Ministère de l'Enseignement Supérieur de la Recherche et de l'Innovation

Université Assane Seck de Ziguinchor
UFR Sciences et Technologies
Département Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master
Mention : Informatique ; Spécialité : Génie Logiciel

Sujet :

Migration du réseau de l'Université Assane SECK de Ziguinchor (UASZ) vers IPv6

Présenté par : M. Diadia William MANGA

Soutenance le 29/06/2020

Sous la direction de : Dr Youssou FAYE

Sous la supervision du : Pr. Salomon SAMBOU

Membres du jury

Salomon SAMBOU	Professeur	Président	UASZ
Youssou FAYE	Maître de Conférence Titulaire	Encadreur	UASZ
Maruis DASYLVA	Enseignent chercheur	Rapporteur	UASZ
Abel DIATTA	Maître de Conférence	Rapporteur	UASZ

Année Universitaire 2019-2020

Dédicace

Toutes les lettres ne sauraient trouver les mots qu'il faut…

Tous les mots ne sauraient exprimer la gratitude, l'amour, le respect, la reconnaissance…

Aussi, c'est tout simplement que

Je dédie ce travail :

*À mes **chers parents (Marcel MANGA et Aminata SAGNA**, mes tuteurs à Ziguinchor **(feu Adolph BASSÈNE** et **Anne Marie BASSÈNE**), à Kamobeul (**Prospère BASSÈNE** et sa femme **Yacine TENDENG**) et à Bambey (**Denis BASSÈNE** et sa femme **Thérèse Aimé FAYE**).*

*À mes chers et adorables frères et sœur, mes neveux et nièces, mes cousin(e)s, mes tantes et oncles, les familles **MANGA**, **SAGNA**, **BASSÈNE**, **TENDENG**, **SENGHOR** …, pour tous vos encouragements, que ce travail soit le témoignage sincère et affectueux de ma profonde reconnaissance, pour tout ce que vous avez fait pour moi.*

En témoignage de mon affection fraternelle, de ma profonde tendresse et reconnaissance, je vous souhaite une vie pleine de bonheur et de succès et que Dieu, le tout puissant, vous protège et vous garde.

*À la mémoire de mon promotionnaire **Mamadou Petit COULIBALY**,*

*À la mémoire de mon ami, frère et promotionnaire, au niveau du premier au Secondaire cycle, **Eba Aka Silombohé Tendeng***

J'avais voulu que vous soyez aujourd'hui là pour encore partager ce moment avec vous mais le tout puissant en a décidé autrement. Que Dieu le tout Puissant et miséricordieux vous accueille dans sa maison céleste.

À mes amis de toujours : José TENDENG, Antoine SAGNA, Julien DIATTA, Kenbougoul DIEDHIOU, Évariste DIATTA, Baudouin BASSENE, Ives Paterne SAGNA, Alain DIEDHIOU, Paul BADIANE…

En souvenir de notre sincère et profonde amitié et des moments agréables que nous avons passés ensemble.

Veuillez trouver dans ce travail l'expression de mon respect le plus profond et mon affection la plus sincère.

À Toutes les personnes qui ont participé à l'élaboration de Ce travail ;

À tous ceux que j'ai omis de citer;

À tous mes camarades de promotion ;

À tous mes enseignants depuis mes premières années d'études jusqu'aujourd'hui ;

À tous ceux qui me sont chers et que j'ai omis de cite.

Remerciements

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma reconnaissance.

Tout d'abord, je tiens à remercier le bon Dieu tout Puissant de m'avoir donné la force et le courage de mener à bien ce modeste travail.

Mes plus chaleureux remerciements à mon encadreur : ***Docteur Youssou FAYE****, Docteur à l'Université Assane SECK de Ziguinchor et Chef du département informatique, d'avoir partagé avec moi ses brillantes intuitions.*

Vous n'avez managé aucun effort à mon égard malgré votre calendrier chargé. Je vous témoigne toute ma gratitude et ma reconnaissance pour m'avoir fait l'honneur de m'encadrer. C'est avec vous que j'ai renforcé ma personnalité dans le sens de la rigueur, la précision, la patience, … dans le travail. Vraiment merci pour ta grande disponibilité, pour vos précieux conseils qui m'ont motivé face à certaines difficultés rencontrées. Votre ouverture d'esprit, de connaissances m'ont été d'une très grande utilité. J'espère seulement que ça continuera dans le futur. Je vous en suis infiniment reconnaissant pour tout.

Je ne terminerai sans remercier les membres de mon jury :

Monsieur Salamon SAMBOU, Professeur à l'université Assane SECk de Ziguinchor pour le temps qu'il a bien voulu consacrer à l'appréciation de ce travail mais aussi de n'avoir honoré en présidant le jury de ma soutenance.

Madame Mendy (Maruis DASILVA), Enseignant chercheur à l'université Assane SECK de Ziguinchor, pour son ouverture mais aussi pour m'avoir fait l'honneur d'être rapporteur du jury de ma soutenance.

Monsieur Abel DIATTA, Docteur à l'université Assane SECk de Ziguinchor pour l'honneur qu'il m'a fait en acceptant de faire partir du jury de ma soutenance en rapporteur.

Je remercie vivement à tous les camarades de promotion, pour tous les beaux moments passés ensemble.

Je voudrais exprimer ma reconnaissance envers les professeurs du département informatique qui m'ont apporté leur support moral et intellectuel tout au long de ce sprint.

*À mes **chers parents (Marcel MANGA et Aminata SAGNA**, mes tuteurs à Ziguinchor **(feu Adolph BASSÈNE** et **Anne Marie BASSÈNE)** et à Kamobeul (**Prospère BASSÈNE** et sa femme **Yacine TENDENG**).*

Aucun remerciement ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être.

Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours.

Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez.

Puisse Dieu, le Très Haut, vous accorde santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

J'exprime toute ma gratitude à toute l'équipe de CRI qui nous a permis d'avoir une idée sur l'architecture du réseau de l'UASZ facilitant ainsi la partie pratique de mon mémoire.

Afin de n'oublier personne, mes vifs remerciements s'adressent à tous ceux qui m'ont aidé à la réalisation de ce modeste mémoire.

Résumé

Actuellement, le protocole de traitement de la couche réseau est IPv4, pour *Internet Protocol* version 4. Plus de quarante ans sont passés et un certain nombre de limitations sont apparues. Tout d'abord, le nombre d'adresses IPv4 disponibles est limité à 4 294 967 296, soit 2^{32} Cette restriction, lors de la création du protocole, semblait ne pouvoir jamais être atteinte. Ainsi, en 1992, après l'ouverture commerciale d'Internet, il fallut, une année plus tard, déclencher un plan d'urgence, puisqu'il ne restait plus aucune adresse de classe B disponible. Ces mesures se concrétisèrent en deux points : ***la création de la notation CIDR*** et la mise en place d'un plan ***d'adressage privé et du NAT*** (traduction d'adresse réseau). Ces mesures palliatives engendrent à leur tour des contraintes et de nouveaux problèmes tels que le ***manque de connectivité de bout en bout.***

Comme La politique informatique de l'Université Assane Seck s'inscrit dans une dynamique d'innovations perpétuelles, nous avons jugé nécessaire d'anticiper sur le basculement vers IPV6. C'est dans ce dynamisme que s'inscrit mon mémoire intitulé : ***la migration du réseau de l'université Assane SECK de Ziguinchor vers IPv6***. Après une étude technique suivie d'une analyse pertinente des besoins, nous avons jugé plus opportun de mettre en place le Dual Stack mieux adaptée pour les environnements similaires. Une implémentation sur Packet Tracer, suivie de tests partiellement sur des équipements réels Cisco nous a permis de pouvoir nous en assurer d'un probable éventuel déploiement réel sur le réseau de l'UASZ sans difficultés.

Sommaire

Table de matière

Liste des Figures

Liste des Tableaux

Glossaire

***IP**: Internet Protocol*

***IPv4**: Internet Protocol version 4*

***IPv6**: Internet Protocol version 6*

***CIDR**: Classless Inter-Domain Routing*

***VLSM**: Variable Length Subnetwork Mask*

***NAT**: Network Address Translation*

***FAI**: Fournisseurs d'Accès à Internet*

ISP: Internet Service Provider

***RIP**: Routing Information Protocol*

***IGRP**: Interior Gateway Routing Protocol*

***OSPF**: open Shortest Path First*

***EIGRP:** Enhanced Interior Gateway Routing Protocol*

***RFC**: Request for Comment*

***IANA**: Internet Assigned Numbers Authority*

***PDA**: Personal Digital Assistant*

***IPng**: Internet Protocol New Generation*

***ID**: Identificateur*

***MAC**: Mediam Access Control*

***EUI-64**: Extended Unique Identifier*

***ICANN**: Internet Cooporation for Assigned Name and Numbers*

***LIR**: Local Internet Registry*

***GPRS**: General Packet Radio Service*

***WLAN**: Wireless Local Area Network*

***DHCP**: Dynamic Host Configuration Protocol*

***DNS**: Domain Name Server*

***DHCPv4**: Dynamic Host Configuration Protocol version 4*

***DHCPv6**: Dynamic Host Configuration Protocol version 6*

***SLAAC**: State less Address Auto Configuration*

***RA**: Router Advertisement*

***DAD**: Duplicate Address Detection*

***RIPv2**: Routing Information Protocol version 2*

***RIPng**: Routing Information Protocol new generation*

***OSPFv2**: open Shortest Path First version 2*

***OSPFv3**: open Shortest Path First version 3*

***IS-IS**: Intermediate System to Intermediate System*

***BGP**: Border Gateway*

***UDP**: User Datagram Protocol*

***AS**: Autonomous System*

***CPU**: Central Processing Unit*

***ISATAP**: Intra-site Automatic Tunnel Addressing Protocol*

***LAN**: Local Area Network*

***NAT- PT**: Network Address Translation-Protocol Translation*

***DNS-ALG**: Domain Name Server- Application Level Gateway*

Introduction Générale

Cela devait arriver un jour, et ce fut le 31 janvier 2012. Mais que s'est-il passé ? [1]Aucune catastrophe annoncée par le calendrier maya, mais un événement prédit il y a une dizaine d'années, et qui était inévitable : l'allocation par l'Internet Assigned Numbers Authority (IANA) des derniers espaces d'adressage public IPv4 disponibles. Cet événement fut annoncé publiquement lors de la conférence de presse, donnée le 3 février 2012. Même s'il reste un stock d'adresses disponibles à chaque Regional Internet Registery (RIR), cela ne durera qu'un temps, comme on peut le voir dans la Figure 1. C'est pourquoi il est l'heure de passer à l'IPv6 !

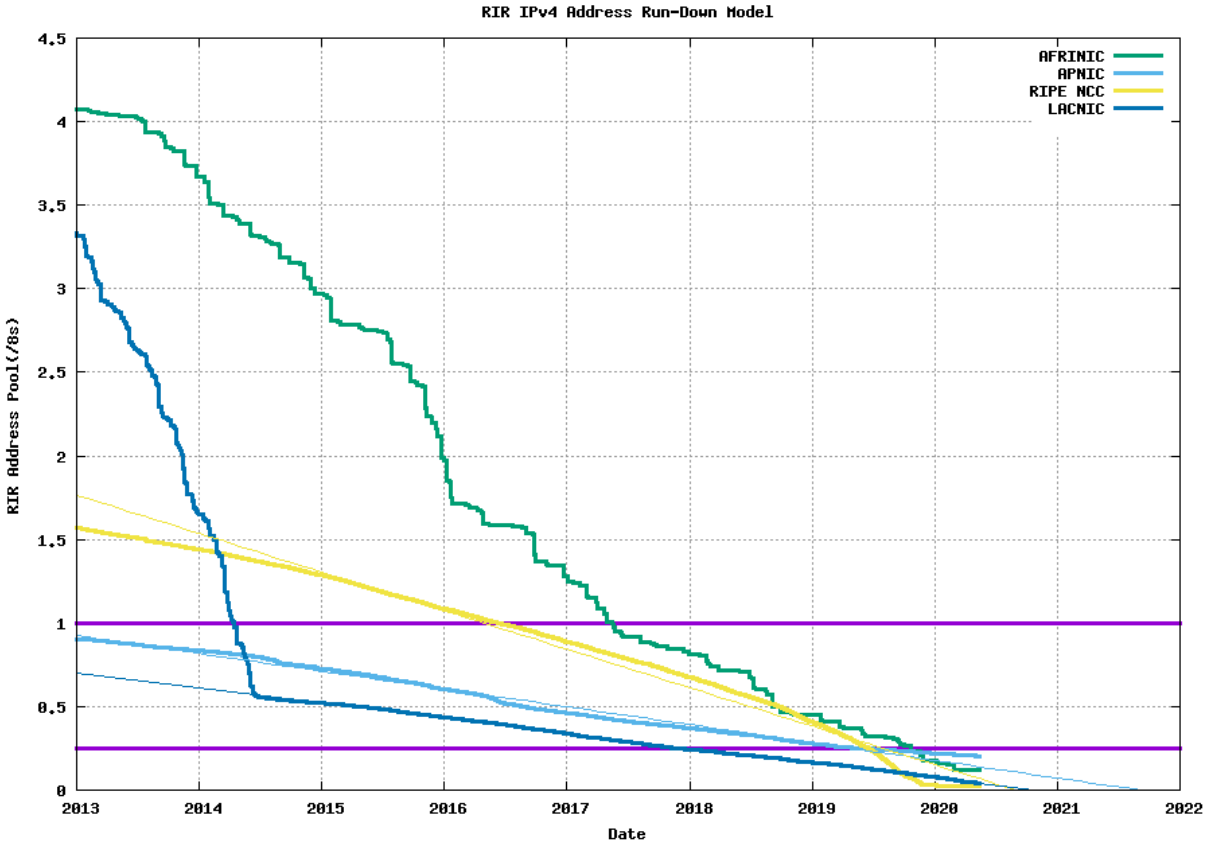


Figure 1: projection de la consommation d'adresse IPv4 restantes chez les différents RIR

Source : https://www.potaroo.net/tools/ipv4/

Avec le développement technologique, un nombre croissant de personnes, d'entreprises et aussi d'objets se connectant sur l'internet afin d'envoyer, recevoir ou consulter des informations sur

cette toile augmente exponentiellement. Ce nombre augmentera de 40 % par an au cours de la prochaine décennie et produira chaque année environ 44 zettaoctets[1].

Pour permettre à tout ce beau monde d'être connecté, chaque appareil a besoin d'une adresse IPv4 qui est en fait un numéro d'identification attribué de façon permanente ou provisoire à une interface de chaque périphérique qui se connecte à internet. Quand on sait que dans le monde chaque personne, entreprise, organisation, entité étatique, etc., dispose de plus d'un appareil qui se connecte à internet, l'on peut se faire une idée de la quantité d'adresses IPv4 utilisées au quotidien. Et ces adresses qui doivent être attribuées étaient reparties en trois classes. Chaque classe dispose d'un pool d'adresses figé. Ce fait occasionne un fort :

- gaspillage des adresses car certaines entreprises ont utilisé des adresses où il s'utilise qu'environ les 1/3 du pool conduisant ainsi à une perte énorme d'adresses.

Cette manière d'adresser une interface est appelée adressage par classe du fait de l'utilisation des classes d'adresses. Elle a aussi entrainé :

- La croissance des tailles des tables de routages, qui permettent de savoir par où les paquets d'information doivent être acheminés en fonction de leur adresse au fur et à mesure que les plages d'adresses sont attribuées.

Face à ce besoin, à la fin 1992, alors que le protocole IP version 4 a plus de 10 ans, P. Gross et P. Almquist, de l'*Internet Engineering Steering Group* publient un document, la ***RFC 1380*** intitulé « *IESG Deliberations on Routing and Addressing* » (Délibérations le l'IESG concernant le routage et l'adressage). Ils constatent que les adresses IPv4 vont rapidement manquer étant donné que le nombre de plages d'adresses attribuées double chaque année.

Devant l'élargissement vertigineux des objets à attribuer une adresse IPv4, des méthodes, telles que le CIDR, VLSM, le NAT et les adresse privées, ont été mises en place pour atténuer la pénurie d'adresses IPv4 et l'explosion des tables de routage. Mais ces méthodes ont à leur tour engendré des problèmes qui ont favorisés la création d'un nouveau protocole qui pourra corriger ces problèmes.

[1] Le zettaoctet est un multiple de l'octet unitaire pour les informations numériques. Le préfixe zetta indique la multiplication par la septième puissance de 1000 ou 10^{21} dans le Système international d'unités. Un zettaoctet est un sextillion d'octets. Le symbole d'unité est ZB.

Ces problèmes sont entre autres :

- Le manque de connectivité de bout en bout dû à la technologie de traduction d'adresses réseaux (NAT) qui est généralement implémentée dans les réseaux IPv4. Cette technologie permet à plusieurs périphériques de partager une adresse IP publique unique.

Pour y remédier, le projet IP *new generation (IPng) ou IPv6* est lancé. Il s'agit de définir une nouvelle version du protocole IP, norme de communication sur Internet. Il est également prévu d'améliorer la sécurité du protocole, et de permettre la transmission de nouvelles formes de flux d'informations.

IPng ou IPv6 est la dernière version du protocole IP. IPv6 a été développé pour pallier à de nombreuses déficiences d'IPv4, notamment le problème de l'épuisement des adresses. Contrairement à IPv4, qui ne dispose que d'environ 4,3 milliards d'adresses disponibles (2 mise à la puissance 32), IPv6 permet d'avoir 3,4 × 10 à la puissance 38 adresses. En plus de la suppression des certains aspect de IPv4 tels le NAT et ARP et l'amélioration d'autres, IPng a d'autres aspects. Il s'agit entre autre de :

- Types d'adresses
  - Unicast
  - Multicast
  - Anycast
- Pour l'adressage
  - State Less Address Auto Configuration (SLAAC)
  - DHCPv6 sans état
  - ***Processus EUI-64*** ou de ***manière aléatoire***
  - …

Le déploiement d'IPv6 se fait donc lentement, alors que l'on continue à utiliser IPv4 sur de nombreux systèmes qui ne supportent pas encore la nouvelle version. Et pour une cohabitation des deux protocoles en attendant le déploiement total d'IPng, les gens ont mis en place des mécanismes qui permettent aux deux mondes de coexister ensemble : ***c'est la transition***.

Pour ne pas, être en retard lorsque le déploiement total sera au rendez-vous, l'université Assane SECK de Ziguinchor comme toute autre entreprise, anticipe en essayant de voir quel mécanisme de transition est plus adéquat à son réseau. Et en parlant de mécanismes nous avons :

- ***Technique de la double pile ou Dual Stack,***
- ***Technique du tunnel,***
- ***Technique de translation.***

C'est dans ce contexte qu'est orienté ce mémoire intitulé : ***la migration du réseau de l'université Assane SECK de Ziguinchor vers IPv6***.

Ainsi pour mieux exposer cette étude, nous organisons ce travail en cinq chapitres.

D'abord dans le premier chapitre nous présentons les Limites de IPv4. Ensuite au second chapitre, il est question de présenter le nouveau protocole internet : Ipv6 ou IPng. Puis le troisième chapitre est consacré au routage et adressage dans IPv6. En quatrième, les mécanismes de transition dans l'avant-dernier chapitre. Et enfin au cinquième chapitre il est question du choix du mécanisme et sa mise en œuvre. Et le tout sera clôturé par une conclusion générale et des perspectives.

chapitre I) IPv4, une P lage asséchée

Introduction

Aujourd'hui, il y a plus de 15 milliards d'appareils connectés à Internet, ce qui est possible grâce notamment aux box qui économisent les adresses IPv4, en donnant la même adresse à tous les appareils connectés du foyer. Or, selon le géant américain des réseaux informatiques Cisco, il y aura en 2020 de l'ordre de 50 milliards d'appareils (téléphones, montres, voitures, etc.) connectés à Internet. Ces derniers ont besoin d'une adresse IP qui les permettra de mettre en œuvre la transmission de données entre des hôtes situées sur un même réseau ou sur des réseaux différents.

Face à ce développement exponentiel, de nombreuses techniques d'adressage ont été utilisé pour essayer de satisfaire chaque machine désirant se connecter à l'internet. Ce sont entre autres :

- Adressage par classe
- Adressage sans classe (CIDR et VLSM)
- NAT

Mais ces techniques ont rencontré des limites que nous tentons étudier dans ce chapitre.

I) L'adressage par classes (obsolète)

Il y a fort longtemps, dans l'informatique, l'adressage IPv4 se faisait par classes. En gros, pour chaque adresse IPv4, un masque de sous-réseau était assigné par défaut en fonction de sa classe. Cela ne se fait plus depuis bien des années, néanmoins, il peut être intéressant de voir ce que c'était pour mieux comprendre certaines notions. Nous allons donc voir quelque chose d'obsolète.

I.1) Adresse IPv4

Une adresse IP est une adresse utilisée afin d'identifier seulement un périphérique sur un réseau IP. L'adresse IPv4 se compose de 32 bits, qui peuvent être divisibles dans une partie réseau (***NET ID***) et une partie hôte (***HOST ID***) avec l'aide d'un masque de sous-réseau.

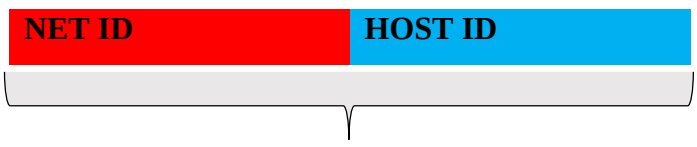


Figure 2:Structure d'une adresse IPv4

Les 32 bits sont répartis en quatre octets (1 octet = 8 bits). Chaque octet est converti au format décimal et séparé par un point. Pour cette raison, il est dit qu'une adresse IPv4 est exprimée au format décimal avec points (par exemple, 172.16.81.100). La valeur de chaque octet s'étend de 0 à 255 en décimale, ou 00000000 - 11111111 en binaire.

Voici comment les octets sont convertis au format décimal : La droite la plupart de bit, ou bit le moins significatif, d'un octet tient une valeur de 2^0. Le bit juste à la gauche de celui tient une valeur de 2^1. Ceci continue jusqu'au bit extrême gauche, ou au bit le plus significatif, qui tient une valeur de 2^7.

Ainsi, si tous les bits de l'octet en binaire sont égaux à 1, l'équivalent décimal serait 255 comme indiqué ci-dessous :

1 1 1 1 1 1 1 1

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0 (128+64+32+16+8+4+2+1=255)

Voici un exemple de conversion d'octets lorsque les bits ne sont pas tous égaux à 1.

0 1 0 0 0 0 0 1

0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65).

Et cet échantillon affiche une adresse IP représentée en binaire et en décimale.

10 . 1 . 23 . 19 (décimal)

00001010 . 00000001 . 00010111 . 00010011 (binaire)

Ces octets sont décomposés pour fournir un modèle d'adressage qui peut s'ajuster aux grands et petits réseaux. Il existe cinq différentes classes de réseaux, de A à E, mais nous nous concentrons sur les classes de A à C, puisque les classes D et E sont réservées.

Remarque

Il existe trois sortes d'adresse comprises dans la plage d'adresses de chaque réseau IPv4 :

I.1.a) Adresse réseau

L'adresse réseau est généralement utilisée pour faire référence à un réseau. Le masque de sous-réseau ou la longueur du préfixe peuvent aussi être utilisés pour décrire une adresse réseau. Par exemple, le réseau peut être appelé le réseau 10.1.1.0, le réseau 10.1.1.0

255.255.255.0 ou le réseau 10.1.1.0/24. Tous les hôtes du réseau 10.1.1.0/24 auront la même partie réseau.

Dans la plage d'adresses IPv4 d'un réseau, ***la première adresse est réservée à l'adresse réseau.*** La partie hôte de cette adresse comprend uniquement des 0. Tous les hôtes du réseau partagent la même adresse réseau.

I.1.b) Adresses d'hôte

Chaque périphérique final nécessite une adresse unique pour communiquer sur le réseau. Avec les adresses IPv4, les valeurs comprises entre l'adresse réseau et l'adresse de diffusion peuvent être attribuées aux périphériques finaux d'un réseau. La partie hôte de cette adresse est composée de n'importe quelle combinaison de bits 0 et 1, mais ***ne peut pas contenir uniquement des bits 0 ou 1***.

I.1.c) Adresse de diffusion

L'adresse de diffusion IPv4 est une adresse spécifique, attribuée à chaque réseau. Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau. Pour envoyer les données à tous les hôtes d'un réseau en une seule fois, un hôte peut envoyer un paquet adressé à l'adresse de diffusion du réseau : chaque hôte du réseau qui recevra ce paquet en traitera le contenu.
L'adresse de diffusion correspond à la plus grande adresse de la plage d'adresses d'un réseau. Il s'agit de l'adresse dans laquelle les ***bits de la partie hôte sont tous des « 1 ».*** Un octet au format binaire ne comportant que des 1 correspond au nombre 255 en notation décimale. Par conséquent, pour le réseau 10.1.1.0/24, dans lequel le dernier octet est utilisé pour la partie hôte, l'adresse de diffusion serait 10.1.1.255. Notez que la partie hôte n'est pas toujours un octet entier. Cette adresse est également désignée sous le nom de diffusion dirigée.

I.2) Classes d'adresse

La notion de classe est obsolète [1] depuis le milieu des années 1990. Les assignations d'adresses du protocole IPv4 (et de son successeur IPv6) ne tiennent plus compte de la classe d'adresse et les protocoles de routage modernes indiquent explicitement le masque réseau de chaque préfixe routé. La classe d'adresse permet d'adapter l'adressage selon la taille du réseau c'est-à-dire selon le besoin en terme d'adresses IP.

Il existe cinq classes d'adresse IP identifiées par les lettres allant de A à E.

I.2.a) Classe A

Une adresse IP de classe A dispose d'un seul octet pour identifier le réseau et de trois octets pour identifier les machines sur ce réseau. Soit XXXX XXXX . XXXX XXXX . XXXX XXXX . XXXX XXXX.

Cette classe peut comporter jusqu'à 2^{24}-2, soit 16 777 214 adresses pour des hosts. *En binaire, une* adresse de classe A commence toujours par la séquence de bits 0.

Exemple :
0 XXX XXXX . XXXX XXXX . XXXXXXXX . XXXX XXXX est une adresse de classe A
1 XXX XXXX . XXXX XXXX . XXXX XXXX . XXXX XXXX n'est pas une adresse de classe A

En décimal, il est donc compris entre 0 et 127 mais certaines valeurs sont réservées à des usages particuliers. Les réseaux disponibles en classe A sont donc les réseaux allant de l'adresse IP 0.0.0.0 à 127.255.255.255 (adresses privées et publiques).

On retrouve dans les adresses de classes A, les grosses entreprises qui ont besoin d'adresser beaucoup de machines comme par exemple Google, les FAI (Neuf, Free dont toutes les adresses commencent par 88, etc.)

NB : L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

I.2.b) Classe B

Une adresse IP de classe B dispose de deux octets pour identifier le réseau et de deux octets pour identifier les machines sur ce réseau. Soit XXXXXXXX . XXXXXXXX . XXXXXXXX . XXXXXXXX

Cette classe peut comporter jusqu'à 2^{16}-2, soit 65 534 adresses machines mais aussi 65 534 réseaux. Le premier octet d'adresse IP d'une classe B commence toujours par la séquence de bits 10 en binaire.

Ex : *10* XX XXXX . XXXXXXXX . XXXX XXXX . XXXX XXXX

En décimal, il est donc compris entre 128 et 191. Les réseaux disponibles en classe B sont donc les réseaux allant de l'adresse IP 128.0.0.0 à 191.255.255.255 (adresses privées et publiques).

Ex : 136.56.0.30 est une adresse de classe B

I.2.c) Classe C

Une adresse IP de classe C dispose de trois octets pour identifier le réseau et d'un seul octet pour identifier les machines sur ce réseau. Soit XXXX XXXX . XXXX XXXX . XXXX XXXX . XXXX XXXX

Cette classe peut comporter jusqu'à 2^8-2, soit 254 adresses machine. Le premier octet d'adresse IP d'une classe C commence toujours par la séquence de bits 110 en binaire.

Ex : *110* XXXXX . XXXXXXXX . XXXXXXXX . XXXX XXXX

En décimal, il est donc compris entre 192 et 223. Les réseaux disponibles en classe C sont donc les réseaux allant de l'adresse IP 192.0.0.0 à 223.255.255.255 (adresses privées et publiques).

I.2.d) Masques de réseau

Un masque de réseau est une adresse IP où tous ***les bits correspondants à la partie NET ID sont mis à 1 et ceux correspondants à le partie machine sont mis à 0***. Il nous aide à identifier la partie de l'adresse qui identifie le réseau et la partie de l'adresse qui identifie les machines. Les réseaux de classe A, B et C ont des masques par défaut, également connus sous le nom de masques naturels, comme indiqué ci-dessous :

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

I.3) Limites de l'adressage par classe

Les besoins de certaines entreprises ou organisations sont couverts par ces trois classes. L'attribution par classe des adresses IP gaspillait souvent de nombreuses adresses [2], ce qui épuisait la disponibilité des adresses IPv4. Par exemple, une entreprise avec un réseau de 260 hôtes devait se voir attribuer une adresse de classe B avec plus de 65 000 adresses.

Bien que ce système par classe ait été abandonné à la fin des années 90, il n'a pas entièrement disparu dans certains des réseaux modernes. Par exemple, lorsque vous attribuez une adresse IPv4 à un ordinateur, le système d'exploitation examine l'adresse en question pour déterminer si elle est de classe A, B ou C. Le système d'exploitation déduit ensuite le préfixe utilisé par cette classe et effectue l'attribution du masque de sous-réseau par défaut. Après l'abandon de l'adressage par classes qu'utilisaient les administrateurs réseaux pour configurer les réseaux : c'était l'adressage sans classe.

II)L'adressage sans classes

Dans les années 90, Internet était en plein développement et la demande d'adresse IPv4 croissait exponentiellement suite à l'afflux des nouveaux utilisateurs d'internet, surtout des entreprises. Les protocoles utilisés alors étaient dits « classfull » [3] (comme RIP v1 et IGRP), c'est-à-dire qu'ils utilisaient les masques par défaut des classes d'adresse utilisées (ex : 255.0.0.0 pour la classe A, 255.255.0.0 pour la classe B et 255.255.255.0 pour la classe C).

Ce système d'attribution des réseaux IP commença à montrer ses limites car la taille des tables de routage se mit à gonfler exponentiellement.

Le gaspillage d'adresse IP était alors conséquent et une pénurie d'adresses de classe B s'annonçait. En effet, en classfull, le nombre de réseaux et le nombre d'hôtes sont fixes, le masque de sous réseau étant lui-même fixe.

Pour résoudre ce problème, on en vint à l'utilisation de protocoles dits « classless » comme RIP v2 et EIGRP. Ces protocoles, contrairement aux protocoles de routages classfull, intègrent le masque de sous réseau dans leurs mises à jour de routage ce qui permet de modifier les masques de sous réseau en fonction des besoins du réseau que l'on adresse, on peut alors au choix faire soit du ***subnetting***, soit du ***surnetting***.

Le VLSM et le CIDR sont deux techniques utilisant les potentialités du routage classless. La technique du VLSM est une évolution de CIDR utilisée en entreprise pour l'adressage d'un réseau ayant une topologie hiérarchique.

II.1) Le CIDR

Dès 1993, il était clair qu'Internet se développait plus vite que prévu. Le système d'adresses IP que nous utilisons (IPv4), est épuisé depuis longtemps. Toutes les adresses possibles (au moins 4 294 967 296) ont déjà été attribuées. Il fallait donc trouver une solution

il y a quelques décennies pour résoudre le problème, ce qui signifiait ***abandonner les classes réseau*** [4]. À l'origine, les adresses IP étaient divisées en cinq classes. Si une entreprise voulait se connecter à Internet, elle devait choisir une adresse IP dans la classe appropriée. Pour chaque classe, différents nombres d'octets (sur les quatre blocs numériques de l'adresse IP) ont été utilisés pour identifier les réseaux. Les octets restants déterminent le nombre d'hôtes dans un réseau.

Par exemple, un réseau de classe A pouvait accueillir plus de 16 millions d'hôtes, mais seulement 128 (0-127) de ces réseaux étaient disponibles. En classe B, par contre, un peu plus de 16 000 réseaux étaient possibles, mais chaque réseau pouvait contenir 65 534 hôtes. Les réseaux de classe C n'avaient plus qu'un octet et ne pouvaient accueillir que 254 hôtes (1-254, puisque 0 et 255 sont toujours réservés). Cela montre que la classification n'était tout simplement pas pratique dans la plupart des cas. Pour de nombreuses entreprises, un réseau ne comptant que 254 participants était beaucoup trop petit, mais plusieurs milliers d'hôtes ont besoin des plus petits réseaux. En fin de compte, il en a résulté beaucoup de gaspillage, car les entreprises devaient inévitablement collecter les adresses inutilisées. Pour mieux répondre aux besoins des internautes, il a été décidé d'assouplir la taille du réseau, de réduire la taille des tables de routage dans les routeurs Internet et de ralentir la diminution du nombre d'adresses IP disponibles d'où l'apparition du CIDR. Le ***CIDR*** aide à augmenter le nombre d'adresses disponibles.

Les tables de routage sont situées dans un routeur et aident à trouver le chemin vers la bonne adresse de destination. Les paquets de données passent par de nombreux nœuds de l'origine à la destination. Pour que les routeurs reconnaissent à quoi ressemble le chemin optimal à travers le réseau, une table correspondante est alimentée avec des informations. La taille du fichier augmente de façon exponentielle lorsqu'un chemin doit être introduit pour chaque cible possible. Comme le CIDR assemble les adresses en blocs, il n'est plus nécessaire de stocker autant d'informations dans les tables de routage. Cela signifie que plusieurs adresses sont combinées en un seul itinéraire.

Le ***CIDR***, qui était prévu comme une solution temporaire est maintenant active depuis plus de 20 ans. Et comme l'introduction généralisée d'IPv6 est encore longue à venir, le ***CIDR*** sera probablement encore là pour plusieurs années. C'est une raison suffisante pour en savoir plus sur le ***CIDR***.

II.1.a) Comment fonctionne le CIDR ?

Le CIDR est basé sur l'idée de masque de sous-réseau. Le ***masque de sous-réseau*** indique au routeur quelle partie de l'adresse IP est attribuée aux hôtes (les différents participants du réseau) et qui détermine le réseau.

Au lieu d'ajouter un masque de sous-réseau, une spécification sous forme de suffixes peut également être intégrée directement dans l'adresse IP en utilisant un classless interdomain routing. Mais cela ne raccourcit pas seulement l'affichage : le CIDR permet également de créer des super-réseaux en plus des sous-réseaux. Cela signifie qu'il est non seulement possible de ***subdiviser un réseau*** plus précisément, mais aussi de ***combiner plusieurs réseaux*** (super-réseau).

Les super-réseaux sont importants, par exemple, si une entreprise a plusieurs sites mais veut traiter tous les ordinateurs dans le même réseau. Les super-réseaux permettent de ***combiner plusieurs réseaux en une seule route***, c'est pourquoi cette technologie est également appelée ***agrégation de routes*** (c'est-à-dire regroupement de routes). Cela signifie que les paquets de données ne sont envoyés qu'à une seule destination, quel que soit l'emplacement des hôtes.

II.1.b) La notation de CIDR

Une adresse IP permettait dans le passé de déterminer à quelle classe elle appartenait. Par exemple, les réseaux de classe C étaient situés entre les adresses 192.0.0.0 et 223.255.255.255. Un masque de sous-réseau (par exemple 255.255.255.0) est comme un masque sur l'adresse IP et spécifie les hôtes. Au format CIDR, ces informations sont stockées sous forme de suffixe dans l'adresse IP elle-même.

Cependant, le principe de base reste le même : le suffixe spécifie quels endroits (bits) de l'adresse IP représentent l'ID réseau et donc quels bits constituent automatiquement la plage de l'ID hôte. Si vous voulez comprendre cela en détail, il est utile de regarder un masque de sous-réseau dans sa forme binaire : 255.255.255.0 = 11111111 11111111 11111111 00000000

En notation CIDR, ce masque de sous-réseau (classe C) serait /24, puisque les 24 premiers bits déterminent le composant réseau de l'adresse IP. Il est possible non seulement de remplir complètement les octets avec des uns ou des zéros, mais aussi de créer des sous-réseaux plus flexibles en utilisant le VLSM. Par exemple, le masque /25 correspond à la valeur binaire 1111111111 11111111 11111111 10000000, qui à son tour (en notation point-décimal) correspond à 255.255.255.128.

II.2) LE VLSM

Le VLSM (Variable Lenght Subnet Mask ou Masque de sous réseau à longueur variable) [3] est une application du principe du CIDR à une organisation. Les conditions d'application du VLSM sont identiques à celles du CIDR.

Pour appliquer VLSM à un réseau il faut procéder comme ceci :

- ✓ Recenser le nombre total d'utilisateurs sur le réseau en prévoyant une marge pour l'évolution de celui-ci (la prévision de l'évolution d'un réseau distingue un bon plan d'adressage d'un très bon) ;
- ✓ Choisir la classe d'adresse à utiliser en fonction du nombre d'utilisateurs du réseau ;
- ✓ Découper la topologie en différentes couches (ex : pays, région, ville, quartier, bâtiment, étage, etc.) ;
- ✓ Réserver un nombre de bits nécessaire à la description de ces couches dans le masque de sous réseau ;
- ✓ Calculer le masque de sous réseau à chaque niveau de l'organisation.

Cette procédure est commune aux deux types d'application du VLSM : VLSM symétrique et VLSM asymétrique, le VLSM asymétrique étant la procédure couramment employée car elle est la plus économe en adresses IP et la plus « intelligente » (l'économie d'adresse IP étant une des raisons principales de l'utilisation des masques à tailles variables et donc des procédures CIDR/VLSM).

II.2.a) Le VLSM symétrique

Le VLSM symétrique est un découpage de la topologie réseau attribuant la même taille à chaque couche (sous réseau).

C'est la méthode la plus simple pour l'application du VLSM mais c'est aussi la moins économe en IP.

Voici un exemple pour illustrer l'application du VLSM symétrique dans une entreprise :

Nous disposons d'une entreprise située dans un bâtiment de 3 étages.

Au 1er étage, il y a deux services nommés 1A et 1B respectivement de 10 et 20 IP

Au 2^{ième} étage, il y a un seul service nommé 2A de 50 IP

Au 3eme étage, il y a trois services nommés 3A, 3B et 3C respectivement de 30, 20 et 30 IP

Procédons comme ceci :

Le total des IP est de 160 utilisateurs, nous utiliserons donc une adresse de classe C (ex : 192.168.0.0) car c'est la classe qu'on peut prendre pour gaspiller moins d'adresses. Le plus gros service est de 50 IP, il faut donc réserver 6 bits (2^6) pour l'adressage des hôtes. Il y a au plus 3 services par étage, il faut donc réserver 2 bits pour la description des services. Enfin, il y a 3 étages, il faut donc également 2 bits pour la description de l'étage. Cela nous donne donc une ip de cette forme :

192.168. 0000 0000 . 00000000

En rouge, les bits réservés aux hôtes, en vert, les bits réservés aux services et enfin en bleu les bits réservés aux étages.

À partir de ce plan, on choisit alors les IP à utiliser de cette manière :

1er étage : 192.168. 0000 0000 . 00000000

Section A : 192.168. 0000 0000 . 0000 0000

Section B : 192.168. 0000 0000 . 0100 0000

2nd étage : 192.168. 0000 0001 . 0000 0000

Section A : 192.168. 0000 0001 . 0000 0000

3eme étage : 192.168. 0000 0010 . 0000 0000

Section A : 192.168. 0000 0010 . 0000 0000

Section B : 192.168. 0000 0010 . 0100 0000

Section C : 192.168. 0000 0010 . 1000 0000

Puis on traduit les adresses binaires en décimale et déterminons le masque de sous réseau à partir des bits communs à chaque couche.

1er étage : 192.168.0.0 /24

Section A : 192.168.0.0 /26

Section B : 192.168.0.64 /26

2nd étage : 192.168.1.0 /24

Section A : 192.168.1.0 /26

3eme étage : 192.168.2.0 /24

Section A : 192.168.2.0 /26

Section B : 192.168.2.64 /26

Section C : 192.168.2.128 /26

II.2.b) VLSM asymétrique

Le VLSM asymétrique est supérieur au VLSM symétrique en un point : Il permet de réduire encore plus le gaspillage d'IP en attribuant des masques de sous réseau différents dans une même couche. En conséquence, le déploiement de cette méthode est plus complexe, car elle demande une réflexion sur chaque élément de chaque couche.

Dans l'exemple précédent, que la section est de 50 IP ou 10, l'on réservait toujours 6 bits à la description des hôtes. Ce qui fait que pour la section 1A, 52 IP étaient inutilisées.

Refaisons à présent le même exercice en utilisant la technique du VLSM asymétrique :

Le total des IP est de 160 utilisateurs, nous utiliserons donc une adresse de classe C (ex : 192.168.0.0).
Le plus gros service est de 50 IP, il faut donc réserver 6 bits pour l'adressage des hôtes. Il y a au plus 3 services par étage, il faut donc réserver 2 bits pour la description des services. Enfin, il y a 3 services, il faut donc également 2 bits pour la description de l'étage.

Cela nous donne donc une IP de cette forme : 192.168. 0000 0000 . 0000 0000

En rouge, les bits réservés aux hôtes, en vert, les bits réservés aux services et enfin en bleu les bits réservés aux étages.

Néanmoins, le service 1A ne dispose pas de 50 IP mais de 10. 10 IP n'ont pas besoin d'être codé sur 6 bits, 4 suffisent à en coder 16.

L'IP pour ce service sera donc de cette forme : 192.168. 0000 0000 . 0000 0000

Cela nous permettra donc de créer des services supplémentaires pour le premier étage parmi les 128 IP attribuables si besoin est.

De même, pour les services disposant de 20 IP :

192.168. 0000 0000 . 0000 0000

Et les services disposant de 30 IP :

192.168. 0000 0000 . 0000 0000

Voici un schéma qui illustre cette idée :

Nous disposons par étage d'un ensemble de 256 IP. Cette ensemble est redécoupé en 2 plages de 128 IP qui sont elles-mêmes « redécoupables » en deux plages de 64 et ainsi de suite jusqu'à en théorie des plages de 2 adresses IP.

Ainsi, en utilisant le découpage symétrique, on utilisait des plages de 64 IP même lorsque le réseau était de 10 IP.

Là où on utilisait une plage de 64 IP pour 10 IP, on peut maintenant utiliser une plage de 16 IP et disposer de :

- 7 autres plages de de 16 IP
- 3 plages de 32 IP et une plage de 16 IP
- 1 plage de 64 IP, une plage de 32 IP et une plage de 16 IP

L'essentiel étant de respecter la forme de ce tableau. Il n'est par exemple pas possible d'utiliser la 2nd et 3eme plage de 16 IP pour former une plage de 32 IP, il faut respecter la répartition des plages supérieures situées plus à gauche dans le schéma.

<table>
<tr><th colspan="5">Plages d'adresses (Nombres d'adresses IP)</th></tr>
<tr><td rowspan="8">256</td><td rowspan="7">128</td><td rowspan="4">64</td><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="3">64</td><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td>128</td><td>64</td><td>32</td><td>16</td></tr>
</table>

<table>
<tr><td rowspan="8"></td><td rowspan="8"></td><td rowspan="3"></td><td></td><td>16</td></tr>
<tr><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="5">64</td><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
</table>

Tableau 1:Plages d'adresses par niveau

À partir de ce plan, on choisit alors les IP à utiliser de cette manière :

<table>
<tr><td colspan="5">Plages d'adresses (Nombres d'adresses IP)</td></tr>
<tr><td rowspan="16">256</td><td rowspan="8">128</td><td rowspan="4">64</td><td rowspan="2">32</td><td>Section 1A</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="2">Section 1B</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="4">64</td><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="8">128</td><td rowspan="4">64</td><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="4">64</td><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
<tr><td rowspan="2">32</td><td>16</td></tr>
<tr><td>16</td></tr>
</table>

Tableau 2: Exemple pour le 1er étage

En jaune, les plages d'IP utilisés entièrement ou partiellement.

En rouge, les plages d'IP inutilisables du fait de l'utilisation d'une plage supérieure.

En vert, les plages d'IP utilisables.

1er étage : 192.168. 0000 0000 . 0000 0000

Section A : 192.168. 0000 0000 . 0000 0000

Section B : 192.168. 0000 0000 . 0010 0000

2nd étage : 192.168. 0000 0001 . 0000 0000

Section A : 192.168. 0000 0001 . 0000 0000

3eme étage : 192.168. 0000 0010 . 0000 0000

Section A : 192.168. 0000 0010 . 0000 0000

Section B : 192.168. 0000 0010 . 0100 0000

Section C : 192.168. 0000 0010 . 1000 0000

Puis on traduit les adresses binaires en décimale et déterminons le masque de sous réseau à partir des bits communs à chaque couche.

1er étage : 192.168.0.0 /24

Section A : 192.168.0.0 /28

Section B : 192.168.0.32 /27

2nd étage : 192.168.1.0 /24

Section A : 192.168.1.0 /26

3eme étage : 192.168.2.0 /24

Section A : 192.168.2.0 /26

Section B : 192.168.2.64 /27

Section C : 192.168.2.128 /26

Dans l'exemple d'utilisation d'adressage symétrique, on utilisait alors 384 IP (6 services multipliés par des plages de 64 IP).

À présent, nous n'utilisons plus que 272 IP (3 services avec des plages de 64 IP, 2 services avec des plages de 32 IP et un service dont la plage est de 16 IP).

L'économie d'IP n'est donc pas négligeable ! Surtout qu'il s'agit ici d'une petite organisation, appliqué à un plus grand réseau, l'économie d'IP croie exponentiellement !

III) NAT

L'adresse IP (Internet Protocole) est un élément qui permet d'identifier les machines et de router les informations sur Internet [5]. Ces adresses sont codées sur 4 octets, soit 32 bits ; ce qui nous permet d'avoir 2^{32} adresses disponibles (un peu plus de 4 milliards d'adresses). Nous assistons à un manque d'adresses IPv4. En attendant un nouveau standard d'adressage permettant d'avoir plus d'adresses disponibles (IPv6=$3{,}4 \times 10^{38}$ adresses), il a fallu trouver des solutions temporaires. Le NAT a notamment été une réponse à cette pénurie d'adresses IPv4. Le NAT permet de faire de la translation d'adresses. Quand un paquet traverse le routeur NAT, l'adresse IP d'une machine dans le réseau local est échangée par l'une des adresses publiques du routeur. De ce fait, une machine avec une adresse privée (non routable sur Internet) pourra dialoguer avec une machine sur internet.

Un routeur fait du NAT (*Network Address Translation* soit « traduction d'adresse réseau ») lorsqu'il fait correspondre les adresses IP internes privées (non-uniques et souvent non routables) d'un intranet à un ensemble d'adresses externes publiques (uniques et routables). Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.

III.1) Adresses non-routables (adresses privées)

Les adresses ***non-routables*** sont des adresses particulières, elles ne peuvent pas être utilisées sur Internet. Elles permettent de réduire la pénurie d'adresse IPv4 vu que plusieurs structures peuvent utiliser les ***même adresses IP***. Voici les plages d'adresses privées :

- ✓ plage de 10.0.0.0 à 10.255.255.255 pour la classe A;
- ✓ plage de 172.16.0.0 à 172.31.255.255 pour la classe B;
- ✓ plage de 192.168.0.0 à 192.168.255.255 pour la classe C.

III.2) Principe du NAT

Le mécanisme de translation d'adresses [6] (en anglais *Network Address Translation* noté NAT) a été mis au point afin de ***répondre à la pénurie d'adresses IP avec le protocole IPv4***. En effet, en adressage IPv4 le nombre ***d'adresses IP routables*** n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet. Le principe du NAT consiste donc à utiliser une ***passerelle*** de connexion à internet, possédant au moins une ***interface réseau connectée sur le réseau interne*** et au moins une ***interface réseau connectée***

à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau nécessitant d'être connectées à internet.

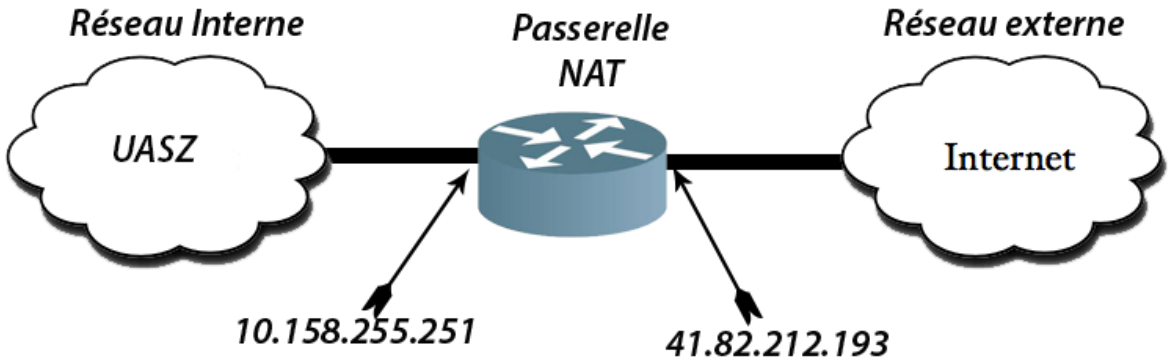


Figure 3: Principe du NAT

Il s'agit de réaliser, au niveau de la passerelle, une translation (littéralement une « traduction ») des paquets provenant du réseau interne vers le réseau externe.

Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP). ***Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande***.

Étant donné que la passerelle camoufle complètement l'adressage interne d'un réseau, le mécanisme de translation d'adresses permet ainsi ***d'assurer une fonction de sécurisation***. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de l'adresse IP de la passerelle.

En fonction de la correspondance entre le nombre d'adresses publiques et privées utilisées, on peut citer le NAT statique et le Nat dynamique.

III.3) Le NAT statique

III.3.a) Principe

Une adresse IP Privée est associée une adresse IP publique. Par exemple : s'il y a trois machines dans le réseau local, il faudra trois adresses IP publiques. Pour 1000 machines, il faudra 1000 adresses IP publiques.

Dans ce cas, la seule action qui sera effectuée par le routeur sera de remplacer l'adresse privée l'adresse publique.

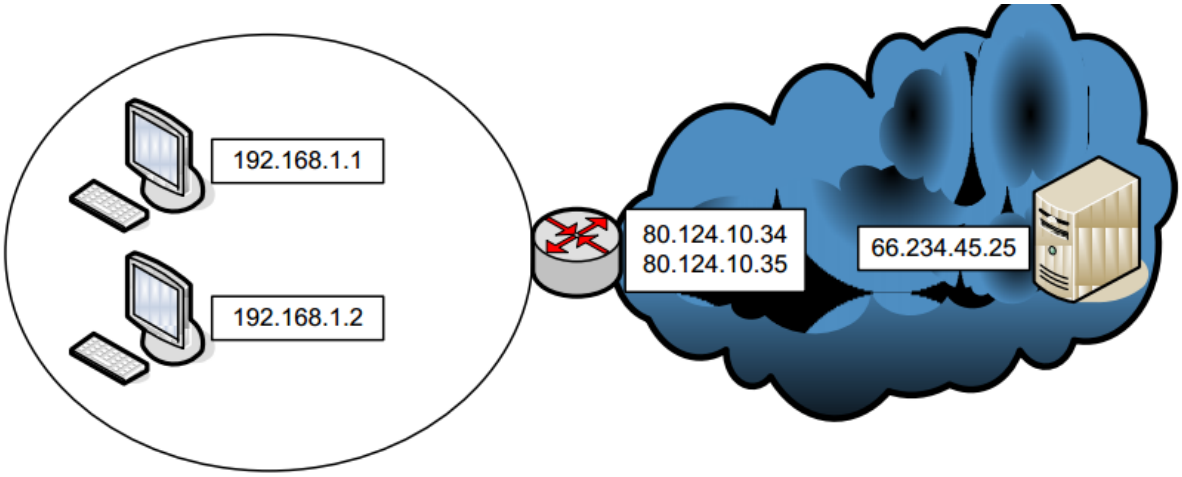


Figure 4: Principe du NAT Statique

III.3.b) Avantages et inconvénients du NAT statique

Il est souvent préférable de garder un adressage uniforme en interne et de ne pas mêler les adresses publiques aux adresses privées. Ainsi, si l'on doit faire des modifications, changements, interventions sur le réseau local, on peut facilement changer la correspondance entre les adresses privées et les adresses publiques pour rediriger les requêtes vers un serveur en état de marche.

En associant une adresse IP publique à une adresse IP privée, nous avons pu rendre une machine accessible d'Internet.

On remarque qu'avec ce principe, on est obligé d'avoir une adresse publique par machine voulant accéder à Internet. Cela ne va pas régler notre problème de pénurie d'adresses IP...

III.4) Le NAT dynamique

III.4.a) Le principe

La NAT dynamique est aussi appelée IP *masquerading*. Contrairement à la NAT statique, la NAT dynamique associe M adresses internes à N adresses externes où M > N (les adresses pour sortir étant choisies dans un *pool*). Ainsi, on peut associer ***une adresse publique*** à ***M adresses privées*** et permettre ainsi à un grand nombre de machines ayant des adresses privées d'accéder à Internet.

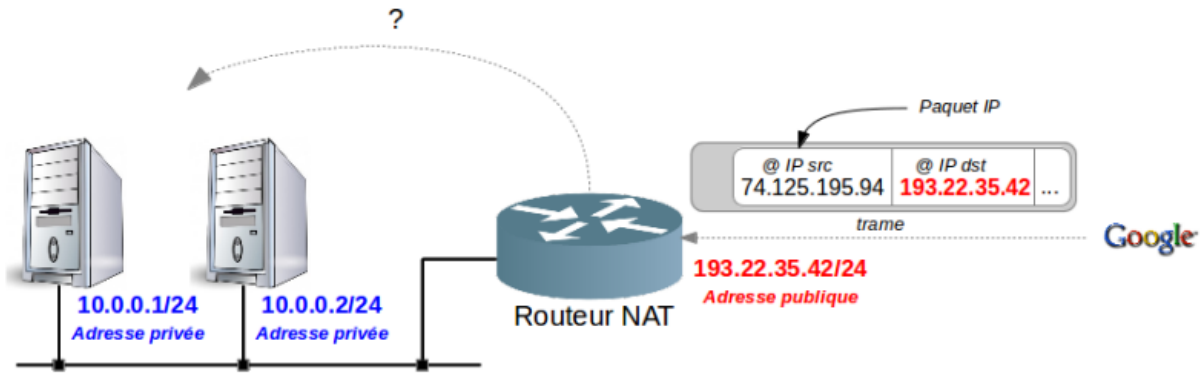


Figure 5: Principe du NAT Dynamique

III.4.b) Fonctionnement du NAT Dynamique

Pour "multiplexer" (partager) les différentes adresses IP sur une ou plusieurs adresses IP triées, le NAT dynamique utilise le mécanisme de traduction de port (PAT - Port Address Translation), attribution d'un port source différent à chaque nouvelle demande afin qu'il puisse maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des terminaux sur Internet, le tout adressé à l'adresse IP du routeur.

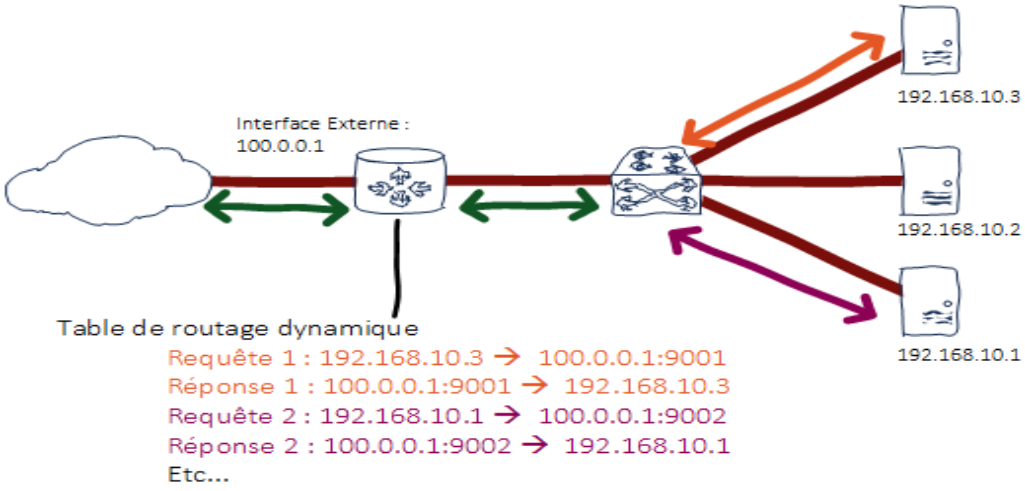


Figure 6: Fonctionnement du NAT Dynamique

Source : https://www.it-connect.fr/nat-statique-ou-dynamique-quelle-difference/

IV) Limites d'IPv4

Le système d'adresse IP (Internet Protocol) était initialement basé sur un protocole IPv4 (Internet Protocol Version 4), lancé au début des années 1980, codé en 32 bits et qui donnait la

possibilité de créer plus de 4 milliards d'adresses appartenant à différentes classes (A, B, C, D et E). Il faut rappeler que ce système n'avait pas été mis en place pour satisfaire un internet du type de celui que nous connaissons aujourd'hui, mais plutôt un internet réservé aux réseaux gouvernementaux et à la recherche.

Personne à cette époque n'aurait pu prévoir un tel développement d'internet. Et cette ***croissance exponentielle, qui a conduite à l'abandon de l'adressage par classes (dû au gaspillage d'adresse IP)*** est loin d'être terminée.

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

- **Manque d'adresses IP**

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, les connexions permanentes et la croissance potentielle des pays en voie de développement entraînent une hausse du nombre d'adresses devant être disponibles.

Cette hausse est également liée à l'apparition des objets connectés, ce qui nécessite la prise en compte de 28 millions d'objets à l'horizon de 2020. Parmi les 4 milliards d'adresses, seul 3,7 milliards peuvent être attribués car le système d'adressage IPv4 sépare les adresses en classes et réserve des adresses pour la multidiffusion, les tests et d'autres usages spécifiques.

- **Croissance de la table de routage Internet**

Les routeurs utilisent des tables dites de routage pour déterminer les meilleurs chemins disponibles et acheminer les datagrammes vers leur destination.

À mesure que le nombre de serveurs (nœuds) connectés à Internet augmente, il en va de même pour le nombre de routes réseaux sur la table de routage. Les routes IPv4 consomment beaucoup de mémoire et de ressources processeur sur les routeurs internet avec le grand nombre de nœuds connectés. Le problème vient du fait que les adresses ont été distribuées sans tenir compte de la localisation géographique des réseaux. En IPv6 par contre, la distribution est faite de manière à ce que des réseaux qui sont géographiquement voisins aient des plages d'adresses voisines.

- **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.

Conclusion

Face à la croissante vertigineuse des objets à attribuer une adresse, des méthodes, telles que le CIDR, VLSM, le NAT et les adresse privées, ont était mise en place pour atténuer la pénurie d'adresses IPv4. Mais ces méthodes ont à leur tour engendré des problèmes qui dans un future proche nécessitent un passage du protocole IPv4 vers IPv6 : c'est la migration.

La migration d'IPv4 vers IPv6 est indispensable pour éviter une dramatique pénurie d'adresses ainsi qu'une explosion des tables de routage. Avant d'effectuer cette migration, il est primordial de connaitre le protocole IPv6. C'est pour cette raison que nous tenterons au chapitre suivant d'étudier ce protocole.

chapitre II) Présentation de IPv6

Introduction

Le protocole de routage principalement utilisé aujourd'hui [8] pour les communications Internet est le protocole IP (Internet Protocol). La version la plus utilisée du protocole IP est la version 4 (IPv4) et n'a fait l'objet d'aucune évolution majeure depuis la publication du document fondateur, la ***RFC (Request For Comment) 791***. Le protocole IP dans sa version 4 s'est avéré assez robuste tout au long de l'essor de l'Internet. Cependant, un certain nombre de caractéristiques et d'évolutions n'ont pas été prises en compte, ce qui a conduit à la nécessité de l'élaboration d'un successeur au protocole IP actuel (IPv4).

Parmi les évolutions actuelles mal considérées par ***IPv4***, on peut citer :

- la croissance rapide de l'Internet qui conduit rapidement à un épuisement des adresses IPv4 disponibles. L'***IANA***[2] ***(Internet Assigned Numbers Authority)*** a distribué les derniers ranges ***IPv4*** récemment.
- la multiplication des systèmes communiquant mobiles (PDA (Personal Digital Assistant), téléphones portables, …) ;
- l'essor de nouveaux services de diffusion multimédia (Vidéoconférence, VoD, …).

Le successeur naturel aurait pu logiquement être ***IPv5***, mais cette version a été attribuée à un protocole expérimental : ST (Internet Stream Protocol) qui n'a jamais atteint le grand public. Le successeur fut donc choisi sous le nom de ***IPv6***, également appelé ***IPng*** (IP New Generation).

Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits pour IPv4. La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (16 bits par groupe) sont séparés par un signe deux points (:).

Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire.

[2] L'Internet Assigned Numbers Authority (IANA) est un département de l'ICANN, une société américaine privée à but non lucratif qui supervise l'allocation globale des adresses IP, l'allocation des numéros de systèmes autonomes, la gestion de la zone racine dans les Domain Name System

Ce chapitre présente la structure une adresse IPv6. Il explique en détail les différents types d'adresses qui ont été retenues pour construire les réseaux IPv6. Il décrit également la manière de notation d'une adresse IPv6.

I) Structure d'une adresse IPv6

Ayant au total 128 bits, les adresses IPv6 [7] sont composées de 8 blocs de 16 bits ayant chacun des nombres hexadécimaux de quatre chiffres. Ces blocs sont séparés par deux points (:).

Ces 128 bits [8] peuvent être divisés en trois parties et l'une d'elles est utilisée pour le sous- réseau IPv6. Quelles sont ces parties d'adresse IPv6? Ces pièces sont:

- ID réseau (48 bits)
- ID de sous-réseau (16 bits)
- ID d'interface (64 bits)

Figure 7: les trois parties d'une adresse IPv6

Source : https://ipcisco.com/lesson/subnetting-in-ipv6-2/

Nous pouvons également diviser la partie ID réseau en deux. Ces parties d'ID de réseau IPv6 sont données ci-dessous:

- Préfixe ISP ou préfixe FAI (/ 32)
- Préfixe de site client (/ 48)

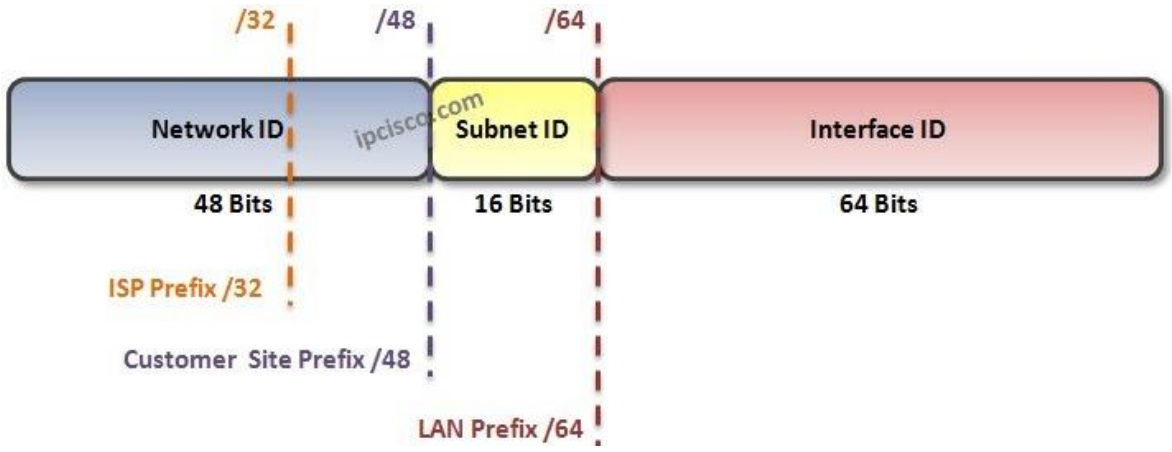


Figure 8: Parties d'ID de réseau IPv6

Source : https://ipcisco.com/lesson/subnetting-in-ipv6-2/

Exemple :

2001:0620:0000:0000:0211:24FF:FE80:C12C

Les premiers 64 bits sont utilisés pour le ***routing*** et désignent le ***préfixe du réseau***. Le préfixe du réseau caractérise le réseau, le sous-réseau ou la plage d'adresse. Les derniers 64 bits sont désignés comme "Interface Identifier" (ID : identificateur d'interface). L'Interface Identifier désigne un hôte dans ce réseau : elle est constituée à partir de l'adresse MAC 48 bits ou de manière aléatoire et est convertie en une adresse 64 bits. Il s'agit là du format EUI-64 modifié. Ainsi, l'interface est clairement identifiable indépendamment du préfixe du réseau.

Le masque réseau ou sous-réseau connu par le protocole IPv4 disparaît avec le protocole IPv6 sans être remplacé.

Pour pouvoir tout de même procéder à une segmentation, la longueur du préfixe est définie et est ajoutée avec un "/" (slash ou barre oblique) à l'adresse IPv6 en soi. Exemple : Un sous-réseau avec les adresses IPv6 entre 2001:0820:9511:0000:0000:0000:0000:0000 et 2001:0820:9511:FFFF:FFFF:FFFF:FFFF:FFFF peut être décrit avec la notation

2001:0820:9511::/48.

II)Types d'adresses IPv6

IPv6 reconnaît trois types d'adresses : ***unicast***, ***multicast*** et ***anycast***. Le type d'adresse définit la cardinalité de la communication: ***à combien de destinataire doit être remis le paquet***.

II.1) Adresses de monodiffusion ou Unicast (point à point)

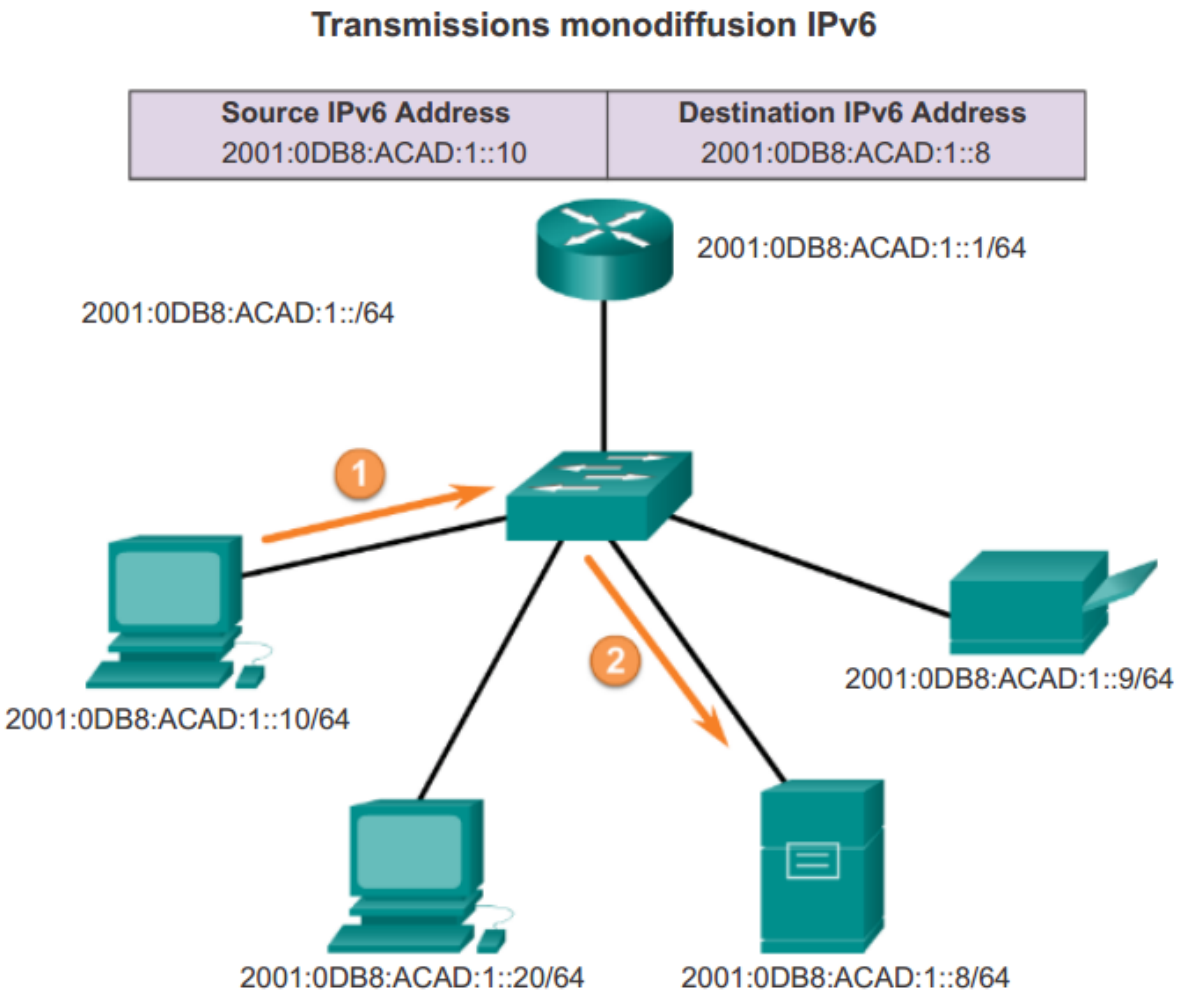


Figure 9: Communication réseau unicast

Source : Google images (adresse unicast)

Les adresses de monodiffusion représentent une seule interface. Les paquets adressés à une adresse unicast seront livrés à une interface réseau spécifique. Il existe trois types d'adresses de monodiffusion IPv6:

II.1.a) Monodiffusion globale

- ✓ **Présentation**

Similaire aux adresses IP publiques IPv4. Ces adresses sont attribuées par l'IANA et utilisées sur les réseaux publics. Ils ont un préfixe 2000 :: / 3 (toutes les adresses commençant par binaire 001).

✓ **Format**

Son format [8] est :

Global routing prefix		Subnet ID	Interface ID
001	48 bits	16 bits	64 bits

Figure 10: Format d'une adresse IPv6 unicast globale

- Les 3 premiers bits de valeur 001 instituant la première tranche d'adresses ouvertes par l'organisme ICANN, il appartient au prefixe de routage globale ;
- Global routing prefix (Préfixe de routage global) : ce champ est codé sur 48 bits. Il constitue le préfixe d'un LIR (Local Internet Registry) utilisé pour le routage inter-domaine dans le réseau public ;
- Subnet ID (identificateur sous-réseaux) : ce champ est codé sur 16 bits et est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site. Plus l'ID de sous-réseau est un nombre important, plus il y a de sous-réseaux disponibles. Associé aux champs précédents il constitue le préfixe complet de l'adresse global unicast
- Interface ID (identificateur interface) : ce champ est codé sur 64 bits représente le suffixe de l'adresse global unicast.

II.1.b) Unique local

✓ **Présentation**

Similaire aux adresses privées IPv4. Elles sont utilisées dans des réseaux privés et ne sont pas routables sur Internet. Ces adresses ont un préfixe FD00 :: / 8.

✓ **Format**

L'adresse unique locale est constituée des champs suivants :

7 bits	1	40 bits	16 bits	64 bits
1111110	L	Global ID	Subnet ID	Interface ID

Figure 11: Structure d'une adresse unique locale

- Un champ de 7 bits de valeur fixe 1111110. Toutes les adresses unique local sont de la forme FC00::/7 ;
  - L : ce bit est positionné à 1 lorsque l'adresse est attribuée localement. L'utilisation de ce bit à 0 n'est pas définie ;
  - Global ID : ce champ codé sur 40 bits représente un identifiant d'une organisation privée.
  - Subnet ID : Ce champ est codé sur 16 bits. Associes aux champs précédents, il constitue le préfixe complet de l'adresse unique local. Il est utilisé pour identifier les réseaux à l'intérieur d'un domaine privé.

L'adresse unique locale a remplacé l'adresse site local qui présentait un préfixe contenant uniquement le champ Subnet ID.

II.1.c) Link local

✓ **Présentation**

Une adresse de liaison locale est utilisée pour communiquer [1] entre des hôtes sur le même lien, donc elle ne traverse aucun routeur. Les adresses de liaison locale sont toujours configurées automatiquement, mais ce n'est pas de l'auto-configuration via SLAAC. Cette adresse est utilisée par exemple pour découvrir les routeurs, grâce au ***Neighbor Discovery*** Protocol, qui sera étudié plus en détail lorsque nous serons sur la partie consacrée à l'ICMPv6. Ces adresses ont un ***préfixe FE80*** :: / 10. La création de cette adresse se déroule en ajoutant le ***préfixe fe80 ::/64*** à l'adresse de ***format EUI-64*** identifiant l'interface. IPv6 nécessite l'attribution d'une adresse de lien local à chaque interface réseau sur laquelle le protocole IPv6 est activé.

✓ Format

Le format est le suivant :

10 bits	54 bits à 0	64 bits
1111111010	0000….0000	Interface ID

Figure 12: Structure d'une adresse Link-local

Le préfixe de l'adresse ***Link-local*** est fixe et est constitué de 10 bits de valeur 1111111010 et de 54 bits à 0. Toutes les adresses ***Link-local*** sont de la forme FE80 ::/64

II.2) Adresses multicast (point à multipoint)

✓ **Présentation**

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. Une communication multicast est une communication dans laquelle un même paquet de données peut être envoyé à un groupe de récepteurs, quel que soit leur localisation. Dans le modèle Internet IPv6, une station peut potentiellement émettre un paquet multicast vers n'importe quel groupe. Comparé aux communications point à point (unicast), le multicast évite la duplication des paquets de données au niveau de la source, et minimise l'utilisation de la bande passante au niveau du réseau.

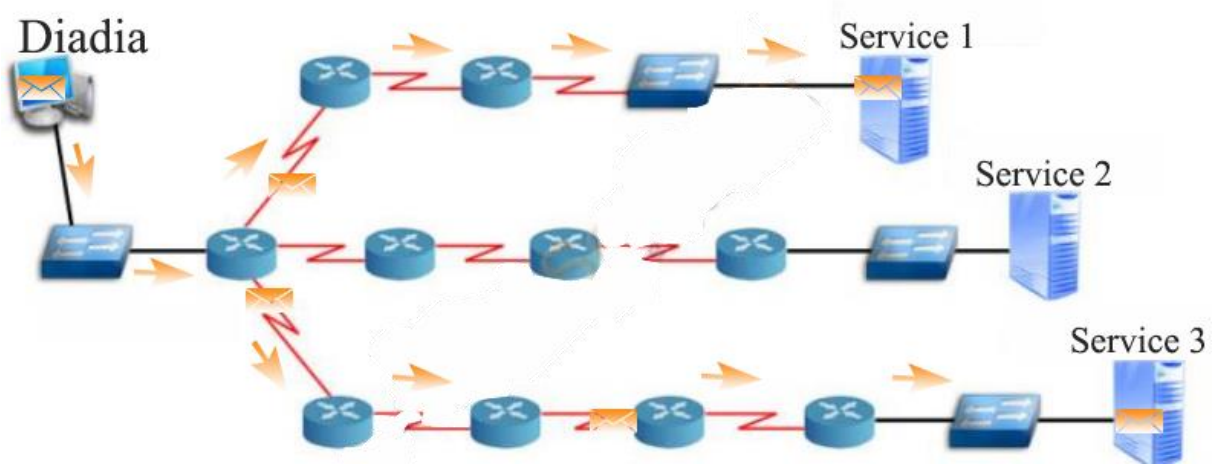


Figure 13: Communication réseau multicast

De plus, il offre un service insensible à l'augmentation du nombre et la localisation des membres d'un groupe. Le multicast peut être utilisé pour la distribution de logiciels, la téléconférence, les applications d'enseignement à distance, la radio ou la télévision sur Internet, les simulations interactives distribuées, les jeux multimédia interactifs, les applications militaires, etc.

✓ **Format** :

Les adresses multicast ont le format suivant [RFC 2373]:

FF	flags	scope	Groupe ID
8 bits	4 bits	4 bits	112 bits

Figure 14:structure d'une adresse multicast

- FF ou 1111.1111: identifie l'adresse comme étant multicast.
  - Flags
    - ✓ Flag 0000 : assigné de façon permanente.
    - ✓ Flag 0001 : assigné de façon provisoire.
  - Scope : valeur qui définit l'étendue d'un groupe multicast.
    - ✓ 0 : réservé
    - ✓ 1 : nœud
    - ✓ 2 : lien (FF02 ::/8)
    - ✓ 3 : sous-réseau
    - ✓ 5 : site
    - ✓ 6 : organisation
    - ✓ E : global
    - ✓ F : réservé

  Exemples : FF02 ::2 représente tous les routeurs sur le même lien que l'expéditeur FF05 ::2 représente tous les routeurs sur le même site que l'expéditeur.

  - Group ID : identifie un groupe multicast au sein de l'étendue spécifiée.

II.3) Adresse Anycast

✓ **Présentation**

Le dernier type, Anycast [8] désigne un groupe d'interfaces, la différence avec le multicast 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.

Anycast est un type de communication réseau IPv6 dans lequel les datagrammes IPv6 d'une source sont routés vers le périphérique le plus proche [9] (en termes de distance de routage) à partir d'un groupe de serveurs fournissant le même service. Tous les nœuds qui fournissent le même service sont configurés avec la même adresse de destination Anycast.

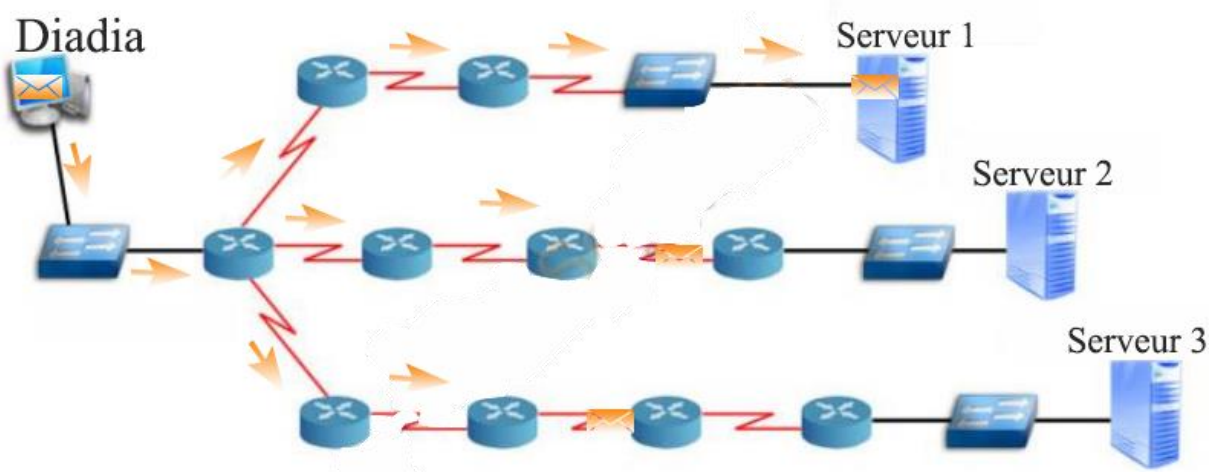


Figure 15 : communication réseau anycast

Reportez-vous à l'image ci-dessus. Ici, nous avons trois serveurs fournissant le même service réseau, mais situés à des distances de routage différentes du réseau source. À l'aide de protocoles de routage, la communication réseau IPv6 Anycast peut identifier le nœud proche à partir d'un groupe de nœuds de serveurs, qui fournit le même service et utilise le service depuis le serveur proche.

- ✓ **Format**

L'adresse IPv6 anycast est constituée des champs suivants :

Subnet Prefix	ID Groupe
n bits	128 – n bits

Figure 16: structure d'une 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 autres structures d'adresses la longueur de ce préfixe n'est pas spécifiée, car une adresse anycast doit s'adapter aussi bien aux plans d'adressages actuels qu'aux futurs plans qui pourraient avoir des tailles différentes.

III) Notation

La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux points :

Exemple : 2001:0db8:0000:85a3:0000:0000:ac1f:8001

Il est permis d'omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à :

2001:db8:0:85a3:0:0:ac1f:8001

De plus, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux points (::) . Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en :2001:db8:0:85a3::ac1f:8001

En revanche l'écriture suivante n'est pas valide :2001:db8::85a3::ac1f:8001 car elle contient plusieurs substitutions (::), il ne peut exister qu'une seule occurrence de la séquence :: dans la notation d'une adresse IPv6.

Pour résumer, la séquence :: dans l'adresse IPv6 signifie que l'on doit combler tout ce qu'il manque avec des 0, donc cette séquence ne peut être utilisée qu'une seule fois.

IV) Quelques Protocoles d'IPv6

Pour Internet et les réseaux locaux, le protocole Internet est un composant indispensable. En effet, pour garantir le transport des informations numériques et l'envoi des paquets de données appropriés à l'hôte cible conforme, un certain nombre de protocoles d'aide et de routage supplémentaires sont nécessaires.

IV.1) **ICMPv6**

Le protocole de message de contrôle Internet (ICMPv4 et ICMPv6) est un protocole qui agit comme un protocole de messagerie de communication entre les périphériques communicants du réseau IP. Les messages ICMP fournissent des fonctions de retour d'information, de rapport d'erreurs et de diagnostic réseau sur les réseaux IP nécessaires au bon fonctionnement d'un réseau IPv6.

Dans IPv4, ICMP signale les informations de transmission de paquets IP et les erreurs au nœud source. ICMP définit certains messages tels que Destination inaccessible, Paquet trop grand,

Temps dépassé, Demande d'écho et Réponse d'écho pour faciliter le diagnostic des erreurs et la gestion des informations.

Le protocole de message de contrôle Internet version 6 (ICMPv6) est l'un des protocoles de base IPv6. Il fournit des mécanismes supplémentaires en plus des fonctions ICMPv4 actuelles. Ceux sont entre autres :

- Rapport d'erreur
- Diagnostic du réseau
- Découverte du voisin
- Rapports sur les membres en multidiffusion
- Sollicitation de routeur et annonces de routeur

Les messages ICMPv6 peuvent être classés en ***messages d'erreur*** ICMPv6 et en ***messages d'information*** ICMPv6.

IV.1.a) Messages d'erreur ICMPv6

Les messages d'erreur ICMPv6 sont utilisés pour signaler des erreurs dans le transfert ou la livraison de paquets IPv6. Les valeurs "Champ de type" ICMPv6 du message d'erreur sont comprises entre 0 et 127. Les messages d'erreur ICMPv6 sont ***Destination inaccessible***, ***Paquet trop volumineux***, ***Temps dépassé*** et ***problème de paramètre***.

Message d'erreur ICMPv6 "Destination inaccessible": Le message d'erreur ICMPv6 Destination inaccessible est généré par l'hôte source ou un routeur lorsqu'un paquet de datagramme IPv6 ne peut pas être remis pour une raison autre que l'encombrement.

Message d'erreur ICMPv6 "paquet trop gros": Les messages d'erreur ICMPv6 sont générés par le routeur lorsqu'un paquet ne peut pas être transmis à la liaison du saut suivant car la taille du datagramme IPv6 est supérieure à celle du MTU (unité de transmission maximale) du lien. Le message d'erreur ICMPv6 "Packet Too Big" inclut également le MTU (Maximum Transmission Unit) du lien suivant. MTU (Maximum Transmission Unit) est la taille de la plus grande unité de données de protocole prise en charge sur la liaison.

Message d'erreur ICMPv6 "Temps dépassé": similaire à la valeur du champ Durée de vie dans l'en-tête de datagramme IPv4, l'en-tête IPv6 inclut un champ Limite de sauts. La valeur du champ Limite de saut dans l'en- tête IPv6 est utilisée pour empêcher les boucles de routage.

Le champ Limite de saut dans l'en-tête de datagramme IPv6 est décrémenté par chaque routeur qui transmet le paquet. Lorsque la valeur du champ limite de saut dans l'en-tête IPv6 atteint zéro, le routeur ignore le paquet de datagramme IPv6 et renvoie un message d'erreur ICMPv6 "Temps dépassé" à l'hôte source.

Message d'erreur ICMPv6 "Problème de paramètre": Le message d'erreur ICMPv6 est généralement lié aux problèmes et erreurs liés à l'en-tête IPv6 lui - même. Lorsqu'un problème ou une erreur avec un en-tête IPv6 empêche un routeur de traiter le paquet, le routeur arrête de traiter le paquet de datagramme IPv6, ignore le paquet et renvoie un message d'erreur ICMPv6 "Problème de paramètre" à l'hôte source.

IV.1.b) Messages d'information ICMPv6

Les messages d'information ICMPv6 sont utilisés pour les fonctions de diagnostic réseau et les fonctions réseau critiques supplémentaires telles que la découverte de voisin, la sollicitation de routeur et les annonces de routeur, les abonnements multidiffusion. Demande d'écho et réponse d'écho (utilisées par de nombreuses commandes et utilitaires tels que "Ping" pour les diagnostics de réseau et les problèmes de communication) sont également des messages d'information ICMPv6. Les messages d'information ICMPv6 ont des valeurs pour le champ Type (nombre binaire sur 8 bits) comprises entre 128 et 255.

- **Messages de diagnostic:** La demande d'écho ICMPv6 et la réponse d'écho sont les messages de diagnostic. Chaque hôte IPv6 doit renvoyer une réponse ICMPv6 Écho lorsqu'il reçoit une demande ICMPv6 Écho. Les messages de requête d'écho et de réponse d'écho sont utilisés par la commande Ping pour vérifier la connectivité réseau entre deux hôtes IPv6.
- **Messages MLD (Découverte d'écouteurs multicast):** Les messages ICMPv6 MLD (Découverte d'écouteurs multicast) sont utilisés par un routeur compatible IPv6 pour détecter les hôtes intéressés par les paquets multicast et les adresses de multidiffusion qui les intéressent. Les messages MLD (Multicast Listener Discovery) sont utilisés par le protocole MLD (Multicast Listener Discovery). Le protocole MLD (Multicast Listener Discovery) est l'équivalent IPv6 du protocole IGMP (Internet Group Management) dans IPv4.
- **Messages ND (découverte du voisin):** Les messages ICMPv6 ND (découverte du voisin) sont utilisés pour le protocole de découverte du voisin (NDP). Les messages ND

(découverte du voisin) comprennent la sollicitation de routeur et l'annonce de routeur, la sollicitation de voisin et l'annonce de voisin

IV.2) Neighbor Discovery Protocol (NDP)

Le protocole de découverte de voisin [1] (NDP, défini dans le document RFC 4861) est un protocole important dans IPv6. Ce protocole de découverte de voisin (NDP) est basé sur ICMPv6 et est utilisé pour identifier les relations entre différents périphériques voisins dans un réseau IPv6. De nombreuses fonctions importantes d'IPv6 telles que la résolution de l'adresse MAC d'une adresse IPv6 (dans IPv4, ARP est utilisé pour cela), la découverte de routeur, etc., sont maintenant exécutées à l'aide du protocole de découverte de voisin (NDP).

Voici les fonctions importantes du protocole de découverte de voisin (NDP).

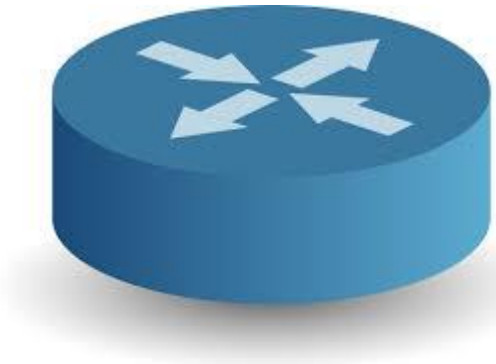
- **Découverte dynamique de routeurs**: le protocole de découverte de voisin (NDP) permet de détecter automatiquement les routeurs d'un réseau IPv6 à l'aide des messages Sollicitation de routeur et Annonce de routeur.
- **Découverte dynamique des préfix réseaux**: le protocole de découverte de voisin (NDP) permet de détecter automatiquement les préfixes réseaux IPv6 auxquels l'hôte appartient, à l'aide des messages de demande de routeur et d'annonce de routeur.
- Résolution d'adresse MAC de manière dynamique: nous utilisons des adresses IP pour la communication, mais les adresses utilisées par les commutateurs LAN pour la livraison de trames Ethernet aux périphériques de destination sont des adresses MAC. En IPv4, Address Resolution Protocol (ARP) est utilisée pour résoudre les adresses IPv4 à l'adresse MAC. Le rôle du protocole ARP (Address Resolution Protocol) dans IPv4 est effectué par le protocole NDP (Neighbor Discovery Protocol) dans IPv6.
- Configuration automatique des adresses IPv6: après avoir appris les préfixes réseaux IPv6 à l'aide des messages de sollicitation de routeur NDP (NPA) et de l'annonce de routeur, les périphériques IPv6 peuvent configurer automatiquement une adresse IPv6 en générant automatiquement la partie hôte de l'adresse IPv6 à l'aide de la méthode EUI-64.
- DAD (Détection d'adresse en double): DAD (Détection d'adresse en double) est un mécanisme NDP (Neighbor Discovery Protocol) permettant de détecter si des adresses IPv6 en double existent dans un réseau IPv6. DAD (Duplicate Address Detection) est

utile car IPv6 dispose de nombreux mécanismes de configuration automatique de l'adresse.

Conclusion

Le protocole IPv6 possède une capacité d'adressage plus importante et différents types d'adresses. Ainsi il permet d'avoir une meilleure construction du réseau Internet pour répondre à une demande croissante des parcs informatiques et des terminaux mobiles (téléphone, GPRS, WLAN). Commencer à déployer IPv6 est une bonne idée puisse que le monde internet est entrain de migrer, mais il serait judicieux d'étudier les protocoles qui nécessitent son bon fonctionnement pour un déploiement plus aisé.

chapitre III)Attribution des adresses IPv6 et routage IPv6



Introduction

Comme IPv4, un hôte peut être adressé de différentes manières dans IPv6; Les deux applications les plus courantes d'IPv4 sont l'adressage statique et la configuration d'adresse dynamique via le protocole DHCP (Dynamic Host Configuration Protocol). Les ingénieurs utilisent souvent DHCP parce qu'il fournit non seulement une méthode d'affectation dynamique des adresses, mais également un moyen d'affecter aux périphériques hôtes d'autres informations de service, telles que les serveurs DNS, les noms de domaine et diverses informations personnalisées.

Pour effectuer la configuration des adresses sur IPv6, il existe les deux méthodes connues d'IPv4 notamment: ***adressage statique et adressage dynamique.***

Celle citée en dernière position comporte quelques méthodes supplémentaires, ***adressage*** dynamique via ***DHCPv6*** (avec état), ***SLAAC*** seul ou ***SLAAC*** avec ***DHCPv6*** (sans état). L'adressage statique IPv6 fonctionne exactement de la même manière que l'adressage statique IPv4, il n'y a donc pas de mystère. Elle se fait avec l'aide de la commande :

ipv6 address @IPv6 / 64

Exemple : *ipv6 address 2001: DB8: 1111: 2222 :: 54/64*

Cependant en plus du ***SLAAC*** pour la configuration automatique, IPv6 offre deux méthodes différentes pour implémenter ***DHCP***: avec ou sans état.

I) State Less Address Auto Configuration (SLAAC)

SLAAC est l'option par défaut sur les routeurs Cisco. Cette option indique au client d'utiliser exclusivement les informations fournies dans le message Router Advertisement (RA) du routeur pour configurer leur adresse IPv6. Il s'agit du préfixe, de la longueur du préfixe, du serveur DNS, du paramètre MTU et des informations sur la passerelle par défaut. Aucune information supplémentaire n'est disponible auprès d'un serveur DHCPv6.

Cette auto configuration se fait à l'aide du ***processus EUI-64*** ou de ***manière aléatoire.***

L'adresse lien-local est créée en prenant le préfixe lien-local (FE80::/64) qui est fixé. L'adresse ainsi constituée est encore interdite d'usage. Elle possède un état provisoire car la machine doit vérifier l'unicité de cette adresse sur le lien au moyen de la ***procédure de détection d'adresse***

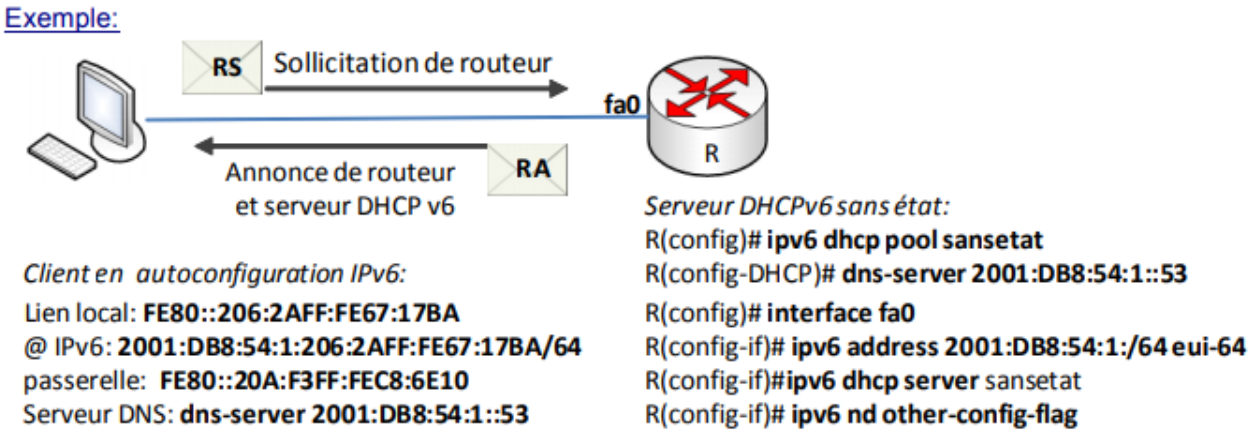
dupliquée. Si la machine détermine l'adresse lien-local n'est pas unique, l'auto configuration s'arrête et une intervention manuelle est nécessaire.

Une fois que l'assurance sur l'unicité de l'adresse lien-local est obtenue, l'adresse provisoire devient une adresse valide pour l'interface. La première phase de l'auto configuration est achevée.

L'adresse de monodiffusion globale IPv6 est créée en combinant le préfixe indiqué dans l'annonce de routeur et un ID d'interface obtenu via le processus EUI-64 ou généré de manière aléatoire.

II)DHCPv6 sans état (annonce de routeur et DHCPv6)

L'option DHCPv6 sans état enjoint le client à utiliser les informations dans le message RA du routeur pour l'adressage, mais les paramètres de configuration supplémentaires sont fournis par un serveur DHCPv6. Le client crée son adresse de monodiffusion globale IPv6 à l'aide du préfixe et de la longueur de préfixe indiqués dans le message RA du routeur, et de l'IID généré via le processus EUI-64 ou aléatoirement. Ce processus est appelé DHCPv6 sans état, car le serveur ne conserve aucune information sur l'état des clients (c'est-à-dire une liste des adresses IPv6 disponibles et attribuées). Le serveur DHCPv6 sans état fournit uniquement des paramètres de configuration pour les clients et non pour les adresses IPv6.



https://www.reseaucerta.org/sites/default/files/Pratique-IPv6-DHCPv6-01-Sujet.pdf

Sur le routeur on configure une étendue DHCPv6 « sansetat » comportant seulement l'option du serveur DNS avec les commandes :

Ipv6 dhcp pool « nomettendu » et ***dns-server « qdresse du serveur »***

Sur l'interface Fa0, on relie l'interface à l'étendue DHCPv6 : ***ipv6 dhcp server sansetat.***

C'est par l'intermédiaire de deux indicateurs de configuration des adresses, figurant dans le message d'annonce du routeur RA, que le client connaît le type de d'auto configuration IPv6 proposé (SLAAC, SLAAC + DHCPv6 sans état ou DHCPv6 avec état) : Indicateur O (« autre ») et indicateur M.

Dans le cadre d'une configuration de type SLAAC + DHPv6 sans état, il faut positionner l'indicateur O à la valeur 1. L'indicateur M est par défaut à 0.

Les différentes combinaisons des indicateurs M et O	M	O
SLAAC (annonce de routeur uniquement)	0	0
DHCPv6 sans état (annonce de routeur et DHCPv6)	0	1
DHCPv6 avec état (DHCPv6 uniquement)	1	0

https://www.reseaucerta.org/sites/default/files/Pratique-IPv6-DHCPv6-01-Sujet.pdf

La commande ***ipv6 nd other-config flag*** modifie la valeur de l'indicateur de configuration « autre » dans le message RA. Il indique aux clients que des informations supplémentaires sont disponibles auprès d'un serveur DHCPv6 sans état.

III) DHCPv6 avec état (DHCPv6 uniquement)

L'auto configuration avec état vise à réduire les efforts d'installation des machines IPv6, tout comme l'auto configuration sans état d'ailleurs. À la différence de cette dernière, elle offre une information de configuration plus riche et un contrôle sur l'affectation des paramètres de configuration.

Cette option est la plus proche de DHCPv4. Dans ce cas, le message RA du routeur enjoint le client de ne pas utiliser les informations qu'il contient. Toutes les informations d'adressage et de configuration doivent être obtenues auprès d'un serveur DHCPv6. On parle de DHCPv6 avec état, car le serveur DHCPv6 maintient à jour les informations relatives à l'état des adresses IPv6. Le principe est similaire à celui d'un serveur DHCPv4 attribuant des adresses pour IPv4

IV) Le Processus EUI-64 et détection d'adresses double

Dans les méthodes ***SLAAC*** et ***DHCP Stateless***, la machine qui se configure ne reçoit que, au maximum les 64 premiers bits de l'adresse IPv6, il lui reste à définir les 64 derniers afin de constituer son adresse complète. Pour cela deux techniques existent:

- Génération selon le format EUI-64
- Génération « aléatoire » des 64 derniers bits

IV.1) Le Processus EUI-64

EUI-64 pour "Extended Unique Identifier" ou "identifiant unique étendu" [1] est une façon de former les adresses IPv6 de type unicast. On dit de cette méthode de formation des adresses qu'elle est unique car elle se base, pour se former, de l'adresse MAC de la carte réseau qu'elle utilise. Pour rappel, les adresses MAC sont des identifiants codés sur 48 bits uniques à chaque carte réseau.

Concrètement, cela permet à un hôte de s'attribuer à lui-même une adresse IPv6. C'est un plus par rapport à l'IPv4 qui nécessitait aux postes, pour avoir une IP afin de communiquer, de repérer un serveur DHCP et de lui demander un IP.

Nous allons maintenant voir comment se calcule une adresse IPv6 en EUI-64

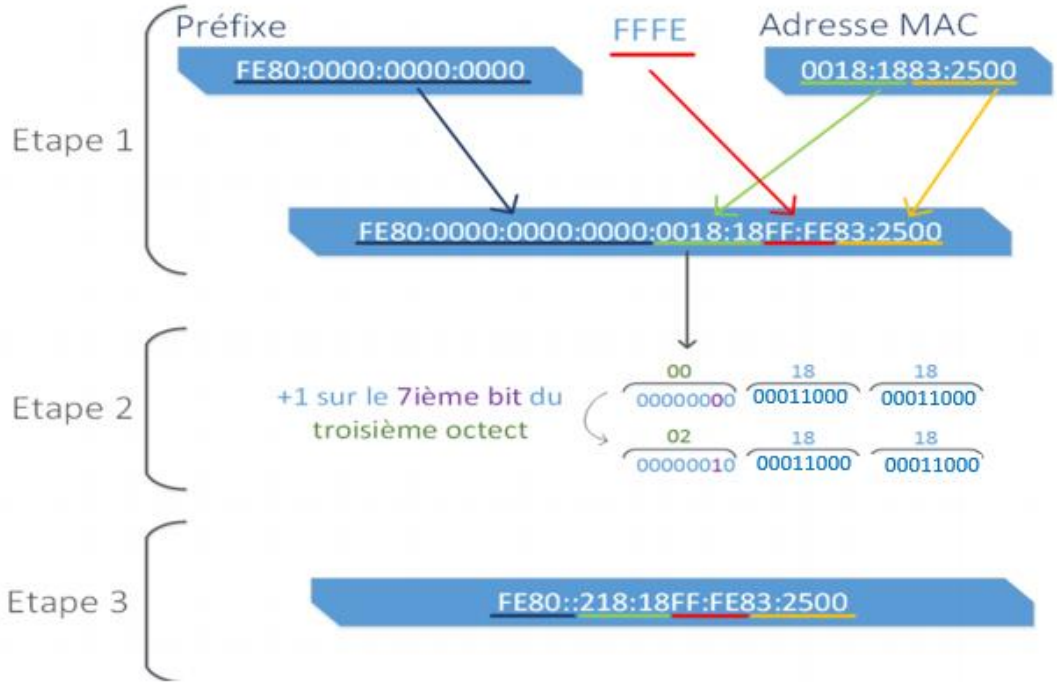


Figure 17 : Fonctionnement de l'EUI-64

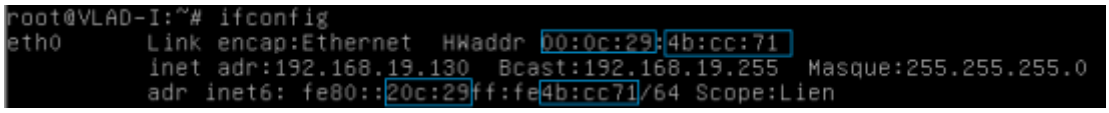
Source : https://www.it-connect.fr/ipv6-quest-ce-que-leui-64-13/

On voit donc que le processus de formation de l'adresse IPv6 en EUI-64 se fait en trois étapes.

- D'abord on prend le préfixe qui est ici "FE80:0000:0000:0000" et l'adresse MAC ici "0018:1883:2500" de la carte réseau concernée. On les combine en prenant le préfixe + 3 premiers octets de l'adresse MAC + **FFFE** + 3 derniers octets de l'adresse MAC

- Ensuite, on effectue une modification sur le septième bit du troisième octet sur lequel on va faire un "+1" modifiant ainsi sa valeur en décimal
- Pour finir, on écrit l'adresse IPv6 finale en enlevant les "0" inutiles.

Nous avons maintenant notre adresse IPv6 (repérable par le "FFFE" entre le 4ième et le 5ième octet de l'adresse MAC) formée en EUI-64



Source : https://www.it-connect.fr/ipv6-quest-ce-que-leui-64-13/

IV.2) Détection d'adresse en double (DAD)

Elle permet de vérifier qu'une adresse IPv6 d'origine est unique sur le réseau local avant que l'adresse ne soit affectée à une interface physique.

Après la réception d'une requête RS, un routeur envoie des informations concernant les préfixes disponibles par le billet d'un message RA. L'interface qui a envoyé la requête RS configure son adresse IP en utilisant les informations contenues dans le message RA qu'il ajoute à l'identifiant interface généré de manière aléatoire ou par EUI-64. Afin d'éviter une double-affectation d'adresses IPv6, l'hôte effectue une détection d'adresses dupliquées (DAD) pour une adresse IPv6 nouvellement générée. Dans ce but, l'hôte envoie une requête à l'adresse générée dans le réseau local. Une adresse Multicast fait office d'adresse de réponse. Lorsqu'une autre station utilise déjà l'adresse IPv6, une réponse est renvoyée. Si aucune réponse de la part de cette adresse n'est envoyée, l'hôte utilise l'adresse IPv6 pour la communication.

V) Routage IPv6

Les principes des protocoles de routage n'ont pas changé avec IPv6. Nous avons toujours besoin d'une adresse IP sur notre interface pour que l'interface soit fonctionnelle au niveau IP. Utiliser une adresse IPv4 ou IPv6 n'affecte en rien la façon dont Ethernet fonctionne ou comment le routeur va router les paquets. Les travaux ont consisté en l'adaptation des protocoles existants au format des adresses.

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Le routage IPv6 est quasiment identique au routage IPv4 sous CIDR (Classless Inter-Domain Routing, routage

inter-domaine sans classe). La seule différence est la taille des adresses qui sont de 128 bits dans IPv6 au lieu de 32 bits dans IPv4.

V.1) Routage statique

Dans le routage statique, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes à emprunter pour aller sur tel ou tel réseau. C'est le même en IPv6 qu'en IPv4, avec bien sûr le préfixe et le next-hop (passerelle) qui sont en IPv6. L'exemple suivant montre comment configurer une route statique par défaut sur un Cisco en IPv4 et en IPv6. Il se réalise à l'aide de la commande en mode configuration globale :

Ipv6 route @ipv6-Réseau/CIDR @ipv6-prochainrouteur ou Ipv6 route @ipv6-Réseau/CIDR Interface-de-sortie

Exemple : *IP route 0.0.0.0 0.0.0.0 10.193.4.1 (*IPv4)

Ipv6 route :: /0 2001 :688 :1F80 :12 ::2 (IPv6)

V.2) Routage dynamique

Le routage dynamique permet quant à lui de se mettre à jour de façon automatique grâce aux protocoles de routage (par exemple : RIPng et OSPFv3). La définition d'un protocole de routage va permettre aux routeurs du réseau de se comprendre et d'échanger les informations de façon périodique ou événementielle afin que chaque routeur soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau. Le routage dynamique comprend le routage interne et le routage externe.

V.2.a) Routage interne

Les protocoles utilisés dans le routage interne permettent une configuration automatique des tables de routage à l'intérieur d'un même système autonome. Les routeurs découvrent automatiquement la topologie du réseau et ***déterminent le plus court chemin*** pour atteindre un réseau distant. Les protocoles essentiellement utilisé dans le routage interne sont : ***RIPng*** (équivalent de RIPv2 pour IPv4), ***OSPFv3*** (équivalent d'OSPFv2 pour IPv4) et ***ISIS***.

I.1.a.1 **RIPng**

C'est protocole à vecteur de distance ("distance vector" en anglais), c'est-à-dire qu'il attribue un coût à chaque lien en fonction de divers paramètres (type du lien...).

Les routeurs diffusent leurs tables de routage sur les liens auxquels ils sont connectés. Les autres routeurs modifient une route dans leur table si la métrique reçue (dans ce cas le nombre de routeurs à traverser pour atteindre une destination) est plus petite que celle déjà stockée dans la table. Si une annonce de route n'est pas présente dans la table, le routeur la rajoute. Ces modifications sont à leur tour diffusées sur les autres réseaux auxquels sont connectés les routeurs. Elles se propagent donc sur l'ensemble du réseau à l'intérieur du système autonome. On montre que cet algorithme converge et qu'en condition stable, aucune boucle n'est créée sur le réseau (c'est-à-dire qu'un paquet ne sera pas transmis indéfiniment de routeur en routeur sans jamais pouvoir atteindre sa destination).

Les tables sont émises périodiquement. Si un routeur tombe en panne ou si le lien est coupé, les autres routeurs ne recevant plus l'information suppriment l'entrée correspondante de leur table de routage.

RIPng est le premier protocole de routage dynamique proposé pour IPv6. Il est une simple extension à IPv6 du protocole RIPv2 d'IPv4. Il en hérite les mêmes limitations d'utilisation (maximum de 15 sauts par exemple). Les paquets RIPng sont émis vers l'adresse de multicast all-rip-router ***FF02::9*** et encapsulés dans un paquet UDP avec le numéro de port 521. Le routage RIP s'initialise dans le processus rip au niveau global de la configuration à l'aide de la commande :

Router (config)# ***ipv6 router rip « nom »***

Et son activation se fait ensuite par interface avec la commande :

Router (config-if)# ***ipv6 rip « nom » enable***

<u>Nb</u> : le nom est une chaine de caractères que vous définissez vous-même.

I.1.a.2 **OSPFv3**

Ce protocole de routage interne, basé sur l'algorithme du plus court chemin, s'appelle OSPF (*Open Shortest Path First*). Relativement plus difficile à mettre en œuvre que ***RIPng***, il est beaucoup plus efficace dans les détections et la suppression des boucles dans les phases transitoires. Ce protocole est basé sur plusieurs sous-protocoles, dont un qui permet une

inondation fiable du réseau. Les routeurs possèdent alors chacun une copie des configurations de tous les routeurs présents sur le réseau, et peuvent calculer simultanément le plus court chemin pour aller vers l'ensemble des destinations.

Pour réduire la durée des calculs et surtout pour éviter un recalcule complet des routes à chaque changement de configuration, ***OSPF*** offre la possibilité de découper le réseau en aires. Une aire principale appelée backbone relie toutes les autres aires. Les réseaux trouvés dans une aire donnée sont envoyés aux autres aires par les routeurs qui sont en frontière d'aire.
OSPF a été adapté à IPv6; la version est passée de 2 à 3. La plupart des algorithmes implémentés dans OSPFv2 ont été réutilisés en ***OSPFv3*** ; bien évidemment, certains changements ont été nécessaires en vue de l'adaptation aux fonctionnalités d'IPv6.

Au niveau global on définit les paramètres globaux au processus ***OSPF***, en précisant les règles d'importations de routes avec la commande suivante:

Router (config)# ***ipv6 router ospf « Process ID »***

Remarque

Le « process ID » est le numéro du processus OSPF qui est lancé sur le routeur. On fixe une valeur locale au routeur qui n'a rien à voir avec les numéros de zones (area).

Au niveau interface, on active OSPFv3 en précisant l'«area» à l'aide de la commande :

(config-if)# ***Ipv6 ospf*** < Process ID > ***area*** <area-id>

V.2.b) Routage externe

La seconde famille des protocoles de routage concerne le routage externe. Le terme externe vient du fait qu'il s'agit d'un échange d'informations de routage entre les deux domaines d'administration distincts que sont les ***systèmes autonomes***. Ces systèmes autonomes sont de deux types : les ***systèmes autonomes terminaux*** (exemple celui d'un client) et les ***systèmes autonomes de transit*** (exemple celui d'un fournisseur d'accès IP). Pour les systèmes autonomes de transit, l'usage de BGP est impératif. Pour les systèmes autonomes terminaux l'usage de BGP est nécessaire dès que le système autonome est multi-connecté (par exemple pour gérer dynamiquement le back-up d'un fournisseur d'accès par un autre).

En IPv4 comme en IPv6, cette notion de domaine d'administration est représentée par un numéro de système autonome codé actuellement sur 2 octets (AS : Autonomous System).

Cette notion de système autonome permet de traiter le problème du routage global de l'Internet (150 000 routes annoncées début 2002) en limitant la complexité. En effet, chaque système autonome (qui peut contenir un grand nombre de routeurs) et ses N routeurs de bord est équivalent pour BGP à un unique routeur virtuel avec N interfaces. La complexité interne au système autonome est donc masquée à l'extérieur de celui-ci.

Avec un protocole de routage externe, il ne s'agit plus de trouver la topologie du réseau, mais d'échanger des informations de routage et de les traiter pour éliminer celles qui ne sont pas pertinentes ou contraires à la politique de routage définie pour le site. En effet, toute annonce de réseau par un domaine implique qu'il accepte de router les paquets vers cette destination.

Conclusion

En plus des deux méthodes d'attribution d'adresse de IPv4 (Statique et DHCP), IPv6 nous une autre méthode à savoir SLAAC qui s'utilise seul ou complété par le DHCP.

Quant aux principes des protocoles de routage, ils n'ont pas changé avec IPv6. Nous avons toujours besoin d'une adresse IP sur notre interface pour que l'interface soit fonctionnelle au niveau IP. Utiliser une adresse IPv4 ou IPv6 n'affecte en rien la façon dont Ethernet fonctionne ou comment le routeur va router les paquets. Les travaux ont consisté en l'adaptation des protocoles existants au format des adresses.

chapitre IV) Etudes des différents mécanismes de migration d'IPv4 vers IPv6

Introduction

Une fois le protocole IPv6 créé, il ne reste plus qu'à le déployer [1], afin de remplacer le vieux IPv4, et de bénéficier de tous les avantages d'IPv6. C'est alors qu'un autre problème se présente : la transition d'un protocole à l'autre.

Figure 18: Absence de passerelle ou de compatibilité entre IPv4 et IPv6

En effet, les transitions ne sont jamais faciles, et celle-ci n'est pas une exception. D'autant plus que la dimension mondiale d'internet rend une transition rapide impossible.

Les créateurs d'IPv6 ont maintenant reconnu que la transition prendrait des années, et qu'il est probable que certains hôtes à l'intérieur d'entreprise utiliseront IPv4 indéfiniment. 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 faut se rendre compte que le réseau est panaché, et que des hôtes IPv4 ou IPv6 devront communiquer en utilisant un réseau IPv4, un réseau IPv6, ou un réseau mixte. Il existe de nombreuses techniques de transition pour migrer de l'IPv4 à l'IPv6, que l'on peut regrouper en trois catégories :

- Dual-Stack (Double pile)
- Techniques de tunneling
- Techniques de translation.

Chacune de ces catégories fait l'objet d'une description détaillée dans les sous parties de ce chapitre.

I) La technique de la double pile

Le mécanisme de double pile IP (Dual Stack) [13] spécifié par le ***RFC 4213*** consiste à doter chaque équipement du réseau d'une double pile protocolaire et d'affecter une adresse IPv4 et IPv6 à chaque interface réseau. Il s'applique à tous les segments d'un réseau. Il est la préférée des techniques de transition, car elle ne fait intervenir aucun mécanisme de tunneling ou de translation d'adresse. 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, switch, firewall, serveur, etc. comme on peut le voir à la Figure 2.

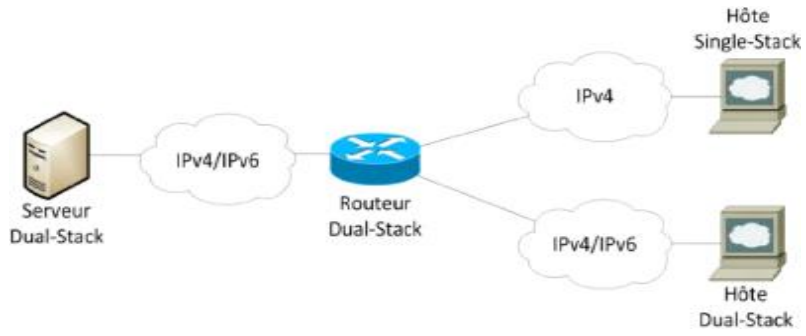


Figure 19:Réseau Dual-Stack (double pile) [1]

Le mécanisme de double pile permet de résoudre les craintes liées à la migration vers IPv6. Dès lors, il ne ***s'agit plus d'une migration mais d'une intégration d'IPv6 dans le réseau existan***t. Le réseau IPv4 reste pleinement fonctionnel et l'intégration d'IPv6 ne risque pas de compromettre le bon fonctionnement des services déployés. En effet, quand cela est possible, la communication se fait en utilisant la nouvelle version du protocole. Dès qu'un des éléments n'est pas compatible (réseau, système d'exploitation, application), le protocole IPv4 est utilisé. Le principal intérêt réside dans ***l'adaptation progressive de son système d'information et de son personnel à IPv6***.

L'avantage principal de cette méthode est de [1] ***pouvoir se connecter aux applications IPv4 existantes via IPv4, tout en ayant accès aux applications IPv6 via le réseau IPv6***. Cependant, comme les deux protocoles fonctionnent simultanément sur une machine, cela peut être couteux en termes de performance et d'utilisation CPU.

En contrepartie, ce mécanisme ***ne prend pas en compte les problèmes de pénurie d'adresses IPv4***. Notons que le déploiement double pile ne doit être que transitoire car il ne résout pas le problème de la pénurie d'adresses puisque chaque machine doit disposer d'une adresse IPv4 et d'une adresse IPv6. Cela complique aussi les mécanismes de configuration automatique et augmente la charge pour l'administrateur réseau. Lors de l'activation d'IPv6 pour un service existant en IPv4, il faut prendre des précautions afin que la qualité perçue par l'utilisateur ne soit pas dégradée.

II)La technique du tunnel

Alors que les portions du réseau internet où l'IPv6 [1] est actif augmentent, une large majorité reste IPv4. Le besoin d'interconnecter ces îles IPv6 à travers le réseau IPv4 s'est donc rapidement fait sentir. C'est pour cela que les techniques de tunneling ont été mises en place pour répondre à ce besoin.

La « tunnélisation » constitue un moyen de faire en sorte que l'infrastructure de routage IPv4 existante reste fonctionnelle mais puisse aussi assurer le trafic IPv6. Les données sont acheminées à travers un tunnel IPv4 selon un processus appelé ***encapsulation***, par lequel le paquet IPv6 passe dans un paquet IPv4. L'encapsulation consiste à ***l'ajout d'un en-tête IPv4 à un paquet IPv6***, afin que ce dernier puisse circuler dans le réseau IPv4 à travers un tunnel, comme illustré à la figure ci-dessous .Autrement dit que les paquets IPv6 seront considérés comme des paquets IPv4 dans le tunnel et à l'entrée et la sortie du tunnel comme des paquets IPv6.

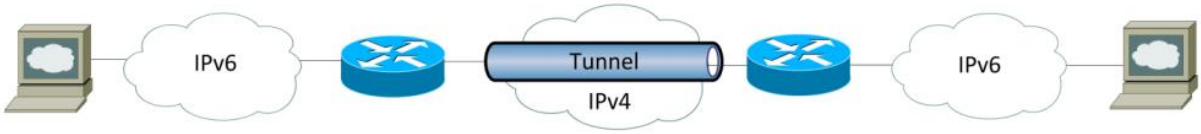


Figure 20:Tunnel d'un paquet IPv6 à l'intérieur d'IPv4

Plusieurs solutions sont disponibles, pour former un tunnel : les paquets IPv6 transitent alors encapsulés dans IPv4, ce qui s'appelle autrement un tunnel IPv4. Nous distinguons les tunnels statiques et les tunnels automatiques.

II.1) Tunnel statique

Les tunnels statiques sont utilisés pour ***relier un réseau ou une machine IPv6 à un réseau IPv6 par l'intermédiaire d'un réseau IPv4***. Ils sont configurés à la main. Les machines qui sont aux extrémités du tunnel doivent avoir une ***double pile IPv4/IPv6*** et disposer chacune d'une adresse ***IPv4 globale***.

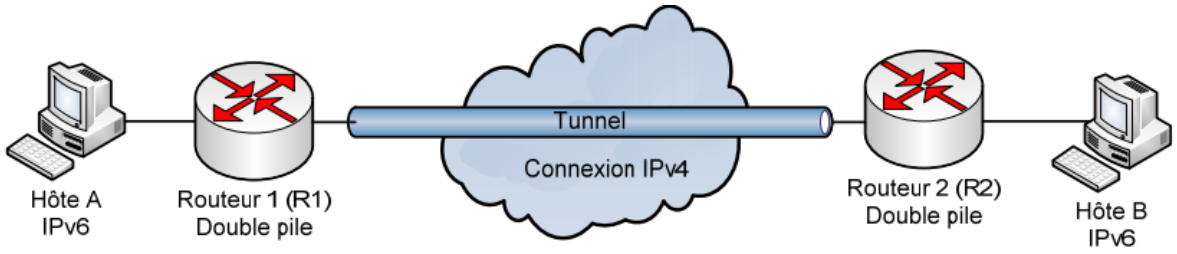


Figure 21:Tunnel statique

Les autres machines du réseau IPv6 n'ont donc pas besoin de ce double pile pour communiquer avec les machines IPv6 situées de l'autre côté du tunnel, mais elle peut être utile pour communiquer avec des machines IPv4 (sans passer par le tunnel).

II.2) Les tunnels semi-automatique et automatiques

Les tunnels automatiques et semi-automatiques servent à communiquer en IPv6 avec une machine connectée sur un réseau IPv4. Cette méthode est souvent utilisée pour ***joindre une machine IPv6 isolée***. Les deux machines établissant le tunnel doivent ***disposer d'une double pile IPv4/IPv6***. La machine de destination du tunnel doit être la machine destinataire du paquet, alors que la machine source du tunnel peut être la machine source du paquet ou un routeur qui a reçu le paquet sur son réseau IPv6. Dans ce cas il faudra que la machine source possède une ***adresse IPv4 compatible***.

Les adresses IPv4 compatibles sont des adresses IPv6 particulières qui sont formées en ajoutant 32 bits d'une adresse IPv4 au ***préfixe ::/96***. Par exemple ::192.168.1.1 est l'adresse IPv4-compatible de 192.168.1.1.

II.2.a) Tunnel broker

La méthode de Tunnel Broker IPv6, décrit dans la RFC 3053, permet à un poste disposant d'une double pile, isolé dans un réseau IPv4, de communiquer vers un réseau natif IPv6 via un tunnel 6over4 configuré de façon semi-automatique.

Le Tunnel Broker [1] est une société tierce fournissant un service de tunnel après une simple demande aux serveurs dédiés appelés « Tunnels Brokers » qui gèrent les demandes de tunnel des utilisateurs. Pour ce faire, il faut généralement ***s'inscrire*** chez le tunnel broker, puis ***demander l'ouverture du tunnel***. Alors, le tunnel broker va configurer un de ses routeurs afin de mettre en place le tunnel. Enfin, il enverra ***un script à exécuter*** sur la machine souhaitant utiliser le tunnel, pour configurer correctement les paramètres réseaux. La machine est alors connectée à l'IPv6 via le service du tunnel broker. Les étapes énumérées ci-avant sont illustrées à la Figure ci-dessous.

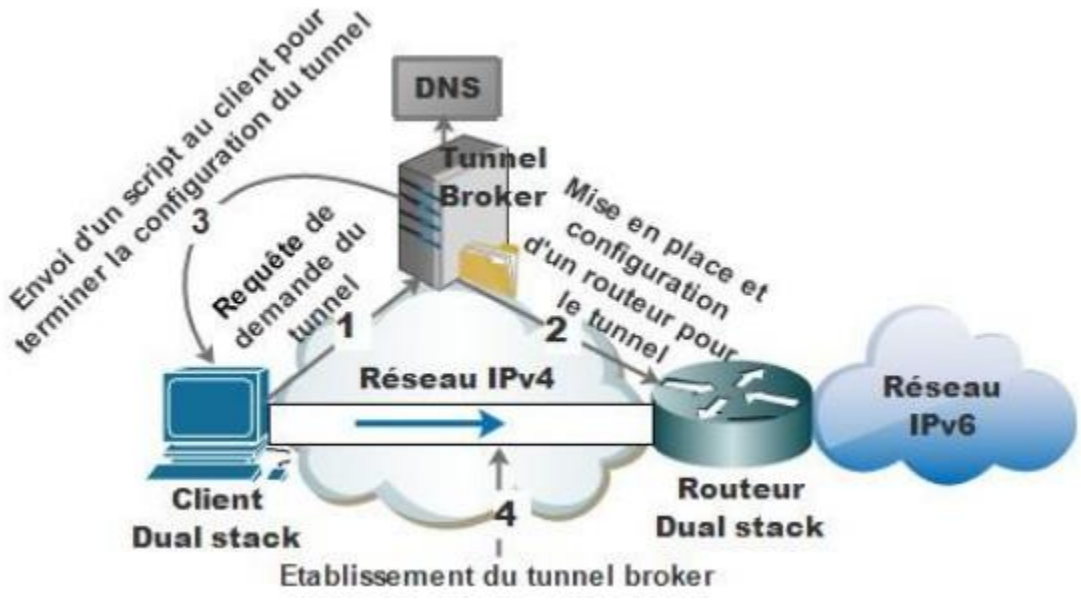


Figure 22: Étapes formation tunnel broker

Avantage :

- Bien adapté pour les petits sites IPv6 isolés et les machines IPv6 isolées sur l'internet IPv4, qui veulent se connecter à un réseau IPv6 existant.

- Mise en place semi-automatique du tunnel après une inscription et demande du tunnel depuis le client.
- Permet à des FAI (Fournisseurs d'Accès à Internet) IPv6 de gérer facilement les contrôles d'accès des utilisateurs, renforçant ainsi leur politique d'utilisation des ressources réseau.

Inconvénients :

- Ne résout pas le problème de la pénurie des adresses IP.
- Les performances dépendent de l'emplacement géographique du routeur du tunnel broker.

II.2.b) ISATAP

ISATAP (Intra-site Automatic Tunnel Addressing Protocol) a été définie pour fournir une connectivité IPv6 à des équipements terminaux ou des routeurs au sein de réseaux IPv4 et pour ainsi permettre un premier déploiement d'applications IPv6, l'infrastructure IPv4 étant vue comme une technologie de niveau liaison.

La méthode ISATAP utilise un format d'identificateur de machine qui inclut l'adresse IPv4. L'adresse ISATAP (voir la figure ci-dessous) est formée d'un préfixe IPv6 global ou lien-local d'une longueur de 64 bits, de l'identificateur propre ***0000:5EFE*** et enfin des 32 bits de l'adresse IPv4 identifiant l'interface.

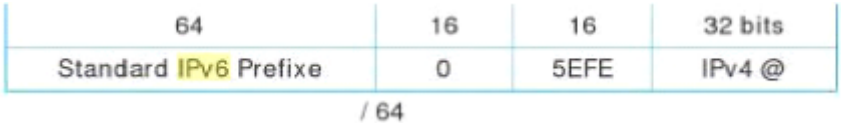


Figure 23:Format de l'adresse ISATAP

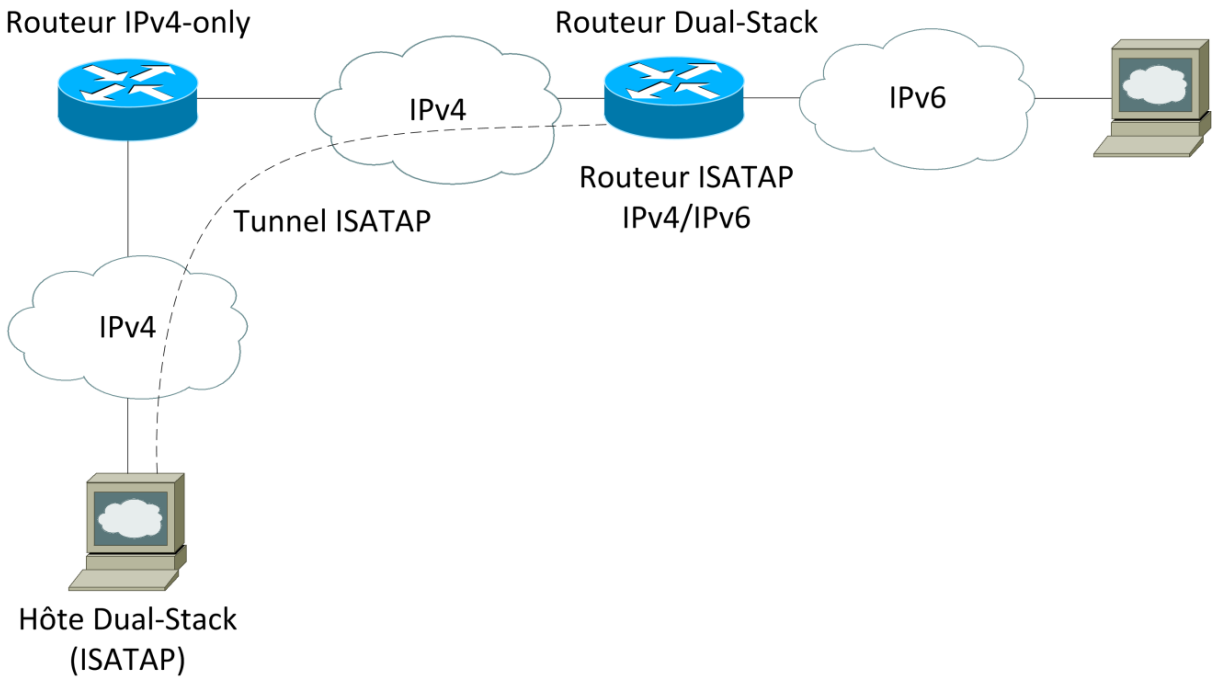


Figure 24: Tunnel ISATAP

Il faut toutefois noter qu'***ISATAP ne supporte pas le NAT, ni le multicast***.

II.2.c) 6to4

Décrit dans la RFC 3056, la méthode 6to4 est un mécanisme de tunnel automatique qui est utilisé pour relier des réseaux IPv6 isolés à travers des réseaux IPv4 en établissant des tunnels de manière implicite.

L'avantage du 6to4 réside dans sa simplicité car elle évite à l'administrateur de configurer les tunnels à la main. Par ailleurs, une seule adresse IPv4 est consommée par LAN IPv6, ce sont des tunnels 6to4 multipoints, et non point-à-point. Une autre particularité est que ce n'est pas un tunnel à proprement parlé. En effet, cela fonctionne en utilisant le ***préfixe réservé 2002::/16 directement suivi de l'adresse IPv4 du routeur 6to4 auquel l'hôte est connecté,*** comme on peut le voir à la Figure ci-dessous. Les 16 bits suivants sont utilisés pour désigner un sous-réseau, et les 64 derniers pour déterminer l'identifiant de l'interface de l'hôte (adresse MAC). Les routeurs 6to4 sont ensuite responsables d'extraire l'adresse IPv4 du routeur de destination à partir de l'adresse IPv6 de destination, et enfin d'encapsuler le paquet IPv6.

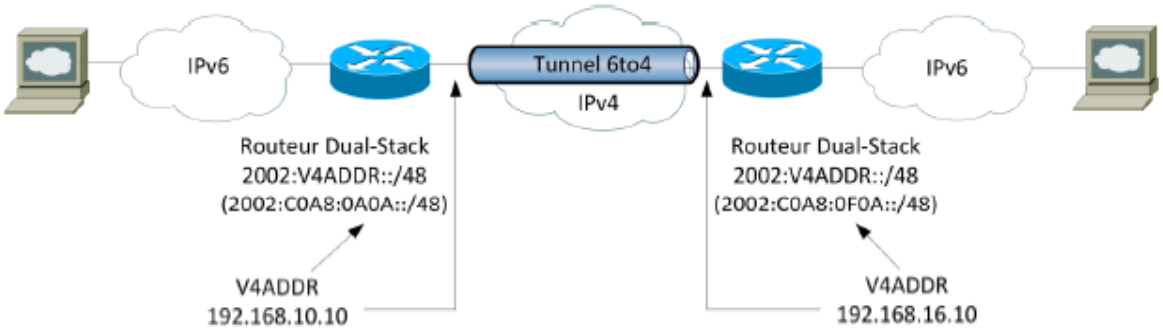


Figure 25: architecture 6to4

Cependant il existe quelques problèmes liés à cette technique. Ce sont entre autres :

- Elle est limitée par le nombre d'adresses IPv4 publiques, puisqu'il est obligatoire pour un routeur d'en posséder une.
- Elle ne supporte pas qu'un NAT soit sur le chemin.
- Elle ne supporte pas l'utilisation du multicast.

I.1.a.3 **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/IPv4. Ce paquet sera donc constitué d'un en-tête IPv4, suivi d'un en-tête UDP, puis d'un en-tête IPv6, et enfin des données IPv6. Une adresse Teredo commence toujours par le ***préfixe 2001::/32***. Il faut noter que ce protocole développé par Microsoft s'adapte automatiquement au type de Nat qu'il doit traverser.

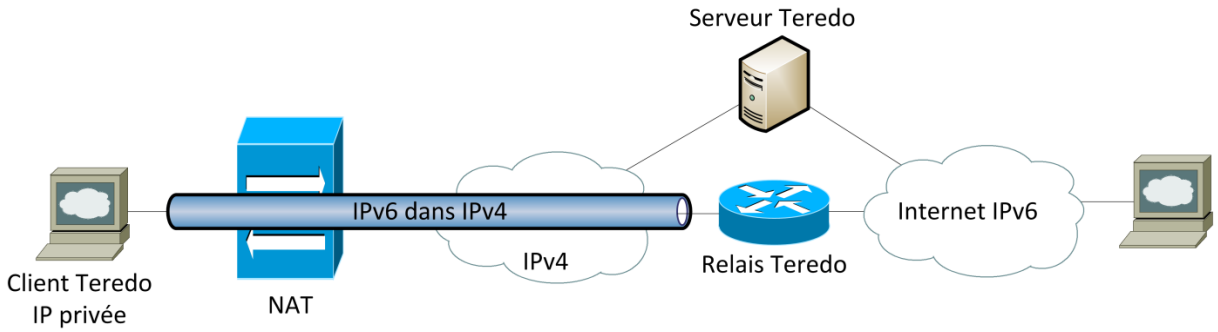


Figure 26: Teredo

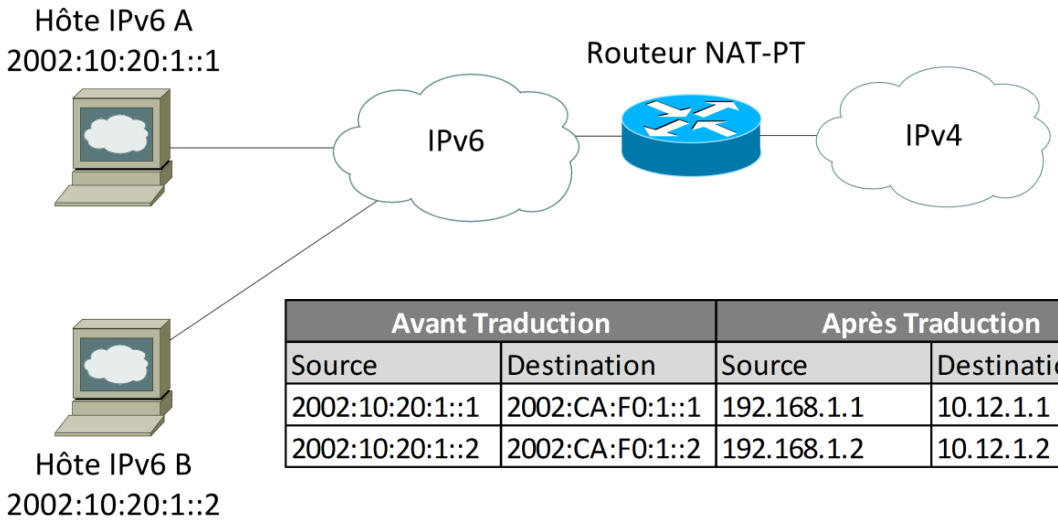
L'infrastructure Teredo est composée d'un client, d'un relais et d'un serveur Teredo, comme illustré à la Figure 9. Le serveur Teredo assiste un client dans sa configuration d'adresse en découvrant son adresse et son port, et facilite la communication entre clients Teredo. Le relais Teredo transmet les paquets à un hôte IPv6. Il existe encore un relais *host-specific* dual-stack, qui peut communiquer directement avec les clients Teredo.

III) Techniques de translation

Ce type de technique repose sur le même principe que NAT actuel, sauf qu'il permet à un ***réseau interne purement IPv6 de communiquer avec le monde IPv4*** en réalisant une traduction entre ces deux mondes. Les réseaux étant encore majoritairement en IPv4, il est nécessaire de devoir garder contact avec eux.

III.1) Network Address Translation-Protocol Translation (NAT-PT)

Le protocole de translation NAT-PT fonctionne comme le NAT actuel et souffre des mêmes limitations que ce dernier. Il fournit des possibilités de traduction bidirectionnelle. Pour assurer la communication entre ces deux mondes, ***des paquets envoyés par un hôte IPv6 vers un hôte IPv4 devront avoir leurs adresses source et de destination changées en IPv4 (par le routeur officiant le NAT-PT) et inversement***.



Avant Traduction		Après Traduction	
Source	Destination	Source	Destination
2002:10:20:1::1	2002:CA:F0:1::1	192.168.1.1	10.12.1.1
2002:10:20:1::2	2002:CA:F0:1::2	192.168.1.2	10.12.1.2

Figure 27: le NAT-PT

Un préfixe, fixé à ***2001::/96*** (préfixe de base, pouvant être remplacé par n'importe quel autre préfixe) permet aux hôtes IPv6 de contacter un hôte IPv4. Chaque hôte IPv4 sera vu par le réseau IPv6 comme ceci :

2001 ::<IPv4 de destination en hexadécimale>

Par exemple, l'hôte IPv4 avec l'adresse ***192.168.3.174*** sera vu par un hôte IPv6 comme ayant l'adresse ***2001::C0A8:3AE***. Une règle de NAT doit être instaurée entre les deux adresses.

Une table de correspondance entre les adresses IPv6 et IPv4 se sera créer par le routeur faisant office du NAT. Pour ce faire, quand le routeur reçoit un paquet d'un hôte IPv6, il va reconnaître que le préfixe utilisé est celui du NAT-PT et retirer les 32 derniers bits qui correspondent à l'adresse IPv4 de destination de l'adresse IPv6 de destination

Comme le NAT, il existe plusieurs types de translation possible :

- Statique : A une adresse IPv4 correspondra une adresse IPv6 et vice-versa. Une règle de translation doit être fixée pour chaque hôte.
- Dynamique : Un pool d'adresses IPv4 est disponible pour les translations. A chaque adresse IPv4 correspond un hôte IPv6 sortant.

- PAT (Port Address Translation) : Permet à de multiples adresses IPv6 de correspondre à une adresse IPv4 en utilisant le numéro de port.

Pour des problèmes de sécurité, de stabilité et d'autres, cette technologie a été dépréciée par l'***IETF*** en 2007 dans la RFC 4966. C'est la première technologie mise au point pour ce type de cas.

Ce dernier est couplé avec un service de type **DNS-ALG** (une application permettant la traduction des requêtes ***DNS*** entre les deux mondes ***v6*** et ***v4***). Ce mécanisme de ***DNS-ALG*** est utilisé conjointement au ***NAT-PT*** pour ***assurer le service DNS au réseau IPv6***. Il permet la traduction des réponses DNS IPv4 embarquées dans les paquets IPv4 en réponses DNS IPv6.

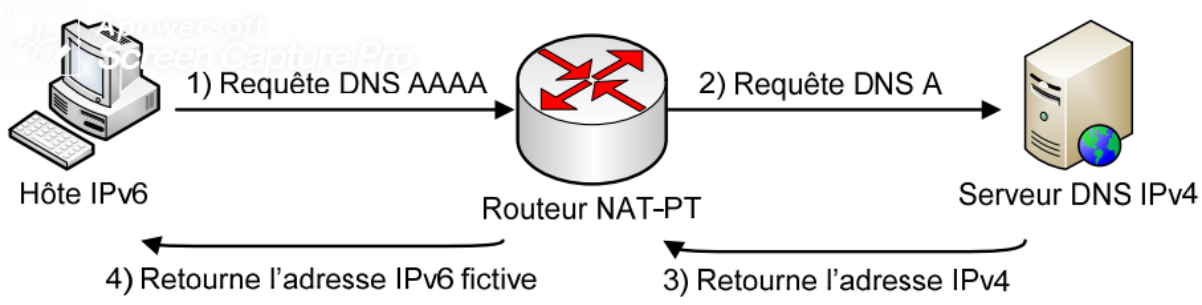


Figure 28:Fonctionnement de DNS-ALG

L'hôte IPv6 commence par émettre une requête AAAA au DNS IPv4. Le routeur, interceptant le paquet, va traduire celle-ci en requête d'adresse IPv4. Le serveur va alors retourner un enregistrement IPv4 du site internet au routeur, qui lui va ajouter le préfixe à celle-ci avec l'aide du DNS-ALG afin de créer une requête DNS AAAA fictive et la transmettre à l'hôte. Ce dernier pourra alors directement se connecter à la page internet grâce au mécanisme IPv4-mapped.

III.2) NAT64/DNS64

Le couplage des protocoles *NAT64* et *DNS64* est la solution la plus actuelle au problème de communication entre les machines IPv6 et IPv4. Ces technologies succèdent au protocole *NAT-PT* qui a été dépréciée par l'IETF. Les deux sont interdépendantes et nécessaires pour réaliser la communication.

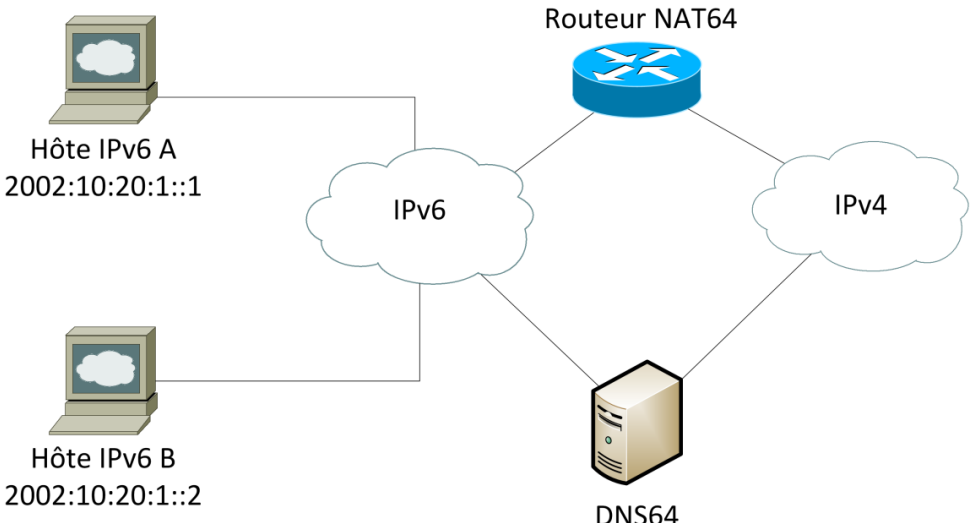


Figure 29: NAT64/DNS64

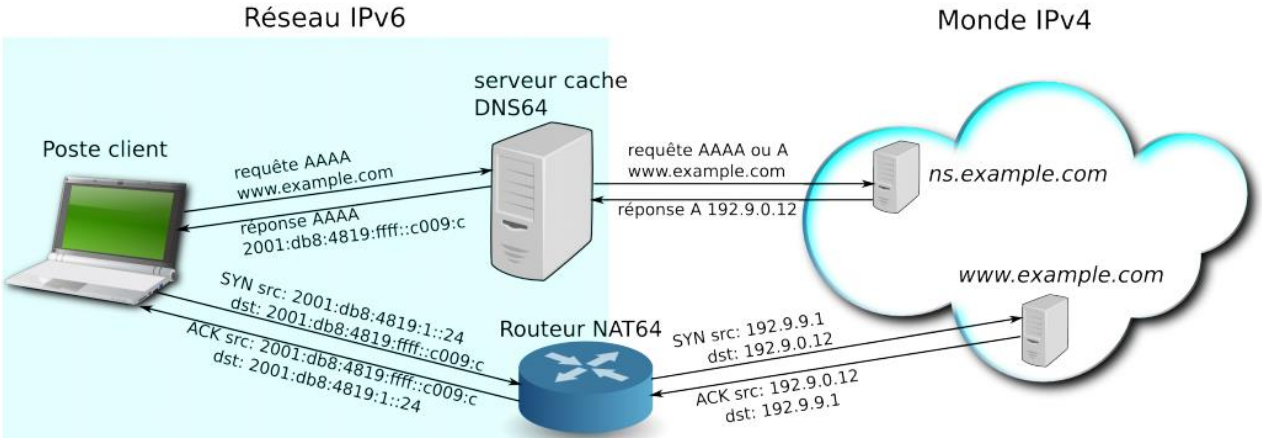


Figure 30: Principe de fonctionnement de NAT64/DNS64

III.2.a) DNS64

Le protocole DNS64 (RFC 6147) agit comme un DNS normal. Il gère les deux cas de demande de résolution de nom de domaine, c'est-à-dire celles avec un nom de domaine IPv4 et celles avec un autre en IPv6 :

Pour la résolution d'un nom de domaine IPv6, tout se passe avec ce protocole. Le client envoie cette requête au serveur DNS64, qui lui va interroger le serveur DNS pour obtenir l'adresse IPv6, et la renvoyer à l'hôte. Dans le cas où le serveur DNS du site web possède seulement un enregistrement IPv4, c'est un peu différent. Le serveur DNS64 va essayer dans un premier temps

d'obtenir un enregistrement AAAA. Le serveur web va alors retourner un message vide signalant qu'il ne possède pas d'adresse IPv6. Le serveur DNS64 va alors renvoyer une requête DNS A. Il va récupérer l'adresse et l'encapsuler à l'aide d'un algorithme dans une adresse IPv6. Une fois cela effectué, il va envoyer cette adresse IPv6 à l'hôte.

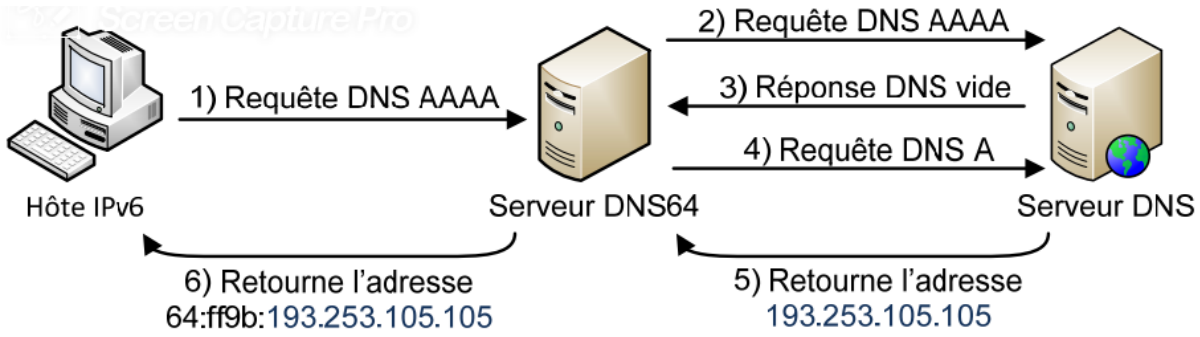


Figure 31: DNS64

L'encapsulation ici utilise le même procédé que le NAT-PT, c'est-à-dire l'utilisation d'un préfixe, ici ***64:ff9b/96*** et de l'adresse IPv4 pour former une adresse IPv6. On peut clairement voir que le DNS64 a remplacé le mécanisme DNS-ALG présent dans le NAT-PT.

III.2.b) NAT64

Le protocole NAT64 (RFC 6146) est l'intermédiaire qui va réaliser la communication entre le réseau IPv6 et celui en IPv4. Vu que le serveur ***DNS64*** a renvoyé une adresse IPv4 encapsulée dans une IPv6, le ***NAT64*** devra se charger de décapsuler le paquet IPv4 pour le transmettre plus loin, mais également gérer le retour d'information et la ré-encapsulation pour les communications entrantes.

Comme son homologue NAT-PT, il va regarder le type de trafic qu'il reçoit. Si celui-ci embarque le préfixe ***64:ff9b/96***, il va le décapsule et l'envoyer sur sa patte IPv4. Sinon, il envoie directement le trafic sur sa patte IPv6.

IV) Synthèse

Action	Tunnel	traduction	Double pile
Relier deux réseaux IPv6 distant	👍	👎	👍

Relier un réseau purement IPv6 à celui pure IPv4	👎	👍	👎
Nécessite l'utilisation d'un autre mécanisme	👍	👎	👎
Transformation du paquet source	👍	👍	👎
Pas besoin de connaitre la pile du ou des réseau(x) de destination	👎	👎	👍
Supporte le NAT	👎(sauf teredo)	👍	👍
Se Familiariser progressivement à IPv6	👎	👎	👍

Tableau 3: Synthèse sur les mecanismes de transition

Legendre du tableau :

👍 : permet de le faire

👎: permet de le faire

Conclusion

La proche pénurie d'IPv4 aidant, fort est à parier qu'IPv6 a de beaux jours devant lui. Tant qu'IPv4 sera présent, ce qui sera le cas encore surement quelques années voir beaucoup plus, il faudra assurer un contact avec ce monde grâce aux différentes techniques vues dans ce dossier. À terme, espérons qu'il n'y aura plus besoins de les utiliser (ou sporadiquement) et qu'on verra enfin apparaitre une connectivité IPv6 générale qui montrera les pleines capacités du protocole.

Dans le cas des entreprises ou des écoles, plusieurs solutions peuvent donc être mises en place:

- La double pile native est de loin la plus facile à installer et la plus robuste
- Une solution à base de tunnel peut être instaurée de différentes manières, cela permet d'obtenir une connectivité IPv6 fonctionnelle, réactive et stable
- Elles peuvent également essayer de se passer totalement de l'IPv4 dans le réseau interne en mettant en place des techniques de translation comme le NAT-PT (en plus d'un accès IPv6). Après expérimentations, cette solution ne semble pas encore complètement au point et souffre encore de trop nombreux défauts pour être jugée comme acceptable. Le couplage

NAT64/DNS64 semble corriger la majorité des défauts du NAT-PT, et a déjà été testé à petite ou grande échelle avec plus ou moins de succès et pourrait donc être utilisé également, mais avec précaution.

Bien évidemment, chacune des solutions est à utiliser selon les disponibilités du fournisseur d'accès, les moyens matériels mis à disposition et les connaissances requises pour leur implémentation.

chapitre V) Le choix du mécanisme et sa mise en œuvre

Introduction

Les mondes IPv4 et IPv6 sont par nature indépendant [1] l'un de l'autre et il n'est pas possible de communiquer nativement du monde IPv4 vers IPv6 et inversement.

Ceci dit, la disparition progressive d'IPv4 ne se produit pas à la même vitesse sur l'ensemble de la planète. La partie APAC 3 a été la première plaque régionale à manquer d'adresses et l'IPv6 est plus largement déployées chez eux que sur la plaque du RIPE. Et portant, on remarque bien la présence de flux venant d'Asie vers les ressources IPv4 : il n'y a qu'à observer les logs SSH pour s'en convaincre.

Afin de permettre ces communications, différents groupes de travail ont publiés plusieurs méthodes permettant de faire des passerelles entre les 2 mondes ou de transporter le monde IPv6 par-dessus le monde IPv4.

I) Le choix du mécanisme

I.1) Mécanismes de tunnels

Ces méthodes permettent en général de relier des ilots IPv6 entre eux à travers une infrastructure IPv4. Ainsi, on va retrouver des mécanismes tels que tunnel broker, 6in4, 6to4, GRE, TEREDO, ISATAP…

Tous ces mécanismes ne permettent pas de passer d'un monde à l'autre mais bel et bien de relier des environnements IPv6 entre eux bien que ceux-ci soient séparés par le monde IPv4. La mise en place est soit automatique, soit manuelle. Dans tous les cas, cette méthode permet d'obtenir une connectivité IPv6 même si le FAI ne le fournit pas nativement.

Les principaux problèmes sont :

- ✓ Ne supporte pas le NAT, ni le multicast si le tunnel implémenté est ISATAP, 6to4 ;
- ✓ **6to4 tunnel** est limitée par le nombre d'adresses IPv4 publiques, puisqu'il est obligatoire pour un routeur d'en posséder une.

[3] APAC ou L'Asie-Pacifique est un ensemble géographique constitué de l'Extrême-Orient, du sous-continent indien et de l'Océanie.

- ✓ Les limitations principales du tunnel broker sont d'une part les performances, l'emplacement géographique du routeur du tunnel broker jouant un rôle important ;

I.2) Mécanismes de traduction et translation

On vient de voir qu'il était possible de créer des liens à travers les différents univers, mais il n'est toujours pas possible de fournir un accès depuis un univers à un autre de manière automatique. C'est l'objectif des mécanismes de traduction qui vont permettre de mettre en place des passerelles.

I.3)Mécanismes de la double pile (Dual-Stack)

Le dual-stack est la préférée des techniques de transition, car elle ne fait intervenir aucun mécanisme de tunneling ou de translation d'adresse. 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, switch, firewall, serveur, etc.

L'avantage principal de cette méthode est de pouvoir se connecter aux applications IPv4 existantes via IPv4, tout en ayant accès aux applications IPv6 via le réseau IPv6. Donc avec ce mécanisme, les périphéries qui n'ont qu'une des piles (IPv4 ou IPv6) continueront à fonctionner.

Cependant, comme les deux protocoles fonctionnent simultanément sur une machine, cela peut-être coûteux en termes de performance et d'utilisation CPU.

Notre choix porte sur la double pile.

I.4) Argumentaire de notre choix

Ici nous avançons l'argument qui nous a poussés à choisir le Dual stack comme solution :

- Après une enquête menée auprès de quelques utilisateurs nous avons constaté que la majorité des équipements d'utilisateurs implémentent IPV4/IPV6
- Nous ne sommes pas en train de relier le réseau IPv6 de l'AUSZ à un réseau IPv6 pour utiliser le tuneling

- Nous ne relions pas également le réseau IPv4 de l'UASZ à un réseau IPv6 pour utiliser la traduction/translation.
- Pas besoin de connaitre la pile du réseau de destination.
- Les équipements qui forment le backbone [4]peuvent également fonctionner en double piles.
- Aucune nécessité de redéployer les protocoles et applications……
- tous les équipements du réseau (ancien et nouvelle génération) peuvent se connecter.
- double pile, les utilisateurs du réseau se familiariseront progressivement au nouveau protocole.
- évite la nécessité de traduire entre les deux piles de protocoles
- facile la conversion entièrement en IPv6 à l'avenir
- double pile il n'aura pas d'encapsulation (Tunnel) ni de traduction/translation

Pour toutes ses raison nous avons choisi la technique du Dual Stack que nous allons mettre en œuvre dans la section suivante.

II)Cadre d'application: le réseau de l'UASZ

Afin de mieux aborder cette partie importante du sujet, nous commençons d'abord par faire l'inventaire des équipements du réseau de l'UASZ, des logiciels et/ou applications qui y sont déployés et de l'usage qui en est fait, des types d'utilisateurs. Tout cela combiné à une étude de l'architecture et de la topologie nous a permis de faire une analyse pertinente et de déterminer la solution la plus adéquate pour le réseau de l'université.

II.1) Bilan du matériel

Le réseau de l'UASZ s'étend sur une zone géographique de 1km2 à peu près, il compte près de cinq milles utilisateurs (ordinateurs, tablettes, téléphone etc...), des serveurs, des switchs, des points d'accès et routeurs. Il est composé d'une partie filaire constituée de 10 salles informatiques, des bureaux. Nous y trouvons également les Wifi auxquels, étudiants, enseignants, personnels et même visiteurs se connectent.

[4] Backbone : une partie d'un réseau informatique qui interconnecte divers éléments du réseau, fournissant un chemin pour l'échange d'informations entre différents réseaux locaux ou sous-réseaux.

…..

II.2) Bilan des logiciels

Le réseau de l'UASZ utilise différents types de logiciel, comme Scolarix par exemple, qui sont hébergés en internes…

II.3) Architecture et topologie

La topologie filaire de l'UASZ est composée de switch de niveau 2, de niveau3, de routeur, de points d'accès. Pour des questions de sécurité, nous n'avons pas jugé nécessaire de faire une représentation. Il est structuré autour de différents VLAN déterminés en fonction en des types d'utilisateurs comme par exemple le VLANs pour les étudiants.

III) La mise en place de la double pile

Pour la mise en place de la double, nous avons utilisé comme adresse IPv6 fourni par le FAI **2001 :AAAA :AAAA ::/48** pour la stimulation avec Paket Tracer. Et au niveau du matériels de Cisco nous avons utilisé » le **2001 :1 :1 ::/48.** Avec le préfixe **2001 :AAAA :AAAA ::/48**, nous avons adressé les VLANs , mais aussi **2001:BBBB:BBBB:BBBB::/64** pour le réseau IPv6 distant. Quant à l'adressage lors de la simulation sur Packet tracer, nous avons utilisé SLAAC au niveau des VLANs et statique au niveau des interfaces du routeur.

III.1) Etat des interfaces des équipements du réseau avant la double pile

Avant la configuration de la double pile, les interfaces des équipements avaient la pile IPv4 mais ne disposaient pas de la pile IPv6. Les commandes ci-dessous nous permettent respectivement d'avoir une aperçue sur l'état des interfaces du routeur UASZ concernant la pile IPv4 et celle IPv6.

```
UASZ#
UASZ#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         192.168.0.2     YES NVRAM  up                    up
GigabitEthernet0/1         172.16.0.254    YES NVRAM  down                  down
UASZ#show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0     [up/up]
    unassigned
GigabitEthernet0/1     [down/down]
    unassigned
UASZ#
```

Figure 32 : Exemple : état des interfaces du le routeur UASZ

Et si nous voulons une idée sur la configuration d'une interface particulière, nous utilisons respectivement pour la pile IPv4 et la pile Ipv6 les commandes :

```
UASZ#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.0.2/24
  Broadcast address is 255.255.255.255
```

```
UASZ#show ipv6 interface g0/0
UASZ#
```

Figure 33 : affichage de la configuration d'une interface particulière (g0/0) en IPv4 et IPv6

Au niveau des machines clientes, la double pile existe dans les machines de la nouvelle génération mais pas dans les anciennes machines.

IV) Configuration des interfaces en IPv6

La pile IPv4 existant déjà sur les différentes interfaces des machines de la dernière génération, il ne reste qu'à configurer la pile IPv6 sur ces interfaces.

Comme venu précédemment au niveau du chapitre 3, une interface d'un équipement dispose en plus des méthodes connues par IPv4 à savoir la méthode statique et celle dynamique avec le DHCPv4 correspondant au ***DHCPv6 avec état*** en IPv6, deux autre méthodes dynamiques d'attribution d'adresse IPv6. C'est entre autre : ***SLAAC*** et ***DHCPv6 sans état***.

IV.1) Au niveau des routeurs

Voici l'état initial des interfaces du routeur :

En IPv4 ;

```
UASZ#
UASZ#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         192.168.0.2     YES NVRAM  up                    up
GigabitEthernet0/1         172.16.0.254    YES NVRAM  down                  down
UASZ#
```

Figure 34 : configuration initiale du routeur nommé UASZ en IPv4

En IPv6.

```
UASZ#show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0     [up/up]
    unassigned
GigabitEthernet0/1     [down/down]
    unassigned
UASZ#
```

Figure 35 : configuration initiale du routeur nommé UASZ en IPv6

IV.1.a) Adressage statique (adresse globale)

Pour configurer statiquement une adresse IPv6 sur l'interface d'un routeur, nous saisissons, après être positionné sur l'interface que nous voulons attribuer une adresse la commande : ***Ipv6 address adresse_ipv6/x***.

Exemple: configuration IPv6 sur l'interface G0/0 du routeur UASZ.

```
UASZ(config-if)#int g0/0
UASZ(config-if)#ipv6 address 2001:1:1:1::1/64
UASZ(config-if)#
```

Figure 36 : adressage IPv6 avec la méthode statique de l'interface G0/0 du routeur UASZ

Nous devons aussi activer la pile IPv6 au niveau de chaque interface du routeur où nous voulons configurer cette pile car par défaut IPv6 est désactivé au niveau des routeurs. Et ceci se fait avec l'aide de la commande : ***ipv6 enable.***

À la fin de la configuration d'IPv6, voici les états des interfaces du routeur en IPv6.

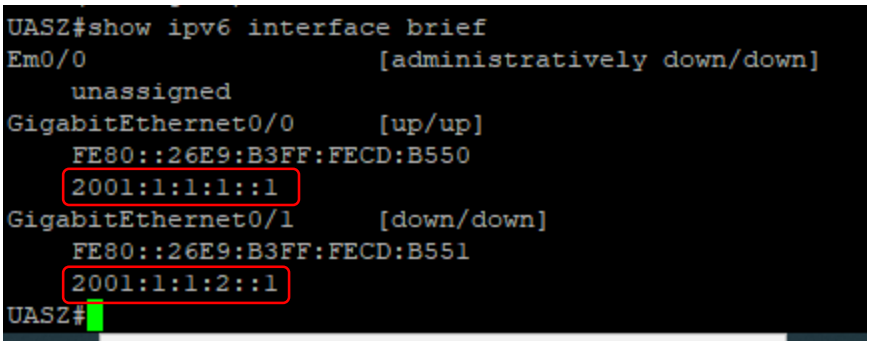


Figure 37 : Affichage de la configuration IPv6 du routeur UASZ

Voici aussi l'état d'une interface spécifique comme par exemple ici l'interface G0/0 du routeur UASZ.

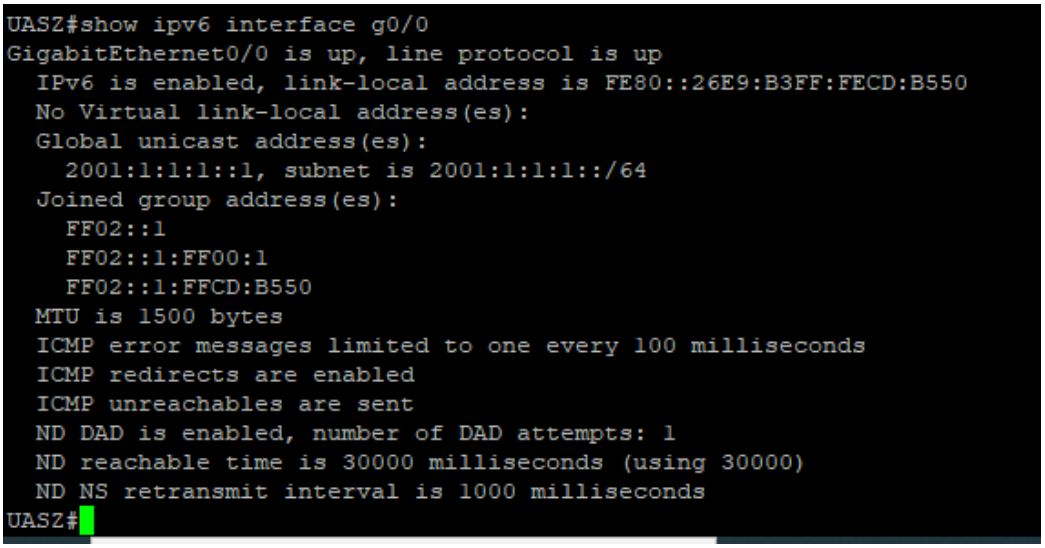


Figure 38 : Affichage de la configuration de l'interface G0/0 du routeur UASZ

Remarque

Nous n'avons configuré qu'une adresse unicast global au niveau de l'interface mais on contacte la présence d'une adresse link-local sur l'interface où IPv6 est activé. Il y a aussi les adresses des groupes multicast auxquels appartient cette interface.

Pour voir la configuration de la double pile, nous affichons la configuration en marche du routeur avec l'aide de la commande : ***show running-config***

```
!
interface GigabitEthernet0/0
 ip address 192.168.0.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:1:1:1::1/64
 no mop enabled
!
interface GigabitEthernet0/1
 ip address 172.16.0.254 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:1:1:2::1/64
!
router rip
 network 172.16.0.0
 network 192.168.0.0
!
```

Figure 39 : la configuration en marche du routeur UASZ

IV.1.b) Adressage dynamique

Pour ce type d'adressage, la partie interface de l'adresse de l'interface est configurée automatiquement (ici avec le processus EUI-64). Cela s'effectuait avec la commande :

Ipv6 address adresse_ipv6/x EUI-64

192.168.0.2 - PuTTY

```
User Access Verification

Password:
UASZ>en
Password:
UASZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
UASZ(config)#int g0/0
UASZ(config-if)#ipv6 address 2001:1:1:1::/64 eui-64
UASZ(config-if)#
```

Figure 40 : adressage dynamique et le processus EUI-64

Ici l'adresse attribuée est incomplète au début mais elle sera complétée par l'adresse MAC de l'interface et le double octet FFFE.

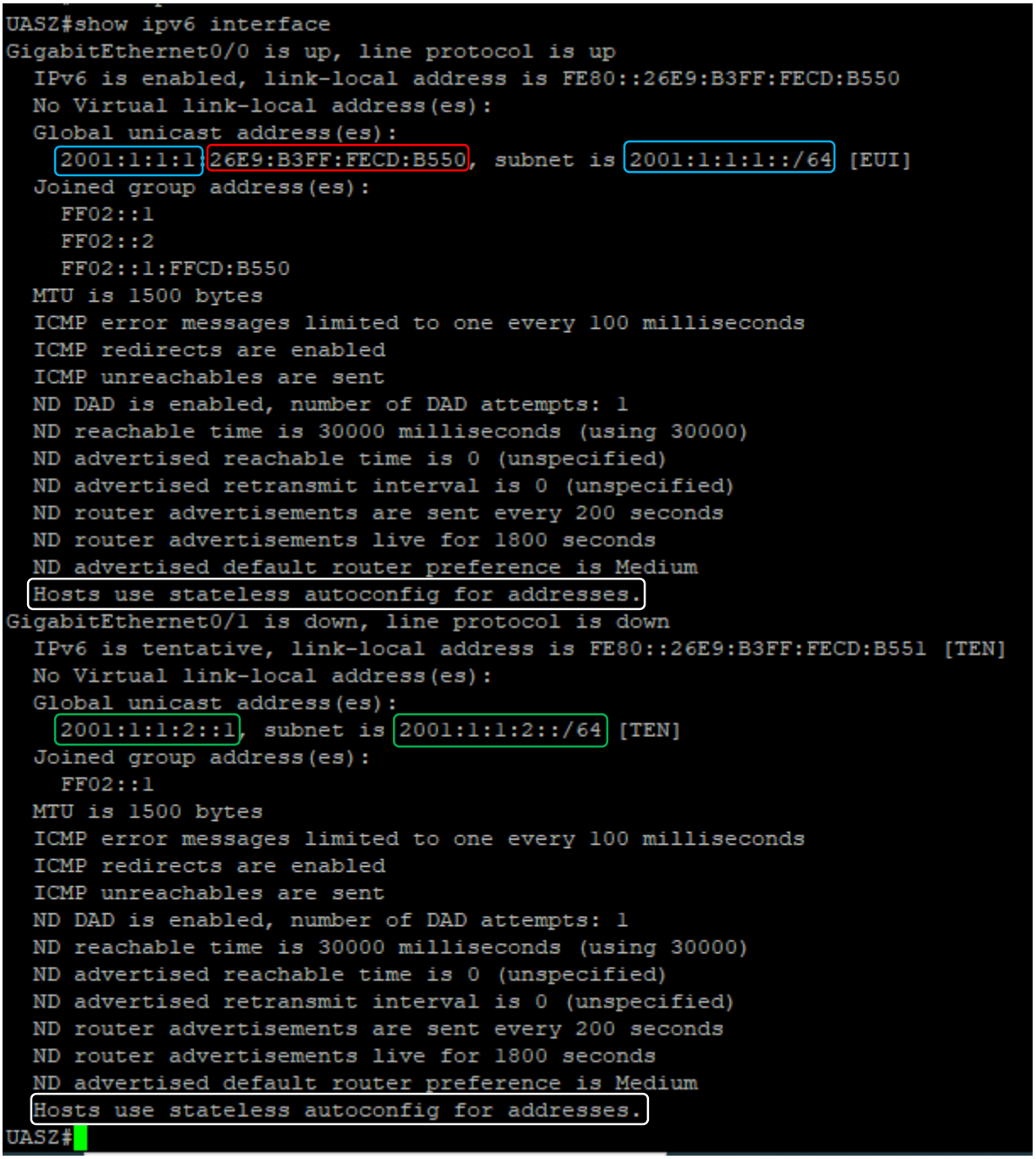


Figure 41 : affichage des informations Ipv6 des interfaces du routeur UASZ

L'affichage de la configuration IPv6 de l'interface G0/0 par exemple nous permet de constater que la partie interface a été configure grâce au processus EUI-64.

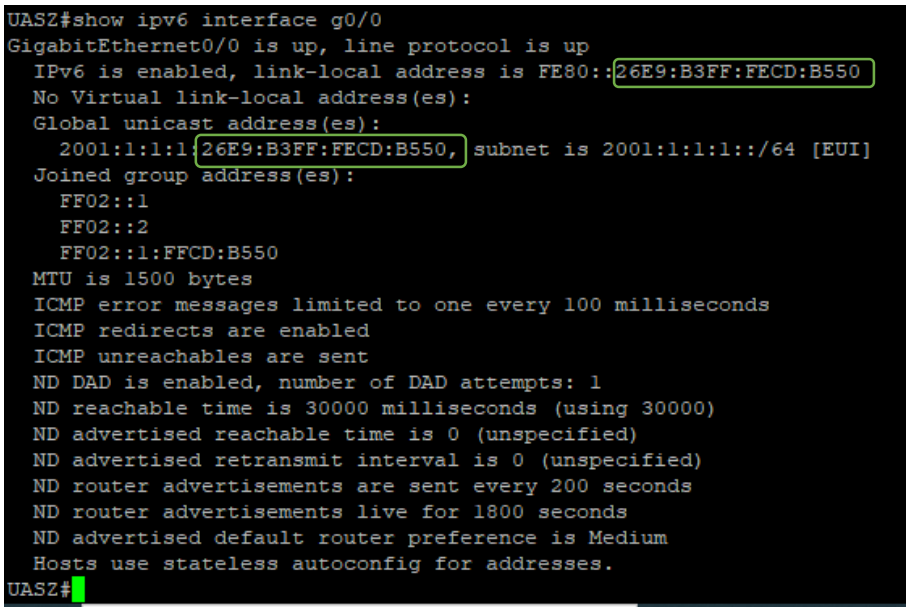


Figure 42 : Affichage des informations Ipv6 de l'interface G0/0 du routeur UASZ

IV.2) Au niveau des machines clientes

IV.2.a) Avant la configuration de la double pile

Avant la configuration de la seconde pile à savoir IPV6, le réseau IPv4 fonctionne correctement.

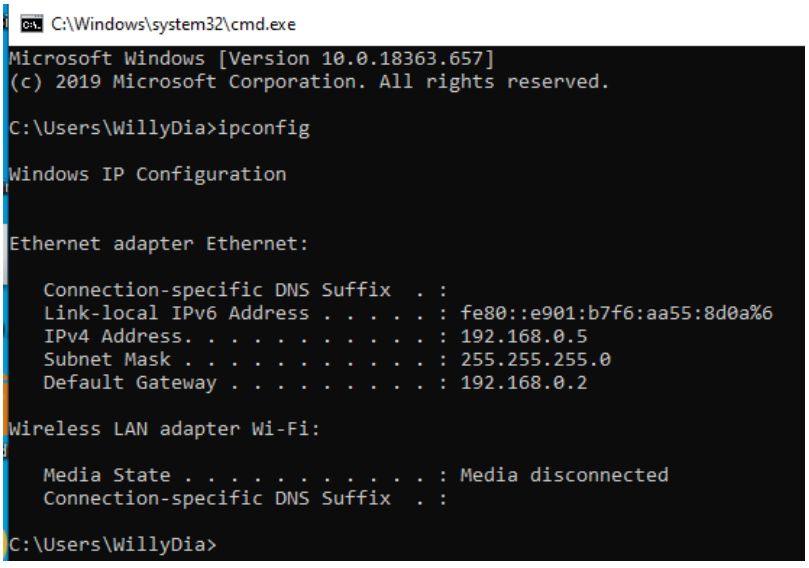


Figure 43 : Affichage de la configuration Ipv4 d'un client avant la double pile

***NB** : la présence de l'adresse Link-local est due au fait que la double pile est déjà actionnée sur les machines de dernière génération. Celle –ci en est une.*

IV.2.b) Configuration de la double pile

En première étape, sur les clients du réseau, nous devons accéder sur : Panneau de configuration → Réseau et Internet → Centre de réseau et partage. Et puis sur « afficher les informations de base de votre et configurer des connexions » au niveau de « afficher vos réseaux actifs.

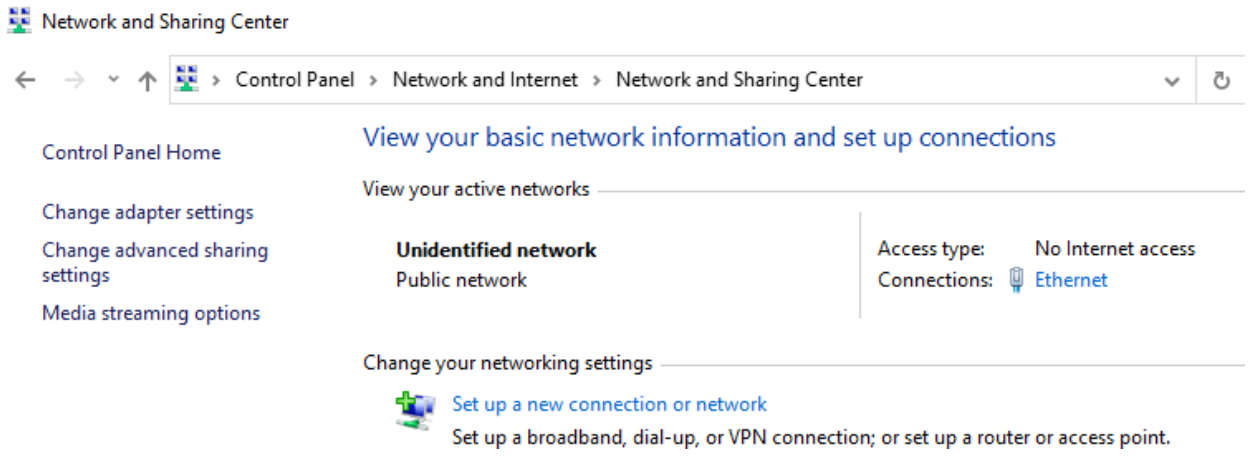


Figure 44 : itinéraire pour la configuration de la pile IPv4 ou Ipv6

En seconde étape, nous cliquons sur le réseau actif que nous désirons configurer (ici le réseau Ethernet), ensuite sur Propriété.

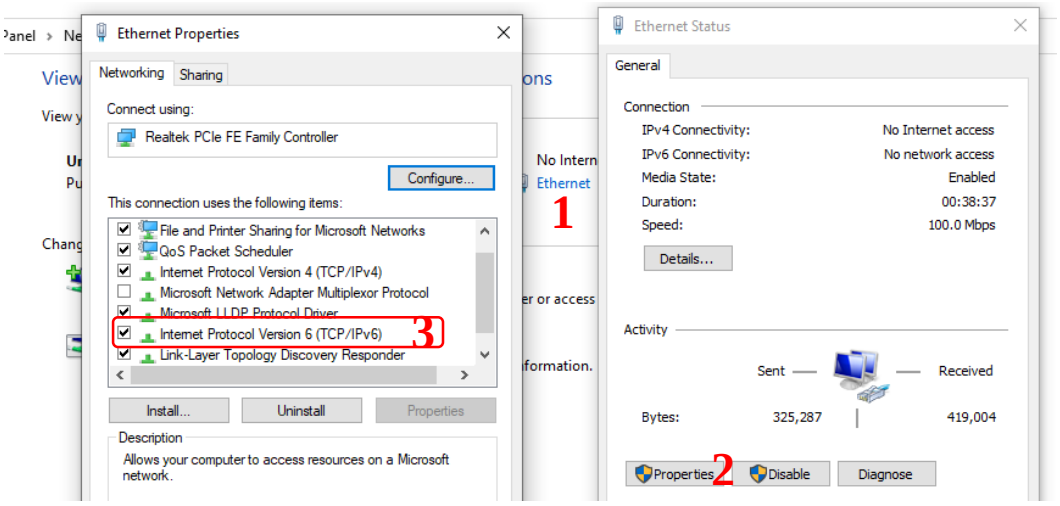


Figure 45 : suite itinéraire pour la configuration de la pile IPv4 ou Ipv6

En troisième étape nous cliquons sur la pile (IPv4 ou IPv6) que nous voulons configurer. Et pour notre cas c'est la pile IPv6 puisse que la pile IPv4 est déjà présente puis sur propriétés pour afficher les propriétés de cette pile et configurer les informations de connexion (@IPv6, passerelle par défaut, DNS, …) de manière statique ou automatique.

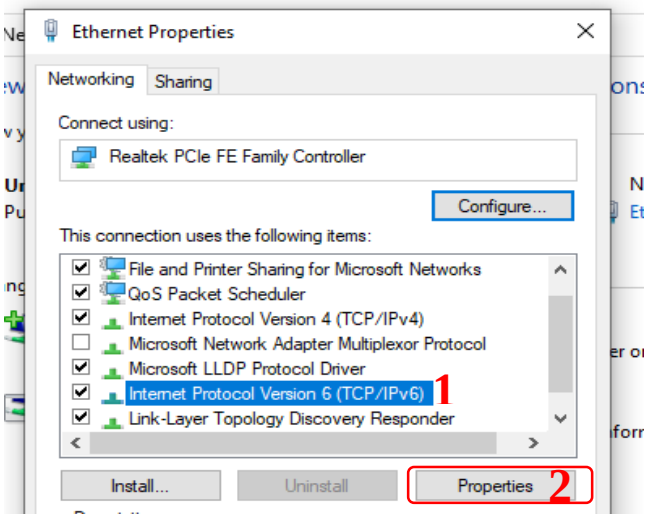


Figure 46 : Affichage propriétés de la pile IPv6

Une fois que vous cliquez sur les propriétés de la pile IPv6, il ne reste que sur vous pour choisir la méthode d'adressage qui vous convient (soit statique ou dynamique).

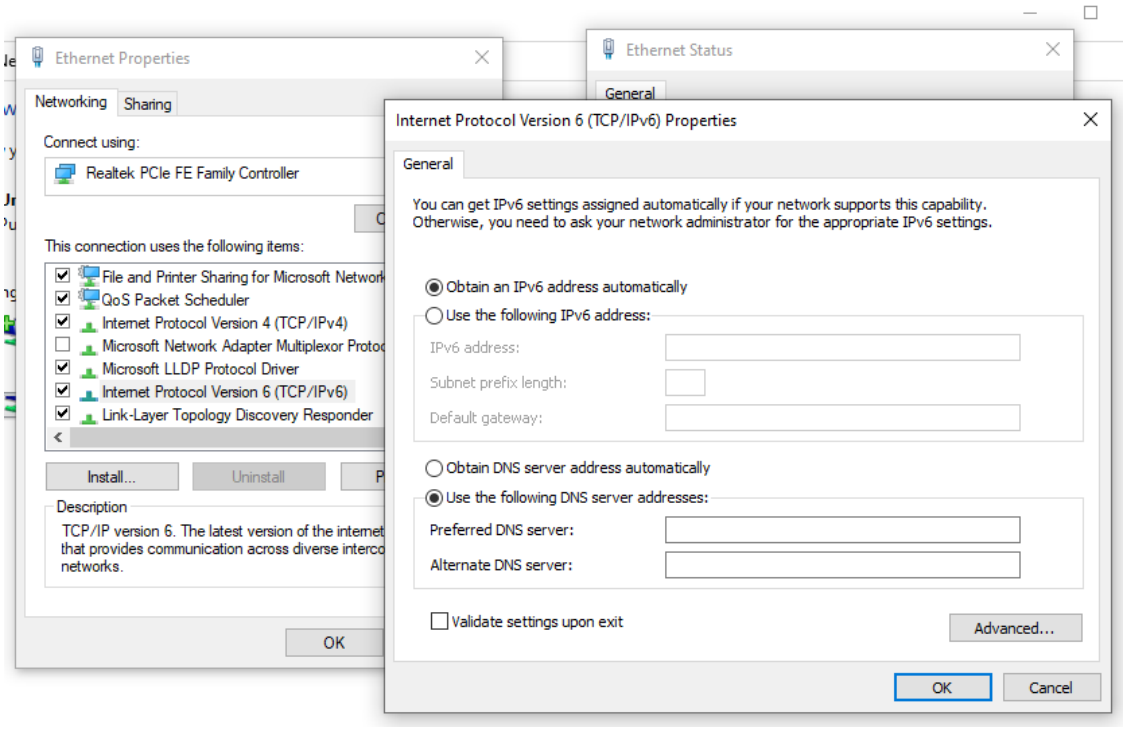


Figure 47 : configuration de la pile IPv6

Remarque :

Si vous choisissait la dynamique, c'est le routeur qui dictera à votre équipement laquelle des sous-méthodes (SLAAC, DHCPv6 avec état ou sans état) de la méthode dynamique à prendre.

Par défaut c'est SLAAC qui est actif au niveau du routeur.

Il faut aussi activer le routage à l'aide de la commande ipv6 unicast-routing pour que le routeur puisse envoyer le préfixe global aux clients pour leur permettre de « s'autoconfigurer ».

V) Implémentation de la topologie de test

Au niveau de l'UASZ, le réseau est réparti en Vlan. Pour l'implémentation nous avons utilisé Paket tracer pour être plus proche de l'architecture du réseau de l'UASZ et quelques équipements de l'académie Cisco pour plus de fiabilité et valeur sur les commandes que nous avons utilisé car il est de pratique sur le physique que sur le virtuel.

V.1) Implémentation sur Paket tracer

Pour être en phase avec cette architecture, voici l'architecture que nous utiliserons pour notre TP sur Paket tracer:

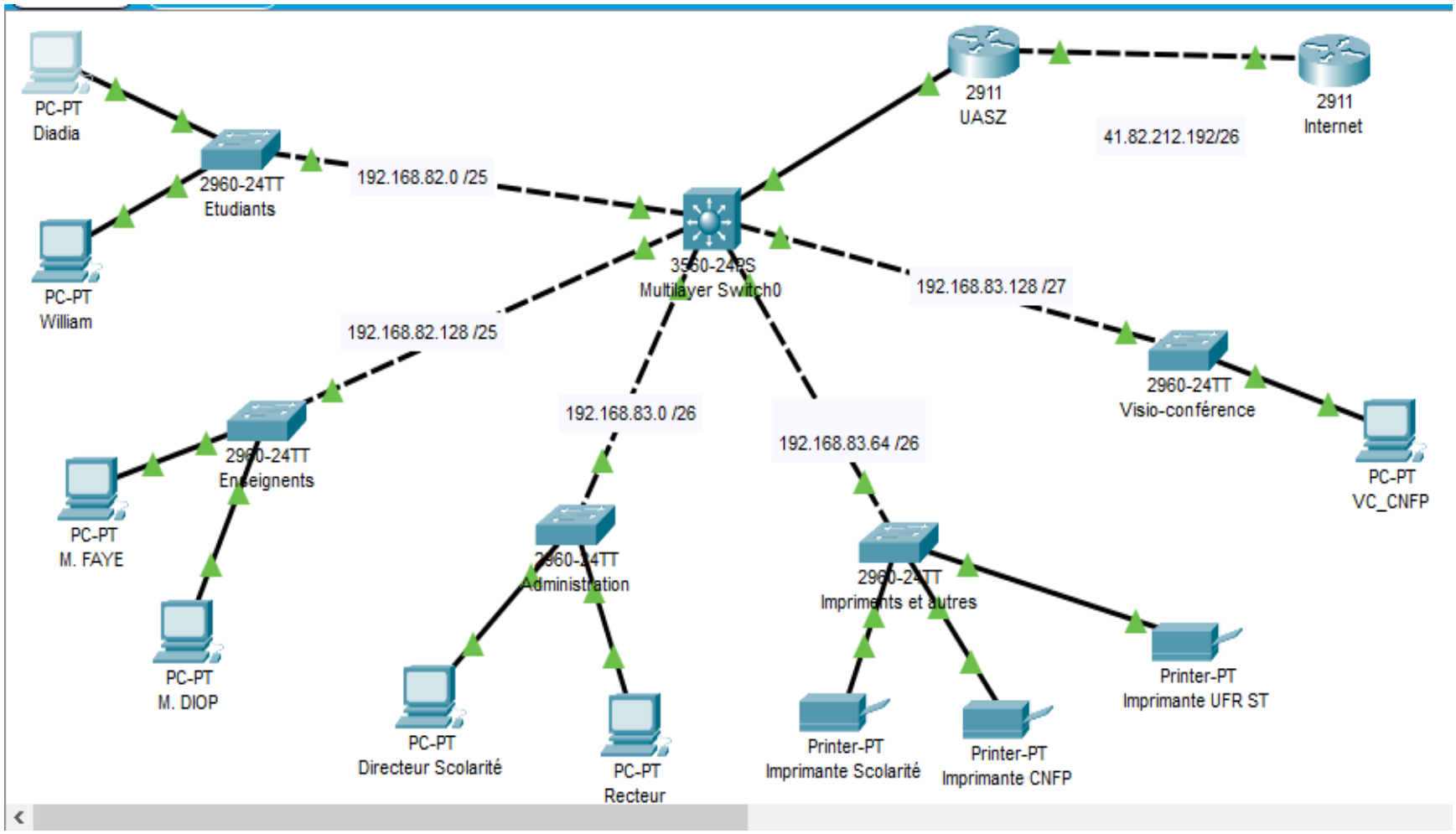


Figure 48 : Topologie du réseau IPv4 de stimulation avant la double Pile

Ci-dessous se trouve la configuration en marche d'interface de sortie (passerelle) du réseau. C'est obtenu à partir de la commande : *show running-config*

```
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.101
 encapsulation dot1Q 101
 ip address 192.168.82.1 255.255.255.128
!
interface GigabitEthernet0/1.102
 encapsulation dot1Q 102
 ip address 192.168.82.129 255.255.255.128
!
interface GigabitEthernet0/1.103
 encapsulation dot1Q 103
 ip address 192.168.83.1 255.255.255.192
!
interface GigabitEthernet0/1.104
 encapsulation dot1Q 104
 ip address 192.168.83.65 255.255.255.192
!
interface GigabitEthernet0/1.105
 encapsulation dot1Q 105
 ip address 192.168.83.129 255.255.255.224
!
```

Figure 49 : Configuration en marche du routeur UASZ

Celle qui suit, est la configuration d'un client du réseau. Nous voyons nettement que c'est seulement la pile IPv4 qui est configuré.

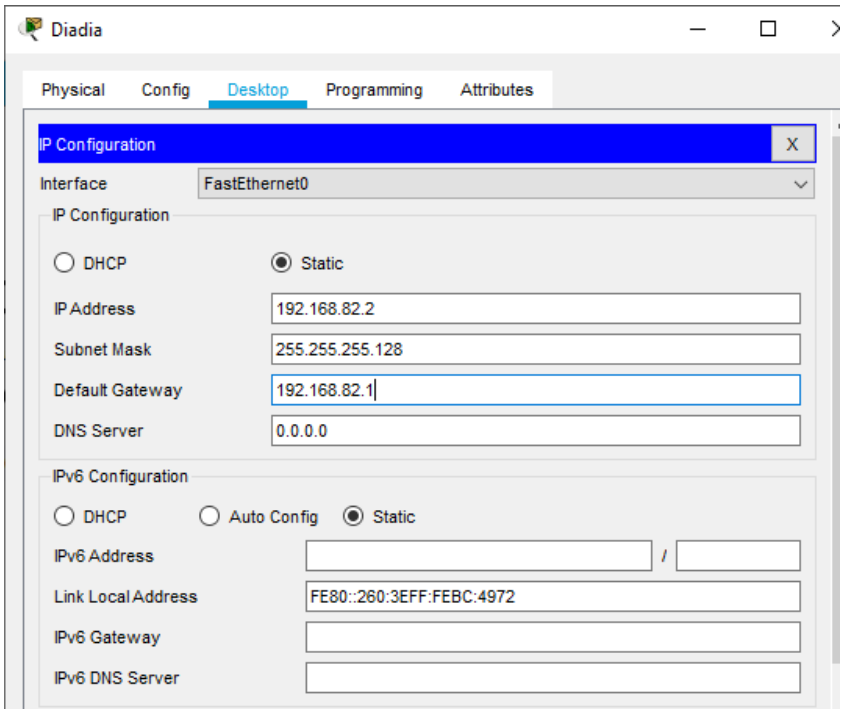


Figure 50 : configuration d'un client (Diadia) du réseau

Nous testons ici la conectivité du reseau.

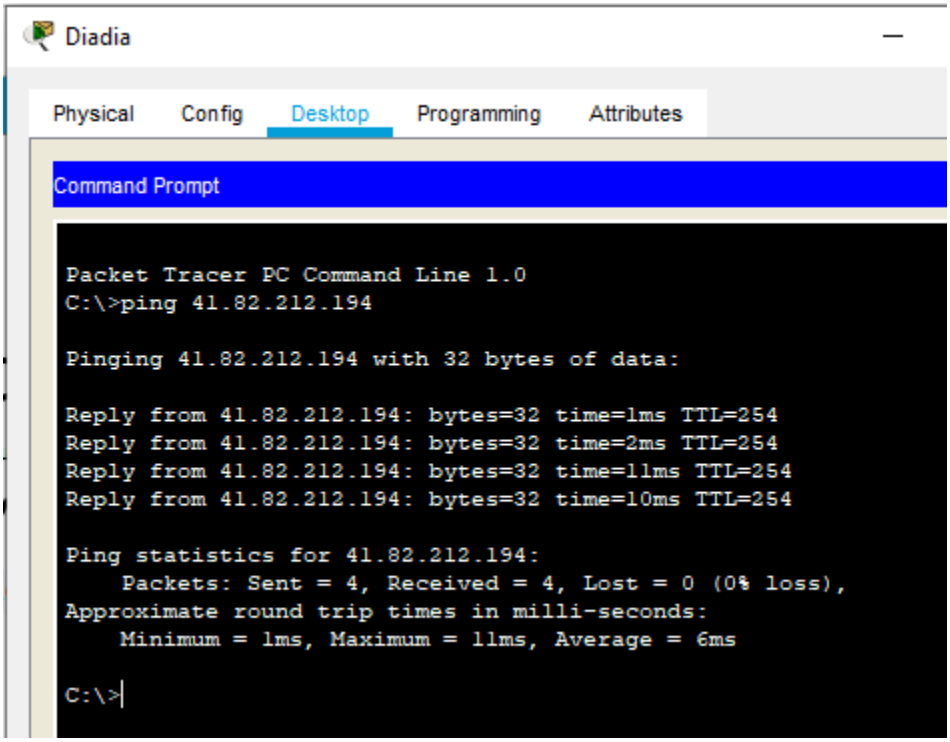


Figure 51 : Teste connectivité de la pile IPv4

Nous utilisons le préfixe global suivant :

2001 :AAAA :AAAA :AAA1 ::/64,

2001:AAAA:AAAA:AAA2::/64,

2001:AAAA:AAAA:AAA3::/64,

2001:AAAA:AAAA:AAA3::/64 ;

2001:AAAA:AAAA:AAA5::/64 ,

2001:BBBB:BBBB:BBBB::/64,

pour les différents VLANs de l'AUSZ et le dernier pour un réseau IPv6 externe. La capture ci-dessous le couple IPv4/IP6 d'adresses réseaux des VLANs.

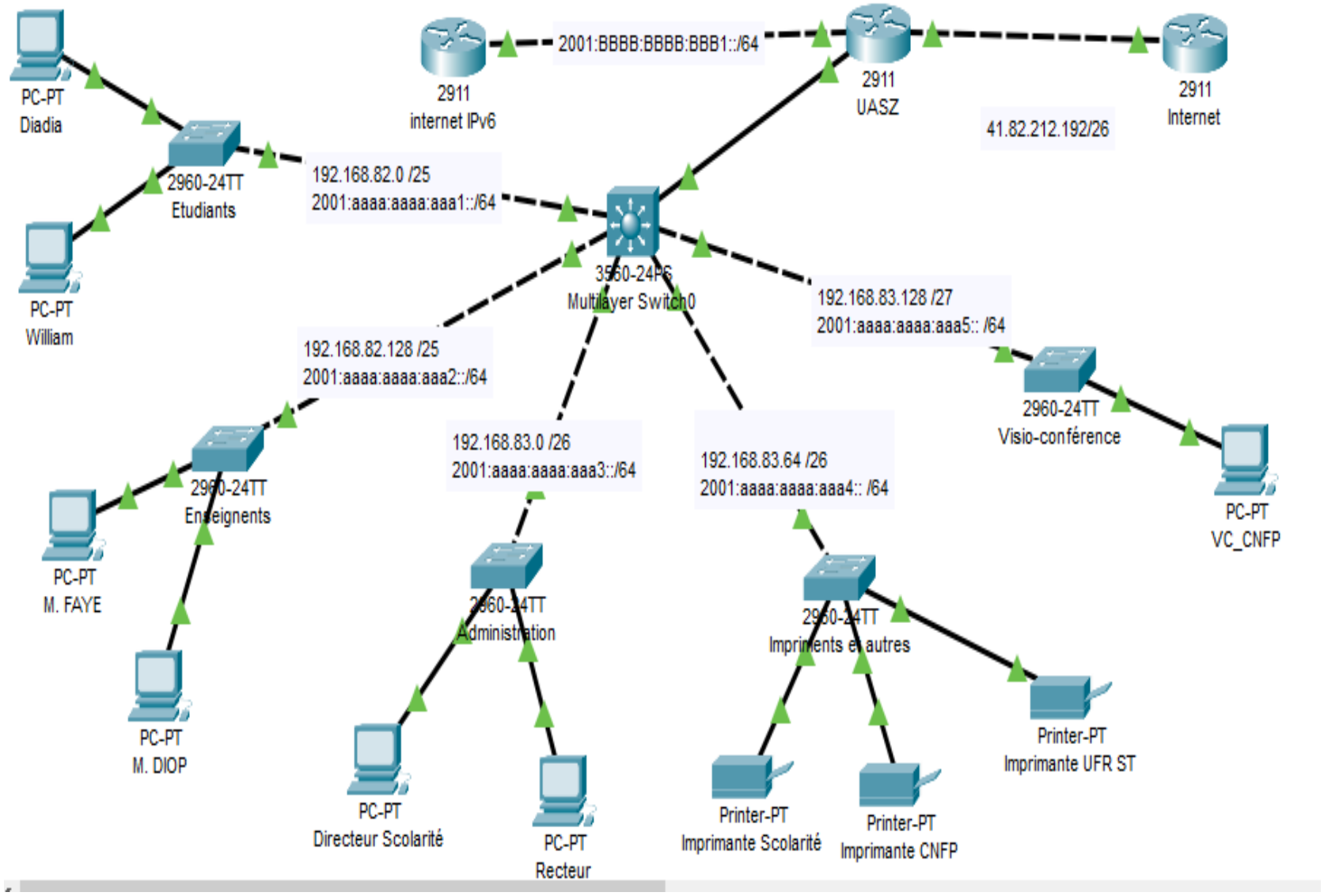


Figure 52 : Topologie du réseau de stimulation avec la double Pile

Après avoir activé le protocole IPv6 sur les sous interface à l'aide de la commande :

```
UASZ(config-subif)#ipv6 enable
UASZ(config-subif)#
```

Et attribuer statiquement les adresses IPv6 aux sous interfaces

```
UASZ(config-subif)#ipv6 address 2001:aaaa:aaaa:aaa1::1/64
UASZ(config-subif)#no sh
```

L'affichage de la configuration en marche du routeur de l'AUSZ, nous permet d'avoir un aperçu de la configuration du routeur.

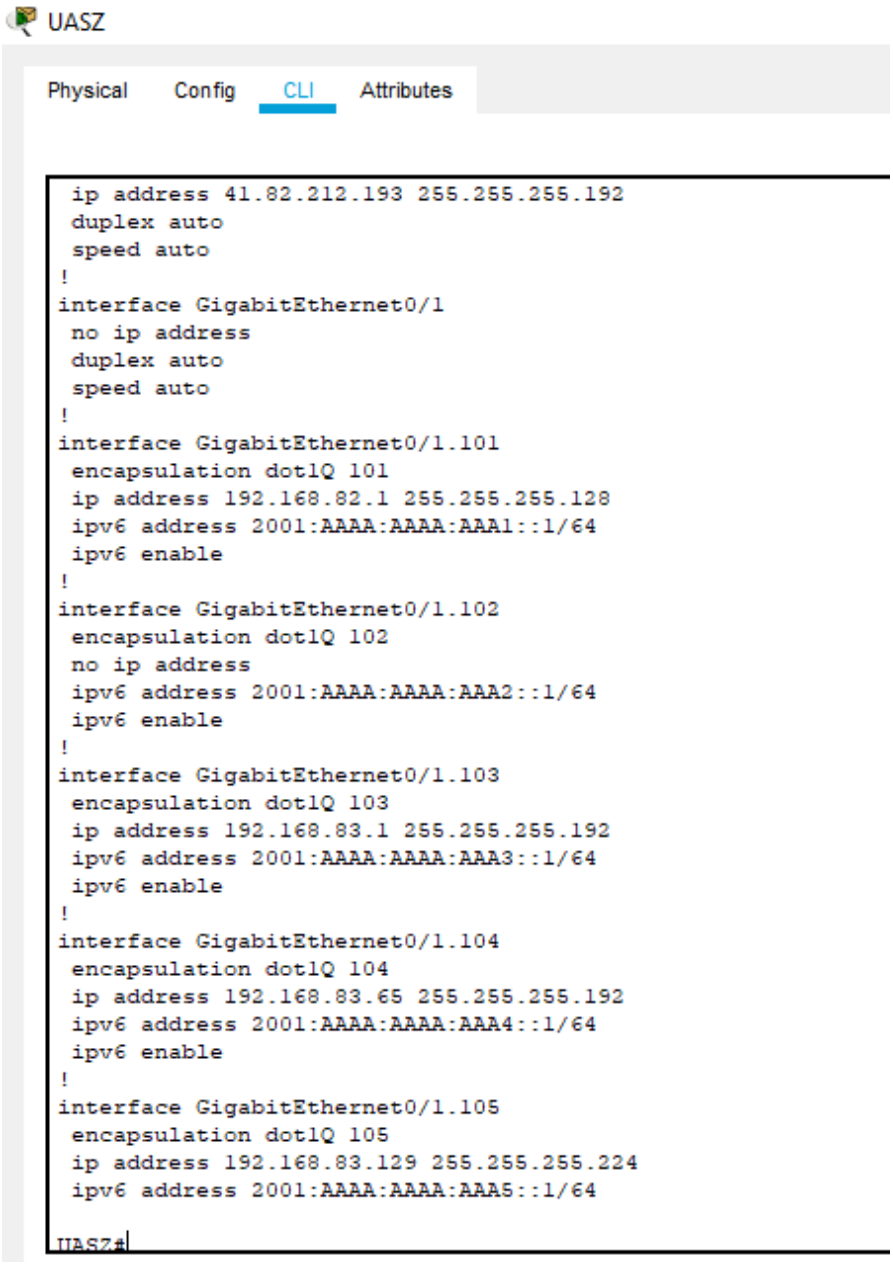


Figure 53 : configuration en marche du routeur après configuration de la double pile

Pour pouvoir utiliser l'adressage dynamique SLAAC, nous activons le routage IPv6 sur le routeur avec l'aide de la commande suivante :

```
UASZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
UASZ(config)#ipv
UASZ(config)#ipv6 u
UASZ(config)#ipv6 unicast-routing
UASZ(config)#
```

Figure 54 : Activation du routage IPv6

Comme vu sur les chapitres précédents, en IPv6 nous avons plusieurs méthodes d'adressage. Ici nous avons utilisé » la méthode statique et SLAAC.

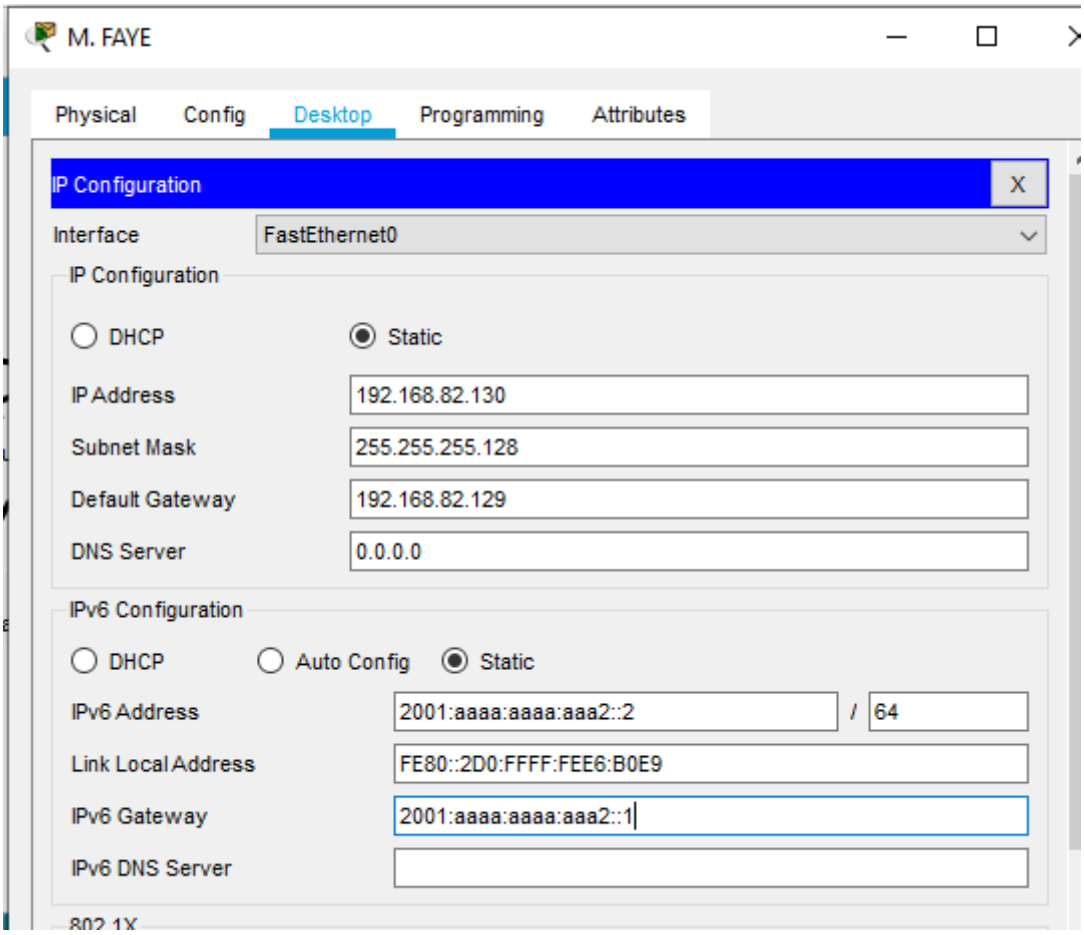


Figure 55 : configuration statique d'un client (M. FAYE)

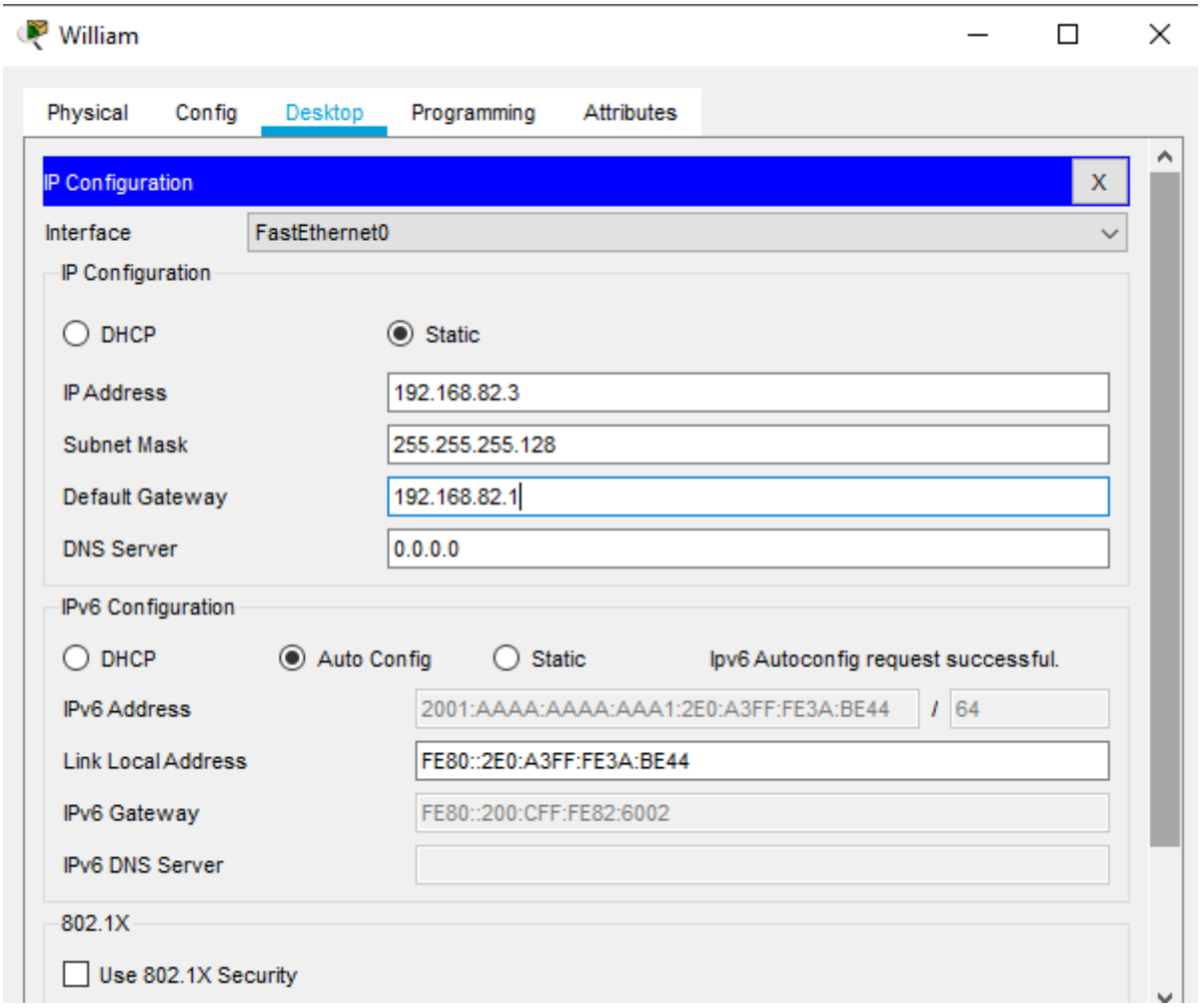


Figure 56: configuration dynamique (SLAAC) d'un client (William)

Nous avons utilisé le protocole de routage RIPng pour le routage. Et pour se faire nous l'avons d'abord initialisé sur le routeur puis nous l'avons activé au niveau des différents sous interface en utilisant respectivement les commandes :

```
UASZ(config)#ipv6 router rip willy
UASZ(config-rtr)#
```

```
UASZ(config)#ipv6 router rip willy
UASZ(config-rtr)#int g0/1.101
UASZ(config-subif)#ipv6 rip willy e
UASZ(config-subif)#ipv6 rip willy enable
UASZ(config-subif)#int g0/1.102
UASZ(config-subif)#ipv6 rip willy enable
UASZ(config-subif)#int g0/1.103
UASZ(config-subif)#ipv6 rip willy enable
UASZ(config-subif)#int g0/1.104
UASZ(config-subif)#ipv6 rip willy enable
UASZ(config-subif)#int g0/1.105
UASZ(config-subif)#ipv6 rip willy enable
UASZ(config-subif)#
```

Figure 57 : initialisation et activation de RIPng

Ici nous procédons à un test de la connectivité de la pile IPv6.

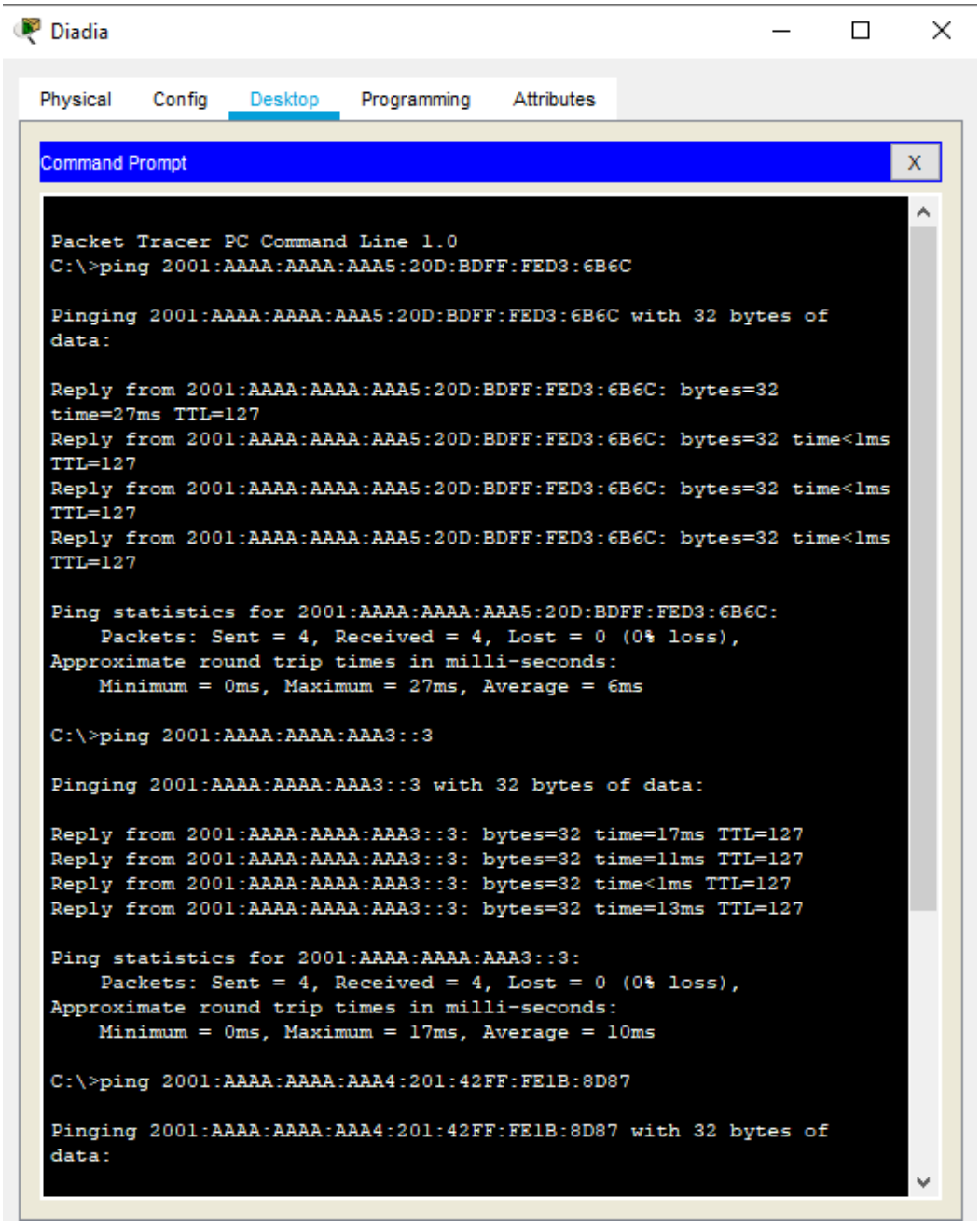


Figure 58 : test de la connectivité de la pile IPv6

V.2) Implémentation avec les équipements de l'académie Cisco

Ce réseau est disposé en Vlan. Ces Vlan sont créés au niveau du switch nommé Diadia.

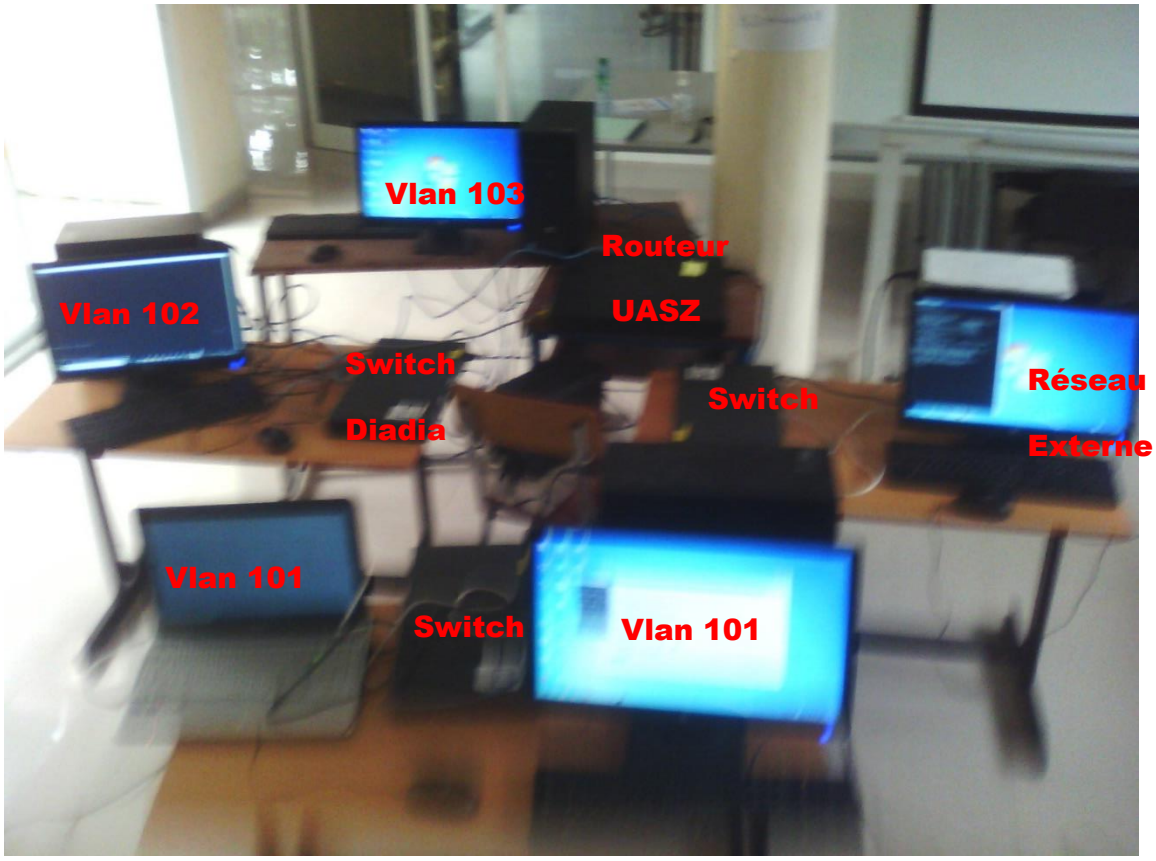


Figure 59: architecture du réseau utilisé pour la stimulation

Le tableau ci-dessous comporte les différents réseaux utilisés pour la pratique.

Réseau	Vlan	Adresse réseau IPv4	Adresse réseau IPv6
Interne	101	192.168.82.0/25	2001 :AAAA :AAAA :AAA1 ::/64
	102	192.168.82.128/25	2001 :AAAA :AAAA :AAA2 ::/64
	103	192.168.83.0/26	2001 :AAAA :AAAA :AAA3 ::/64
Externe		41.82.212.192/26	2001 :BBBB : BBBB: BBBB::/64

Tableau 4: Adresses réseaux utilisés

V.2.a) Vérification connectivité de la pile IPv4 avant la double pile

La pile IPv4 est déjà configure. Il ne reste qu'à configurer la pile IPv6.

Voici les différents Vlan et les ports auxquels ils sont attribués :

```
Diadia#
*Mar  1 00:39:46.894: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to up
Diadia#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/2
101  Etudiants                        active    Fa0/1
102  Enseignents                      active    Fa0/2
103  administration                   active    Fa0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Diadia#
*Mar  1 00:40:07.261: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan103, changed state to up
Diadia#
```

Figure 60: Vlan et les ports auxquels ils sont attribués

Il y a aussi un autre client du Vlan 101 qui se situe sur l'autre switch.

Le routeur UASZ dispose d'un réseau externe sur l'interface G0/1 et sur l'interface G0/0 de trois (3) réseaux interne (un réseau par VLAN) configurés sur des sous-interfaces de G0/0.

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 no mop enabled
!
interface GigabitEthernet0/0.101
 encapsulation dot1Q 101
 ip address 192.168.82.1 255.255.255.128
!
interface GigabitEthernet0/0.102
 encapsulation dot1Q 102
 ip address 192.168.82.129 255.255.255.128
!
interface GigabitEthernet0/0.103
 encapsulation dot1Q 103
 ip address 192.168.83.1 255.255.255.192
!
interface GigabitEthernet0/1
 ip address 41.82.212.193 255.255.255.192
 duplex auto
 speed auto
```

Figure 61: État en marche du routeur UASZ

Voici aussi la configuration d'un client avant la configuration de la pile IPv6. Ici un client du Vlan 102.

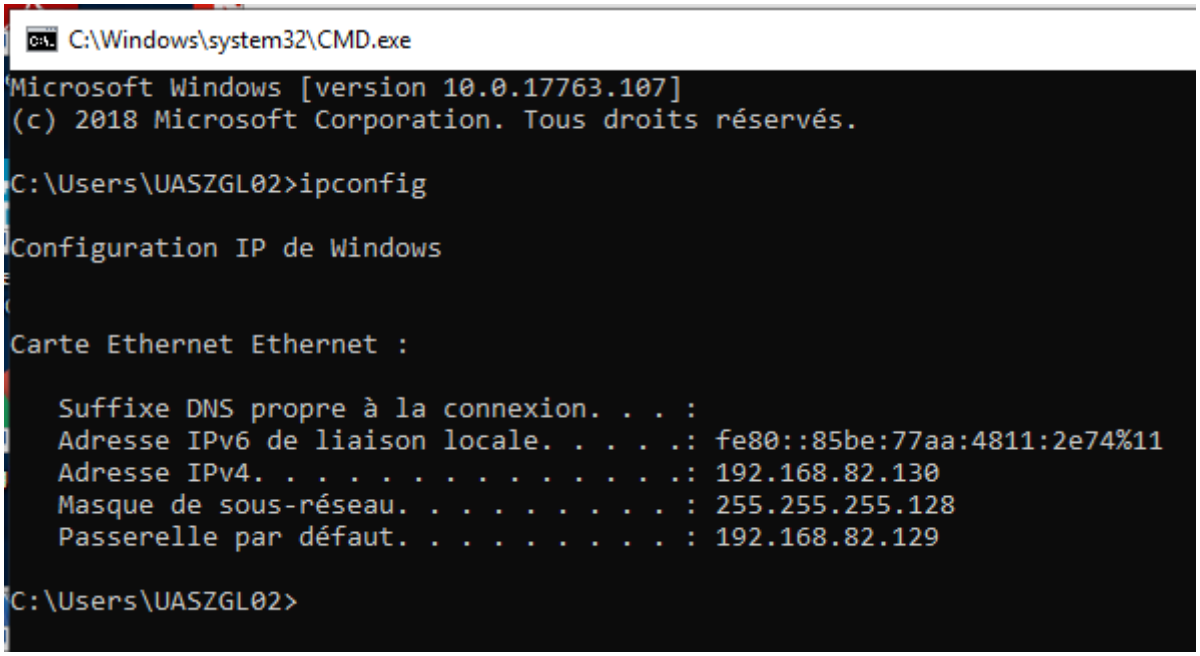


Figure 62: Exemple de configuration d'un client du Vlan 102

Tout d'abord vérifions la connectivité de la pile déjà configurée (IPv4)

- En interne

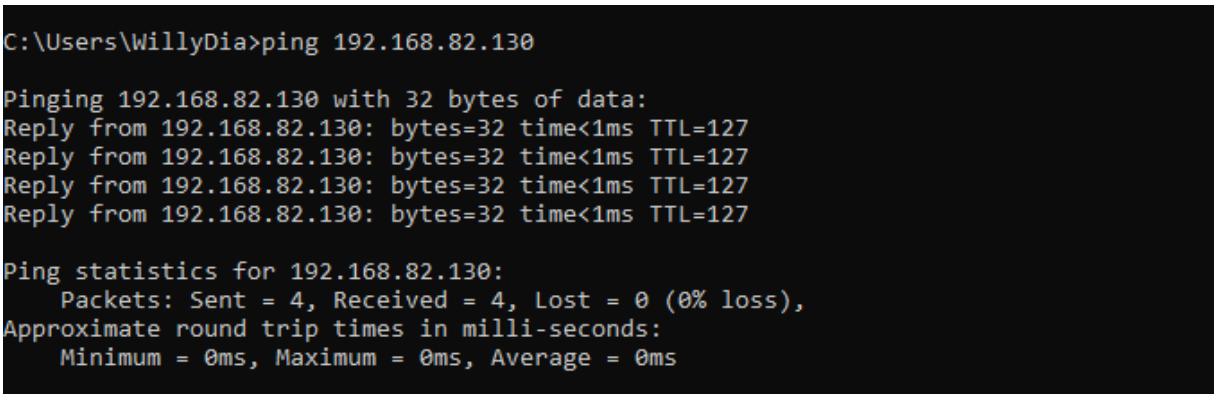


Figure 63: Test connectivité IPv6 entre Vlan

- Vers l'extérieur :

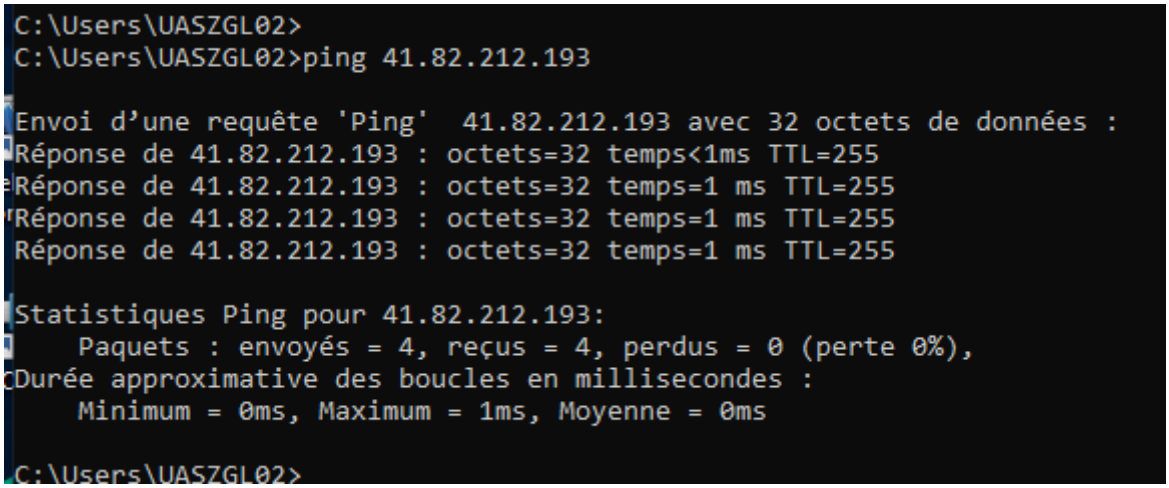


Figure 64 : test connectivité IPv4 vers un réseau distant

Le réseau est bien fonctionnel en interne qu'en externe.

V.2.b) Configuration pile IPv6

La pile IPv4 est présente et fonctionnelle sur les différentes interfaces. À présent nous nous focalisons sur la configuration de la pile IPv6.

I.1.a.4 Au niveau du routeur UASZ

Pour attribuer des adresses aux interfaces et sous-interface du routeur, nous nous positionnons sur chaque interface ou sous-interface que nous aimerons configurer.

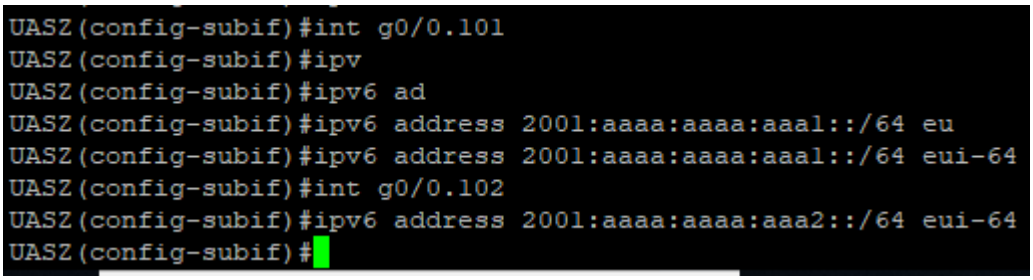


Figure 65: Configuration interface et sous interface du routeur

Ici nous avons utilisé le processus EUI-64 pour la configuration de l'adresse complète de la sous-interface.

La saisie de la commande Show ipv6 interface, nous permet de voir l'adresse complète de la sous-interface.

```
UASZ#show ipv6 interface g0/0.101
GigabitEthernet0/0.101 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::26E9:B3FF:FECD:B550
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:AAAA:AAAA:AAA1:26E9:B3FF:FECD:B550, subnet is 2001:AAAA:AAAA:AAA1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::1:FFCD:B550
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
UASZ#
UASZ#
```

Figure 66: État du sous interface g0/0.101

Voici la configuration en marche du routeur UASZ après la configuration de la nouvelle pile (IPv6). Elle est obtenue avec l'aide de la commande : *Show running-config*

```
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 enable
 no mop enabled
!
interface GigabitEthernet0/0.101
 encapsulation dot1Q 101
 ip address 192.168.82.1 255.255.255.128
 ipv6 address 2001:AAAA:AAAA:AAA1::/64 eui-64
 ipv6 enable
!
interface GigabitEthernet0/0.102
 encapsulation dot1Q 102
 ip address 192.168.82.129 255.255.255.128
 ipv6 address 2001:AAAA:AAAA:AAA2::/64 eui-64
!
interface GigabitEthernet0/0.103
 encapsulation dot1Q 103
 ip address 192.168.83.1 255.255.255.192
 ipv6 address 2001:AAAA:AAAA:AAA3::/64 eui-64
!
interface GigabitEthernet0/1
 ip address 41.82.212.193 255.255.255.192
 duplex auto
 speed auto
 ipv6 address 2001:BBBB:BBBB:BBBB::1/64
!
```

Figure 67 : configuration en marche du routeur après activation double pile

Remarque : *Pour permettre aux clients de pouvoir s'auto-configurer, il faut saisir en mode configuration globale la commande : ipv6 Unicast routing et activer IPv6 sur les interfaces avec la commande : IPv6 enable.*

```
UASZ(config)#
UASZ(config)#ipv
UASZ(config)#ipv6 un
UASZ(config)#ipv6 unicast-routing
UASZ(config)#int g0/0.101
UASZ(config-subif)#ipv6 en
UASZ(config-subif)#ipv6 enable
UASZ(config-subif)#int g0/0.102
UASZ(config-subif)#ipv6 enable
UASZ(config-subif)#int g0/0.103
UASZ(config-subif)#ipv6 enable
UASZ(config-subif)#
```

Figure 68 : activation ipv6 sur une interface

I.1.a.5 **Au niveau des clients**

Pour la configuration, il suffit aller au niveau de centre de réseau et partage puis sur modifier les paramètres de la carte réseau ensuite sur la carte réseau que nous voulons configurer. Nous affichons les propriétés de cette carte puis nous choisissons le protocole IP que nous voulons configurer (ici IPv6). Et en fin nous choisissons le type d'adressage que nous aimerions utiliser.

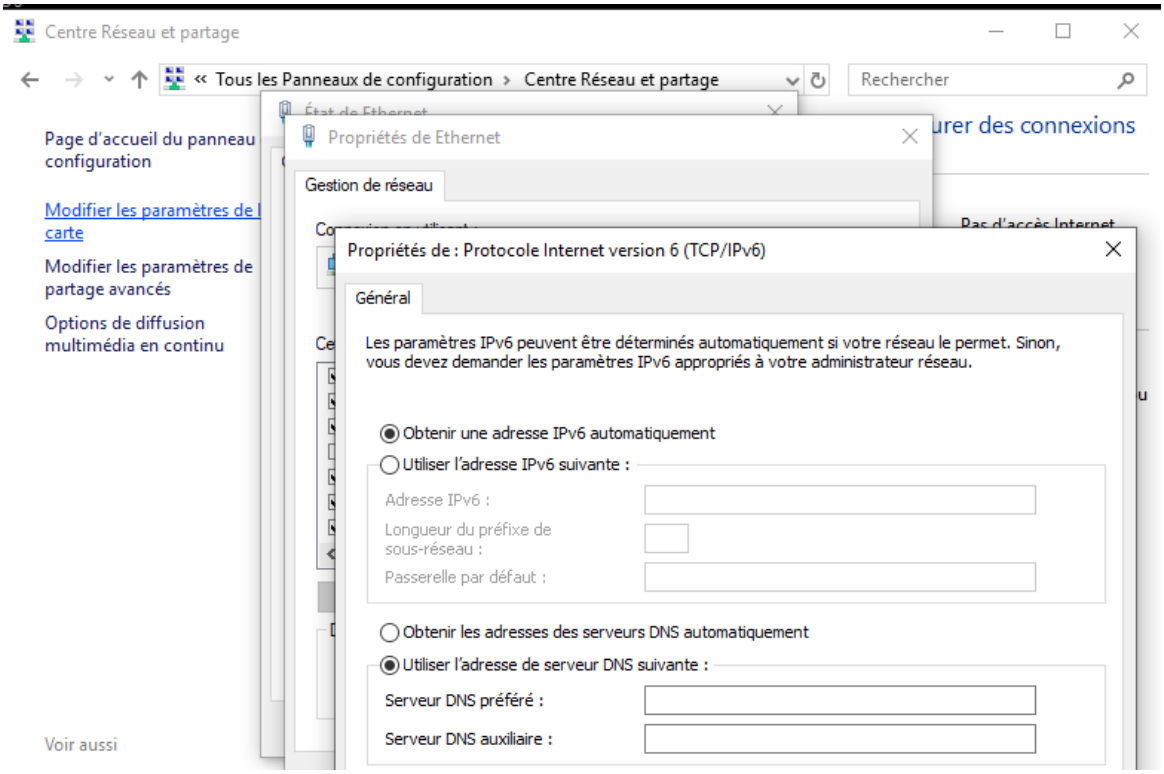


Figure 69: choix du type d'adressage à utiliser

Voici un exemple de configuration d'un client du Vlan 102.

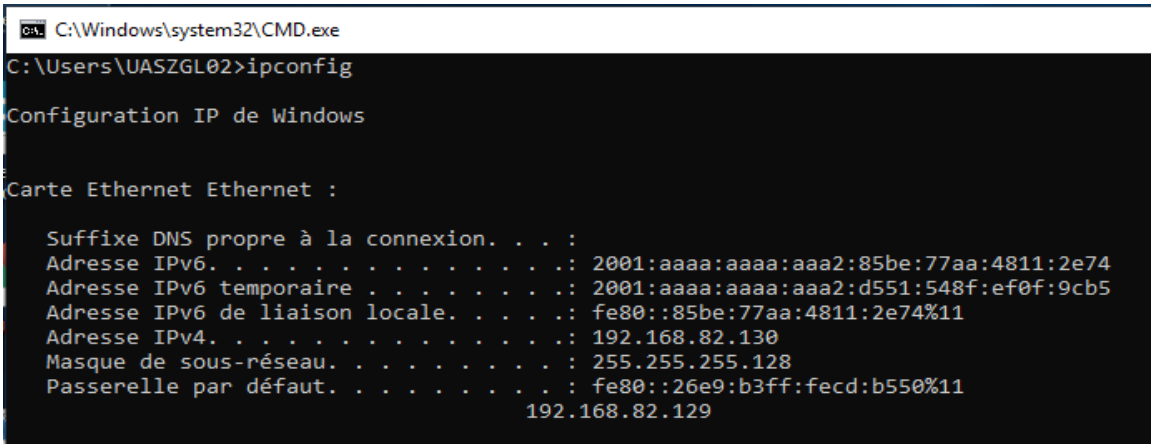


Figure 70: configuration d'un client du Vlan 102

V.2.c) Test connectivité IPv4 et IPv6

Testons à nouveau si la configuration de la nouvelle pile (IPv4) n'a pas détérioré la connectivité de l'ancienne pile (IPv4) puis celle de la pile IPv6 en interne.

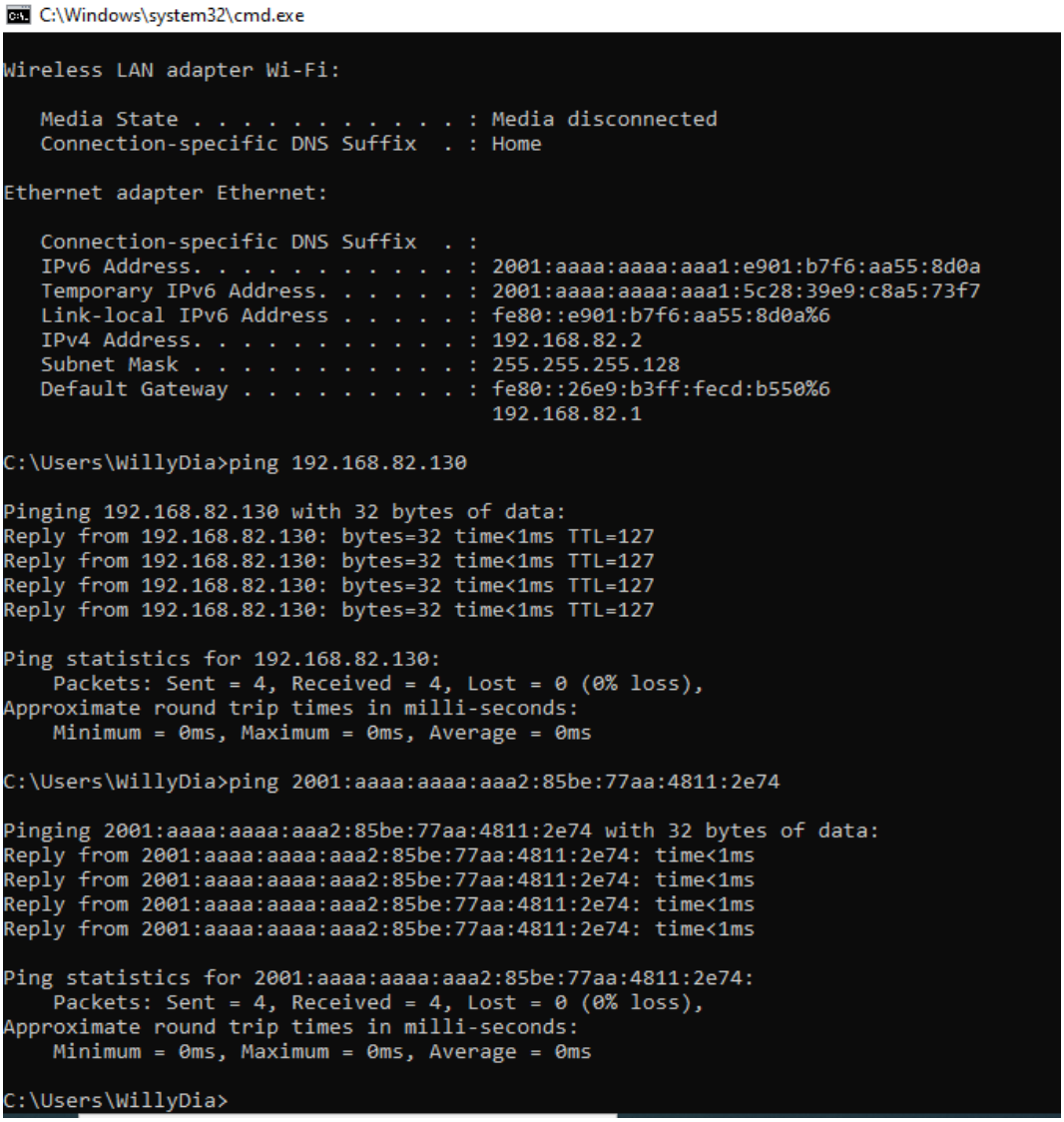


Figure 71: Test connectivité Ipv4 après configuration IPv6

Nous procédons au test de la connectivité d'IPv6 vers un réseau externe.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:aaaa:aaaa:aaa1:e901:b7f6:aa55:8d0a
   Temporary IPv6 Address. . . . . . : 2001:aaaa:aaaa:aaa1:89b7:5f7f:b968:6713
   Link-local IPv6 Address . . . . . : fe80::e901:b7f6:aa55:8d0a%6
   IPv4 Address. . . . . . . . . . . : 192.168.82.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.128
   Default Gateway . . . . . . . . . : fe80::26e9:b3ff:fecd:b550%6
                                       192.168.82.1

C:\Users\WillyDia>ping 2001:bbbb:bbbb:bbbb:b1ce:7da7:9e7f:ddaa

Pinging 2001:bbbb:bbbb:bbbb:b1ce:7da7:9e7f:ddaa with 32 bytes of data:
Reply from 2001:bbbb:bbbb:bbbb:b1ce:7da7:9e7f:ddaa: time<1ms
Reply from 2001:bbbb:bbbb:bbbb:b1ce:7da7:9e7f:ddaa: time<1ms
Reply from 2001:bbbb:bbbb:bbbb:b1ce:7da7:9e7f:ddaa: time<1ms
Reply from 2001:bbbb:bbbb:bbbb:b1ce:7da7:9e7f:ddaa: time<1ms

Ping statistics for 2001:bbbb:bbbb:bbbb:b1ce:7da7:9e7f:ddaa:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\WillyDia>
```

Figure 72 : tester la connectivité IPv6 vers un réseau externe

NB :

- Il faut autoriser la double pile au niveau des switch pour que ces derniers puis transmettre des paquets IPv6. Et pour le faire nous utilisons la commande :

```
swl(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
swl(config)#end
```

Figure 73 : Permettre au switch de transmettre des paquets IPv4 et IPv6

- Parfois si le Ping, il faut vérifier au niveau du Pare-feu s'il est autorisé.

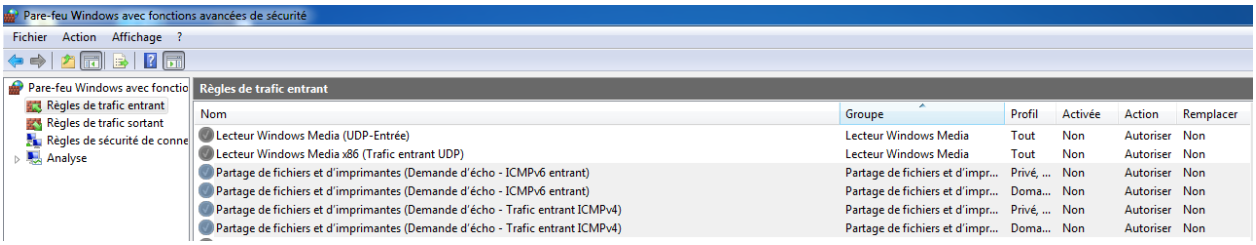


Figure 74: Autorisation ICMPv4 et CMPv6

Conclusion

Puisque IPv6 n'est qu'un novice pour les utilisateurs, la double pile est la mieux placée pour assurer la transition car elle permettra aux users de s'y adapter progressivement. Elle permettra aussi aux machines de dernière génération mais aussi les anciennes de fonctionner correctement soit avec IPv6 ou IPv4 ou encore les deux.

Conclusion générale et Perpectives

La croissance de l'Internet a rendu IPv4 obsolète. Le nouveau protocole IPv6 vise à retrouver le principe de "bout en bout". Ce principe fondateur de l'Internet a assuré son succès. C'est par ce principe que l'Internet est devenu une source d'innovation et le support de l'économie du numérique. La migration d'IPv4 vers IPv6 est bien plus qu'un simple changement de tuyau. C'est tout l'écosystème qui est appelé à évoluer. Aussi, la sensibilisation de tous les acteurs à la problématique de la migration est cruciale. Le déploiement d'IPv6 se conduit, comme un projet, avec une planification. Il touche tous les métiers du système d'information.

Le déploiement d'IPv6 doit se faire en tenant compte de l'existant et de manière progressive. IPv6 est appelé à coexister avec IPv4. Autrement dit, il est une évolution d'IPv4 et non le moyen de faire un Internet parallèle et disjoint de l'existant. Pour maintenir cette connectivité globale, IPv6 comporte des mécanismes transitoires pour qu'il puisse interagir avec IPv4. Ces mécanismes sont maintenant connus. Ils sont responsables en grande partie de l'image de complexité que peut dégager le passage à IPv6. Cependant, ils ne sont pas tous à utiliser : il faut retenir celui qui permet de faire interagir IPv6 avec son système de communication. Au cours de cette séquence, nous avons présenté 3 techniques d'intégration :

- la double pile, qui est la solution par excellence du déploiement progressif ;
- le tunnel, pour interconnecter des îlots IPv6 par des liens virtuels en IPv6, établis sur des liaisons réelles en IPv4 ;
- la traduction, lorsque la double pile ne peut plus être utilisée du fait du manque d'adresses IPv4, ou pour rendre des services accessibles à IPv6 sans avoir à mettre à jour le serveur.

Dans ce mémoire, après une analyse technique basé sur la topologie, les équipements, les logiciels et la politique d'administration réseau menée par le CRI, nous avons choisi d'implémenter la double pile parce qu'elle correspond à la technique la mieux adaptée du fait de sa simplicité et répond plus aux exigences des acteurs et utilisateurs. Un déploiement sur Packet Tracer suivie de tests partiellement intempestifs sur des équipements réels Cisco nous

permet de pouvoir avec un degré de certitude élevé dire que le déploiement réel sur le réseau de l'UASZ se fera sans difficultés.

Comme, aujourd'hui, les réseaux IPv6, seuls ou déployés conjointement avec IPv4, deviennent de plus en plus courants, il est important d'avoir les bonnes pratiques de déploiement et d'administration qui émergent progressivement. Il est donc important de se tenir informé, de partager et d'adapter ses propres pratiques en fonction des expériences de chacun.

Et dans le futur, nous comptons nous pencher dans l'impact qu'apporte IPng sur la performance et la QoS des réseaux, Mais également sur la sécurité.

Bibliographie et webographie

[1] S. Dunand, «Publication de services web IPv4 sur Internet IPv6,» heig-vd, filière Télécommunication, orientation réseaux et services, Vaud, 2012.

[2] J. D. D. K. BAHATI, «SUPINFO, École Supérieure d'Informatique,» 26 07 2017. [En ligne]. Available: https://www.supinfo.com/articles/single/4843-adresses-ip-privees-publiques. [Accès le 10 01 2019].

[3] «ISN - Les réseaux informatiques,» [En ligne]. Available: http://silanus.fr/sin/formationISN/Parcours/Reseaux/co/Reseau_11.html.

[4] ZiCodji, «E-help,» [En ligne]. Available: http://e-help.freehostia.com/index.php?option=com_content&task=view&id=15&Itemid=32. [Accès le 12 01 2019].

[5] «Digital Guide,» 04 12 2018. [En ligne]. Available: https://www.ionos.fr/digitalguide/serveur/know-how/cidr/. [Accès le 10 01 2019].

[6] Lycée de la mare carrée, *Routage NAT.*

[7] J.-F. PILLOU, «Commentçamarche.net,» 20 04 2011. [En ligne]. Available: https://www.commentcamarche.net/contents/527-nat-translation-d-adresses-port-forwarding-et-port-triggering. [Accès le 12 01 2019].

[8] CERT-FR, *Migration IPv6 : enjeux de sécurité,* Paris: CERTA-2006-INF-004-004, 2006.

[9] [En ligne]. Available: https://whstatic.1and1.com/help/CloudServer/FR/d857941.html.

[10] ipcisco, «ipcisco.com,» [En ligne]. Available: https://ipcisco.com/lesson/subnetting-in-ipv6-2/. [Accès le 12 2019].

[11] «www.memoireonline.com,» [En ligne]. Available: https://www.memoireonline.com/12/15/9316/m_Migration-des-reseaux-ipv4-vers-ipv67.html.

[12] «www.Omnisecu.com,» [En ligne]. Available: http://www.omnisecu.com/tcpip/ipv6/unicast-multicast-anycast-types-of-network-communication-in-ipv6.php.

[13] «NDP (Neighbor Discovery Protocol), fonctions de NDP, sollicitation et annonce de voisin, sollicitation de routeur et annonce,» [En ligne]. Available: www.omnisecu.com/tcpip/ipv6/ndp-neighbour-discovery-protocol-functions-of-ndp.php. [Accès le 19 Aôut 2019].

[14] M. Dorigny, «IT-Connect.fr,» 09 12 2013. [En ligne]. Available: https://www.it-connect.fr/ipv6-quest-ce-que-leui-64-13/. [Accès le 26 avril 2019].

[15] P. Anelli, B. Stévant, P.-U. Tournoux et J. Grouffaud, *L'intégration d'IPv6 dans l'Internet,* Institut Mines-Télécom / G6, 2015.

[16] Autorité de Régulationdes telecommunication/TC de cote d'ivoire, «GUIDE PRATIQUE DE MIGRATION VERS IPV6».

[17] MARC, «I23 TECHNOLOGIES,» 28 septembre 2015. [En ligne]. Available: https://i23technologies.wordpress.com/2015/09/14/ospfv3/. [Accès le 08 mai 2019].

[18] Marc, «https://i23technologies.wordpress.com/,» 22 septembre 2015. [En ligne]. Available: https://i23technologies.wordpress.com/. [Accès le 08 mai 2019].

[19] Marc, «i23technologies,» 22 septembre 2015. [En ligne]. Available: https://i23technologies.wordpress.com/2015/09/22/ipv6-stateful-configuration-dhcpv6/. [Accès le 08 mai 2019].

[20] V. Popeskic, «how does internet work,» [En ligne]. Available: https://howdoesinternetwork.com/2013/slaac. [Accès le 09 mai 2019].

[21] V. Popeskic, «HOW DOES INTERNET WORK,» 22 mars 2018. [En ligne]. Available: https://howdoesinternetwork.com/2013/slaac-ipv6-stateless-address-autoconfiguration. [Accès le 09 mai 2019].

[22] F. Goffinet, «cisco.goffinet.org,» 23 septembre 2019. [En ligne]. Available: https://cisco.goffinet.org/ccna/ipv6/plans-adressage-ipv6/. [Accès le octobre 2019].

[23] «cisco.goffinet.org,» [En ligne]. Available: https://cisco.goffinet.org/categories/ipv6. [Accès le octobre 2019].

[24] F. Goffinet, «cisco.goffinet.org,» 23 septembre 2019. [En ligne]. Available: https://cisco.goffinet.org/ccna/ipv6/introduction-adresses-ipv6/. [Accès le octobre 2019].

[25] T. A. Conta, C. S. S. Deering et é. T. N. M. Gupta, «Request for Comments : 4443,» mars 2006.

[26] oreilly Media, «www.oreilly.com,» [En ligne]. Available: https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch25s03.html. [Accès le 12 2019].

[27] Z. Tuo. [En ligne]. Available: https://www-l2ti.univ-paris13.fr/~zhang/contenu/TP6-IPv6-2014.pdf. [Accès le 2019].

[28] Cisco networking accademy, 2014. [En ligne]. Available: http://touchardinforeseau.servehttp.com/ccna2014/course/files/8.2.5.3%20Packet%20Tracer%20-%20Configuring%20IPv6%20Addressing%20Instructions.pdf. [Accès le 2019].

[29] A. MOUSSAUD, «supinfo.com,» 07 10 2016 . [En ligne]. Available: https://www.supinfo.com/articles/single/2459-configurer-router-ipv6. [Accès le 2019].

[30] ipcisco.com, «ipcisco.com,» [En ligne]. Available: https://ipcisco.com/lesson/ipv6-address-types-2/. [Accès le 2019].

[31] SHEFFERKIMANZI, «COMPUTER NETWORKING,» 5 JUILLET 2018. [En ligne]. Available: https://computernetworking747640215.wordpress.com/2018/07/05/basic-ipv6-configuration-in-packet-tracer-2/. [Accès le 2019].

Annexes

Annexe1 : Autorités attribuant les adresses IP et hiérarchie d'allocation d'adresse IPv6

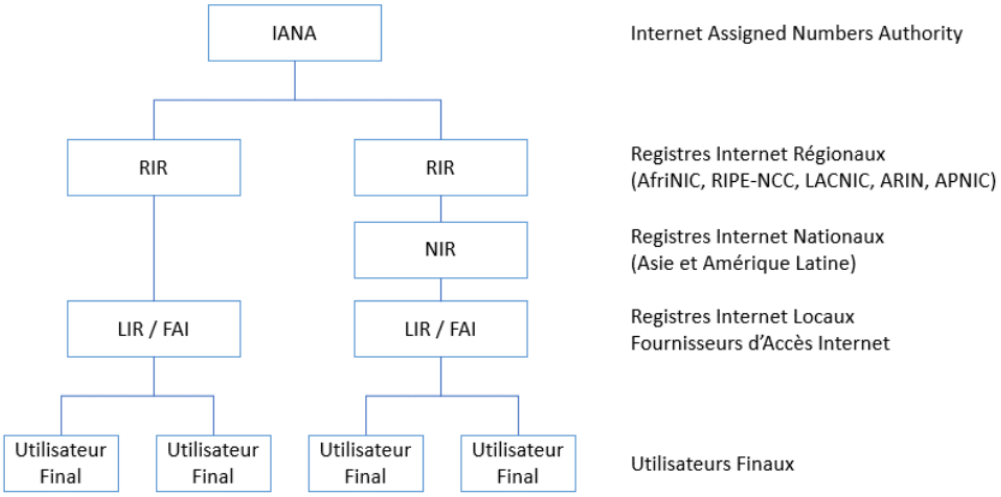


Figure 75:Autorités attribuant les adresses IP [15]

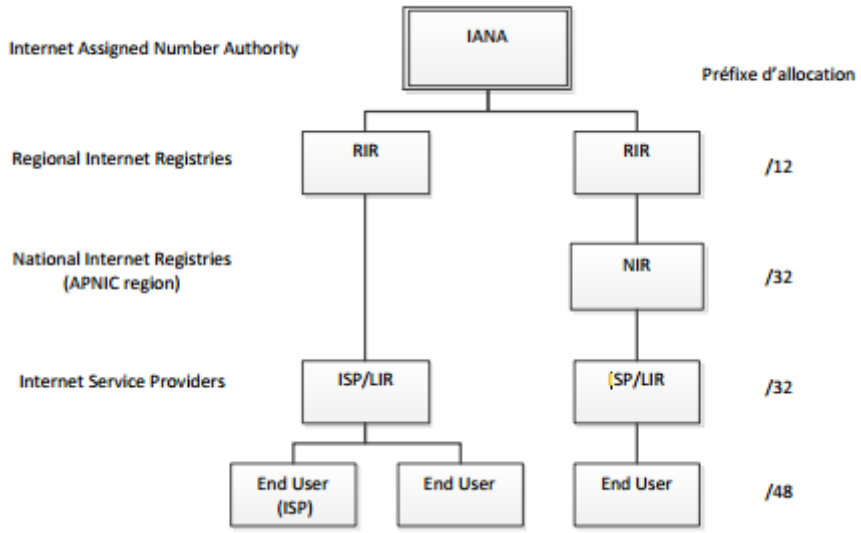


Figure 76: hiérarchie d'allocation d'adresse IPv6[5]

[5] Basé sur le graphique disponible à l'adresse http://www.ripe.net/ripe/docs/ripe-552

Annexe 2 Récapitulatif des préfixes

Type d'adresse	Préfixe binaire	Notation IPv6
Non-spécifié	00…0 (128 bits)	::/128
Localhost	00…1 (128 bits)	::1/128
IPv4-compatible (deprecated)	00…0 (96 bits)	::IPv4/128
IPv4-mapped	00..0 1111 1111 1111 1111	::ffff:IPv4/128
Global Unicast	001	2001::/3
Unique Local Unicast (ULA)	1111 110	fc00::/7
Lien-local Unicast	1111 1110 10	fe80::/10
Site-local Unicast (deprecated)	1111 1110 11	fec0::/10
Multicast	1111 1111	ff00/8
Réservé	Tout le reste	

Tableau 5: Récapitulatif des préfixes d'adresse

Annexe 3 : Entête Paquet IPv4 et IPv6

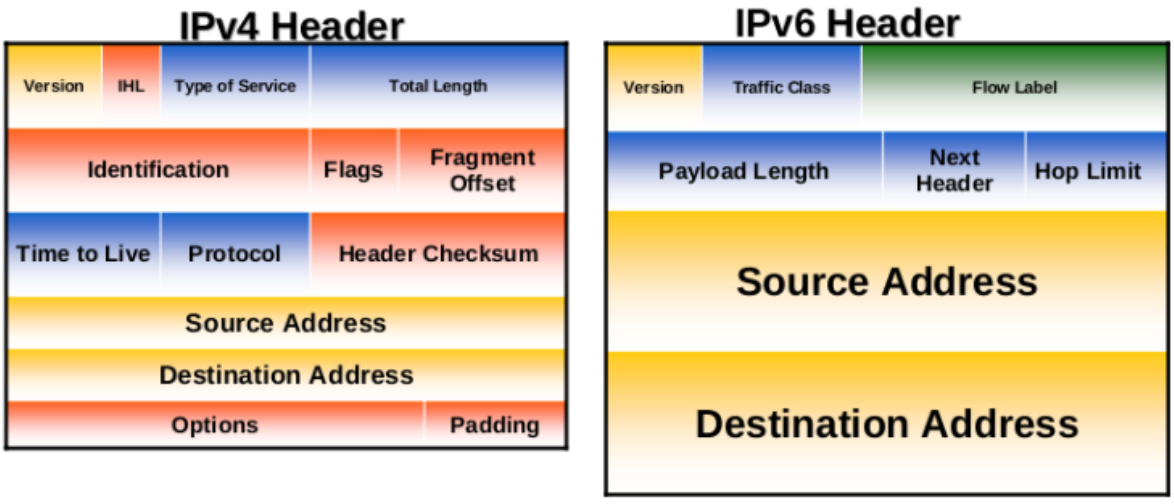


Figure 77: comparaison de l'en-tête IPv4 et IPv6 [1][6]

[6] • En jaune les champs du header IPv4 gardé en IPv6
• En rouge les champs n'ayant pas été conservés dans le header IPv6
• En bleu les champs ayant changé de nom et de position
• En vert le nouveau champ de l'en-tête IPv6

Annexe4 : Les principales différences entre IPv4 et l'IPv6

Caractéristique	IPv4	IPv6
Longueur d'adresse	32 bits	128 bits
Support de la QoS	Existant	Amélioré
Fragmentation	Par l'émetteur et les routeurs	Par l'émetteur seulement
Taille du paquet	576 octets	1280 octets
Checksum dans l'en-tête	Oui	Non
Option dans l'en-tête	Non	Non
Résolution d'adresse	ARP en broadcast	Multicast Neighbor Discovery
Multicast membership	IGMP	Multicast Listener Discovery
Découverte de routeur	En option	Requise
Utilisation du broadcast	Oui	Non
Configuration d'IP	Manuelle ou DHCP	Manuelle, automatique, DHCP
Requête de nom DNS	A records	AAAA records
Requête DNS inverse	IN-ADDR.ARPA DNS IP6.ARPA	IP6.ARPA

Tableau 6: Différences entre IPv4 et IPv6