pour la communication entre des hôtes/applications IPv4 et IPv6. Plusieurs mécanismes peuvent être utilisés pour cette raison : NAT-PT/DNS-PT, NAPT-PT, NAT64 /DNS64, SIIT , BIS, BIA, BIH, SOCKS64, Dual Stack ALG, Reverse Proxy et TRT. Parmi ces mécanismes il y'a ceux qui font la translation au niveau de la couche réseau, ceux qui font la translation au niveau de la couche application et ceux qui font la translation au niveau de la couche transport. Par conséquent ces mécanismes peuvent être divisés en 3 catégories : mécanismes de translation de la couche réseau, mécanismes de translation de la couche application et mécanismes de translation de la couche transport comme on peut le voir à la Figure 4.10 ci-dessous : **[12]**

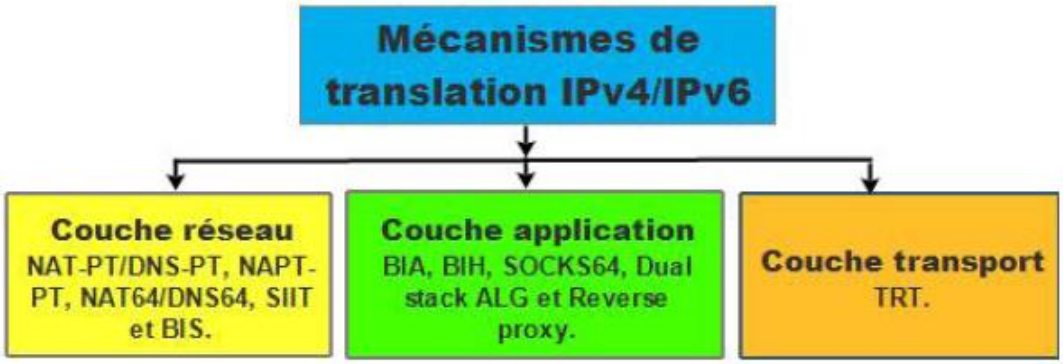


Figure 4.10 Classification des mécanismes de transition IPv4/IPv6 de la famille Translation

IV.2.3.1 Catégorie 1 : Translation de la couche réseau

IV.2.3.1.1 NAPT-PT

NAPT-PT (Network Address Port Translation-Protocol Translation) prend la traduction des adresses IP d'une étape supplémentaire en ajoutant le numéro du port, comme le montre la Figure 4.11 ci-après. C'est un cas particulier du NAT dynamique. Les ports TCP et UDP des nœuds IPv6 sont convertis en des ports TCP et UDP d'adresses IPv4. Cela permet aux ports TCP et UDP d'un certain nombre d'utilisateurs privés d'être multiplexés dans des ports TCP et UDP d'une seule adresse externe.

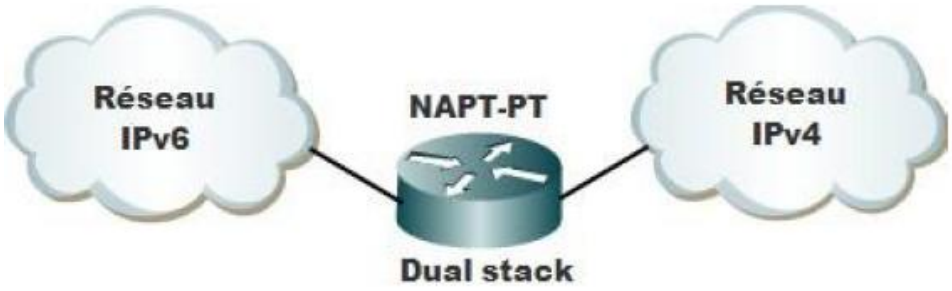


Figure 4.11 NAPT-PT

Avantages :

- Résout le problème de la pénurie d'adresses IP à court terme par rapport à NAT-PT
- Permettre à des hôtes IPv4/IPv6 de se connecter entre eux
- Ajoute des numéros de ports (une seule adresse externe)

Inconvénients :

- Malgré l'utilisation d'une seule adresse publique externe avec l'ajout des numéros de ports, NAPT-PT ne peut pas résoudre le problème de la pénurie des adresses IP à long terme
- Augmente les coûts en termes de performance et d'utilisation CPU du fait que toutes les demandes/réponses relatives à une session sont acheminées via le même routeur NAPT-PT.
- La sécurité de la couche réseau n'est pas possible, car IPsec (Internet Protocol Security) est intégré par défaut en IPv6 (l'inverse en IPv4) **[12]**

IV.2.3.2 Catégorie 2 : Translation de la couche application

IV.2.3.2.1 Dual stack ALG

Dual Stack Application Level Gateway est un dispositif IP qui fonctionne à double piles et peut être accessible à la fois en IPv4 et IPv6. Comme son nom l'indique, un ALG est actif à la couche application du modèle OSI, et peut être utilisé pour effectuer la traduction entre IPv6 et IPv4. Pour ce faire, il inspecte les paquets, et s'ils sont conformes aux règles établies, l'ALG remplaces les adresses et numéros de ports IPv4 par de l'IPv6, et inversement, comme on peut le voir à la Figure 4.12 ci-dessous. Des serveurs dual stacks sont utilisés comme des proxys pour exécuter le protocole de traduction par application (http, ftp, smtp, etc).

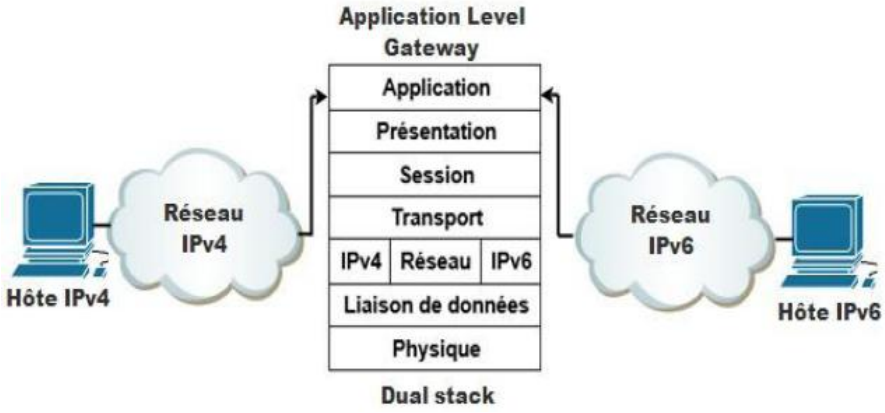


Figure 4.12 Dual stack Application Level Gateway

Avantages :

- Permettre à des nœuds IPv4/IPv6 d'échanger des informations entre eux.
- Très peu d'adresses IPv4 sont nécessaires (elles ne sont nécessaires que pour les proxys).
- Pas besoin de faire migrer les applications IPv4 vers IPv6 ou inversement.

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP.
- Incapable de prendre en mesure la gestion de tous les services, en particulier ceux qui fonctionnent de bout en bout.
- Implémentation dépendant du protocole de la couche application qui sera pris en charge. **[12]**

IV.2.3.3 Catégorie 3 : Translation de la couche transport

IV.2.3.3.1 TRT

Le mécanisme TRT (Transport Relay Translator) fonctionne sur la couche de transport du modèle TCP/IP. Il permet à des hôtes IPv6 d'échanger du trafic TCP et UDP avec des hôtes IPv4 en traduisant le TCP over IPv6 en TCP over IPv4 et inversement, comme on peut le voir à la Figure 4.13 ci-dessous. Le mécanisme TRT fonctionne de la même manière pour le trafic UDP. Le système TRT peut être situé sur un hôte dual stack ou un routeur.

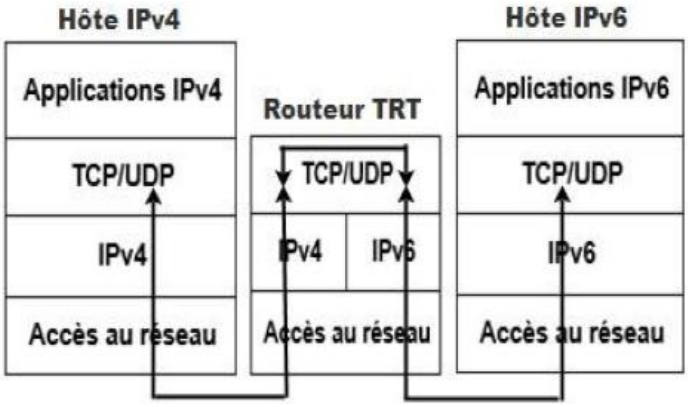


Figure 4.13 TRT

Avantages :

- Solution pour des hôtes IPv4/IPv6 qui veulent communiquer et échanger des informations entre eux.
- Pas besoin de faire migrer les applications IPv4 vers IPv6 ou inversement.
- Ne nécessite aucune modification supplémentaire sur les hôtes IPv4/IPv6 uniquement initiateurs.

Certains mécanismes de translation nécessitent des modifications sur les hôtes IPv6 uniquement initiateurs ce qui limite les possibilités de déploiement.

- Les convertisseurs d'en-têtes IPv4/IPv6 doivent prendre soin du chemin MTU et des problèmes de fragmentation. TRT est libre de ce problème.

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP
- TRT prend en charge le trafic bidirectionnel seulement. Les convertisseurs d'en-têtes IPv4/IPv6 peuvent être en mesure de soutenir d'autres cas, tels que les datagrammes unidirectionnels multicast
- La sécurité, car IPsec ne peut pas être utilisé dans le système TRT **[12]**

IV.3 Application et simulation

Dans ce chapitre nous allons présenter la méthode de tunneling, on va créez un tunnel IPv6 via le réseau IPv4 via lequel le trafic IPv6 sera acheminé.
On va simuler la méthode en utilisant le logiciel de simulation graphique packet tracer.

IV.4 Présentation de logiciel de simulation packet tracer

Packet Tracer est un simulateur de réseaux dédié aux matériels Cisco *(entreprise californienne créée en 1984 spécialisée dans les équipements réseaux).*
C'est un outil gratuit qui permet de reproduire virtuellement un réseau et d'y simuler le comportement de différents protocoles.
L'avantage majeur de Packet Tracer est qu'il évite de dépenser beaucoup d'argent dans des équipements CISCO qui coûtent très chers, et de pouvoir manipuler et tester, comme dans un environnement réel.

IV.5 Installation de Packet Tracer

Pour commencer, nous avons installé le logiciel (Cisco Packet Tracer) sur notre pc (Windows 7 64 bits) et pour ça nous avons suivi les étapes suivantes :
Avec une double clique sur le fichier source PacketTracer 6.2, on aura la Figure 4.14

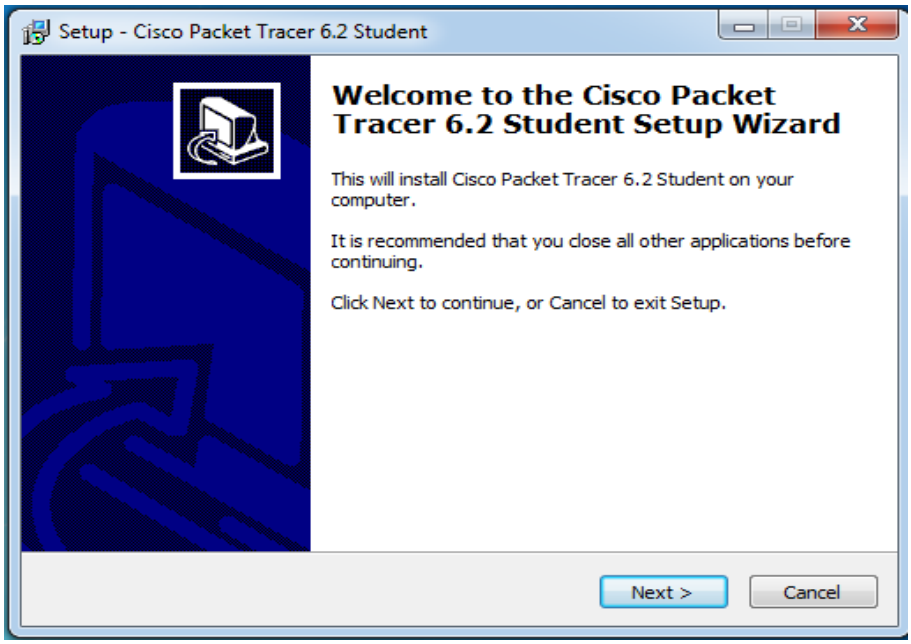


Figure 4.14 Présentation de la première étape de l'installation du logiciel

En cochant la case (I accept the agreement) puis en cliquant sur **Next** (figure 4.15) à chaque fois qui apparaître puis sur install jusqu'à la fin de l'installation en obtiendra une icône de raccourcis de packet tracer sur le bureau (figure 4.17)

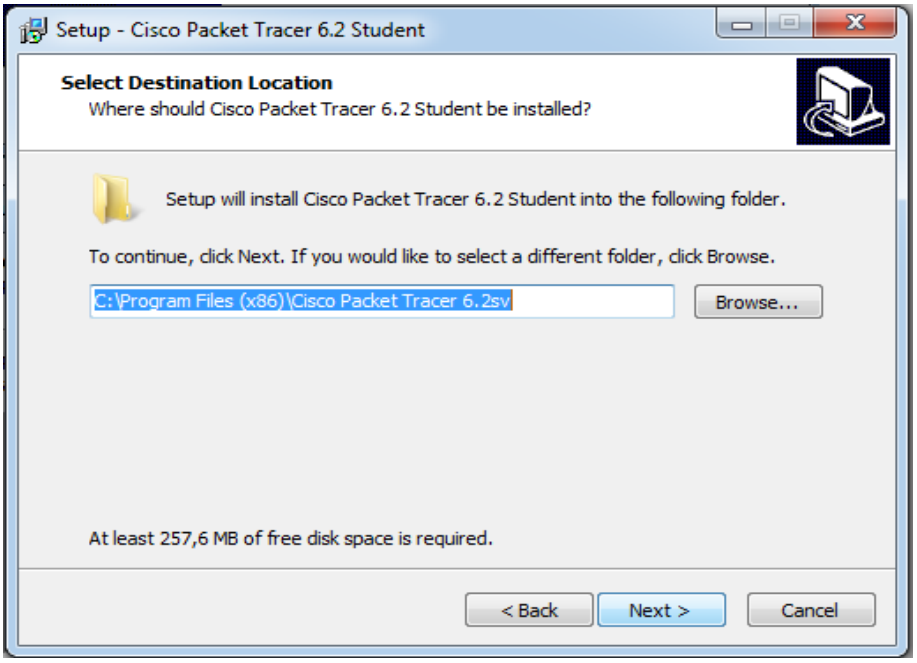


Figure 4.15 Présentation de la deuxième étape de l'installation du logiciel

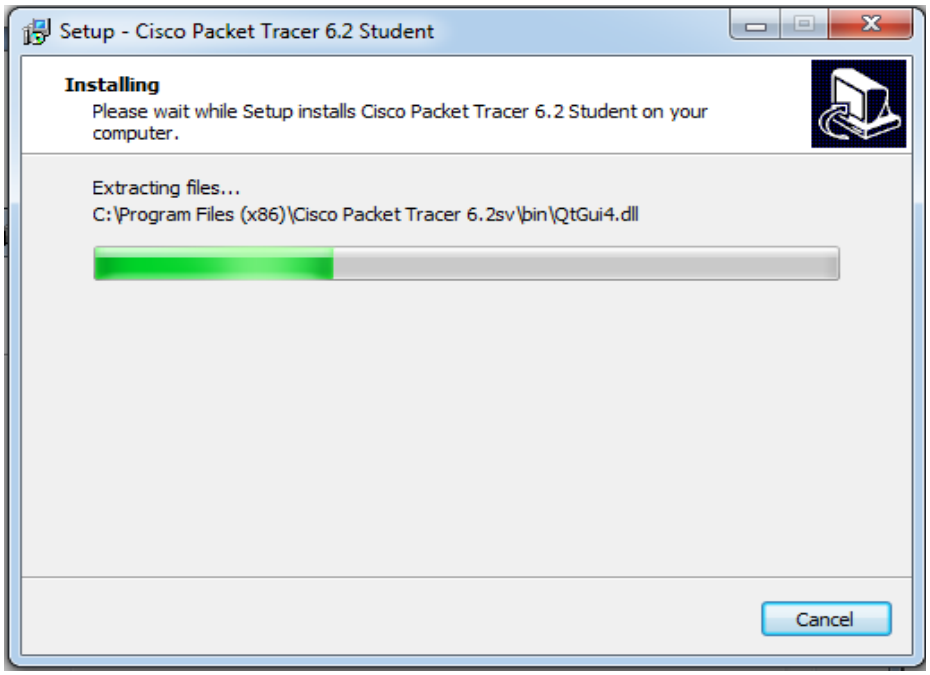


Figure 4.16 Présentation de l'installation du logiciel

Figure 4.17 Icône de raccourcis de packet Tracer

Après l'exécution, la fenêtre de packet tracer s'affichera (figure 4.18)

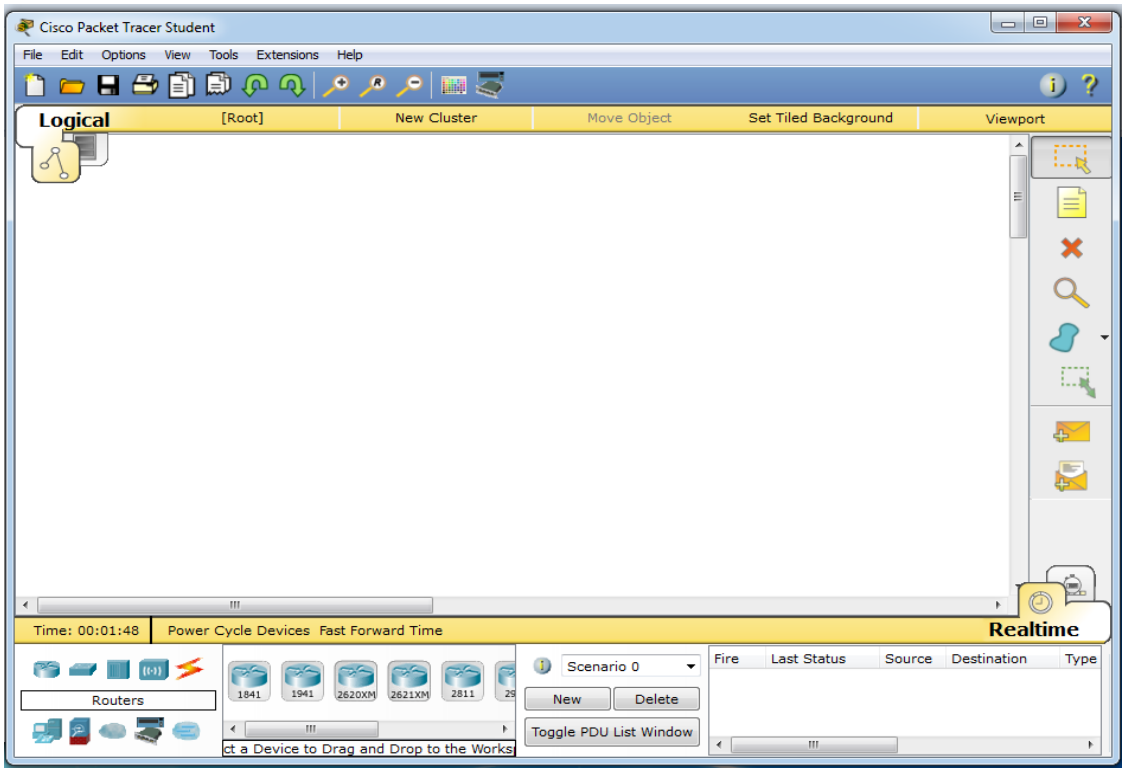


Figure 4.18 Fenêtre de Packet Tracer v.6.2

IV.9 La topologie utilisée

Nous allons réaliser une topologie avec utilisation de protocole de routage dynamique EIGRP.
Le schéma suivant illustre la topologie que nous avons mise en place pour l'implémentation de cette technique :

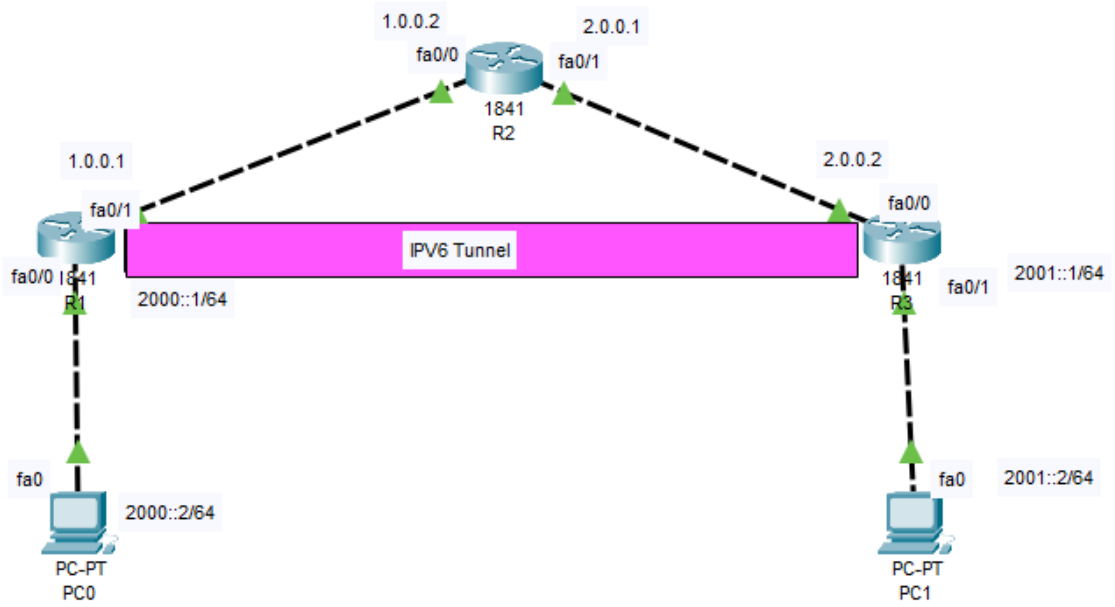


Figure 4.19 Présentation de la topologie utilisée**.**

On a utilisé trois routeurs cisco1841 et deux PCs PC0 et PC1 pour réaliser les tests ou bien la simulation. On a procédé comme suit :

Sélectionner les routeurs cisco1841 (R1, R2 et R3)

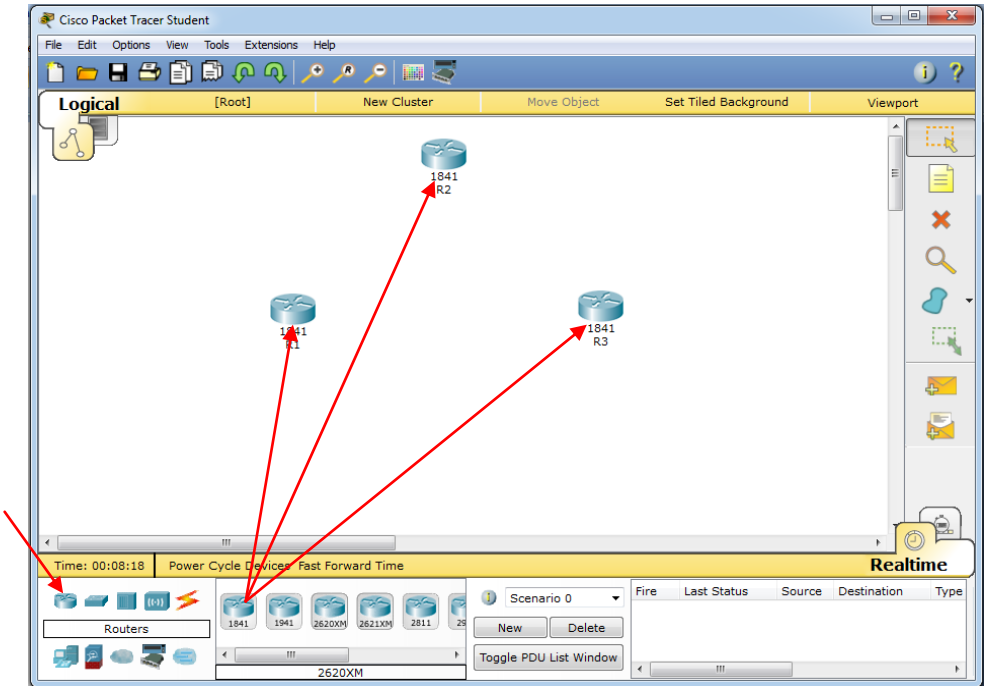


Figure 4.20 : Présentation des routeurs sur packet tracer**.**

Sélectionner les PCs PC0 et PC1 :

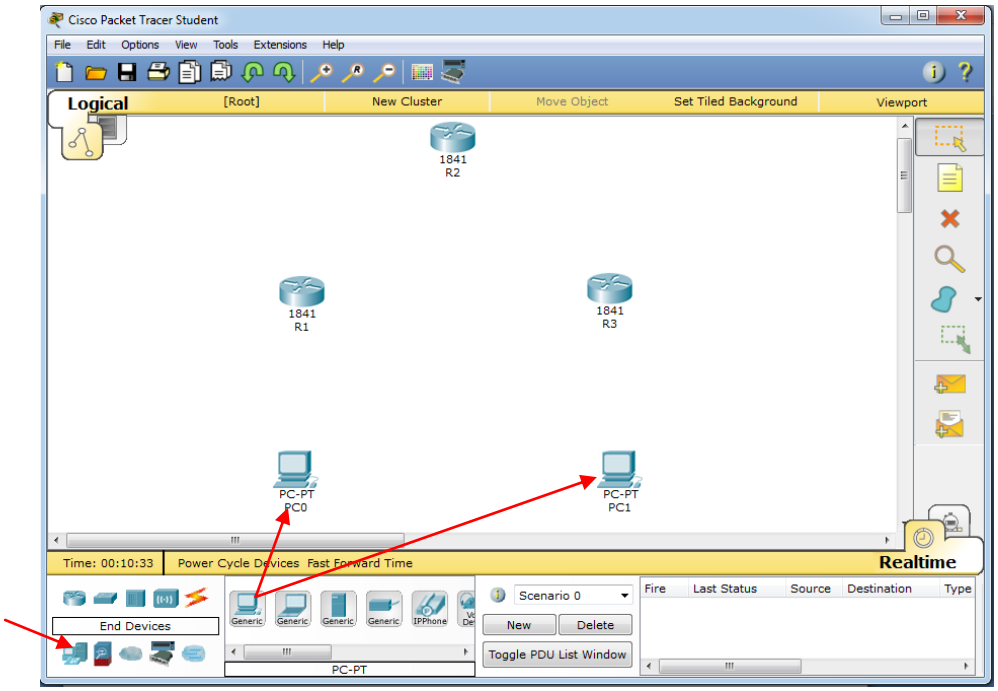


Figure 4.21 Présentation des PCs sur packet tracer

Puis on va faire connecter tous les équipements comme le montre la figure suivante :

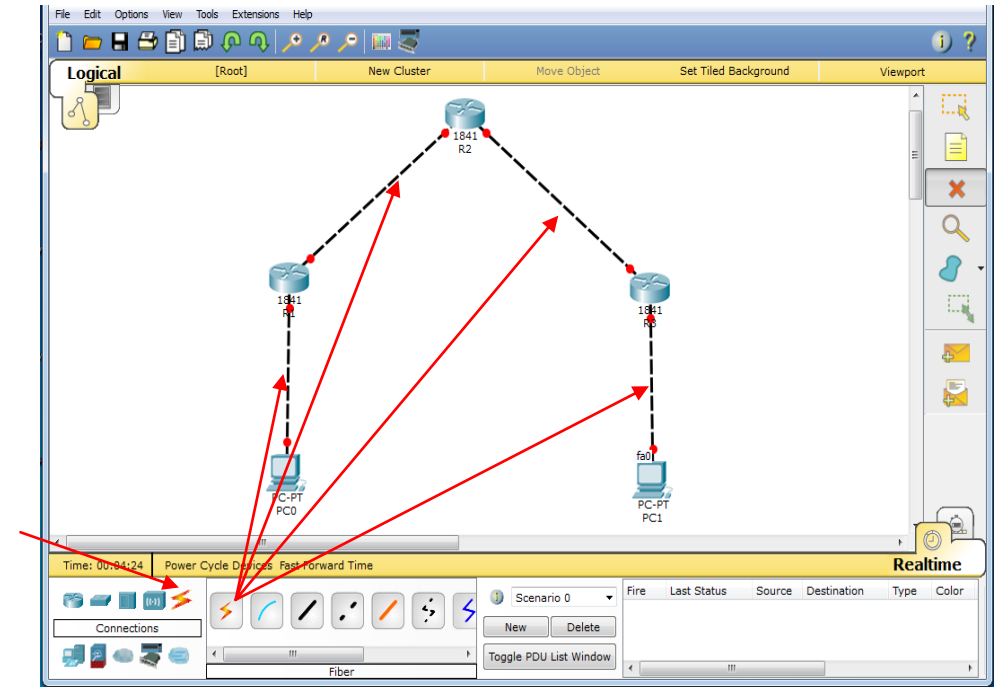


Figure 4.22 Présentation des équipements connectés

IV.7 La configuration des équipements

Pour configurer le tunneling ipv6 vers ipv4, nous devons d'abord créer une interface de tunnel sur chaque routeur de périphérie à double pile.
La configuration des équipements de ce réseau et comme suite :

- **Le routeur R1**

La fenêtre de configuration du routeur va s'ouvrir en Mode Utilisateur

```
Router>
```

En passant vers le mode Utilisateur privilégié

```
Router>enable
```

En passant vers le mode configuration globale

```
Router#config t
```

On renomme notre routeur

```
Router(config)#hostname R1
```

On configure l'adresse IPv6 sur le routeur R1:

```
R1(config)#ipv6 unicast-routing
R1(config)#int fa0/0
R1(config-if)#ipv6 add 2000::1/64
```

Allumer l'interface

```
R1(config-if)#no shut
```

On configure l'adresse IPv4 sur le routeur R1:

```
R1(config)#int fa0/1
R1(config-if)#ip add 1.0.0.1 255.0.0.0
```

Allumer l'interface

```
R1(config-if)#no shut
```

On configure EIGRP sur le routeur R1

```
R1(config-if)#router eigrp 1
R1(config-router)#network 1.0.0.0 0.255.255.255
R1(config-router)#
```

On crée un tunnel sur le routeur R1

```
R1(config)#int tunnel 0
R1(config-if)#tunnel source fa0/1
R1(config-if)#tunnel destination 2.0.0.2
R1(config-if)#tunnel mode ipv6ip
R1(config-if)#ipv6 address 2010::2/64
```

On configure la route statique IPv6 sur le routeur R1:

```
R1(config)#ipv6 route 2001::/64 2010::1
```

- **Le routeur R2**

```
Router>enable
Router#config t
Router(config)#hostname R2
R2(config)#int fa0/0
R2(config-if)#ip add 1.0.0.2 255.0.0.0
R2(config-if)#no shut
R2(config)#int fa0/1
```

```
R2(config-if)#ip add 2.0.0.1 255.0.0.0
R2(config-if)#no shut
```

On configure EIGRP sur le routeur R2

```
R2(config)#router eigrp 1
R2(config-router)#network 1.0.0.0 0.255.255.255
R2(config-router)#network 2.0.0.0 0.255.255.255
```

- **Le routeur R3**

```
Router>enable
Router#config t
Router(config)#host R3
R3(config)#ipv6 unicast-routing
R3(config)#int fa0/1
R3(config-if)#ipv6 add 2001::1/64
R3(config-if)#no shut
R3(config)#int fa0/0
R3(config-if)#ip add 2.0.0.2 255.0.0.0
R3(config-if)#no shut
```

On configure EIGRP sur le routeur R3

```
R3(config)#router eigrp 1
R3(config-router)#network 2.0.0.0 0.255.255.255
```

On crée un tunnel sur le routeur R3

```
R3>enable
R3#config t
R3(config-if)#int tunnel 0
R3(config-if)#tunnel source fa0/0
R3(config-if)#tunnel destination 1.0.0.1
R3(config-if)#tunnel mode ipv6ip
R3(config-if)#ipv6 address 2010::1/64
```

On Configure la route statique Ipv6 sur le routeur R3

```
R3(config)#ipv6 route 2000::/64 2010::2
```

- **Configuration des PCs**

Il nous reste à configurer les hôtes. Il suffit d'introduire les adresses IPv6 pour les deux PCs. Nous donnons, comme le montre les figures IV.11 et figure IV.12 l'adresse 2000::2 et 2000 ::1 passerelle par défaut pour PC0 et 2001 ::2 et 2001 ::1 passerelle par défaut pour PC1.

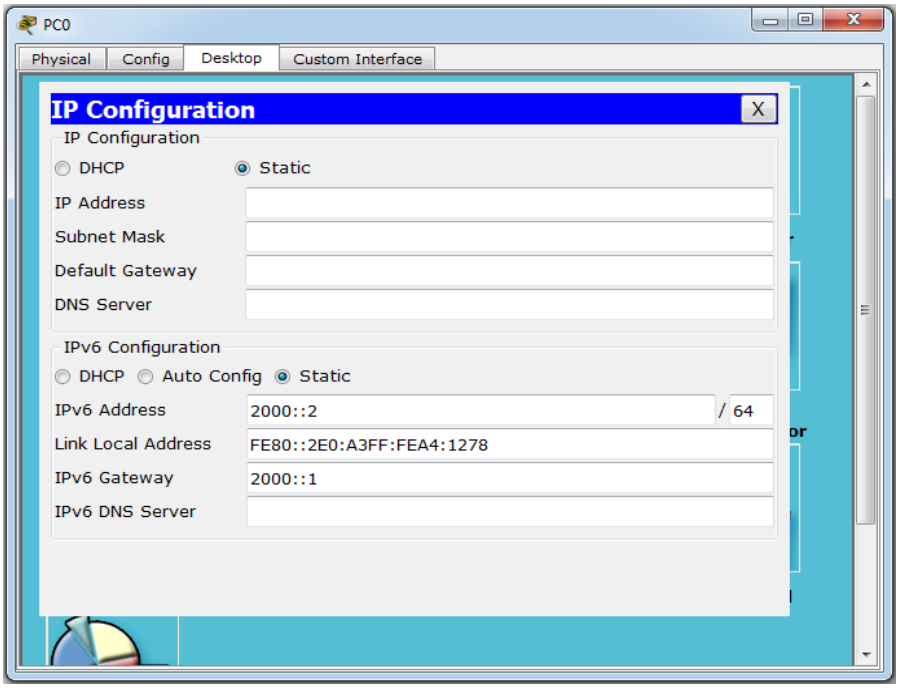


Figure 4.23 Configuration de PC0

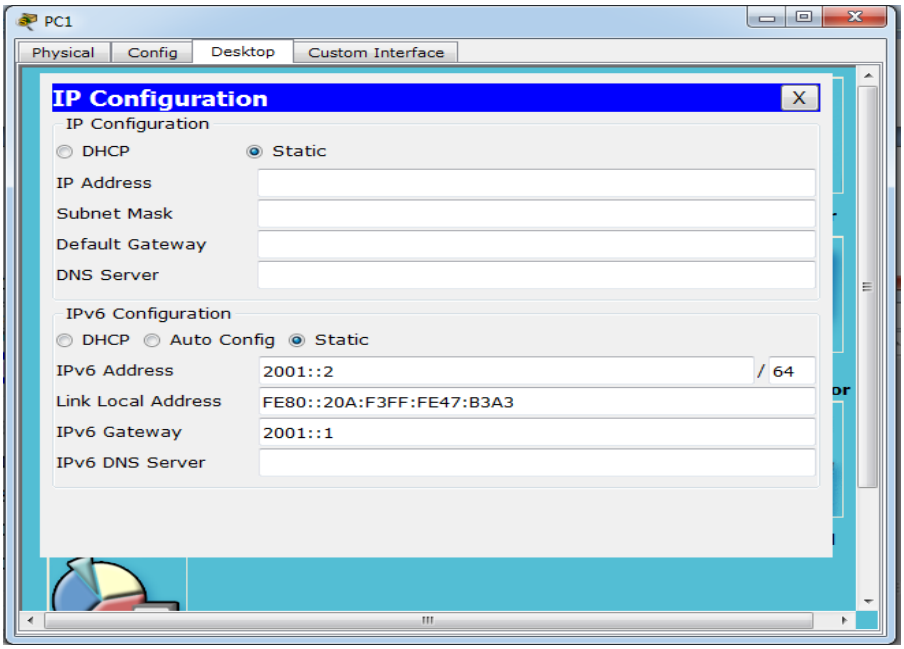


Figure 4.24 Configuration de PC1

V.8 Vérification de connectivité

En teste maintenant la communication entre les deux PCs. Pour ce faire, nous utilisons la commande **ping** Pour faire le teste en cliquant sur pc1 puis sur **command prompt**, en écrit :
PC>ping 2000::2
Et nous allons voir est ce que le tunnel fonctionne malgré la discontinuité de l'adressage IPv6 par les réseaux IPv4 utilisés par le Routeur R2.

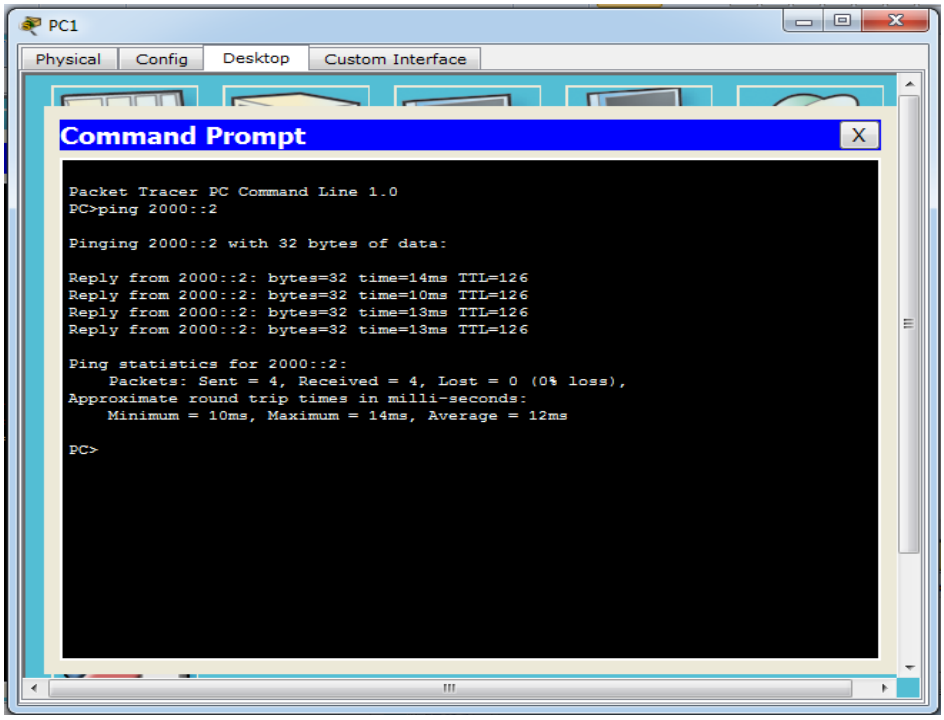


Figure 4.25 teste de communication entre les deux PCs

Nous allons tester la connectivité entre 2 hôtes IPv6 en exécutant la commande **tracert** sous PC0 vers le PC1.

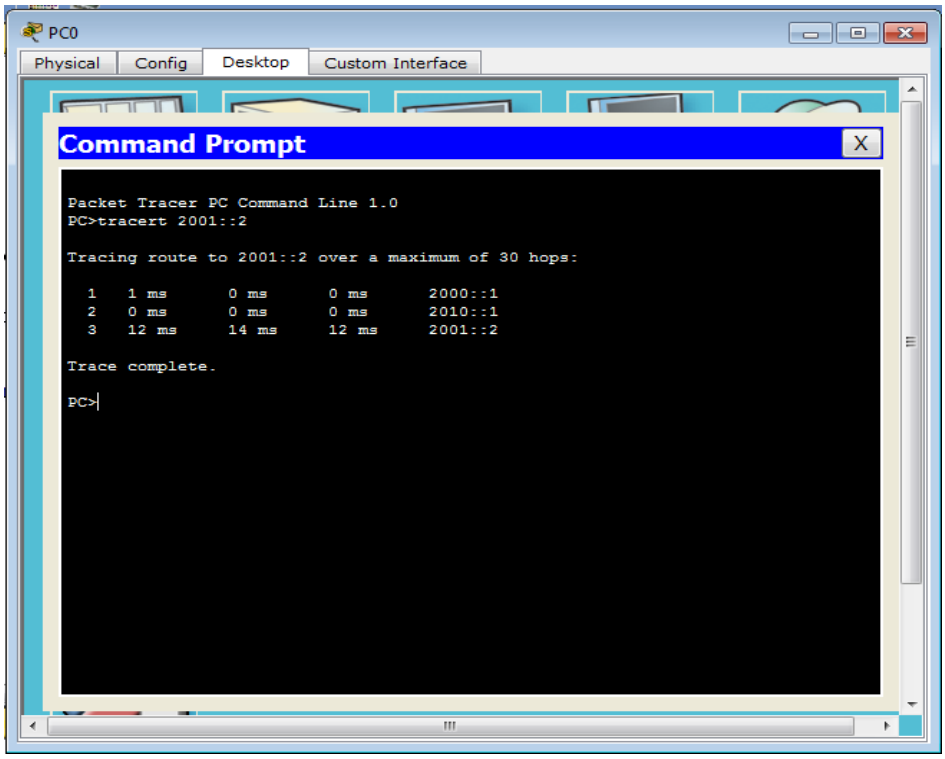


Figure 4.26 teste de connectivite entre les deux pcs avec la commande **tracert**

En Exécutant maintenant la commande **tracert** à partir de PC1

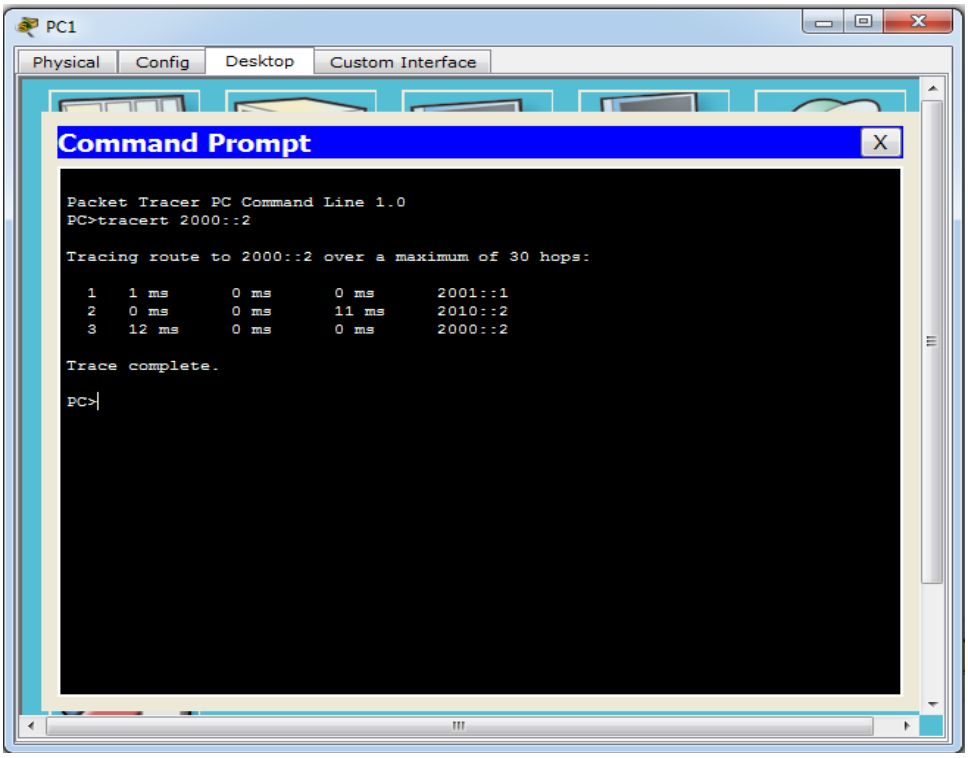


Figure 4.27 teste de connectivite entre les deux pcs avec la commande **tracert**

Ce teste indique bien que l'on passe par le tunnel.
Maintenant, voyant la route du routeur R1:

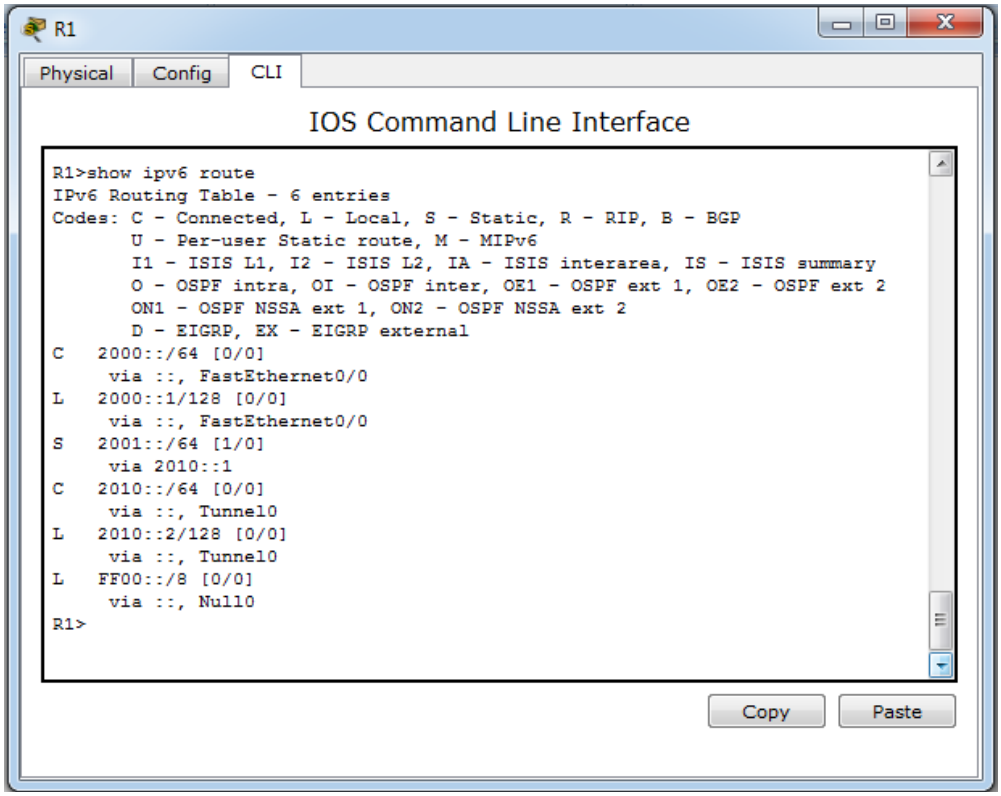


Figure 4.28 la route du routeur R1

Voyant la table de routage IPv4 du routeur R1:

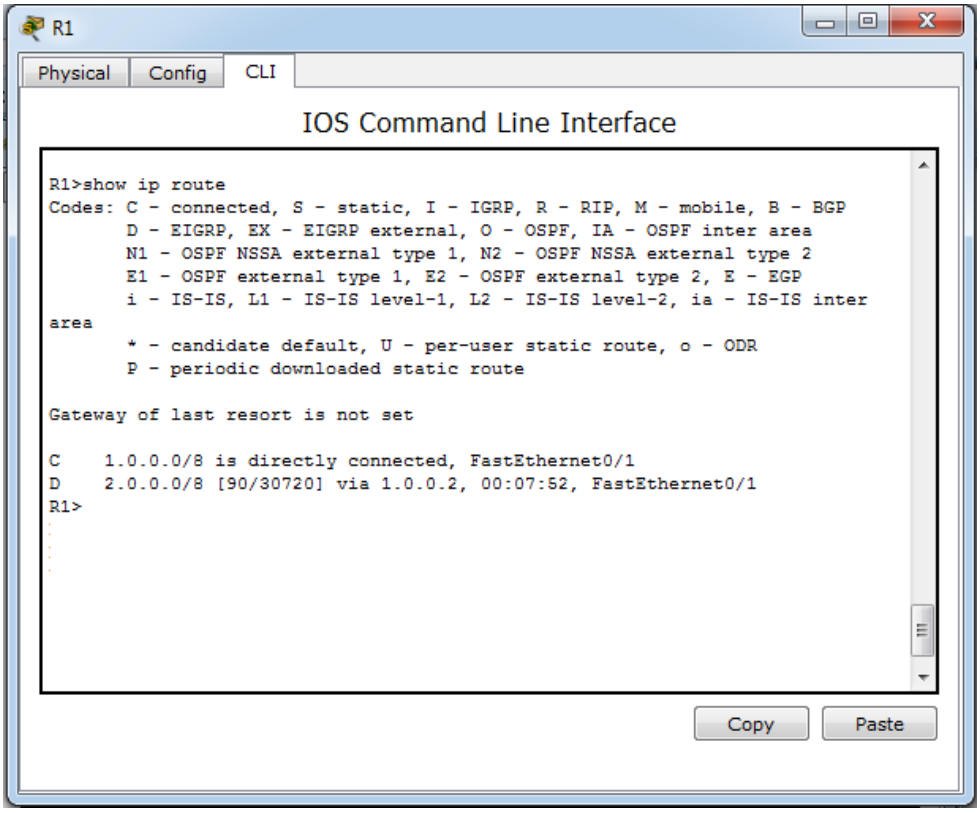


Figure 4.29 la table de routage IPV4 du routeur R1

IV.9 Conclusion

Nous remarquons que le teste à confirmer la fonctionnalité du tunnel réalisé.
Nous avons utilisé le logiciel de simulation Packet tracer avec lequel nous avons réussi à faire réaliser le tunnel qui nous permet de connecter un réseau IP version 4 avec un réseau IP de version6.
La méthode de tunneling est considérée comme une méthode de transport de paquets IPv6 à travers un IPv4 dans un réseau unique.

Conclusion générale

Durant mes études de l'ingéniorat en électronique et mes expériences dans les domaines électronique et informatique, ce mémoire m'a éclairé dans le domaine de l'informatique, notamment dans les réseaux informatique de connaitre les différents réseaux informatiques, comment fonctionne l'internet, connaitre les deux modèles de référence OSI et TCP/IP, les différents types de services réseaux, c'est quoi un adressage et un routage, les différents méthodes pour que les machines IPv4 et IPv6 de cohabiter et de communiquer entre elles, de configurer et de tester un routeur et un pc sur un réseau, et de maitriser un des logiciels de simulation virtuelle d'un réseau le « packet tracer ».

Vu le nombre important des méthodes de la migration, j'ai essayé de présenter au moins une méthode de chaque catégorie.

Dans le dernier chapitre j'ai réussi à faire simuler le tunnel qui nous permet de connecter un réseau IP4 avec un réseau IP6, et nous avons vue comment les machines IPv4 et IPv6 ce cohabiter et ce communiquer entre elles sans changer les machines ipv4 par ipv6.

Le protocole IPv6 possède une capacité d'adressage plus importante. Ainsi il permet d'avoir une meilleure construction du réseau Internet pour répondre à une demande croissante des parcs informatiques et des terminaux mobiles (téléphone, GPRS, WLAN).

L'opération de migration des réseaux IPv4 vers IPv6 n'est pas facile à mettre en pratique. Cependant, elle est nécessaire pour la mise en cohabitation aux réseaux de protocoles différents.

De manière générale, la cohabitation IPv4/IPv6 est nécessaire afin de pouvoir accéder à l'ensemble des sites Internet. La double pile doit alors être appliquée au routeur de sortie jusqu'à ce que l'ensemble des réseaux mondiaux ait fait leur transition vers IPv6.

En outre, notre étude révèle qu'il n'existe pas une solution unique pour résoudre le problème de la transition entre IPv4 et IPv6. Les solutions varient selon les besoins et les exigences des utilisateurs. Différents mécanismes de transition peuvent être appropriés pour différents exigences en différents réseaux à différents points, mais il n'existe pas de solution unique et universelle répondant aux besoins de tous les clients.

Bibliographie

[1] TCP IP Apprendre le fonctionnement des réseaux ; ERIC Lalitte 3e Edition EYROLLES.

[2] : Internet: Services et Réseaux - Cours, exercices corrigés et QCM ; Dominique Présent, Stéphane Lohier Edition DUNOD

[3] : Réseaux et Transmissions ; Stéphane Lohiet et Dominique Présent, Edition DUNOD 6e édition

[4] : Tout sur les réseaux et internet, 2e édition (jeaun françois PILLOU/fabrice LEMANOIQUE) , Edition DUNOD.

[5] : Architecture des réseaux; (Danièle Dromard et Dominique Seret), collection Synthex

[6] URL: https://www.frameip.com/tcpip/ Consulté le 14/05/2020

[7] URL: https://fr.wikipedia.org/wiki/Bootstrap_Protocol Consulté le 26/05/2020

[8] Etude et simulation d'un réseau de téléphonie sur IP (TOIP) mémoire de fin d'étude présenté par TAHRA Zahia 2008 pour l'obtention du Diplôme d'ingénieur d'état en Informatique Option : Informatique Industrielle

[9] Proposition de solution de sécurité pour le Réseau local de l'hôpital d'Amizour: Fares KHELOUFI et Yacine IKHLEF (2015) Université Abderrahmane Mira de Béjaïa

[10] URL: https://baptiste-wicht.developpez.com/tutoriels/reseau/introduction/?page=7 Consulté le 05/09/2020

[11] URL: https://sites.google.com/site/grivelstudies/home/module1/chapitre-7 Consulté le 01/09/2020

[12] Article Etude comparative des mécanismes de transition de l'IPv4 à l'IPv6 : Article · Janvier 2017, 04 auteurs : Khalid el Khadiri, Najib EL KAMOUN, Ouidad Labouidya, Hilal Rachid de l'Université Chouaib Doukkali, Maroc

[13] URL: ww2.ac-poitiers.fr/electronique/sites/electronique/IMG/doc/Cours_reseaux-Modele_OSI-TCP-IP.doc Consulté le 14/05/2020

[14] URL: http://www.zeitoun.net/articles/les_protocoles_reseaux/start Consulté le 16/05/2020

[15] URL: https://fr.wikipedia.org/wiki/Enhanced_Interior_Gateway_Routing_Protocol Consulté le 15/09/2020