République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

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

Mémoire de fin d'études
De MASTER ACADEMIQUE

Domaine**: Sciences et Technologies**
Filière**: Génie électrique**
Spécialité**: Réseaux et Télécommunication.**

Thème :

MIGRATION IPV4 VERS IPV6 AVEC LA METHODE DE TUNNEL ISATAP

Proposé et encadré par :
Mme : LAHDIR .L

Présenté par :
BOURFIS SAFIA

CHERGUI FARIDA

Les membres de jury :

OUALOUCHE FETHI (Président) [MA/A].

ALOUACHE DJAMEL (Examinateur) [MA/B].

LAZRI MOURAD (Examinateur) [MC/B].

LAHDIR LEILA (Encadreur) [MA/B].

Promotion: 2014/2015

Remerciement

Nous tenons à remercier tout d'abord DIEU le tout puissant qui nous a donnée, durant toutes ces années, la santé, le courage pour arriver à ce jour.

Nous ne pouvons, réellement, trouver les expressions éloquentes que mérite notre promotrice Mme. LAHDIR. LEILA qui a acceptée de diriger notre travail, afin de la remercier pour sa sympathie, ses encouragement, son aide, ses précieux conseils , et sa présence totale, au cour de ce modeste travail.

Nous adressons nos remerciements aux membres de jury qui nous ont fait l'honneur de juger, d'examiner, et d'enrichir notre modeste travail.

Nos remerciements vont également à tous les enseignants et les responsables de notre département.

Sans oublier à remercier tous ceux qui nous ont aidés, conseillés et encouragés à fin de réaliser ce modeste travail.

Dédicace

Je dédie ce modeste travail à :

- Mes très chers parents (longue et belle vie inchaa allah avec beaucoup de santé).
- Mes chers frères : RACHID et MUSTAPHA et leurs familles.
- Mes chères sœurs : NORA, DJAMILA, NACERA et leurs familles.
- Ma grande mère.
- Mes amies :SOUHILA, SAMIA , ZAHIA, KAHINA, SONIA , LYNDA…..
- Mon cher binôme : SAFIA.
- Tous ceux que j'aime et ceux qui m'aime.

.

FARIDA

Dédicace

Je dédie ce modeste travail à :

- Mes très chers parents (longue et belle vie inchaa allah avec beaucoup de santé).
- Mon fiancé
- Mes chers frères.
- Mes chères sœurs
- Ma grande mère.
- Mes amies
- Mon binôme : FARIDA.
- Tous ceux que j'aime et ceux qui m'aime.

.

SAFIA

Sommaire

Glossaire

Liste des figures

Liste des tableaux

Introduction générale.....2

Introduction.....3
I.1.Définition Réseau informatiques.....3
I.2. Intérêt d'un réseau informatique.....3
I.3.Les différents types du réseau.....4
a)Type du réseau selon l'étendu.....4
b) Type du réseau selon l'architecture.....5
I.4.Les Topologies réseaux.....7
I.5.Les équipements d'interconnexion.....9
I.6.La transmission des données.....11
I.7.Le modèle OSI.....16
I.7.1.Les différentes couches du modèle.....17
I.8.Le modèle TCP/IP.....20
I.8.1.Les couches du modèle.....20
Discussion.....24

Chapitre II : L'adressage IPv4 et IPv6

Introduction.....25
II.1.Protocole IP version 4 (IPv4).....25
II.1.1.Définition.....25
II.1.2. Caractéristiques d'adressage IPv4.....25
II.1.2.1. En-tête de paquet IPv4.....25
II.1.2.2 Anatomie d'un adressage IPV4.....27
II.1.2.3.Adressesparticulières.....28
II.1.2.4.Masque des sous réseau.....29
II.1.3. Attribution des adresses.....29
II.1.3.1Attribution statique d'adresses.....29
II.1.3.2. Attribution dynamique d'adresses.....30
II.1.4.Limites des adresses IPv4.....30
II.2. Le protocole version 6 (IPv6).....31
II.2.1.Définition.....31
II.2.2. Caractéristiques d'adressage IPv6.....31
II.2.2.1. En-tête de paquet IPv6.....31
II.2.2.2. Adressage.....32
II.2.2.3. Masque de sous réseau.....35

II.2.3. Auto configuration des adresses IPv6 36
Discussion 36

Chapitre III : Les méthodes de migration

Introduction 37
III. Méthode de migration 37
III.1 La méthode DUAL-STACK (Double Pile) 37
III.2 La méthode de Translation..... 38
II1.2.1 - Translation statique 39
II1.2.2 - Translation dynamique 40
III.3 la méthode de Tunnel 41
III.3.1- Tunnel statique (manuel) 42
III.3.2.Tunnel semi-automatique (Tunnel BROKER) 42
III.3.3.Tunnel automatique 44
a. Tunnel Téredo 44
b. Tunnel 6over4..... 45
c. Tunnel 6to4..... 46
d. Intra-site automatic tunnel addressing protocol(ISATAP) 48
Discussion 48

Chapitre VI : Application et simulation

Introduction 49
VI.1.Définition de logiciel de simulation 49
VI.2.Installation 49
VI.2.1. Ajouter des IOS.....52
VI.2.1. Présentation de l'application 53
VI.3. Configuration des routeurs 55
VI.3.1. Configuration de routeur R1 56
VI.3.2.Configuration de routeur R3 58
VI.3.3. Configuration de Routeur R2 58
VI.4.Configuration des PCs Local2 et Local.....59
VI.5.Tests.....60
Discussion 61

Conclusion générale.....62

Références bibliographiques

Glossaire

ARPANET	Advanced Research Project Agency NETwork
BNC	British Naval Connector
DHCP	Dynamic Host Control Protocol
DHCPv6	Dynamic Host Control Protocol version 6
DNS	Domain Name Server
EIGRP	Enchanched Interior Gateway Routing Protocol
EUI	Extended Unique Identifier
FAI	Fournisseur d'Accès Internet
GNS3	Graphical Network Simulator
HTML	Hyper Text Markup Language
IETF	Internet Engeneering Task Force
IHL	Internet Header Lengh
IOS	Intenetwork Operating system
IP	Internet Protocol next generation
IPng	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Adressing Protocol
LAN	Local Area Network
MAC	Medium Access Control
MAN	Metropolitan Area Network
NAT	Network Address Translation
NAT-IP	Network Address Translation-Protocol Translation
OSI	Open System Interconnexion
OSPF	Open Short Path File
PC	Personal computer
RJ45	Registred jack
STP	shielded twisted pairs
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Time To Live

Glossaire

UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTP	Unshielded twisted pairs
WAN	Wide Area Network

Liste des figures

FigureI.1 : Réseau LAN 4
Figure I.2 : Réseau MAN 4
Figure I.3 : Réseau WAN 5
Figure I.4 : Architecture Client/serveur 6
Figure I.5 : Réseau Poste à Poste 6
Figure I.6 : Topologie en bus 7
Figure I.7: Topologie en étoile 8
Figure I.8 : La topologie en anneau 8
Figure I.9 : Equipements d'interconnection 9
Figure I.10 : Câble à paires torsadées avec connecteur RJ45 12
Figure I.11 : câble STP 12
Figure I.12 : Câble UTP 13
Figure I. 13 : câble coaxial avec connecteur BNC 13
Figure I.14 : Câble à fibre optique 14
Figure I.15 : liaison infrarouge 15
Figure I.16 : liaison hertzienne 16
Figure I.17 : le modèle OSI 17
Figure I.18: Les couches de modèle TCP/IP 21
Figure I.19: Encapsulation des données 21
FigureII.1 : Présentation de l'Entête lP 25
Figure II.2: Format d'en-tête IPv6 31
Figure III.1 : Schéma de dual-stack 37
Figure III.2 : Schéma de présentation de NAT-PT 39
Figure III. 3 : Scénario d'utilisation de méthode NAT-PT 41
Figure III.4 : Schéma d'un tunnel statique 42
Figure III.5 : Schéma d'un tunnel Broker 43
Figure III.6 : Schéma d'un tunnel Téredo 45
Figure III.7: Schema d'un tunnel 6to4 47
Figure III.8 : Schéma d'un tunnel ISATAP 48
Figure VI.1 : Présentation de la première étape de l'installation du logiciel 50
Figure VI.2 : Illustration des conditions appartienne au logiciel 50
Figure VI.3 : Présentation de fichier ou en peut installer le GNS3 51
Figure VI.4 : L'icône du logiciel GNS3 51
Figure VI.5 : Présentation de tous les dossiers qui forme GNS3 52
Figure VI.6 : L'ajout des IOS dans le répertoire de GNS3 52
Figure VI.7 : Création d'un dossier pour le fichier IOS 53
Figure VI.8 : Présentation de la topologie de réseau. 53
Figure VI.9 : Présentation des routeurs sur GNS3. 54
Figure VI.10 : Présentation des PCs sur GNS3. 54
Figure VI.11 : Présentation des équipements connectés 55
Figure VI.12 : Configuration de routeur R1 56
Figure VI.13 : Configuration de routeur R3 58
Figure VI.14 : Configuration de routeur R2 59
FigureVI.15 : Configuration du pc local2 59
Figure VI.16 : Configuration du pc local 3 ..... .60
Figure VI.17: Confirmation de fonctionnement de tunnel au niveau de local 2 ..... .60
Figure VI.18 : Confirmation de fonctionnement de tunnel au niveau de local 3 ..... .61

Liste des tableaux

Tableau II.1 : la signification des champs de l'En-tête IPv6. 32
Tableau II.2 : Présentation de la forme de quelques exemple d'adresse. 33
Tableau II.3 : Présentation d'un résumé de différent type d'adresse. 35
Tableau VI.1 : les commandes utilisées pour la configuration de R1.....57
Tableau VI.2 : les commandes utilisées pour la configuration de R2……...59

A la fin des années 60, le Département américain de la Défense décide de réaliser un grand réseau à partir d'une multitude de petits réseaux [1]. Il a fallu trouver le moyen de faire coexister ces réseaux et de leur donner une visibilité extérieure, la même pour tous les utilisateurs. D'où l'appellation d'Inter-Network (inter-réseau), abrégée en Internet.

L'architecture Internet se fonde sur une idée simple : demander à tous les réseaux qui veulent en faire partie, de transporter un type unique de paquet, d'un format déterminé par le protocole IP. Ce paquet IP doit transporter une adresse définie avec suffisamment de généralité pour pouvoir identifier chacun des ordinateurs et des terminaux dispersés à travers le monde.

La première version du protocole IP est le protocole IPv4. Actuellement, il est celui utilisé sur tous les réseaux, il a été conçu pour une communauté restreinte d'utilisateurs mais, depuis les années 80, Internet connaît un succès très important au-delà des prévisions les plus optimistes prévues lors de sa création. Les raisons de ce succès sont liées aux services variés offerts sur Internet et à l'architecture du protocole de communication IP utilisée. La majeure partie des entreprises y est maintenant directement connectée, le nombre de particuliers détenteurs d'un abonnement Internet auprès d'un FAI est en constante croissance. Avec l'explosion des besoins en services et en adressage des utilisateurs, le réseau a menacé d'atteindre la saturation et certains ont prédit son effondrement total en 1994. Comme toute prédiction de ce genre, elle s'est révélée fausse. Les ingénieurs et chercheures travaillant au sein de l'organisme de standardisation de l'internet ont conçu une nouvelle version de protocole, s'affranchissant des limites imposées par l'actuelle version. Pour éviter toute confusion, la version initial est désormais appelée IPv4 et la version issue de ces travaux été baptisée IPv6. Ses limites qui ont conduit à la conception d'adressage IPv6.

La version 6 d'IP a été introduite en 1998 par l'IETF[2] 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.

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.

Dans notre travail, nous nous sommes intéressés à la migration IPv4 vers IPv6 avec la méthode du tunnel ISATAP, nous allons utilisée le logiciel GNS3, tel que nous avons choisi une topologie de trois routeur(le 2 est configuré en IPV4, le 1 et le 3sont configurés en IPV 6) et deux PCs (sont configurés en IPV6), nous allons crée un tunnel de manière que le réseau IPV6 communique avec l' autre réseau IPV6 à travers un réseau IPV4, et pour cela, nous avons organisé notre mémoire en quatre chapitres. Dans le premier chapitre, nous allons défini c'est quoi le réseau informatique, ses

types et les différents équipements implémentés pour qu'il soit réalisé, puis nous allons cité les couches du modèle OSI, aussi celles du modèle TCP/IP. Dans le deuxième chapitre, nous étudierons l'adressage IP version4, ses caractéristiques, ses limites, puis nous passerons à l'étude de l'adressage IPv6 et ses caractéristiques. Le troisième chapitre sera consacré aux quelques méthodes de déploiement et de migration IPv4 vers IPv6. Et dans le dernier chapitre, nous allons simulé une de ces méthodes qui est la méthode ISATAP avec le logiciel GNS3.

Et, nous terminerons notre travail par une conclusion générale.

Introduction :

Grace à l'évolution des capacités réseaux, le traitement automatisé des informations a considérablement évolué depuis une quarantaine d'années. A la fin des années 60 [3]. Le département de la défense américaine a commencé le développement de protocoles et de matériels. En 1970 le réseau ARPANET voit le jour, ce qui constitue un premier point d'appui qui jouera un rôle essentiel dans le développent futur de l'internet.

I.1.Définition d'un réseau informatique : [1][4][5][6]

Un réseau informatique est un ensemble des moyens matériels et logiciels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques. Il permet à différentes machines d'accéder en commun à la plupart des ressources aussi efficacement que dans le cadre d'un système centralisé.

I.2. Intérêt du réseau informatique :

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

Un réseau informatique peut servir plusieurs buts distincts :

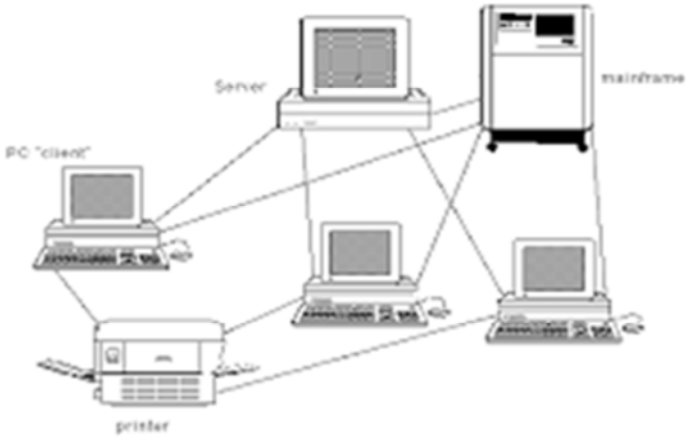
- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct, etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau)
- Diffusion multimédia (processus d'envoi de contenu multimédia numérique : photos, musique ou vidéos)
- Jeux en réseau (jouer avec d'autres personnes sur Internet).

I.3.Les différents types du réseau :

a)Type du réseau selon l'étendu :

a.1.Les réseaux locaux (LAN) :

Un réseau local ou encore LAN (Local Area Network) est un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une zone géographique restreinte (jusqu'à 10Km environ).



FigureI.1 : Réseau LAN

a.2.Les réseaux métropolitains (MAN) :

Les **MAN** (*Metropolitan Area Network, réseaux métropolitains*) interconnectent plusieurs LAN au niveau d'une ville ou d'une région (au maximum quelques dizaines de kilomètres). Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

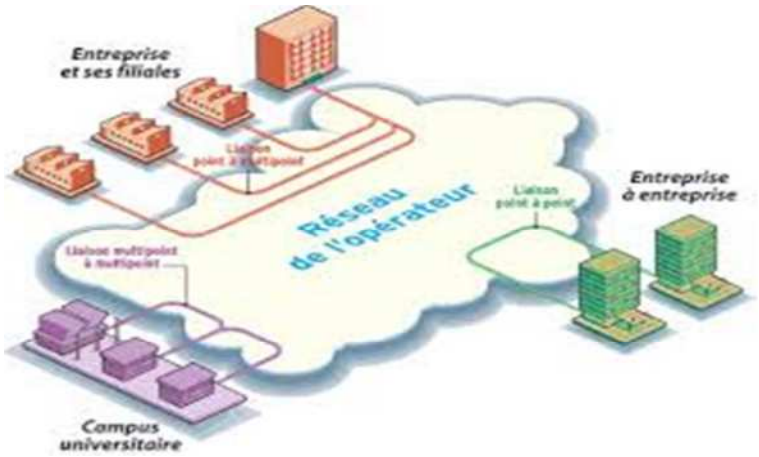


Figure I.2 : Réseau MAN

a.3.Les réseaux grande distance (WAN) :

Un réseau étendu, souvent désigné par son acronyme anglais WAN (*Wide Area Network*), est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Les réseaux à grande distance nécessitent de mettre en œuvre des moyens particuliers (modem, routeurs, commutateurs, passerelles…). Le plus grand WAN est le réseau Internet.

Figure I.3 : Réseau WAN

b) Type du réseau selon l'architecture :

b.1.Architecture clients /serveurs :

Les réseaux Client/serveur comportent plusieurs ordinateurs, en général un ordinateur servant de serveur et la plupart des stations sont des « **postes clients** », c'est à dire des ordinateurs dont se servent les utilisateurs.

Les « **postes serveurs** » sont en général de puissantes machines, elles fonctionnent à plein régime et sans discontinuité.

Les serveurs peuvent être réservés ou dédiés à une certaine tâche, donc, on peut avoir des serveurs de fichiers, des serveurs d'impression, les serveurs de bases de données…etc.

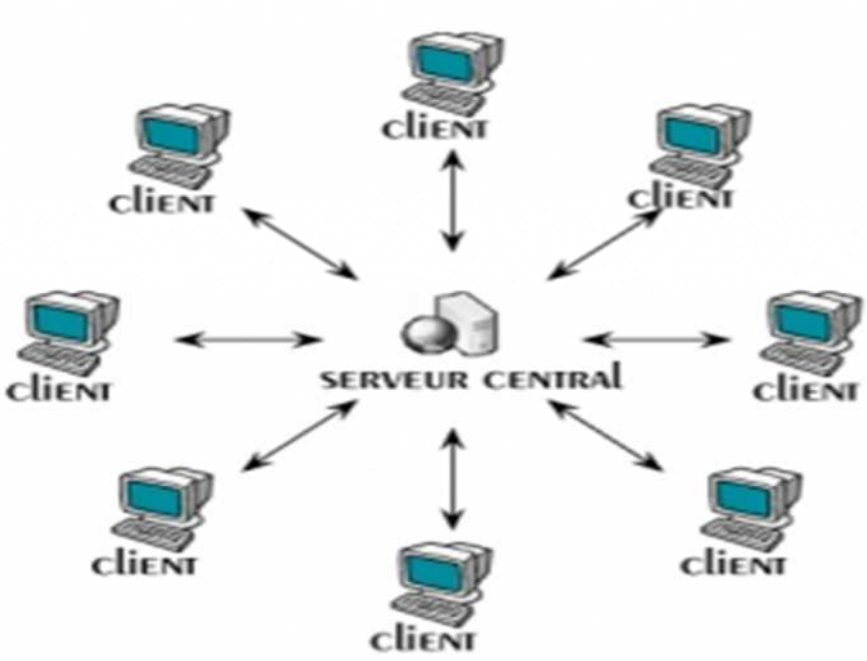


Figure I.4 : Architecture Client/serveur

b.2.Les réseaux à architecture postes à postes (Peer to Peer) :

Les réseaux « postes à postes » sont également appelés des réseaux « Peer to Peer » en anglais. Les réseaux postes à postes ne comportent en général que peu de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, Dans un réseau Peer to Peer chaque poste est à la fois client et serveur. Toutes les stations ont le même rôle, et il n'y a pas de statut privilégié pour l'une des stations. Chaque utilisateur décide lui-même des partages sur son disque dur et des permissions qu'il octroie aux autres utilisateurs.

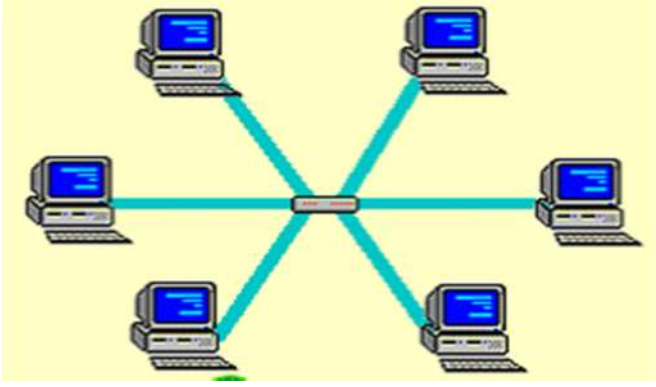


Figure I.5 : Réseau Poste à Poste

I.4.Les Topologies réseaux :

La topologie d'un réseau représente la façon dans laquelle les machines sont connectées.

I.4.1.La topologie en Bus :

Dans cette topologie un même câble relie en série tous les nœuds d'un réseau sans périphérique de connectivité intermédiaire .Les deux extrémités du réseau en bus sont équipées terminateurs qui arrêtent les signaux une fois arrivés à destination .On utilise un câble coaxial pour ce type de topologie.

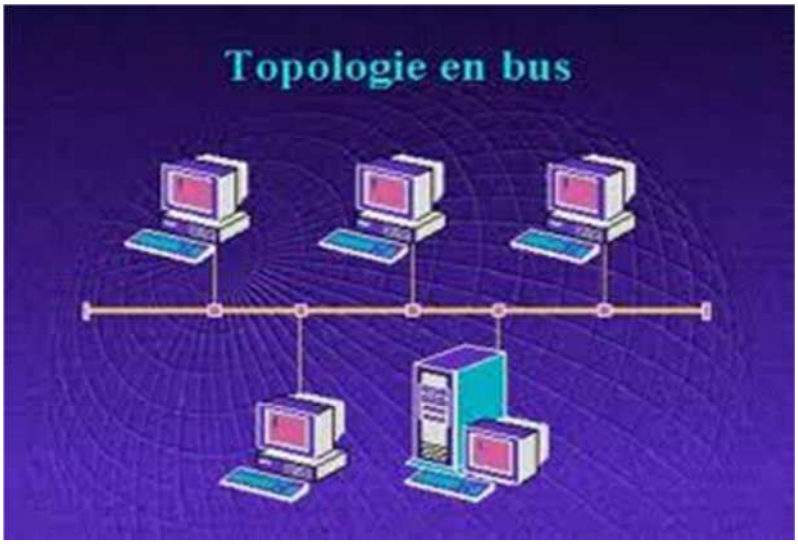


Figure I.6 : Topologie en bus.

I.4.2.La topologie en étoile :

Dans cette topologie, chaque nœud du réseau est relié à un périphérique central, tel qu'un commutateur (Switch) ou un concentrateur (hub). Un même câble de réseau en étoile ne peut relier que deux périphériques, donc la panne d'un nœud ne perturbera pas le fonctionnement global du réseau. En revanche, l'équipement central (un concentrateur (hub) et plus souvent sur les réseaux modernes, un commutateur (Switch)) qui relie tous les nœuds constitue un point unique de défaillance : une panne à ce niveau rend le réseau totalement inutilisable. En général on utilise un câble à paire torsadé dans cette topologie.

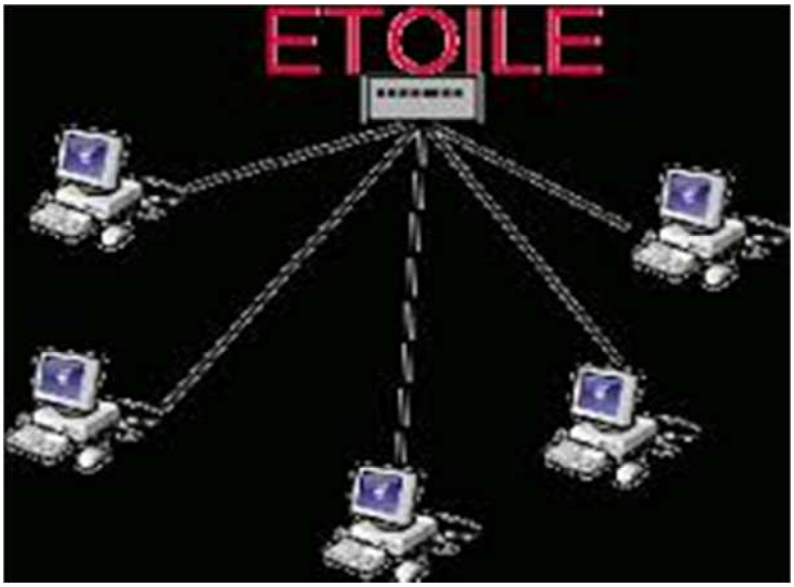


Figure I.7: Topologie en étoile

I.4.3. La topologie en anneau :

Dans une topologie en anneau, chaque nœud est relié aux deux nœuds les plus proches, et l'ensemble du réseau forme un cercle ou bien une boucle. Chaque station joue le rôle de station intermédiaire. Chaque station qui reçoit une trame, l'interprète et la transmis à la station suivante de la boucle si c'est nécessaire. La défaillance d'un hôte rompt la structure d'un réseau en anneau si la communication est unidirectionnelle.

Figure I.8 : La topologie en anneau

Les topologies en étoile, en bus et en anneau sont les plus utilisées en pratique mais il existe d'autres topologies qui sont :

- Une topologie maillée.
- topologie en arbre.
- le réseau en grille.
- le réseau en hypercube.

I.5.Les équipements d'interconnexion :

Un réseau local sert à interconnecter les ordinateurs d'une organisation, toute fois une organisation a généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux. Lorsqu'il s'agit de deux réseaux de même type, il suffit de faire passer les trames de l'un sur l'autre. Dans le cas contraire, c'est-à-dire lorsque les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à la conversion du protocole avant de transférer les trames.

Ainsi, les équipements à mettre en œuvre sont différents selon la configuration face à laquelle on se trouve.

Figure I.9 : Equipements d'interconnection.

I.5.1.Le répéteur :

Il permet d'interconnecter deux segments d'un même réseau. Le répéteur est passif au sens ou il ne fait qu'amplifier le signal .Il ne permet pas de connecter deux réseaux de types différents. Il travaille au niveau de la couche1 du modèle OSI. Ces fonctions sont :

La répétition des bits d'un segment à l'autre, la régénération du signal pour compenser l'affaiblissement, changer de média (passer d'un câble coaxial à une paire torsadée).

I.5.2.Les ponts :

Ce sont des équipements qui décodent les adresses machines et qui peuvent donc décider de faire traverser ou non les paquets. Le principe général du pont est de ne pas faire traverser les trames dont l'émetteur et le destinataire sont du même coté, afin d'éviter du trafic inutile sur le réseau.

I.5.3.Le concentrateur (HUB):

C'est un boitier qui a la fonction de répéteur. Mais sa fonction principale, est de pouvoir concentrer plusieurs lignes en une seule.

On peut y connecter plusieurs stations, dont le nombre dépend du type de HUB.

Un HUB sera connecté sur un autre HUB ou sur un serveur qu'avec une seule et unique ligne.

I.5.4.Le commutateur (Switch) :

Le commutateur (ou Switch) est un boitier assurant l'interconnexion de stations ou de segment d'un LAN en leur attribuant l'intégralité de la bande passante, à l'inverse du concentrateur qui la partage.

Les commutateurs ont donc été introduits pour augmenter la bande passante globale d'un réseau d'entreprise et sont une évolution des concentrateurs (ou hubs).

Plusieurs communications simultanées peuvent avoir lieu à condition qu'elles concernent des ports différents du commutateur. En recevant une information, un Switch

décode l'entête pour connaitre le destinataire et l'envoie uniquement vers le port associé. Ceci réduit le trafic sur l'ensemble du câblage réseau par rapport à un HUB qui renvoie les données sur tous les ports, réduisant la bande passante en provoquant plus de collisions.

I.5.5.Le routeur :

Les routeurs sont les machines clés d'internet car se sont des dispositifs qui permettent de choisir le chemin qu'un message va emprunter. Lorsque nous demandons une URL, le client web interroge le DNS, celui-ci indique l'adresse IP de la machine visée. Notre poste de travail envoie la requête au routeur le plus proche (en général la passerelle du réseau) qui choisit la prochaine à laquelle il va faire circuler la demande de telle façon que le chemin choisit soit le plus court.

I.5.6.Les passerelles :

Ce sont des systèmes matériels et /ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents, l'information est codée et transportée différemment sur chacun de ces réseaux.

Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en termes de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre.

I.6.La transmission des données :

La transmission de données désigne le transport d'information. Cela signifie l'envoi de flux de bits d'un endroit à un autre en utilisant des technologies ou bien des supports de transmission. Comme exemples concrets, on peut citer l'envoi de données d'un appareil à un autre et l'accès à un site web.

I.6.1.Les supports de transmission :

Nous entendons par "Supports de transmission" tous les moyens par lesquels on peut transmettre un signal de son lieu de production à sa destination avec le moins possible de dispersions ou distorsions.

Les supports de transmission qu'on utilise dans la pratique sont :

I.6.1.1.Les câbles à paires torsadées :

Les câbles à paires torsadées possèdent 4 paires torsadées. Pour les user, on utilise les connecteurs RJ 45.

Figure I.10 : Câble à paires torsadées avec connecteur RJ45

On distingue deux types de câbles à paires torsadées :

a)Les câbles STP

Les câbles STP (shielded twisted pairs) sont des câbles blindés. Chaque paire est protégée par une gaine blindée comme celle du câble coaxial. Théoriquement les câbles STP peuvent transporter le signal jusqu'à environ 150m à 200m.

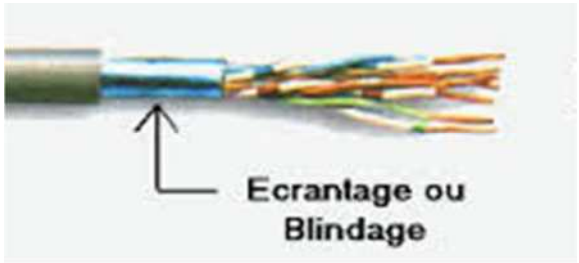


Figure I.11 : câble STP

b) Les câbles UTP

Les câbles UTP (Unshielded twisted pairs) sont des câbles non blindés, c'est-à-dire aucune gaine de protection n'existe entre les paires des câbles. Théoriquement les câbles UTP peuvent transporter le signal jusqu'à environ 100m.

Figure I.12 : Câble UTP

I.6.1.2. Les câbles coaxiaux :

Le câble coaxial est composé d'un fil de cuivre entouré successivement d'une gaine d'isolation, d'un blindage métallique et d'une gaine extérieure.

Figure I. 13 : câble coaxial avec connecteur BNC

On distingue deux types de câbles coaxiaux :

a) les câbles coaxiaux fins :

Le câble coaxial fin (thinNet) est en mesure de transporter le signal à une distance de 185m avant que le signal ne soit atténué.

b) les câbles coaxiaux épais :

Le câble coaxial épais (thickNet) est en mesure de transporter le signal à une distance de 500m avant que le signal ne soit atténué.

Pour le raccordement des machines avec les câbles coaxiaux, on utilise des connecteurs BNC.

I.6.1.3.Les câbles à fibre optique :

La fibre optique reste aujourd'hui le support de transmission le plus apprécié. Il permet de transmettre des données sous forme d'impulsions lumineuses avec un débit nettement supérieur à celui des autres supports de transmissions filaires. La fibre optique est constituée du cœur, d'une gaine optique et d'une enveloppe protectrice.

Figure I.14 : Câble à fibre optique

On distingue deux sortes des fibres optiques :

a) la fibre Multimode :

La fibre Multimode ou MMF (Multi Mode Fiber) a été la première fibre optique sur le marché. Le cœur de la fibre optique Multimode est assez volumineux, ce qui lui permet de transporter plusieurs trajets (plusieurs modes) simultanément. Il existe deux sortes de fibre Multimode :

- La fibre Multimode à saut d'indice.
- la fibre optique Multimode à gradient d'indice.

Les fibres Multimodes sont souvent utilisées en réseaux locaux.

b) la fibre monomodes :

La fibre monomode ou SMF (Single Mode Fiber) a un cœur si fin. Elle ne peut pas transporter le signal qu'en un seul trajet. Elle permet de transporter le signal à une distance beaucoup plus longue (50 fois plus) que celle de la fibre Multimode. Elle utilisé dans des réseaux à long distance.

I.6.1.4. Les liaisons infrarouges :

La liaison infrarouge est utilisée dans des réseaux sans fil (réseaux infrarouges). Il lie des équipements infrarouges qui peuvent être soit des téléphones soit des ordinateurs…

Théoriquement les liaisons infrarouges ont des débits allant jusqu'à 100Mbits/s et une portée allant jusqu'à plus de 500m.

Figure I.15 : liaison infrarouge

I.6.1.5.Les liaisons hertziennes :

La liaison hertzienne est une des liaisons les plus utilisées. Cette liaison consiste à relier des équipements radio en se servant des ondes radio.

Figure I.16 : liaison hertzienne

Voici quelques exemples des systèmes utilisant la liaison hertzienne :

- Radiodiffusion
- Télédiffusion
- Radiocommunications
- Faisceaux hertziens
- Téléphonie
- Le Wifi
- Le Bluetooth

I.7.Le modèle OSI :[1][4]

L'objectif de la norme OSI est de définir un modèle de toute architecture de réseau basé sur un découpage en sept couches [figureI.17], chacune de ces couches correspondant à une fonctionnalité particulière d'un réseau. Les couches 1, 2, 3 et 4 dites basses sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les couches 5, 6 et 7 dites hautes sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines

d'extrémité qui peuvent être séparées par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants.

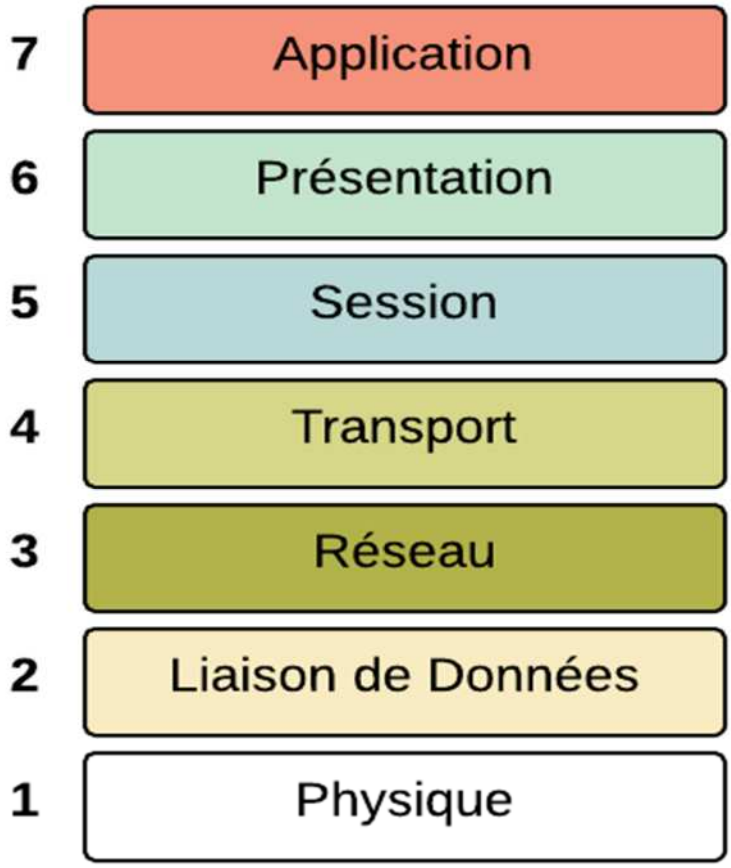


Figure I.17 : le modèle OSI

I.7.a.Les différentes couches du modèle:

Chaque couche de modèle OSI doit exécuter une série de fonction pour que les paquets de données puissent circuler d'un ordinateur source vers un ordinateur de destination sur un réseau.

I.7.a.1.La couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les

caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données. L'unité d'information typique de cette couche est le bit, représenté par une certaine différence de potentiel.

I.7.a.2.La couche liaison de données

Le rôle principal de la couche liaison de données est de faire en sorte qu'un moyen de communication brut apparaisse à la couche réseau comme étant une liaison exempte de la transmission. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données. La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur. L'unité d'information de la couche liaison de données est la trame qui est composées de quelques centaines à quelques milliers d'octets maximum.

I.7.a.3.La couche réseau

La couche réseau s'intéresse à l'interconnexion de plusieurs réseaux physique. Les problèmes à résoudre sont l'acheminement d'un paquet d'un point du réseau à un autre ce qu'on appelle le routage, sachant que l'arrivée et le départ ne sont pas sur le même support physique, l'interconnexion de support physique et de réseau hétérogènes ainsi que le contrôle et la régulation du trafic sur le réseau. A ce niveau apparaissent des protocoles de communications réseau tels que le protocole IP utilisé par Internet.

I.7.a.4.Couche transport

Cette couche est responsable du bon acheminement des messages. Le rôle principal de cette couche est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du

message à la réception des morceaux.

Cette couche est également responsable de l'optimisation des ressources du réseau. Cette couche est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, diffusion du message à plusieurs destinataires à la fois... Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau et également assure le contrôle de flux. L'unité d'information de la couche réseau est le message.

I.7.a.5. La couche session

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

I.7.a.6.La couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

I.7.a.7. La couche application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie...

I.8.Le modèle TCP/IP:[4][6]

TCP/IP, comme son nom l'indique, est en fait constitué de deux protocoles TCP et IP, TCP (Transmission Control Protocol) se situe au niveau transport du modèle OSI, il s'occupe donc d'établir une liaison virtuelle entre deux ordinateurs. Au niveau de l'ordinateur émetteur, TCP reçoit les données de l'application dans un buffer, les sépare en datagrammes pour pouvoir les envoyer séparément, l'ordinateur distant (qui utilise le même protocole) à la réception doit émettre un accusé de réception, sans celui-ci, le datagramme est ré émis. Au niveau de l'ordinateur récepteur, TCP ré assemble les datagrammes pour qu'ils soient transmis à l'application dans le bon ordre.

IP (Internet Protocol) assure l'acheminement de chaque paquet sur le réseau en choisissant la route la plus appropriée.

La relation entre TCP et IP et la suivante, TCP fait passer à IP un datagramme accompagné de sa destination, IP ne s'occupe pas de l'ordre d'expédition, c'est TCP qui s'occupe de tout remettre en ordre, il se contente de trouver la meilleure route possible.

I.8.a.Les couches du modèle TCP/IP:

Le modèle TCP/IP s'inspire du modèle OSI (modèle comportant 7 couches), il prend l'approche modulaire (utilisation de couches) mais contient uniquement 4 couches, le but essentiel reste la normalisation des communications entre ordinateurs [figure I.18], mais avant de définir les déférentes couches on va d'abord expliquer c'est quoi l'encapsulation des données.

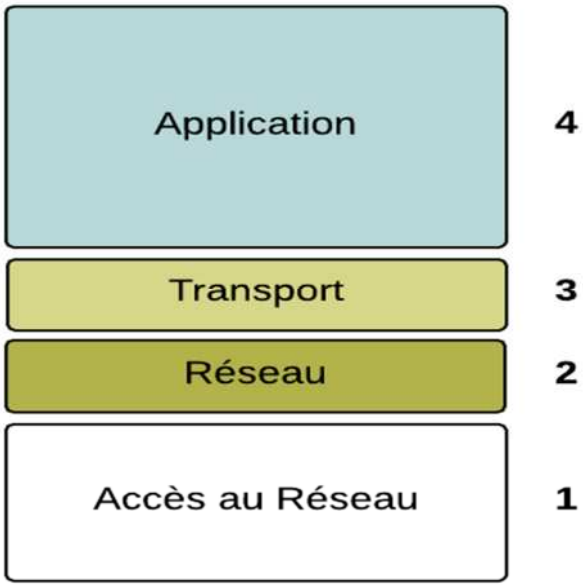


Figure I.18: Les couches de modèle TCP/IP

- **Encapsulation des données:**

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

Ainsi, à la réception, le message est dans son état originel.

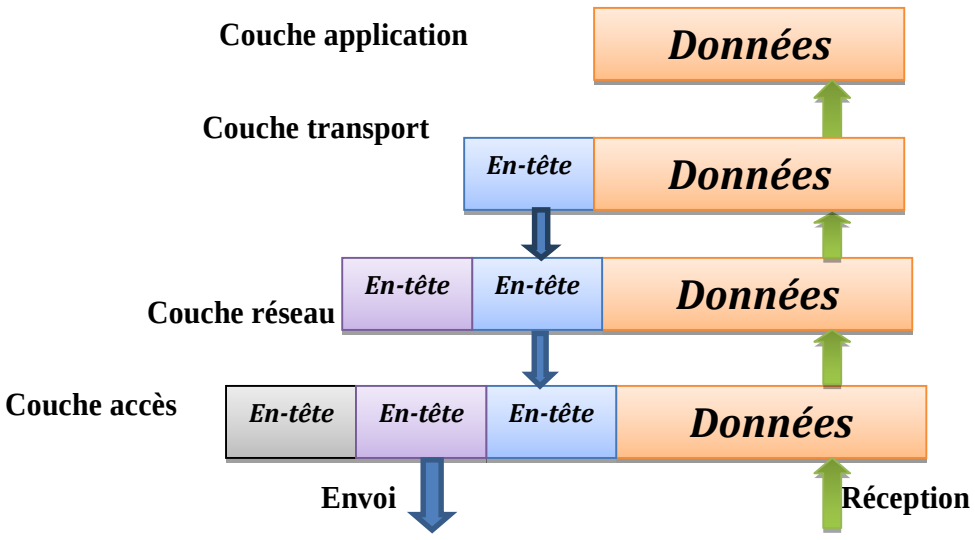


Figure I.19: Encapsulation des données

I.8.a.1 .Couche Application:

Le modèle TCP/IP n'inclut pas de couche session ni de couche présentation, ces couches ayant été jugées inutile. L'expérience du modèle OSI a confirmé la pertinence de ce choix puisque la plupart des applications ne les utilisent pas.

Il inclut en revanche une couche application, directement au-dessus de la couche transport, qui contient tous les protocoles de haut niveau.

I.8.a.2.Couche Transport:

La vocation de la couche transport est de permettre le transfert d'information de la machine émettrice vers la machine réceptrice de manière fiable et économique, indépendamment de la nature du ou des réseaux mis en place. Pour remplir cette fonction, la couche transport utilise deux protocoles différents TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

1) Le protocole TCP:

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

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

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

environnement Client-Serveur.

Les machines dans un tel environnement communiquent en mode connecté, c'est-à-dire que la communication se fait dans les deux sens.

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

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

2) Le protocole UDP:

Le protocole User Datagram Protocol (UDP) est défini dans le but de fournir une communication par paquet unique entre deux processus dans un environnement réseau étendu. Ce protocole suppose l'utilisation du protocole IP comme support de base â la communication.

Ce protocole définit une procédure permettant à une application d'envoyer un message court à une autre application, selon un mécanisme minimaliste. Ce protocole est transactionnel, et ne garantit ni la délivrance du message, ni son éventuelle duplication. Les applications nécessitant une transmission fiabilisée et ordonnée d'un flux de données implémenteront de préférence le protocole TCP (Transmission Control Protocol).

I.8.a.3. Couche Inter réseau:

Cette couche reçoit des datagrammes en provenance de la couche haut, qu'elle doit analyser pour déterminer s'ils lui sont adressés ou pas. Dans le premier cas elle doit décapsuler son en-tête du datagramme pour transmettre les données à la couche de transport et aux bons protocoles de cette couche (TCP, UDP ...).

Cette couche prend aussi en charge la communication de machine à machine. Elle accepte des requêtes venant de la couche de transport avec une identification de la machine vers laquelle le paquet doit être envoyé.

Elle utilise alors l'algorithme de routage pour décider si le paquet doit être envoyé vers

une passerelle ou vers une machine directement accessible.

La couche réseau utilise le protocole IP qu'on va expliquer dans le deuxième chapitre.

I.7.a.4 Couche Accès:

La couche la plus basse représente la connexion physique avec les câbles, les circuits d'interfaces électriques (transceivers), les cartes coupleurs, les protocoles d'accès au réseau.

La couche accès réseau est utilisée par la couche internet.la couche accès réseau TCP/IP intègre généralement les fonctions des deux couches inférieurs du modèle de référence OSI (liaison de données et physique).

Discusion :

La connaissance préalable d'une infrastructure réseau et différents équipements utilisés dans le réseau est une étape nécessaire pour acquérir la maitrise globale d'un environnement réseau. Dans ce chapitre nous avons décrit les types de réseaux, les supports de transmission ainsi que les équipements qui les constituent, et nous avons cité les couches de modèle OSI, et celles de modelé TCP/IP. La suite du travail va définir l'adressage IP version 4, version 6, et leurs caractéristiques.

Introduction :

Les réseaux sont né de besoin de transporter des informations d'un réseau a un autre et ces informations sont découpées en blocs, appelés paquets IP. Et chaque paquet doit transportées une adresse pour identifier chaque équipement. Dans ce chapitre nous allons présenter les deux adresses IP version 4 et version 6, nous allons présenté l'adresse IPv4,son en-tête et ses différents champs, ses caractéristiques et ses limites puis nous allons passé à la présentation de l'en-tête d' adresse IPv6 et ces caractéristiques.

II.1.Protocole IP version 4 (IPv4) :[7]

II.1.1.Définition :

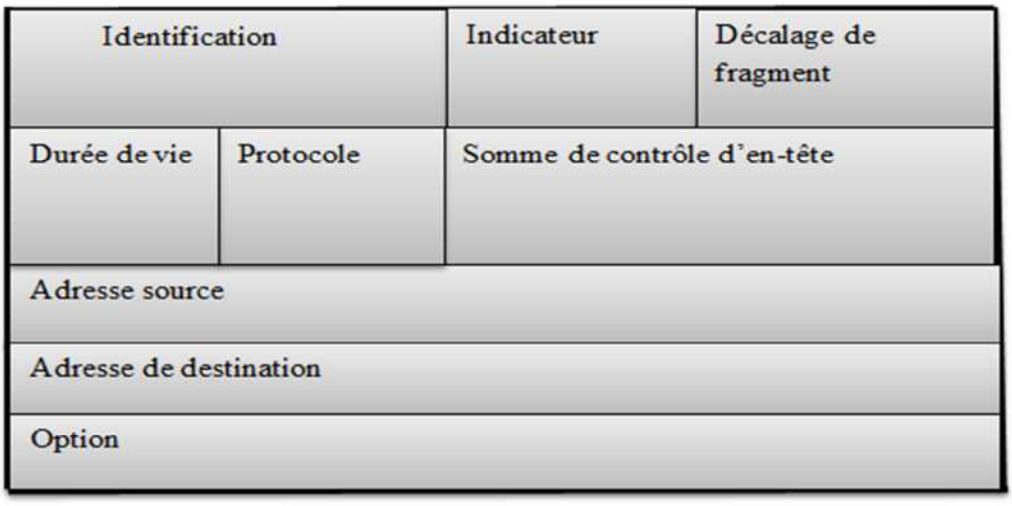
La première version d'internet Protocol (IP) largement déployée est appelée IPv4 (Internet Protocole Version 4 avec la valeur 4 pour le numéro de version), il a été créé dans les années 70, et mis en application en 1980.

Les adresses IPv4 sont codées sur 32 bits ce qui permet d'attribuer environ 4.3 milliards d'adresses. Elles sont sous la forme de quatre chiffres compris entre 0 et 255. Une adresse IPv4 est constituée d'une partie réseau identifiant le réseau et d'une partie hôte désignant l'interface correspondante.

II.1.2. Caractéristiques d'adressage IPv4:

II.1.2.1. En-tête de paquet IPv4:

Comme l'illustre la figure suivante, un protocole IPv4 définit de Nombreux champs différents dans l'en-tête de paquet. Ces champs contiennent des valeurs binaires que les Services lPv4 référencent lors de la transmission de Paquets sur le réseau.



FigureII.1 : Présentation de l'Entête lPv4

a-Adresse de destination IP:

Le champ d'adresse de destination IP contient une valeur Binaire de 32 bits représentant l'adresse de couche réseau de l'hôte destinataire du paquet.

b-Durée de vie:

La durée de vie (TTL, Time to live) est une valeur binaire de 8 bits indiquant la durée de vie restante du paquet. La valeur TTL est décrémentée de *1* à chaque fois que le paquet est traité par un routeur (c'est-à-dire à chaque saut). Lorsque la valeur devient nulle, le routeur supprime ou abandonne le paquet. Ce mécanisme évite que les paquets ne pouvant atteindre leur destination ne soient transférés indéfiniment d'un routeur à l'autre dans une boucle de routage.

c-Protocole:

Cette valeur binaire de 8 bits indique le type de données utiles que le paquet transporte. Le champ de protocole permet à la couche réseau de transmettre les données au protocole de couche supérieure appropriée.

d-Type de service:

Le champ de type de service contient une valeur binaire de 8 bits utilisée pour définir la priorité de chaque paquet.

e-Décalage de fragment:

Un routeur doit fragmenter un paquet lors de sa transmission d'un média à un autre. Lorsqu'une fragmentation se produit, le paquet IPv4 utilise le champ de décalage de fragment de l'en-tête IP pour reconstruire le paquet à son arrivée sur l'hôte de destination. Le champ de décalage de fragment identifie l'ordre dans lequel placer le fragment de paquet dans la reconstruction.

f- Indicateur (indicateur de fragments supplémentaires/ indicateur ne pas fragmenter) :

L'indicateur de fragments supplémentaires est un seul bit du champ Indicateur utilisé avec le décalage de fragment pour la fragmentation et la reconstruction de paquets. Si le bit indicateur de fragments supplémentaires est défini, ceci indique qu'il ne s'agit pas du dernier fragment d'un paquet.

L'indicateur Ne pas fragmenter est un seul bit du champ Indicateur stipulant que la fragmentation du paquet n'est pas autorisée. Si le bit de l'indicateur Ne pas fragmenter est défini, la fragmentation de ce paquet n'est pas autorisée.

Autres champs de l'en-tête IPv4:

- **Version** : contient le numéro de version IP (4).
- **Longueur d'en-tête (IHL)**: spécifie la taille de l'en-tête de paquet.

- **Longueur du paquet:** ce champ donne la taille du paquet entier, En-tête et données compris, en octets.
- **Identification:** ce champ sert principalement à identifier de manière unique les fragments d'un paquet IP d'origine.
- **Somme de contrôle d'en-tête:** le champ de somme de contrôle est utilisé pour vérifier l'absence d'erreurs dans l'en-tête de paquet.
- **Options:** des champs supplémentaires sont prévus dans l'en-tête IPv4 afin de fournir d'autres services, mais ils sont rarement utilisés.

II.1.2.2.Sructure d'un adressage IPV4:

Tous les périphériques appartenant à un réseau doivent être identifiés de manière unique. Au niveau de la couche réseau, les paquets de communication doivent être identifiés par les adresses source et de destination des systèmes des deux côtés.

Avec l'adressage lPv4, cela implique que chaque paquet comporte, dans l'en-tête de la couche réseau, une adresse source 32 bits et une adresse de destination 32 bits. Dans le réseau de données, ces adresses servent de configurations binaires. À l'intérieur des périphériques, une logique numérique est appliquée.

Pour les utilisateurs, une chaîne de 32 bits est difficile à interpréter et encore plus difficile à mémoriser. Par conséquent, nous représentons les adresses IPv4 à l'aide d'une décimal à point.

- **Décimal à point:**

Les configurations binaires représentant des adresses lPv4 sont exprimées en décimal à point, en séparant chacun des octets par un point. Le nom d'« octet » s'explique par le fait que chaque nombre décimal représente 8 bits. La notation en décimale à point est un moyen plus pratique pour les utilisateurs d'entrer des adresses et de s'en souvenir.

Exemple:

L'adresse: **10101100.00010000.00000100.00010100** est exprimée en décimal à point de la manière suivante: **172.16.4.20**

- **Parties réseau et hôte:**

Pour chaque adresse lPv4, une partie des bits de valeur supérieure représente l'adresse réseau. Au niveau de la couche réseau, un réseau se définit par un groupe d'hôtes dont la partie adresse réseau de l'adresse contient la même configuration binaire.

Bien que l'ensemble de 32 bits définisse l'adresse lPv4 d'un hôte, un nombre variable de bits constitue la partie hôte de l'adresse. Le nombre de bits contenus dans la partie hôte détermine le nombre d'hôtes possible sur un réseau. Ainsi, plus le nombre de bits réservé au réseau est petit, plus celui-ci peut contenir plus d'ordinateurs. Les adresses IP sont donc réparties en classes, c'est-à-dire selon le nombre d'octets qui représentent le réseau.

Classe A:

Dans une adresse IP de classe A, le premier octet représente le réseau. Le bit de poids fort (le premier bit, celui de gauche) est à zéro, ce qui signifie qu'il y a 2^7(00000000 à 01111111) possibilités de réseaux, c'est-à-dire 128. Toutefois le réseau 0 (00000000) n'existe pas et le nombre 127 est réservé pour désigner votre machine, les réseaux disponibles en classe A sont donc les réseaux allant de **1.0.0.0** à **126.0.0.0** (lorsque les derniers octets sont des zéros cela indique qu'il s'agit d'un réseau et non d'un ordinateur)

Les trois octets de droite représentent les ordinateurs du réseau, le réseau peut donc contenir:

2^{24}-2^1 = 16777214 ordinateurs

Classe B:

Dans une adresse IP de classe B, les deux premiers octets représentent le réseau. Les deux premiers bits sont 1 et 0, ce qui signifie qu'il y a 2^{16} (10 000000 00000000 à 10 111111 11111111) possibilités de réseaux, c'est-à-dire 16384. Les réseaux disponibles en classe B sont donc les réseaux allant de **128.0.0.0** à **191.255.0.0.**

Les deux octets de droite représentent les ordinateurs du réseau, le réseau peut donc contenir:

2^{16}-2^1 = *65534* ordinateurs.

Classe C :

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1,1 et 0, ce qui signifie qu'il y a 2^{21} possibilités de réseaux, c'est-à-dire 2097152. Les réseaux disponibles en classe C sont donc les réseaux allant de **192.0.0.0** à **223.255.255.0**

L'octet de droite représente les ordinateurs du réseau, le réseau peut donc contenir: 2^8-2^1 = *254* ordinateurs.

Le but de la division des adresses IP en trois classes A, B et C est de faciliter la recherche d'un ordinateur sur le réseau. Les adresses de classe A sont réservées aux très grands réseaux, tandis que l'on attribuera les adresses de classe C à des petits réseaux d'entreprise par exemple.

II.1.2.3. Adresses particulières :

a. Adresse de diffusion

L'adresse de diffusion lPv4 est une adresse spécifique, attribuée à chaque réseau. Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau. Pour cela, un hôte peut envoyer un seul paquet adressé à l'adresse de diffusion du réseau.

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

Pour le réseau 10.0.0.0 avec 24 bits réseau, l'adresse de diffusion serait 10.0.0.255. Cette adresse est également désignée sous le nom de diffusion dirigée.

b. Adresses privées :

Un certain nombre d'adresses IP ont été réservées pour une utilisation en intranet. Ces adresses permettent d'assurer à un serveur proxy (qui partage la connexion internet de l'entreprise), une différenciation satisfaisante entre le réseau public (internet) et le réseau privé (intranet).

Ces adresses IP privées sont :
10.0.0.0 à 10.255.255.255 ;
172 .16.0.0 à 172.31.255.255 ;
192.168.0.0 à 192.168.255.255 ;

II.1.2.4.Masque des sous réseau :

Les masques de sous-réseau utilisent la même représentation que celles des adresses IPv4. En IPv4, une adresse IP est codée sur 4 octets, soit 32 bits (représentés en notation décimale à point). Un masque de sous-réseau possède lui aussi 4 octets. Bien que la norme IPv4 n'interdise pas que la partie significative du masque contienne des bits à 0, on utilise en pratique des masques constitués (sous leur forme binaire) d'une suite de 1 suivis d'une suite de 0, il y a donc 32 masques réseau possibles.

II.1.3. Attribution des adresses :

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

II.1.3.1Attribution statique d'adresses:

Avec ce type d'attribution, l'administrateur réseau doit configurer manuellement les informations de réseau pour un hôte. Ces informations comportent, au minimum, l'adresse IP, le masque de sous-réseau et la passerelle par défaut. Les adresses statiques présentent certains avantages sur les adresses dynamiques. Par exemple, elles conviennent pour les imprimantes, les serveurs et d'autres périphériques réseau, qui doivent être accessibles pour les clients d'un réseau. Si les hôtes ont l'habitude d'accéder à un serveur à une adresse IP particulière, cela peut- poser des problèmes en cas de modification de cette adresse. De plus, l'attribution statique des informations d'adressage permet de mieux contrôler les ressources réseau. Toutefois, la configuration IP sur chaque hôte prend du temps.

II.1.3.2. Attribution dynamique d'adresses:

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

Le DHCP est généralement la méthode d'attribution d'adresses IP privilégiée pour les réseaux de grande taille, dans ce cas le risque d'erreur de saisie est quasiment éliminé.

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

II.1.4.Limites des adresses IPv4 :

Insuffisances d'adresses :

Une adresse IPv4 est codée sur 32 bits et permet théoriquement d'adresser 2^{32} machines, soit à peu près 4 milliards. Ce nombre pourrait paraitre au premier abord très élevé, mais les ordinateurs ne sont pas numérotés séquentiellement. Ils sont regroupés par réseaux. A chaque réseau est affecté un numéro qui est codé sur une partie de 32 bits de l'adresse. Avec l'explosion croissante des besoins des utilisateurs, la demande d'adresse dépasse aujourd'hui largement les possibilités offerte par le protocole IPv4.

Le principal problème de cette technologie est le manque d'adresses qui freine son développement.

L'explosion des besoins des utilisateurs a pour conséquences non seulement la raréfaction des adresses mais aussi l'augmentation de la taille des tables de routage. En effet la taille des mémoires des routeurs est fixe alors que la table de routage utilisant ces mémoires augmente suivant les nouvelles routes qui sont apprises par le routeur.

Pour répondre aux besoins des clients, des études ont été faites et elles ont aboutis à la conception de protocole IPv6.

II.2. Le protocole version 6 (IPv6):

II.2.1.Définition : [8]

Le protocole IPv6, initialement appelé IPng (IP next generation), est l'aboutissement des travaux menés au sein de l'IETF pour succéder à IPv4.

Ce protocole a pour principaux objectifs de conserver les principes qui ont fait le succès d'IP, de corriger les défauts de la version courante (v4) et d'anticiper les besoins futurs. IPv6 permet aussi de réduire au minimum les impacts sur les protocoles des couches supérieures et inférieures. Outre un format d'adressage qui permet de disposer d'un stock d'adresses extrêmement important, IPv6 prévoit un adressage hiérarchique, permettant d'optimiser le routage. L'usage commercial est envisagé, et le nouvel IP peut supporter de façon native le multicast, l'auto-configuration, la gestion de la mobilité, la sécurisation par défaut.

II.2.2. Caractéristiques d'adressage IPv6 :

II.2.2.1. En-tête de paquet IPv6 :

L'en-tête IPv6 est constitué de 40 octets et ne contient que huit domaines. Ceci implique que l'en-tête IPv6 est plus facile à manipuler.

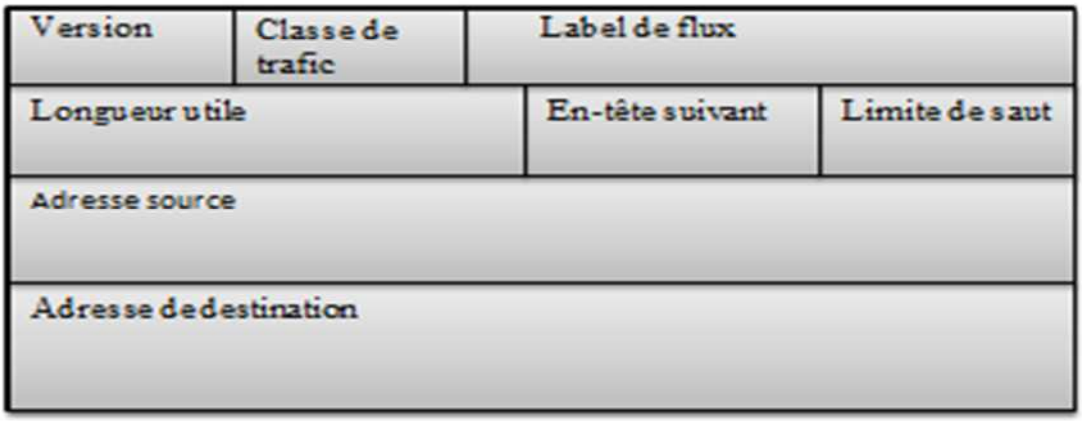


Figure II.2: Format d'en-tête IPv6.

La signification des champs est assignée dans le tableau (II.1):

Champs	Taille	Rôle
Version	4 bits	Décrit la version du protocole. il vaut 6 pour IPv6
Classe de Trafic	8 bits	Ce champ indique le type de trafic.
Label de flux	20 bits	Il est utilisé pour identifier les paquets appartenant à un même flux de données.
Longueur utile	16 bits	Désigne la longueur en octet de la charge utile du paquet.
En-tête suivant	8 bits	Décrit l'en-tête de la couche immédiatement supérieure ou la prochaine extension
Limite de saut	8 bits	Définit le nombre maximum de routeurs que le paquet peut traverser.
Adresse Source	128 bits	Contient l'adresse unicast de l'émetteur du paquet
Adresse Destination	128 bits	Représente l'adresse de destination du paquet. Il peut être unicast, anycast ou multicast.

Tableau II.1 : la signification des champs de l'En-tête IPv6.

II.2.2.2. Adressage :

Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales. Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique ; pour un total de 32valeurs hexadécimales. Les adresses IPv6peuvent être notées en minuscules ou en majuscules.

a. Structure d'adresse IPV6 :

Les adresses IPv6 sont constituées de 16 octets (128 bits).

Une adresse IPv6 est composée de 8 chiffres distincts représentant 16 bits chacun et est écrit en base 16 (notation hexadécimale). Les chiffres hexadécimaux (0 à 9 et A à F) et le séparateur de colonne « : » sont les seuls caractères qui peuvent être utilisés pour l'écriture d'une adresse IPv6.

Exemple d'adressage IPv6 :

FEDC : 0000 :0000 :0000 :0400 :A987 :6543 :210F

Cette notation peut être comprimée et simplifiée en deux cas différents :

- Il est possible de mettre un zéros à la place de 4 zéros qui apparaissent dans tout groupement hexadécimal délimité par deux points.

  L'adresse précédente peut s'écrire :

  FEDC : 0 :0 :0 :400 :A987 :6543 :210F
- Plusieurs zéros consécutifs peuvent être remplacés par « :: ». Ainsi l'adresse précédente peut être écrite comme suit :

  FEDC::400 :A987 :6543 :210F

  Les « :: » ne peuvent être apparaître qu'une seule fois au plus dans une adresse.

  Le tableau suivant nous donne la forme abrégée de quelques exemples :

Exemple d'adresse	Forme abrégée
1080 :0 :0 :0 :8 :800 :200C :417A	1080 ::8 :800 :200C :417A
FF01 :0 :0 :0 :0 :0 :0 :101	FF01 ::101
0 :0 :0 :0 :0 :0 :0 :1	::1

Tableau II.2 : Présentation de la forme de quelques exemple d'adresse.

b. Les différents types d'adresses

Les adresses IPv6 sont des identificateurs d'interface ou d'ensemble d'interfaces. On distingue trois types d'adresses : les adresses unicast, multicast et anycast.

1. Les adresses unicast

Les adresses unicast peuvent identifier un nœud de manière unique (carte réseau ou interface de routeur).

Un paquet envoyé à l'intention d'une adresse unicast sera uniquement délivré à l'interface identifiée par cette adresse.

Il existe trois types d'adresses unicast :

- Les adresses unicast globales.
- Les adresses unicast locales.
- Les adresses unicast de liaison locales.

A noter que les adresses anycast sont extraites de la plage d'adresse « unicast globales ».

- **Les adresses unicast globales :**

L'adresse unicast globale est définie de la façon suivante :

2000 ::/3	001x xxxx	xxxx xxxx	2000-3FFF

« 2000 ::/3 » signifie que les « 3 » bits de poids fort présents dans les 16 bits « 2000 ::/3 » sont figés.

« 2 » est codé sur 4 bits en binaire en « 0010 » ;

« 0 » s'écrit « 0000 » en binaire ;

Une fois le préfixe hexadécimal transcrit en binaire, on identifie les 3 bits de poids fort (les plus à gauche) précisés après le « / » dans l'écriture du préfixe. Ces bits doivent rester figés lorsque les combinaisons possibles sont énumérées.

Ainsi, 2000 ::/ veut dire que les bits de poids fort pourront s'écrire avec les valeurs « minimum » et « maximum » suivantes :

0010 0000 0000 0000 ;

Et 0011 1111 1111 1111 ;

- **Les adresses unicast locales :**

Le préfixe de base qui désigne ce type d'adresses est FC00-FDFF (FC::/7).

L'adresse unicast locale est définie de la façon suivante :

FC ::/7	1111 110x	xxxx xxxx	FC00-FDFF

Comme dans le cas d'adresse unicast globale, l'écriture FC ::/7 signifie que les 7 bits de poids fort sont figés.

« F » en binaire s'écrit « 1111 » ;

« C » en binaire s'écrit « 1100 » ;

Ainsi, FC ::/ veut dire que les bits de poids fort pourront s'écrire avec les valeurs « minimum » et « maximum » suivantes :

1111 1100 0000 0000 ;

Et 1111 1101 1111 1111 ;

- **Adresse unicast de liaison locale :**

La structure de cette adresse est la suivante :

FE80 ::/10	1111 1110	10xx xxxx	FE80-FEBF

Les 10 bits de poids fort sont figés.

2. Les adresses multicast :

Un paquet envoyé à une adresse multicast sera transmis à toutes les interfaces identifiées par cette adresse.

Le préfixe associé aux adresses multicast est FF00 ::/8 soient les adresses de FF00 à FFFF.

La structure de cette adresse est la suivante :

FF00 ::/8	1111 1111	0000 0000	FF00-FFFF

Le tableau suivant nous résume les différents types d'adresses en précisant leurs plages d'adresse.

Catégories d'adresses	préfixes	mini	Maxi
Unicast globale	2000::/3	2000	3FFF
Unicast locale	FC00::/7	FC00	FDFF
Unicast de liaison locale	FE80 ::/10	FE80	FEBF
multicast	FF00 ::/8	FF00	FFFF

Tableau II.3 : Présentation d'un résumé de différent type d'adresse.

II.2.2.3. Masque de sous réseau :

Un masque de sous-réseau, au sens large, est un ensemble d'adresses IPv6 commençant par une même séquence binaire. Le nombre de bits que comporte cette séquence est notée en décimal derrière une barre oblique (/).

Ainsi, 2001:db8:1:1a0::/59 est le sous-réseau correspondant aux adresses comprises entre

2001:db8:1:1a0:0:0:0:0 et 2001:db8:1:1bf:ffff:ffff:ffff:ffff

II.2.3. Auto configuration des adresses IPv6 :[9]

Il existe deux types d'auto configuration :

- La configuration avec état ;
- La configuration sans état ;

➢ **Configuration avec état :**

Dès que l'hôte IPv6 détecte la présence d'un routeur, il va examiner les messages d'annonces envoyés par celui-ci, pour savoir si un serveur DHCPv6 a été configuré. Si le routeur précise que le service DHCPv6 peut être pris en charge, l'hôte va envoyer un message de sollicitation pour tenter de trouver un serveur DHCPv6. Ce message est envoyé en utilisant une adresse multicast spécifique.

A noter qu'en IPv6, la notion d'adresse de diffusion n'existe pas contrairement à IPv4, elle est remplacée par des adresses multicast spécifiques.

➢ **La configuration sans état :**

L'hôte IPv6 s'appuie sur les informations reçues par le routeur pour configurer une adresse sur son interface. Il va simplement récupérer les 64 premiers bits de l'adresse source de routeur envoyant une annonce et compléter avec son identifiant d'interface.

Ainsi, dès que les adresses IPv6 sont configurées manuellement, tous les hôtes « sans état » vont s'aligner sur le bon numéro de réseau (celui reçu des routeurs).

Discussion :

Dans ce chapitre nous avons étudié les déférents champs des en-têtes lPv4 et IPv6, les caractéristiques d'adressage dans les deux versions (les classes d'adresse en IPv4 et les types d'adresse en IPv6), nous avons aussi abordé les limites d'IPv4 et la nécessité d'un autre type d'adressage qui est IPv6 pour satisfaire les besoins présent et future. Dans le chapitre qui suit on va donner quelques méthodes de migration les plus utilisées et qui sont proposées par les chercheurs et les spécialistes de réseau pour faciliter la circulation des données entre les deux protocoles.

Introduction :

Le passage d'un réseau internet entièrement IPv4 vers un réseau internet entièrement IPv6 est prévu pour durer très longtemps (plusieurs années). Il est donc nécessaire pendant cette période de transition de permettre aux machines IPv4 et IPv6 de cohabiter et de communiquer entre elles. Un certain nombre de méthodes ont donc été étudiées pour réaliser cette cohabitation et ainsi faciliter la transition.

III. Méthodes de migration : [10]

IPv6 n'est pas rétro-compatible avec IPv4, et les systèmes IPv4 à eux seuls ne peuvent pas utiliser les services IPv6 ou communiquer avec les hôtes IPv6. La transition d'IPv4 vers IPv6 est prévue pour prendre un temps considérable. Comme les systèmes et applications requièrent l'interopérabilité entre IPv4 et IPv6, les méthodes de transition sont alors nécessaires. Dans l'environnement de transition, trois différents types d'hôtes existent: IPv4 uniquement, IPv6 uniquement, et double pile IPv4/IPv6. Il existe différents méthodes de transition dont Dual Stack, Tunneling et Translation.

III.1 La méthode DUAL-STACK (Double Pile) :

Dans le cas où l'on dispose d'une pile IPv4/IPv6, d'applications IPv4/IPv6 et que l'on est sur un réseau IPv4/IPv6, on n'a pas besoin de méthodes 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.

Figure III.1 : Schéma de dual-stack.

Ce schéma montre que les hôtes implémentant uniquement la version 4 du protocole IP échangent entre eux indépendamment des hôtes implémentant la version 6 et les deux flux se superposent dans le même réseau physique. En plus de la table de routage IPv4, pour effectuer l'acheminement des paquets IPv6, une nouvelle table de routage a été ajoutée au routeur. En effet un routeur double pile possède deux tables de routage pour assurer le routage dans un réseau comme celui que nous avons dans la figure précédente.

❖ **Avantages et inconvénients :**

➢ **Avantage :**

- Méthode de transition la plus simple et la plus souple.

➢ **Inconvénients** :

- Ne résoudre pas le problème de manque des adresses puisque chaque machine doit disposer d'une adresse IPv4 et d'une adresse IPv6.
- Routeurs doivent pouvoir acheminer les deux types de paquets.
- Impossibilité de communication avec des réseaux utilisant d'anciens routeurs qui disposent uniquement de la pile d'adresse IPv4.
- Sécuriser les deux protocoles IPv4 et IPv6 (solution couteuse).

III.2 La méthode de Translation :

Pour faire communiquer des machines IP4 avec des machines IPv6, il est nécessaire d'implémenter des méthodes de traduction ou de conversion de paquets. Comme il y a de grandes différences entre IPv4 et IPv6, ces méthodes ne peuvent pas marcher dans toutes les circonstances. Il se peut donc que certains protocoles et certaines options (mobilité, qualité de service, ...) ne marchent pas (ou de façon dégradé) avec des méthodes de traduction.

NAT-PT signifie Network Address Translation and Protocol Translation. Cette méthode réalise donc à la fois une translation d'adresse et de protocole pour permettre à un équipement uniquement IPv6 de communiquer avec des équipements IPv4 (et inversement).

NAT-PT repose sur le maintien d'une table de correspondance au niveau du routeur entre adresses IPv6 et adresses IPv4. Il existe deux techniques de translations d'adresses différentes pour construire cette table : la translation statique, et la translation dynamique

II1.2.1 - Translation statique :

La translation statique consiste à ce que l'administrateur réalise en personne l'ajout des entrés dans la table de correspondance. L'exemple suivant illustre une utilisation de ce type de translation :

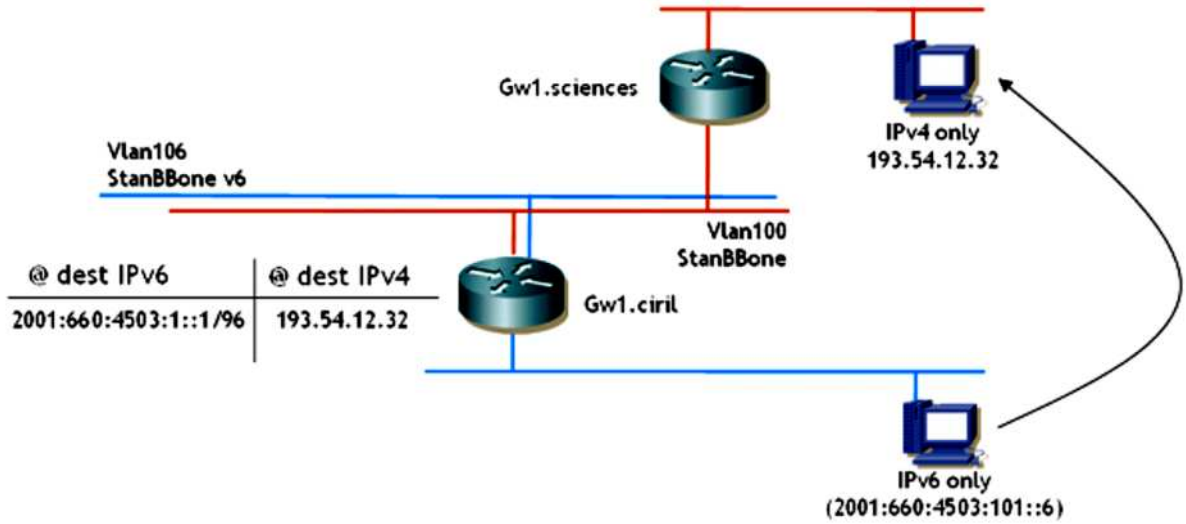


Figure III.2 : Schéma de présentation de NAT-PT

Dans ce cas précis, imaginons que le poste IPv6 connecté à Gw1.ciril veut communiquer avec le poste IPv4 connecté à Gw1.sciences. Il est alors nécessaire de définir au niveau du routeur une correspondance entre l'adresse IPv4 193.54.12.32 et une adresse IPv6 définie dans une plage d'adresses spécifiquement réservée au méthode de NAT-PT. Cette plage d'adresses appelée préfixe NAT devra avoir une longueur de 96 bits afin de pouvoir faire correspondre l'ensemble des adresses IPv4 existantes. Ainsi lorsque le routeur recevra un paquet dont l'adresse destination sera comprise dans ce préfixe alors il appliquera le méthode de NAT-PT. Dans notre exemple il translatera donc l'adresse destination 2001:660:4503:1::1 en 193.54.12.32. Afin de simplifier au maximum, nous considérerons que l'adresse source sera également translatée statiquement vers une adresse IPv4 prédéfinie.

II1.2.2 - Translation dynamique :[11]

La translation statique est utile pour communiquer avec un poste précis mais il est inconcevable de mettre en place statiquement une table permettant d'accéder à tout l'Internet. Dans ce contexte il était donc nécessaire de mettre en œuvre une seconde méthode permettant de remplir dynamiquement la table de correspondance au fur et à mesure des besoins. Pour se faire la solution consiste à utiliser les réponses aux requêtes DNS traversant le routeur pour mettre à jour les correspondances. L'utilisation de la translation dynamique nécessite donc la mise en place d'une entrée statique permettant de communiquer avec le serveur de noms.

Voici les différentes étapes permettant la création d'une entrée dynamique (Figure III. 3) :

1 : Le poste IPv6 émet une requête de résolution de noms de type AAAA pour www.google.fr. L'adresse destination utilisée est 2001:660:4503:1::1.

2 : Le routeur reçoit le paquet et s'aperçoit que l'adresse destination fait partie du préfixe NAT. Le paquet est donc translaté selon l'entrée statique correspondante et la requête de type AAAA et transformée en une requête de type A et une seconde de type AAAA.

3 : Le serveur de noms répond aux deux requêtes. S'il retourne une adresse IPv6 alors cette adresse est communiquée au client qui pourra alors accéder directement au site (sans NAT-PT). Dans le cas inverse le routeur utilisera l'adresse IPv4 retournée pour ajouter dynamiquement une entrée dans la table NAT. L'adresse IPv6 correspondante sera constituée du préfixe NAT suivie de l'adresse IPv4 convertie en caractères hexadécimaux (66.249.85.104=42F9.5568).

4 : Le routeur translatera ainsi la réponse de type A en réponse de type AAAA avec comme résultat à la requête, l'adresse constituée précédemment (2001:660:4503:1:42F9:5568).

5 : La communication peut avoir lieu puisqu'une entrée dans la table NAT a été créée.

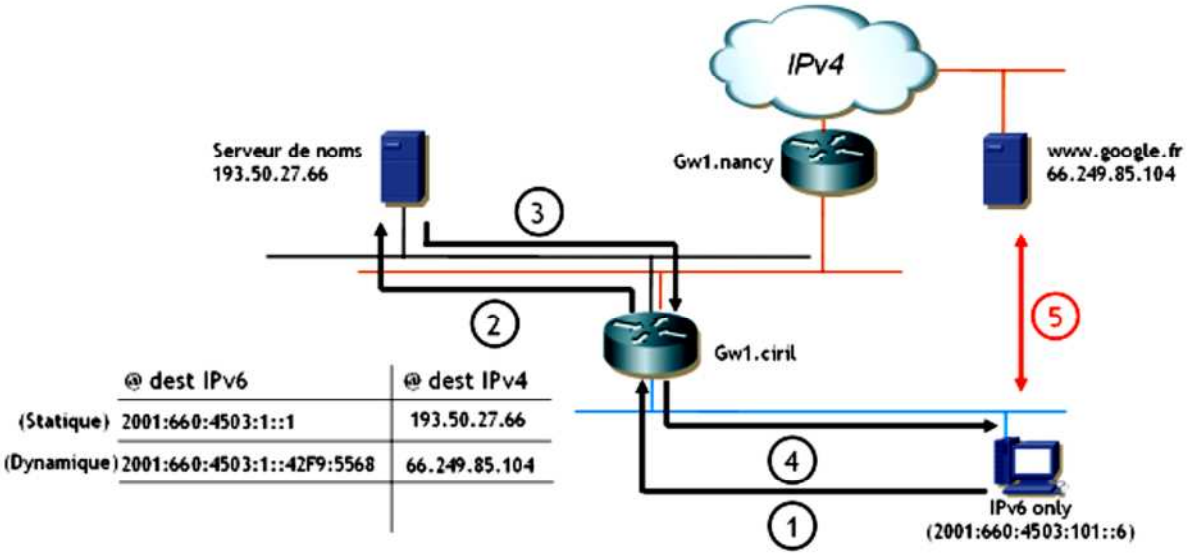


Figure III. 3 : Scénario d'utilisation de méthode NAT-PT

III.3 la méthode de Tunnel :[12]

En IPv6 la notion de tunnel est très importante. Elle va notamment permettre la prise en charge de l'IPv6 sur des réseaux distants y compris lorsque la connectivité IPv6 n'est pas disponible de bout en bout. La réalisation d'un Tunnel est généralement basée sur les techniques d'encapsulation qui sont utilisées dans le cas où l'on doit faire communiquer des machines IPv6 qui ne sont reliées que par un réseau IPv4. Les paquets IPv6 sont alors encapsulés dans des paquets IPv4 le temps de traverser ces points.

On peut dire qu'il existe trois types de Tunnels :

- Les Tunnels statiques.
- Les Tunnels semi automatiques.
- Les Tunnels automatiques.

III.3.1- Tunnel statique (manuel) :

Les tunnels statiques sont utilisés pour relier un réseau ou une machine IPv6 à un autre réseau IPv6 par l'intermédiaire d'un réseau IPv4. Ils sont configurés à la main et sont mis en place avec une durée de vie importante. Les machines qui sont aux extrémités du tunnel doivent avoir une double pile IPv4/IPv6. Les autres machines du réseau IPv6 n'ont donc pas besoin de cette double pile pour communiquer avec les machines IPv6 situées de l'autre côté du tunnel, mais elle peut être utile pour communiquer avec des machines IPv4 (sans passer par le tunnel).

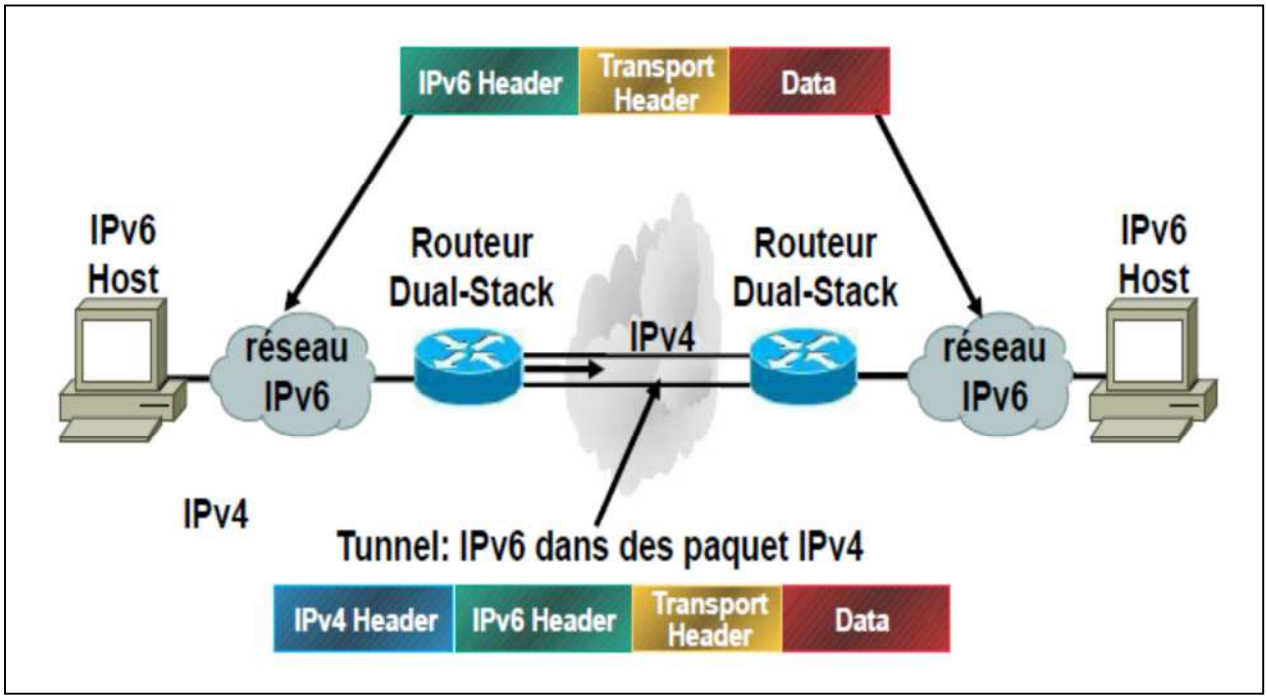


Figure III.4 : Schéma d'un tunnel statique

III.3.2.Tunnel semi-automatique (Tunnel BROKER) :

Un tunnel BROKER est un service proposé sur Internet permettant la création et la configuration automatique d'un tunnel statique pour accéder à Internet v6 par l'intermédiaire d'un réseau IPv4. Cela peut être vu comme un fournisseur d'accès à IPv6.

Le service Tunnel Broker repose sur une architecture à base de client/serveur. Côté usager l'installation d'un simple client permet de faire la demande de tunnels au serveur. Ce client est en général authentifié. Pour le prestataire, il faut mettre en œuvre un serveur qui a plusieurs fonctions : l'interface HTML pour accueillir les demandes de tunnels des usagers et

la « comptabilité » qui peut l'accompagner, le configurateur de tunnels qui envoie les paramètres d'extrémité du tunnel entre l'équipement de concentration et celui de l'usager d'une part et le concentrateur de tunnels d'autre part.

L'accès à un *Tunnel Broker* est réalisé de la façon suivante:

L'utilisateur s'enregistre sur le site Web en indiquant les informations suivantes:

- Identification (nom, login/password, ...).
- Nombre de machines à connecter (une machine ou un site de x machines).
- Système d'exploitation et adresse IPv4 de la machine qui met en place le tunnel.

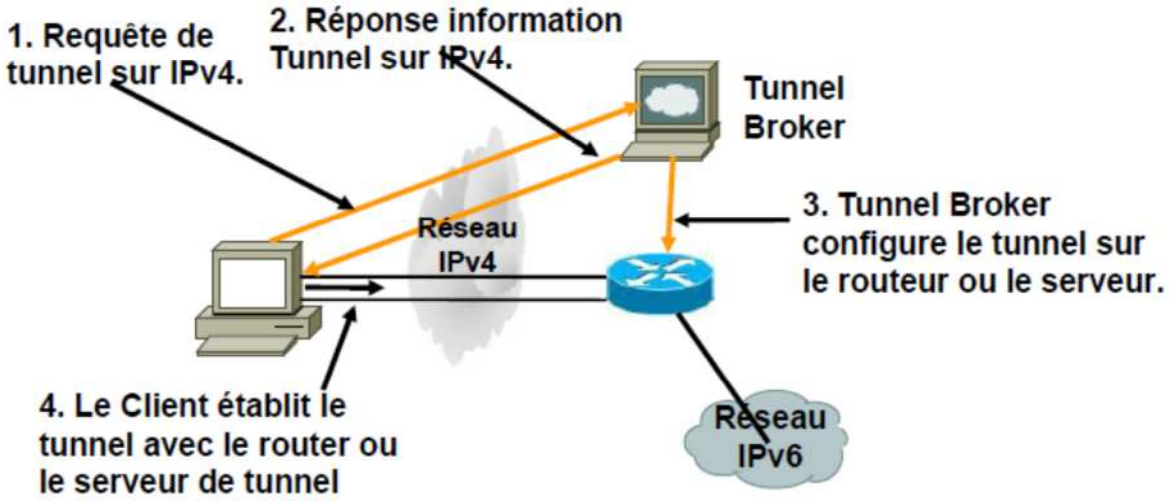


Figure III.5 : Schéma d'un tunnel Broker

Ce schéma montre comment un tunnel Broker peut être crée :

Le poste client veut se connecter au réseau IPv6 (dans cet exemple le réseau IPv6 est représenté par le routeur), pour ce faire le poste client envoie une requête au pc serveur (fournisseur de service tunnel Broker) en s'identifiant à ce serveur à travers un site web spécifique (site web des fournisseurs de ce service), le serveur renvoie une réponse au client comportant la création de tunnel entre ce dernier et le réseau IPv6.

❖ **Avantages et inconvénients :**

➢ **Avantage :**

- Facile à réaliser pour des petites topologies.

➢ **Inconvénients :**

- Il faut avoir un compte.
- payer un abonnement.
- limiter le nombre de machines.

III.3.3.Tunnel automatique :

Il s'agit d'un tunnel ouvert dynamiquement, à la demande, l'objectif est de permettre d'étendre la connectivité IPv6 en traversant des réseaux IPv4.

Les méthodes de tunnels automatiques les plus connus sont :

- Les tunnels Teredo ;
- Les tunnels 6over4 ;
- Les tunnels 6to4 ;
- Les tunnels ISATAP ;

a. Tunnel Téredo :

Il s'agit de faire passer un tunnel IPv6 dans un réseau IPv4 en s'appuyant sur une méthode de translation d'adresse NAT.

Cette méthode repose sur l'existence d'hôtes spécifiques (serveurs) agissant en tant que serveur Téredo.

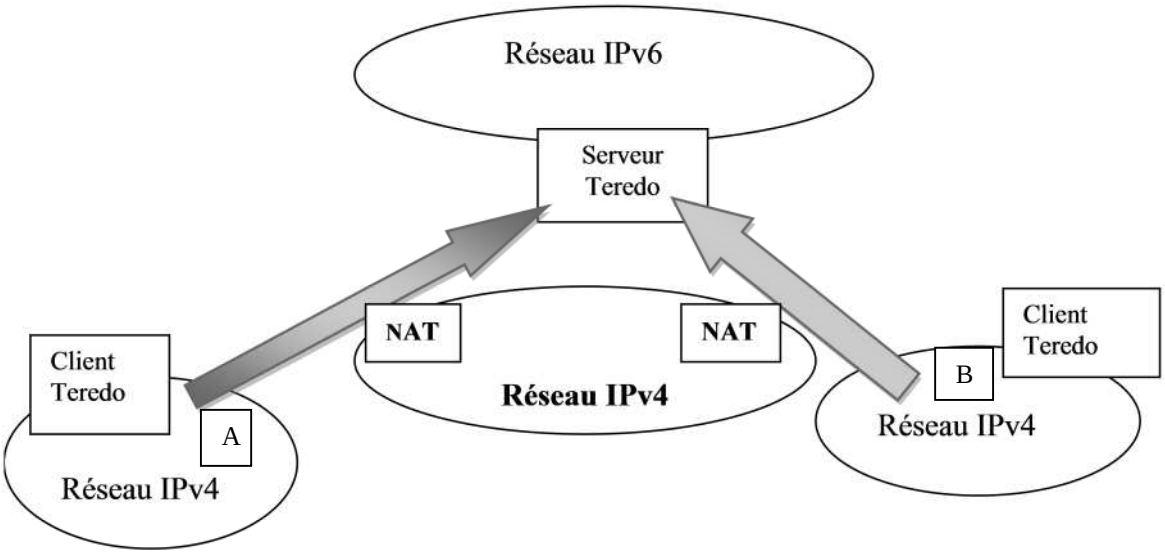


Figure III.6 : Schéma d'un tunnel Téredo

Cette figure montre que A et B sont accessibles par le biais d'une translation d'adresse.
Le principe est le suivant :
L'adresse IP de serveur est directement incluse dans la partie réseau des adresses A et B.

b. Tunnel 6over4

La méthode 6over4 permet à plusieurs machines IPv6 isolés (mais connectées par un réseau IPv4 supportant le multicast), de créer un réseau local IPv6 (comme si elles étaient situés sur le même lien) en s'appuyant sur un domaine multicast IPv4. De plus, si l'une de ces machines est un routeur IPv6 connecté à un autre réseau IPv6, toutes les machines peuvent avoir accès à ce réseau. L'identifiant d'interface utilisée pour déterminer l'adresse d'une machine est l'adresse IP. L'adresse lien-local d'une machine utilisant le protocole *6over4* est donc FE80::192.168.1.1 ou 192.168.1.1 est son adresse IPv4. On peut également utiliser un préfixe IPv6 propre au site s'il y a un routeur IPv6 pour faire l'annonce du préfixe. Le domaine IPv4 doit obligatoirement pouvoir transmettre du trafic multicast car le multicast est utilisé pour transmettre les paquets multicast IPv6, lui-même nécessaire pour le fonctionnement du lien local.

c. Tunnel 6to4

La méthode *6to4* peut être utilisée pour interconnecter entre eux des sites *6to4* par l'intermédiaire d'un réseau IPv4. Les routeurs *6to4* ont besoin d'une double pile IP et d'une adresse IPv4 unique pour pouvoir relier un site entier.

Pour cela, chaque routeur se crée un préfixe IPv6 unique (sans avoir besoin de l'allouer auprès d'une quelconque instance) et l'utilise sur tous son site. Le préfixe est construit en ajoutant l'adresse IP du routeur au préfixe 2002::/16. On obtient ainsi un préfixe de 48 bits auquel on peut ajouter un identifiant de réseau (16 bits) et l'identifiant de l'interface. Chaque machine dispose donc d'une adresse IPv6 unique sans avoir à en faire la demande. Ces adresses peuvent même (et c'est conseillé) être renvoyés par le serveur de DNS pour pouvoir être joint en IPv6 par les autres sites 6to4.

Quand une machine veut envoyer un paquet à une machine située sur un domaine 6to4, elle effectue la démarche suivante:

- Requête DNS avec le nom long
- Le serveur de DNS renvoie l'adresse 2002::c001::0203::0001::ID_Interface
- La machine source envoie le paquet sur son réseau IPv6
- Le paquet va arriver à un routeur *6to4* (qui peut router le préfixe2002::/16)
- Celui-ci va encapsuler le paquet IPv6 dans un paquet IPv4 et l'envoyer à l'adresse 192.1.2.3 (c001::0203)
- La machine 192.1.2.3 (qui est un routeur 6to4) des encapsule le paquet IPv6 et l'envoie sur son réseau IPv6 .

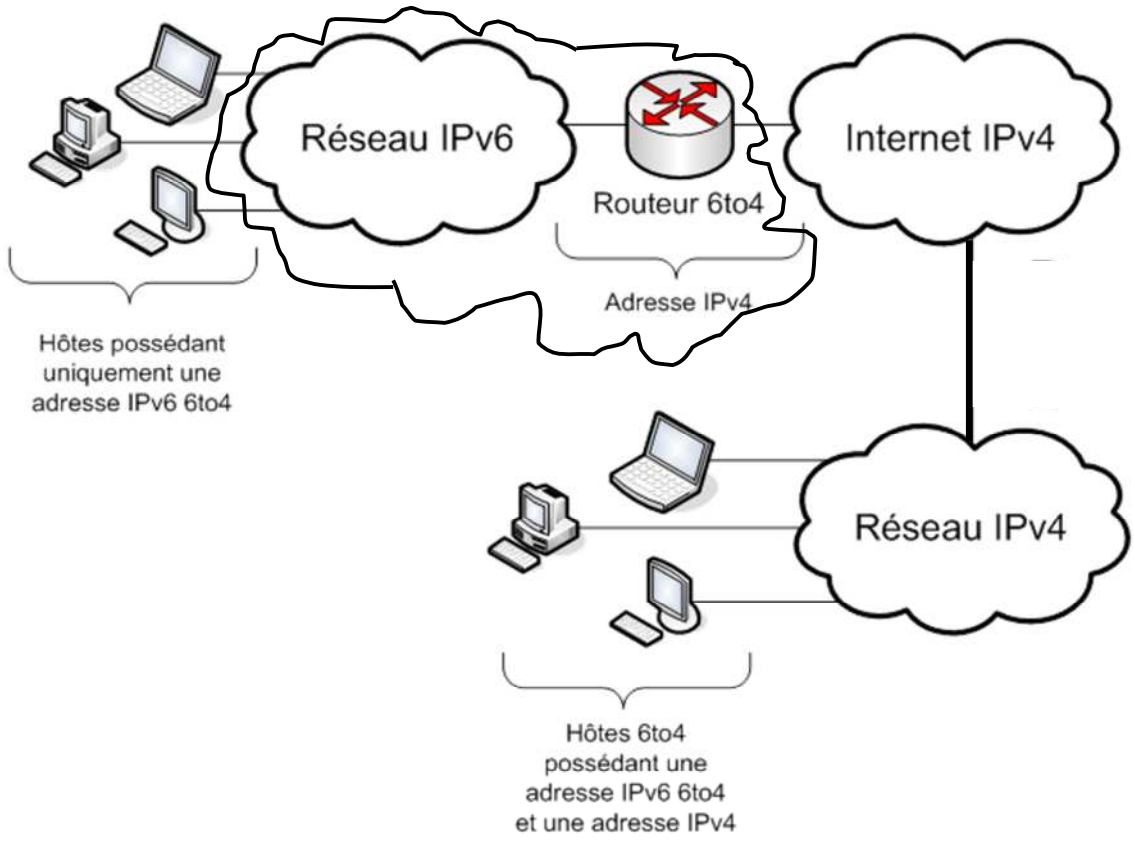


Figure III.7: Schéma d'un tunnel 6to4.

❖ **Avantages et inconvénients :**

➢ **Avantages:**

- Permet de router du traffic IPv6 même si l'infrastructure du réseau est IPv4.

➢ **Inconvenient:**

- Routage peut être asymétrique.
- Délais peuvent être élevés à cause des tunnels.

d. Intra-site automatic tunnel addressing protocol(ISATAP):

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), est une technique de tunneling qui autorise la communication en *IPv6* au travers d'un réseau *IPv4* de deux machines entre elles, ou de deux routeurs entre eux, ou encore d'une machine et d'un routeur.

ISATAP sera utilisé lorsqu'il n'y a pas de connexion IPv6 native. Ce protocole définit une méthode pour générer une adresse à partir d'une adresse IPv4.

L'adresse est déterminée en réunissant [Préfixe de 64 bits]:0:5EFE: et les 32 bit de l'adresse IPv4 de la machine.

Le préfixe de 64 bits peut-être de type local, global ou encore 6to4. Il sera en général, annoncé par un routeur. Ainsi, une machine possédant une adresse 192.168.41.30 aura pour adresse ISATAP de lien local (après simplification des zéros) FE80::5EFE:192.168.41.30.

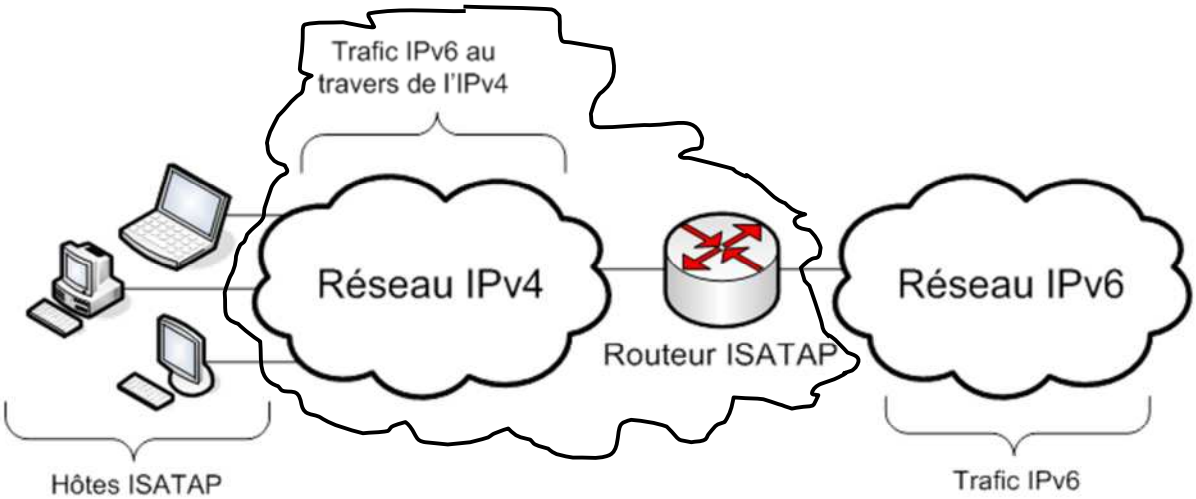


Figure III.8 : Schéma d'un tunnel ISATAP

Discussion :

Les méthodes Dual Stack, Tunneling et Translation permettent un déploiement d'IPv6 dans un environnement IPv4. Différents scénario de transition ont été élaborés pour permettre un passage progressif vers le nouveau protocole. C'est pour ça que nous avons choisi une de ces méthode, et la faire la simuler avec le logiciel GNS3. Nous allons présenté notre application qui consiste à réaliser un Tunnel ISATAP.

Introduction :

Dans ce chapitre nous allons présenter notre application qui consiste à créer un tunnel ISATAP entre deux machines qui ont toute les deux une adresse ipv6 mais situées dans un réseau IPv4 puis, on va simuler la solution en utilisant le logiciel de simulation graphique GNS3.

Commençons d'abord par la présentation de GNS3.

VI.1.Définition de logiciel de simulation :

GNS3 est un simulateur (ou bien Émulateur) de réseau graphique qui permet de simuler des réseaux complexes.

GNS3 est un excellent outil complémentaire, utiles pour les ingénieurs réseaux et administrateur réseaux et toute personne souhaitant passer les certifications CISCO. Il peut également être utilisé pour expérimenter les fonctionnalités d'IOS ou pour vérifier des configurations destinées à être déployées sur de vrais routeurs. GNS3 est un logiciel libre qui fonctionne sur de multiples plateformes, incluant Windows, Linux.

L'avantage majeur de GNS3 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.

VI.2.Installation :

Pour commencer nous avons installé le logiciel GNS3 sur notre pc (Windows 8) et pour ça, nous avons suivi les étapes suivantes :

Avec un double clic sur le fichier source GNS3 -0.8.6-all-in-one , on aura la(figure VI.1).

Figure VI.1 : Présentation de la première étape de l'installation du logiciel.

On cliquant sur **Next** l'assistant de l'installation du logiciel GNS3, nous invitera à finaliser les étapes de l'installation en suivant les figures VI.2, et VI.3 ; tout en cliquant sur **Install,** pour avoir à la fin l'icône du logiciel figure VI.4.

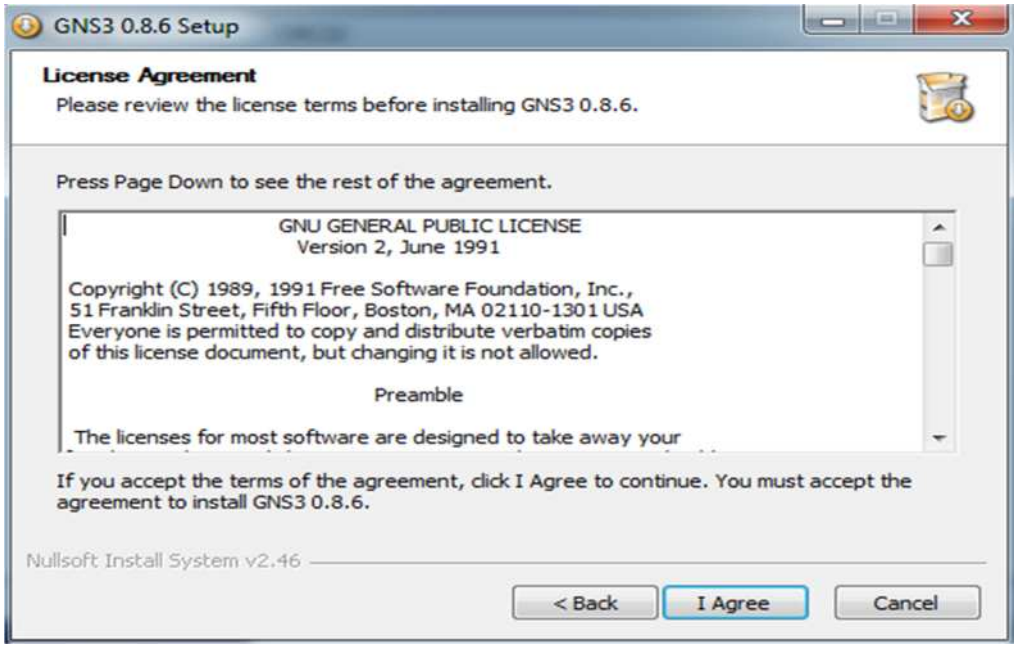


Figure VI.2 : Licence agreement de GNS3.

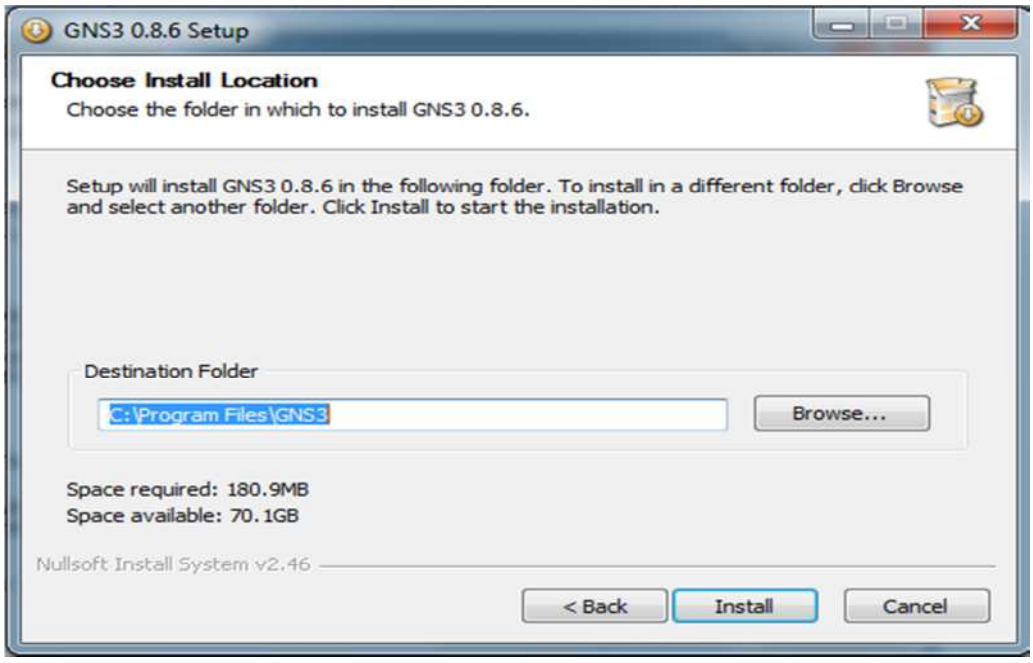


Figure VI.3 : Installation de GNS3

Une fois l'installation est terminée on aura sur le bureau de notre ordinateur l'icône suivante :

Figure VI.4 : L'icône du logiciel GNS3

En cliquant sur l'icône précédente, la fenêtre suivante s'affichera :

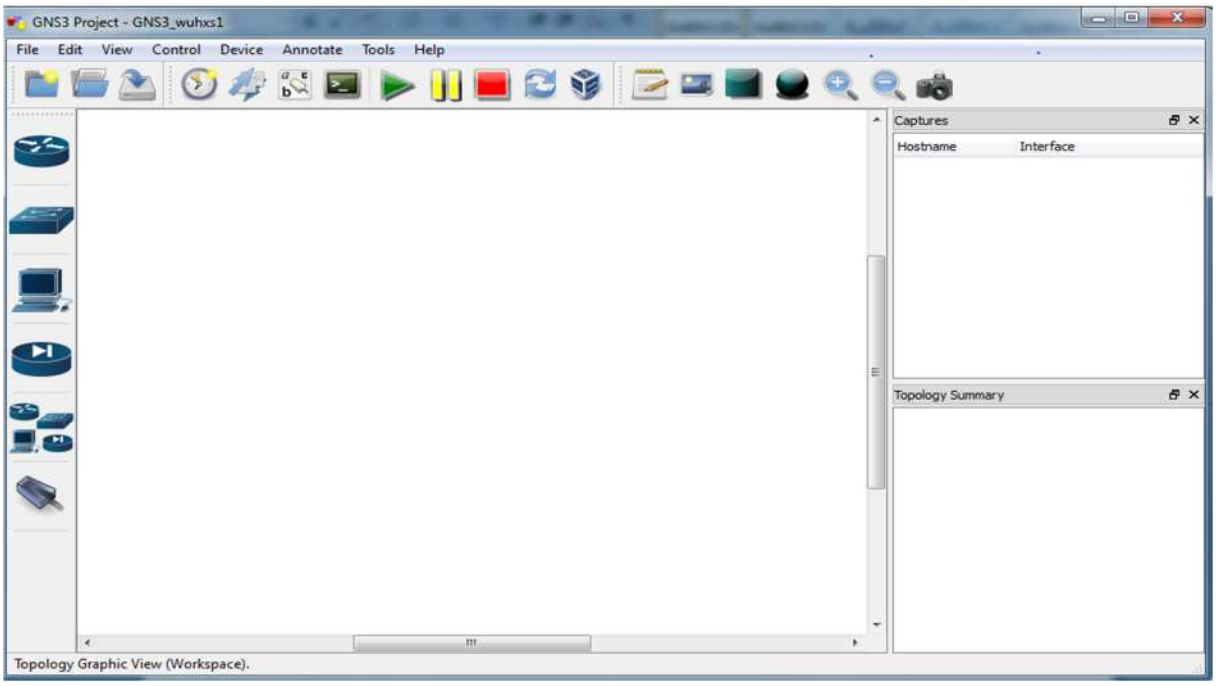


Figure VI.5 : Présentation de l'interface GNS3.

Pour utiliser GNS3 avec les Routeurs proposés dans son interface, il est nécessaire de les associer à un fichier IOS.

VI.2 .1. L'ajouter des IOS :

On crée un sous-répertoire IOS dans le répertoire de GNS3 dans lequel on va mettre nos IOS téléchargés. L'ajout des IOS se fait comme suit :

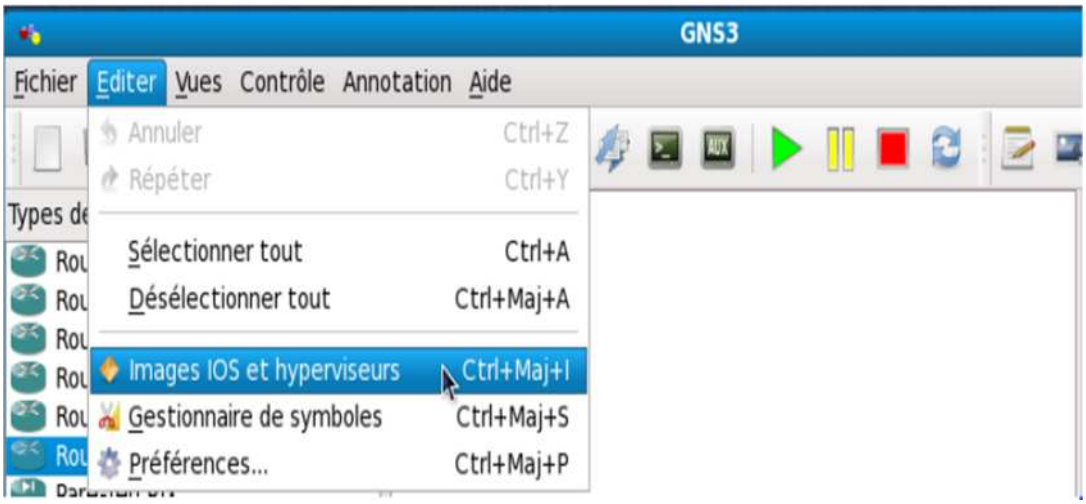


Figure VI.6 : L'ajout des IOS dans le répertoire de GNS3

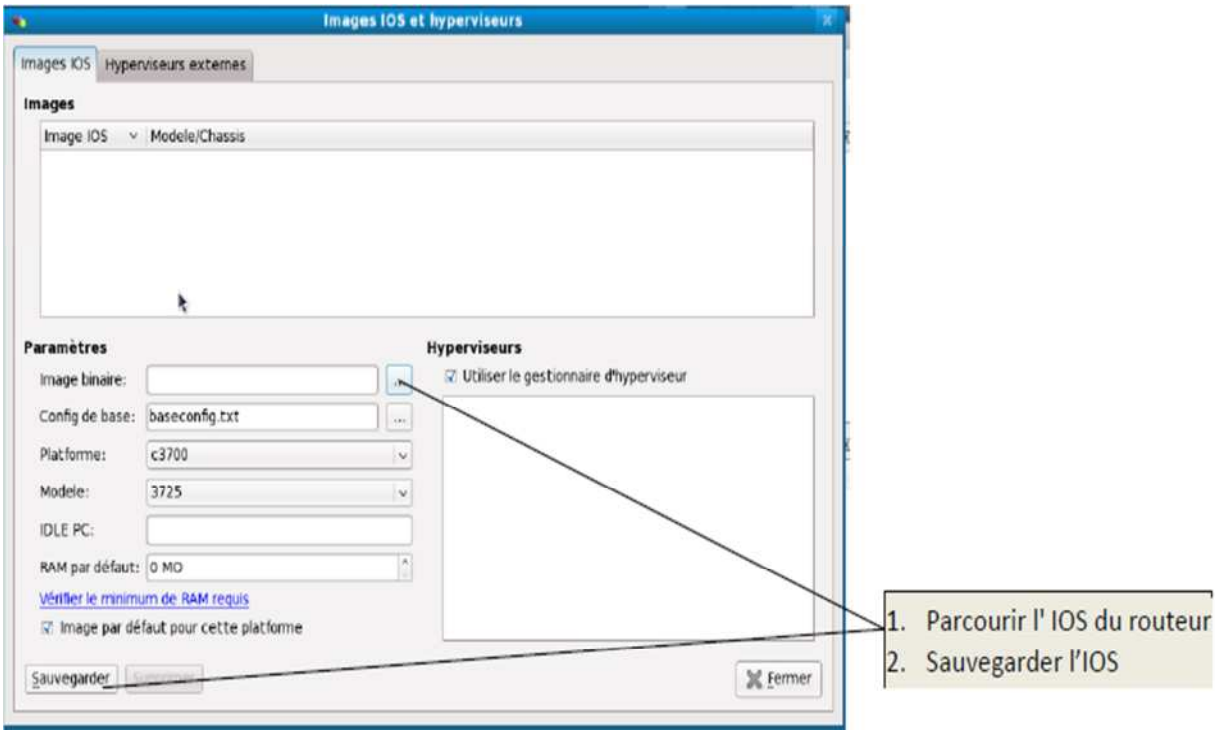


Figure VI.7 : Création d'un dossier pour le fichier IOS.

VI.2.2. Présentation de l'application :

Nous allons réaliser la topologie suivante avec utilisation des protocoles de routage dynamique comme OSPF et EIGRP:

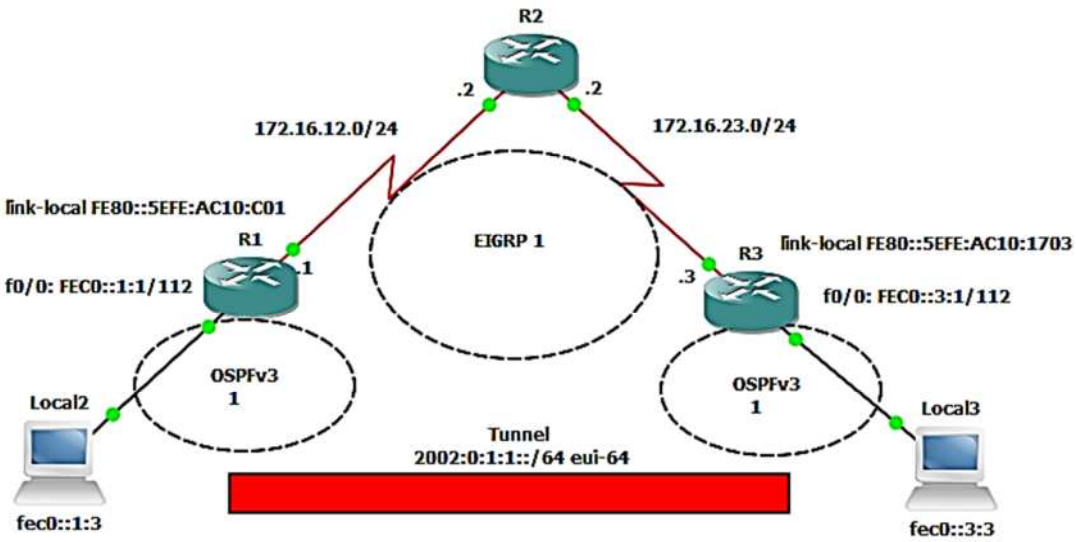


Figure VI.8 : Présentation de la topologie de réseau.

On a utilisé trois routeurs c3700 et deux PCs local2 et local3 pour réaliser les tests ou bien la simulation. On a procédé comme suit :

Sélectionner les routeurs c3700 (R1, R2 et R3)

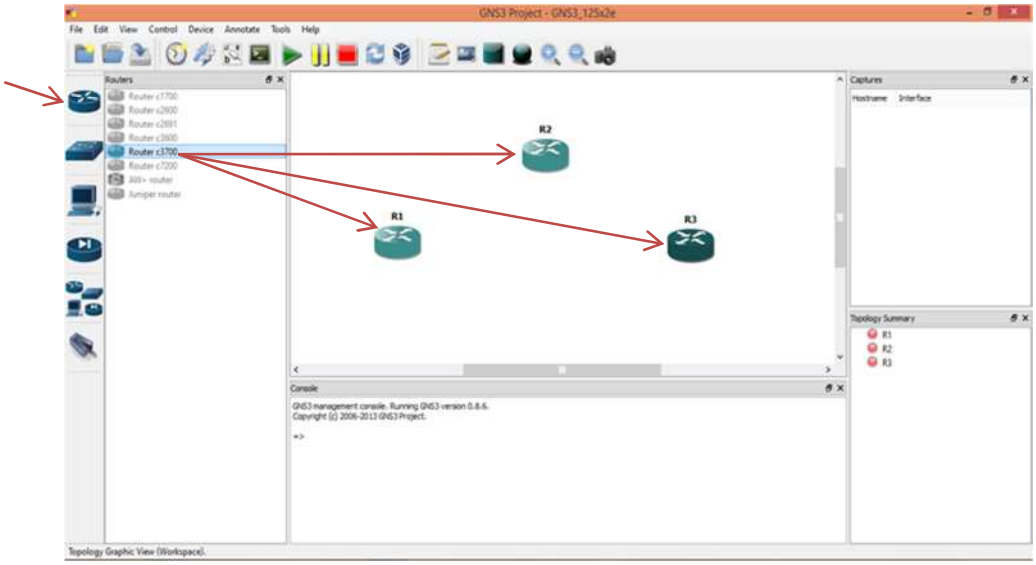


Figure VI.9 : Présentation des routeurs sur GNS3.

Ramener les PCs Local2 et Local3 :

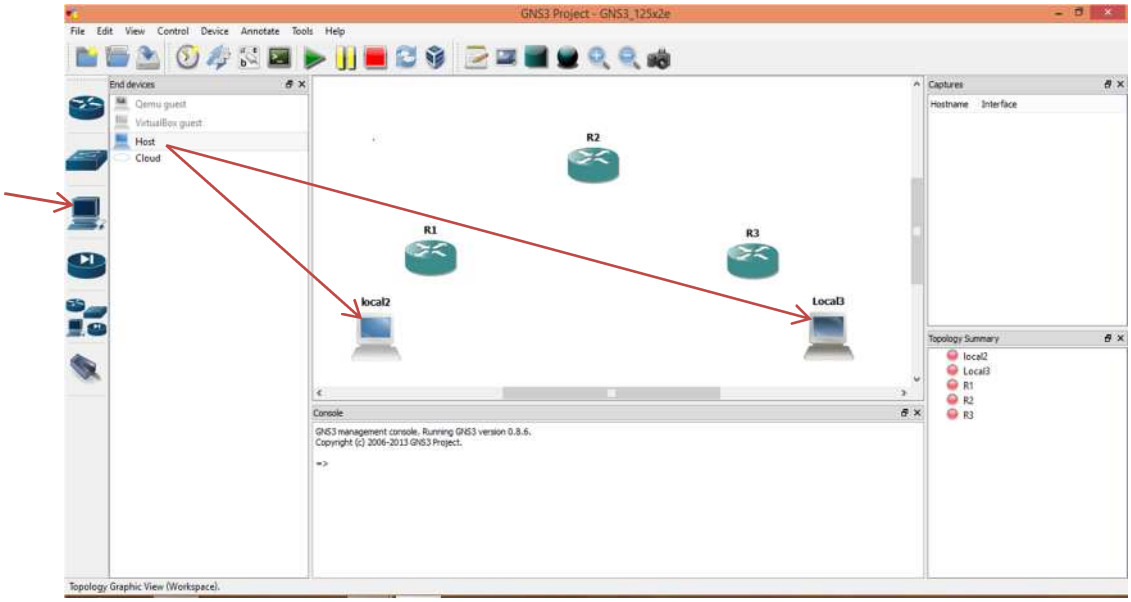


Figure VI.10 : Présentation des PCs sur GNS3.

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

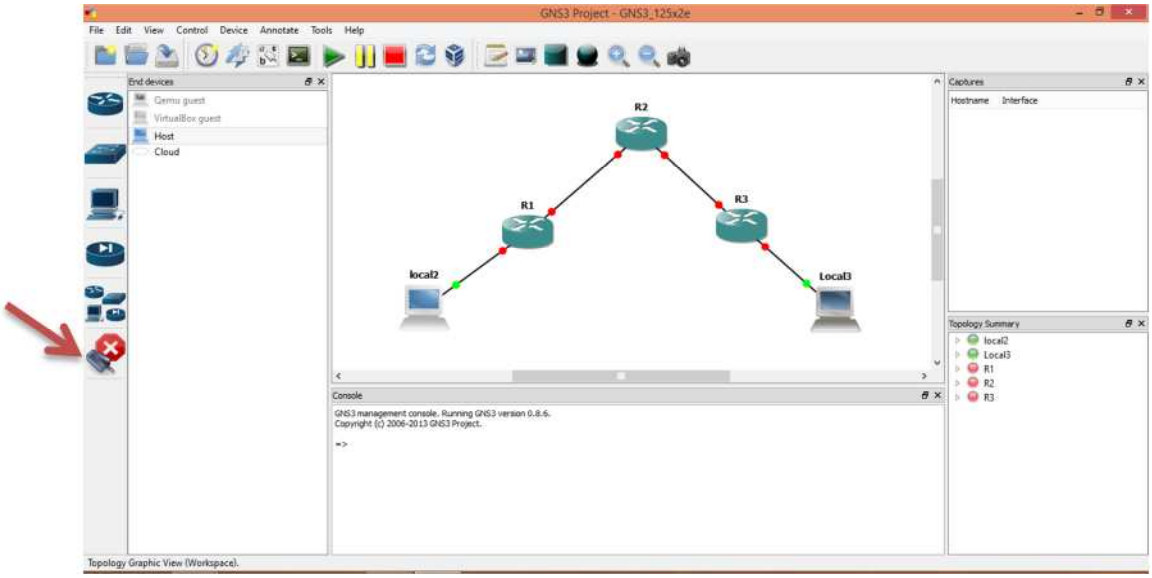


Figure VI.11 : Présentation des équipements connectés

VI.3. Configuration des routeurs :

Pour effectuer la configuration nécessaire des routeurs, il faut accéder à la Console de chaque routeur, pour cela, il suffit de cliquer sur l'icône « Start console ».

Pour la configuration des routeurs R1 et R3, on crée une interface virtuelle nommée Tunnel0 qui utilise la plage d'adresse IPv6 2002 :0 :1 :1 ::/64. EUI-64 pour "Extended Unique Identifier" ou "identifiant unique étendu" est une façon de former les adresses IPv6 de type unicast. On dit de cette méthode de formation des adresses qu'elle est unique car elle se base, pour se former, de l'adresse MAC de la carte réseau qu'elle utilise. Pour rappel, les adresses MAC sont des identifiants uniques à chaque carte réseaux. Cela permet à un hôte de s'attribuer à lui-même une adresse IPv6. C'est un plus par rapport à l'IPv4 qui nécessitait aux postes, pour avoir une IP afin de communiquer, de repérer un serveur DHCP et de lui demander un IP.

Pour la former, il suffit d'ajouter à partir du troisième octet de l'adresse MAC de l'interface des deux octet FF FE.

Il faut aussi activer le tunnel ISATAP au niveau des interfaces et utiliser bien sûr des protocoles de routage dynamique. Notre choix est porté sur OSPF pour IPv6 et EIGRP pour IPv4. Pour les interfaces séries, l'utilisation de l'adresse link-local a pour but d'échanger les mises à jour de routage entre les liens directement connectés. Cette adresse est utilisée pour identifier l'interface au niveau lien uniquement. Elle permet à un hôte de communiquer simplement avec les autres hôtes placés sur le même lien. Elle est utilisée notamment pour l'auto configuration. Les datagrammes ayant cette adresse dans le champ source ne sont jamais transmis hors du lien par les routeurs.

VI.3.1. Configuration de routeur R1 :

L'ensemble de la configuration du routeur R1 est montrée par la figure suivante :

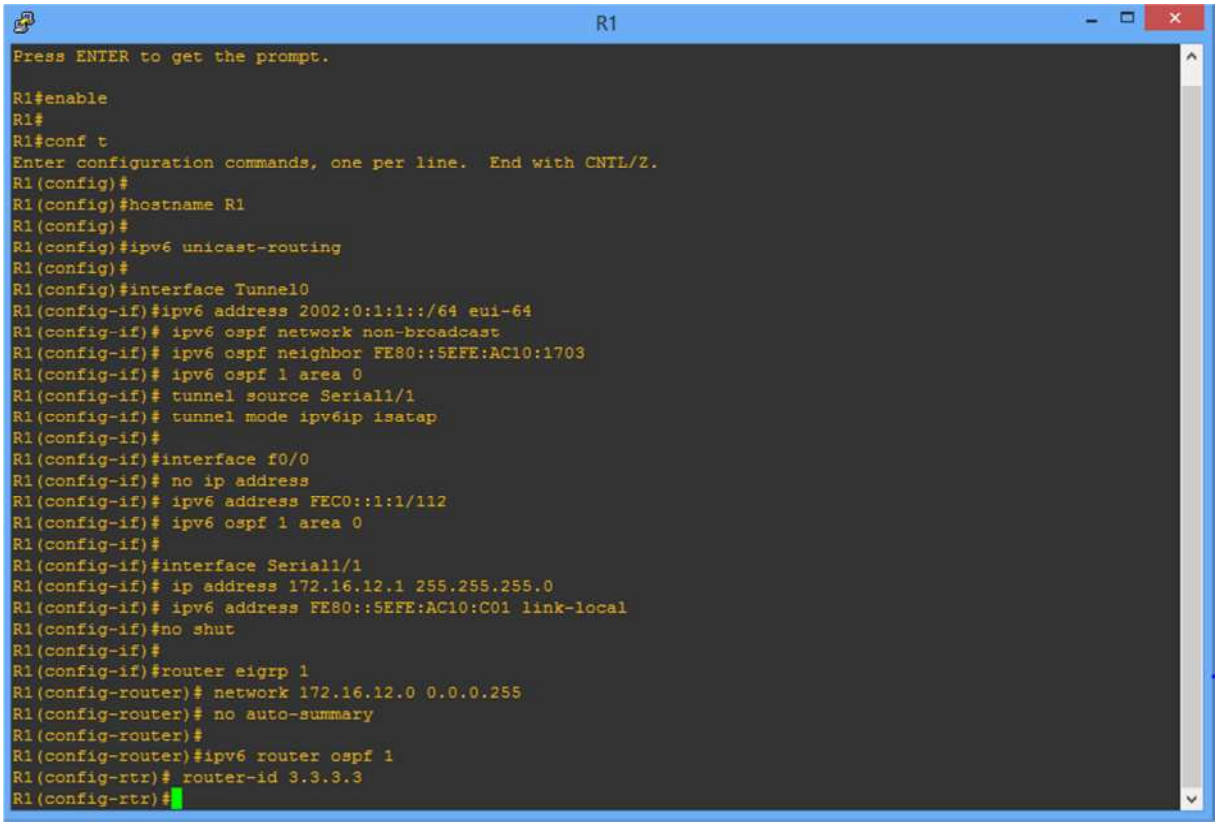


Figure VI.12 : Configuration de routeur R1.

Nous allons expliquer le fonctionnement des commandes utilisées pour la configuration du routeur R1 dans le tableau suivant:

Commande	**Fonctionnement**
hostname R1	Fixer le nom du routeur comme R1
ipv6 unicast-routing	Activer le routage ipv6
interface Tunnel0	Créer une interface virtuelle Tunnel0
ipv6 address 2002 :0 :1 :1 ::/64 eui-64	Attribuer une adresse ipv6 à l'interface Tunnel0 en utilisant l'option eui-64.
ipv6 ospf network non-broadcast	Désactiver la diffusion des mises à jour OSPF sur les Routeurs. Les interfaces Tunnel sont des interfaces point-à-point alors qu'ISATAP est une solution point-vers-multipoints. Dans le cas d'utilisation de la diffusion, les mises à jour ne vont pas être circulées. Donc la solution est d'annuler la diffusion est d'utiliser la solution statique avec la déclaration du saut suivant.

ipv6 ospf neighbor FE80::5EFE:AC10 :1703	Cette commande utilise la diffusion statique de la mise à jour du routage car nous allons declarer l'adresse du prochain saut FE80::5EFE:AC10:1703. AC10:1703 corresponds à 172.16.23.3 de R3, avec en HEXA: 172 = AC, 16 = 10, 23 = 17, 3 = 03.
ipv6 ospf 1 area 0	Activer le Protocol du routage dynamique OSPF au niveau de l'interface Tunnel0 avec un numéro de processus 1 et la zone 0.
tunnel source Serial1/1	Définir l'interface Serial1/1 comme la source du tunnel
tunnel mode ipv6 isatap	Activer le mode tunnel ISATAP au niveau de l'interface Tunnel0
interface f0/0	Accéder à l'interface fast-ethernet 0/0
no ip address	Désactiver l'adressage ipv4
ipv6 address FEC0::1 :1/112	Attribuer une adresse ipv6 à l'interface f0/0 avec un masque sous-réseau 112.
ipv6 ospf 1 area 0	Activer le routage dynamique OSPF.
interface Serial1/1	Accéder à l'interface série 1/1
ip address 172.16.12.1 255.255.255.0	Attribuer l'adresse ipv4 avec un masque sous réseau /24 à l'interface série 1/1.
ipv6 address FE80 ::5EFE :AC10 :C01 link-local	Utiliser l'adresse link-local pour l'interface Serial1/1. Pour l'acheminement des paquets, c'est l'adresse ipv4 qui sera utilisée, par contre l'adresse link-local sera utilisée seulement pour l'acheminement des mises-à-jour.
no shut	Activer l'interface. Nous pouvons ne pas utiliser cette commande car dans le cas d'utilisation de GNS3 les interfaces sont activées après l'utilisation de "Start".
router eigrp 1	Activer le protocole de routage dynamique EIGRP avec un numéro de processus 1 pour les réseaux ipv4.
network 172.16.12.0 0.0.0.255	Déclarer le réseau ipv4 directement connecté au routeur R1.
no auto-summary	Désactiver la sommation des réseaux car nous avons deux réseaux ipv4 non adjacent.
ipv6 router ospf 1	Activer le protocole ospf pour ipv6 dans le mode global sur le routeur R1.
router-id 3.3.3.3	Donner un ID pour le R1 qui est 3.3.3.3 pour le fixer comme DR (Designated Router).

Tableau VI.1 : les commandes utilisées pour la configuration de R1.

VI.3.2.Configuration de routeur R3 :

La configuration du routeur R3 se fait de la même façon que la configuration de routeur R1, seul les adresses et le nom de routeur changent.

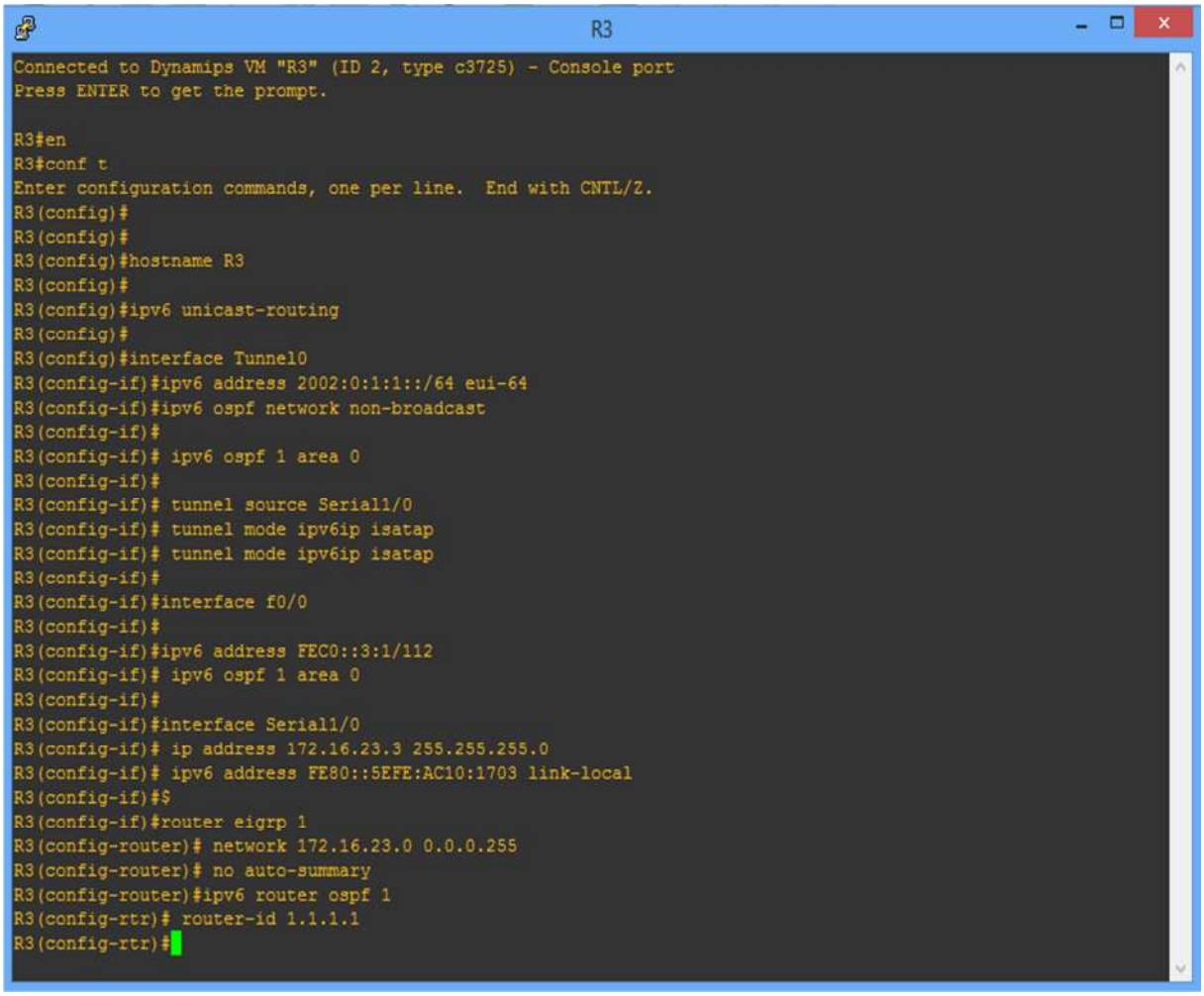


Figure VI.13 : Configuration de routeur R3.

VI.3.3. Configuration de Routeur R2 :

La configuration de R2 comporte seulement l'adressage ipv4 avec EIGRP, donc l'ensemble des commandes utilisées sont listées dans le tableau précédent seul les adresses changent et les réseaux déclarés pour le routage dynamique.

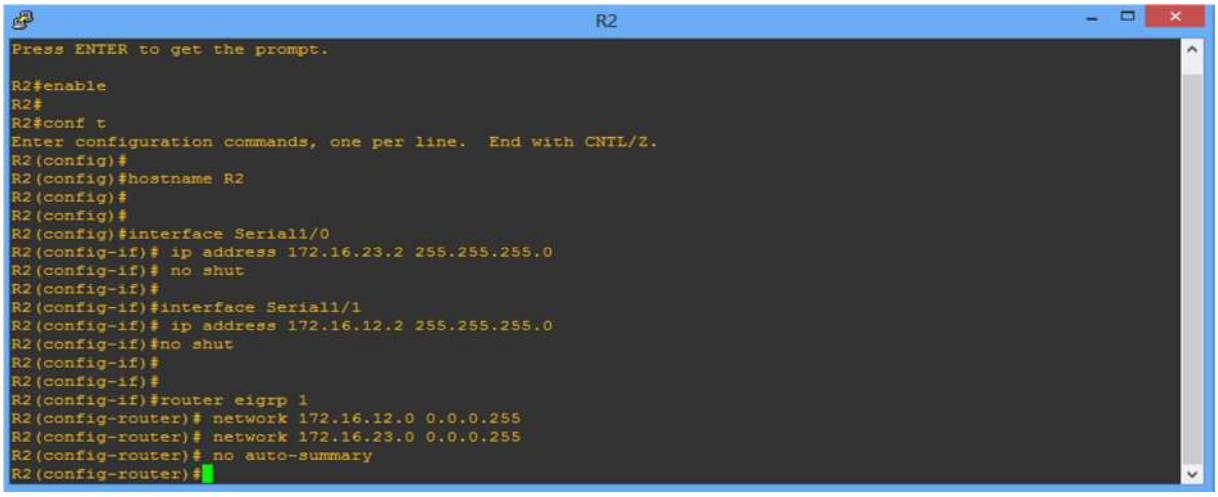


Figure VI.14 : Configuration de routeur R2.

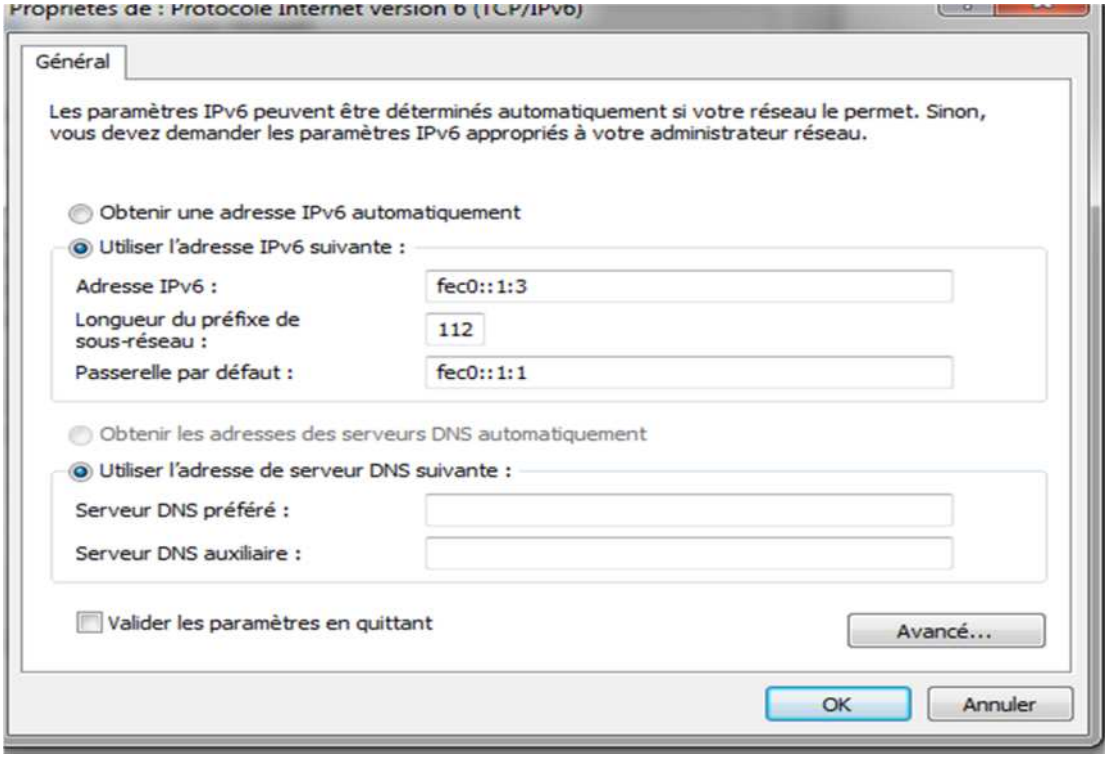
Nous allons expliquer le fonctionnement des commandes utilisées pour la configuration du routeur R2 dans le tableau suivant:

hostname R2	Fixer le nom du routeur comme R2
interface Serial1/0	Accéder à l'interface série 1/0
ip address 172.16.23.2 255.255.255.0	Attribuer l'adresse ipv4 avec un masque sous réseau /24 à l'interface série 1/0.
no shut	Activer l'interface. Nous pouvons ne pas utiliser cette commande car dans le cas d'utilisation de GNS3 les interfaces sont activées après l'utilisation de "Start".
interface Serial1/1	Accéder à l'interface série 1/1
ip address 172.16.12.2 255.255.255.0	Attribuer l'adresse ipv4 avec un masque sous réseau /24 à l'interface série 1/1.
no shut	Activer l'interface. Nous pouvons ne pas utiliser cette commande car dans le cas d'utilisation de GNS3 les interfaces sont activées après l'utilisation de "Start".
router eigrp 1	Activer le protocole de routage dynamique EIGRP avec un numéro de processus 1 pour les réseaux ipv4.
network 172.16.12.0 0.0.0.255	Déclarer le réseau ipv4 directement connecté au routeur R1.
network 172.16.23.0 0.0.0.255	Déclarer le réseau ipv4 directement connecté au routeur R1.
no auto-summary	Désactiver la sommation des réseaux car nous avons deux réseaux ipv4 non adjacent.

Tableau VI.2 : les commandes utilisées pour la configuration de R2.

VI.4. Configuration des PCs Local2 et Local3 :

Il nous reste à configurer les hôtes. Il suffit d'introduire les adresses IPv6 pour les deux PCs Local2 et Local3. Nous donnons, comme le montre les figures VI.15 et VI.16 l'adresse fec0 ::1 :3 pour Local2 et fec0 ::3 :3 pour Local3.



FigureVI.15 : Configuration du pc local2.

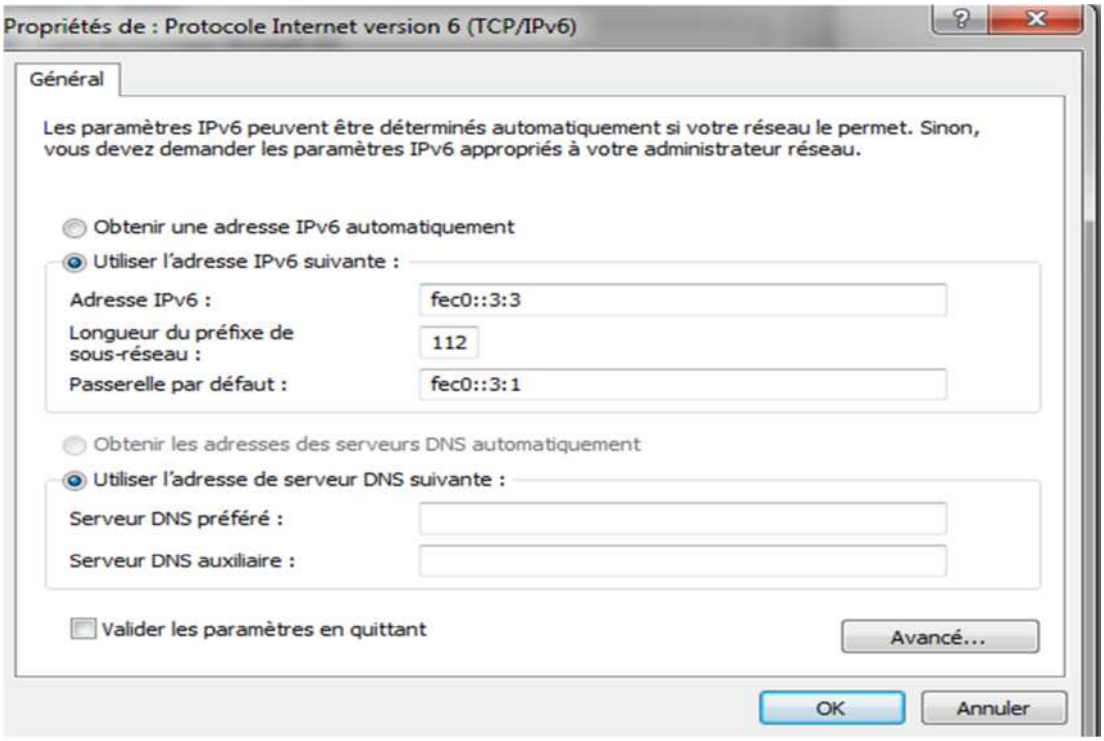


Figure VI.16 : Configuration du pc local 3.

VI.5. Tests :

Nous allons maintenant tester le fonctionnement du tunnel. Pour ce faire, nous utilisons la commande « ping » du bout au bout. Nous allons introduire sur l'invité de commande de l'hôte Local2 la commande « ping fec0 ::3 :3 » 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.

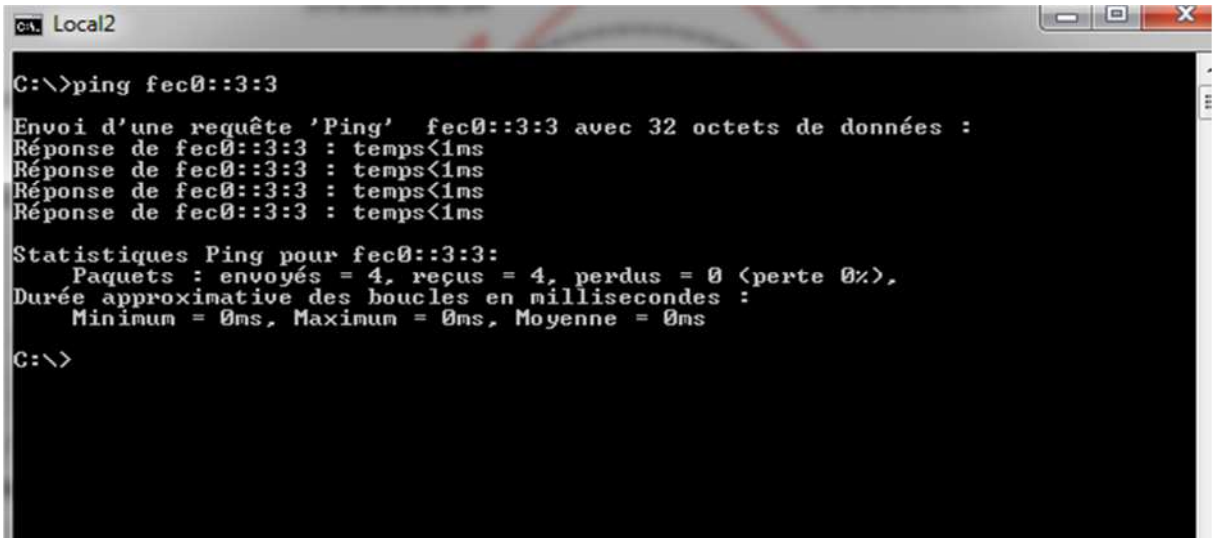


Figure VI.17: Confirmation de fonctionnement du tunnel au niveau de local 2.

Nous remarquons que le tunnel fonctionne correctement malgré la non disposition de l'adressage IPv6 pour le routeur R2 et la non disposition de l'adressage IPv4 au niveau des hôtes.

Nous allons effectuer le teste au niveau de Local3 avec l'introduction de la commande « ping fec0 ::1 :3 » juste pour confirmer la fonctionnalité du tunnel.

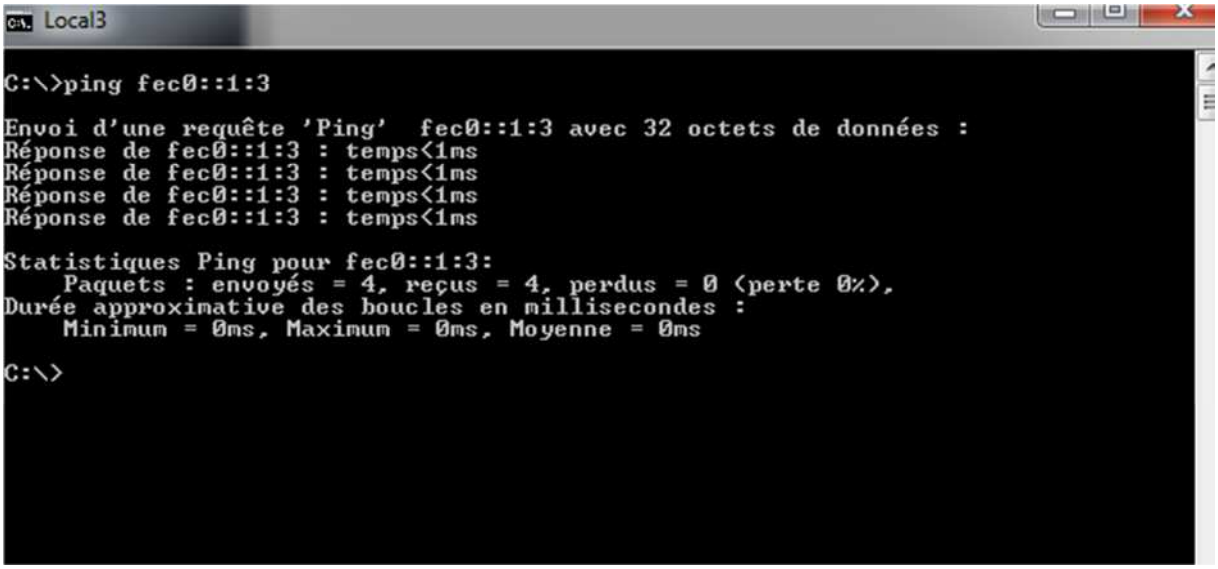


Figure VI.18 : Confirmation de fonctionnement du tunnel au niveau de local 3.

Nous remarquons que le teste à confirmer la fonctionnalité du tunnel ISATAP réalisé.

Discussion :

Afin de mener notre application à terme nous avons utilisé le logiciel de simulation GNS3 avec lequel nous avons réussi à faire réaliser le tunnel qui nous permet de connecter un réseau IP version 4 avec un réseau de version 6.

L’objectif de notre travail est d’établir une transition ou bien une migration IPv4 vers IPv6 et pour cela, on a choisi de réaliser un tunnel ISATAP qui est une des méthodes de migration dite tunnel automatique.

Pour ce faire, nous avons proposé une topologie ou bien une plateforme, cette topologie contient trois routeurs et deux PCs. Les routeurs R1et R3 sont en IPv6 et le routeur R2 est en IPv4.

Pour pouvoir réaliser ce tunnel, il fallait configurer les trois routeurs, et pour les PCs il fallait juste attribuer une adresse IPv6 pour chacun d’eux.

Nous avons simulé cette application à l’aide du logiciel GNS3.

Notre objectif (réalisation de tunnel) est atteint, de fait que le teste de connexion effectué en utilisant la commande « ping » a donné de réponse.

On peut dire que si IPv6 devient incontournable dans les années à venir, la migration va occuper des informaticiens pendant plusieurs années que ce soit pour faire la migration des réseaux, des systèmes, et des logiciels.

Ce travail nous a permet d’apprendre beaucoup à propos du protocole IP version 4, et version 6 et des réseaux en général. Ces connaissances concernent les spécifications du protocole IPv6, de son fonctionnement et de son déploiement au cœur du réseau IPv4 existant. Nous avons pu aussi renforcer, les bases théoriques acquises au sein de notre université concernant les réseaux et leurs architectures, ainsi leurs caractéristiques.

Aussi, à travers ce travail, nous avons découvert les principales méthodes de transition d’IPv4 vers IPv6 existantes actuellement (double pile, translation et tunnel) qui permettent de de faire une liaison entre les deux versions et nous avons pu nous familiariser avec le simulateur graphique GNS3 qui est très utilisé dans les réseaux.

Bibliographie

[1] : Les réseaux .Guy Pujolle, édition EYROLLES, [2006].

[2] : Réseaux informatique (Notions fondamentales) .José Dordoigne, édition eni, [2011].

[3] : Transition d'IPv4 vers IPv6 au Sénégal .Doudou Gaye [2011],

[4] :Les réseaux édition 2003 : deuxième édition -Guy Pujolle avec la contribution de Olivier Salvaton

[5] : Apprendre les réseaux ;Paul Whithead. édition First interactive[1999].

[6] : Cour TCP/IP : école régionale de télécommunication de Constantine.Benlaksira Ramzi .[2006]

[7]: Adressage réseau IPv4 vers IPv6 .Mansouri Sofiane[2011], l'université Mouloud Mammeri.

[8] : La prise en compte de la qualité de service Q_oS dans le protocole IPv6. Berkani Nassim[2011], l'université Mouloud Mammeri.

[9] :Rapport de stage de fin d'étude, Ahmed Sahnoun, l'université de Lyon,[2002].

[10] : Migration IPv4/IPv6. M.Lafon , master, l'université de layon, [2000].

[11] : Cours IPv6, Salmon Nicolas,[2010] .

[12] :IPv4-to-IPv6 transition and co-existence strategies, Tim Roney,édition BT diamond ip,[2011].