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

Université Mouloud Mammeri De Tizi-Ouzou
Faculté De Génie Electrique Et Informatique
Département D'Électronique

Mémoire De Fin D'étude Pour L'obtention Du Diplôme De Master En Réseaux Et Télécommunications

Présenté par :

Mr : REKHIS Mourad

Mr : SEGUENI Achour

Thème

Migration De IPv4 vers IPv6

Devant le jury composé de :

Président : Mr ZIANI Arezki	Professeur
Examinateur : Mr ATTAF Youcef	Maitre de conférence classe B
Encadreur : Mr SEHAD Mounir	Maitre de conférence classe A

Promotion 2018

Remerciements

Avant tout, nous remercions Allah tout puissant d’avoir donné la force et le courage pour
surmonter toutes les difficultés rencontrées durant toute l’année.

Nous remercions nos parents, pour tout leur amour, leur encouragement, et leur soutien.

Nous tenons à remercier notre encadreur SEHAD Mounir pour sa disponibilité, son écoute et ses conseils.

.

Nos remerciements également à tous les professeurs et enseignants qui ont collaboré à notre formation depuis le premier cycle d’études jusqu'à la fin de notre deuxième cycle.

Nous remercions les membres du jury qui ont bien voulu nous honorer, assister à notre soutenance et évaluer notre travail.

Et enfin à tous ceux qui ont soutenu et enrichi ce travail de près ou de loin par leur réflexion et leur expérience.

DÉDICACES

En premier lieu, je dédie ce travail à :

Mon exemple éternel mon très cher et adorable père Brahim
La flamme de mon cœur, ma vie et mon bonheur
ma très chère et
douce et adorable mère Saliha qui m'ont aidé durant tout mon cursus,
pour leurs encouragements, leurs patiences et leurs précieux conseils.
Je m'adresse à dieu les vœux
les plus ardents pour la conservation de leur santé et de leur vie.

Mes chères sœurs : Louiza, Tinhinane ,Ferroudja et Kenza

Et à tous mes amis et à tous mes camarades de session

Et à tous ceux qui m'ont aidé de près ou de loin, pour leur soutien moral.

Enfin je dédie ce travail à moi et mon binôme : Mourad à qui je souhaite un avenir plein de joie et de réussite.

Achour

DÉDICACES

Je dédie ce modeste travail qui est le résultat d'accomplissement de longues années

d'études, en premier lieu à :

A ma très chère mère Houria, pour son grand amour, son fort soutien et ses précieux conseils,

qui ma éclairé le chemin de ma réussite. Que dieu la protège.

A mon très cher père Amar, qui m'as vraiment aidé durant toutes ces années avec son soutien et ses conseils.

A mes frères et mes sœurs qui mon vraiment soutenu

et me donner du courage durant mon cursus.

A toute ma famille sans particulier, et à tous mes amies qui me connais

A mon binôme Achour que j'ai l'honneur de travailler avec

lui et qui je souhaite un

avenir plein de joie et de réussite.

A toutes les personnes qui mon soutenu de près ou de loin durant mes année d'études.

Mourad

Tables Des Matières

La table des matière

Liste Des Figures

Liste des figures

Liste Des Abréviations

Liste des abréviations

6rdI : Pv6 Rapid Deployment

AH: Application Header

AFRINIC: African Network Information Centre

APNIC: Asia Pacific Network Information Centre

ARIN: American Registry for Internet Numbers

ASCII: American Standard Code for Information Interchange

BSD : Berkeley Software Distribution

CIDR: *Classless Inter-Domain Routing*

DCS: Digital Cellular System ou Digital Communication System

DF: Don't Fragment

DH: Data Header

DH : Délimitateur de trame

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

EBCDIC: Extended Binary Coded Decimal Interchange Code

ETTD : Equipement terminal de traitement de données

FAI: Fournisseur d'accès à Internet

FTP: File Transfer Protocol

GRE: Generic Routing Encapsulation

GSM: Global System for Mobile Communications

HTTP: HyperText Transport Protocol

IANA: Internet Assigned Numbers Authority

ICANN: Internet Corporation for Assigned Names and Numbers

ICMP: Internet Control and error Message Protocol

ID*:* Identity

IEEE: Institute of Electrical and Electronics Engineers

IP: Internet Protocol

IPv4: Protocol Internet version 4

IPv6: Internet Protocol version 6

ISATAP: Intra-site Automatic Tunnel Addressing Protocol

LAN: Local Area Network

LACNIC : Réseaux d'Amérique Latine et des Caraïbes.

MAC: Media Access Control

MF: More Fragments

MAN: Metropolitan Area Network

MTU: Maximum Transfer Unit

NAT: Network Address Translation

NAT-PT: Network Address Translation-Protocol Translation

NH: Network Header

OS: Operating System

P2P: peer-to-peer

PAN: Personal Area Network

PH: Presentation Header

PH: Processing Header

PPP: Point to Point Protocol

RFC: Request For Comments

RIR ou **RIAR:** Regional Internet Address Registries

RIPE-NCC : Réseaux IP Européen (Network Coordination Centre),

SH: Session Header

SIIT: Stateless IP/ICMP Translator

SMTP: Simple Mail Transfer Protocol

TELNET: Terminal network ou Telecommunication network

TH: Transport Header

TOS: Type of Service

TTL: Time to Live

UDP: User Data Protocole

WAN: Wide Area Network

Wi-Fi: Wireless Fidelity

Introduction Générale

Introduction Générale

Dès le début des années 1990, l'évolution du réseau Internet semblait compromise à très court terme, car la conception du protocole IP (Internet Protocol) limitait le nombre d'équipements qui pouvaient s'y connecter. À l'origine, en 1973, ce réseau ne devait servir qu'à relier une centaine de machines. En fait, de nombreuses catégories d'utilisateurs sont très vite venues s'y joindre. Ce furent tout d'abord les scientifiques et les universitaires ; puis, en 1992, le réseau fut ouvert aux activités commerciales avec le succès que l'on sait. L'Internet n'avait pas été prévu pour supporter la croissance exponentielle du nombre d'équipements connectés. Le réseau est 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. En effet, dès 1993, des mesures d'urgence avaient été prises. Cela a permis de retarder l'échéance de quelques années.

Les ingénieurs et chercheurs travaillant au sein de l'organisme de standardisation de l'Internet ont mis à profit ce délai pour concevoir une nouvelle version du protocole, s'affranchissant des limites imposées par l'actuelle version. Pour éviter toute confusion, la version initiale est désormais appelée IPv4. La version 5 ayant déjà été attribuée à un protocole expérimental, la version issue de ces travaux a été baptisée IPv6.

À travers ce thème, nous allons étudier l'adressage IPv4 et IPv6, et diverses notions d'IPv6 et IPv4 se qui permettra au lecteur de se plonger dans les deux versions du protocole internet. Même si les différences peuvent paraître importantes, le changement est important pour chaque personne habituée à travailler avec un réseau IPv4. Enfin on va présenter les différents mécanismes de transition d'IPv4 vers IPv6 ainsi que des scénarios de déploiement.

Ce travail est organisé en quatre chapitres :

Le premier chapitre porte sur les notions et concepts de base des réseaux .

Le deuxième chapitre est dédié à la présentation de deux versions du protocole IP qui appartient à la famille de protocoles de communication de réseau informatique conçus pour être utilisés par Internet. Le protocole IP est au niveau 3 dans le modèle OSI.

Le troisième chapitre est consacré à la présentation des différents moyens de transition IPv4 vers IPv6 permettra d'y voir un peu plus clair dans la multitude des normes et des techniques existantes, à savoir la double pile, le tunneling et la translation.

Dans le quatrième chapitre nous présentons le test par simulation au moyen du logiciel «Packet Tracer» de 3 méthodes de translation IPv4 vers IPv6 à savoir : la double pile, le tunneling et la translation. Et nous terminons par une conclusion.

CHAPITRE I :

Notions Et Concepts De Base Sur Les Réseaux

I.1 Préambule :

Dans cette partie, nous allons apprendre beaucoup de théorie. Dans un premier temps nous nous attardons sur cette question : qu'est-ce qu'un réseau ? Nous étudierons et comprendrons ce que c'est qu'un réseau. Nous verrons de quoi est composé un réseau, le matériel nécessaire, et la forme qu'un réseau peut prendre. Nous nous arrêtons ensuite sur architecture du modèle OSI *(Open Systems Interconnection)*, qui est un standard de communication, en réseau, de tous les systèmes informatiques.

I.2 Définition d'un réseau informatique :

Un réseau informatique (Computer network) est un ensemble d'équipements électroniques (ordinateurs, imprimantes, scanners, modems, routeurs, commutateurs...) interconnectés et capables de communiquer (émettre et recevoir des messages) par l'intermédiaire d'un support de communication.

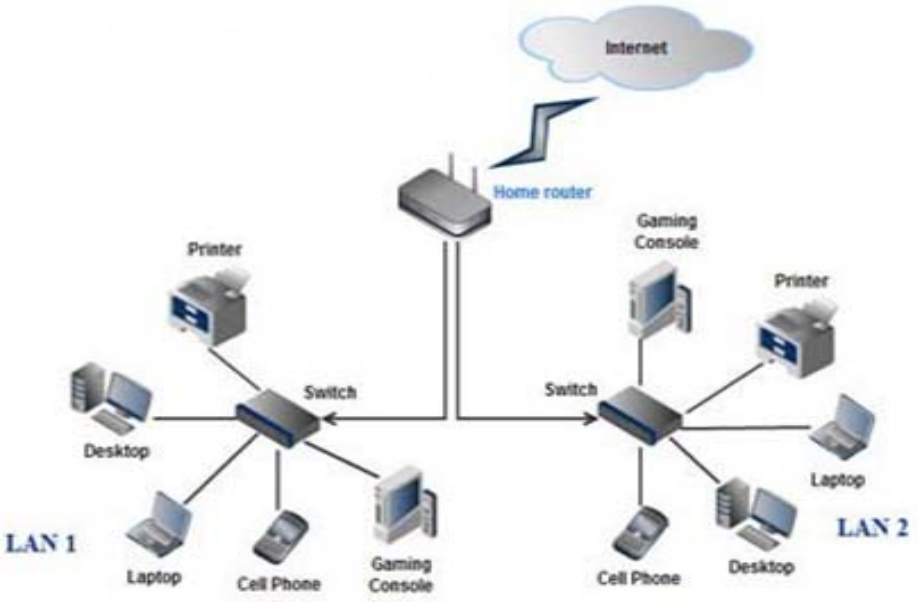


Figure 1 : Réseau informatique

Un réseau informatique peut servir de plusieurs buts distincts :

- **Communication**: les réseaux permettent de communiquer et d'échanger des messages très facilement en quelques secondes (e-mail, forum, …).

- **Partage d'information**: il peut s'agir par exemple de document textuel ou data (vidéo, audio) dans une base de données.

- **Partage de ressources**: les ordinateurs reliés en réseaux peuvent partager des périphériques appelés ressources. Le partage permet de réduire leurs dépenses. Ainsi, au lieu d'avoir à acheter une imprimante pour chaque employé, on peut se limiter à une seule imprimante centrale commune à l'ensemble des utilisateurs des réseaux.[15]

- **Partage de programme ou application**: avec un réseau, il est également possible de rendre certains programmes accessibles à l'ensemble des utilisateurs. En les installant sur un serveur central, les différentes personnes reliées au réseau peuvent utiliser leurs propres ordinateurs pour accéder à ce programme et s'en servir comme s'il était installé sur leur ordinateur.

I.3 Classification des réseaux de communication :

Les réseaux de communications peuvent être classés en fonction du type d'informations transportées et de la nature des entités impliquées. On distingue ainsi trois principales catégories de réseaux :

I.3.1 Les réseaux télécommunication : le mot télécommunication (abrégé télécom) signifie communication à distance. Les réseaux Télécom ont pour objectif l'acheminement de communications vocales entre individus. Exemples : Réseau Téléphonique Commuté Public, Numéris, Réseaux mobiles GSM/DCS.

I.3.2 Les réseaux de télédiffusion : plus récents, ils servent à la diffusion de canaux de télévisions entre les studios TV et les particuliers. On retrouve les réseaux de distribution terrestre des câblo-opérateurs et les réseaux satellites.[7]

I.3.3 Les réseaux informatiques : ils servent à l'échange des données numériques et le partage de ressources (imprimantes, disques, …). Ces communications (liaisons) étaient uniquement destinées au transport des données informatiques.

La tendance actuelle tend vers la réunion de tous ces types de réseaux : les réseaux multimédias.

I.3.4 Les réseaux multimédias : parviennent à faire passer ces différents médias (textes, sons, images fixes et animées) en même temps sur un même réseau.[8] Il peut arriver aussi que chaque média soit transporté par un réseau particulier et que l'ensemble soit resynchronisé à la sortie.

Les réseaux informatiques peuvent aussi être catégorisés par relation fonctionnelle entre les composants :

- **Client-Serveur** : désigne un mode de communication à travers un réseau entre plusieurs programmes : l'un, qualifié de client, envoie des requêtes ; l'autre ou les autres, qualifiés de serveurs, attendent les requêtes des clients et y répondent.

- **Pair-à-Pair** : le **pair à pair** (en anglais *peer-to-peer*, souvent abrégé « P2P ») est un modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur. Les termes « pairs», « nœuds », et « utilisateurs » sont généralement utilisés pour désigner les entités composant un réseau P2P.

I.4 Construire un réseau informatique:

I.4.1 Le matériel nécessaire : il faut savoir que pour construire un réseau, il faut du matériel. Nous verrons donc quels sont les appareils et comment ils sont reliés entre eux : câbles, Switch, routeur...

I.4.1.1 Les supports de transmission :

Le support de transmission est évidemment l'élément indispensable pour transmettre des signaux d'un émetteur vers un récepteur. Les principaux supports utilisés dans les réseaux sont les câbles métalliques dans lesquels circulent des signaux électriques (paires torsadées,

câble coaxial), la fibre optique qui propage des ondes lumineuses, et les supports immatériels sans fil (transmission sans fil) en utilisant l'atmosphère où circulent des ondes radio.

a. Paires torsadées : c'est le type de câble le plus utilisé pour connecter des ordinateurs entre eux dans un réseau local. À moins que le réseau soit entièrement sans-fil. Une paire torsadée non blindée se compose de deux conducteurs en cuivre, isolés l'un de l'autre et enroulés de façon hélicoïdale autour de l'axe de symétrie longitudinal. Généralement plusieurs paires sont regroupées sous une enveloppe protectrice appelée **gaine** pour former un câble [2].

L'enroulement réduit les conséquences des inductions électromagnétiques parasites sur les paires voisines. L'immunité aux parasites peut être améliorée en protégeant le faisceau par un écran. L'écran est constitué d'un ruban d'aluminium qui entoure les paires et les protège des perturbations électromagnétiques. Un conducteur de cuivre nu étamé (drain) permet la mise à la terre de l'écran.

La paire torsadée suffit pour les réseaux locaux d'entreprise où les distances se limitent à quelques kilomètres. Ses avantages sont nombreux : technique maitrisée, facilité de connexion et d'ajout de nouveaux équipements, faible coût.

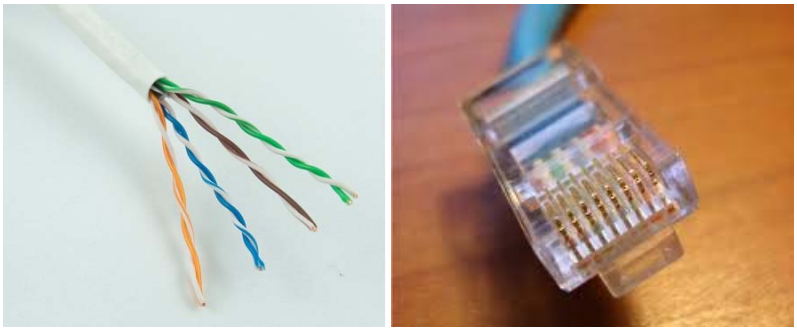


Figure 2 : Paires torsadées

b. Câble coaxial : une paire coaxiale ou câble coaxial (Figure 3) est constitué de deux conducteurs concentriques maintenus à distance constante par un diélectrique. Le conducteur extérieur, tresse métallique en cuivre appelée **blindage**, est mis à la terre. L'ensemble est protégé par une gaine isolante [1]. Le câble coaxial possède des caractéristiques électriques supérieures à celles de la paire torsadée. Il autorise des débits plus élevés et est peu sensible aux perturbations électromagnétiques extérieures.

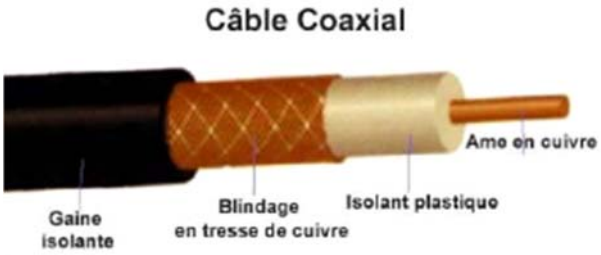


Figure 3 : Câble coaxiale

c. Fibre optique : une fibre optique (Figure 4) est constituée d'un fil de verre très fin. Elle comprend un cœur, dans lequel se propage la lumière émise par une diode électroluminescente ou une source laser et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre.

Les avantages de la fibre optique sont nombreux : diamètre extérieur (gaine) de l'ordre de 0.1 mm, autorise des vitesses de communication très élevées (plus de 100 Gigabits/s) en milieu très fortement parasité. Cette réduction de la taille la rend facile à utiliser. En outre, sa très grande capacité en débit permet la transmission simultanée de nombreux canaux de télévision, de téléphone ... . Les points de régénération des signaux sont plus éloignés (jusqu'à 200 km), du fait de l'atténuation moindre de la lumière.

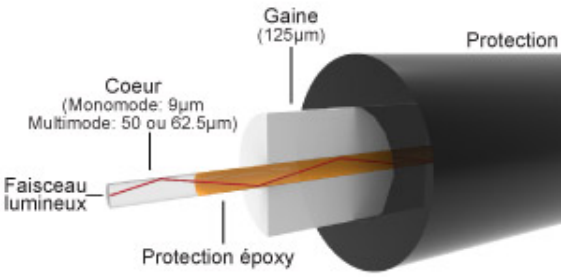


Figure 4 : Fibre optique

d. Transmission sans fil : les ondes radio (radiofréquences entre 3 kHz et 300 GHz) permettent de connecter des machines entre elles sans utiliser de câbles. La norme la plus utilisée actuellement pour les réseaux sans fil est la norme IEEE 802.11, mieux connue sous le

nom de Wi-Fi (Figure 5). Le Wi-Fi permet de relier des machines à une liaison haut débit (de 11 Mbit/s théoriques ou 6 Mbit/s réels en 802.11b) sur un rayon de plusieurs dizaines de mètres en intérieur (plusieurs centaines de mètres en extérieur).

Figure 5 : Carte sans fil

Le choix du support est en fonction des critères suivants :

- La distance maximum entre stations.

- Les débits minimum et maximum.

- Le type de transmission (numérique ou analogique).

- La nature des informations échangées (données, voix, vidéo...).

- La fiabilité, le coût.

I.4.1.2 Les équipements terminaux :

La fonction principale d'un équipement terminal est de permettre à l'utilisateur d'accéder aux ressources du réseau. La famille de terminaux comprend les téléphones, les imprimantes, les ordinateurs (souvent appelées stations), les scanneurs, tablette,... .

a) Serveurs :

Les serveurs sont des ordinateurs puissants qui fournissent des ressources partagées aux utilisateurs. Ils disposent d'une carte réseau, d'un ou plusieurs processeurs, d'une

mémoire vive importante, de plusieurs disques durs et des composants logiciels de communication. Un serveur assume un seul ou plusieurs des tâches suivantes :

- Serveur de fichiers : stockage des données des utilisateurs.

- Serveurs d'impression : un serveur d'impression est un serveur qui permet de partager une ou plusieurs imprimantes entre plusieurs utilisateurs (ordinateurs) situés sur un même réseau informatique.

- Serveurs d'authentification : gère les connexions des utilisateurs.

b) Clients :

Tout type d'ordinateur ou de terminal, quel que soit son système d'exploitation (Windows, Linux, Mac OS), muni d'une carte réseau et des composants logiciels de communication. Les clients accèdent aux ressources partagées fournies par un serveur de réseau.

c) La carte réseau (Network Interface Card) :

La carte réseau est le composant le plus important, elle est indispensable. C'est par elle que transitent toutes les données à envoyer et à recevoir du réseau dans un ordinateur [16]. Chaque carte réseau possède une adresse unique, appelée adresse MAC (adresse physique). Cette adresse a été définie lors de la fabrication de la carte. Elle sert à identifier chaque carte réseau lorsque des informations sont envoyées ou reçues au sein du réseau.

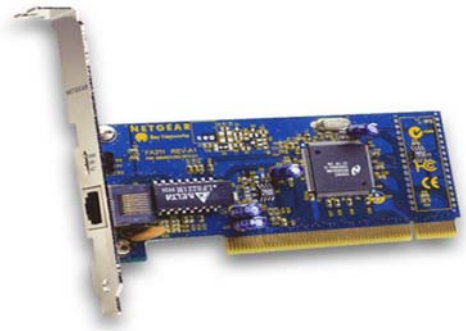


Figure 6 : Une carte réseau

I.4.1.3 Les équipements d'interconnexion :

L'interconnexion des réseaux c'est la possibilité de faire dialoguer plusieurs sous réseaux initialement isolés, par l'intermédiaire de périphériques spécifiques (répéteur, concentrateur, commutateur, routeur,...), ils servent aussi à interconnecter les ordinateurs d'une organisation, d'un campus, d'un établissement scolaire, d'une entreprise…..

a. Concentrateur (hub) :

C'est un matériel permettant de relier plusieurs ordinateurs entre eux. Il ne fait aucune distinction du destinataire de l'information. Ce qui signifié que l'information envoyée par un poste est dirigée vers tous les postes. Le signal est en général réamplifié.

Figure 7 : Un concentrateur (hub)

b. Commutateur (Switch) :

Un commutateur fonctionne à peu près comme un hub, sauf qu'il est plus discret. Il analyse les trames arrivant sur ses ports d'entrée afin de les aiguiller uniquement sur les ports adéquats, donc il n'envoie pas tout ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire, les autres ne savent rien des données ne leur étant pas destinées.

Figure 8 : Un commutateur (Switch)

c. Le routeur :

Dans un routeur, le paquet qui arrive doit posséder l'adresse complète du destinataire, de sorte que le nœud puisse décider de la meilleure ligne de sortie à choisir pour l'envoyer vers un nœud suivant. Une décision de routage a donc lieu selon un ensemble de règles.

d. Répéteur :

Son intérêt est de renvoyer ce qu'il reçoit par l'interface de réception sur l'interface d'émission, mais plus fort. On dit qu'il régénère et réémet le signal.

I.4.2 Les Types de réseaux :

On distingue : les réseaux PAN, les réseaux locaux LAN, les réseaux métropolitains MAN et les réseaux étendus WAN.

a. Réseau personnel PAN (Personal Area Network) :

Le réseau personnel permet aux équipements de communiquer à l'échelle individuelle. Un exemple courant est celui du **réseau sans fil**, qui relie un ordinateur à ses périphériques. Pratiquement tous les ordinateurs s'accompagnent d'un moniteur, d'un clavier, d'une souris et d'une imprimante. En l'absence de liaisons sans fil, les connexions doivent être câblées. [3]

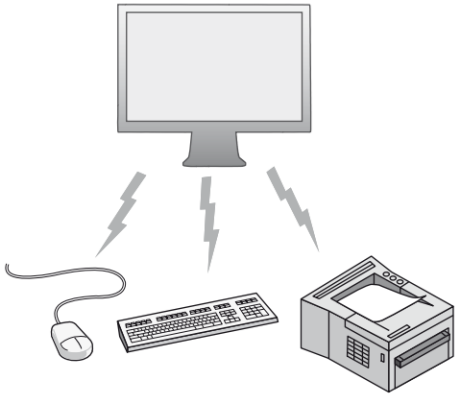


Figure 9 : Réseaux PAN

b. Réseau local (Local Area Network) :

Le réseau local est un réseau limité à un espace géographique comme un bâtiment, un immeuble de bureaux ou une usine (quelques centaines de mètres et n'excèdent pas quelques kilomètres). Par exemple, l'ensemble des ordinateurs dans une école forme un LAN. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde.

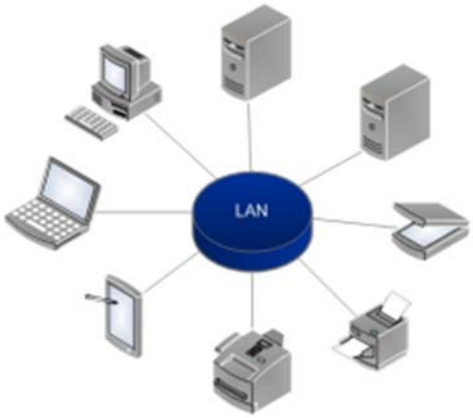


Figure 10: Réseaux locaux LAN

c. Réseau métropolitain MAN (Metropolitan Area Network) :

Le réseau métropolitain correspond à la réunion de plusieurs réseaux locaux (LAN) à l'intérieur d'un même périmètre d'une très grande Entreprise ou d'une ville, pouvant relier des points distants de 10 à 25 Km. [9]

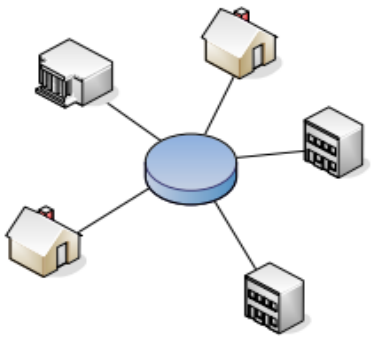


Figure 11 : Réseaux MAN

d. Réseau étendu WAN (Wide Area Network) :

Il s'agit là des réseaux d'opérateur, et qui assurent la transmission des données sur des longues distances à l'échelle d'un pays ou de la planète. Internet est un réseau de type WAN.

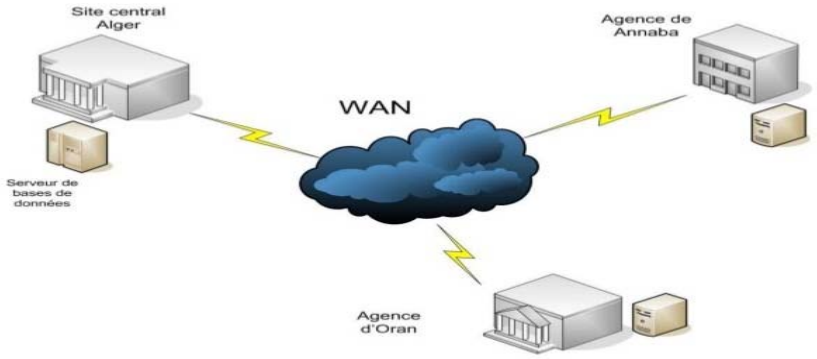


Figure 12 : Réseaux WAN

Après avoir parlé sur les différents types de réseaux, nous allons maintenant voir ce qu'une topologie et ses différents types.

I.4.3 Définition de la topologie :

On distingue la topologie physique qui définit la manière dont les équipements sont interconnectés entre eux, de la topologie logique qui précise la manière dont les équipements communiquent entre eux.

a. Topologie en bus : le bus s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, celles-ci circulent sur toute la longueur du bus et la station destinataire peut les récupérer [13]. Cette topologie a l'avantage de ne pas être perturbée par la panne d'une machine du bus et la simplicité de sa mise en œuvre. Par contre, en cas de rupture de bus le réseau devient inutilisable, étant donné que le câble de transmission est commun, une seule station peut émettre à la fois.

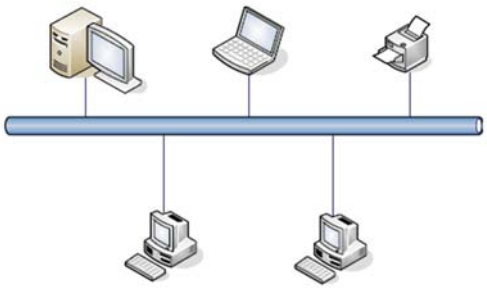


Figure 13 : Topologie en bus

b. **Topologie en anneau :** cette architecture est principalement utilisée par les réseaux Token Ring. Elle utilise la technique d'accès par «Jeton». Les informations circulent de station en station, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite…

   Cette topologie permet d'avoir un débit proche de 90% de la bande passante. De plus, le signal qui circule est régénéré par chaque station. Par contre, la panne d'une station rend l'ensemble du réseau inutilisable.

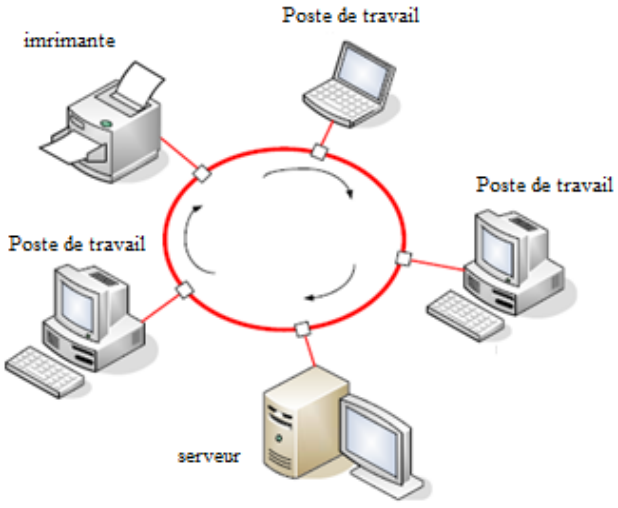


Figure 14 : Topologie en anneau

c. **Topologie en étoile :** c'est la topologie la plus courante, toutes les stations sont reliées à un unique composant central, n'importe quel appareil (routeur, commutateur, concentrateur,...) peut être au centre d'un réseau en étoile. Quand une station émet vers le composant central, celui-ci envoie les données à celle qui en est le destinataire (switch) ou à toutes les autres machines (hub). Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau [17]. Par contre, il faut plus de câbles que pour les autres topologies, et si le composant central tombe en panne, tout le réseau est hors d'état de fonctionner. De plus, le débit pratique est moins bon que pour les autres topologies.

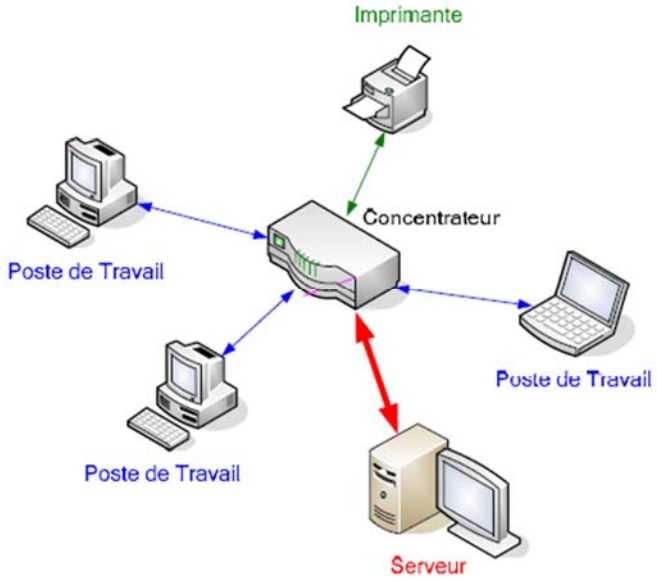


Figure 15 : Topologie en étoile

d. **Topologie hybride :** c'est juste le regroupement de plusieurs topologies différentes. Par exemple, Internet est une parfaite illustration d'un réseau hybride car il joint des réseaux en anneau avec des réseaux en bus, avec des réseaux en étoile, ...

I.4.4 Protocole :

Maintenant qu'on a fait un rapide tour du matériel, il faudrait atteindre l'objectif des réseaux qui est de pouvoir s'échanger des informations. Étant donné que nous discutons entre des machines très différentes, qui elles-mêmes ont des systèmes d'exploitation très différents

(Windows, Mac OS, Linux, etc.), nous devons créer un langage de communication commun pour se comprendre. C'est le protocole.

I.4.4.1 Définitions d'un protocole : est un ensemble de règles qui définissent comment se produit une communication dans un réseau informatique.

I.5 Les réseaux à commutation:

Le concept de réseau à commutation est né de la nécessité de mettre en relation un utilisateur avec n'importe quel autre utilisateur (relation de 1 à 1 parmi n) et de l'impossibilité de créer autant de liaisons point à point qu'il y a de paires potentielles de communicants [1].

Les réseaux à commutation permettent à tout équipement informatique connecté de communiquer directement avec tout autre équipement à travers un réseau de type maillé

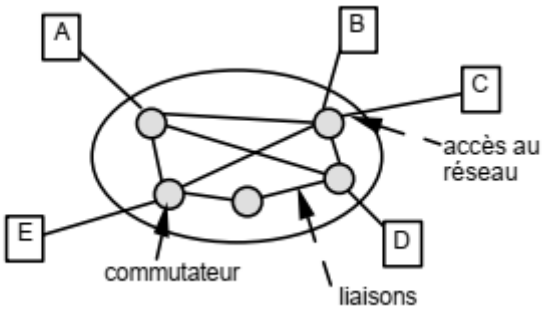


Figure 16 : Réseaux commuté

Ce type de réseaux est formé d'un ensemble d'ETTD (équipement terminal de traitement de données). Les liaisons sont gérées par des commutateurs ou nœuds de commutation chargés de trouver un chemin entre les stations communicantes et d'établir la liaison entre elles. Ces réseaux sont souvent opposés aux réseaux locaux dans lesquels les liaisons entre stations sont permanentes.

I.5.1 Technique de transfert :

On distingue trois principaux modes de commutation (nous verrons qu'en réalité que deux modes sont bien différenciés):

- Commutation de **circuits**
- Commutation de **messages**
- Commutation de **paquets** (qui est une amélioration de la commutation de messages)

a. La commutation de circuits: (en anglais *circuit switching*) est une méthode de transfert de données consistant à établir un circuit dédié au sein d'un réseau.
Dans ce type de scénarios, un circuit constitué de lignes de communication entre un nœud émetteur et un nœud récepteur est réservé le temps de la communication afin de permettre le transfert de données et est libéré à la fin de la transmission. Il s'agit notamment de la méthode utilisée dans le **réseau téléphonique commuté(RTC)**. En effet, en réservant une ligne téléphonique entre deux abonnés, il est possible de garantir la meilleure performance possible pour le transfert des données. Dans le cas d'une communication vocale par exemple, il est essentiel que la ligne ne soit pas coupée pendant tout le temps de la transmission.

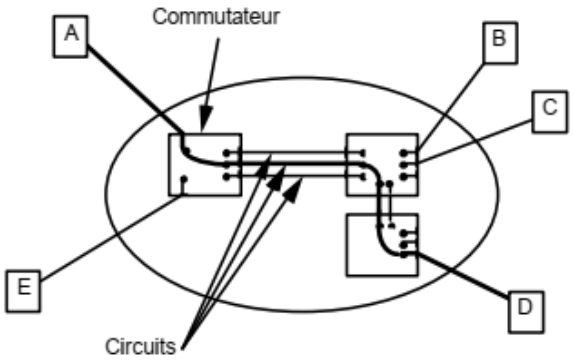


Figure 17 : Commutation de circuits

b. **Commutation de message :** technique d'acheminement de messages sans établissement au préalable d'une connexion de bout en bout entre l'émetteur et le récepteur. Un message peut être envoyé même en l'absence de son destinataire.

Le message est mémorisé par chaque nœud, avant d'être retransmis au nœud suivant. Dans le cas où le destinataire n'est pas connecté, le nœud final mémorise le message, celui-ci sera délivré lors de sa prochaine connexion. Par contre, les principaux inconvénients résident dans la nécessité d'une mémoire de masse importante dans les commutateurs. Le temps d'acheminement non connu, pas adapté aux applications temps réel. Si un message est corrompu, il devra être retransmis intégralement.

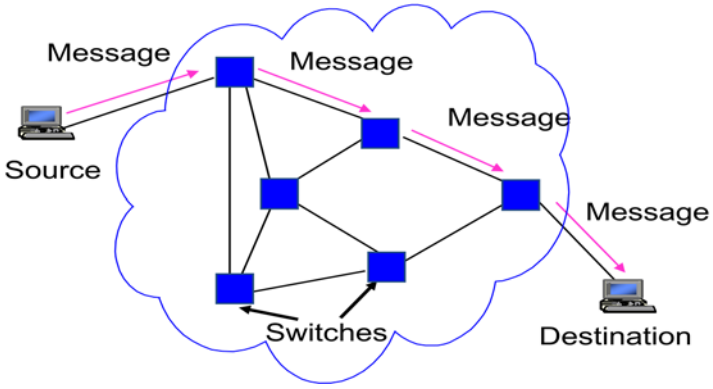


Figure 18 : Commutation de message

c. **Commutation de paquets :** lors d'une transmission de données par **commutation de paquets** (en anglais *packet switching*), les données à transmettre sont découpées en paquets de données (on parle de **segmentation**) émis indépendamment sur le réseau.

Les nœuds du réseau sont libres de déterminer la route de chaque paquet individuellement, selon leur table de routage. Les paquets ainsi émis peuvent emprunter des routes différentes et sont réassemblés à l'arrivée par le nœud destinataire.

Dans ce type de scénario les paquets peuvent arriver dans un ordre différent que l'ordre d'envoi et peuvent éventuellement se perdre. Des mécanismes sont ainsi intégrés dans les paquets pour permettre un réassemblage ordonné et une réémission en cas de perte de paquets.

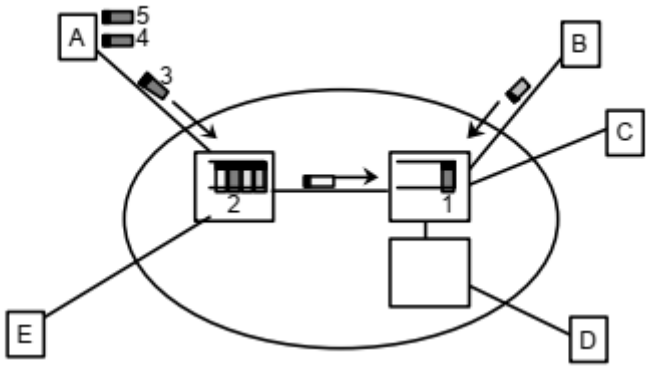


Figure 19 : Commutation de paquets

I.6 Le modèle OSI (Open System Interconnection) :

Pour établir une communication entre deux ordinateurs il faut tenir compte des différences entre le matériel et le logiciel de chaque machine.

Ces difficultés pour établir une communication se multiplient lorsqu'il s'agit d'interconnecter des réseaux mettant en jeu des matériels et des systèmes informatiques très différents.

Pour créer un réseau il faut utiliser un grand nombre de composants matériels et logiciels souvent conçus par des fabricants différents. Pour que le réseau fonctionne, il faut que tous ces appareils soient capables de communiquer entre eux.

Pour faciliter cette interconnexion, il est apparu indispensable d'adopter une norme, qui est en fait des accords documentés décrivant des spécifications des produits ou des services. Exemple : format d'une carte bancaire (longueur, largeur, épaisseur, position de la bande magnétique, etc.). Cette norme établie par l'**I**nternational **S**tandard **O**rganization (**ISO**) est appelé modèle **O**pen **S**ystem **I**nterconnection (**OSI**, interconnexion de systèmes ouverts).

I.6.2 Qu'est-ce que le modèle OSI ? :

Le modèle OSI est une façon standardisée de segmenter en plusieurs blocs le processus de communication entre deux entités. Chaque bloc résultant de cette segmentation est appelé couche. Une couche est un ensemble de services accomplissant un but précis. La beauté de cette segmentation, c'est que chaque couche du modèle OSI communique avec la

couche au-dessus et au-dessous d'elle (on parle également de couches adjacentes). La couche au-dessous doter des services de la couche en cours utilise, et la couche en cours pourvoit des services dont la couche au-dessus d'elle aura besoin pour assurer son rôle.

Voici un schéma pour illustrer ce principe de communication entre couches :

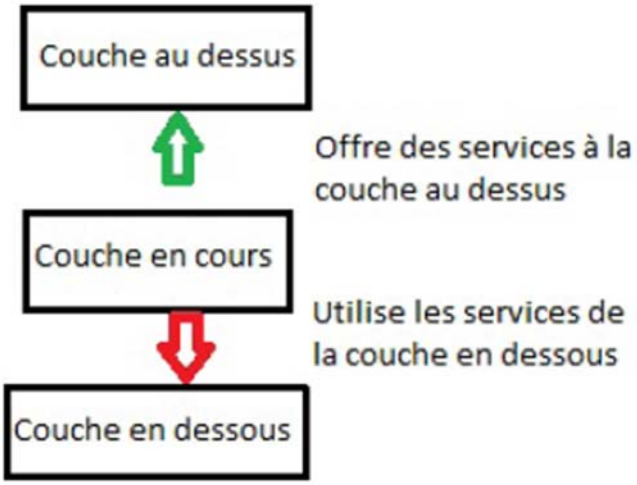


Figure 20: Principe de communication entre couches

Le modèle OSI a segmenté la communication en sept couches :

a) **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 permettent par exemple le transfert de fichier, rédiger un mail, d'établir une session à distance, de visualiser une page web…[18]. Plusieurs protocoles assurent ces services, dont FTP (pour le transfert des fichiers), Telnet (pour l'établissement des sessions à distance), SMTP (pour l'envoi d'un mail), etc.

b) **La couche présentation :** elle assure la mise en forme des données**,** la conversion d'un fichier codé en EBCDIC (*Extended Binary Coded Decimal Interchange Code*) vers un fichier codé en ASCII (*American Standard Code for Information Interchange*), si nécessaire, pour délivrer à la couche application un message dans une

syntaxe compréhensible. Elle peut aussi assurer le cryptage et la compression des données. C'est donc la première couche non impliquée dans le transfert d'information.

c) **La couche session :** la couche session du modèle OSI permet principalement d'ouvrir une session, de la gérer et de la clore. La demande d'ouverture d'une session peut échouer. Si la session est terminée, la « reconnexion » s'effectuera dans cette couche.

d) **La couche transport :** cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport 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. La couche de transport modifie également l'en-tête des données en y ajoutant plusieurs informations, parmi lesquelles les numéros de ports de la source et de la destination. Le protocole TCP (*Transmission Control Protocol*) est le plus utilisé dans la couche de transport.

e) **La couche réseau :** la couche réseau se charge du routage (ou relai) des données du point A au point B et de l'adressage. Ici aussi, l'en-tête subit une modification. Il comprend désormais l'en-tête ajouté par la couche de transport, l'adresse IP source et l'adresse IP du destinataire. Le protocole le plus utilisé à ce niveau est bien sûr le protocole IP.

f) **La couche liaison de données :** là où la couche réseau effectue une liaison logique, la couche de liaison effectue une liaison de données physique. En fait, elle transforme la couche physique en une liaison, en assurant dans certains cas la correction d'erreurs qui peuvent survenir dans la couche physique. Elle fragmente les données en plusieurs trames, qui sont envoyées une par une dans un réseau local.

g) **La couche physique :** la couche physique reçoit les trames de la couche de liaison de données et les « convertit » en une succession de bits qui sont ensuite mis sur le média pour l'envoi. Cette couche se charge donc de la transmission des signaux électriques ou optiques entre les hôtes en communication. On y trouve des services tels que la détection de collisions, le multiplexage, la modulation, etc.

I.6.2 Le parcours des données dans le modèle OSI :

Quand un hôte A envoie un message à un hôte B, le processus d'envoi va de la couche application à la couche physique. En revanche, quand il s'agit de recevoir, le message emprunte le chemin inverse : il part de la couche physique pour arriver à la couche application.

Au début, nous n'avons que les données initiales, que l'on pourrait également appeler données d'application. Une fois dans la couche applicative, un en-tête AH (*Application Header* : « en-tête d'application ») est ajouté à cette donnée initiale, c'est le principe **d'encapsulation**. La couche applicative transmet cela à la couche de présentation au-dessous. Par l'encapsulation, cette couche ajoute un en-tête PH au résultat de la couche applicative. La couche de présentation envoie ce « nouveau » message à la couche de session et cette dernière encapsule son entête avec le résultat obtenu de la couche présentation.

Et ainsi de suite jusqu'à la couche liaison, qui a la particularité d'ajouter également un *trailer*. Finalement, toutes ces données sont converties en une série de bits et mises sur le média pour la transmission.

À la réception, le récepteur devrait recevoir des données erronées puisque la donnée initiale n'avait pas tous ces en-têtes, mais le modèle OSI est assez intelligent. En effet, dans la procédure de réception, chaque entête est enlevé lorsque le message « grimpe » les couches de la couche physique à la couche application, tel qu'illustré par le schéma ci-dessous. Cette « suppression » d'entête, c'est la **décapsulation**.

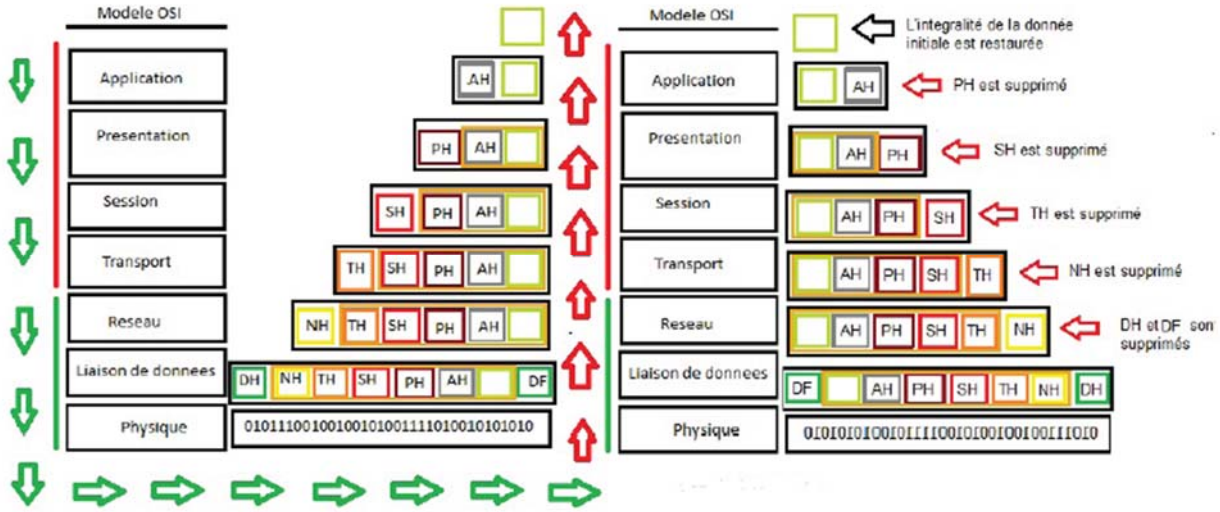


Figure 21 : Principe de l'encapsulation et décapsulation

AH (*Application Header*) : en-tête application.

PH (*Presentation Header*) : en-tête présentation.

SH (*Session Header*) : en-tête session

TH (*Transport Header*) : en-tête transport.

NH (*Network Header*) : en-tête réseau.

DH (*Data Header*) : en-tête liaison

PH (*Processing Header*) : en-tête physique

DH : Délimitateur de trame.

I.6.3 Critique du modèle OSI :

La chose la plus frappante à propos du modèle OSI est que c'est peut-être la structure réseau la plus étudiée et la plus unanimement reconnue et pourtant ce n'est pas le modèle qui a su s'imposer. Les spécialistes qui ont analysé cet échec en ont déterminé 3 raisons principales

I.6.3.1 La technologie :

Le modèle OSI est peut-être trop complet et trop complexe. Cette complexité peut faire douter de l'utilité de certaines couches. Par exemple, les couches présentation et session sont assez rarement utilisées.

Comme nous l'avons vu en survolant les couches de ce modèle, certaines fonctions se partagent entre plusieurs niveaux. Par conséquent, la complexité même du modèle OSI réduit l'efficacité de la communication.

Le comité rédacteur de la norme à même du laisser de côté certains points techniques, comme la sécurité et le codage, tant il était délicat de conserver un rôle bien déterminé à chaque couche ainsi complétée. Ce modèle est également redondant (le contrôle de flux et le contrôle d'erreur apparaissent pratiquement dans chaque couche).

I.6.3.2 L'implémentation :

À cause de la complexité de ce modèle, ses premières implémentations ont été très difficiles, lourdes et surtout lentes.

I.6.3.3 La durée et l'investissement :

En technologie, il faut sortir le bon produit au bon moment, OSI n'a pas respecté cette règle. Les recherches de l'ISO pour mettre au point un modèle normalisé ont pris du temps : OSI est sorti alors que le modèle TCP/IP (qu'on va le voir dans le prochain chapitre) était déjà utilisé. De ce fait, l'ISO a rencontré des difficultés pour trouver un investissement, le monde n'étant pas tellement intéressé par une deuxième suite de protocoles.

I.6.3.4 L'avenir d'OSI :

Au niveau de son utilisation et implémentation, et ce malgré une mise à jour du modèle en 1994, OSI a clairement perdu la guerre face à TCP/IP. Seuls quelques grands constructeurs dominants conservent le modèle, mais il est amené à disparaître d'autant plus vite qu'Internet explose.

Le modèle OSI restera cependant encore longtemps dans les mémoires pour plusieurs raisons. C'est d'abord l'un des premiers grands efforts en matière de normalisation du monde des réseaux, et l'un des structures réseau les plus étudiées car il permet de bien comprendre les principes. OSI marquera aussi les mémoires pour une autre raison : même c'est TCP/IP qui est concrètement utilisé, les gens ont tendance et utilisent OSI comme le modèle réseau de référence actuel. En fait, TCP/IP et OSI ont des structures très proches, et c'est surtout l'effort de normalisation d'OSI qui a imposé cette "confusion" générale entre les 2 modèles. On a communément tendance à considérer TCP/IP comme l'implémentation réelle d'OSI.

I.7 Discussion :

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 du modèle OSI, la suite du travail va définir le modèle TCP/ IP et le protocole internet IP en ces deux versions.

CHAPITRE II :

Protocole Internet Version 4 Et 6

II.1 Préambule :

Dans un réseau, les paquets doivent être transportés d'une extrémité à une autre. Le niveau paquet, couche 3 du modèle de référence, a la responsabilité de cet acheminement. Les paquets proviennent de la fragmentation des messages que les utilisateurs souhaitent s'échanger. Pour être transporté sur une ligne physique, le paquet est encapsulé dans un datagramme. Afin de permettre ce transport de bout en bout, le paquet doit satisfaire à trois grandes fonctions : l'adressage, le routage et le contrôle de flux. Ce chapitre donne un exemple de protocole de niveau paquet, l'IP (Internet Protocol).

II.2 Historique du modèle TCP/IP :

Dans les années 70, la DARPA (Defense Advanced Research Project Agency) possédait plusieurs réseaux d'ordinateurs de marques différentes, qui ne pouvaient dialoguer qu'avec d'autres ordinateurs de même marque.

Pour résoudre ces problèmes, le ministère de la Défense demanda à la DARPA de définir une famille de protocoles pour :

– Simplifier les communications : grâce à un jeu de protocoles, tous les appareils pourraient communiquer entre eux.

– Développer la compétition entre les différentes sociétés informatiques.

– Efficacité et productivité : Les fabricants consacrent du temps à l'implémentation des protocoles et non à leur développement.

En 1969, une première expérimentation permit de relier les 4 sites suivants :

Université de Californie de L.A., Santa Barbara, Utah, et le SRI Internationnal. Cette expérience fut le début du projet ARPANET (Advanced Research Project Agency

Network). L'expérience fut un succès, et d'autres sites se sont intégrés à ce réseau.

ARPANET continua de se développer et en 86, il englobait la plupart des grandes universités nord-américaines, le réseau militaire MILNET et d'autres centres de recherche internationaux. Peu à peu, le réseau ARPANET fut remplacé par l'Internet.

Celui-ci dépassa le domaine exclusif des universités et passa très vite dans le domaine commercial. Actuellement, la communauté Internet regroupe à la fois des organisations

commerciales et de simples utilisateurs. On y trouve les universités, les organismes de recherche, les fournisseurs d'accès, les institutions et les utilisateurs.

Initialement TCP/IP a été implémenté sous UNIX BSD 4. Ce système a constitué une version de base d'Unix, ce qui explique sa popularité.

Aujourd'hui, TCP/IP est le protocole standard de tous les réseaux, du LAN au WAN. De récentes adaptations autorisent les flux multimédias et, en particulier, la voix.

II.3 Définition du modèle TCP/IP:

TCP/IP est une suite de protocoles. Le sigle TCP/IP signifie «Transmission Control Protocol/Internet Protocol».

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Elle est conçue pour répondre à un certain nombre de critères parmi lesquels :

- Le fractionnement des messages en paquets
- L'utilisation d'un système d'adresses
- L'acheminement des données sur le réseau (routage)
- Le contrôle des erreurs de transmission de données.

II.3 .1 Organisation de l'architecture TCP/IP :

Le protocole TCP/IP étant antérieur au modèle OSI, il ne suit pas réellement celui-ci. Cependant, on peut faire grossièrement correspondre les différents services utilisés et proposés par TCP/IP avec le modèle OSI, et obtenir ainsi un modèle en 4 couches.

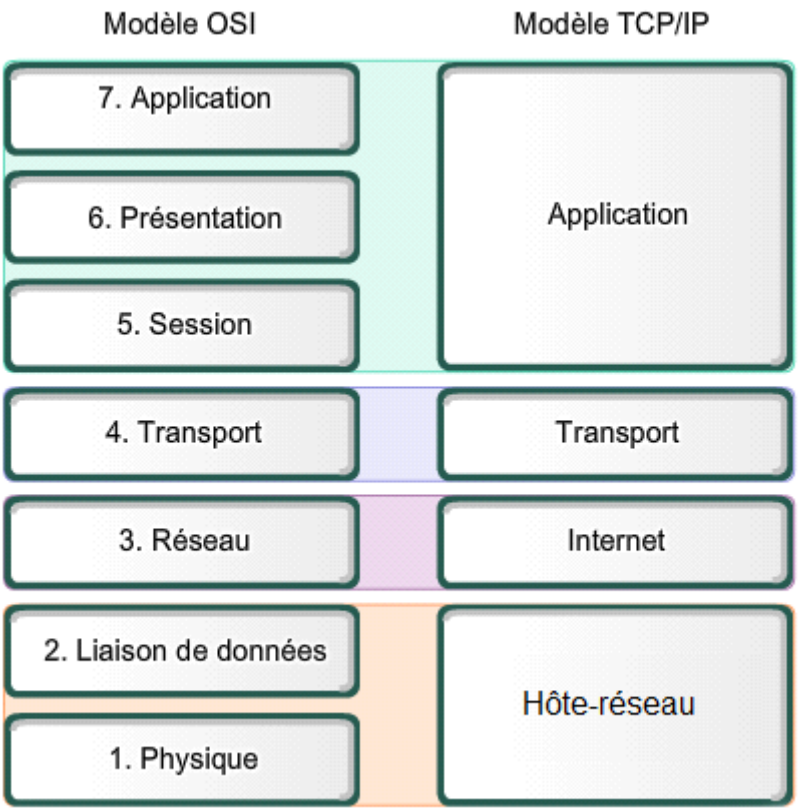


Figure 22 : modèle OSI et TCP/IP

Les services des couches 1 et 2 (physique et liaison) du modèle OSI sont intégrés dans une seule couche (hôte-réseau) ; les couches 5 et 6 (session et présentation) n'existent pas réellement dans le modèle TCP/IP et leurs services sont réalisés par la couche application si besoin est.

II.3.1.1 Hôte-réseau :

La couche **hôte-réseau**, intégrant les services des couches physique et liaison du modèle OSI, a en charge la communication avec l'interface physique afin de transmettre ou de récupérer les paquets de données qui lui sont transmis de la couche supérieure. [21] Le protocole utilisé pour assurer cet interfaçage n'est pas explicitement défini puisqu'il dépend du réseau utilisé ainsi que du nœud.

II.3.1.2 Internet :

La couche **internet**, correspondant à la couche réseau du modèle OSI, s'occupe de l'acheminement, à bonne destination, des paquets de données indépendamment les uns des autres, soit donc de leur routage à travers les différents nœuds par rapport au trafic et à la

congestion du réseau. Il n'est en revanche pas du ressort de cette couche de vérifier le bon acheminement.

Le protocole IP (Internet Protocol) assure intégralement les services de cette couche, et constitue donc l'un des points-clefs du modèle TCP/IP. Le format et la structure des paquets IP sont précisément définis.

II.3.1.3 Transport :

La couche **transport**, similaire de la couche homonyme du modèle OSI, gère le fractionnement et le réassemblage en paquets du flux de données à transmettre. Le routage ayant pour conséquence un arrivage des paquets dans un ordre incertain, cette couche s'occupe aussi du réagencement ordonné de tous les paquets d'un même message [21].

Les deux principaux protocoles pouvant assuré les services de cette couche sont les suivants :

TCP en mode connecté (établissement d'une session de communication), UDP en 1mode non connecté.

II.3.1.4 Application :

La couche **application**, similaire à la couche homonyme du modèle OSI, correspond aux différentes applications utilisant les services réseaux pour communiquer à travers un réseau.

Un grand nombre de protocoles divers de haut niveau permettent d'assurer les services de cette couche :

- Telnet : ouverture de session à distance.
- FTP (File Transfer Protocol) : protocole de transfert de fichiers.
- HTTP (HyperText Transfer Protocol) : protocole de transfert de l'hypertexte.
- SMTP (Simple Mail Transfer Protocol) : protocole simple de transfert de courrier.
- DNS (Domain Name System) : système de nom de domaine.
- etc.

II.3.2 Suite de protocoles :

Le modèle TCP/IP correspond donc à une **suite de protocoles** de différents niveaux participant à la réalisation d'une communication via un réseau informatique. Beaucoup de ces protocoles sont régulièrement utilisés par tous du fait de l'essor d'internet.

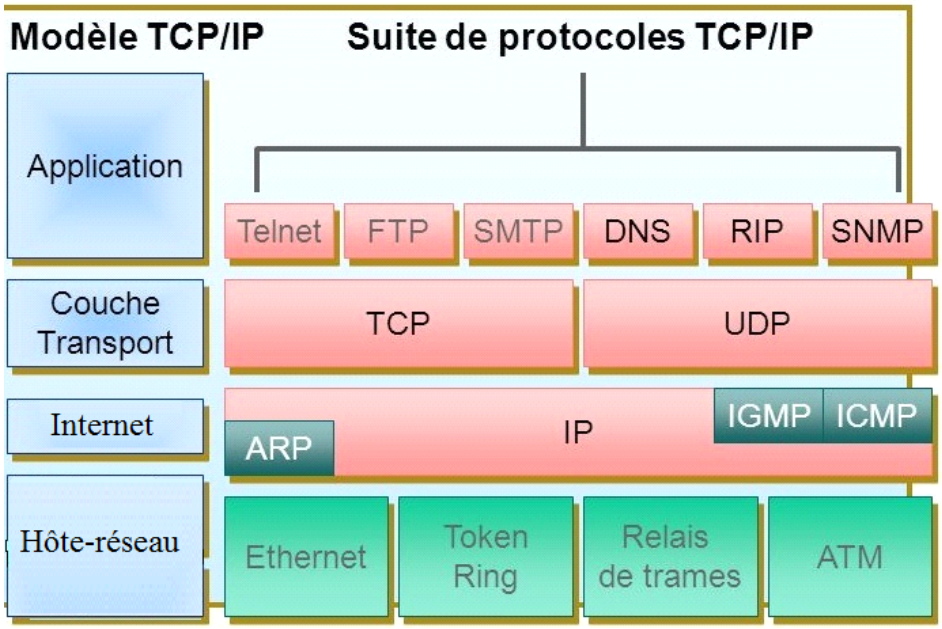


Figure 23 : Suite de protocoles du modèle TCP/IP

On parle aussi de **pile de protocoles** afin de rappeler qu'il s'agit bien d'une architecture en couches, et que les données issues d'un protocole d'une couche sont encapsulées dans un protocole de la couche inférieure. Ainsi, une requête HTTP est transportée dans un segment TCP, lui-même encapsulé dans un datagramme IP, etc.

La suite des protocoles TCP/IP sont :

–HTTP, *HyperText Transport Protocol*, assure le transfert des fichiers hypertextes entre un serveur Web et un client Web.

– **FTP**, *File Transfer Protocol*, est un système de manipulation de fichiers à distance (transfert, suppression, création...).

– **TELNET**, *Terminal network* ou *Telecommunication network*, système de terminal virtuel, permet l'ouverture de sessions avec des applications distantes.

– **SMTP**, *Simple Mail Transfer Protocol*, offre un service de courrier électronique.

– **DNS**, *Domain Name System*, est un système de bases de données réparties assurant la correspondance d'un nom symbolique et d'une adresse Internet (adresse IP).

– **ICMP**, *Internet Control and error Message Protocol*, assure un dialogue IP/IP et permet notamment : la signalisation de la congestion, la synchronisation des horloges et l'estimation des temps de transit... Il est utilisé par l'utilitaire **Ping** qui permet de tester la présence d'une station sur le réseau.

– **PPP**, *Point to Point Protocol*, protocole d'encapsulation des datagrammes IP, il assure la délimitation des trames, identifie le protocole transporté et la détection d'erreurs.

II.4 Le protocole internet version 4 (IPV4) :

Le protocole IPv4 (Internet Protocol version 4) est la première version d'Internet protocole (IP) à avoir été largement déployée, et qui forme encore en 2018 la base de la majorité des communications sur Internet. Le protocole IP assure le service attendu de la couche internet du modèle TCP/IP. Son rôle est donc de gérer l'acheminement des paquets (issus de la couche transport) entre les nœuds de manière totalement indépendante.

Le protocole IP offre un fonctionnement non fiable et sans connexion, à base d'envoi/réception de datagrammes (flux de bits structurés) :

- non fiable : absence de garantie que les datagrammes arrivent à destination, les datagrammes peuvent être perdus, retardés, altérés ou dupliqués sans que ni la source ou la destination ne le sachent, on parle de « remise au mieux » (*best effort delivery*).
- sans connexion (mode non-connecté) : chaque datagramme est traité et donc acheminé de manière totalement indépendante des autres. [21]

II.4.1 Structure du datagramme IPv4 :

Le datagramme IP comprend un en-tête et des données. L'en-tête contient principalement les adresses IP de la source et du destinataire, et des informations sur la nature des données transportées.

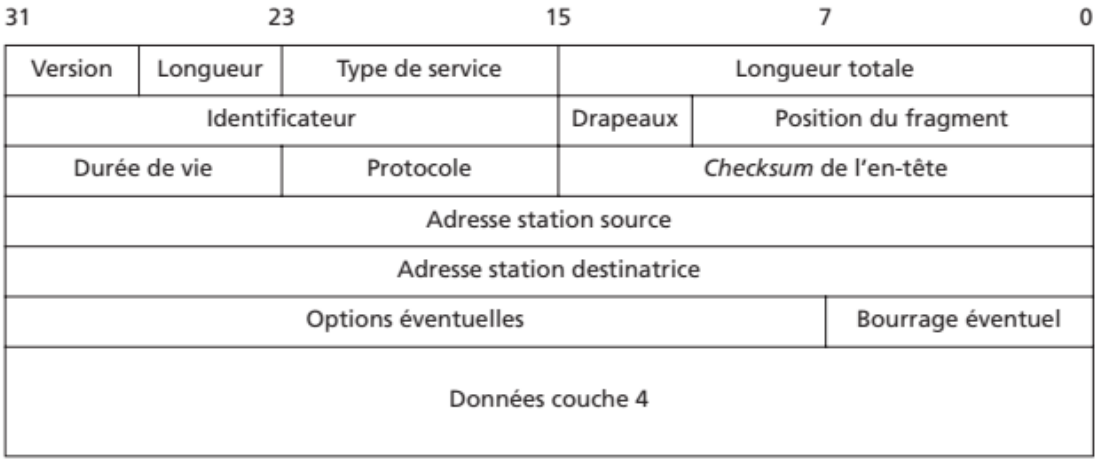


Figure 24 : Datagramme IPv4

Le paquet IPv4, ou datagramme IPv4, est organisé en champs de 32 bits (Figure 24) :

- **Version** : il s'agit de la version du protocole IP qu'on utilise (ici, c'est la version 4 ou IPv4). La version est codée sur 4 bits.

- **Longueur :** longueur de l'en-tête codée sur 4 bits : il s'agit du nombre de mots de 32 bits constituant l'en-tête (en hexadécimal) au maximum F mots de 32 bits, soit 60 octets.

- **Type de service (TOS) : ce** champ de 8 bits indique la façon dont le datagramme doit être traité. Par exemple, il était possible de demander que le datagramme soit traité sur la route la plus rapide, sur celle qui offrait le meilleur débit, la plus fiable, etc.

- **Longueur totale** (16bits) : longueur totale du datagramme (en-tête et données) exprimée en octets. La longueur maximale d'un datagramme est donc 65 Ko, mais des raisons physiques imposent des tailles inférieures dans la plupart des réseaux.

- **Identificateur :** un numéro de 16 bits attribué à chaque datagramme. Chaque fragment d'un même datagramme reprend le même identifiant, pour permettre le réassemblage correct du datagramme initial chez le destinataire.

- **Drapeaux:** le champ drapeaux (*flags*) occupe 3 bits et sert à gérer uniquement à la fragmentation. Chaque bit est interprété indépendamment, comme suit :

-(Premier bit) actuellement non utilisé.

-(Deuxième bit), appelé DF (*Don't Fragment*), autorise ou non la fragmentation du datagramme (si DF = 0 la fragmentation est autorisée et interdite si DF = 1).

- (Troisième bit), appelé MF (*More Fragments*), signifie « encore des fragments » positionné à 1 il indique que d'autres fragments suivent, positionné à 0, soit le fragment est le dernier, soit le paquet n'a pas été fragmenté.

- **Position du fragment :** ce champ (13 bits) indique, en cas de fragmentation, la position du fragment dans le datagramme d'origine. Ce champ indique la position du premier bit du fragment dans le datagramme d'origine, en multiple de 8 octets. En conséquence, tous les fragments, sauf le dernier, ont une longueur multiple de 8 octets.

- **Durée de vie :** ce champ durée de vie (*Time To Live*) représente la durée de validité du datagramme. Cette valeur est décrémentée toutes les secondes ou à chaque passage à travers une passerelle. Lorsque le TTL est égal à 0, le datagramme est détruit. La passerelle qui détruit un datagramme envoie un message d'erreur ICMP à l'émetteur.

- **Protocole :** le champ protocole occupe un octet indiquant à quel protocole sont destinées les données véhiculées dans le datagramme. Les valeurs les plus courantes sont : 1 pour ICMP, 6 pour TCP, 17 pour UDP, etc.

- **Checksum de l'en-tête** : ces 16 bits suivants contrôle l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission. Si la somme de contrôle est invalide, le paquet est abandonné sans message d'erreur.

- **Adresses station destinatrice et source :** les adresses destination et source désignent respectivement l'adresse IP de l'hôte émetteur et celle de l'hôte censé recevoir le datagramme.

- **Les champs options** (0 à 32 bits) : les informations optionnelles (sécurité, gestion, route, datation, etc.) de champ en-tête sont moins utilisées.

- **Le champ bourrage** (0 à 7 bits) : il permet de combler le champ option afin d'obtenir un en-tête IP multiple de 32 bits. La valeur des bits de bourrage est 0.

II.4.2 Contrôle de la fragmentation sous IP:

Maintenant que nous connaissons les détails du format d'un datagramme, examinons comment le fragmenter. La couche de liaison impose une taille limite, le MTU (Maximum Transfer Unit). Par exemple, cette valeur est de 1500 pour une trame Ethernet. Dans ces conditions, si la couche IP doit transmettre un bloc de données de taille supérieure au MTU, il y a fragmentation.

La fonction de fragmentation dans IP peut être utilisée pour découper les datagrammes trop grands en morceaux, de façon à ce que chacun de ces derniers tienne dans une trame liaison. Chaque nouveau fragment possède un en-tête, qui reprend la plupart des informations de l'en-tête d'origine.

Figure 25 : Fragmentation datagramme

La fragmentation d'un datagramme se fait au niveau des routeurs, c'est-à-dire lors de la transition d'un réseau dont le MTU est important à un réseau dont le MTU est plus faible.

II.4.3 Le routage IP :

Le routage IP fait partie intégrante de la couche internet de la suite TCP/IP. Le routage consiste à assurer l'acheminement d'un datagramme IP à travers un réseau en empruntant le meilleur chemin à l'aide d'algorithme de routage [4]. Ce rôle est assuré par routeurs.

II.4.4L'adresse IPv4 :

Une **adresse IPv4** (avec IP pour Internet Protocol) est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque branchement à un réseau informatique utilisant l'Internet Protocol [22]. Cette adresse est assignée soit individuellement par l'administrateur du réseau local dans le sous-réseau correspondant, soit automatiquement via le protocole DHCP. L'adresse IP est à la base du système d'acheminement (le routage) des paquets de données sur Internet.

Les adresses IPv4 sont codées sur 32 bits représentées sous la forme de quatre nombres entiers séparés par des points comme 193.43.55.67, comportent deux parties : le numéro de réseau (*Net_id*) et le numéro de la machine sur le réseau (*Host_id*).

II.4.4.1 La conception de l'adresse IP et son évolution :

Au début de sa conception, le protocole TCP/IP supposait que la plupart des communications IP seraient monodestinataire (*unicast*). Cependant, ses concepteurs avaient prévu que certains hôtes auraient besoin d'envoyer des messages à plusieurs destinataires d'un coup (*multicast*). Il fut donc décidé de diviser l'espace d'adressage en trois catégories inégalement réparties, une catégorie d'adresses monodestinataire, une catégorie d'adresses multidestinataire (*multicast*) et enfin une catégorie d'adresses réservées [5]. La part la plus

importante de cette partition était dévolue à la catégorie monodestinataire, elle-même subdivisée en trois classes disjointes (une adresse IP ne pouvait appartenir qu'à une seule classe à la fois).

L'appartenance à une classe ou à une autre déterminait la partie de l'adresse IP à interpréter comme étant l'adresse réseau. Chacun des groupes, à savoir d'une part les trois classes d'adresses unicast, et d'autre part les adresses multicast et réservées, ont été respectivement appelées classes d'adresses A, B, C, D et E, comme illustré sur la figure (26).

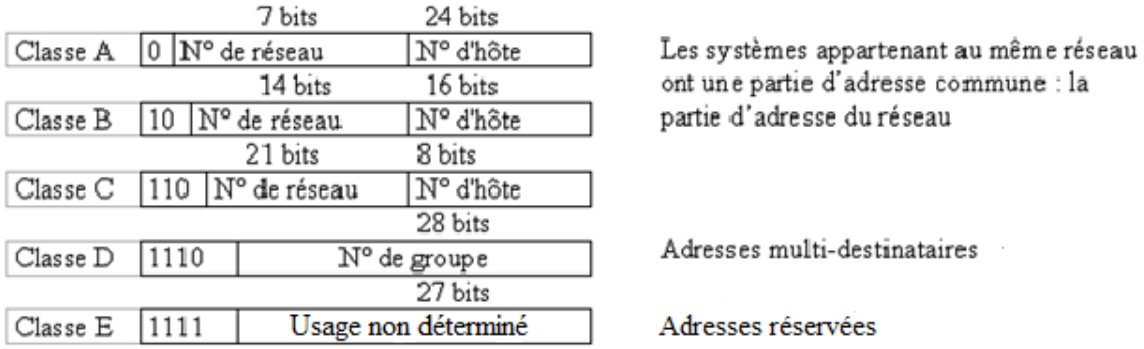


Figure 26 : Classe d'adressage IPv4

- ***Classe A*** **:** 128 réseaux et 16 777 214 hôtes (7 bits pour les réseaux et 24 pour les hôtes), la classe A défini une fourchette de réseaux d'adresses IP allant de 1.0.0.0 à 126.255.255.255

- ***Classe B*** **:** 16 384 réseaux et 65 534 hôtes (14 bits pour les réseaux et 16 pour les hôtes), la classe B définit une fourchette de réseaux d'adresses IP allant de 128.0.0.0 à 191.255.255.255.

- ***Classe C*** **:** 2 097 152 réseaux et 254 hôtes (21 bits pour les réseaux et 8 pour les hôtes). la classe C définit une fourchette de réseaux d'adresse IP allant de 192.0.0.0 à 223.255.255.255.

- ***Classe D*** **:** ne désignent pas une machine particulière sur le réseau, mais un ensemble de machines voulant partager la même adresse et ainsi participer à un même groupe : adresses de groupe de diffusion (*multicast*).

- ***Classe E*** **:** le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées par IANA à un usage non déterminé. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

Les autres adresses sont particulières ou réservées :

– 0.0.0.0 : est une adresse non encore connue, utilisée par les machines ne connaissant pas leur adresse IP au démarrage.

– L'adresse dont la partie hôte est constituée de bits à 0 est une adresse réseau ou sous-réseau, 210.24.25.0 pour une classe C par exemple.

– L'adresse dont la partie hôte est constituée de bits à 1 est une adresse de diffusion (broadcast), 130.24.255.255 pour une classe B.

– 127.0.0.1 : une adresse de bouclage (loopback en anglais) est une adresse utilisée par une interface pour s'envoyer un message à elle-même. Cette adresse sert à tester le fonctionnement de carte réseau. Un **Ping 127.0.0.1** doit retourner un message correct.

Pour chaque classe, certaines plages d'adresses sont réservées à un usage privé :

- classe A : 10.0.0.0.à 10.255.255.255
- classe B : 172.16.0.0 à 172.31.255.255
- classe C : 192.168.0.0 à 192.168.255.255

Il est important de savoir que les adresses appartenant à ces blocs ne sont pas autorisées sur Internet et doivent être filtrées (rejetées) par les routeurs Internet.

La plupart des entreprises utilisent des adresses IPv4 privées pour leurs hôtes internes. Toutefois, ces adresses ne sont pas routables via Internet et doivent être traduites en adresses IPv4 publiques. La traduction d'adresses réseau (NAT) est utilisée pour convertir les adresses IPv4 privées en adresses IPv4 publiques. Généralement, cette opération s'effectue sur le routeur qui connecte le réseau interne à celui du FAI

II.4.4.2 Pénurie d'adresses :

Il apparut très tôt au cours de l'évolution de l'Internet que le schéma initial d'adressage IP ne conviendrait plus, du fait que peu de réseaux prenaient en charge un nombre d'hôtes

dépassant le millier. En d'autres termes, l'espace d'adressage des classes A et B était en bonne partie gaspillé. Et la classe C, de son côté, ne disposait pas d'un nombre suffisant d'hôtes. Ce manque de souplesse entre les classes explique les différentes solutions mises en œuvre dès les années 1990 : l'utilisation d'adresses privées, notions de sous-réseau et masque, adresses sans classe et la distribution dynamique des adresses.

II.4.4.3 Notions de sous-réseaux et masque :

En 1984, devant la limitation du modèle de classes, la RFC 917 (*Internet subnets*) crée le concept de *sous-réseau*. Ceci permet par exemple d'utiliser une adresse de Classe B comme 256 sous-réseaux de 256 ordinateurs au lieu d'un seul réseau de 65534 ordinateurs, sans toutefois remettre en question la notion de classe d'adresse.

Deux raisons militent en faveur du découpage en sous-réseaux.

- La première est l'allocation plus efficace de l'espace d'adressage IP. Si Internet était limité aux adresses des classes A, B et C, chaque réseau se verrait attribuer 254, 65 534 ou 16 millions d'adresses IP pour ses équipements hôtes. Malheureusement, tout réseau qui franchirait (de si peu soit-il) la barre des 254 périphériques devrait recevoir une allocation de classe B, ce qui entraînerait un gaspillage de dizaines de milliers d'adresses IP.
- La seconde raison qui justifie le découpage en sous-réseaux est que, même si une organisation possède des milliers de périphériques de réseau, les faire fonctionner avec un même ID de réseau ralentirait terriblement le fonctionnement du réseau. Le protocole TCP/IP impose que tous les ordinateurs ayant un même identifiant de réseau soient présents sur le même réseau physique. Pour améliorer les performances, les réseaux sont généralement divisés en domaines de diffusion bien plus petits que l'espace d'adressage d'une classe C.

II.4.4.3.1 Les Sous-réseaux :

Un sous-réseau est un réseau qui fait partie d'un autre réseau (de classe A, B ou C).

Les sous-réseaux sont créés en utilisant un ou plusieurs bits de la partie hôte de classe A, B ou C pour étendre l'identifiant de réseau. Par conséquent, plutôt que d'avoir un identifiant de réseau standard de 8, 16 ou 24 bits, un sous-réseau peut avoir un identifiant de n'importe

quelle longueur. Plus précisément, lorsqu'une segmentation en sous-réseaux est nécessaire, la partie hôtes (Host_id Initial) de l'adresse IP peut être découpée en deux parties (Figures 27) :

- Partie sous-réseau (Subnet_id).
- Partie hôte dans le sous-réseau (Host_id).

Figure 27 : Découpage en sous-réseau

II.4.4.3.2 Masques de sous-réseaux :

Un masque de sous-réseau a le même format qu'une adresse IPv4. Les bits à « 1 » désignent la partie réseaux et sous-réseau (Net_id et Subnet_id) de l'adresse, et les bits à « 0 »désignent la partie machine (Host_id) sur le sous-réseau [6].

L'administrateur local choisit le nombre de bits à consacrer pour le découpage de l'identifiant machine en deux champs (Sous-réseau et Machine) grâce au *masque de sous-réseau* (ou *subnet mask*). Celui-ci, également codé sur 32 bits.

Dans un réseau subdivisé, chaque machine connaît son adresse IP et le masque utilisé, ce qui lui permet de savoir dans quel sous-réseau elle se trouve. Pour cela il suffit de faire un ET logique (AND) entre son adresse IP et le masque :

Adresse IPv4	91.198.174.2	01011011.11000110.10101110.00000010
	AND	
Masque de sous-réseau	255.255.224.0	11111111.11111111.11100000.00000000
Adresse de sous-réseau	91.198.160.0	01011011.11000110.10100000.00000000

En l'absence de segmentation en sous-réseau, les masques sont ceux par défaut des classes standards :

– classe A : 255.0.0.0

– classe B : 255.255.0.0

– classe C : 255.255.255.0

II.4.4.4 Les adresses sans classe CIDR (Class less Inter Domain Routing) :

Le CIDR a été proposé à partir de 1994. L'idée est d'organiser une adresse réseau indépendamment de sa classe. Le masque de sous-réseau indiquant le nombre de bits réservés à l'identifiant réseau est alors fixé librement par l'administrateur. Par exemple, pour réaliser l'équivalent de deux adresses de classe C contiguës, l'administrateur choisira un masque /23.

Le masque sous-réseau étant de taille variable, les fournisseurs d'accès Internet peuvent allouer à leurs clients un espace d'adressage adapté à leur besoin. Le protocole CIDR permet d'agréger des classes C ou d'affecter une partie seulement d'une classe B en utilisant des préfixes pour indiquer aux routeurs qu'un seul sous-réseau correspond à trois classes C.

Exemple : un fournisseur d'accès disposant d'un bloc d'adresses 206.0.64.0/18, soit 16 382 adresses machines. Si un client demande 800 adresses, avec CIDR, le fournisseur peut assigner à son client le bloc 206.0.68.0/22, soit 1022adresses, les 22 premiers bits de gauche représentent le masque sous-réseau (nombre de bits à 1).

II.4.4.5La distribution dynamique des adresses :

Une autre solution pour gérer la pénurie des adresses consiste à utiliser une plage d'adresses, en allouant temporairement les adresses IP disponibles aux seules machines connectées et en partant de l'hypothèse que toutes ne le seront pas simultanément. Pour assurer la distribution dynamique des adresses, le protocole DHCP (*Dynamic Host Configuration Protocol*) fournit automatiquement à un ordinateur qui vient d'être installé dans le réseau de l'entreprise ses paramètres de configuration réseau (adresse IP et masque de sous-réseau).

III.4.5 Les limites d'IPv4 :

Au fil des années, l'IPv4 a été mis à jour afin de relever de nouveaux défis. Cependant, même avec des modifications, l'IPv4 a toujours trois problèmes majeurs :

- **Manque d'adresses IP** – l'IPv4 a un nombre limité d'adresses IP publiques disponibles. Bien qu'il existe environ 4 milliards d'adresses IPv4, le nombre croissant

de périphériques IP, la croissance potentielle des pays en voie de développement entraînent une hausse du nombre d'adresses devant être disponibles. [23]

- **Croissance de la table de routage Internet** – une table de routage est utilisée par les routeurs pour déterminer les meilleurs chemins disponibles. À mesure que le nombre de nœuds connectés à Internet augmente, il en va de même pour le nombre de routes réseau. Ces routes IPv4 consomment beaucoup de mémoire et de ressources processeur sur les routeurs Internet. [23]

- **Manque de connectivité de bout en bout** – la technologie de traduction d'adresses réseau (NAT) est généralement implémentée dans les réseaux IPv4. Cette technologie permet à plusieurs périphériques de partager une adresse IP publique unique. Cependant, étant donné que l'adresse IP publique est partagée, l'adresse IP d'un hôte interne du réseau est masquée. Cela peut être problématique pour les technologies nécessitant une connectivité de bout en bout.

II.5 Internet Protocole version 6 (IPv6):

II.5.1 Adressage IPv6 :

Une adresse IPv6est codée sur 128 bits et s'écrit sous la forme de 8 nombres hexadécimaux représentant chacun 16 bits séparés par « :», comme par exemple : FEDC:BA98:7654:3210: EDBC:A987:6543:210F

Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.

II.5.2 Ecriture simplifiée des adresses IPv6 :

Il est permis d'omettre de un à trois chiffres zéros non significatifs dans chaque groupe de quatre chiffres hexadécimaux. Cette règle s'applique uniquement aux zéros de début de segment et non aux zéros de fin. L'omission de ces derniers rendrait l'adresse ambiguë. Par exemple, l'hextet « ABC » peut être « 0ABC » ou « ABC0 », mais ce sont deux valeurs différentes.

Une suite de deux deux-points (::) peut remplacer toute chaîne unique et continue d'un ou plusieurs segments de 16 bits (hextets) comprenant uniquement des zéros. Cette suite (::) ne peut être utilisée qu'une seule fois dans une adresse, sinon celle-ci devient ambiguë. C'est ce qu'on appelle le **format compressé**.

Recommandé	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Sans zéros en début de segment	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compressé	FE80::123:4567:89AB:CDEF

Figure 28 : Ecritures des adresses IPv6

La représentation des préfixes IPv6 est similaire à la notation CIDR utilisée pour les préfixes IPv4. Un préfixe IPv6 est donc représenté par la notation :

adresse-ipv6/longueur du préfixe

Les formes abrégées avec «::» sont autorisées.

3EDC:BA98:7654:3210:0000:0000:0000:0000/64

3EDC:BA98:7654:3210:0:0:0:0/64

3EDC:BA98:7654:3210::/64

Ainsi, l'adresseIPv6 ci-dessus est équivalente à la suivante :

3EDC:BA98:7654:3210::/64

II.5.3 Objectifs et amélioration a porté :

– Adressage étendu (128 bits au lieu de 32 bits).

– En-tête simplifié autorisant un routage plus efficace.

– Sécurité accrue en incluant des mécanismes d'authentification, de cryptographie et en garantissant l'intégrité des données.

– Implémentation d'un mécanisme de découverte du MTU optimal. La fragmentation n'est plus réalisée dans le réseau mais par le nœud source.

– Réduire la taille des tables de routage.

– Donner la possibilité a un ordinateur de se déplacer sans changer son adresse.
– Permettre au protocole une évolution future.

– Accorder a l'ancien et au nouveau protocole une coexistence pacifique.

II.5.4 Le datagramme IPv6 :

Pour améliorer le traitement des datagrammes dans les routeurs, la structure même du datagramme a été modifiée en supprimant notamment le champ option et les champs obsolètes. Par conséquent, l'en-tête du datagramme est de longueur constante (40 octets). Les champs relatifs à la fragmentation (Identificateur, Drapeaux, Position du fragment) disparaissent de l'en-tête. IPv6 implémente un mécanisme de découverte de la MTU. La fragmentation est réalisée par la source et le réassemblage par le destinataire ce qui allège considérablement le travail des routeurs intermédiaires

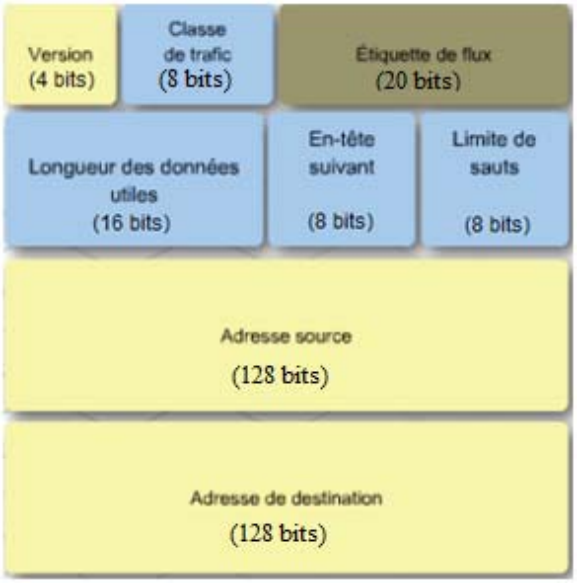


Figure 29 : Datagramme IPv6

Les différentes informations du champ en-tête sont les suivantes :

- **Version (4 bits) :** il s'agit de la version du protocole IP que l'on utilise (ici la valeur de version est 6) afin de vérifier la validité du datagramme.

- **Classe du Trafic, en anglais Traffic Class (8 bits) :** permet de garantir la qualité de service.

- **Etiquette de Flux, en anglais Flow Label (20 bits) :** champ relatif au flux d'information. Ce champ contient un numéro unique choisi par la source, pour marquer les paquets pour lesquels un traitement spécial doit être fait par les routeurs et la mise en œuvre des fonctions de qualité de service.

- **Longueur des données utiles, en anglais Payload Length (16 bits) :** indique la longueur totale du datagramme en octet (sans tenir compte de l'en-tête). Ce champ étant de 2 octets, la longueur maximale du datagramme est de 64 Ko.

- **En-tête suivant, en anglais Next Header (8 bits) :** identifie le type de l'entête qui suit l'entête IPv6

- **Nombre de Sauts Maximum, en anglais Hop Limit (8bits) :** décrémenté de 1 pour chaque nœud que le paquet traverse. Le paquet est éliminé si le Nombre de Sauts Maximum arrive à zéro.

- **Adresse Source, en anglais Source Address (128 bits) :** adresse IPv6 du nœud source sur 16 octets

- **Adresse Destination, en anglais Destination Address (128 bits) :** adresse IPv6 du nœud destination sur 16 octets

II.5.4 Types d'adresses IPv6 :

II.5.4.1 Les adresses unicast : une adresse de ce type désigne une interface unique. Un paquet envoyé à une telle adresse, sera donc remis à l'interface ainsi identifiée.

II.5.4.2 Les adresses multicast : une adresse de type multicast désigne un groupe d'interfaces qui en général appartiennent à des nœuds différents pouvant être situés n'importe où dans l'Internet. Lorsqu'un paquet a pour destination une adresse de type multicast, il est acheminé par le réseau à toutes les interfaces membres de ce groupe. Il faut noter qu'il n'y a plus

d'adresses de type **broadcast** comme sous IPv4 ; elles sont remplacées par des adresses de type multicast qui saturent moins un réseau local constitué de commutateurs.

II.5.4.3 Les adresses anycast: ces adresses introduites par IPv6 correspondent à une restriction des adresses de multicast. La différence étant que lorsqu'un paquet a pour destination une telle adresse, il est acheminé à un des éléments du groupe et non pas à tous.

II.5.5 Plan d'adressage d'IPv6:

II.5.5.1 Adresses Globales Unicast : adresses équivalentes aux adresses publiques IPv4, routables aussi bien dans un réseau privé que publique. La plage d'adresses 2000::/3 est réservée par l'IANA pour l'adressage publique.

Une adresse de diffusion globale se compose de trois parties :

- Préfixe de routage global
- ID de sous-réseau
- ID d'interface

La figure 30 illustre la structure d'une adresse globale unicast utilisant le préfixe de routage global /48. Les préfixes /48 sont les préfixes de routage global les plus couramment attribués.

Figure 30 : Adresses Globales unicast

II.5.5.2 Adresses unicast de lien local (link-local) :

Une adresse link-local IPv6 permet à un périphérique de communiquer avec d'autres périphériques IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau). Les paquets associés à une adresse link-local source ou de destination ne peuvent pas être acheminés au-delà de leur liaison d'origine [10].

Les adresses link-local IPv6 se trouvent dans la plage FE80::/10. Indique que les 10 premiers bits sont 1111 1110 10xx xxxx. Le premier hextet dispose d'une plage comprise entre 1111 1110 10**00 0000** (FE80) et 1111 1110 10**11 1111** (FEBF).

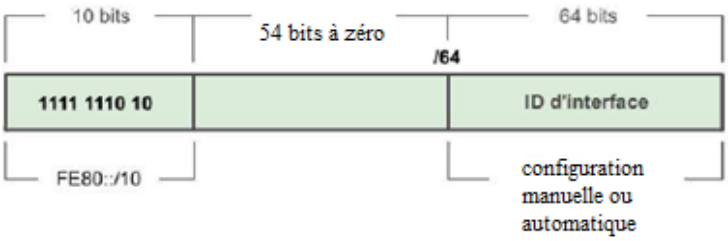


Figure 31 : Adresses unicast de lien local

II.5.5.3 Adresses unicast de site local :

Ces adresses sont destinées à l'utilisation sur un site unique sans l'utilisation d'un préfixe global. Par exemple, un site qui n'est pas encore connecté à Internet pouvait utiliser ces adresses, ce qui lui évitera de demander un préfixe de réseau. C'est en quelque sorte des adresses IP privées. Les routeurs ne doivent pas transmettre des paquets avec ce type d'adresse en dehors du site concerné.

Une adresse site-local était construite en concaténant le préfixe FEC0::/48, un champ de 16 bits qui permet de définir plusieurs sous-réseaux, et les 64 bits de l'identifiant d'interface.

1111 1110 11	38 bits à zéro	Id sous-réseau (16 bits)	Id d'interface (64 bits)

Figure 32 : Adresse unicast de site local

II.5.5.4 Adresse anycast :

Au lieu d'envoyer un paquet à une interface déterminée, on envoie ce paquet à une adresse (anycast) qui représente un ensemble de machines dans un domaine bien défini. Une adresse anycast permet de désigner un service par une adresse bien connue, de cette manière, il n'est pas nécessaire d'interroger un serveur pour connaître la localisation d'un équipement. La figure 33 donne la structure de l'adresse anycast. On y retrouve une partie préfixe et une partie identifiant anycast. La partie préfixe est la même que celle utilisée pour les adresses unicast. Contrairement aux structures d'adresses vue précédemment, la longueur de ce préfixe n'est pas spécifiée, car une adresse anycast doit s'adapter aussi bien aux plans d'adressage actuels (où la longueur est généralement de 64 bits) qu'aux futurs plans qui pourraient avoir des tailles différentes. Etant donné qu'il n'y a aucun moyen de différencier une adresse anycast d'une adresse unicast, et le nœud auquel cette adresse est attribuée doit être configuré pour savoir qu'il s'agit d'une adresse *anycast*.

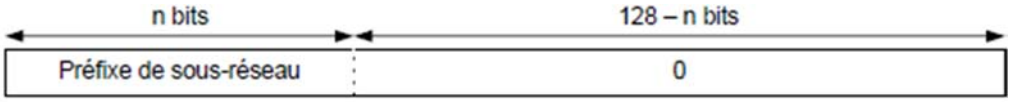
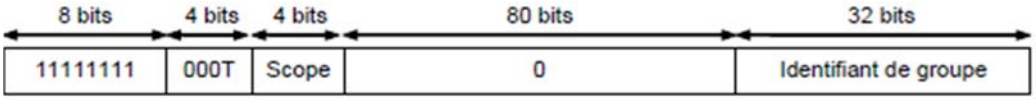


Figure 33 : Adresses d'anycast

II.5.5.5Adresse multicast

Contrairement aux autres types, les adresses multicast ne sont pas attribuées à des interfaces, mais représentent un groupe d'interfaces cibles dans un réseau local ou en dehors, selon la portée de l'adresse. L'adresse multicast comporte 4 champs (figure 34), le premier identifie une adresse de multicast (préfixe FF00::/8). Le second, le champ flags, est un champ de bits (4 bits) dont seul le dernier bit est défini, il s'agit du bit T, ce bit à « 0 » indique que l'adresse est permanente ou à «1» indique adresse temporaire. Le champ suivant indique le niveau de diffusion (*scope*).



Le bit T à "1" indique que le groupe est temporaire.
Le champ "Scope" définit la portée du groupe multicast.

Scope	Portée du groupe	Préfixe
1	Nœud local	FF01
2	Lien local	FF02
5	Site local	FF05
8	Organisation locale	FF08
E	Portée globale	FF0E

Figure 34 : Adresses multicast

II.5.6 Les adresses particulières :

a) **Adresse indéterminée :** l'adresse indéterminée (*unspecified address*) correspond à l'adresse 0.0.0.0 d'IPv4, elle est utilisée comme adresse source par un nœud du réseau pendant son initialisation, avant d'acquérir une adresse. Sa valeur est 0:0:0:0:0:0:0:0 (en abrégé ::).

Cette adresse est utilisée uniquement par des protocoles d'initialisation, elle ne doit jamais être attribuée à un nœud et ne doit jamais apparaître comme adresse destination d'un paquet IPv6.

b) **Adresse de bouclage :** l'adresse de bouclage (*loop back address*) vaut 0:0:0:0:0:0:0:1 (en abrégé ::1). C'est l'équivalent de l'adresse 127.0.0.1 d'IPv4. Elle est utilisée par un nœud pour s'envoyer à lui-même des paquets IPv6.

Un paquet IPv6 transitant sur le réseau ne peut avoir l'adresse de bouclage comme adresse source ni comme adresse destination.

c) **Adresses IPv4 mappées :** elles sont représentées sous la forme **::FFFF:a.b.c.d** où **a.b.c.d** est une adresse IPv4. On peut bien entendu aussi les écrire sous la forme **::FFFF:XXXX:YYYY** où **XXXXYYYY** est la représentation hexadécimale de l'adresse IPv4 **a.b.c.d** .

Cela permet d'écrire des serveurs (au sens client/serveur) qui peuvent répondre à la fois à des requêtes IPv4 et IPv6 dans le même programme. Cela nécessite bien sûr d'avoir une machine à double pile de communication IPv4 et IPv6

II.6 Le service DNS :

Le service DNS (*Domain Name System*, système de noms de domaines) est un service TCP/IP permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine. Sans DNS, vous achèteriez des livres sur 87.238.83.167 plutôt que sur www.amazon.fr, et vous lanceriez des recherches sur 209.85.229.103 plutôt que sur www.google.com. Se souvenir de 209.85.229.103 est déjà compliqué, mais quand vous surfez sur 40 sites différents par jour, cela fait quelques adresses à retenir. Et ça, on ne sait pas faire. Ainsi, avec l'arrivée d'IPv6, le DNS devient plus que jamais un service critique pour le fonctionnement des applications TCP/IP classiques.

II.7Attribution des adresses IP et standardisation des protocoles :

Pour que les entreprises ou organisations puissent prendre en charge les hôtes réseau (par exemple les serveurs web) accessibles depuis Internet, elles doivent disposer d'un bloc d'adresses publiques. N'oublions pas que les adresses publiques doivent être uniques et que l'utilisation des adresses publiques est régulée et dépend de chaque organisation. Cela vaut pour les adresses IPv4 et IPv6.

Elles sont gérées par l'ICANN (Internet Corporation for Assigned Names and Numbers).L'ICANN est un organisme international créé en octobre 1998 pour remplacer l'IANA (Internet Assigned Numbers Authority). Beaucoup de spécifications de protocoles comportent des nombres, mots clés et paramètres qui doivent être affectés de manière unique, par exemple les numéros de versions, les numéros de protocoles, les numéros de ports. C'est l'ICANN qui affecte les valeurs de ces paramètres pour l'Internet. L'ICANN publie aussi les tables de toutes les valeurs affectées dans des documents appelés RFC (Request for Comments) nommés Assigned Numbers. L'ICANN sert aussi de "sommet de la pyramide" pour la gestion des domaines de noms (DNS) et l'affectation des adresses et en établit les règles et les attribue aux organismes d'enregistrement Internet locaux (RIR).

Les RIR ou RIAR (*Regional Internet Address Registries*) reçoivent une délégation de l'ICANN pour distribuer les adresses IPv4 et IPv6 à des FAI qui, à leur tour, fournissent des blocs d'adresses IPv4 aux entreprises et aux FAI de plus petite envergure. Ils sont au nombre de quatre actuellement, répartis sur 4 continents pour assurer une gestion de "proximité" à cette échelle. Ce sont :

- APNIC : Asia Pacific Network Information Centre,
- ARIN : American Registry for Internet Numbers,
- RIPE-NCC : Réseaux IP Européen (Network Coordination Centre),
- LACNIC : Réseaux d'Amérique Latine et des Caraïbes.

Un cinquième, l'AFRINIC destiné à assurer la couverture du continent Africain est en cours de gestation (l'Afrique dépend actuellement du RIPE et de l'APNIC).

Figure 35 : Les organismes d'enregistrement Internet locaux

II.8 Discussion:

Actuellement, IPv4, version actuelle du protocole IP, est largement utilisée, mais dernièrement elle a connu des limites : espace d'adressage limité vu la croissance exponentielle de la taille de l'internet et du nombre d'équipements connectés actuellement, en qualité de service, en mobilité et en sécurité. En outre, malgré l'utilisation de certaines solutions provisoires, telles que le NAT et le CIDR pour retarder cette transition dans une certaine période, les spécialistes n'ont pas pu résoudre le problème du manque des adresses IPv4. Toutes ces limites ont été résolues en IPv6, la nouvelle version du protocole IP développé par l'IETF (Internet Engineering Task Force) qui a ajouté de nombreuses améliorations notamment, un espace d'adressage énorme sur 128 bits au lieu de 32 bits en IPv4, une meilleure gestion de la bande passante à l'aide du multicast et anycast, un meilleur support de qualité de service pour toutes les applications. La transition vers l'IPv6 n'aura pas lieu à une date fixe. L'IETF a créé divers protocoles et outils qu'on va étudie dans ce troisième chapitre.

CHAPITRE III :

Les Méthodes De Transition d'IPv4 Vers IPv6

III.1 Préambule:

Une fois le protocole IPv6 conçu, il ne reste plus qu'à le déployer, afin de remplacer le vieil IPv4, et de bénéficier de tous les avantages précités. C'est alors qu'un autre problème se présente : la transition d'un protocole à l'autre. En effet, les transitions ne sont jamais faciles, et celle-ci n'est pas une exception. D'autant plus le passage de l'IPv4 à l'IPv6 est complexe, et ne sera pas un projet du jour au lendemain. Le déploiement de l'IPv6 ne peut se faire que progressivement et étape par étape. Pour cette raison IETF a mis en place plusieurs mécanismes de transition qui représentent des solutions provisoires en attendant la migration vers IPv6.

Ce chapitre porte sur l'étude des méthodes de transition de l'IPv4 à l'IPv6 que nous avons classé en trois catégories : pour chacune d'entre elles nous allons décrire les mécanismes concernés et leurs principes de fonctionnement.

III.2 Phases de transition vers IPv6 :

La transition de l'IPv4 vers l'IPv6 peut se découpe en trois phases :

- **Phase où seuls des équipements IPv4 existent :** On arrive aujourd'hui à la fin de cette phase, puisque de nombreux constructeurs proposent déjà les premières versions d'IPv6 pour les postes de travail et les routeurs.

- **Phase de coexistence d'équipements IPv4 et IPv6 :** vise à généraliser la double pile et en même temps mettre en place des mécanismes de coexistence des équipements IPv4 et IPv6 comme (tunneling, translation).

- **Enfin, phase où seuls les équipements IPv6 subsisteront :** voit l'abandon progressif d'IPv4 sur Internet. Certains réseaux privés continuent à s'en servir, dans la mesure où la connectivité Internet ne leur est pas nécessaire.

III.3 Les méthodes de transition :

Une méthode de transition est un mécanisme ou un procédé pour connecter des hôtes/réseaux utilisant les mêmes ou des protocoles IP différents. La transition d'IPv4 vers IPv6 ne peut se faire que d'une manière progressive qui va s'étaler sur une longue période en raison de la complexité de la taille de l'internet et du nombre énorme de dispositifs connectés au temps actuel [11]. Et même si la migration de tout le réseau reste le but à long terme, la coexistence des deux protocoles est le but à court terme. Pour cela, il existe de nombreuses techniques de transition d'IPv4 vers IPv6, que l'on peut regrouper en trois catégories :

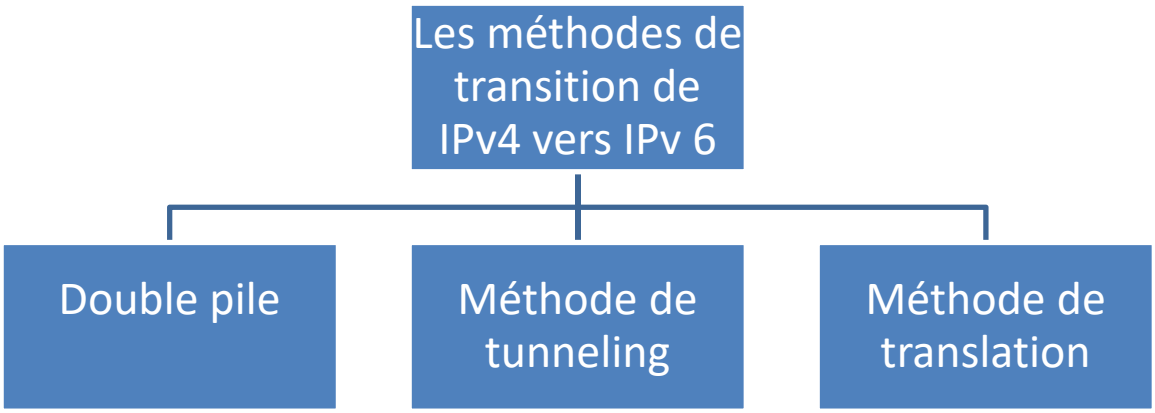


Figure 36 : Les méthodes de transition d'IPv4 vers IPv6

III.3.1 La double pile :

La double pile (dual-stack) est la préférée des techniques de transition, car elle ne fait intervenir aucun mécanisme de tunneling ou de translation d'adresse [14]. Cela signifie que les deux protocoles IPv4 et IPv6 fonctionnent côte-à-côte sur la même infrastructure et sur tous les équipements connectés au réseau : ordinateur, routeur, commutateur, firewall, serveur, etc. comme on peut le voir à la figure suivante :

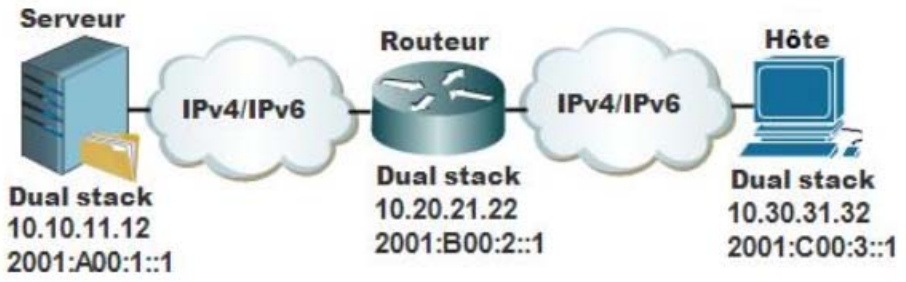


Figure 37 : Réseau double pile

Pour déterminer la version du protocole IP à utiliser, l'hôte source interroge le DNS lors de l'envoi d'un paquet à une destination. Si le DNS renvoie une adresse IPv4, l'hôte source envoie un paquet IPv4. Si le DNS renvoie une adresse IPv6, l'hôte source envoie un paquet IPv6. La double pile est très utilisée et d'ailleurs beaucoup d'autres mécanismes (tunneling et translation) ont besoin au moins un hôte ayant une double pile.

III.3.2 Le tunneling (encapsulation) :

Le tunneling (encapsulation) est une technique utilisée lorsque deux hôtes ou réseaux utilisant IPv6 veulent communiquer et les paquets IPv6 doivent passer à travers une région purement IPv4. Pour passer à travers cette région, le paquet doit avoir une adresse IPv4. Ainsi, les paquets IPv6 son encapsulés dans des paquets IPv4 à l'entrée du tunnel en ajoutant un entête IPv4 et décapsulés et traités comme s'ils provenaient du réseau IPv6 à la sortie du tunnel. Le tunneling peut aussi être utilisé à l'inverse pour envoyer des paquets IPv4 à travers une infrastructure IPv6. Cependant, compte tenu de la rareté relative aux réseaux purement IPv6, ce type de tunnel est beaucoup moins utilisé.

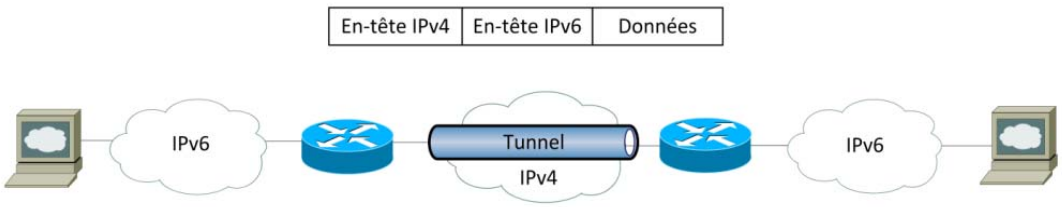


Figure 38 : Encapsulation d'un paquet IPv6 à l'intérieur d'IPv4

III.3.2.1 Les types de tunnels :

On peut distingues plusieurs types de tunnels

- **Routeur à routeur**: deux routeurs interconnectés via le réseau IPv4 et ayant une connexion au réseau IPv6 peuvent transporter des paquets IPv6 en les encapsulant.

- **Hôte à routeur :** l'hôte peut créer un tunnel jusqu'à un routeur ayant une connectivité IPv6. Le paquet sera envoyé en IPv6 natif depuis le routeur jusqu'à la destination, comme illustré à la figure ci-dessous.

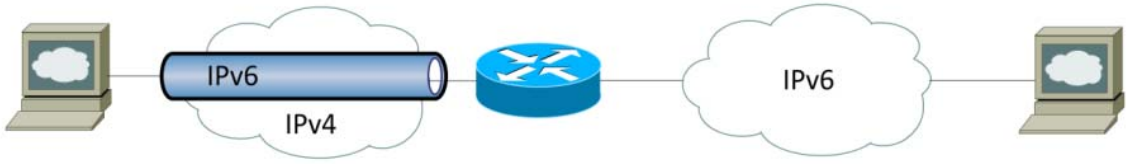


Figure 39 : Tunnel hôte à routeur

- **Hôte à Hôte :** un hôte source effectue l'encapsulation, et le tunnel se termine chez l'hôte de destination.

III.3.2.2 Les mécanismes de tunneling:

Il existe plusieurs types de mécanismes de tunneling. Ces mécanismes incluent :

- Configurer manuellement
  -IPv6 over IPv4 Tunnel manuel (RFC2893)
  - GRE (RFC2473)
- Semi-automatiques
  - Tunnel broker
- Automatiques
  - 6to4 (RFC3056)
  - 6rd
  - ISATAP
  -Teredo

Tous les mécanismes de tunneling nécessitent que les points d'extrémités du tunnel soient équipés en double pile et exécutent tous les protocoles IPv4 et IPv6 d'une manière simultanée.

III.3.2.2.1 Configuration manuellement :

a. IPv6 over IPv4 Tunnel manuel :

Dans le tunneling manuel, l'adresse IPv4 du point final du tunnel est déterminée à partir des informations de configuration du nœud d'encapsulation. Pour chaque tunnel, le nœud d'encapsulation doit préciser l'adresse du point final du tunnel. Lorsqu'un paquet IPv6 est transmis sur un tunnel, l'adresse IPv4 du nœud final du tunnel configurée dans le nœud d'entré du tunnel est utilisée comme adresse de destination pour l'en-tête IPv4 encapsulant l'IPv6.

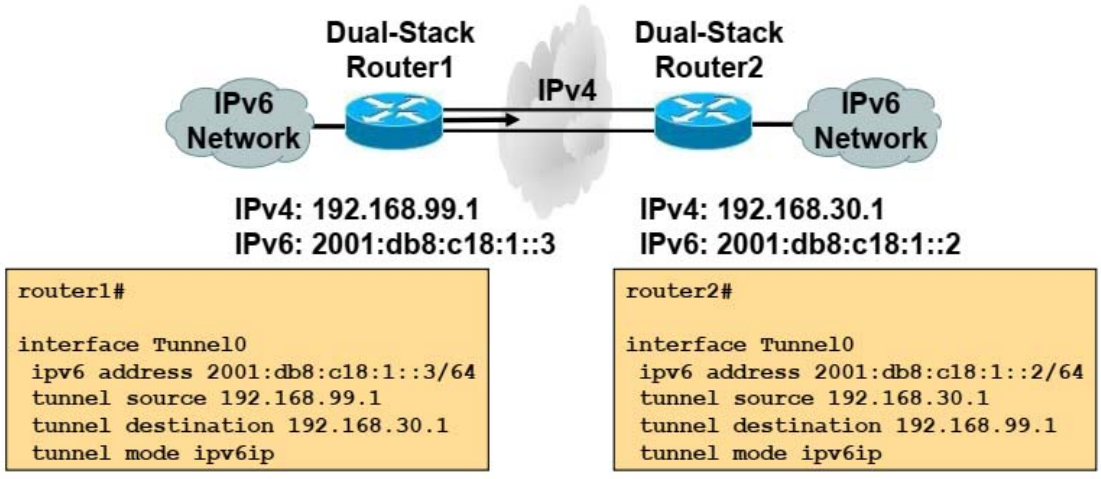


Figure 40 : Tunnel configuré manuel

La détermination des paquets à transmettre par tunnel est généralement réalisée via une table de routage, qui dirige les paquets en fonction de leurs adresses destination en utilisant le préfixe et la technique de correspondance.

b. Tunnel IPv6 GRE (Generic Routing Encapsulation):

Le tunnel GRE a été développé par Cisco et peut encapsuler une large gamme de paquets de différents protocoles dans des paquets IP. Le protocole encapsulé dans ce cas l'IPv6 appelé protocole passager et l'entité IPv4 utilisée pour encapsuler est appelé le protocole porteur. Ce tunnel a une en-tête d'encapsulation supplémentaire c'est l'en-tête GRE, par conséquent, le tunnel aura un paquet IPv6 encapsulé dans l'en-tête GRE, puis dans l'en-tête IPv4.

La configuration d'un tunnel GRE est manuelle. Sur les deux extrémités du tunnel comme la montre la figure 41 :

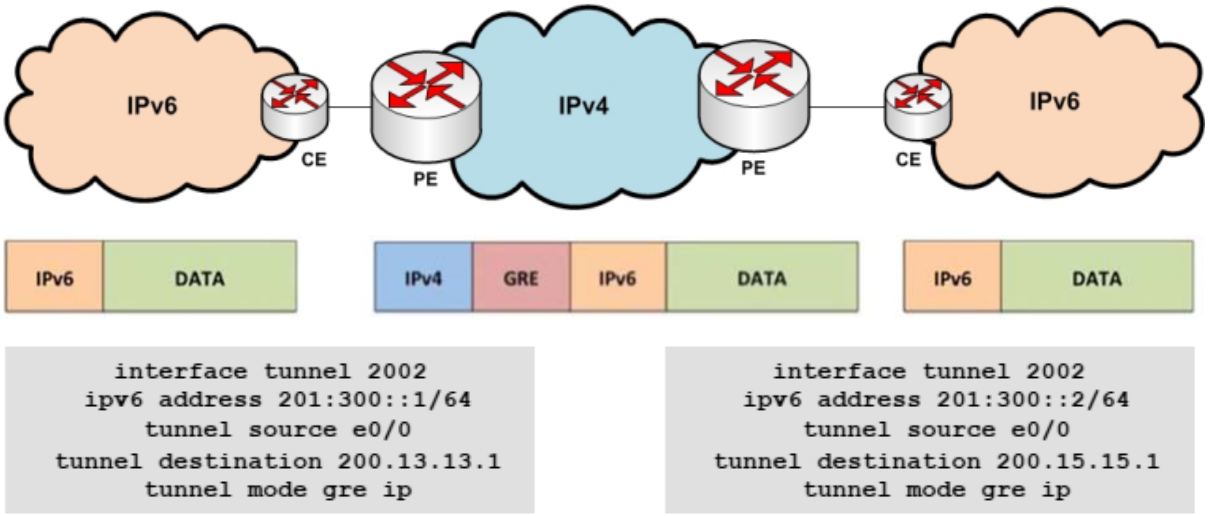


Figure 41 : Tunnel IPV6 GRE

III.3.2.2.2 Semi-automatique :

a. Tunnel broker :

Pour obtenir une connectivité IPv6 indépendante des FAI locaux, on peut faire appel à un fournisseur de tunnel IPv6.

Le tunnel broker est une société tierce fournissant un service de tunnel. Pour ce faire, il faut généralement s'inscrire chez le tunnel broker, puis demander l'ouverture d'un tunnel. Alors, le tunnel broker va configurer un de ses routeurs afin de mettre en place le tunnel. Enfin, il enverra un script à exécuter sur la machine souhaitant utiliser le tunnel, pour

configurer correctement les paramètres réseaux. La machine est alors connectée à l'IPv6 via le service du tunnel broker [12]. Les étapes énumérées ci-avant sont illustrées à la Figure 42.

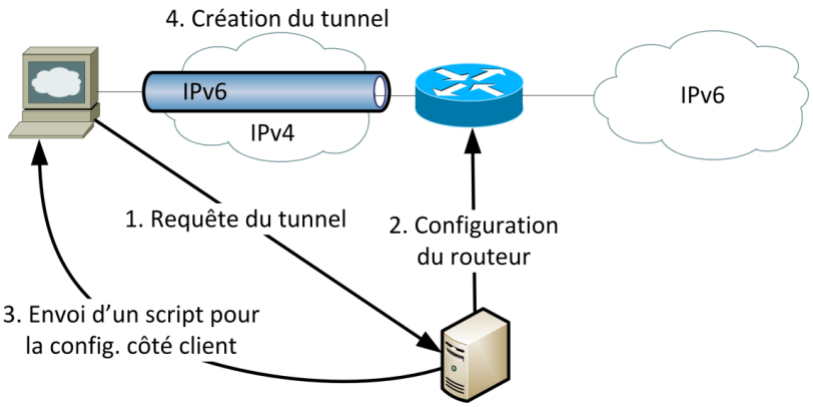


Figure 42 : Tunnel broker

III.3.2.2.3 Automatique:

a. Le mécanisme 6to4:

Le 6to4 va nous permettre d'établir des tunnels IPv6 sur un réseau IPv4 de type point-to-multipoint de façon totalement dynamique entre des sites IPv6 isolés. La force de cette méthode est de pouvoir par exemple, ajouter 100 routeurs dans votre topologie sans pour autant remettre en cause la configuration de vos routeurs existants puisque tout s'établit de façon dynamique [24]. Une adresse IPv6 spéciale (2002::/16) indique que ce nœud utilisera un tunnel 6to4 pour se connecter au réseau mondial IPv6. Cette dernier est définie comme suit :

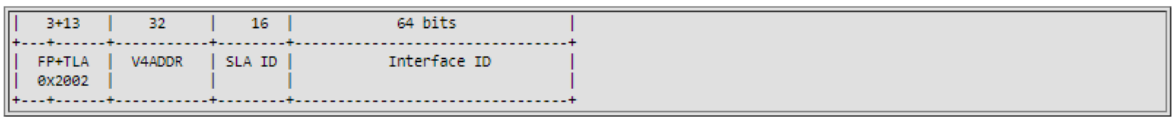


Figure 43 : Adressage 6to4

FP et TLA ensemble (16 bits) ont la valeur 2002. V4ADDR est l'adresse IPv4 globale et unique du nœud (en notation hexadécimale). SLA est l'identifiant de sous-réseau.

Au niveau du routage, la figure 44 présente l'envoi d'un paquet IPv6 de l'hôte A vers l'hôte B. Il est important de noter ici que A et B sont des hôtes ayant une adresse IPv6

prise dans le plan d'adressage 6to4. Dans un premier temps, A interroge le DNS pour connaître l'adresse IPv6 de B. Dans notre exemple, la réponse est 2002:c000:301:1::8051. Dans un second temps, l'hôte A émet le paquet vers cette destination. Ce paquet IPv6 doit passer par un tunnel 6to4. C'est au routeur 6to4 (routeur configuré avec un tunnel 6to4) du site de A qu'il revient d'effectuer cette opération. Ce dernier analyse l'adresse IPv6 de destination et trouve l'adresse IPv4 de l'autre extrémité du tunnel (dans notre exemple 2002:**c000:301**:1::8051). Il pourra alors effectuer la transmission en encapsulant le paquet IPv6 dans un paquet IPv4. C'est cette encapsulation qui forme le tunnel. Le routeur 6to4 du coté de B décapsule le paquet IPV6 et le route normalement vers sa destination finale B en utilisant le routage interne. [25]

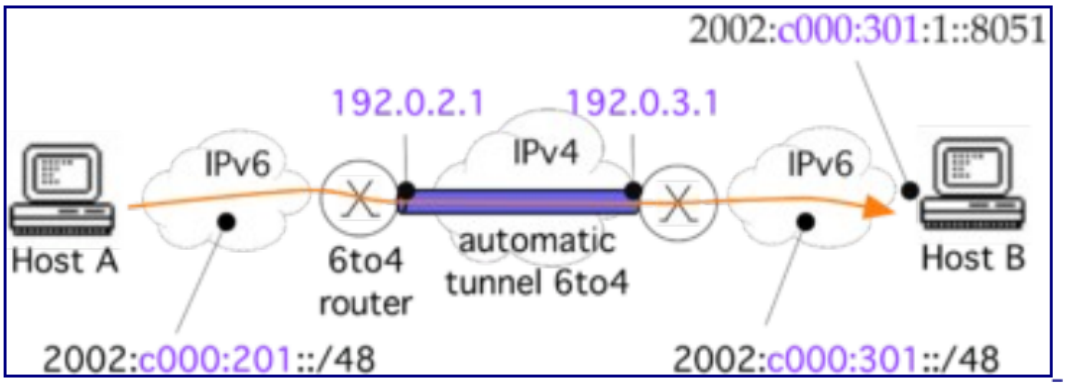


Figure 44 : Acheminement d'un paquet IPv6 en 6to4.

b. Le mécanisme 6rd :

Il a effectivement été constaté en 2010 qu'environ 15% des connexions IPv6 qui échouent sont des connexions 6to4. Il a donc été proposé à l'IETF une extension le protocole 6rd (IPv6 rapid deployment). Le protocole 6rd reprend les principes de fonctionnement du protocole 6to4, tout en corrigeant ses défauts. A la place d'utiliser un seul et unique préfixe (2002::/16 pour 6to4), 6rd utilise un préfixe différent pour chaque FAI, de même les routeurs 6to4 sont remplacés par des routeurs 6rd [27].

c. Le mécanisme ISATAP :

ISATAP (Intra-site Automatic Tunnel Addressing Protocol) est un mécanisme automatique de tunneling défini dans la RFC 5214, permettant la communication entre hôtes

IPv6 à l'intérieur d'un même site (intranet), en utilisant l'infrastructure IPv4 existante. Ceci est illustré à la Figure 45. Les adresses ISATAP sont composées d'un préfixe unicast valide 64 bits et d'un identificateur d'interface **::0:5EFE:w.x.y.z** où **0:FE5E** désigne une adresse ISATAP et **w.x.y.z** représente l'adresse IPv4 au format décimal pointé. Il faut toutefois noter qu'ISATAP ne supporte pas le NAT.

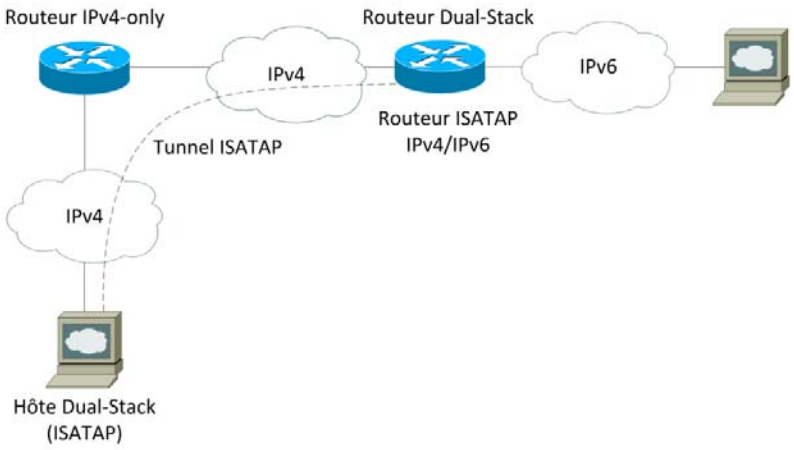


Figure 45 : Tunnel ISATAP.

d. Le mécanisme Teredo :

Les diverses méthodes qui consistent à encapsuler le paquet IPv6 dans un paquet IPv4 ne marchent pas lorsqu'un NAT se trouve dans la chaine de communication. Teredo est une méthode qui permet de pallier ce problème en encapsulant le paquet IPv6 non plus directement dans un paquet IPv4 mais dans un paquet UDP puis dans IPv4.

Les adresses Teredo utilisent le préfixe 3FFE:831F::/32. Au-delà des 32 premiers bits, Teredo aborde l'adresse IPv4 encodée d'un serveur Teredo, drapeaux, adresse et numéro de port (en sortie de NAT) du client Teredo

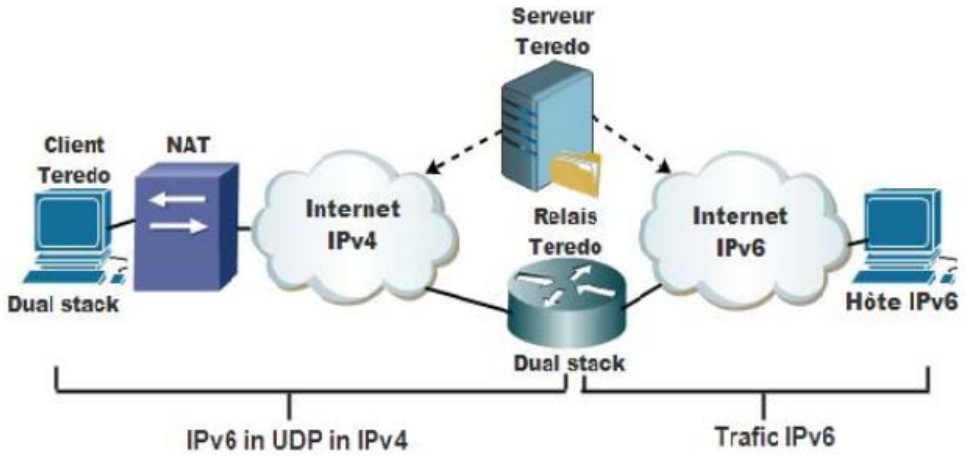


Figure 46 : Tunnel Teredo

L'infrastructure Teredo est composée d'un client, d'un relais et d'un serveur Teredo, comme illustré à la figure 46. Le serveur Teredo assiste un client dans sa configuration d'adresse en découvrant son adresse et son port, et facilite la communication entre clients Teredo. Le relais Teredo transmet les paquets à un hôte IPv6.

III.3.3 La technique de Translation :

III.3.3.1 NAT-PT/DNS-PT :

NAT-PT (Network Address Translation-Protocol Translation) est un dispositif résidant à la frontière d'un réseau IPv4/IPv6, permettant la communication entre des nœuds IPv4 résidant dans un réseau IPv4 et des nœuds IPv6 résidant dans un réseau IPv6 et vice versa en faisant la translation des adresses IP, comme illustré sur la figure 47 ci-dessous. Le NAT-PT conserve une plage d'adresses IPv4 routables globalement et attribue des adresses IPv4 aux nœuds IPv6 et vice versa. Ceci est similaire au NAT IPv4 traditionnel. La NAT-PT peut être combiné avec un DNS-PT. DNS-PT offre la résolution automatique des noms IPv4 en IPv6 et vice versa.

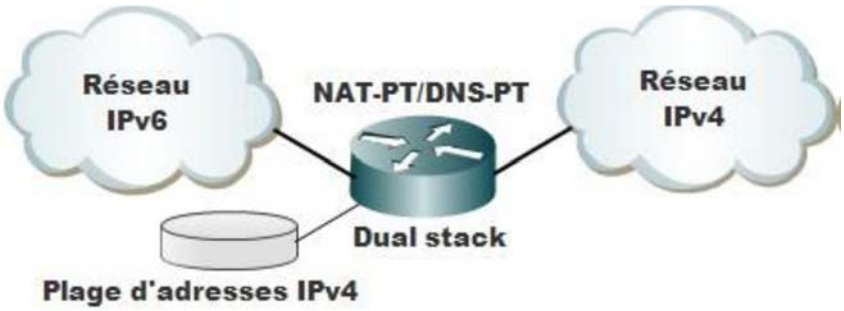


Figure 47 : Translation NAT-PT/DNS-PT

III.3.3.2 NAT64/DNS64

La majorité des services et contenus internet sont aujourd'hui disponibles uniquement sur IPv4. En attendant la migration vers IPv6, les clients IPv6 ont également besoin d'accéder à ces services sur IPv4, NAT64 et DNS64 permettent cela. Le NAT64 permet à des clients "IPv6- only" de contacter un serveur IPv4, comme on peut le voir à la figure 48 ci-dessous. Il faut noter que la communication ne peut s'initier que dans ce sens. En combinant le NAT64 avec un DNS64, aucun changement de configuration n'est nécessaire, ni du côté des hôtes IPv6, ni du côté du serveur IPv4. Les requêtes DNS de l'utilisateur final IPv6 sont reçues par l'équipement DNS64. S'il y a un enregistrement DNS IPv6 (enregistrement AAAA), alors la résolution est transmise à l'utilisateur final qui pourra accéder directement à la ressource. S'il n'y a pas d'adresse IPv6 mais une adresse IPv4 (enregistrement A), alors DNS64 convertit l'enregistrement A en enregistrement AAAA en utilisant son préfixe NAT64 et le transmet a l'utilisateur final. Celui-ci peut alors accéder à l'équipement NAT64 qui « Translate » ce trafic vers le serveur IPv4.

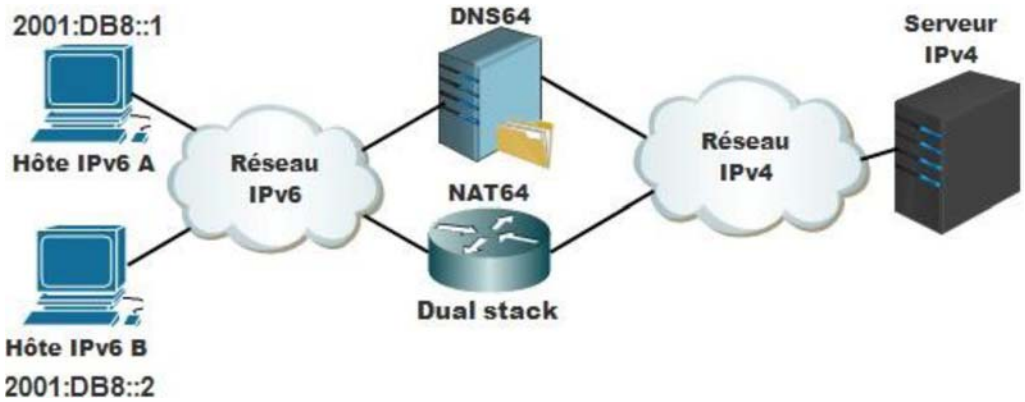


Figure 48: Translation NAT64/DNS64

III.3.3.3 SIIT (Stateless IP/ICMP Translator):

SIIT est un mécanisme de transition utilisant un algorithme de traduction bidirectionnel pour convertir des en-têtes IPv4 en IPv6 et ICMPv4 en ICMPv6 et inversement, comme le montre la Figure 49 ci-dessous. Cet algorithme peut être utilisé comme une partie d'une solution qui permet à des nœuds IPv6 qui ne possèdent pas des adresses IPv4 attribuées (assigned IPv4 address) de communiquer avec des hôtes IPv4. Lors de la communication, la boite de traduction attribue une adresse IPv4 au site IPv6, et en outre le site IPv6 utilise des adresses IPv6/IPv4 mappées pour envoyer les paquets au site IPv4.

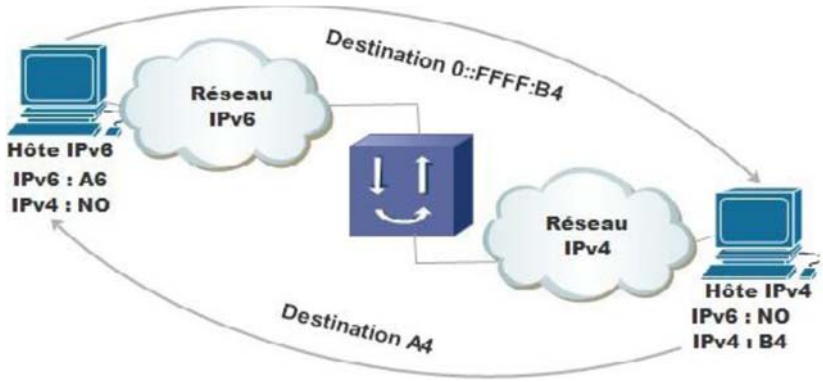


Figure 49 : Translation SIIT

III.4 Discussion :

Dans ce chapitre, une étude a été réalisée sur les mécanismes de transition de IPv4 vers IPv6. Cette étude n'est pas uniquement destinée pour comparer chaque mécanisme contre l'autre mais également pour décrire leurs principes de fonctionnement afin de montrer et aider les clients qui veulent utiliser ou se connecter en IPv6 de choisir le mécanisme approprié en fonction de leurs besoins en attendant la migration vers IPv6.

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

CHAPITRE IV :

Simulation Des Méthodes De Transition De IPv4 Vers IPv6 Sur Packet Tracer

IV.1 Présentation de Packet Tracer :

Le logiciel Packet Tracer est un simulateur de réseau qui permet de configurer les différents composants d'un réseau informatique. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc . . .

IV.2 Installation :

Pour commencer, nous avons installé le logiciel (Cisco Packet Tracer) sur notre pc (Windows 7) et pour ça nous avons suivi les étapes suivantes :

Avec un double clique sur le fichier source **Packet Tracer 7.1.1 for Windows 64 bits**, on aura la figure 50.

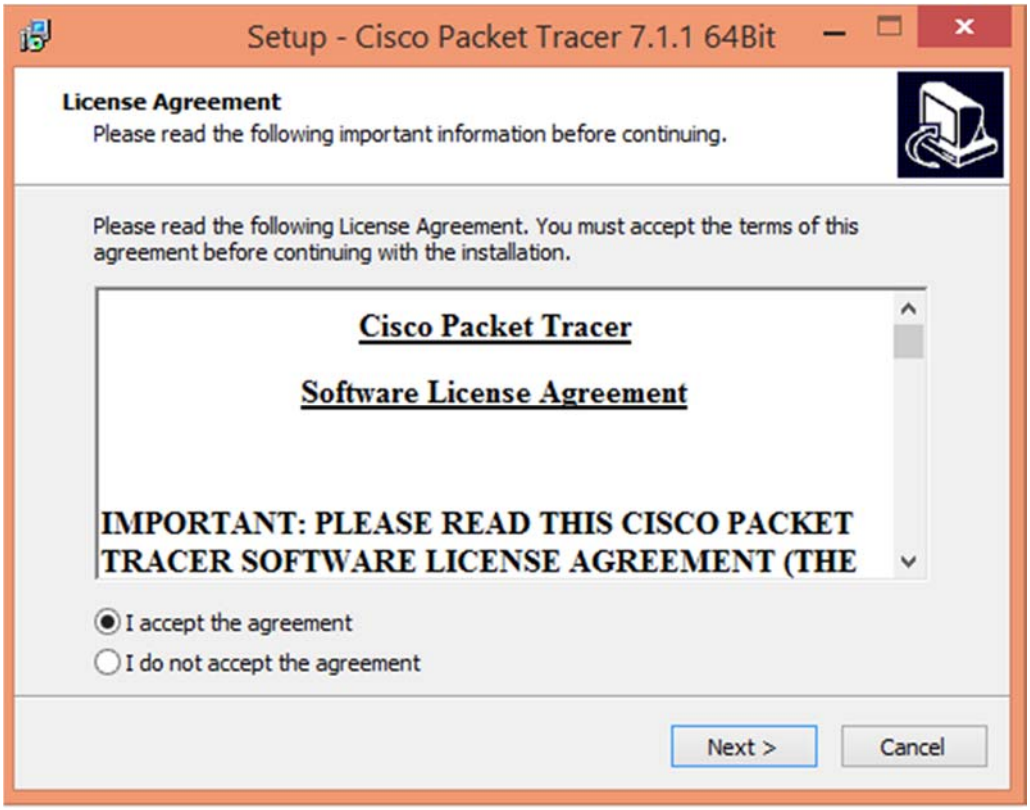


Figure 50 : Présentation de la première étape de l'installation du logiciel

On coche la case (I accept the agreement) puis on clique sur **Next**, l'assistant d'installation de Cisco Packet Tracer, nous invitera à finaliser les étapes d'installation on suivant les figures 51 et 52, tout en cliquant sur **Install**, pour avoir à la fin l'icône du logiciel figure 53.

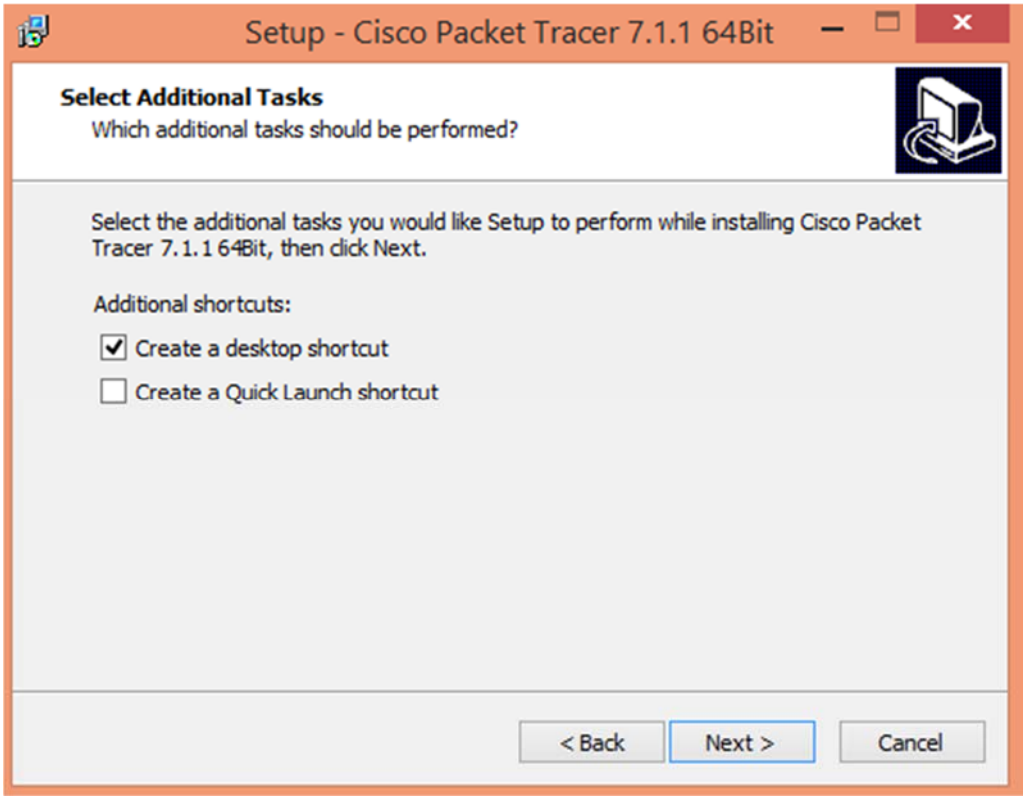


Figure 51 : Présentation de la deuxième étape de l'installation du logiciel

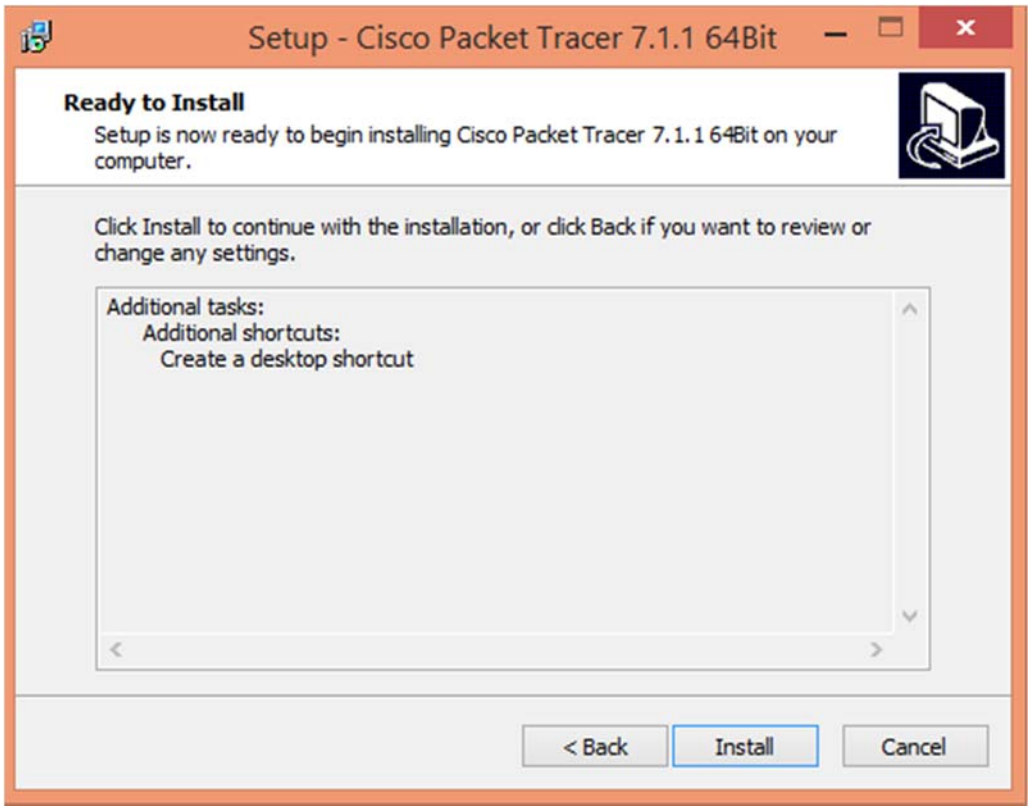


Figure 52: Installation de Packet Tracer

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

Figure 53: Icône de Cisco Packet Tracer

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

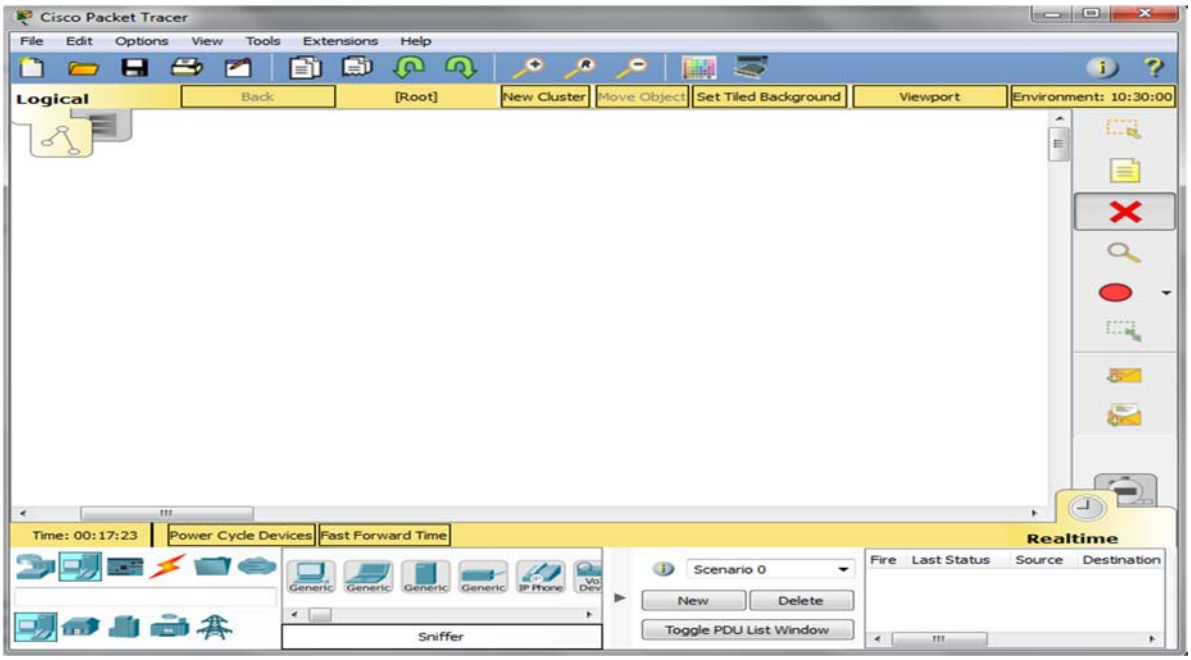


Figure 54: Fenêtre de Packet Tracer

IV.3 Description de Packet Tracer :

La fenêtre Packet Tracer est divisée en plusieurs zones semblables à un éditeur de photo. La numérotation dans la capture d'écran ci-dessous, montre les différentes zones avec les explications donnée après :

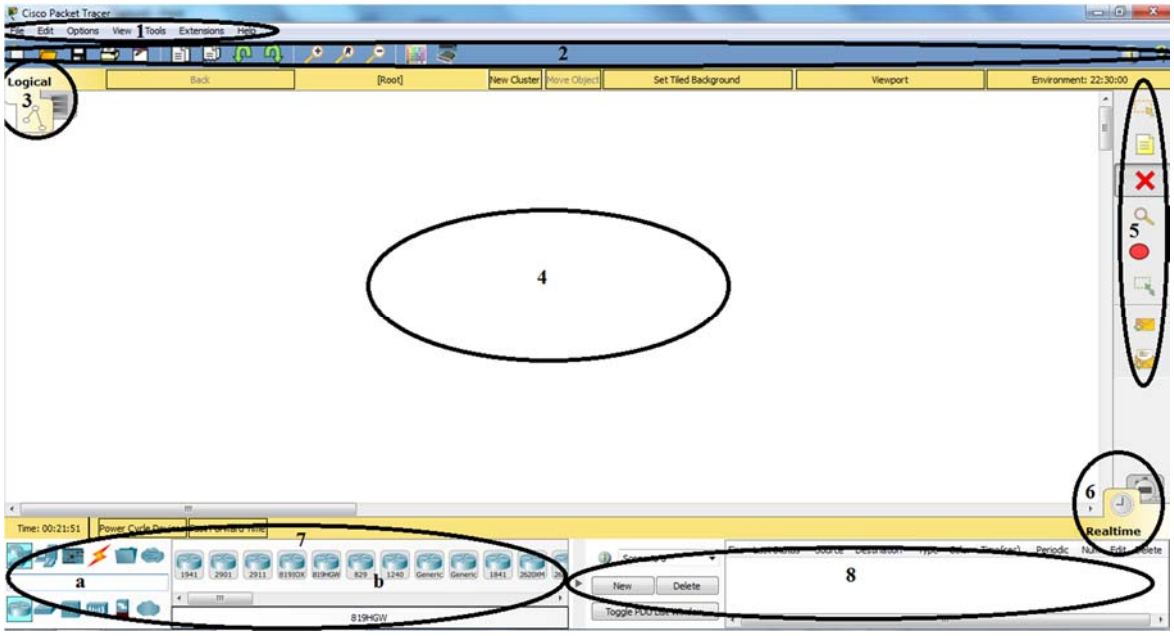


Figure 55:Différente zones de Packet Tracer

Les composants de l'interface de Packet Tracer sont comme suit :

- **Zone 1 : Barre de menus** – il s'agit d'un menu commun trouvé dans toutes les applications logicielles, il est utilisé pour ouvrir, enregistrer, imprimer, modifier les préférences et ainsi de suite.

- **Zone 2 : Barre d'outils principale –**cette barre fournit des icônes de raccourcis vers des options de menu qui sont généralement accessibles, comme ouvrir, enregistrer, zoom, annuler (Undo) et rétablir (Redu), et sur le côté droit nous trouvons une icône pour la saisie des informations de réseau pour le réseau actuel.

- **Zone 3 : Onglet d'espace de travail Logique/Physique –** ces onglets permettant de basculer entre les zones de travail logiques et physiques.

- **Zone 4 : Espace de travail –** c'est la zone où les topologies sont crées et les simulations sont affichées.

- **Zone 5 : Barre d'outils commune** – cette barre d'outils fournit des contrôles permettant de manipuler les topologies, comme sélectionner, déplacer la mise en page, placer des notes, supprimer, inspecter, redimensionner la forme et ajouter des PDUs (Protocol Data Unit) simple / complexe.

- **Zone 6 : Onglets Realtime/Simulation** – ces onglets sont utilisés pour basculer entre les modes temps réel et simulation. Des boutons sont également fournis pour contrôler le temps et capturer les paquets.

- **Zone 7 : Boite de composants réseau** – ce volet contient tous les périphériques réseau (Intermédiaires et finaux) disponible avec Packet Tracer et est divisé en deux zones :
- **Zone 7 a : Boite de sélection de type de périphérique** – cette zone contient les catégories d'équipements.

- **Zone 7 b : Boite de sélection spécifiques à l'appareil** – quand une catégorie d'appareil est sélectionné, cette boite de sélection affiche les différents modèles d'appareils dans cette catégories.

- **Zone 8 : Boite de paquet créé par l'utilisateur** – les utilisateurs peuvent créer des paquets hautement personnalisés pour tester leur topologie de cette zone, et les résultats sont affichés sous forme de liste.

IV.4 Simulation des trois méthodes de transition :

Pour réaliser la transition d'IPv4 vers IPv6, et c'est ça que ce chapitre présente. En premier temps, nous allons appliquer la technique de Double pile et en suite la réalisation d'un tunnel IPv6 over IPv4 manuel pour la communication entre 2 réseaux ipv6 à travers un réseau ipv4, et enfin la communication entre équipements IPv4 et IPv6 par la méthode Translation.
Dans cette partie, on va présenter l'implémentation des 3 scénarios de la migration de l'ipv4 vers l'ipv6 citée ci-dessus sur le logiciel Packet Tracer.

IV.4.1 La double pile :

Le principe de la double pile est que les hôtes peuvent s'échanger des messages en utilisant les deux versions du protocole d'internet. Ainsi les réseaux à double pile possèdent deux plans d'adressage IPv4 et IPv6 pour acheminement des deux protocoles.

IV.4.1.1 La topologie utilisée et les configurations des équipements :

La topologie que nous avons utilisé pour cette méthode est la suivante :

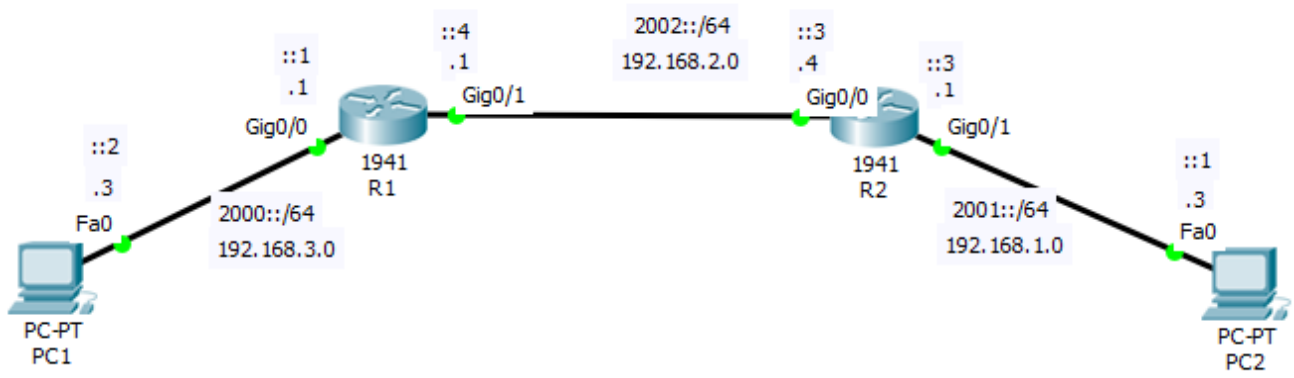


Figure 56 : Topologie utilisé pour la double pile

La configuration des équipements de se réseau et comme suite :

- **Le routeur R1**

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

Router>

On passant vers le mode **Utilisateur privilégié**

Router>en

On passant vers le mode **configuration globale**

Router#conf t

On renomme notre routeur

Router(config)#hostname R1

On configure les deux interfaces de R1

R1(config)#int g0/0

R1(config-if)#ip address 192.168.3.1 255.255.255.0

R1(config-if)#ipv6 address 2000::1/64

Allumer l'interface.

R1(config-if)#no shut

R1(config)#int g0/1

R1(config-if)#ip address 192.168.2.1 255.255.255.0

R1(config-if)#ipv6 address 2002::4/64

R1(config-if)#no shut

Activer le routage IPv6.

R1(config)#ipv6 unicast-routing

Activer le protocole de routage dynamique RIP et on ajoute les réseaux directement connectés.

R1(config)#router rip

R1(config-router)#network 192.168.2.0

R1(config-router)#network 192.168.3.0

On définir la route par défaut vers l'extérieur donc vers ::/0 par 2002::3.

R1(config)#ipv6 route ::/0 2002::3

- **Le routeur R2**

Router>en

Router#conf t.

Router(config)#hostname R2

R2(config)#int g0/0

R2(config-if)#ip address 192.168.2.4 255.255.255.0

R2(config-if)#ipv6 address 2002::3/64

R2(config-if)#no shutdown

R2(config)#interface GigabitEthernet0/1

R2(config-if)# ip address 192.168.1.1 255.255.255.0

R2(config-if)#ipv6 address 2001::3/64

R2(config-if)#no shutdown

On active le routage IPv6.

R2(config)#ipv6 unicast-routing

Activer le protocole de routage dynamique RIP et ajouter les réseaux directement connectés.

R2(config)#router rip

R2(config-router)#network 192.168.1.0

R2(config-router)#network 192.168.2.0

Définir la route par défaut vers l'extérieur donc vers ::/0 par 2002::4.

R2(config-router)#ipv6 route ::/0 2002::4

- **Le PC 1 :** 192.168.3.3 comme adresse IPv4 et 2000::2 comme adresse IPv6. La passerelle par défaut :192.168.3.1 comme adresse IPv4 et 2000::1 comme adresse IPv6.
- **Le PC2 :** 192.168.1.3 comme adresse IPv4 et 2001::1 comme adresse IPv6. La passerelle par défaut :192.168.1.1 comme adresse IPv4 et 2000::3 comme adresse IPv6.

IV.4.1.2 Vérification de connectivite :

Après l'exécution de ces commandes ci-dessus, si un hôte appartenant à l'un des LANs envoie un message vers un hôte appartenant à l'autre LAN, ce message doit être transféré correctement. Dans notre cas nous avons testé la connectivité entre 2 hôtes en exécutant la commande ping sur command Prompt sous PC2, une fois avec une adresse IPv6, et la seconde fois avec une adresse IPv4, dont le résultat est ci-dessous :

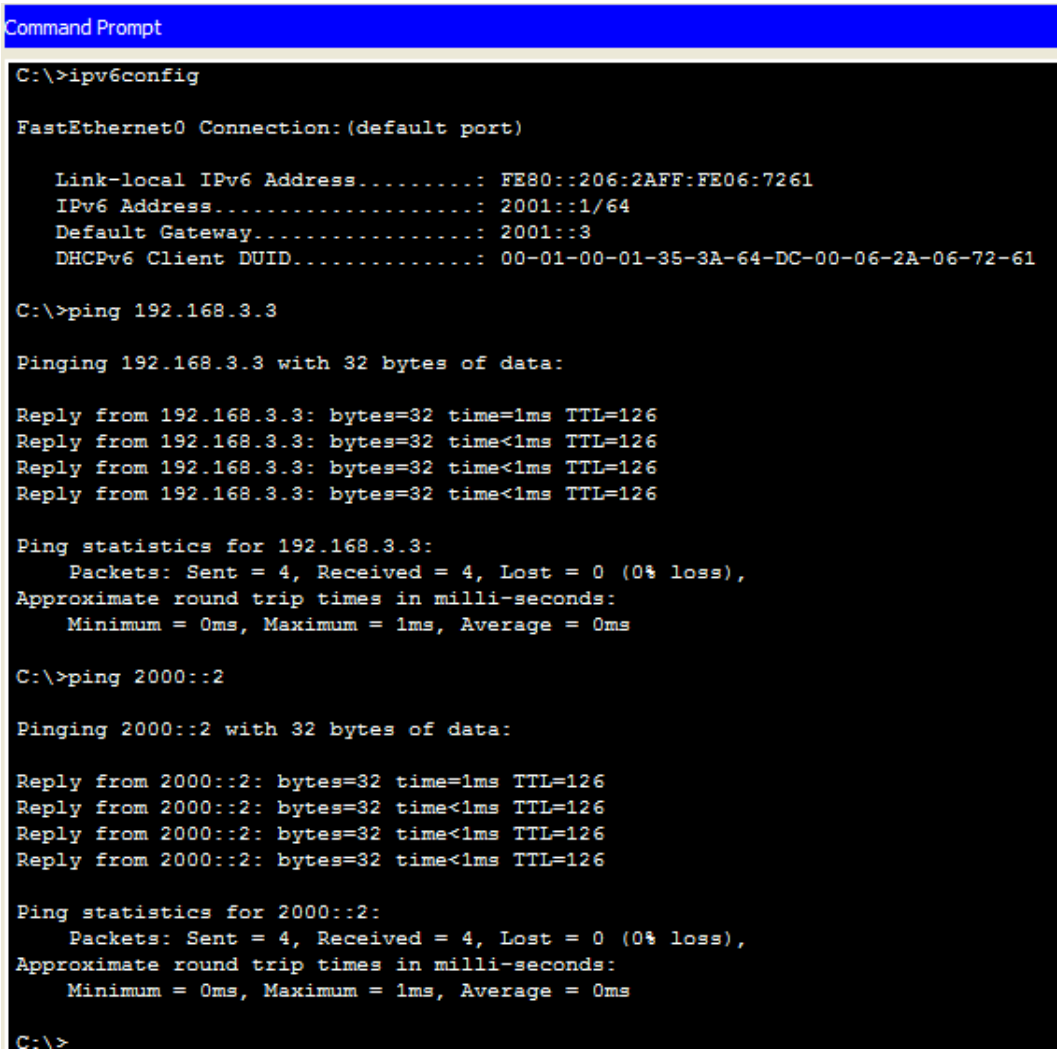


Figure 57 : Vérification de connectivité entre deux hôtes avec les deux protocole IPv4 et IPv6.

IV.4.2 Le tunneling :

Dans cette partie on va présenter comment configurer un tunnel IPv6 over IPv4 manuel, qui permet de faire communiquer des hôtes IPv6 à travers un réseau IPv4 par l'intermédiaire d'un tunnel, en encapsulant les paquets IPv6 dans des paquets IPv4.

IV.4.2.1 La topologie utilisée et les configurations des équipements:

Le schéma suivant illustre la topologie que nous avons mis en place pour l'implémentation de cette technique :

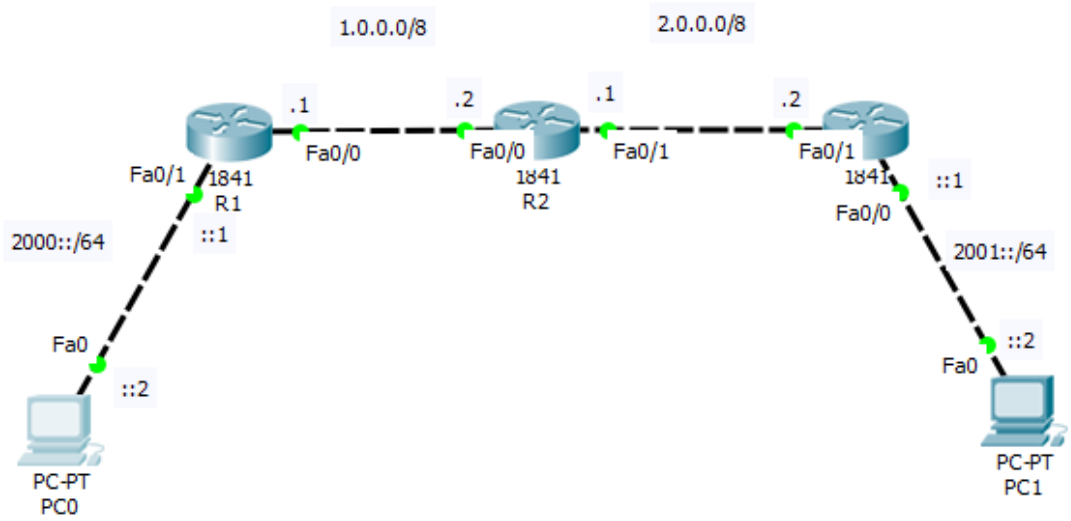


Figure 58 : Topologie utilisé pour la méthode de tunneling

La configuration des équipements de se réseau et comme suite :

- **Le routeur R1 :**

  Router>en

  Router#conf t

  Router(config)#hostname R1

On configure les deux interfaces.

  R1(config)#interface FastEthernet0/0

  R1(config-if)#ip address 1.0.0.1 255.0.0.0

  R1(config-if)#no shutdown

  R1(config)#interface FastEthernet0/1

  R1(config-if)#ipv6 address 2000::1/64

R1(config-if)#no shutdown

Activer le routage IPv6.

R1(config)#ipv6 unicast-routing

R1(config)#router rip

R1(config-router)#network 1.0.0.0

R1(config)#interface Tunnel0

R1(config-if)# ipv6 address 2020::2/64

R1(config-if)# tunnel source FastEthernet0/0

R1(config-if)# tunnel destination 2.0.0.2

R1(config-if)# tunnel mode ipv6ip

Une route statique pour déclencher notre tunnel et utiliser celui-ci en cas de sollicitation.

R1(config)#ipv6 route 2001::/64 2020::1

- **Le routeur R2**

Router>en

Router#conf t

Router(config)#hostname R2

R2(config)#interface FastEthernet0/0

R2(config-if)#ip address 1.0.0.2 255.0.0.0

R2(config-if)#no shutdown

R2(config)#interface FastEthernet0/1

R2(config-if)#ip address 2.0.0.1 255.0.0.0

R2(config-if)#no shutdown

Activer le protocole de routage dynamique RIP et ajouter les réseaux directement connectés.

```
R2(config)#router rip
R2(config-router)#network 1.0.0.0
R2(config-router)#network 2.0.0.0
```

- **Le router R3**

```
Router>en
Router#conf t
Router(config)#hostname R3
R3(config)#interface FastEthernet0/0
R3(config-if)#ipv6 address 2001::1/64
R3(config-if)#no shut
R3(config)#interface FastEthernet0/1
R3(config-if)#ip address 2.0.0.2 255.0.0.0
R3(config-if)#no shut
R3(config)#ipv6 unicast-routing
R3(config)#router rip
R3(config-router)#network 2.0.0.0
```

On configure le tunnel.

```
R3(config)#interface Tunnel0
```

Adresse IPv6 du tunnel.

```
R3(config-if)# ipv6 address 2020::1/64
```

Adresse IPv4 source du tunnel, on spécifié l'interface de sorite.

R3(config-if)# tunnel source FastEthernet0/1

Adresse ipv4 de l'autre extrémité du tunnel.

R3(config-if)# tunnel destination 1.0.0.1

On lui précise que le tunnel fera du ipv6 dans ipv4.

R3(config-if)# tunnel mode ipv6ip

Une route statique pour déclencher notre tunnel et utiliser celui-ci en cas de sollicitation.

R3(config)#ipv6 route 2000::/64 2020::2

- **Le PC 0 :** 2000::2 comme adresse IPv6. La passerelle par défaut : 2000::1 comme adresse IPv6.
- **Le PC 1 :** 2001::2 comme adresse IPv6. La passerelle par défaut : 2001::1 comme adresse IPv6.

IV.4.2.2 Vérification de connectivite :

Si un hôte appartenant à l'un des LANs IPv6 envoie un message vers un hôte appartenant à l'autre LAN IPv6, ce message doit être transféré correctement.

Nous avons testé la connectivité entre 2 hôtes IPv6 en exécutant la commande tracert sous PC0 vers le PC1. Ce qui indique bien que l'on passe par le tunnel :

```
Command Prompt

C:\>ipv6config

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::20C:85FF:FE3C:35BD
   IPv6 Address.....: 2000::2/64
   Default Gateway.....: 2000::1
   DHCPv6 Client DUID.....: 00-01-00-01-DA-A3-A9-9E-00-0C-85-3C-35-BD

C:\>tracert 2001::2

Tracing route to 2001::2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      2000::1
  2    10 ms     12 ms     14 ms     2020::1
  3    11 ms     14 ms     11 ms     2001::2

Trace complete.

C:\>ping -n 1 2001::2

Pinging 2001::2 with 32 bytes of data:

Reply from 2001::2: bytes=32 time=20ms TTL=126

Ping statistics for 2001::2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 20ms, Average = 20ms
```

Figure 59 : Test de la méthode du tunneling

IV.4.3 La Translation :

Cette partie explique comment implémenter la NAT-PT statique qui illustre un exemple de configuration où les nœuds du réseau IPv4 communiquent avec les nœuds du réseau IPv6 par utilisation d'une table de translation au niveau du routeur NAT-PT entre les adresses IPv6 et adresses IPv4.

IV4.3.1 La topologie utilisée et les configurations des équipements :

Le schéma suivant illustre la topologie que nous avons mis en place pour l'implémentation de cette technique :

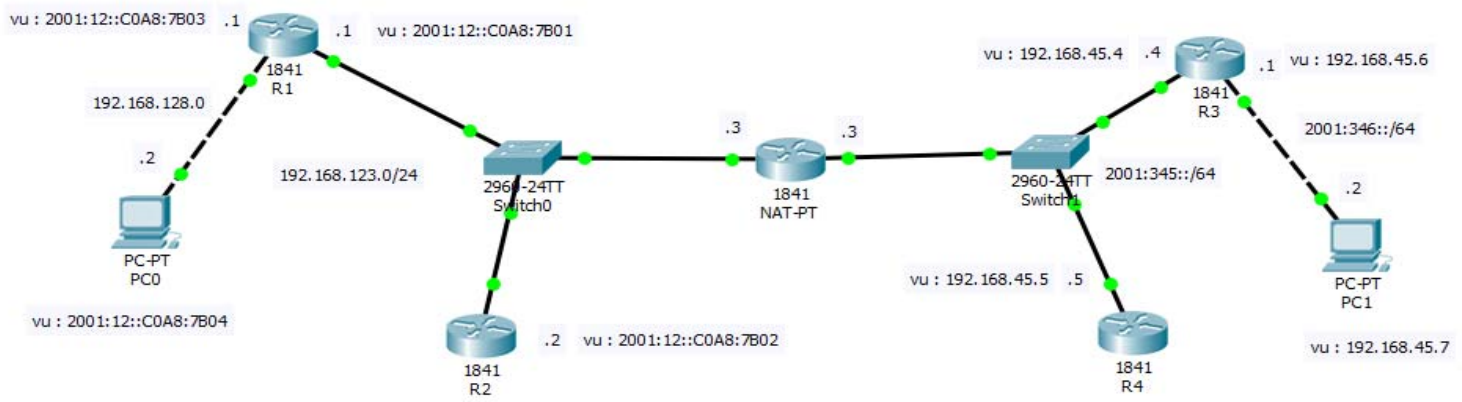


Figure 60 : Topologie utilisée pour la méthode translation

La configuration des équipements de se réseau et comme suite :

- **Le routeur R1**

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.123.1 255.255.255.0
R1(config-if)#no shutdown
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 192.168.128.1 255.255.255.0
R1(config-if)#no shutdown
R1(config)#ip route 192.168.123.0 255.255.255.0 192.168.123.3 90
R1(config)#ip route 192.168.45.0 255.255.255.0 FastEthernet0/0
```

- **Le routeur R2**

```
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 192.168.123.2 255.255.255.0
R2(config-if)#no shutdown
```

Route par défaut pour renvoyer vers les réseaux extérieurs.

R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.123.3

- **Le routeur R3**

Router>en

Router#conf t

Router(config)#hostname R3

R3(config)#ipv6 unicast-routing

R3(config)#interface FastEthernet0/0

R3(config-if)#ipv6 address 2001:345::4/64

R3(config-if)#no shutdown

R3(config)#interface FastEthernet0/1

R3(config-if)#ipv6 address 2001:346::1/64

R3(config-if)#no shutdown

R3(config)#ipv6 route 2001:346::/64 FastEthernet0/1 2001:346::2

R3(config)#ipv6 route ::/0 2001:345::3

- **Le routeur R4**

Router>en

Router#conf t

Router(config)#hostname R4

R4(config)#interface FastEthernet0/0

R4(config-if)#ipv6 address 2001:345::5/64

R4(config-if)#no shutdown

R4(config)#ipv6 route ::/0 2001:345::3

- **Le routeur NAT-PT**

Router>en

Router#conf t

Router(config)#hostname NATPT

Activer le routage IPv6.

NATPT(config)#ipv6 unicast-routing

NATPT(config)#interface FastEthernet0/0

NATPT(config-if)#ip address 192.168.123.3 255.255.255.0

On doit mettre obligatoirement ipv6 nat (Mise en route NAT-PT) sur les interfaces.

NATPT(config)#ipv6 nat

NATPT(config)#no shutdown

NATPT(config-if)#interface FastEthernet0/1

NATPT(config-if)#ipv6 address 2001:345::3/64

NATPT(config-if)#ipv6 nat

NATPT(config)#no shutdown

NATPT(config)#router rip

NATPT(config-if)#network 192.168.123.0

NATPT(config)#ip route 192.168.128.0 255.255.255.0 192.168.123.1 90

On spécifie que si une adresse destination correspond au préfixe ci-dessous, on fait la translation.

NATPT(config)#ipv6 nat prefix 2001:12::/96

Il est ensuite nécessaire de définir une entrée statique dans la table de translation afin de pouvoir correspondre les adresses IPv4 vers IPv6 en utilisant la commande **ipv6 nat v4v6**.

NATPT(config)#ipv6 nat v4v6 source 192.168.123.1 2001:12::C0A8:7B01

NATPT(config)#ipv6 nat v4v6 source 192.168.123.2 2001:12::C0A8:7B02

NATPT(config)#ipv6 nat v4v6 source 192.168.128.1 2001:12::C0A8:7B03

NATPT(config)#ipv6 nat v4v6 source 192.168.128.2 2001:12::C0A8:7B04

Définir une entrée statique dans la table de translation afin de pouvoir correspondance les adresse IPv6 vers IPv4 en utilisant la commande **ipv6 nat v6v4 source**.

NATPT(config)#ipv6 nat v6v4 source 2001:345::4 192.168.45.4

NATPT(config)#ipv6 nat v6v4 source 2001:345::5 192.168.45.5

NATPT(config)#ipv6 nat v6v4 source 2001:346::1 192.168.45.6

NATPT(config)#ipv6 nat v6v4 source 2001:346::2 192.168.45.7

NATPT(config)#ipv6 route ::/0 2001:345::4

- **Le PC 1 :** 192.168.128.2 comme adresse IPv4. La passerelle par défaut : 192.168.128.1 .
- **Le PC2 :** 2001:346::2 comme adresse IPv6. La passerelle par défaut : 2001:346::1 .

IV4.3.2 Vérification de connectivite :

Les deux figures suivantes illustrent la vérification de connectivité entre un hôte IPv6 et un hôte IPv4. Dans la premiere figure nous avons testé la connective du PC0 vers PC1 avec la commande ping sur Command Prompt on utilisant l'adresse 192.168.45.7 attribuée à l'hôte 2001:346::2.

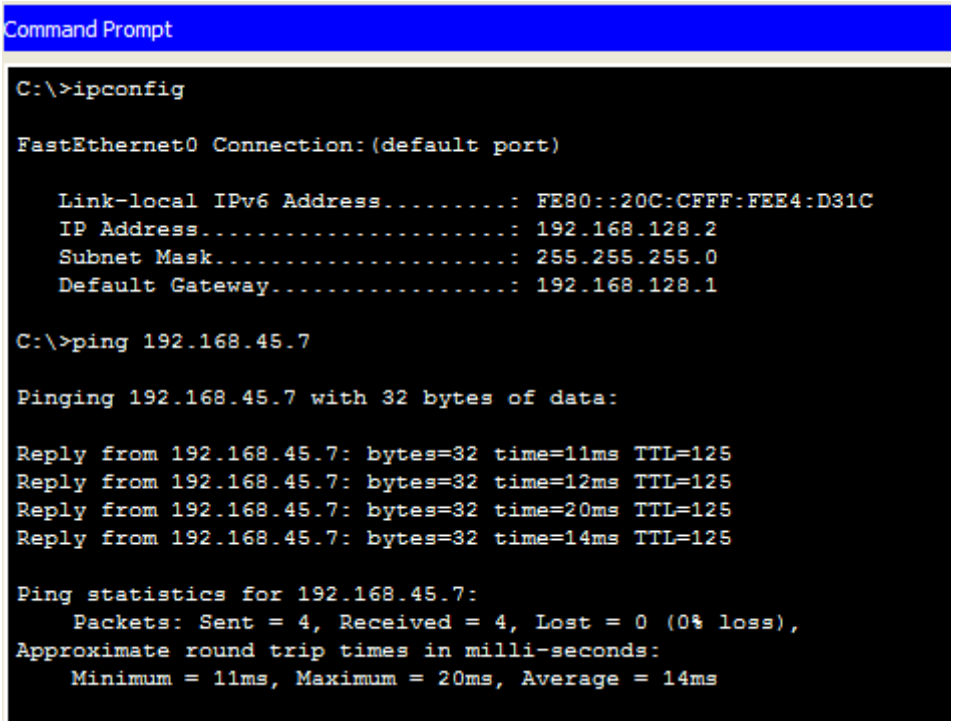


Figure 61 : Connexion d'IPv4 vers IPv6

Cette deuxième figure le Ping et établie du PC1 vers PC0 avec l'adresse 2001:12::C0A8:7B04 attribuée à l'hôte 192.168.128.2.

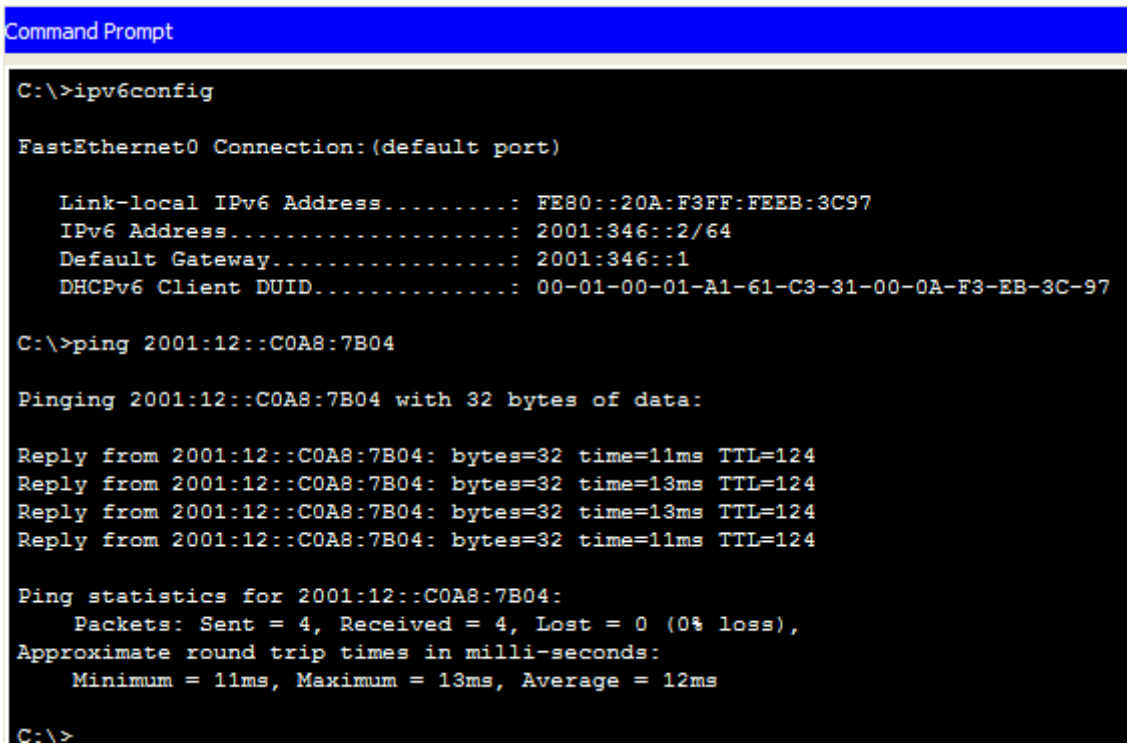


Figure 62: Connexion D'IPv6 vers IPv4

IV.5 Discussion :

Au terme de ce chapitre, les résultats obtenus dans les tests de connectivité sont bons. Ils nous ont montré que les méthodes de transition d'IPv4 vers IPv6 mises par IETF sont supportées par les nouvelles versions des routeurs Cisco. Chaque méthode de transition est utilisée dans un cas bien précis. Dans cette simulation nous avons implémenté sur Packet Tracer trois méthodes de transition pour trois cas de scénarios. Le premier scénario, la communication entre hôtes en deux versions du protocole internet on utilise la méthode de la double pile. Ensuite, le deuxième scénario communiqué 2 réseaux IPv6 isolés par un réseau IPv4 c'est la méthode de tunneling qui est utilisée. Enfin le dernier scénario, établir la connexion entre hôtes IPv4 et IPv6 et vice versa par la méthode de translation.

.

Conclusion

Conclusion

Avec l'évolution d'internet le protocole IPv6 devient une nécessité. La phase de test est aujourd'hui dépassée et il faudra passer à l'étude et à la mise en œuvre de ce protocole. Avec IPv6, les adresses sont codées sur 128 bits, ce qui permet de s'affranchir de toutes les contraintes liées à la pénurie d'adresses, et ce même à long terme. De nouveaux mécanismes de transition IPv4 vers IPv6 ont été également développés. Les mécanismes d'auto-configuration permettent à une nouvelle machine d'intégrer facilement le réseau en déterminant automatiquement les paramètres à appliquer. Implémentation d'un mécanisme de découverte du MTU optimal. La fragmentation n'est plus réalisée dans le réseau mais par le nœud source. En-tête simplifié autorisant un routage plus efficace.

.

Le présent projet nous a permis d'étudier les différentes méthodes de transition IPv4/IPv6, à savoir : la double pile, le tunneling et la translation, ainsi que des scénarios de déploiement et surtout la mise en œuvre de ses méthodes par simulation sur Packet Tracer. Ce projet a également été, une initiation à la conception et l'administration d'un réseau IPv6.

Bibliographie

Bibliographie

Ouvrages

[1] Claude Servin, «Réseaux et télécoms», 2003, Editeur Dunod, p54-55, p162-168

[2] Danièle D, Dominique S, «Architecture des réseaux», 2009, Editeur Pearson Education France, p2-3

[3] Andrew T, David W, «Réseaux», 5e édition, 2011, Editeur Pearson Education France, p23

[4] Jean-François P, Fabrice L, «Tout sur les Réseaux et internet», 2015, 4éme édition, Editeur Dunod, p78-80

[5] Innokenty Rudenko, «Configuration IP des routeurs Cisco»,2001, Editeur Eyrolles, p22-29

[6] Stéphane L, Dominique P, «Réseaux et transmissions, protocoles, infrastructures et services », 2016, 6éme éditions, Editeur Dunod, p143-161.

Cours

[7] Ahmed Mehaoua, «Réseaux & Sécurité», 2006-2007, Université Lille1, p9.

[8] Claude Duvallet, «Les réseaux informatiques», Université Havre, p11-12

[9] Rziza Mohammed, «Cours des réseaux Informatiques», 2010-2011, Université de ouargla

[10] Cour Cisco CCNA 1, Chapitre 8, «Adressage IP»

Publications

[11] El Khadiri K, El Kamoun N, Hilal R, «Etude comparative des mécanismes de transition de l'IPv4 à l'IPv6», 2017, université chouaib doukkali, maroc, p2

[12] Simon Dunand, «Publication de services web IPv4 sur Internet IPv6», 2012, Haute école spécialisé de suisse occidentale

Sites web

[13] «architecture d'un réseau informatique», http://sitelyceejdarc.org/autodoc/cours/010%201S/Sciences%20de%20l%20ingenieur/Reseaux/001%20Presentation.pdf

[14] «Stratégie de migration IPV4 vers IPV6 », http://www.academia.edu/20061600/Strat%C3%A9gie_de_migration_IPV4_vers_IPV6

[15] http://metier-formation.blogspot.com/2011/12/metier-formation-tsri.html

[16] «Les réseaux de zéro», https://openclassrooms.com/courses/1561696-les-reseaux-de-zero/3199418-construire-un-reseau-le-materiel

[17] P Eugé, «Les réseaux informatique», http://www4.ac-nancy-metz.fr/lyc-vuillaume-mirecourt/pages/Pedagogie/DATA/Technique/Informatique/les%20reseaux/Les%20Reseaux.pdf

[18] «Les couches du modèle OSI», https://www.astuces-pratiques.fr/informatique/les-couches-du-modele-osi

[19] «Introduction à Tcp/Ip», http://docplayer.fr/5141053-Tcp-ip-1-introduction-a-tcp-ip-1-1-introduction-1-2-vue-d-ensemble.html

[20] «TCP/IP», https://www.commentcamarche.com/contents/539-tcp-ip

[21] «Réseaux informatiques, modèle osi et protocole tcp/ip», https://fr.scribd.com/document/309697340/Rsx-OSI-TCPIP-cours

[22] «Adresse IP», https://fr.wikipedia.org/wiki/Adresse_IP

[23] «Les limites du protocole IPv4», http://touchardinforeseau.servehttp.com/ccna2014/course/module6/6.1.4.1/6.1.4.1.html

[24] «protocole de transiton ipv6 : 6to4» http://ccie.julienberton.fr/2011/10/04/protocoles-de-transition-ipv6-6to4/

[25] Pascal A, Bruno S, Pierre-Ugo T**,** Joë**l** G, Séquence 4, «L'intégration d'IPv6 dans l'Internet», https://www.fun-mooc.fr/c4x/MinesTelecom/04012/asset/sequence-4-vfinal.pdf, p 28

[26] «réseau», http://pageperso.lif.univ-mrs.fr/~emmanuel.godard/ens/reseaux/05_reseauIPv6.cours.pdf

Résumé

Ce travail traite des méthodes de transition de l'IPv4 à l'IPv6 qui est étudié pour faciliter le déploiement de l'IPv6. IPv4 et IPv6 sont deux protocoles incompatibles. En outre l'infrastructure réseau actuelle et la majorité des services internet sont disponibles sur IPv4, et par conséquent, il est impossible d'émigrer de l'IPv4 à l'IPv6 en un jour. IPv4 et IPv6 doivent coexister pendant une longue période et le déploiement de l'IPv6 ne peut se faire que progressivement. Plusieurs mécanismes de transition ont été développés et peuvent être utilisés pour cette raison. Dans ce travail nous allons présenter une étude des mécanismes de transition de l'IPv4 à l'IPv6 que nous avons classé en 3 catégories : Double pile, Tunneling, Translation. Pour chacune d'entre elles nous allons décrire les mécanismes concernés et leurs principes, pour pouvoir choisir le mécanisme de transition le plus convenable en fonction des exigences et des besoins particuliers des utilisateurs.

Mots clés : IPv4, IPv6, Mécanismes de transition, Double pile, Tunneling, Translation, Simulation.