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

Université Abderahmane Mira de BEJAIA
Faculté des Sciences Exactes
Département Informatique

Mémoire de Fin de Cycle En vue de l'obtention du diplome de Master en Informatique

Option
Administration et Sécurité des Réseaux

Thème

Technique d'immigration IPv4 vers IPv6

Réalisé par :

Mr.KADRI Belkacem

Mr.MAHDI Badderdine

Soutenu le 29 Septembre 2022, Devant le jury composé de :

Président	**Dr A. BOUKERRAM Samira**	**Maître assistant. A**	**U. A/Mira Béjaia.**
Examinateur	**Dr B. AISSANI Soufiane**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Encadrant	**Dr C. MOKTEFI Mohand**	**Maître de conf. B**	**U. A/Mira Béjaia.**

Béjaia, Septembre 2022.

Table des matières

Table des figures

Remerciment

On remercie ALLAH qui nous a donné la santé et la force pour réaliser ce memoire ainsi que notre promoteur M*r* MOKTEFI MOHAND d'avoir accepté de nous encadrer, et de nous suivre durant toute l'année en assurant le suivi scientifique et technique du présent mémoire. On le remercie pour sa grande contribution à l'aboutissement de ce travail.
Veuillez, cher Maitre, trouvé dans ce modeste travail l'expression de notre haute considération, de notre sincère reconnaissance et de notre profond respect.
Nos remerciements vont aussi aux membres du jury pour l'honneur qu'ils nous ont faits en acceptant de juger ce modeste travail.
Pour conclure, nous tenons à remercier nos chères familles respectives maternelles et paternelles et tous ceux qui ont participé de près ou de loin à l'élaboration de ce travail.

Dédicace

Je dédie ce mémoire
À Yemma qui m'a soutenu et encouragé durant ces années d'études.
Qu'elle trouve ici le témoignage de ma profonde reconnaissance.
À mon frère, mon père à ma famille et ceux qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail. Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.
A tous mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de succès et à mon chér ami OUAZENE BILAL qui m'a accompagné durant la réalisation de ce mémoire.

Introduction

❑ IPv4 manque d'adresses. C'est pourquoi les administrateurs réseau devraient se familiariser avec IPv6. Le protocole IPv6 est conçu pour être le successeur de l'IPv4. L'IPv6 possède un plus grand espace d'adressage de 128 bits pour un total de 340 undécillions (c'est-à-dire 340 suivi de 36 zéros) d'adresses disponibles.

Avec le nombre toujours croissant d'appareils mobiles, les fournisseurs de téléphonie mobile ont été à l'avant-garde de la transition vers l'IPv6. Les deux principaux fournisseurs de téléphonie mobile aux États-Unis indiquent que plus de 90% de leur trafic passe par IPv6. La pluPartie des principaux FAI (fournisseur d'accès internet) et fournisseurs de contenu tels que YouTube, Facebook et NetFlix ont également fait la transition. De nombreuses entreprises comme Microsoft, Facebook et LinkedIn sont entrain de passer à l'IPv6 uniquement en interne. En 2018, le FAI à haut débit Comcast a fait état d'un déploiement de plus de 65% et British Sky Broadcasting de plus de 86%.

Par rapport aux dernières décennies, l'Internet d'aujourd'hui est sensiblement différent. Désormais, Internet est principalement utilisé pour la messagerie électronique, la navigation sur le web et le transfert de fichiers entre ordinateurs. Internet est en passe de devenir un Internet des objets. Les appareils pouvant accéder à Internet ne sont plus seulement des ordinateurs, des tablettes et des smartphones. Demain, les appareils connectés et équipés de capteurs concerneront tous les objets du quotidien, notamment les automobiles, les équipements biomédicaux, l'électroménager, et même les écosystèmes naturels. Avec l'utilisation croissante d'Internet, un espace limité d'adresses IPv4, des problèmes liés à la fonction NAT et l'Internet of Everything, le moment est venu d'entamer la transition vers IPv6.

L'objectif de ce mémoire est de réaliser un manuel de référence contenant toutes les bonnes pratiques et les différentes techniques de *"L'immigration vers L'IPv6 "* en s'assurant que la sécurité fait partie de notre plan de transition, pour atteindre cet objectif, nous avons organisé notre mémoire en 4 chapitres dont le contenu est brièvement décrit dans les points suivants :

➟ Le premier chapitre intitulé ≺ `Adressage IPv6` ≻: Explique comment les adresses IPv6 sont représentées, Comparer les types d'adresses réseau IPv6, la configuration d'adresse IPv6 monodiffusion globale et les adresses réseau IPv6 link-local statiquement et dynamiquement et enfin identifier des adresses IPv6 et segmenter un réseau IPv6.

➟ Le deuxième chapitre intitulé ≺ `La sécurité IPv6` ≻: Explique l'avantage qu'IPv6 à apporter en termes de sécurité, comment examiner les menaces contre un réseau IPv6 puis décrit les moyens de les combattre en appliquant les meilleures pratiques actuelles.

➟ Le troisième chapitre intitulé ≺ `Sécuriser les mécanismes de transitions` ≻:
Aborde les différentes techniques qui sont utilisées pour aider les organisations à migrer d'IPv4 à IPv6. Les techniques de migration Dual-stack, tunnel, et NAT sont abordées ainsi que leurs problèmes de sécurité et leurs propres solutions de sécurité.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

Chapitre I

Adressage IPv6

I.1 Introduction

Une adresse IPv4 comporte 32 bits et a un aspect familier. Une adresse IPv6 possède 128 bits et semble complexe au premier coup d'œil. L'extension de l'espace d'adressage a été l'une des principales raisons du développement d'IPv6, ainsi que l'optimisation des tables de routage, en particulier sur Internet. Il y a beaucoup plus à comprendre que l'adresse de 128 bits.L'architecture d'adressage a été étendue et le vaste espace d'adressage offre la possibilité de concevoir de nouvelles adresses (L'architecture d'adressage IPv6 est définie dans la RFC 4291). Donc un administrateur réseaux doit travailler sur un plan d'adressage avant de plonger dans le domaine de L'IPv6.Ce chapitre vous aidera à vous familiariser avec l'espace d'adressage étendu et vous expliquera également le fonctionnement de l'adressage IPv6 et pourquoi il a été conçu de cette manière.

I.2 Formats d'adresses IPv6

Les adresses IPv6 sont bien plus vastes que les adresses IPv4, les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales. Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique,pour un total de 32 valeurs hexadécimales, comme l'illustre la figure. Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.

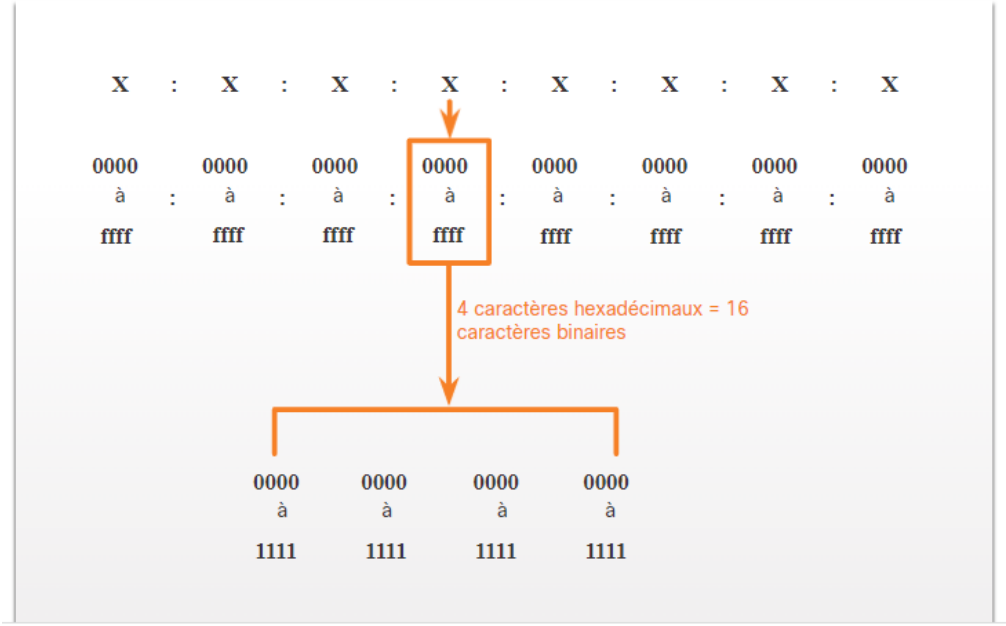


FIGURE I.1 – Segments ou hextets 16 bits

I.2.1 Format Préféré

Comme le montre la figure précédente, le format préféré pour écrire une adresse IPv6 est x :x :x :x :x :x :x :x, chaque "x" étant constitué de quatre valeurs hexadécimales. Le terme octet fait référence aux huit bits d'une adresse IPv4. Pour les adresses IPv6, hextet est le terme officieux qui désigne un segment de 16 bits ou de quatre valeurs hexadécimales. Dans la section suivante, nous verrons deux règles permettant de réduire le nombre de chiffres requis pour représenter une adresse IPv6. Cela présente des exemples d'adresses IPv6 au format privilégié.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

```
2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000: 0200
2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000: 1234
2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a: 19ac
2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000: 0000
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
fe80 : 0000 : 0000 : 0000 : c012 : 9aff : fe9a: 19ac
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0000
```

FIGURE I.2 – exemples d'adresses IPv6 au format privilégié

.

I.2.2 Règle 1 - Omettre les zéros en début de segment

La première règle pour réduire la notation des adresses IPv6 consiste à omettre les zéros (0) du début d'une section de 16 bits (ou hextet). Voici quatre exemples de façons d'omettre les zéros principaux :

- ➥ 01AB est équivalent à 1AB
- ➥ 09f0 est équivalent 9f0
- ➥ 0a00 est équivalent a00
- ➥ 00AB est équivalent à AB

❑ Cette règle s'applique uniquement aux zéros de début de segment et NON aux zéros de fin. L'omission de ces derniers rendrait l'adresse ambiguë. Par exemple, l'hextet "abc" peut être "0abc" ou "abc0", mais ce sont deux valeurs différentes comme illustre la figure suivante :

Type	Format
Recommandé	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Sans zéros en début de segment	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200
Recommandé	2001 : 0db8 : 0000 : 00a3 : ab00 : 0ab0 : 00ab : 1234
Sans zéros en début de segment	2001 : db8 : 0 : a3 : ab00 : ab0 : ab : 1234
Recommandé	2001 : 0db8 : 000a : 0001 : c012 : 90ff : fe90 : 0001
Sans zéros en début de segment	2001 : db8 : a : 1 : c012 : 90ff : fe90 : 1
Recommandé	2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000
Sans zéros en début de segment	2001 : db8 : aaaa : 1 : 0 : 0 : 0 : 0

FIGURE I.3 – Omission des zéros en début de segment

.

I.2.3 Règle 2 - Double deux-points

La deuxième règle permettant d'abréger la notation des adresses IPv6 est qu'une suite de deux fois deux points (: :) peut remplacer toute chaîne unique et contiguë d'un ou plusieurs segments de 16 bits (hextets) composés uniquement de zéros. Par exemple 2001 :db8 :cafe :1 :0 :0 :0 :1 (0 premiers omis) pourrait être représenté comme 2001 :db8 :cafe :1 : :1. Le double deux-points (: :) est utilisé à la place des trois hextets tout-0 (0 :0 :0). Une suite de deux fois deux points (: :) peut être utilisée une seule fois par adresse : sinon, il

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

serait possible d'aboutir sur plusieurs adresses différentes. Lorsque l'omission des zéros de début de segment est utilisée, la notation des adresses IPv6 peut être considérablement réduite. Il s'agit du "format compressé". Voici un exemple d'utilisation incorrecte du double deux-points : 2001 :db8 : :abcd : :1234. Le double deux-points est utilisé deux fois dans l'exemple ci-dessus. Voici les extensions possibles de cette adresse de format compressée incorrecte :

- 2001 :db8 : :abcd :0000 :0000 :1234
- 2001 :db8 :0000 :abcd : :1234
- 2001 :db8 :0000 :0000 :abcd : : 1234

Type	Format
Recommandé	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressés/Espaces	2001 : db8 : 0 : 1111 : : 200
Compressé	2001:db8:0:1111::200
Recommandé	2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000
Compressés/Espaces	2001 : db8 : 0 : 0 : ab00 ::
Compressé	2001:db8:0:0:ab00::
Recommandé	2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000
Compressés/Espaces	2001 : db8 : aaaa : 1 ::
Compressé	2001:db8:aaaa:1::
Recommandé	fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdef
Compressés/Espaces	fe80 : : 123 : 4567 : 89ab : cdef
Compressé	fe80::123:4567:89ab:cdef
Recommandé	fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
Compressés/Espaces	fe80 : : 1
Compressé	fe80::1

FIGURE I.4 – Omettre les zéros en début et les séquences composées uniquement de zéros

.

I.3 Types d'adresses IPv6

Comme avec IPv4, il existe différents types d'adresses IPv6. En fait, il existe trois grandes catégories d'adresses IPv6 :

❶ Monodiffusion : Une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique.

❷ Multidiffusion : Une adresse de multidiffusion IPv6 est utilisée pour envoyer un seul paquet IPv6 vers plusieurs destinations.

❸ Anycast :Une adresse anycast IPv6 est une adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques. Un paquet envoyé à une adresse anycast est acheminé vers le périphérique le plus proche ayant cette adresse.

I.3.1 Longueur de préfixe IPv6

- Le préfixe (ou la partie réseau) d'une adresse IPv4 peut être identifié par un masque de sous-réseau en notation décimale à point ou une longueur de préfixe (notation de barre oblique). Par exemple :l'adresse IPv4 192.168.1.10 et le masque de sous-réseau en notation décimale à point 255.255.255.0 correspondent à 192.168.1.10/24.

- Dans IPv4, le /24 est appelé le préfixe. Dans IPv6, il est appelé la longueur du préfixe.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

➟ Le protocole IPv6 n'utilise pas la notation décimale à point du masque de sous-réseau. La longueur du préfixe IPv6 est utilisée pour indiquer la partie réseau de l'adresse IPv6.La longueur de préfixe peut être comprise entre 0 et 128.

➟ Il est fortement recommandé d'utiliser un ID d'interface 64 bits pour la pluPartie des réseaux comme illustré dans la figure 9.En effet, la configuration automatique d'adresse sans état (SLAAC) utilise 64 bits pour l'ID d'interface. Il facilite également la création et la gestion des sous-réseaux.

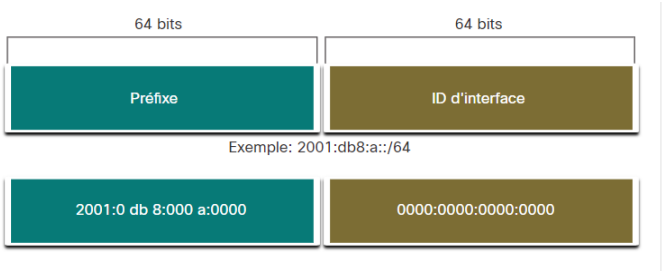


FIGURE I.5 – Longueur de préfixe IPv6

.

I.3.2 Autres types d'adresses IPv6 de monodiffusion

I.3.3 Adresses IPv6 de monodiffusion

Un paquet envoyé à une adresse de monodiffusion est reçu par l'interface correspondant à cette adresse. Comme c'est le cas avec l'IPv4, une adresse source IPv6 doit être une adresse de monodiffusion. L'adresse IPv6 de destination peut, quant à elle, être une adresse de monodiffusion ou de multidiffusion. La figure montre les différents types d'adresses de monodiffusion IPv6.

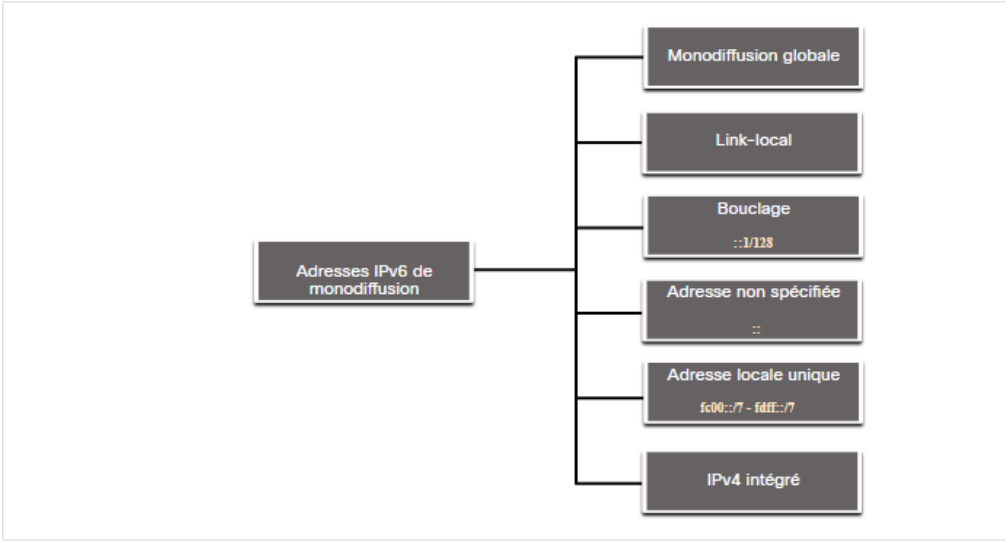


FIGURE I.6 – Adresses de monodffusion

.

❑ Contrairement aux périphériques IPv4 qui n'ont qu'une seule adresse, les adresses IPv6 ont généralement deux adresses monodiffusion :

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

❶ **Adresse GUA (Global Unicast Address)** : Cette adresse est similaire à une adresse IPv4 publique. Ces adresses sont uniques au monde et routables sur Internet. Configurées de manière statique ou attribuées dynamiquement.

❷ **Adresse LLA (Link-Local Address)** : Ceci est requis pour chaque périphérique compatible IPv6.Les LLAs sont utilisées pour communiquer avec d'autres équipements sur la même liaison, les routeurs ne transmettent aucun paquet avec une adresse source ou de destination link-local.

Les adresses locales uniques (gamme fc00 : :/7 à fdff : :/7) ne sont pas encore couramment implémentées.Les adresses locales uniques peuvent éventuellement être utilisées pour adresser des périphériques qui ne devraient pas être accessibles depuis l'extérieur, tels que des serveurs internes et des imprimantes.

Remarque :

⇨ De nombreux sites utilisent également le caractère privé des adresses RFC 1918 pour sécuriser ou masquer leur réseau et limiter les risques. Cependant, ce n'est pas le but premier de ces technologies et l'IETF a toujours recommandé que les sites prennent les précautions de sécurité nécessaires au niveau de leur routeur connecté à Internet.

I.3.4 GUA IPv6

❑ L'ICANN (Internet Committee for Assigned Names and Numbers), opérateur de l'IANA, attribue des blocs d'adresses IPv6 aux cinq organismes d'enregistrement Internet locaux. Actuellement, seules des adresses de monodiffusion globale dont les premiers bits sont 001 ou 2000 : :/3 sont attribuées. La figure montre la plage de valeurs pour le premier hextet où le premier chiffre hexadécimal pour les GUA actuellement disponibles commence par un 2 ou un 3.

Remarque :

⇨ L'adresse 2001 :0DB8 : :/32 a été réservée à des fins de documentation, notamment pour être utilisée dans des exemples.Le graphique montre les trois parties d'une GUA : d'abord le préfixe de routage global, puis l'ID de sous-réseau, puis enfin l'ID d'interface. Les trois premiers bits du préfixe de routage global sont 001. La plage du premier hextexte est comprise entre 0010 0000 0000 0000 (2000) et 0011 1111 1111 1111 1111 (3fff).

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

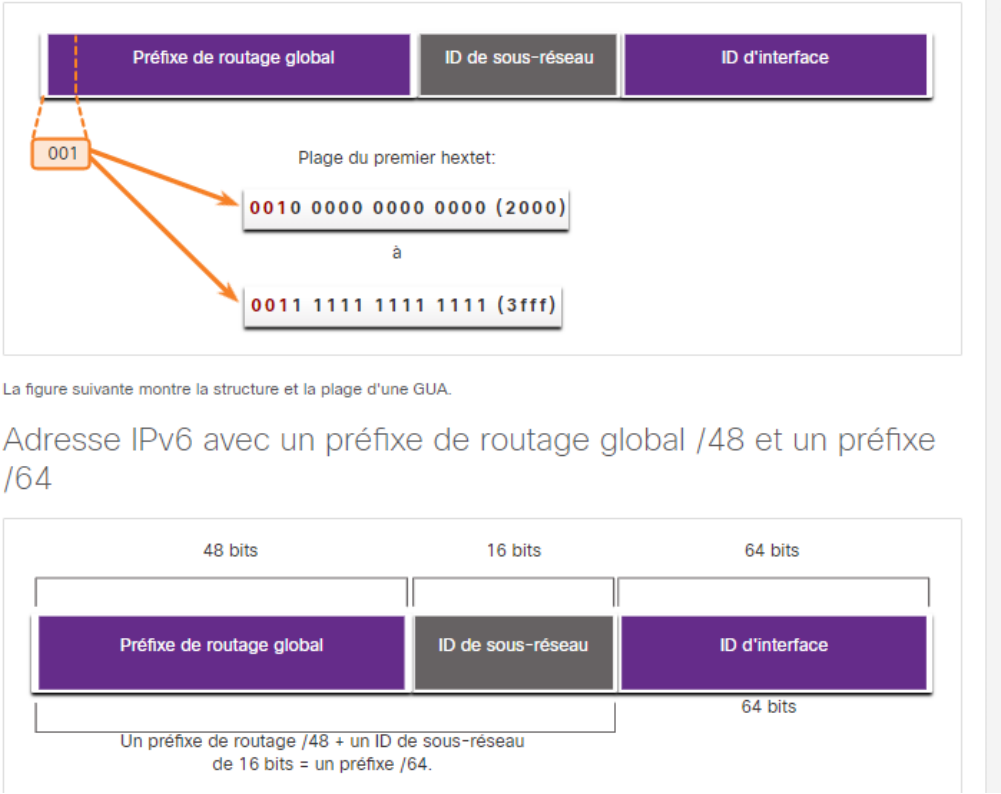


FIGURE I.7 – La GUA IPv6

.

I.4 Structure de GUA IPv6

I.4.1 Préfixe de Routage Global

- ➟ Le préfixe de routage global est le préfixe ou la partie réseau de l'adresse attribué(e) par le fournisseur (par exemple un FAI) à un client ou à un site.
- ➟ La taille du préfixe global de routage détermine la taille de l'ID de sous-réseau.
- ➟ Les préfixes /48 sont les préfixes de routage global les plus couramment attribués. Par exemple, l'adresse IPv6 2001 :0DB8 :ACAD : :/48 a un préfixe indiquant que les 48 premiers bits (3 hextets) (2001 :0DB8 :ACAD) constituent le préfixe ou la partie réseau de l'adresse. La suite de deux fois deux points (: :) avant la longueur de préfixe /48 signifie que le reste de l'adresse contient uniquement des 0.

I.4.2 ID de Sous-Réseau

- ❑ Le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface. Contrairement à IPv4 où vous devez emprunter des bits de la partie hôte pour créer des sous-réseaux, IPv6 a été conçu avec le sous-réseau à l'esprit. L'ID de sous-réseau 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.

Note :

- ➢ De nombreuses organisations reçoivent un préfixe de routage global /32. L'utilisation du préfixe /64 est recommandé pour créer un ID d'interface 64 bits. Cela signifie qu'une organisation avec un préfixe de routage global /32 et un ID de sous-réseau 32 bits aura 4,3 milliards de sous-réseaux.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

I.4.3 ID de L'interface

➟ L'ID d'interface IPv6 est l'équivalent de la partie hôte d'une adresse IPv4. Le terme ID d'interface est utilisé, car un hôte unique peut avoir plusieurs interfaces,chacune dotée d'une ou de plusieurs adresses IPv6.

Remarque :

⇨ contrairement à l'adressage IPv4, avec IPv6, les adresses d'hôte contenant uniquement des 0 ou uniquement des 1 peuvent être attribuées à un périphérique L'adresse tout-1 peut être utilisée car les adresses de diffusion ne sont pas utilisées dans IPv6. L'adresse contenant uniquement des 0 ne doit être attribuée qu'aux routeurs.

I.4.4 Configuration GUA statique sur un routeur

❑ Il est facile de configurer statiquement les GUA et LLA IPv6 sur les routeurs pour vous aider à créer un réseau IPv6,la commande pour configurer une GUA IPv6 sur une interface est **ipv6-address/prefix-length.** Notez qu'il n'y a aucun espace entre l'adresse IPv6 et la longueur du préfixe.La configuration utilisée en exemple utilise la topologie de la figure et les sous-réseaux IPv6 suivants :

➟ 2001 :db8 :acad :1 : /64

➟ 2001 :db8 :acad :2 : /64

➟ 2001 :db8 :acad :3 : /64

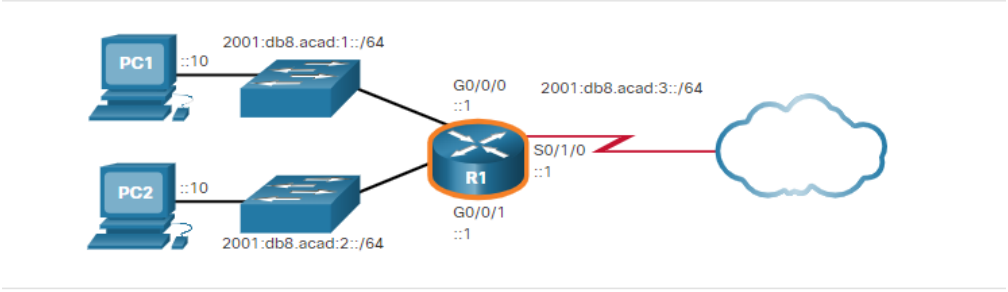


FIGURE I.8 – Exemple de topologie

❑ La figure indique également les commandes nécessaires pour configurer l'adresse de diffusion globale IPV6 sur les interfaces Gigabit Ethernet 0/0/0, GigabitEthernet 0/0/1 et Série 0/0/0 de R1.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# Interface série 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

FIGURE I.9 – Configuration de GUA IPv6 sur le routeur R1

‘

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

I.4.5 Configuration statique de GUA sur un hôte Windows

- La configuration manuelle de l'adresse IPv6 sur un hôte est similaire à celle d'une adresse IPv4.Comme le montre la figure, l'adresse de la passerelle par défaut configurée pour PC1 est 2001 :DB8 :ACAD :1 : :1. Il s'agit de l'adresse de diffusion globale de l'interface GigabitEthernet de R1 sur le même réseau.

  L'adresse de la passerelle par défaut configurée peut également être celle de l'adresse link-local de l'interface GigabitEthernet. L'utilisation de la LLA du routeur comme adresse de passerelle par défaut est considérée comme la meilleure pratique. Ces deux configurations fonctionnent.

  Tout comme avec l'IPv4, la configuration des adresses statiques sur les clients ne convient pas aux environnements de grande taille. Pour cette raison, la pluPartie des administrateurs de réseaux IPv6 utilisent l'attribution dynamique des adresses IPv6.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

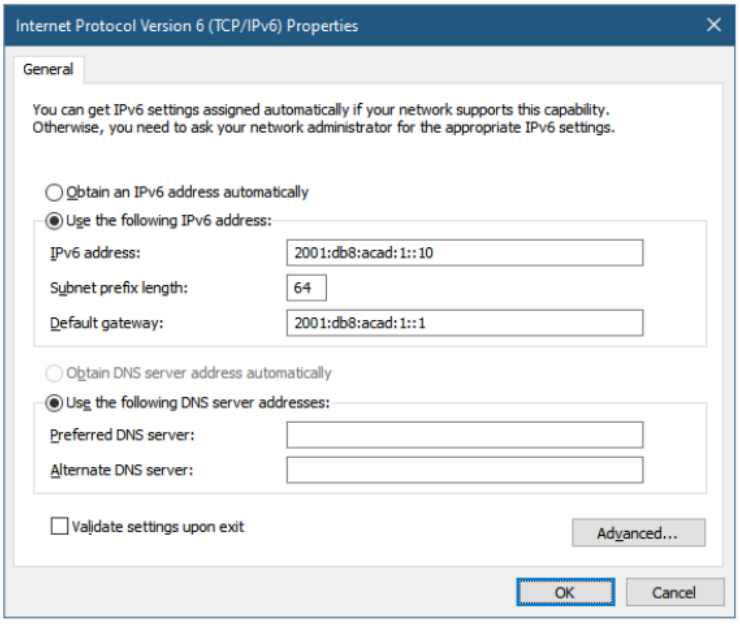


FIGURE I.10 – Configuration statique de GUA sur un hôte Windows

Un périphérique peut obtenir automatiquement une adresse de diffusion globale IPv6 de deux façons :

❶ SLAAC (configuration automatique des adresses sans état)

❷ DHCPv6 avec état.

Remarque :

⇨ Lorsque la méthode DHCPv6 ou SLAAC est utilisée, l'adresse link-local du routeur local est automatiquement définie comme étant l'adresse de la passerelle par défaut.

I.5 IPv6 LLA

I.5.1 Présentation

❑ Les ALL IPv6 se trouvent dans la plage fe80 : :/10. /10 Indique que les 10 premiers bits sont 11111110 10xx xxxx. Le premier hextet dispose d'une plage comprise entre 1111 1110 1000 0000 (fe80) et 1111 1110 1011 1111 (febf). Si une adresse link-local n'est pas configurée manuellement sur une interface, le périphérique crée automatiquement sa propre adresse sans communiquer avec un serveur DHCP même si aucune adresse de monodiffusion globale IPv6 n'a été attribuée aux périphériques. La figure présente un exemple de transmission à l'aide d'adresses link-local IPv6. Le PC est capable de communiquer directement avec l'imprimante à l'aide des LLA.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

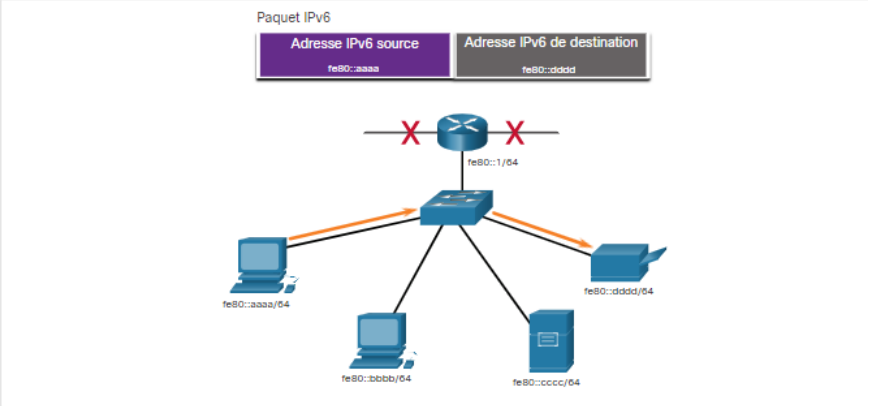


FIGURE I.11 – Communications link-local IPv6

➢ La figure suivante montre certaines utilisations des LLA IPv6 :

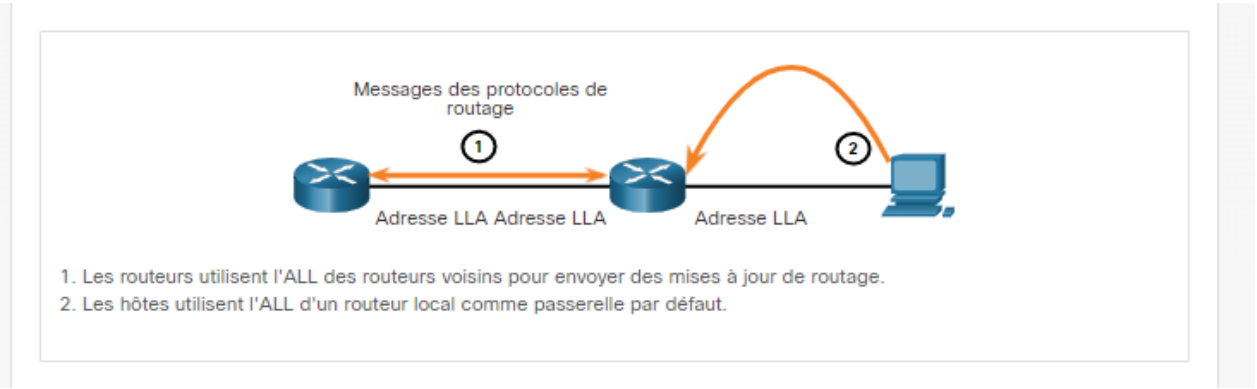


FIGURE I.12 – Utilisations des LLA IPv6.

I.5.2 Les méthodes d'obtention d'une LLA

Un périphérique peut obtenir un LLA de deux façons :

❶ **Statique** : Cela signifie que le périphérique a été configuré manuellement.

❷ **Dynamique** :Cela signifie que le périphérique crée son propre ID d'interface en utilisant des valeurs générées aléatoirement ou en utilisant la méthode Extended Unique Identifier (EUI), qui utilise l'adresse MAC du client avec des bits supplémentaire

I.6 Les GUA de l'adressage Dynamique de l'IPV6

I.6.1 Messages RS et RA

❑ La pluPartie des périphériques obtiennent leurs GUA IPv6 dynamiquement à l'aide des messages de publicité de routeur (RA) et de sollicitation de routeur (RS). Il ya une grande différence entre les trois méthodes qu'une publicité de routeur peut utiliser, ainsi que la façon dont le processus EUI-64 pour créer un ID d'interface diffère d'un processus généréaléatoirement Pour le GUA, un périphérique obtient

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

l'adresse dynamiquement via des messages ICMPv6 (Internet Control Message Protocol version 6). Les routeurs IPv6 envoient des messages d'annonce de routeur ICMPv6 toutes les 200 secondes à tous les périphériques IPv6 du réseau.Un message d'annonce de routeur est également envoyé en réponse à un hôte qui envoie un message de sollicitation de routeur ICMPv6, qui est une demande de message RA. Les deux messages sont affichés sur la figure.

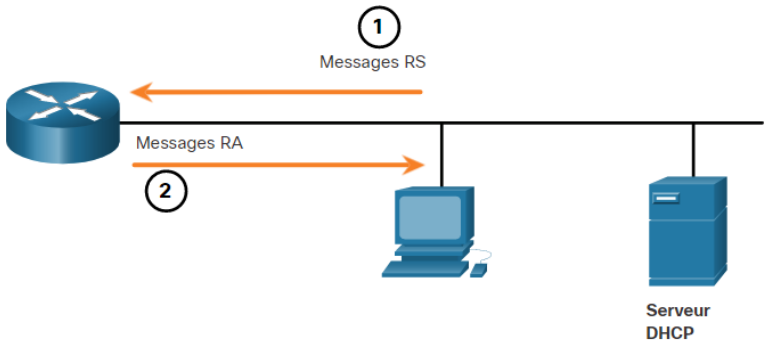


FIGURE I.13 – Messages RS et RA ICMPv6

❑ Les messages RA sont sur les interfaces Ethernet du routeur IPv6. Le routeur doit être activé pour le routage IPv6, ce qui n'est pas activé par défaut. Pour sélectionner l'IPv6 sur un routeur,la commande de configuration globale **ipv6 unicast-routing** doit être utilisée.Le message d'annonce de routeur ICMPv6 indique à un périphérique comment obtenir une adresse de diffusion globale IPv6. La décision finale revient au système d'exploitation de l'appareil. Le message d'annonce de routeur(RA) contient les éléments suivants :

1) **Le préfixe de réseau et la longueur de préfixe :** qui indiquent au périphérique le réseau auquel il appartient.
2) **l'adresse de la passerelle par défaut :** qui est une adresse link-local et l'adresse IPv6 source du message d'annonce de routeur.
3) **les adresses DNS et le nom de domaine :** Ils sont des adresses des serveurs DNS et un nom de domaine.

Il existe trois méthodes pour les messages RA :

➟ **Method 1 : SLAAC** : "J'ai tout ce dont vous avez besoin, y compris le préfixe, la longueur du préfixe et l'adresse de passerelle par défaut".

Le message d'annonce de routeur suggère au périphérique récepteur d'utiliser les informations qu'il contient pour créer sa propre adresse de diffusion globale IPv6,Comme le montre la figure 20, les deux parties de l'adresse sont créées comme suit :

❶ **Préfixe** :Ceci est annoncé dans le message RA.
❷ **ID d'interface** : il utilise la méthode EUI-64 ou est obtenu par la génération d'un nombre à 64 bits aléatoire, selon le système d'exploitation de l'appareil.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

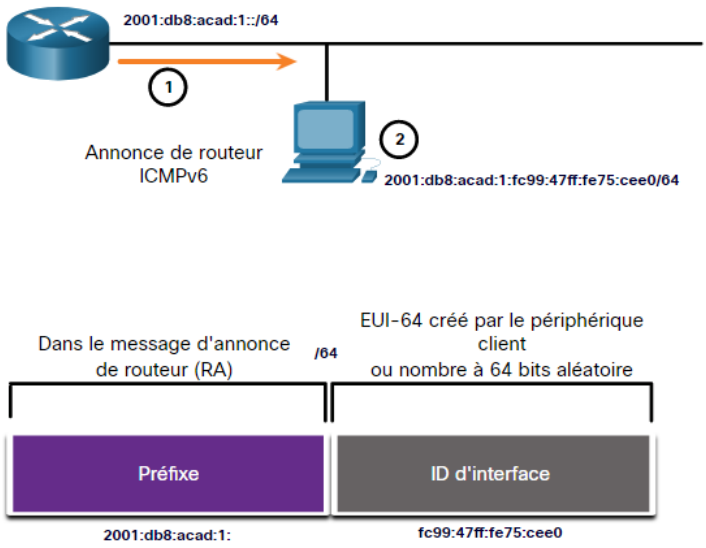
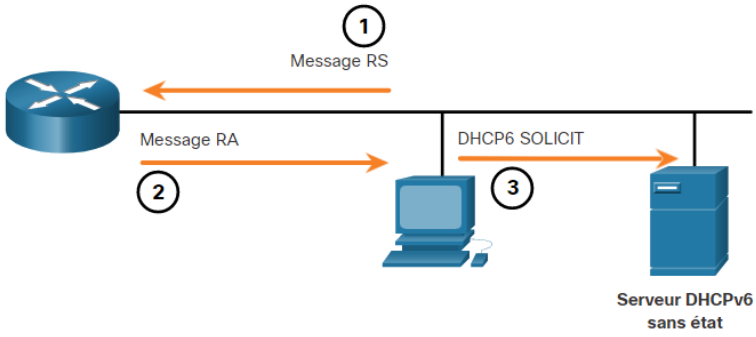


FIGURE I.14 – SLAAC

❑ **Method 2 : SLAAC avec un serveur DHCPv6 sans état** : "Voici mes coordonnées, mais vous avez besoin d'informations complémentaires telles que les adresses DNS d'un serveur DHCPv6".Un serveur DHCPv6 sans état distribue les adresses des serveurs DNS et les noms de domaine. Il n'alloue pas les GUA.



1. Le PC envoie un RS à tous les routeurs IPv6, «J'ai besoin d'informations d'adressage».
2. Le routeur envoie un message RA à tous les nœuds IPv6 avec la méthode 2 (SLAAC et DHCPv6) spécifiée. Voici votre préfixe, une longueur de préfixe et des informations sur la passerelle par défaut. Mais vous aurez besoin d'obtenir des informations DNS à partir d'un serveur DHCPv6.»
3. Le PC envoie un message de sollicitation DHCPv6 à tous les serveurs DHCPv6. J'ai utilisé SLAAC pour créer mon adresse IPv6 et obtenir mon adresse de passerelle par défaut, mais j'ai besoin d'autres informations d'un serveur DHCPv6 sans état.

FIGURE I.15 – SLAAC et DHCPv6 sans état

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

❑ **Method 3 : Stateful DHCPv6 (pas de SLAAC)** : "Je peux vous donner votre adresse de passerelle par défaut. Vous devez demander à un serveur DHCPv6 avec état pour toutes vos autres informations".Comme le montre la figure, avec cette méthode, le message RA suggère que les appareils utilisent ce qui suit : l'adresse link-local du routeur, l'adresse IPv6 source du message d'annonce de routeur comme adresse de la passerelle par défaut. un serveur DHCPv6 avec état pour obtenir une adresse de diffusion globale,l'adresse d'un serveur DNS, un nom de domaine et toutes les autres informations.

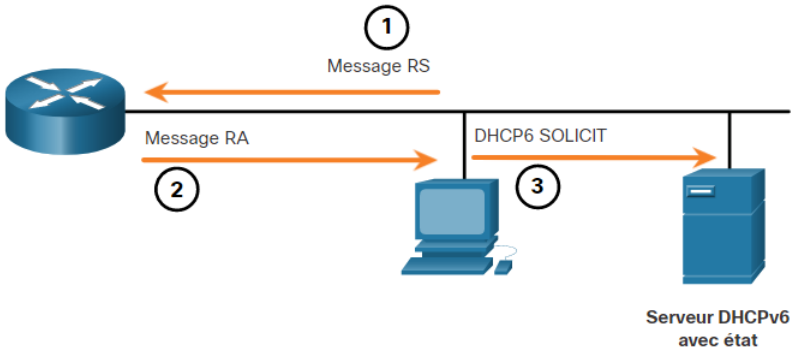


FIGURE I.16 – DHCPv6 avec état

Remarque :

⇨ L'adresse de la passerelle par défaut peut uniquement être obtenue de manière dynamique à partir du message d'annonce de routeur. Le serveur DHCPv6 avec ou sans état ne fournit pas l'adresse de la passerelle par défaut.

I.6.2 Méthode EUI-64 et génération aléatoire

❑ Le client connaît la partie préfixe de l'adresse grâce au message d'annonce, mais il doit créer son ID d'interface. L'ID de L'interface peut utiliser la méthode EUI-64 ou un nombre à 64 bits généré aléatoirement, comme le montre la figure :

I.6.3 Méthode EUI-64

❑ L'IEEE a défini l'identifiant unique étendu (EUI), ou format EUI-64 modifié. Ce processus utilise l'adresse MAC Ethernet à 48 bits d'un client et insère 16 autres bits au milieu de cette adresse MAC pour créer un ID d'interface de 64 bits. Les adresses MAC Ethernet sont généralement représentées au format hexadécimal et sont constituées de deux parties :

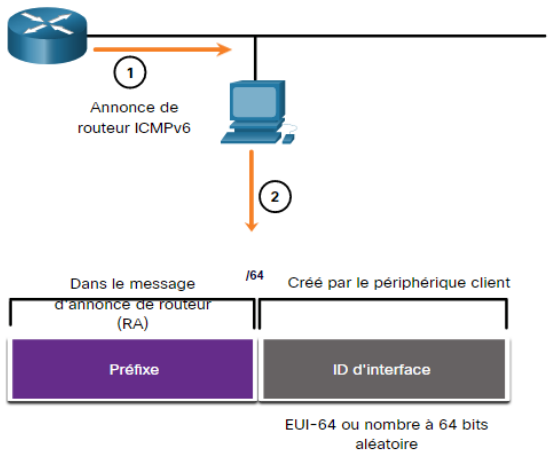
❶ **Identifiant unique d'entité (OUI)** :Un code de fournisseur de 24 bits (6 caractères hexadécimaux) attribué par l'IEEE.

❷ **ID de périphérique** : Une valeur unique de 24 bits (6 caractères hexadécimaux) contenue dans un OUI standard.

Un ID d'interface EUI-64 est représenté au format binaire et comprend trois parties :

❶ le code OUI sur 24 bits, provenant de l'adresse MAC du client, mais dont le septième bit (universellement/localement, U/L) est inversé. Cela signifie que si le septième bit est un 0, il devient un 1, et vice versa.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021



1. Le routeur envoie un message RA
2. Le PC utilise le préfixe dans le message RA et utilise EUI-64 ou un nombre 64 bits aléatoire pour générer un ID d'interface

FIGURE I.17 – Création dynamique d'un ID d'interface

❷ La valeur de 16 bits FFFE intégrée (au format hexadécimal).

❸ ID de périphérique de 24 bits de l'adresse MAC du client.

Le processus EUI-64 est présenté à la figure, avec l'adresse MAC GigabitEthernet FC99 :4775 :CEE0 de R1.

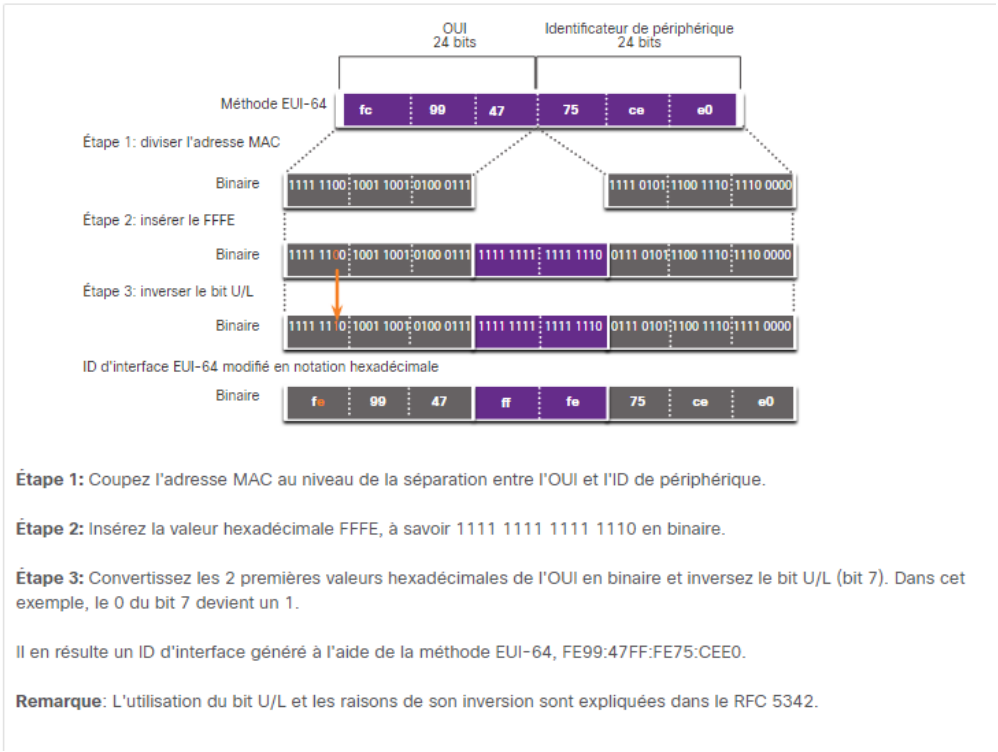


FIGURE I.18 – Le processus EUI-64

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

L'exemple de sortie de la commande **ipconfig** montre la GUA IPv6 créée dynamiquement à l'aide de SLAAC et du processus EUI-64.Pour savoir si une adresse a été créée via la méthode EUI-64 il suffit d'analyser la valeur fffe située dans l'ID d'interface.

FIGURE I.19 – ID d'interface généré par la méthode EUI-64

L'avantage de la méthode EUI-64 est que l'adresse MAC Ethernet peut être utilisée pour déterminer l'ID d'interface. Elle permet également aux administrateurs réseau de suivre facilement une adresse IPv6 jusqu'à un périphérique final en utilisant une adresse MAC unique. Cependant, cela a causé des problèmes de confidentialité parmi de nombreux utilisateurs qui craignaient que leurs paquets puissent être retracés jusqu'à l'ordinateur physique réel. Pour éviter ce problème, un ID d'interface généré aléatoirement peut également être utilisé.

I.6.4 ID d'interface générés aléatoirement

❏ Selon le système d'exploitation, un périphérique peut utiliser un ID d'interface généré aléatoirement. Windows XP et les systèmes d'exploitation précédents utilisaient la méthode EUI-64. À partir de la version Windows Vista, Windows utilise un ID d'interface généré aléatoirement,comme la montre la figure :

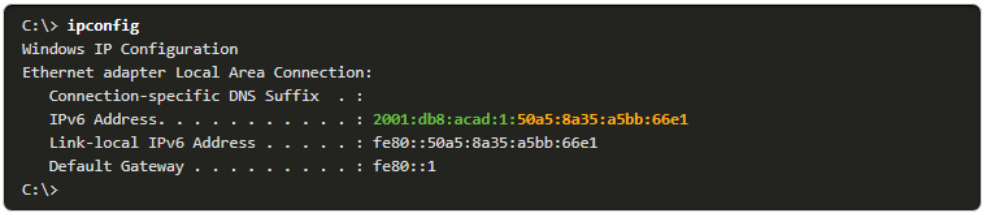


FIGURE I.20 – ID d'interface généré par le nombre à 64 bits aléatoire

Remarque :

⇨ Pour s'assurer que les adresses de monodiffusion IPv6 sont uniques, le client peut utiliser le processus de détection d'adresse dupliquée (DAD). Le principe est similaire à une requête ARP pour sa propre adresse. En l'absence de réponse, l'adresse est unique.

I.7 Les LLA de l'adressage dynamique de l'IPV6

I.7.1 LLA dynamiques

❏ La figure montre que l'adresse link-local est créée dynamiquement à partir du préfixe FE80 : :/10 et de l'ID d'interface à l'aide de la méthode EUI-64 ou d'un nombre à 64 bits généré aléatoirement.

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

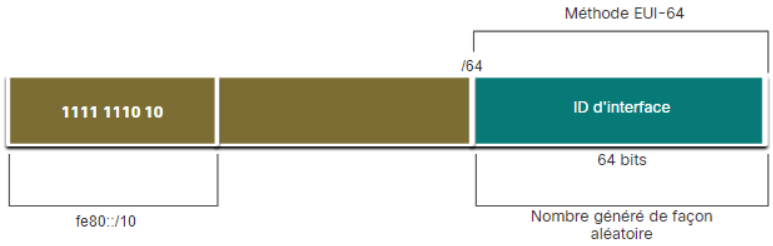


FIGURE I.21 – Création de l'adresse link-local

I.7.2 LLA dynamiques sous Windows

❑ Les systèmes d'exploitation, tels que Windows, utilisent généralement la même méthode à la fois pour un GUA créé par SLAAC et un LLA attribué dynamiquement. Consultez les zones mises en surbrillance dans les exemples suivants qui ont été montrés précédemment.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

FIGURE I.22 – ID d'interface généré par la méthode EUI-64

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

FIGURE I.23 – ID d'interface généré par le nombre à 64 bits aléatoire

1. CISCO,CCNA,Introduction to Network,Edition 7,année 2021

I.7.3 LLA dynamiques sur les routeurs Cisco

❑ Les routeurs Cisco créent automatiquement une adresse link-local IPv6 dès qu'une adresse de diffusion globale est attribuée à l'interface. Par défaut, les routeurs Cisco IOS utilisent la méthode EUI-64 pour générer l'ID d'interface de toutes les adresses link-local sur des interfaces IPv6. Pour les interfaces série, le routeur utilise l'adresse MAC d'une interface Ethernet. Souvenez-vous qu'une adresse link-local doit être unique seulement sur sa liaison ou son réseau. Toutefois, un inconvénient de l'utilisation de l'adresse locale-lien attribuée dynamiquement est son long ID d'interface : il est en effet difficile d'identifier et de mémoriser les adresses attribuées. L'exemple indique l'adresse MAC sur l'interface Gigabit Ethernet 0/0 de R1. Cette adresse est utilisée pour créer dynamiquement le LLA sur la même interface, ainsi que pour l'interface Série 0/1/0.

Pour simplifier l'identification et la mémorisation de ces adresses sur les routeurs, il est courant de configurer les adresses link-local IPv6 de manière statique sur les routeurs.

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0   [up/up]
    FE80::7279:B3FF:FE92:3640
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1   [up/up]
    FE80::7279:B3FF:FE92:3641
    2001:DB8:ACAD:2::1
Serial0/1/0            [up/up]
    FE80::7279:B3FF:FE92:3640
    2001:DB8:ACAD:3::1
Serial0/1/1            [down/down]
    unassigned
R1#
```

FIGURE I.24 – IPv6 LLA utilisant EUI-64 sur le routeur Routeur Cisco.

I.8 Adresses de multidiffusion IPv6

I.8.1 Adresses de multidiffusion IPv6 attribuées

Les adresses de multidiffusion IPv6 sont semblables aux adresses de multidiffusion IPv4. Les adresses de multidiffusion IPv6 ont le préfixe FF00 : :/8.

Remarque :

⇨ les adresses de multidiffusion ne peuvent être que des adresses de destination et non des adresses source.

Il existe deux types d'adresses de multidiffusion IPv6 :

❶ Les adresses de multidiffusion attribuées

❷ Les adresses de multidiffusion de nœud sollicité

I.8.2 Les adresses de multidiffusion attribuées :

❑ Des adresses de multidiffusion IPv6 connues sont attribuées. Les adresses de multidiffusion attribuées sont des adresses de multidiffusion réservées à des groupes ou périphériques prédéfinis. Une adresse de

2. Cédric Llorens,Laurent Levier,Denis Valois,Benjamin Morin, Tabeaux de bord de la sécurité ré- seau,EDITIONS EYROLLES 61,bd Saint-GERMAIN 75240 Paris cedex 05 www.editions-eyrolles.com.

multidiffusion attribuée est une adresse unique utilisée pour joindre un groupe de périphériques exécutant un service ou un protocole commun. Les adresses de multidiffusion attribuées sont utilisées avec des protocoles spécifiques, tels que DHCPv6.Deux groupes de multidiffusion IPv6 attribuée courants :

- ff02 : :1 groupe de multidiffusion à tous les nœuds :il s'agit d'un groupe de multidiffusion que tous les périphériques IPv6 peuvent rejoindre. Un paquet envoyé à ce groupe est reçu et traité par toutes les interfaces IPv6 situées sur la liaison ou le réseau. Cette opération a le même effet qu'une adresse de diffusion IPv4. La figure illustre un exemple de communication via l'adresse de multidiffusion à tous les nœuds. Un routeur IPv6 envoie des messages d'annonce de routeur ICMPv6 au groupe de multidiffusion à tous les nœuds.

- ff02 : :2 groupe de multidiffusion à tous les routeur :Il s'agit d'un groupe de multidiffusion que tous les routeurs IPv6 rejoignent. Un routeur devient membre de ce groupe lorsqu'il est activé en tant que routeur IPv6 avec l'adresse ipv6 unicastrouting . Un paquet envoyé à ce groupe est reçu et traité par tous les routeurs IPv6 situés sur la liaison ou le réseau.

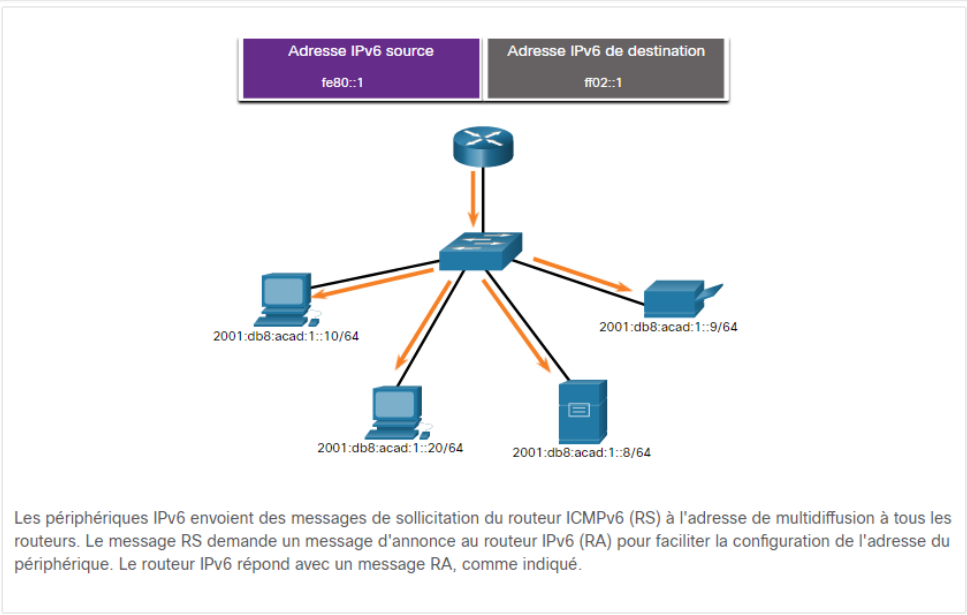


FIGURE I.25 – Groupe de multidiffusion vers tous les nœuds : Message RA

I.8.3 Adresses de multidiffusion IPv6 de nœud sollicité

- Une adresse de multidiffusion de nœud sollicité est comparable à une adresse de multidiffusion à tous les nœuds. Elle offre l'avantage d'être mappée à une adresse de multidiffusion Ethernet spéciale. Cela permet à la carte réseau Ethernet de filtrer la trame en examinant l'adresse MAC de destination sans l'envoyer au processus IPv6 pour voir si le périphérique est la cible prévue du paquet IPV6.

2. Cédric Llorens,Laurent Levier,Denis Valois,Benjamin Morin, Tabeaux de bord de la sécurité ré- seau,EDITIONS EYROLLES 61,bd Saint-GERMAIN 75240 Paris cedex 05 www.editions-eyrolles.com.

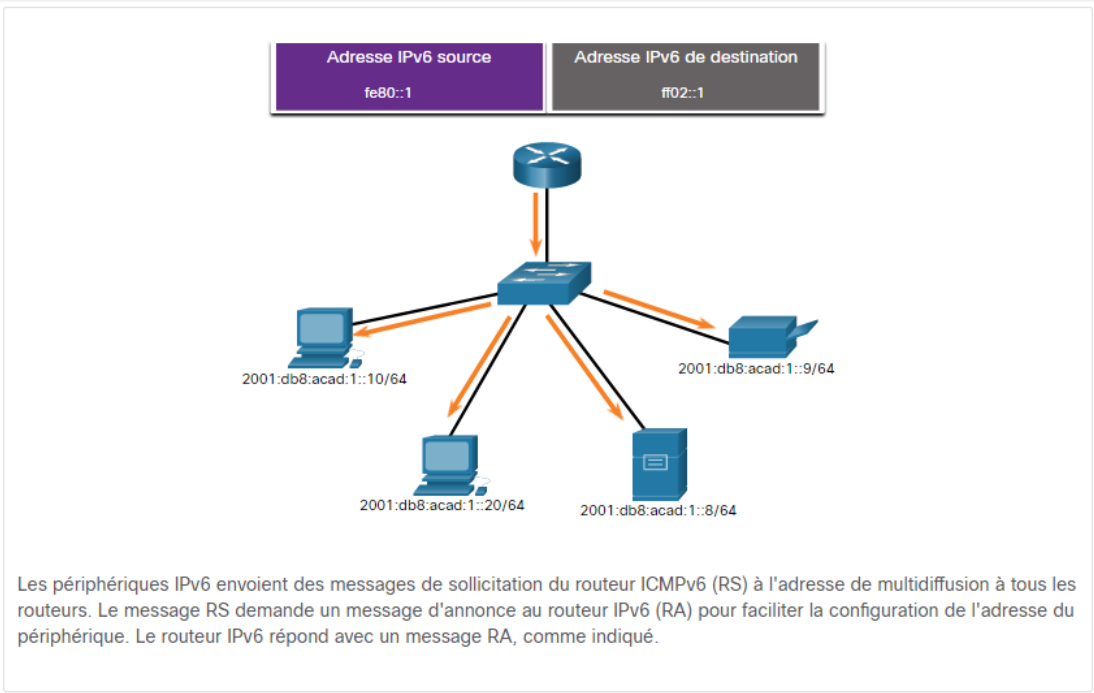


FIGURE I.26 – Adresses de multidiffusion IPv6 de nœud sollicité

I.9 Segmenter un réseau IPv6 en sous-réseaux

I.9.1 Segmenter le réseau en sous-réseaux à l'aide d'ID de sous-réseau

❑ Avec IPv4, nous devons emprunter des bits de la partie hôte pour créer des sous-réseaux,IPv6 a été conçu avec le sous-réseau à l'esprit.Comme le montre la figure, le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface.

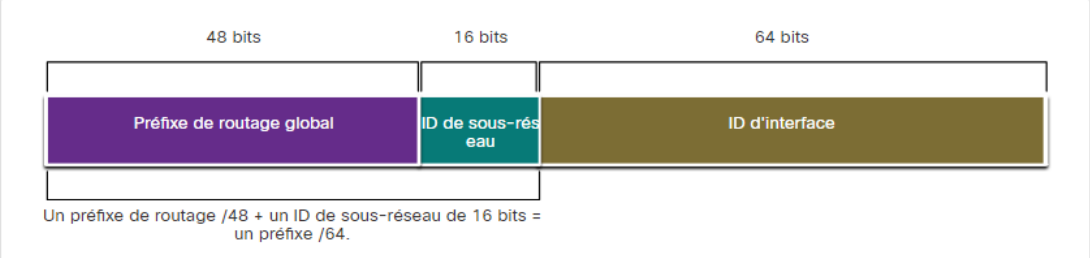


FIGURE I.27 – GUA avec un ID de sous-réseau 16 bits

exemple : si le préfixe de routage global est /48, et en utilisant un 64 bits standard pour l'ID d'interface, cela créera un ID de sous-réseau 16 bits :

❶ L'ID de sous-réseau 16 bits : Crée jusqu'à 65536 sous-réseaux.

❷ L'ID de l'interface 64 bit : prendre en charge jusqu'à 18 quintillions d'adresses IPv6 d'hôte par sous-réseau (i.e., 18,000,000,000,000,000,000).

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

Remarque :

⇨ La segmentation en sous-réseaux dans l'ID d'interface à 64 bits (ou partie hôte) est également possible, mais rarement nécessaire.

La mise en œuvre des sous-réseaux IPv6 est également plus simple que celle des sous-réseaux IPV4, puisqu'aucune conversion en binaire n'est requise.

I.9.2 Exemple de sous-réseau IPv6

❑ Par exemple, supposons que le préfixe de routage global 2001 :0DB8 :ACAD : :/48 avec un ID de sous-réseau de 16 bits a été attribué à une entreprise. Elle peut alors créer des sous-réseaux /64, comme le montre la figure. Notez que le préfixe global de routage est identique pour tous les sous-réseaux. Seul l' hextet (segment de 16 bits) représentant l'ID de sous-réseau est incrémenté en hexadécimal pour chaque sous-réseau.

FIGURE I.28 – Segmentation du réseau en sous-réseaux à l'aide de l'ID de sous-réseau

I.9.3 Attribution de sous-réseaux IPv6

❑ Avec plus de 65000 sous-réseaux disponibles, la mission de l'administrateur réseau revient à concevoir un schéma logique pour répondre aux besoins du réseau.

Comme le montre la figure, cet exemple de topologie exige cinq sous-réseaux pour chaque réseau local ainsi que pour la liaison série entre R1 et R2. Contrairement à l'exemple pour IPv4, avec IPv6, le sous-réseau de liaison série aura la même longueur de préfixe que les LAN. Bien que cela entraîne un «gaspillage» d'adresses, ce n'est pas un problème avec l'approche IPv6.

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

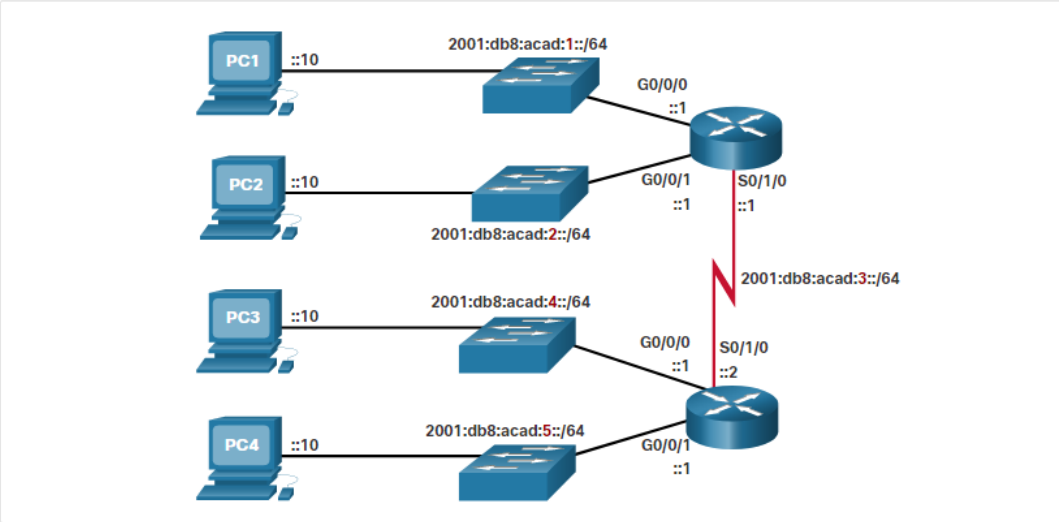


FIGURE I.29 – Exemple de topologie

➢ Comme indiqué à la figure, nous allons attribuer cinq sous-réseaux IPv6 avec le champ d'ID de sous-réseau 0001 à 0005 dans cet exemple. Chaque sous-réseau /64 propose plus d'adresses qu'il ne sera jamais nécessaire :

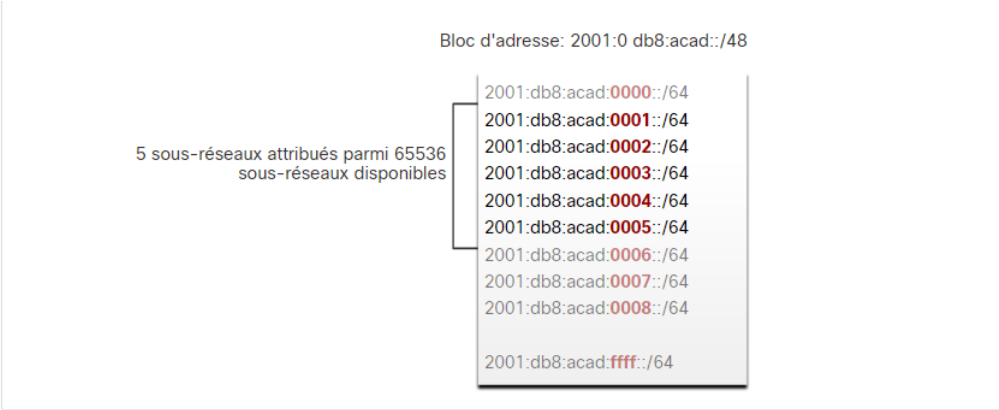


FIGURE I.30 – Exemple

I.9.4 Routeur configuré avec des sous-réseaux IPv6

❑ Comme pour la configuration IPv4, l'exemple indique que chacune des interfaces du routeur a été configurée pour utiliser un sous-réseau IPv6 différent.

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# Interface série 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

FIGURE I.31 – Configuration de l'adresse IPv6 sur le routeur R1

I.10 Conclusion :

- Le moment est venu d'entamer la transition vers IPv6 parceque L'IPv4 est limité 4,3 milliards d'adresses,les adresses privées associées à NAT ont contribué à ralentir l'épuisement de l'espace d'adressage IPv4.

- Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales. le format privilégié pour noter une adresse IPv6 est x :x :x :x :x :x :x :x, où chaque "x" est constitué de quatre valeurs hexadécimales.

- Il existe trois types d'adresses IPv6 : monodiffusion, multidiffusion et anycast (monodiffusion aléatoire).

- Un périphérique obtient une (GUA,LLA) dynamiquement via des messages ICMPv6 RA (Router advertisment) et RS(Router solicitation),ou statiquement.

- IPv6 a été conçu en pensant au sous-réseau. Le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface. L'avantage d'une adresse 128 bits est qu'elle peut prendre en charge plus de sous-réseaux et d'hôtes par sous-réseau,**ID de sous-réseau 16 bits :** Crée jusqu'à 65536 sous-réseaux,**ID de l'interface 64-bit :** prend en charge jusqu'à 18 quintillions d'adresses IPv6 d'hôte par sous-réseau (i.e., 18,000,000,000,000,000,000).

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

Chapitre II

La sécurité IPv6

II.1 Introduction

L'IPv4 présente certaines limites qui n'avaient pas été prévues lors de sa création. Comme IPv6 surmonte bon nombre de ces limites, il est le seul remplacement viable à long terme d'IPv4. Les vulnérabilités de sécurité d'IPv6 existent actuellement, et comme la popularité du protocole IPv6 augmente, le nombre de menaces augmente également.Lorsqu'un responsable de la sécurité veut sécuriser une organisation, il doit être conscient de toutes les menaces potentielles, Il vaut mieux être sûr que désolé..ce chapitre peut vous aider à comprendre les menaces qui existent dans les réseaux IPv6 et vous donner des moyens de vous en protéger ainsi que des conseils sur la façon d'améliorer la sécurité des réseaux IPv6.

II.2 Les attaques IPv4

II.2.1 Attaques permettant d'interférer avec une session réseau

La plupart des protocoles réseau n'ayant prévu aucun mécanisme d'authentification véritable, ils subissent des attaques qui s'appuient sur ces faiblesses d'authentification, au premier rang desquelles les attaques ARP spoofing et man-in-the-middle.

II.2.2 Présentation de ARP :

Si Notre réseau utilise le protocole de communication IPv4, le protocole de résolution d'adresse, ou ARP, est ce dont nous avons besoin pour mapper les adresses IPv4 aux adresses MAC. Chaque périphérique IP d'un réseau Ethernet possède une adresse MAC Ethernet unique. Lorsqu'un périphérique envoie une trame Ethernet, celle-ci contient deux adresses :

- **Adresse MAC de destination :** Adresse MAC Ethernet du périphérique de destination sur le même segment de réseau local . Si l'hôte de destination se trouve sur un autre réseau, l'adresse de destination dans la trame serait celle de la passerelle par défaut (c'est-à-dire le routeur).
- **Adresse MAC source :** L'adresse MAC de la carte réseau Ethernet de l'expéditeur. La figure illustre le problème lors de l'envoi d'une trame à un autre hôte sur le même segment sur un réseau IPv4.

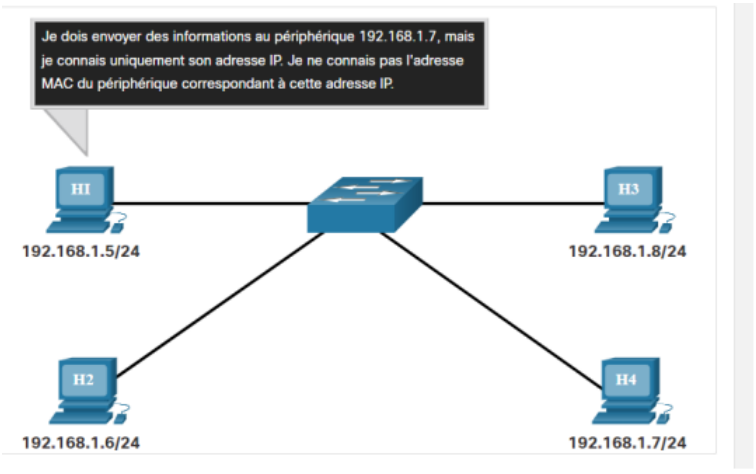


FIGURE II.1 – Envoi d'une trame à un autre hôte sur le même segment sur un réseau IPv4.

4. Silvia Hagen,IPv6 Essentials,Third Edition,Printed in the United States of America.Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

II.2.3 Fonctions du protocole ARP

- ➟ Quand un paquet est envoyé à la couche liaison de données pour être encapsulé dans une trame Ethernet, le périphérique consulte une table stockée dans sa mémoire pour connaître l'adresse MAC qui est mappée à l'adresse IPv4. Cette table est stockée temporairement dans la mémoire RAM et est appelée table ARP ou cache ARP.
- ➟ Le périphérique expéditeur recherche dans sa table ARP une adresse IPv4 de destination et une adresse MAC correspondante. Si l'adresse IPv4 de destination du paquet appartient au même réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de destination dans sa table ARP.
- ➟ Si l'adresse IPv4 de destination du paquet appartient à un autre réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de la passerelle par défaut dans sa table ARP.Dans les deux cas, il recherche une adresse IPv4 et l'adresse MAC correspondante du périphérique.
- ➟ La table ARP stocke temporairement (dans la mémoire cache) le mappage des périphériques du réseau local.Si le périphérique localise l'adresse IPv4, l'adresse MAC correspondante est utilisée comme adresse MAC de destination dans la trame. Si l'entrée n'existe pas,le périphérique envoie une requête ARP.

II.2.4 Problèmes ARP - Diffusion de l'ARP et usurpation d'identité de l'ARP :

- ❑ Comme les trames de diffusion, les requêtes ARP sont reçues et traitées par chaque périphérique du réseau local. Sur un réseau d'entreprise type, ces diffusions auraient probablement une incidence minime sur les performances du réseau.Toutefois, si un grand nombre de périphériques sont mis sous tension et accèdent aux services du réseau au même moment, les performances du réseau peuvent s'en trouver réduites sur un court laps de temps, comme l'illustre la figure. Si les périphériques envoient les messages de diffusion ARP initiaux et disposent des adresses MAC nécessaires, l'impact sur le réseau sera minimisé. Le diagramme montre sept appareils sur des supports partagés (accès multiple) tous allumés en même temps.

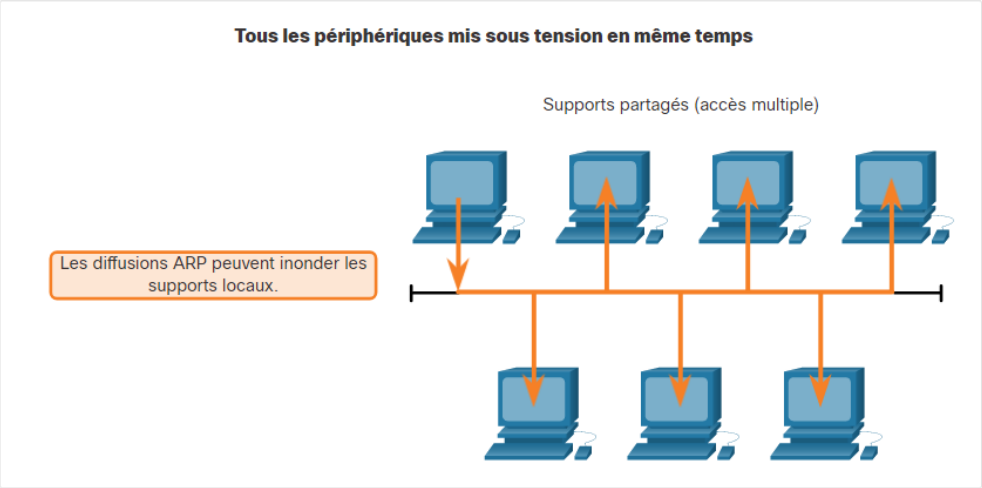


FIGURE II.2 – Problèmes de performances

II.2.5 Attaque ARP spoofing

l'utilisation du protocole ARP peut créer un risque de sécurité potentiel. Un acteur de menace peut utiliser l'usurpation ARP pour effectuer une attaque d'empoisonnement ARP. Il s'agit d'une technique utilisée par un acteur de menace pour répondre à une requête ARP concernant l'adresse IPv4 d'un autre périphérique tel que la passerelle par défaut.

4. Silvia Hagen,IPv6 Essentials,Third Edition,Printed in the United States of America.Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

- comme l'illustre la figure. L'acteur de menace envoie une réponse ARP avec sa propre adresse MAC. Le récepteur de la réponse ARP ajoute la mauvaise adresse MAC à sa table ARP et envoie les paquets à l'acteur de menace.
- la faiblesse d'authentification du protocole ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne.
- Le système du pirate reçoit donc tout le trafic à destination de la passerelle. Il lui suffit d'écouter ou de modifier passivement le trafic et de router ensuite les paquets vers leur véritable destination.

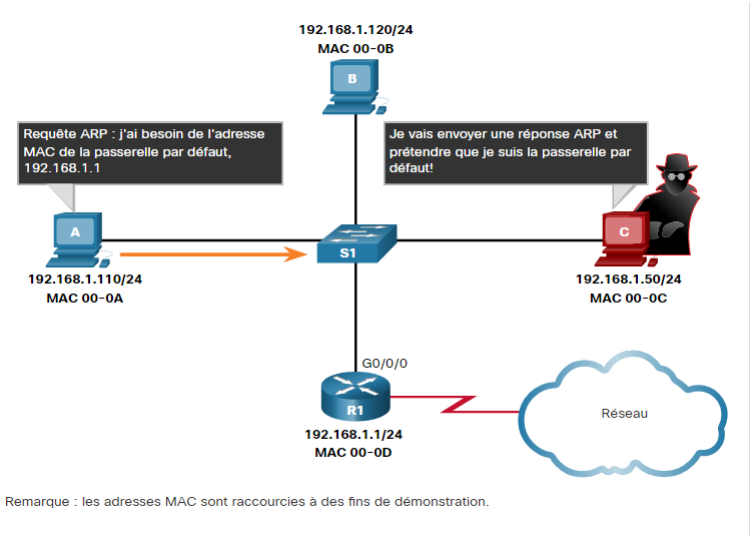


FIGURE II.3 – ARP Spoofing

II.2.6 Projection dans un monde IPv6

Le protocole ARP est complètement disparu dans la migration vers IPv6, le principe reste le même. Là où ARP faisait ses annonces en broadcast, ICMPv6 les fait en multicast.Un système IPv6 possède une table de ses voisins (Neighbor Cache) qui est mise à jour par le biais de messages ICMPv6 de type NS (Neighbor Sollicitation) et NA (Neighbor Advertisement), les attaques visant ARP sont toujours possibles en IPv6.Il est toujours possible d'envoyer de faux messages NS et NA pour corrompre les tables de voisinage d'un système IPv6 et ainsi attirer le trafic vers son adresse MAC.

II.3 Attaques permettant de dévoiler le réseau

II.3.1 Attaque par cartographie du réseau

❶ Traceroute crée un paquet avec les adresses source et destination et une valeur de durée de vie TTL initiale (nombre de passerelles traversées) égale à 1.

❷ Ce paquet s'arrête donc au premier routeur rencontré, et le routeur envoie un message d'erreur ICMP (time Exceeded).

❸ Traceroute enregistre cette information et crée un nouveau paquet avec un TTL de 2.

❹ La traversée du premier routeur met le TTL à 1. Le paquet génère une erreur sur le deuxième routeur. Comme précédemment, le deuxième routeur envoie un message d'erreur ICMP avec son adresse, laquelle est mémorisée par Traceroute.

4. Silvia Hagen,IPv6 Essentials,Third Edition,Printed in the United States of America.Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

❺ Une fois le système cible atteint, une erreur ICMP est générée par ce système cible, et Traceroute affiche la liste des passerelles traversées ainsi que le RTT (Round Trip Time), ou temps aller-retour, pour chacune d'elles.

⇨ Le pirate utilise la technique du balayage (scanning) pour construire l'image du réseau, car elle fournit des informations plus rapidement.

4. Silvia Hagen,IPv6 Essentials,Third Edition,Printed in the United States of America.Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

II.3.2 Projection dans un monde IPv6

Une adresse IPv6 est codée sur 128 bits, contre 32 bits pour une adresse IPv4.

- ➟ Une adresse IPv4 a une taille de 32 bits. Avec un outil efficace de balayage de réseau appelé ZMap et un un ordinateur avec une connexion gigabit, nous pouvons scanner l'ensemble de l'espace l'espace d'adresses IPv4 en 45 minutes.
- ➟ En IPv6, on trouvera des tailles de sous-réseaux de l'ordre de 264, représentant près de 180 milliards de milliards d'adresses et ne pouvant dès lors faire l'objet d'une cartographie complète qu'en millions d'années.

II.3.3 Attaque par balayage ICMP

La méthode de balayage consiste à utiliser le protocole ICMP et sa fonction ping. Elle consiste à ce que le client envoie vers le serveur un paquet ICMP echo-request, le serveur répondant (normalement) par un paquet ICMP echo-reply. Il existe deux méthodes pour cartographier le réseau par cette technique :

- ➟ En balayant (scanning) le réseau et en interrogeant chaque adresse IP possible, ce qui n'est pas très discret.
- ➟ En visant une seule fois l'adresse de broadcast du réseau, ce qui fait répondre toutes les machines présentes. laisser passer les réponses à de telles demandes.

II.3.4 Projection dans un monde IPv6

ICMPv6 intègre notamment les fonctionnalités suivantes :

- ❶ Découverte des voisins,découverte des routeurs,remontée des erreurs et ping
- ❷ découverte des préfixes utilisés sur le réseau (pour s'autoconfigurer) et des adresses dupliquées(DAD) .
- ❸ identification des groupes multicast en intégrant les fonctionnalités du protocole d'accès multicast.
- ⇨ ICMPv6 embarque ainsi des fonctionnalités plus riches, mais offre en contrepartie des possibilités plus avancées pour mener des attaques.

II.3.5 Attaques sur les bogues des piles IP/TCP

Les bogues(erreurs de programmation) sont parmis les faiblesses de la piles TCP/IP,ils peuvent être exploitées par des attaque afin de de gagner des privilèges. Les principales attaques qui s'appuient sur les erreurs de programmation associées aux piles TCP/IP sont le *ping de la mort*,*le baiser de la mort*, *le win nuke*,*l'attaque land* et *l'attaque teardrop.*

- ➟ **Attaque PING** :Consiste à envoyer une suite de fragments d'une requête de type écho ICMP. Une fois à nouveau assemblés par la pile IP/TCP du système cible, ces fragments forment un paquet d'une taille supérieure à la taille maximale autorisée (65 507 octets) et peuvent faire déborder les variables internes, provoquant un comportement anormal du System.
- ➟ **Attaque IGMP** :Consiste à envoyer un paquet IGMP (Internet Group Management Protocol) mal construit, mettant les machines Windows en refus de service.
- ➟ **Le win nuke** :Envoie un paquet TCP mal construit avec des données OOB (Out Of Band),mettant les machines Windows en refus de service.
- ➟ **L'attaque de type land** :Demande une ouverture de session TCP avec l'adresse source du paquet égale à l'adresse destination et le port source égal au port destinataire. Cette attaque utilise principalement le port 139 TCP (NetBIOS Session) afin de viser le système d'exploitation Windows.

6. Bob Vachon,CCNA Security Portable Command Guide,210-260,Published by :Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

- **L'attaque de type teardrop** : envoie un paquet fragmenté de telle façon que les en-têtes du second paquet écrasent ceux du premier

II.3.6 Projection dans un monde IPv6

La programmation d'une pile réseau IPv6 n'est pas simple et doit suivre les recommandations internationales en termes de comportement. Il est donc à parier que l'ère d'IPv6 (encore trop immature) mettra en avant de nouvelles attaques exploitant des faiblesses de programmation et comportement de la pile.

II.3.7 Attaque par identification des routeurs

- L'écoute d'un réseau, par exemple,peut permettre d'analyser les trames échangées, de capturer les mises à jour des tables de routage et d'identifier les routeurs participant au routage du réseau.
- Lancement des requêtes spécifiques afin de forcer ces mêmes routeurs à répondre. Par exemple, des requêtes ICMP,de routage (OSPF, BGP,etc.).
- Envoie des requêtes IRDP (ICMP Router Discovery Protocol) vers l'adresse de broadcast afin de connaître la route par défaut du réseau.

II.3.8 Attaque par fragmentation des paquets IP

Deux techniques permettent de jouer sur la fragmentation des paquets :

❶ Tiny Fragments

❷ Fragment Overlapping.

II.3.9 Attaque par Tiny Fragments

L'attaque par Tiny Fragments consiste à fragmenter sur deux paquets IP une demande de connexion TCP tout en traversant et en déjouant (par le mécanisme de fragmentation) *un filtrage IP.*

- Le premier paquet IP contient des données telles que les huit premiers octets de l'en-tête TCP :les ports source et destination et le numéro de séquence.
- Le second paquet contient la demande de connexion TCP effective (flag SYN à 1 et flag ACK à 0).
- Les premiers filtres IP appliquaient la même règle de filtrage à tous les fragments d'un paquet. Le premier fragment n'indiquant aucune demande de connexion explicite, le filtrage le laissait passer.
- Lors de la défragmentation au niveau IP de la machine cible, le paquet de demande de connexion était reconstitué et passé à la couche TCP. La connexion s'établissait malgré le filtre IP.

II.3.10 Attaque par Fragment Overlapping

L'attaque par Fragment Overlapping consiste à fragmenter deux paquets IP au moyen de l'option *Overlapping* pour faire une demande de connexion TCP ou une demande sur une machine cible tout en traversant un filtrage IP.

- Le premier paquet IP contient les données de l'en-tête TCP avec les indicateurs à 0. Le second paquet contient les données de l'en-tête TCP avec la demande de connexion TCP (flag SYN à 1 et flag ACK à 0).
- la demande de connexion est fragmentée en deux paquets IP contenant les fragments 0 et 1, chacun d'eux passant le système de filtrage
- Le système cible reconstitue un mauvais paquet TCP dû au chevauchement (overlapping) des fragments 0 et 1.

6. Bob Vachon,CCNA Security Portable Command Guide,210-260,Published by :Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

II.3.11 Projection dans un monde IPv6

En IPv6, seule la machine émettrice peut fragmenter les paquets,les équipements de sécurité de protection du périmètre doivent être en mesure de contrôler la fragmentation des paquets.

II.3.12 La VoIP :

dans le context de la convergence des réseaux de communications vers L'IP,les entreprises utilisent la technologie VOIP pour économiser de l'argent sur les couts de communications et assurer la mobilité,la présence des fonctions liées et la messagerie unifiée. deux problèmes fondamentaux font obstacle à l'évolutivité de la VoIP :

❶ Le premier probème est le manque facto intrinsèque QOS dans de nombreux réseaux IP,à la fois au niveau du support et de l'entreprise.

❷ Il est difficile de transporter des paquets VoIP à travers les Pare Feu(firewalls) à cause de traduction d'adresses réseaux NAT(Network Address Translation),donc il y'aura sûrement des problèmes de sécurité.

⇨ La prochaine génération de résaux VoIP basés sur IPV6 est en phase de développement pour assurer l'évolutivité et la fiabilité de qualité commerciale.

II.3.13 Les apport d'IPV6 de la qualité de service :

Certain champs de l'en-tete IPv4 ont été enlevés ou rendu optionels.L'en-tete est passée de 15 à 8 champs.Ceci réduit donc le couts de gestion des paquets dans les situations classiques et limite le besoin en bande passante pour cet en-tete.

II.3.14 La qualité de service (QOS) :

❑ Pour supporter la qualité de service,il faut pouvoir différencier et garantir certains flux.Les champs supportant la QOS sont "FLOW label" et "Traffic Class" dans l'en-tete IPv6.Ces champs surviront comme indicateur à l'hote pour identifier les paquets nécessitant un traitement spécial des routeurs compatible IPv6.Les routeurs pourront ainsi procéder à un service en temps réel ou de la qualité soutenue.

Définition expérimentale du champ "Traffic Class"(1 octet) :

➢ bit D(1bit) : privilégie le délais par rapport au débit.

➢ Prio (3 bits) :définition de la priorité pour la remise des paquets.

➢ Réservé(4 bits).

II.4 Les vulnérabilités de IPV6 :

❑ les implémentations d'IPv6 sont relativement nouvelles sur le marché, et le logiciel qui a créé ces systèmes n'a pas été testé sur le terrain de manière aussi approfondie que son homologues IPv4,il y aura probablement une période de temps où des défauts seront trouvés, et les fournisseurs devront réagir rapidement pour corriger leurs bugs.Microsoft, Juniper, Linux, Sun, BSD,Cisco ont tous publié des vulnérabilités de leurs logiciels.

❑ IPv6 peut être utilisé comme une (porte dérobée) car de nombreux systèmes de sécurité sécurisent uniquement IPv4 et ignorent les paquets IPv6.Pour ces raisons, il est important de sécuriser IPv6 avant qu'il ne soit largement déployé.

Les attaques contre les réseaux relèvent généralement de l'une des catégories suivantes :

6. Bob Vachon,CCNA Security Portable Command Guide,210-260,Published by :Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

- Internet (DMZ, fragmentation, pages Web, pop-ups).
- Usurpation IP, fusée de protocole, manipulation d'en-tête, détournement de session, homme du milieu, reniflage.
- Débordements de mémoire tampon, injection SQL, scripts intersites.
- E-mail (pièces jointes, phishing, canulars).
- Vers, virus, déni de service distribué (DDoS).chevaux de Troie, logiciels espions, logiciels malveillants, enregistreurs de frappe. VPN, entreprise à entreprise (B2B) Chat, poste à poste (P2P)

Note :

- Les attaques contre les éléments du réseau proviennent généralement d'Internet.
- les attaques sur les périphériques intranet proviennent d'initiés malveillants.
- La plupart des routeurs internes ont des mécanismes de protection simples comme des mots de passe simples et (SNMP),donc sont constamment sensibles à de nombreuses formes d'attaques différentes.
- Les routeurs ne sont généralement pas capables d'exécuter un logiciel serveur traditionnel ou d'autres applications qui peuvent avoir des vulnérabilités. Cependant, ils peuvent être la cible d'un débordement de tampon, où l'attaquant tente d'envoyer des informations au routeur pour dépasser une mémoire tampon interne.
- Les effets secondaires peuvent être tout ce qui va d'un comportement erratique à une panne de logiciel ou de gagner l'accès à distance.
- En 2007, Computer Security Institute (CSI —http ://www.gocsi.com) 12e annuel Selon l'enquête sur la criminalité informatique et la sécurité, 59% des répondants à l'enquête a été victime d'abus d'accès au réseau.

II.4.1 Les pirates

- Peu d'attaques IPv6 existent ou sont connues du public et il existe peu de bonnes pratiques en matière de sécurité IPv6. Cependant, quelques pirates sophistiqués utilisent déjà IPv6 pour Chats Relais Internet (IRC) canaux et portes dérobé pour leurs outils.

II.4.2 Techniques d'atténuation de la sécurité IPv6

Les architectures de sécurité IPv6 ne sont pas substantiellement différentes de celles d'IPv4. Les organisations peuvent toujours avoir les mêmes topologies de réseau lors de la transition vers IPv6 . Avec IPv6, la conception du périmètre a la même pertinence que pour IPv4.Le problème est que la plupart des organisations consacrent leurs efforts à la sécurisation du périmètre, et ils négligent la sécurité interne de leur environnement.

Les zones suivantes d'un environnement informatique doivent être protégées :

- Protections périmétriques contre L'Internet et les entités externes.
- Sécurisée la Connectivité à des sites distants avec les technologies de réseau privé virtuel (VPN).

  Mesures de protection de l'infrastructure pour assurer une base de réseau sécurisée.
- Sécurité du serveur pour protéger les actifs et les données informatiques critiques.
- Mesures de sécurité du client pour atténuer la menace interne.

Les principes de sécurité informatique standard s'appliquent toujours à la sécurité d'un réseau IPv6 :

- Utilisations de plusieurs stratégies qui se soutienne mutuellement.

6. Bob Vachon,CCNA Security Portable Command Guide,210-260,Published by :Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

➟ Toutes les parties de protections doivent être fortifier comme un chateau càd avoir une architecture de sécurité qui a un périmètre et des contrôles internes pour atténuer non seulement les menaces Internet, mais également les menaces internes se genre de défense est comme avoir "une ceinture et une bretelles" pour bien serrer son pantalon".

II.4.3 Les vulnérabilités de la sécurité du protocole IPv6

❑ Le remplacement d'IPv4 par IPv6 modifie uniquement la couche réseau. Cependant, il peut y avoir de nouvelles menaces introduite par IPv6 en raison de la façon dont il interagit avec les couches de protocole au-dessus et au-dessous de couche réseau.

II.5 Pésentation de L'en-tête de protocole IPv6 :

II.5.1 Définition

l'en-tête de protocole IPv6 est défini par l'IETF dans la RFC 2460. L'en-tête est basé sur les limites 32 bits pour faciliter l'utilisation de sa structure par les processeurs 32 bits.L'en-tête IPv6 comporte de nombreuses modifications par rapport à l'en-tête IPv4 et, en raison de ces modifications, IPv6 représente un protocole complètement différent d'IPv4.

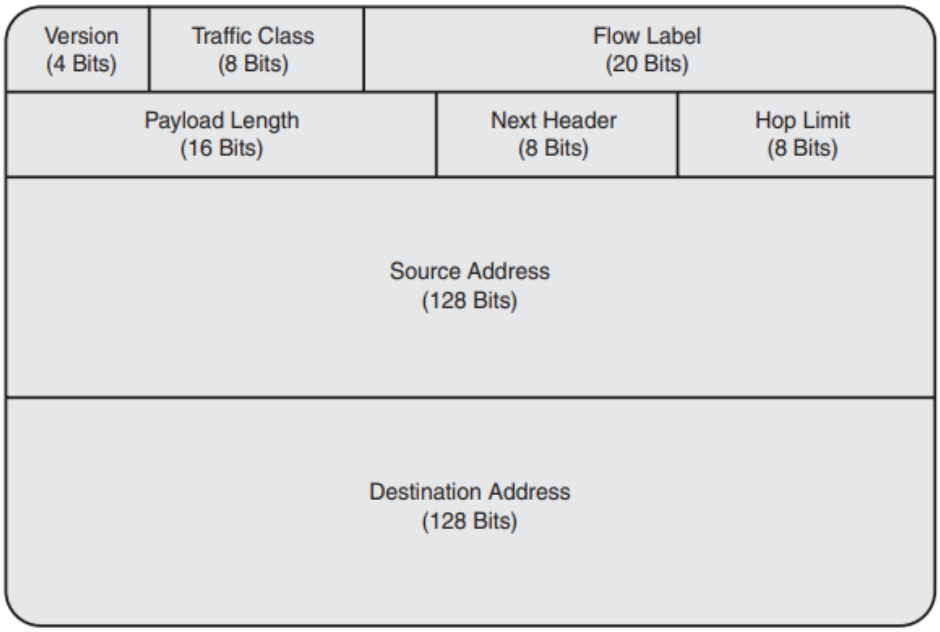


FIGURE II.4 – l'en-tête IPv6.

II.5.2 Les champs de L'en-tête IPv6

– **Version :**Le champ « Version » est codé sur 4 bits. Il représente le numéro de version du Protocole Internet. Sa valeur est donc égale à 6 (0110 base 2).

– **Classe (Traffic Class) :** Le champ « Classe » est codé sur 8 bits. Il définit la priorité du datagramme afin que des noeuds origines et des routeurs transmetteurs puissent identifier et distinguer la classe ou la priorité du paquets IPv6 en question.

7. Prabhu Thiruvasagam and K. Jijo George,Journal of ICT standardization,NEC India Private Limited, India.Received 02 December 2018 ; Accepted 06 January 2019.

Label (Flow Label) : Le champ « Label » est codé sur 20 bits. Il peut être utilisé par une source pour nommer des séquences de paquets pour lesquels un traitement spécial de la part des routeurs IPv6 est demandé. Ce traitement spécial pourrait être une qualité de service différente du service par défaut ou un service "temps réel".
Longueur (Payload Length) : Le champ "Longueur" est codé sur 16 bits. Le champ " Longueur" de l'entête IPv4 indiquait la longueur des données incluant l'entête IPv4 elle même. Contrairement à cela, cette fois le champ "Longueur" de l'entête IPv6 indique le nombre d'octet des données qui suivent cette entête IPv6. Il faut noté que les options de l'entête IPv6 sont considérés comme de la donnée et font donc partie du calcul du champ "Longueur ".

Entête suivante (Next Header) :Le champ " Entête suivante " est codé sur 8 bits. Il identifie le type de la Data ou de l'option qui se trouve derrière l'entête IPv6. Les valeurs employées sont identiques au champ « Protocole » de l'entête IPV4. Vous trouverez tous les détails des types de protocole dans la RFC 1700 qui remplace désormais la RFC 1340.

Saut maximum (Hop Limit) : Le champ "Saut maximum" est codé sur 8 bits. Il indique le nombre de routeur maximum que le datagramme pourra traverser. Identiquement au champ « TTL » de l'entête IPV4, il est décrémenté de 1 par chaque noeud traversé par le paquet.
Adresse source (Source Address) : Le champ « Adresse source » est codé sur 128 bits. Il représente l'adresse IP de l'émetteur.
Adresse destination (Destination Address) : Le champ « Adresse destination » est codé sur 128 bits. Il représente l'adresse IP du destinataire.

Remarque :

⇨ Protocole IPv6 et l'en-tête lui-même ne représentent aucune vulnérabilité de sécurité. Plutôt la façon dont ces paquets sont créés et traités c'est ce qui peut conduire à des problèmes de sécurité. Les paquets IPv6 ne piratent pas les ordinateurs,les pirates piratent les ordinateurs.

⇨ Les canaux cachés sont un domaine qui peut causer des maux de tête aux praticiens de la sécurité IPv6. Certains d'entre eux,les communications ne peuvent pas être facilement détectées. Il est possible d'utiliser le protocole IPv6 lui-même comme canal secret. Les bits de ces champs peuvent être utilisés pour envoyer des données entre deux hôtes au cours de plusieurs paquets.

II.6 ICMPv6

❑ ICMPv6, est défini par la RFC 4443,c'est un protocole vital pour le fonctionnement d'IPv6. ICMPv6 possède des fonctionnalités qui sont des éléments requis qui ne peuvent pas être complètement filtrés.

❑ ICMP fournit des fonctionnalités qui activent les utilitaires, tels que ping et traceroute, pour aider à vérifier la connectivité IP de bout en bout,il fournit également des informations renvoyées aux noeuds sur les erreurs de communication.

Problématique :

⇨ les attaquants ont essayé d'utiliser ICMP pour des exploitations , et les administrateurs réseau ont dû recourir au filtrage complet du protocole pour prévenir ces attaques. Cela limite l'efficacité du protocole parce que les fonctionnalités utiles d'ICMP sont désactivées. Les pare-feu IPv4 ne doivent pas bloquer tout le trafic ICMP entrant mais devrait plutôt permettre certains paquets ICMP spécifiques.

7. Prabhu Thiruvasagam and K. Jijo George,Journal of ICT standardization,NEC India Private Limited, India.Received 02 December 2018 ; Accepted 06 January 2019.

II.6.1 Fonctions et types de messages ICMPv6 :

- ➟ Le protocole de découverte de voisin (NPD), annonces de voisin (NA) et sollicitations des voisin (NS) est équivalent au protocole ARP (Address Resolution Protocol) de L'ipv4.
- ➟ Les annonces de routeur (RA) et les sollicitations de routeur (RS) aident les noeuds à déterminer des informations sur leur réseau local, telles que le préfixe réseau, la passerelle par défaut.
- ➟ Echo Request et Echo Reply prennent en charge l'utilitaire Ping6.
- ➟ PMTUD détermine la taille de MTU appropriée pour les communications.(les routeur intermidiaires peuvent fragmenter le packets (IPv4),(les routeur intermidiaires ne peuvent pas fragmenter les packets IPv6).
- ➟ Multicast Listener Discovery (MLD) fournit une fonctionnalité de type IGMP pour les communications de jonctions et de sorties de multidiffusion IP.
- ➟ Multicast Router Discovery (MRD) découvre les routeurs de multidiffusion.
- ➟ La requête d'informations sur les noeuds (NIQ) partage des informations entre les noeuds.
- ➟ Secure Neighbor Discovery (SEND) permet de sécuriser les communications entre les voisins.
- ➟ Mobile IPv6 est utilisé pour les communications mobiles.

- ❑ Les messages ICMPv6 contiennent un type (1 octet) et un code (1 octet) qui associent les détails du message au type de message,les messages d'erreur utilisent les types 0 à 127, alors que les messages d'information utilisent types 128 à 255.
- ❑ Tous Les noeuds IPv6 doivent rejeter/ignorer tout paquet NDP dont la limite de saut est inférieure à 255 pour limiter la propagation de ce dernier.
- ❑ En outre, si le récepteur reçoit un paquet ayant une limite de saut inférieure à 255, il sait que ce paquet pourrait être conçu et il devrait le rejeter,lorsque le routeur ou le pare-feu supprime le paquet, il envoie un Message ICMPv6 de temps dépassé, renvoyé à la source de ce dernier.

Problématique :

- ➟ Si un attaquant sait que c'est le comportement par défaut d'un pare-feu, cette personne peut générer une grande quantité de paquets qui atteignent le pare-feu au moment où leur limite de saut est décrémentée à 0. Cela peut être une technique pour provoquer une attaque de consommation de ressources sur le pare-feu.

La limite de saut des messages suivants doit être définie sur 255 :

❶ RS : Type 133, RA : Type 134.

❷ NS : Type 135, NA : Type 136.

❸ Redirection : Type 137.

❹ Sollicitation de découverte de voisin inverse : Type 141.

❺ Annonce de découverte de voisin inverse : Type 142.

❻ Sollicitation de chemin de certificat (SEND) : Type 148.

Remarques :

1) PMTUD et d'autres messages d'erreur ICMPv6 sont l'exception à cette règle car ils ont des limites de saut utilisées pour la traversée des réseaux.
2) Vous devez également inspecter les adresses IPv6 source et de destination d'un paquet ICMPv6.

7. Prabhu Thiruvasagam and K. Jijo George,Journal of ICT standardization,NEC India Private Limited, India.Received 02 December 2018 ; Accepted 06 January 2019.

3) Souvent, les messages d'erreur ICMPv6 contiennent une partie du paquet qui a créé l'erreur.

4) Si l'adresse de destination du message d'erreur ne correspond pas à la source du paquet ICMPv6 , il y a quelque chose qui ne va pas avec le paquet.

II.6.2 Attaques ICMPv6 et techniques d'atténuation :

ICMPv6 est une partie importante des communications IPv6,donc il est également le foyer d'attaques. Ces attaques peuvent être une simple usurpation de messages ICMPv6 ou ils peuvent être utilisées pour attaquer directement l'infrastructure réseau.Dans les deux cas , ICMPv6 doit être soigneusement contrôlé et sécurisé. Une technique consiste à simplement bloquer tous les types de messages ICMPv6 qui n'ont pas encore été alloués par l'IANA. Les types de message ICMPv6 suivants ne doivent être affichés sur aucun réseau et doivent être supprimés :

❶ Messages d'erreur non alloués : Type 5-99 et type 102-126.

❷ Messages d'information non alloués : Type 155-199 et type 202-254.

❸ Messages expérimentaux : Type 100, 101, 200, 201.

❹ Numéros de type d'extension : Type 127, 255.

Remarque :

⇨ Si de nouveaux messages sont alloués par l'IANA, des ajustements doivent être apportés à ces filtres.

➢ Les messages suivants devrait être autorisé à partir et vers l'Internet :

➢ Type 1 : Destination Unreachable.

➢ Type 2 : Packet Too Big—PMTUD.

➢ Type 3 : Time Exceeded.

➢ Type 4 : Parameter Problem.

➢ Autoriser les messages de type 128 et 129 (echo request et echo reply)

➢ Ignoer les messages de requetes d'informations type (139,140) au niveau du périmetre et réseau.

Attaque :

➟ Les messages d'erreur peuvent contenir une partie du packets dorigine qui a causé l'erreur dans le payload(la charge util),il y'a une possibilité que tout le contenu entier du paquet d'origine se situe dans le payload,donc cette payload peut etre utilisée comme un canal caché entre deux noeud.

Soultion

✓ les pare-feu doivent inspecter le fragment de paquet dans l'erreur ICMPv6 pour voir s'il est légitime. Si le fragment de paquet d'erreur ne contient pas adresses IPv6 légitimes ou si le paquet d'erreur ICMPv6 n'est pas envoyé avec état en réponse à l'erreur s'écoulant dans la direction opposée, le paquet doit être abandonné.

Attaque :

➟ Un attaquant pourrait génerer beaucoup de paquets illégaux (comme des paquets extrêmement volumineux ou, dans le cas d'un chemin d'expiration de nombre de sauts) et les envoyer à un périphérique réseau,cela peut entraîner une utilisation élevée de CPU du périphérique pour entraîner des dégradation de performance ou même une défaillance.(attaque par déni de service (DoS)).

7. Prabhu Thiruvasagam and K. Jijo George,Journal of ICT standardization,NEC India Private Limited, India.Received 02 December 2018 ; Accepted 06 January 2019.

✓ **Solution**

➟ Le contrôle de la vitesse à laquelle un routeur génère tous les messages d'erreur ICMP IPv6. Ces messages d'erreur ICMPv6 générés par le routeur peuvent être limité à l'aide de la commande **ipv6 icmp error-interval milliseconds**.

❑ il faut autoriser précisément les messages ICMPv6 que vous souhaitez transférer et tous les autres seront refusés au lieu de supprimer les paquets qui n'ont pas été explicitement autorisés.

II.6.3 Sécurité de la multidifusion

Attaques :

➟ Si un attaquant pouvait envoyer du trafic à un groupes de multidiffusion afin que tous les systèmes qui font partie de ces groupes répondent.L'attaquant aurait des informations sur tous les routeurs dans le réseau IPv6 et tous les hôtes DHCPv6.Ensuite l'attaquant pourrait déterminer quels autres ordinateurs sont contenus dans le réseau, soit via des caches de voisins, des mises à jour de liaison ou des journaux DHCPv6.

➟ La multiduffusion peut etre utilisée pour l'amplification du volume de traffic pour les attaques DOS(attaque de Schtroump).

➟ Usurper l'@source d'un paquet distiné à une multidiffusion entrainera une amplification du trafic vers la source usurpée.

Solution :

✓ RFC 2463 indique que « un message d'erreur ICMPv6 ne doit pas être envoyé suite à la réception d'un paquet destiné à une multidiffusion IPv6».

✓ Verification de l'@source des paquets plutôt que de vérifier l'@ de destination,refuser les paquets qui utilisent l'@multidiffusion comme @source

✓ Les paquets envoyés au @multidiffusion ont généralement l'@de monodiffusion du serveur de multidiffusion comme @source du paquet.

✓ Recevoir un paquets avec une @source de multidiffusion implique paquet fabriquer donc pas de message d'erreur icmpv6 en retour.

II.6.4 Sécurité du périmètre IPv6

❑ Le périmètre est la première ligne de défense contre les menaces extérieures. Cependant, le périmètre n'est pas la seule stratégie de sécurité à utiliser pour empêcher tous type d'attques.Le modèle de périmètre n'est qu'un des nombreux composants essentiels requis dans une diversité de conception de la défense.

❑ Le modèle de périmètre commence à s'effondrer lorsqu'une organisation place toute sa confiance en elle et n'utilise pas de couche architecture de sécurité qui protège contre les menaces provenant de l'intérieur.

❑ ses organisations sont victimes d'attaques de logiciels malveillants ciblant les ordinateurs des utilisateurs finaux. Si le périmètre est le seul mécanisme de sécurité utilisé, ces menaces internes exploiteront complètement le réseau interne.

7. Prabhu Thiruvasagam and K. Jijo George,Journal of ICT standardization,NEC India Private Limited, India.Received 02 December 2018 ; Accepted 06 January 2019.

Note :

- ➢ IPv6 est ajouté au périmétre de l'IPv4 actuel.
- ➢ L'immigration d'une organisation vers un environnement à double pile ne signifie pas le remplacement de ses défenses périmétriques actuelles.
- ➢ La plupart des organisations vont ajouter simplement des capacités IPv6 à leurs points de sortie existants, et le modèle de périmétre reste pendant la migration vers IPv6.
- ➢ Des responsabilités supplémentaires IPv6 vont être ajouté aux architectures de sécurtié et aux dispositifs de protection qui existent pour IPv4.
- ➢ La politique d'autorisation de trafic des applications sur IPv6 sera similaire à la politique d'IPv4 actuelle,C'est parce que les couches de transport TCP et UDP fonctionnent de la même manière sur la couche 3.

Exemple :

- ❑ Notre université Abdrahmane Mira BEJAIA dispose actuellement d'une règle autorisant les demandes Web sortantes,L'administrateur réseaux ajoute une règle similaire pour les connexions TCP port 80 (HTTP) sortantes dans notre stratégie de sécurité IPv6. À l'exception de ICMPv6,le filtrage périmétrique ne sera pas radicalement modifié comme étant une partie de la migration vers IPv6.

II.6.5 Les Par-feu IPv6

- ❑ Les règles de filtrage de paquets séparent les ordinateurs à différents niveaux de confiance. Ces pare-feu peuvent être mis à niveau pour s'exécuter en mode double pile. Cela signifierait que les pare-feu IPv4 existants doivent avoir les protocoles IPv4 et IPv6 configurés dans le mode double pile et les stratégies de sécurité des deux protocoles doivent offrir une protection égale.

Problématique :

- ➠ Les pare-feu IPv4 actuels risquent de ne pas pouvoir gérer l'ajout de la sécurité IPv6 !.

Solution :

- ✓ Les entreprises doivent envisager d'ajouter de nouveaux pare-feu uniquement IPv6 au périmètre pour appliquer une stratégie spécifique à IPv6.
- ✓ Une organisation doit séparer ses stratégies de sécurité facilement, et le pare-feu IPv6 ne communiquera qu'avec IPv6.
- ✓ Les stratégies des pare-feu IPv6 doivent correspondrent à la stratégie des pare-feu IPv4.
- ✓ Tous les pare-feu doivent être construits avec la politique *"ce qui n'est pas expressément autorisé est refusé"*. Les pare-feu IPv6 seront les mêmes à cet égard.

Note :

- ⇨ Un pare-feu IPv6 séparé pourrait également réduire l'impact potentiel de IPv6 sur un pare-feu IPv4 existant : Aucune mise à niveau logicielle n'est requise et la maintenance est plus facile car il y a actuellement moins de trafic IPv6.

2. Cédric Llorens,Laurent Levier,Denis Valois,Benjamin Morin, Tabeaux de bord de la sécurité ré- seau,EDITIONS EYROLLES 61,bd Saint-GERMAIN 75240 Paris cedex 05 www.editions-eyrolles.com.

II.6.6 Filtrage des adresses IPv6 Non-Allouée :

- ❑ Le filtrage d'entrée et de sortie des d'adresses attribuées par une organisation est considérée comme une bonne pratique, vous devez prendre en compte les plages d'adresses valide du protocole IPv6 et filtrer les paquets qui utilisent les adresses non allouées.
- ❑ Les pare-feu doivent bloquer les paquets provenant de, ou destinés à, un espace d'adressage IPv6 non alloué.

  La plupart des implémentations de filtrage périmétrique IPv4 refusent les adresses non allouées et réservées et autorisent toutes les autres adresses IPv4. Ceci ne suit pas la règle *ce qui n'est pas explicitement autorisé doit être refusé* .
- ❑ La sécurité peut être améliorée parce que la politique de sécurité n'autoriserait que les paquets provenant des préfixes de l'espace d'adresse IPv6 alloué et toutes les autres adresses IPv6 seraient bloquées.
- ❑ Les paquets légitimes destinés à ces adresses doivent être autorisés.Les paquets entrants doivent également avoir ces adresses de monodiffusion IPv6 légitimes comme adresses sources,voici les grands blocs d'adresses qui ont été attribués par L'IANA :

- ✦ 2001 : :/16—IPv6 unicast addresses
- ✦ 2002 : :/16—6to4 tunneling
- ✦ 2003 : :/18—RIPE NCC
- ✦ 2400 : :/12—APNIC
- ✦ 2600 : :/12—ARIN (US DoD)
- ✦ 2610 : :/23—ARIN
- ✦ 2620 : :/23—ARIN
- ✦ 2800 : :/12—LACNIC
- ✦ 2A00 : :/12—RIPE NCC
- ✦ 2C00 : :/12—AfriNIC

Remarque :

- ⇨ Les messages ICMPv6 Duplicate Address Detection (DAD) peuvent utiliser l'adresse non spécifiée (: :/128) comme adresse source.

  Même s'il s'agit d'une utilisation légitime de l'adresse non spécifiée,ces paquets ne doivent pas traverser un périmètre de réseau ou une frontière Internet. Les messages DAD qui utilisent l'adresse non spécifiée ne doivent être vus que sur les liens du réseau local avec une limite de saut fixée à 255. Les autres types de paquets IPv6 ne doivent pas utiliser l'adresse non spécifiée comme adresse source. Le bloc d'adresses 2001 :db8 : :/32 a été défini dans la RFC 3849, pour une utilisation dans la documentation. Cet espace d'adressage peut être utilisé pour exemples pédagogiques mais ne doit pas être utilisé dans un environnement de production.

Problématique :

- ➠ Les addresses link-local(LLA) sont légitimes que sur un réseau local elles ne doivent pas être utilisées comme source ou destination du trafic en provenance ou à destination d'Interne. Cependant, leur filtrage au niveau du périmètre peut poser des problèmes pour les périphériques directement connectés. Par exemple, selon la façon dont le protocole Border Gateway Protocol (BGP) est configuré, le blocage des adresses locales de liaison peut empêcher le BGP externe (EBGP) de fonctionner correctement.

2. Cédric Llorens,Laurent Levier,Denis Valois,Benjamin Morin, Tabeaux de bord de la sécurité ré- seau,EDITIONS EYROLLES 61,bd Saint-GERMAIN 75240 Paris cedex 05 www.editions-eyrolles.com.

II.6.7 Les pare-feu et l'entete IPV6 :

Même si l'en-tête IPv6 est plus grande que l'en-tête IPv4,Les routeurs et les pare-feu IPv6 n'ont qu'à analyser l'en-tête et à faire attention aux adresses et à la limite de saut.

Note :

➢ Les routeurs et les pare-feux IPv4 doivent analyser une variété de champs d'en-tête, dont les suivants : Time-to-Live (TTL), les ID/offset des fragments et la longueur.

➢ Les routeurs IPv4 doivent ensuite calculer une nouvelle somme de contrôle de l'en-tête avant de transmettre le paquet.

❑ La conception de l'IPv6 minimise le travail requis par les dispositifs intermédiaires et confie aux nœuds finaux la responsabilité d'analyser l'ensemble de la structure de l'en-tête.L'objectif est d'essayer d'effectuer plus d'opérations sur les en-têtes dans le matériel et moins dans le logiciel pour améliorer les performances.

Il est évident qu'un pare-feu devrait abandonner les paquets avec des en-têtes d'option inconnus,les paquets IPv6 peuvent être trafiqués pour tenter de provoquer une attaque DoS ou consommer les ressources du pare-feu. Par conséquent, les pare-feu doivent également éliminer les paquets qui ne respectent pas les règles d'en-tête standardisées ou qui violent les règles de base de l'intégrité des paquets (élimination des paquets comportant cinq en-têtes d'option de destination).

II.6.8 Pare-feu de couche 2 :

❑ Il existe des cas où le pare-feu de couche 2 (transparent) est avantageux.Un pare-feu de couche 2 IPv4 doit transmettre les diffusions et les multidiffusions spécifiques au sous-réseau (Address Resolution Protocol [ARP] par exemple,le pare-feu de couche 2 IPv6 doit effectuer le même type de transfert.

Avec IPv6, il y a beaucoup plus de types de paquets à autoriser sur la couche de liaison de données. Voici une liste des messages IPv6 qu'un pare-feu IPv6 transparent de couche 2 devrait transférer sur toutes ses interfaces :

❶ Autoriser les messages ICMPv6 de découverte des voisins.

❷ autoriser les paquets de multidiffusion IPv6 (adresses MAC 3333.0000.0000 à 3333.FFFF.FFFF).

❸ Permettre les messages Neighbor Advertisement (NA), Neighbor Solicitation (NS), et les paquets DAD (Duplicate Address Detection).

❹ Permettre les messages Router Advertisement (RA) et Router Solicitation (RS) pour SLAAC.

II.6.9 Les pare-feux génèrent des ICMP inaccessibles :

❑ Lorsque des paquets IPv6 invalides sont abandonnés, un pare-feu ou un routeur ne doit pas renvoyer automatiquement un message d'erreur ICMPv6. Ce message d'erreur serait renvoyé à l'attaquant et pourrait lui donner des informations qui pourraient être exploitées.

❑ Le message d'erreur pourrait également indiquer à l'attaquant que le pare-feu est sensible à une attaque par consommation de ressources, car le traitement des paquets ICMP inaccessibles sont gérés par la CPU du pare-feu,l'attaquant pourrait envoyer une grande quantité de paquets invalides au pare-feu, provoquant ainsi un éventuel déni de service (DoS). Dans de nombreux cas, il est préférable de laisser tomber le paquet en silence.

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

II.6.10 Journalisation et performance :

❶ Il faut toujours enregistrer les paquets qui sont bloqués par la politique de sécurité du périmètre Internet.

❷ Lorsque ces journaux sont examinés, vous pouvez voir les paquets provenant des adresses illégitimes et vous pouvez voir les adresses sources des faux paquets qui arrivent sur votre réseau.

❸ la journalisation de ces informations et la révision périodiquement est une bonne pratique.

❹ La quantité de journalisation effectuée par un pare-feu est directement liée à ses performances. Plus il y a de journalisation sur le trafic passé ou bloqué, plus le pare-feu sera lent.

Afin d'implémenter IPv6 il faut :

❶ Comprendre les différences entre IPv4 et IPv6.

❷ Comprendre les vulnérabilités dans IPv6,les lister.

❸ Enfin la mise en oeuvre des techniques d'atténuation de sécurité afin de fournir une couverture adéquate pour notre environnement.

II.6.11 Création d'une politique de sécurité IPv6

❑ La première étape de la création d'un plan de sécurité consiste à définir la politique de sécurité. Sans une politique de sécurité bien définie, toutes les autres activités de sécurité sont inutiles. Lors de la création d'une politique de sécurité à l'échelle de l'entreprise, vous devez vous assurer qu'elle possède les caractéristiques critiques suivantes. Si l'une d'entre elles fait défaut, la politique de sécurité est vouée à l'échec :

❶ Elle doit être mise par écrit.

❷ Elle doit être approuvé par la direction.

❸ Elle doit être accepté par tous et bénéficier d'une participation universelle.

❹ Elle doit faire l'objet d'une bonne publicité.

❺ Elle doit être contrôlé et appliqué.

❻ Elle doit être régulièrement révisé et mis à jour.

II.6.12 Configuration d'un pare-feu :

Les étapes de configuration du pare-feu IOS sont :

❶ Définir la politique d'inspection et définir les différents protocoles qui doivent être inspectés en utilisant la commande **ipv6 inspect**.

❷ Appliquer le nom de la politique d'inspection à l'interface.

La syntaxe de ces commandes est la suivante :

```
ipv6 inspect name inspection-name protocol [alert {on ¦ off}] [audit-trail {on ¦
  off}] [timeout seconds]
interface FastEthernet0/0
 ipv6 inspect inspect-name {in ¦ out}
```

FIGURE II.5 – Commande de configuration

➡ Le pare-feu IOS peut effectuer une inspection des protocoles sur les paquets FTP, TCP, UDP et même ICMP.

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

- Le pare-feu IOS peut également vérifier les en-têtes de routage avec la commande **ipv6 inspect routing-header** ,et la commande **no ipv6 inspect routing-header** abandonne les paquets d'en-tête de routage.
- Si le pare-feu IOS observe un trop grand nombre de paquets SYN, ce qui se traduit par de nombreuses connexions semi-ouvertes, il aide à protèger les systèmes en réinitialisant les connexions pour permettre l'établissement de nouvelles connexions,afin d'éviter les attaques **SYN flood** qui endommagent les serveurs d'infrastructure.
- La valeur par défaut est de 30 secondes,mais vous pouvez l'augmenter à 60 secondes si vous avez un réseau très encombré,vous pouvez la définir à 15 secondes afin être plus précis dans votre inspection des sessions TCP.

La commande suivante définit la durée pendant laquelle le CBAC gère une session TCP après qu'elle ait été fermée avec le double échange bidirectionnel FIN. La valeur par défaut est de 5 secondes,mais vous pouvez la définir à 1 seconde si vous avez un réseau très actif où vous voulez supprimer les connexions fermées très rapidement :

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

```
ipv6 inspect tcp finwait-time {seconds}
```

FIGURE II.6 – Commande de configuration

La commande suivante définit la durée pendant laquelle le CBAC gère une session TCP sans activité. La valeur par défaut est d'une heure (3 600 secondes), mais 30 minutes (1 800 secondes) pourrait être une meilleure valeur pour faire vieillir les sessions inactives plus rapidement.

```
ipv6 inspect tcp idle-time {seconds}
```

FIGURE II.7 – Commande de configuration

La commande suivante définit la durée pendant laquelle le CBAC gère une connexion UDP sans activité. La valeur par défaut est de 30 secondes, mais vous devrez peut-être augmenter cette durée à 60 secondes si votre réseau est fortement encombré par le trafic UDP. Vous pouvez également définir une valeur 15 secondes, afin d'être plus précis dans votre inspection des sessions UDP.

```
ipv6 inspect udp idle-time {seconds}
```

FIGURE II.8 – Commande de configuration

Vous pouvez utiliser la commande suivante pour définir les valeurs des paramètres de prévention DoS spécifiques à l'hôte. Cette commande définit le nombre maximal de connexions semi-ouvertes par hôte.

```
ipv6 inspect tcp max-incomplete host <value> [block-time <minutes>]
```

FIGURE II.9 – Commande de configuration

- Lorsque le nombre de connexions semi-ouvertes dépasse le niveau maximal défini dans le routeur, le pare-feu IOS réinitialise les connexions jusqu'à ce que le nombre de connexions semi-ouvertes descende en dessous du seuil minimum.
- Le routeur envoie également des messages **syslog** indiquant que le nombre maximal de connexions semi-ouvertes a été atteint, que le blocage a commencé,et également lorsque le fonctionnement normal a été rétabli.

Vous pouvez utiliser les commandes suivantes pour définir le nombre maximal de connexions semi-ouvertes par hôte et la valeur de rétablissement du bas de gamme. La valeur par défaut est de 500 connexions semi-ouvertes, et la valeur par défaut de la valeur limite basse est fixée à 400.

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

```
ipv6 inspect max-incomplete high <value>
ipv6 inspect max-incomplete low <value>
```

FIGURE II.10 – Commande de configuration

- La commande **ipv6 inspect audit-trail** permet au pare-feu IOS d'enregistrer toutes les tentatives de connexion dans le journal du routeur. Elle est désactivée par défaut pour améliorer les performances du pare-feu IOS, mais elle peut être activée pour de courtes périodes de test.
- La commande **no ipv6 inspect alert-off** active la fonction d'alerte de session du pare-feu IOS, car elle est désactivée par défaut. Si cette fonction est activée, vous recevrez des messages d'alerte dans le journal lorsque des connexions illégales sont établies et abandonnées. Voici un exemple de message qui pourrait s'afficher :

```
*Dec 12 05:01:17.003: %IPV6-6-ACCESSLOGP: list FILTER-IN/40 denied tcp
2001:DB8:11:0:20C:29FF:FE50:7F0D(53950) -> 2001:DB8:22:0:20C:29FF:FEFD:F35E(80), 1
  packet
```

FIGURE II.11 – Commande de configuration

II.7 Conclusion

Si vous choisissez de déployer IPv6 sans sécurité, cela revient à exécuter un protocole de porte dérobée sur les systèmes à double pile qui pourrait potentiellement être exploité.Ce qu'on a vu précédemment dans ce chapitre peuvent nous aider à être plus sûr. De nombreux problèmes de sécurité qui existent encore aujourd'hui continueront à exister après la transition vers IPv6.IPv6 a des caractéristiques uniques qui le rendent légèrement plus sûr qu'IPv4. IPv6 change la façon dont vous communiquez et vos architectures de sécurité doivent s'adapter à ce changement. Les produits de sécurité IPv6 s'améliorent et ont la parité de fonctionnalités entre IPv4 et IPv6.

3. Eric Vyncke,IPv6 Security,Scott Hogg, CCIE No. 5133,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

Chapitre III

Sécuriser les mécanisme de transitions

III.1 Introduction

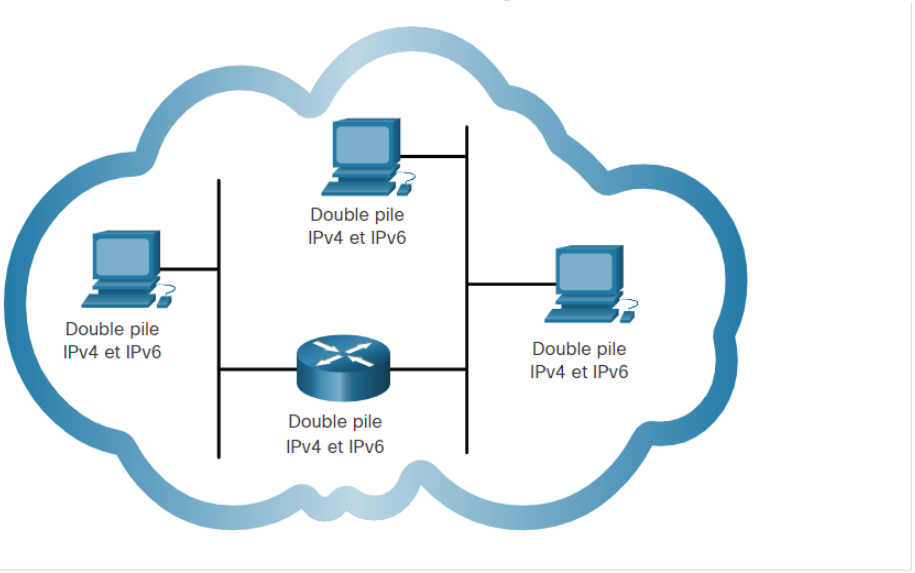
La migration vers un internet IPv6 ne se fera pas du jour au lendemain. IPv4 et IPv6 devront coexister pendant plusieurs années avant la disparition progressive d'IPv4. L'Internet Engineering Task Force (IETF) a donc mis au point plusieurs mécanismes, dont **la double pile,les tunnels et la traduction**, afin de permettre la communication pendant cette phase de transition qui devrait durer pendant plusieurs années car elle n'a pas de date de début ou de fin définitive.

III.2 techniques de transitions IPv4-IPv6

III.2.1 Double pile

La technologie dual-stack (double pile) permet aux adresses IPv4 et IPv6 de coexister sur un même segment de réseau. Les périphériques double pile exécutent les piles de protocoles IPv4 et IPv6 simultanément. Connu sous le nom d'IPv6 natif, cela signifie que le réseau client dispose d'une connexion IPv6 à son FAI et est en mesure d'accéder au contenu trouvé sur Internet via IPv6.

FIGURE III.1 – Double pile



Inconvénient :

- ➢ L'utilisation de la double pile résulte une consomation accrue de la mémoire des routeurs,car deux tables de routage sont nécessaire une pour ipv6 et une pour ipv4.
- ➢ Une augmentation légère de la CPU dans les routeurs.
- ➢ Hôtes (certains temporisateurs doivent être dupliqués).

Question :

Si un hôte est à double pile, comment un initiateur de connexion peut-il décider d'utiliser soit IPv4, soit IPv6 ?

8. Chen Su , Renjie Liu ,Xing Li,Department of Electronic Engineering, Tsinghua University Beijing, China,2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC 2019)

✓ Dans tous les systèmes d'exploitation, IPv6 est toujours préféré à IPv4 lorsqu'il existe une connectivité IPv6 native, comme l'illustre la figure.

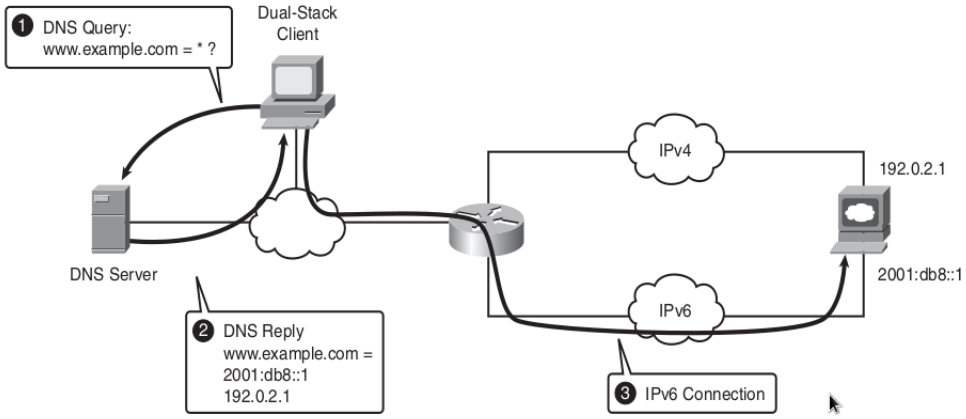


FIGURE III.2 – Choisir entre IPv4 ou IPv6

❶ Lorsqu'un client dual-stack veut se connecter à un serveur, tel que http :// www.example.com, il demande d'abord à un serveur DNS (Domain Name System) la liste des adresses de http ://www.example.com.

❷ La réponse du DNS contient la liste de toutes les adresses IPv4 et IPv6 de http :// www.example.com. Les adresses IPv4 sont dans un enregistrement de ressources (RR) d'adresse (A), et les adresses IPv6 sont dans un RR différent : AAAA (les adresses IPv6 sont quatre fois plus grandes que les adresses IPv4).

❸ Le client sélectionne l'adresse IPv6 parce qu'elle est préférée localement par la `politique de sélection d'adresses` par défaut, et le client utilise IPv6 pour se connecter à l'adresse IPv6 du serveur, 2001 :db8 : :1.

8. Chen Su , Renjie Liu ,Xing Li,Department of Electronic Engineering, Tsinghua University Beijing, China,2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC 2019)

Remarque :

⇨ Presque tous les systèmes d'exploitation (OS) récents utilisent cette technique de transition par défaut.Cela inclut Windows Vista, Mac OS X et de nombreuses distributions UNIX et Linux.

III.2.2 Les tunnels :

Question :

Comment un hôte peut-il utiliser IPv6 s'il n'y a pas de connectivité IPv6 native ?

Réponse :

✓ Dans ce cas, les tunnels entrent en jeu. Les tunnels ajoutent une surcharge en termes de taille de paquets et de procédures de fonctionnement, cette approche n'est donc pas la préférée. Cependant, l'approche par tunnel pourrait être la seule option pratique pendant quelques années, jusqu'à ce que l'IPv6 devienne omniprésent.

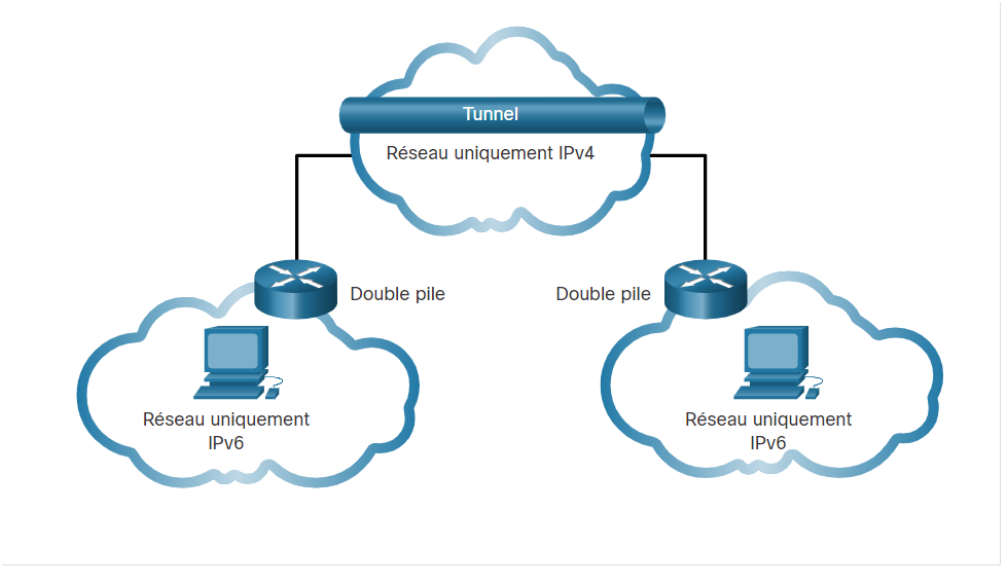


FIGURE III.3 – Tunneling

III.2.3 Tunnels

La transition de tunneling est utilisée pour la transmission sécurisée de données. Le tunneling permet aux paquets de données d'un réseau privé d'être transmis sur un réseau public grâce au processus d'encapsulation. Le tunneling fournit un chemin sécurisé pour transmission de données à travers un réseau ouvert ou non fiable.

❶ **Les adresses de source et de destination :** Les adresses IPv4 des routeurs de terminaison de tunnel.

❷ **Type de protocole :** 41 (c'est-à-dire 0x29), pour indiquer qu'IPv6 est encapsulé dans IPv4.

❸ **Autres champs :** Ont leur valeur habituelle ,l'ID et le décalage de fragment peuvent être utilisés si la fragmentation est nécessaire après l'encapsulation, Time-to-Live (TTL) est défini à une valeur par défaut.

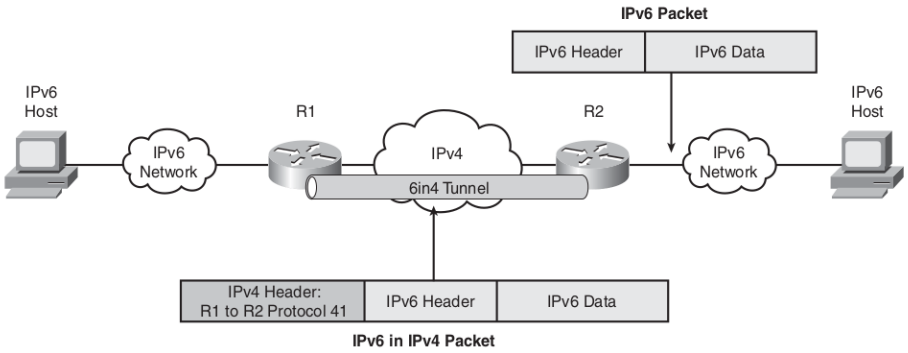


FIGURE III.4 – Tunnels configurés, structure du paquet

❶ **Tunnels 6to4 :** Connecter un ensemble ouvert de réseaux IPv6 à travers l'Internet IPv4 et ajouter une connectivité à l'internet IPv6. Les adresses IPv6 sont dérivées de l'adresse IPv4 du routeur 6to4.

❷ **Tunnels ISATAP :** Connecter un ensemble ouvert d'hôtes IPv6 distants à un réseau IPv6 à travers tout réseau IPv4. Les adresses IPv6 sont créées à partir d'un préfixe unicast global et des adresses IPv4.

❸ **Tunnels Teredo :** Semblables à ISATAP mais utilisent l'encapsulation du port UDP 3544 afin de pouvoir traverser un dispositif NAT.

III.2.4 La Traduction

La traduction d'adresses de réseau 64 (ou NAT64) permet aux périphériques IPv6 de communiquer avec des périphériques IPv4 à l'aide d'une technique de traduction analogue à la NAT pour IPv4. Un paquet IPv6 est traduit en un paquet IPv4, et inversement.

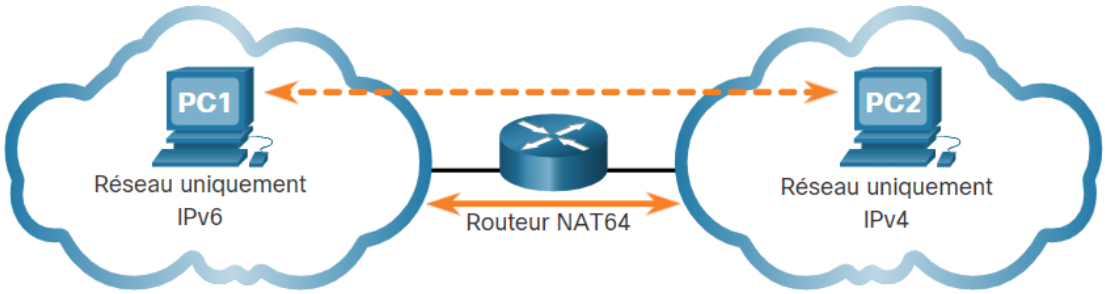


FIGURE III.5 – Traduction

4. Silvia Hagen,IPv6 Essentials,Third Edition,Printed in the United States of America.Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

III.2.5 protocole de translaion :

La traduction d'adresse de réseau - traduction de protocole (NAT-PT), permet aux hôtes IPv6 natifs de communiquer avec les hôtes IPv4 natifs et vice versa. Chaque dispositif NAT-PT dispose d'un pool d'adresses IPv4 routables au niveau mondial, à attribuer dynamiquement aux hôtes IPv6. Les dispositifs NAT-PT disposent de passerelles de niveau Application Level Gateways (ALG) telles qu'un dispositif NAT IPv4 ou un pare-feu. Par exemple, la Figure décrit le ALG DNS :

❶ Le nœud IPv4 émet une requête DNS pour l'adresse IPv4 de www.example.com, et le NAP-PT traduit cette requête en une requête générique pour tout type d'adresses pour www.example.com.

❷ Lorsque la réponse à la requête DNS ne contient qu'une adresse IPv6 (enregistrement AAAA), la requête est interceptée par le NAP-PT.

❸ Une mise en correspondance dynamique entre l'adresse IPv6 de www.example.com et une adresse Ipv4 du pool NAT-PT est synthétisé.

❹ La réponse DNS interceptée est ensuite réécrite à l'adresse IPv4 allouée de façon dynamique du pool NAT-PT.

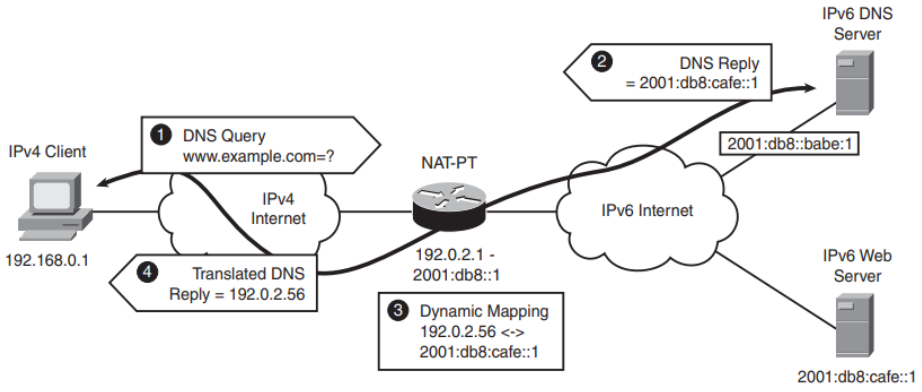


FIGURE III.6 – Architecture NAT-PT et DNS ALG en action

❶ Le client IPv4 à l'adresse 192.168.0.1 envoie ensuite des paquets à l'adresse IPv4 192.0.2.56, reçue dans le message de réponse à la requête DNS.

❷ Le dispositif NAT-PT traduit ensuite les paquets IPv4 avec la paire d'adresses suivante . <192.168.0.1, 192.0.2.56> en paquets IPv6 utilisant une paire d'adresses de <2001 :db8 : :1, 2001 :db8 :cafe : :1>.

❸ On suppose que les charges utiles de la couche 4, telles que TCP ou UDP, sont simplement copiées des paquets IPv4 vers les paquets IPv6 et vice versa.Certains protocoles intègrent des adresses IP dans leurs données utiles (comme FTP, SIP, etc.), et des ALG supplémentaires doivent modifier ces données utiles en conséquence.

NAPT-PT :

⇨ NAT-PT peut être étendu à Network Address Port Translation-Protocol Translation (NAPT-PT),une variante de NAT-PT dans laquelle plusieurs adresses IPv6 sont mappées à une seule adresse IPv4. Le démultiplexage se fait par le biais de ports TCP ou UDP.

9. Hrithik Goyal,Ravi KumarSchool of Electronics Engineering (SENSE) Vellore Institute of Technology Vellore, India2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN

III.3 Mise en œuvre de la sécurité à double pile

III.3.1 Exploitation de l'environnement à double pile

Le principal problème avec les hôtes à double pile est que l'IPv6 est activé par défaut sur plusieurs systèmes d'exploitation récents (notamment Microsoft Vista et certaines versions de Mac OS X et Linux), et qu'une politique de sécurité IPv6 n'est pas toujours appliquée,un responsable de la sécurité établit une politique de sécurité stricte et bien comprise pour le réseau IPv4 mais peut être ignore le réseau IPv6. Ce dernier point est assez dangereux car même si un réseau n'exécute pas IPv6, les hôtes à double pile sont ouverts aux attaques IPv6 locales.

L'exemple est une capture d'écran du renifleur de protocole Wireshark sur un réseau fonctionnant officiellement en IPv4,les étapes appliquer pour attaquer la machine MAX OS X :

❶ L'attaquant sait qu'il y a quelques machines Mac OS X avec IPv6 activé par défaut sur ce réseau local.

❷ L'utilisateur malveillant sait également que toutes les machines Mac OS X sont protégées contre les attaques IPv4 mais pas contre les attaques IPv6.

❸ L'attaquant attend alors simplement qu'un Mac cible transmette sa sollicitation périodique de routeur RS (trame 6) et la réponse d' annonce de routeur RA (trame 8) qui contient un préfixe : 2001 :db8 :dead : :/64.

❹ L'hôte Mac compléte son @ IPv6 avec l'Autoconfiguration (SLAAC).

❺ La victime exécute une détection d'adresse en double en envoyant la trame 9,il s'agit d'une sollicitation de voisin pour sa nouvelle adresse IPv6 : (2001 :db8 :dead :0 :20d :93ff :fe38 :c874) (qui est une adresse d'extension de confidentialité composée du RA et d'un nombre aléatoire).

❻ L'attaquant dispose maintenant de suffisamment d'informations pour lancer une attaque IPv6 contre la machine Mac OS X.

Remarque :

⇨ Le succès de l'attaque dépend du fait que la victime ne soit pas protégée contre les attaques IPv6 (par exemple, l'utilisateur Mac peu méfiant n'a pas de pare-feu IPv6 personnel). De plus, si le système de détection d'intrusion dans le réseau (NIDS) ne connaît pas IPv6 le NIDS ne détectera pas ces attaques.

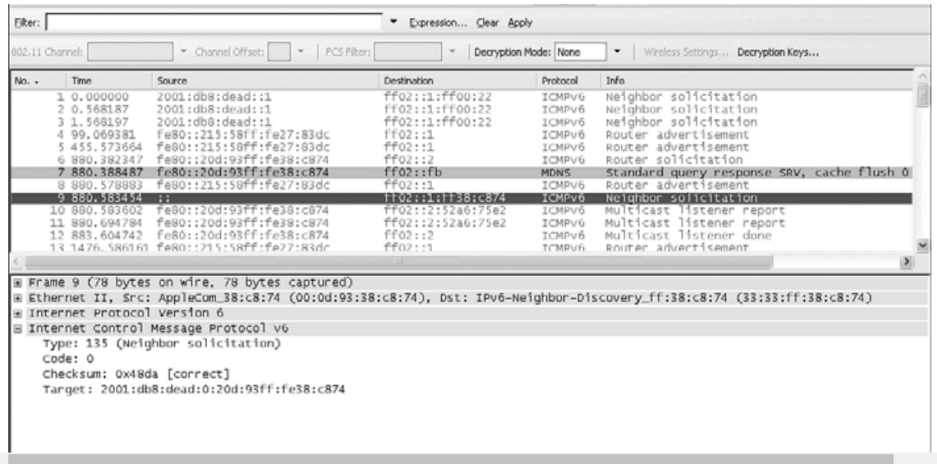


FIGURE III.7 – Capture Wireshark.

9. Hrithik Goyal,Ravi KumarSchool of Electronics Engineering (SENSE) Vellore Institute of Technology Vellore, India2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN

Problématique :

- ➢ Certains produits de sécurité ne prennent pas en charge IPv6.
- ➢ Les produits de sécurité prenant en charge IPv6 ne sont pas toujours configurés pour IPv6 parce que l'administrateur de sécurité ne sait pas comment configurer ses produits pour IPv6 ou parce qu'il ne sait pas qu'IPv6 existe.
- ➢ La prise en charge d'IPv6 par les produits est généralement récente et n'a pas toujours fait ses preuves sur le terrain. Cela peut entraîner des bogues et des vulnérabilités dans le nouveau code logiciel.

III.3.2 Protection des hôtes à double pile

Il existe de nombreuses façons de protéger un hôte à double pile contre les vulnérabilités :

❶ **Pare-feu IPv6 personnel :** Certains produits existants prennent en charge IPv6,ils doivent simplement être configurés correctement.

❷ **Cisco Security Agent (CSA) 6.0 :** Peut agir comme un pare-feu personnel et est conscient de l'IPv6. Les menaces latentes liées à IPv6 peuvent également être écartées en désactivant la pile IPv6 ou en bloquant tout le trafic IPv6.

Cette désactivation d'IPv6 peut se faire de plusieurs manières :

→ **L'agent de sécurité Cisco (CSA) 6.0** : Peut bloquer tout le trafic IPv6 à destination et en provenance d'une machine.

→ **Objets de stratégie de groupe (GPO)** de Microsoft Windows : Peuvent être utilisés dans un domaine Active Directory pour désactiver le protocole IPv6 sur toutes les interfaces.

→ **Bloquer tout le trafic IPv6 natif :** Un commutateur de couche 2 pourrait bloquer toutes les trames Ethernet avec Ethertype 0x86dd.

III.4 Le piratage du tunnel

III.4.1 Injection dans un tunnel

Tous les différents mécanismes de tunnellisation (de 6in4 à Teredo) n'intègrent pas de sécurité c-à-d : pas d'authentification, pas de contrôle d'intégrité et pas de confidentialité. Cela se traduit par plusieurs menaces génériques applicables à tous les mécanismes de tunnel :

❶ **Injection dans le tunnel :** Le pirate peut injecter du trafic dans le tunnel en se faisant passer pour un utilisateur légitime en usurpant un utilisateur légitime (@IPv4 externe , @IPv6 interne).

❷ **Reniflage du tunnel :** Un espion situé sur le chemin IPv4 du tunnel peut renifler les paquets IPv6 transmis par le tunnel et avoir accès à l'information.

10. Ashis Saklani1 , S. C. Dimri2 Department of Computer Science, H.N.B Garhwal Central University, Srinagar Garhwal, Uttarakhand, India International Journal of Science and Research (IJSR), India Online ISSN : 2319-7064

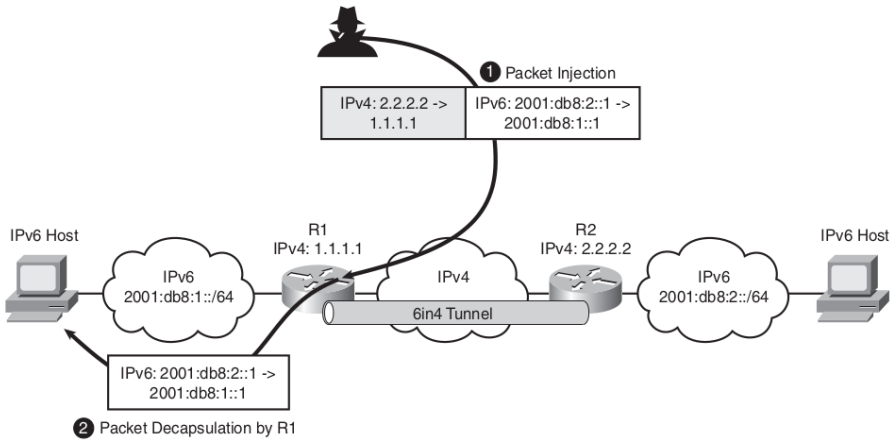


FIGURE III.8 – Injection dans un tunnel

III.4.2 Attaque par réflexion sur un hôte interne

L'injection d'un hôte intermédiaire comme illustrée sur la figure :

- ❶ L'attaquant génère un paquet IPv4 contenant un paquet IPv6 TCP SYN destiné à l'hôte IPv6 intermédiaire.
- ❷ Le point terminal du tunnel R1 décapsule et transmet le paquet IPv6 à la destination IPv6, à savoir l'hôte IPv6 intermédiaire.
- ❸ L'hôte IPv6 intermédiaire répond au TCP SYN par un paquet TCP SYN+ACK destiné à l'adresse IPv6 source usurpée.
- ❹ En passant par le tunnel entre R1 et R3, le paquet TCP SYN+ACK IPv6 atteint sa destination.

Dans les deux cas, la victime remarque les paquets provenant de 2001 :db8 :3 : :1, et il est pratiquement impossible de retracer ces paquets IPv6. Retrouver la trace de l'attaque nécessite une collaboration active de tous les routeurs IPv6 et de tous les ISP IPv4 sur le chemin des paquets injectés.

III.4.3 Attaque par réflexion à l'extrémité du tunnel

- ❷ L'attaquant génère un paquet IPv4 contenant un paquet IPv6.
- ❸ Le paquet injecté atteint d'abord le point final du tunnel R1, où il est décapsulé, transféré et réencapsulé vers le point final du tunnel R3.
- ❹ Le point final du tunnel R3 décapsule le paquet IPv6 et le transmet à la destination finale IPv6.

III.4.4 Sécuriser le tunnel statique (6in4) :

Les extrémités du tunnel sont configurés statiquement, le réseau dispose de suffisamment d'informations pour renforcer la sécurité des tunnels,vous pouvez protéger les tunnels configurés en combinant les techniques suivantes :

- ❶ **Vérifiez l'adresse source IPv4 :** Rejeter tous les paquets du tunnel dont l'adresse source ne correspond à aucune source des tunnels configurés,dans se cas l'attaquant doit découvrir les deux extrémités du tunnel.

10. Ashis Saklani1 , S. C. Dimri2 Department of Computer Science, H.N.B Garhwal Central University, Srinagar Garhwal, Uttarakhand, India International Journal of Science and Research (IJSR), India Online ISSN : 2319-7064

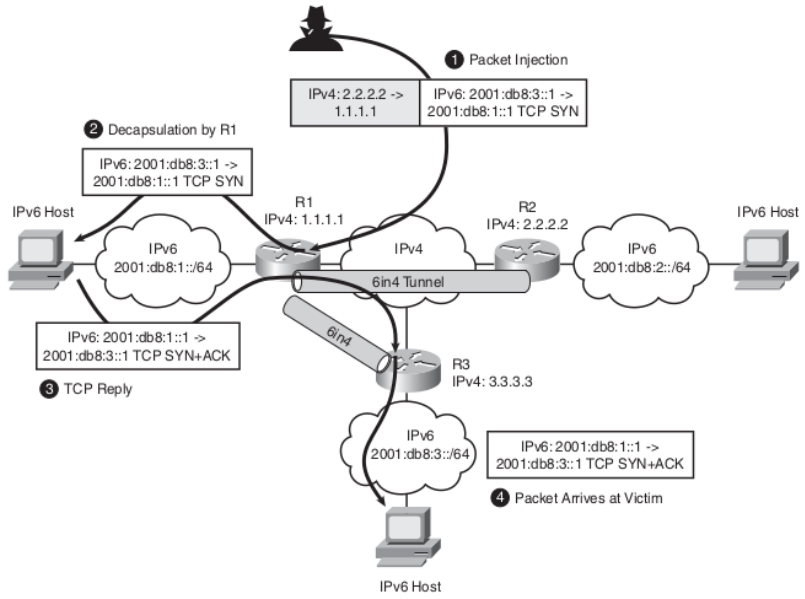


FIGURE III.9 – Attaque par réflexion sur un hôte interne

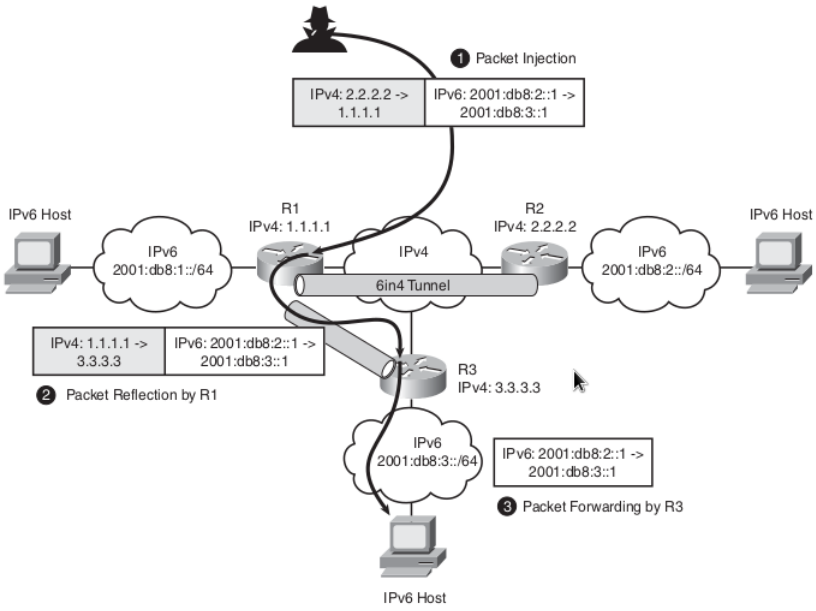


FIGURE III.10 – Attaque par réflexion à l'extrémité du tunnel

❷ **Utilisez des techniques anti-spoofing :** Rejetez les paquets IPv6 qui sortent du mauvais tunnel,Cela bloque l'attaque par réflexion.

❸ **Utiliser IPsec :** IPsec peut être utilisé pour protéger tout trafic,y compris le trafic tunnelé,cela permet d'éviter les attaques par injection et par reniflage.

10. Ashis Saklani1 , S. C. Dimri2 Department of Computer Science, H.N.B Garhwal Central University, Srinagar Garhwal, Uttarakhand, India International Journal of Science and Research (IJSR), India Online ISSN : 2319-7064

Note :

⇨ L'IPsec seul n'empêche pas l'usurpation d'identité entre sites légitimes. Cela se produit lorsqu'il y a un utilisateur malhonnête (ou un cheval de Troie) situé dans un réseau légitime qui envoie des paquets IPv6 usurpés.C'est pourquoi l'IPsec doit être associé à des vérifications **Unicast RPF(Reverse Path Forwarding)** comme illustre la figure suivante :

```
! CEF is required to enable uRPF checks
ipv6 cef

interface Tunnel1
 description IPv6 tunnel
 no ip address
 ipv6 address 2001:db8::1/64
 ipv6 enable
 ipv6 mtu 1472
```

FIGURE III.11 – Tunnel configuré avec une vérification RPF Unicast activée

```
 ipv6 verify unicast reverse-path
 tunnel source Dialer0
 tunnel destination 192.0.2.11
 tunnel mode ipv6ip
```

FIGURE III.12 – Tunnel configuré avec ube vérification RPF Unicast activée(suite)

N'oubliez pas les points suivants lorsque vous utilisez les contrôles RPF d'unicast :

➟ Le CEF doit être activé pour que la vérification RPF d'unicast fonctionne sinon même les paquets légitimes sont abandonnés.

➟ Lorsque vous utilisez un protocole de routage tel que Open Shortest Path First (OSPF), vous devriez activer l'authentification pour ces protocoles sinon, l'attaquant pourrait injecter des informations erronées pour empoisonner la vérification RPF.

III.5 Attaque de NAT-PT

Avec NAT-PT il n'y a aucun moyen de configurer un tunnel IPsec entre un hôte uniquement IPv4 et un hôte uniquement IPv6, tout le trafic doit être en clair pour que pour que l'ALG fonctionne. Comme NAT-PT modifie les réponses DNS, DNSSec ne peut pas être utilisé.

Remarque :

⇨ DNSSec est l'abréviation de DNS Security. Il s'agit d'une extension standard du DNS qui signe essentiellement tous les paquets DNS et toutes les informations DNS. Comme le NAT-PT modifie le contenu de l'information DNS, cela rend la signature invalide.

Les attaques NAT-PT sont :

10. Ashis Saklani1 , S. C. Dimri2 Department of Computer Science, H.N.B Garhwal Central University, Srinagar Garhwal, Uttarakhand, India International Journal of Science and Research (IJSR), India Online ISSN : 2319-7064

```
Router# show ipv6 interface tunnel 1
Tunnel1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C000:201
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8::1, subnet is 2001:DB8::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::9
    FF02::1:FF00:1
    FF02::1:FF00:201
  MTU is 1472 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Input features: RPF
  Unicast RPF
    Process Switching:
      0 verification drops
      0 suppressed verification drops
    CEF Switching:
      7 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  Hosts use stateless autoconfig for addresses.
```

FIGURE III.13 – Vérification des paquets rejetés.

❶ **Attaque par épuisement du pool :** Un utilisateur IPv6 malveillant envoie plusieurs requêtes sortantes (chacune avec une adresse IPv6 différente et usurpée) à certains serveurs IPv4, et chaque demande consomme une adresse IPv4 du pool NAT-PT. Après plusieurs requêtes, le pool est épuisé, et aucune autre demande n'est acceptée.

❷ **Attaque du CPU de l'ALG :** Les ALGs ne peuvent pas être implémentés en matériel à cause de la complexité du protocole. Par conséquent, ils sont exécutés sur une unité centrale polyvalente,qui pourrait être débordé si un attaquant continue à envoyer un grand nombre de requêtes qui nécessitent une inspection ALG (comme les requêtes DNS).

Solution :

✔ Limitation de débit au sein du dispositif NAT-PT.

✔ L'épuisement du pool peut être évité en luttant contre l'usurpation d'identité dans le réseau (avec des mécanismes tels que la protection de la source IP).

Remarque :

⇨ Le fait que le NAT-PT s'appuie sur les ALG cela ne supprime pas la nécessité d'un pare-feu pour une organisation qui se connecte à Internet. Les ALGs dans NAT-PT ne sont là que pour le NAT et non pour la sécurité. L'application des proxys entre les mondes IPv6 et IPv4 présentent les mêmes vulnérabilités en matière de sécurité que l'approche NAT-PT : épuisement du CPU. Par conséquent, les mêmes techniques d'atténuation s'appliquent également.

8. Chen Su , Renjie Liu ,Xing Li,Department of Electronic Engineering, Tsinghua University Beijing, China,2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC 2019)

III.5.1 Les politiques relatives aux mécanismes de transition

❶ Préférer la double pile comme mécanisme de transition, mais sécuriser chaque protocole de manière égale.

❷ Utiliser uniquement des tunnels configurés manuellement - en privilégiant IPsec - et effectuer un filtrage sur les extrémités des tunnels.

❸ Éviter le protocole 6to4 s'il n'est pas nécessaire.

❹ Empêcher les ordinateurs Windows d'utiliser Teredo, sauf si une dérogation spéciale à la politique de sécurité a été signée. de sécurité a été signée.

❺ Ne pas autoriser les tunnels IPv6-in-IPv4 (protocole IP 41) à travers le périmètre, sauf si cela est nécessaire.

III.6 Conclusion

III.7 Comparaison de la sécurité d'IPv4 et d'IPv6

III.7.1 Similitudes entre IPv4 et IPv6

➢ Si l'on considère la pile de protocoles TCP/IP, la couche Internet (couche réseau de l'Open Systems Interconnexion [ISO]) est la seule différence entre IPv4 et IPv6.

➢ IP peut fonctionner sur Ethernet, les liaisons PPP, SONET .

➢ IP prend en charge de nombreux protocoles de transport différents (par exemple, User Datagram Protocol [UDP], Transmission Control Protocol [TCP], Stream Control Transmission Protocol [SCTP], et le protocole de contrôle de congestion des datagrammes [DCCP]).

➢ Lors de la transition vers IPv6, les couches supérieures et inférieures à IPv6 resteront les mêmes. Si votre application web est vulnérable dans un environnement IPv4, elle sera également vulnérable aux attaques lorsque IPv6 sera mis en place.

➢ Il existe de nombreuses similarités entre les deux en-têtes IPv4 et IPv6. Les deux en-têtes comportent toujours une version, un champ (QoS), un champ de longueur de la charge utile, un compteur pour détecter la distance parcourue par le paquet, la valeur du protocole de la couche supérieure suivante, et de la valeur de l'en-tête.

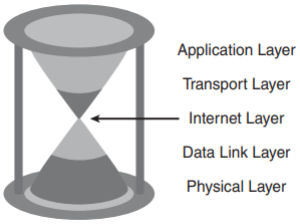


FIGURE III.14 – Le sablier du protocole Internet

❑ De nombreux types d'attaques sont similaires entre IPv4 et IPv6, notamment les suivants :

➟ Attaques au niveau de la couche application.

➟ Accès non autorisé.

➟ Attaques de type Man-in-the-Middle.

7. Prabhu Thiruvasagam and K. Jijo George,Journal of ICT standardization,NEC India Private Limited, India.Received 02 December 2018 ; Accepted 06 January 2019.

- ➟ Reniflage.
- ➢ Attaques par déni de service (DoS).
- ➟ Paquets falsifiés : fausses adresses et autres champs.
- ➟ Attaques contre les routeurs et autres dispositifs de mise en réseau Attaques contre les couches physique ou de liaison de données.

III.7.2 différences entre l'Ipv6 et l'Ipv4

Voici la liste des menaces qui ne sont que légèrement modifiées par IPv6 :

- ➟ Les attaques basées sur le réseau local (protocole de résolution d'adresse [ARP] ou protocole de découverte de voisins [NDP]).
- ➟ Attaques contre DHCP ou DHCPv6.
- ➟ Fragmentation (routeurs IPv4 effectuant la fragmentation Vs hôtes IPv6 utilisant un en-tête d'extension fragmenter)
- ➟ Attaques par amplification de paquets (IPv4 utilise la diffusion ,IPv6 utilise la multidiffusion)
- ❑ Si vous choisissez de déployer IPv6 sans sécurité, cela revient à exécuter un protocole de porte dérobée sur les systèmes à double pile qui pourrait potentiellement être exploité. De nombreux problèmes de sécurité qui existent aujourd'hui continueront d'exister après la transition vers IPv6. IPv6 a des caractéristiques uniques qui le rendent légèrement plus sûr qu'IPv4. IPv6 change la façon dont vous communiquez et vos architectures de sécurité doivent s'adapter à ce changement. Les produits de sécurité IPv6 s'améliorent et ont la parité de fonctionnalités entre IPv4 et IPv6.

5. Rick Graziani,IPv6 Fundamentals,Second Edition,Straightforward Approach to Understanding IPv6,Cisco Press 800 East 96th Street Indianapolis, IN 46240

Chapitre IV

Déploiement d'une solution IPv6 pour une Coursuprme

IV.1 Simulation des architectures réseaux avec GNS3

Un technicien, administrateur ou ingénieur des systèmes d'informations,doit installer ou assurer la maintenance d'un réseau existant, en évitant de mettre en danger la production.

GNS3 (Graphical Network Simulator) permet de tester virtuellement une architecture réseau, Cet outil simple et intuitif permet de créer des réseaux, les tester, les installer et paramétrer des switchs, des routeurs, et même des serveurs. Le simulateur GNS3 permet en effet de connecter également un hyperviseur de machines virtuelles depuis Vmware ou virtualbox.

En bref, un administrateur réseaux pourrait architecturer des réseaux simples et complexes, et les simuler.

IV.1.1 Emuler, simuler, virtualiser : de quoi parle t-on ?

IV.1.1.1 Qu'est-ce que la Simulation ?

La simulation, en général, est une représentation fictive de la réalité. Il s'agit d'imiter une situation,la simulation réseau revient à reproduire l'architecture d'un réseau et cela sans utiliser de machine physique.

Pour cela, la simulation passe par un logiciel qui calcule ou qui modélise et donc prédit les événements qui seraient amenés à se produire en prenant en compte leurs caractéristiques.

- ➢ Il existe de nombreux outils pour réaliser ces simulations, comme par exemple :
- ➥ GNS3
- ➥ Cisco Packet Tracer
- ➥ Cisco Virl
- ➥ Marionnet
- ➥ Eve

Certains sont gratuits, d'autres payants.

5. Approach to Understanding IPv6,Cisco Press 800 East 96th Street Indianapolis, IN 46240

IV.1.1.2 Qu'est-ce que l'Emulation ?

Un peu plus ambitieuse que la simulation, l'émulation permet non pas de modéliser, mais bel et bien de *reproduire à l'identique* le comportement d'un logiciel et son architecture matérielle. Ce terme n'apparaît qu'en informatique.

IV.1.1.3 Et la Virtualisation ?

La virtualisation, en général, signifie rendre virtuel c'est-à-dire qui n'existe pas. Cette notion s'oppose au monde physique.*"JACK SLATE"(POLICIER DANS UN JEU VIDEO PLAYSTATION 1,2,3)* n'est pas un vrai policier que vous pouvez appeler en cas de danger !
Dans le cadre des systèmes et réseaux, la virtualisation reprend les concepts de l'émulation, à quelques différences notables près. Elle utilise l'architecture du système hôte, alors que l'émulation la reproduisait de manière logicielle.

IV.2 Architecture de sécurité

C'est d'organiser le système d'information de manière à pouvoir mieux le contrôler pour ainsi mieux le surveiller et détecter d'éventuelles menaces et évidemment y réprendre !
On va se concentrer sur les composants de sécurité réseau. On va parler de Firewall,DMZ, Proxy, Reverse Rroxy, IDS et IPS.

➢ l'objectif de ça et de donner la vision global de :

✦ comment ces 5 différents éléments fonctionnent ensemble.

✦ comment ils sont integrés au sein de système d'information.

✦ et comment ils sont complémentaires entre eux pour assurer la sécurité niveau réseau.

❑ Le réseau permet à des machines de communiquer entre elles pour s'échanger des données. Le réseau permet aussi de faire communiquer des machines internes avec l'extérieur notamment internet, et donc de communiquer avec d'autres machines en dehors de réseau local,et à l'inverse avec cette ouverture du réseau interne, les machine deviennent accessibles à des personnes extérieurs du réseau.

Comme on a vu dans les chapitres précédents le problème est que internet est aussi une porte potentiel pour des actions malveillants comme de l'espionnage ou des attaques informatique pour compromettre le système informatique, et justement l'architecture de sécurité explique comment mettre en place des éléments structurants pour protéger les machines interne, on parle aussi de la défense périmétrique.
La première pierre périmétrique est le *Farewall.*

IV.2.1 Revu sur le Firewall

❑ Le Firewall a pour fonction de sécuriser un réseau en définissant les communications autorisées ou interdites. Il permet d'interconnecter des réseaux de niveaux de sécurité différent.
Le Firewall a pour but de filtrer les communications entre les zones que ce soit en entrée ou en sortie pour les analyser, et enfin de les autoriser ou de les rejeter selon les régles de sécurité en vigueur.

➢ À savoir les critères les plus courants du filtrage sont les suivants :

✦ L'origine ou/et la destination de paquets avec l'adresse IP et les ports notamment.

✦ Les options contenues dans les données comme leurs fragmentations ou leur validité (par exemple les données elle même, et même les utilisateurs pour les Firewall les plus récents)...

5. Rick Graziani,IPv6 Fundamentals,Second Edition,Straightforward Approach to Understanding IPv6,Cisco Press 800 East 96th Street Indianapolis, IN 46240

IV.2.2 La DMZ

❑ La DMZ est un sous réseau isolé qui sépare le réseau local (le LAN), et un réseau considéré comme moins sécurisés comme internet.

Le deuxième Firewall permet de créer la DMZ, elle héberge des machines de réseau interne, mais se sont des machines qui ont besoin d'être accessibles depuis l'extérieur.

Les serveurs de LAN ne sont jamais exposés directement à internet, et à l'inverse les utilisateurs depuis internet n'ont jamais accès directement aux ressources de LAN, tout doit d'abord transiter par la DMZ, en termes de sécurité cela aussi veut dire qu'en cas de compromission d'un service dans la DMZ, le pirate n'auras accès qu'aux machines dans la DMZ et non dans le réseau local.

IV.2.3 Un serveur proxy

❑ Un serveur proxy est un serveur intermédiaire qui va permettre à une machine d'accéder à Internet, dans ce cas l'utilisateur va d'abord se connecter au serveur proxy et lui envoyer sa requête et c'est le serveur proxy qui va à son tour transmettre le message aux serveurs distants.

IV.2.4 Différence entre un firewall et un proxy

❑ Les Firewall peuvent bloquer tout ou partie des communications dans les deux sens entre les réseaux auxquels il est raccordé, tandis que le serveur proxy masque essentiellement le réseau interne sur Internet.

IV.2.5 Un reverse proxy

❑ Un reverse proxy joue le rôle inverse du proxy, il permet à un utilisateur d'Internet d'accéder à des serveurs interne.
Le reverse proxy centralise alors le flux entrant depuis internet vers les machines interne.

IV.2.6 IDS (Intrusion Détection Système)

❑ IDS s'agit d'un mécanisme qui a pour objectif de repérer tout type de trafic partiellement malveillants (par exemple les tentatives d'intrusion, les attaques virales, les débits trop importants) ou tout trafic sortant de l'ordinaire.

IDS surveille et voit tout le trafic et lance des alertes mais il n'arrête pas le trafic, il s'appuie sur une norme pour repérer des activités cible qui peut être un réseau ou des machines hôtes et si l'activité s'éloigne de la norme, IDS lancera une alerte.

IV.2.7 IPS (Intrusion prévention Système)

❑ L'IPS va réagir en temps réel en stoppant le trafic suspect qu'il reconnaît notamment en bloquant les ports, l'IPS est comme un IDS, mais qui bloque.

IV.2.8 Différence entre Firewall et IPS

➟ IPS : Son rôle est de détecter des attaques sur le réseau à partir d'une base données de signature d'attaque (comme antivirus) et les bloques si nécessaire.

➟ Firewall : Son rôle est différent puisque son but est de faire du filtrage d'accès en définissant des communications autorisées ou interdites.

6. Bob Vachon,CCNA Security Portable Command Guide,210-260,Published by :Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

IV.2.9 IPsec

- L'architecture IPSec est une suite de protocoles fournissant l'ensemble des extensions IP pour la mise en œuvre de la sécurité dans la couche réseau (IP) à la fois pour IPv4 et IPv6.

  IPSec prend en charge deux protocoles de sécurité : Authentification (AH) et Encapsulation des données utiles de sécurité (ESP). AH fournit des fonctions de sécurité d'intégrité, d'authentification. ESP, quant à lui, fournit tous les services de sécurité fournis par AH ainsi que la confidentialité. Le protocole IPSec prend en charge deux modes de fonctionnement, à savoir le mode tunnel et le mode transport. Les services de sécurité sont fournis par IPSec sont une combinaison d'algorithmes cryptographiques et de protocoles de sécurité. La norme IPSec fournit l'architecture nécessaire à la mise en place d'un tunnel IP sécurisé.

IV.3 Implémentation d'une coursupreme au niveau d'une justice :

IV.3.1 Présentation de la topologie :

La figure suivante présente la Topologie au niveau de gns3 :

6. Bob Vachon,CCNA Security Portable Command Guide,210-260,Published by :Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

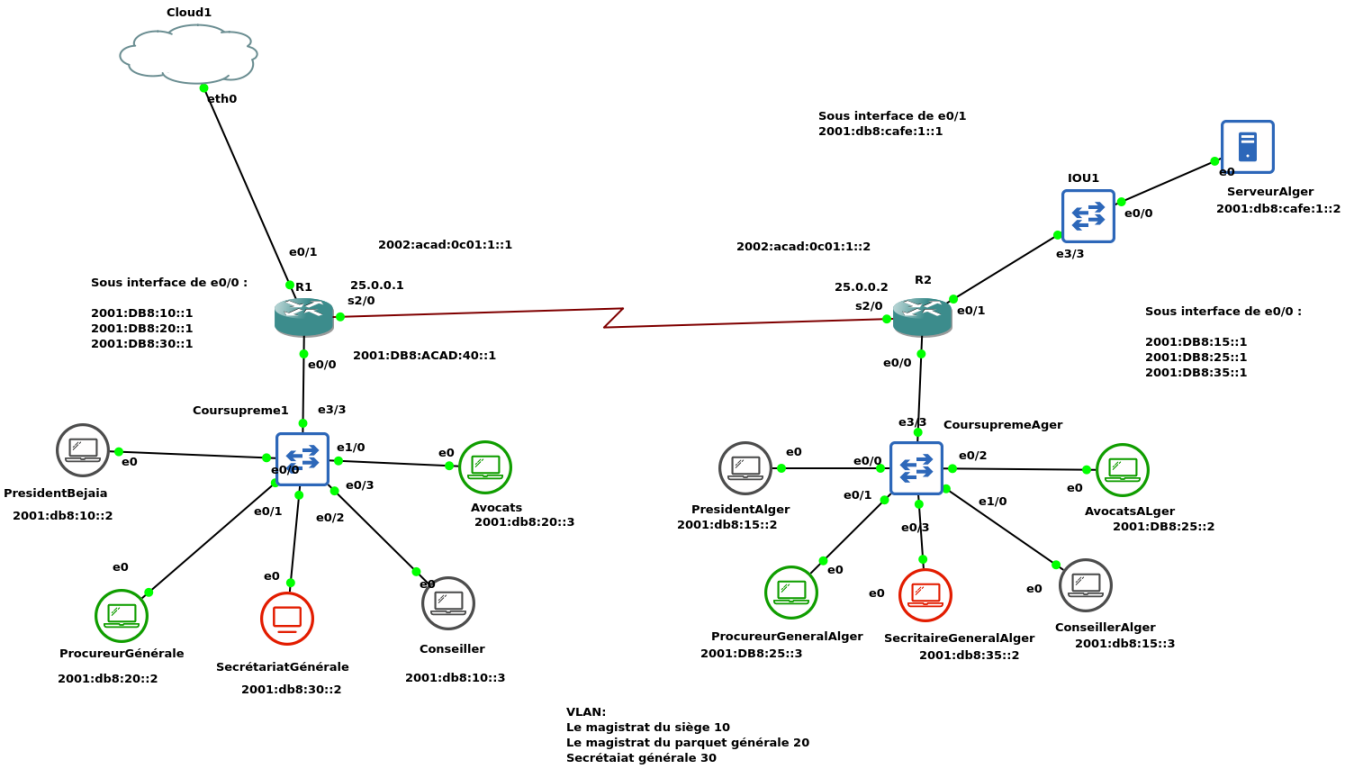


FIGURE IV.1 – Topologie de la coursupreme

IV.3.2 Configuration des Vlans IPv6

Le réseau de BEJAIA contient une succursale située sur Alger les deux contiennent une coursupreme qui est divisée en trois bureaux :

❶ Magistrat du siege : (Président du Tribunal,Conseiller).

❷ Magistrat du parquet général :(Procureur général, Avocats)

❸ Et enfin le bureau de la secrétariat général.

comme le montre la figure : le président du Tribunal et le conseiller appartiennent au même Vlan (10), le Procureur général appartienne au même Vlan (20) également,et puis enfin le secrétariat à 30 comme Vlan.

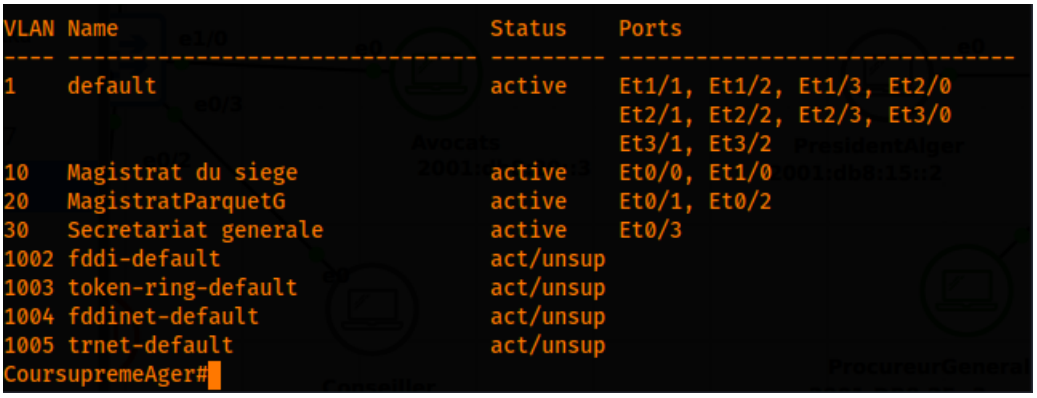


FIGURE IV.2 – Topologie de la coursupreme

Note :

⇨ La coursupreme de BEJAIA contient exactement les mêmes informations que celle d'Alger.

IV.3.3 Le routage interVlan avec la méthode : Router-on-a-Stick

La figure suivante représente l'implémentation du protocole *DOT.1Q* aux sous interfaces montrer ci-dessus avec la méthode *ROUTER-ON-A-STICK*

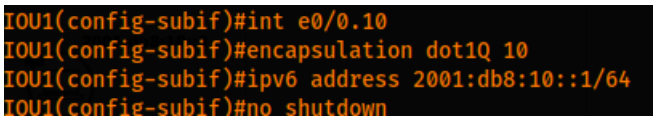


FIGURE IV.3 – Implémentation du protocole DOT.1Q

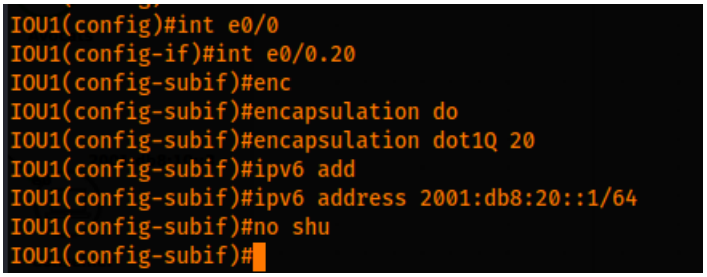


FIGURE IV.4 – Implémentation du protocole DOT.1Q

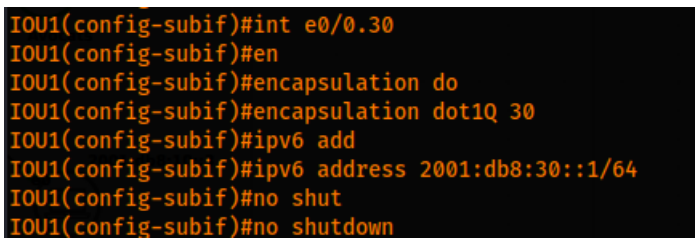


FIGURE IV.5 – Implémentation du protocole DOT.1Q

IV.3.4 Configuration du Tunnel IPv6 6 IN 4

Le tunnel IPv6 utilise le protocole 41 afin d'encapsuler le paquet IPV6 dans un paquet IPv4,la configuration des deux tunnels sur les deux extrimités des routeurs R1 et R2 sont illutrés dans les figures suivantes :

```
R1(config)#interface serial 2/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#exit
R1(config)#in
R1(config)#interface tu
R1(config)#interface tunnel 0
R1(config-if)#i
R1(config-if)#ipv6 en
R1(config-if)#ipv6 enable
R1(config-if)#tun
R1(config-if)#tunnel sou
R1(config-if)#tunnel source s
R1(config-if)#tunnel source serial 2/0
R1(config-if)#tu
R1(config-if)#tunnel d
R1(config-if)#tunnel destination 209.165.201.1
R1(config-if)#tunn
R1(config-if)#tunnel m
R1(config-if)#tunnel mo
R1(config-if)#tunnel mode ip
R1(config-if)#tunnel mode ipv
R1(config-if)#tunnel mode ipv6i
R1(config-if)#tunnel mode ipv6ip
```

FIGURE IV.6 – Extrémité du Routeur R1

```
R2(config)#interface tunnel 0
R2(config-if)#ip
R2(config-if)#ip
*Sep 17 13:53:26.912: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
hanged state to down
R2(config-if)#ip s
R2(config-if)#ip sou
R2(config-if)#tunn
R2(config-if)#ip
R2(config-if)#ipv
R2(config-if)#ipv6 en
R2(config-if)#ipv6 enable
R2(config-if)#tunn
R2(config-if)#tunnel sou
R2(config-if)#tunnel source s2/0
R2(config-if)#tun
R2(config-if)#tunnel de
R2(config-if)#tunnel destination 209.165.200.225
R2(config-if)#tunn
R2(config-if)#tunnel mode ipv6ip
R2(config-if)#exit
```

FIGURE IV.7 – Extrémité du Routeur R1

```
interface Tunnel0
 no ip address
 ipv6 address 2002:ACAD:C01:1::2/64
 ipv6 enable
 ipv6 eigrp 100
 tunnel source Serial2/0
 tunnel mode ipv6ip
 tunnel destination 25.0.0.1
```

FIGURE IV.8 – Information sur le tunnel R2

IV.3.5 Le protocole EIGRP

Pour assurer la communication de bout en bout entre le réseau de BEJAIA et celui d'ALGER nous avons fait appel à l'implémentation du protocole de routage EIGRP sur les deux router, pour que le routage prend effet on doit l'activer sur les interfaces de chaque réseau LAN comme le montre les figures suivantes :

```
R1(config)#ipv6 router eigrp 100
R1(config-rtr)#no shut
R1(config-rtr)#ei
R1(config-rtr)#eigrp r
R1(config-rtr)#eigrp router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#in
R1(config)#interface s2/0
R1(config-if)#ipv6 ei
R1(config-if)#ipv6 eigrp 100
R1(config-if)#interface tunnel 0
R1(config-if)#ipv6 eigrp 100
R1(config-if)#exit
```

FIGURE IV.9 – EIGRP sur R1

```
R2(config)#ipv6 router eigrp 100
R2(config-rtr)#no shutdown
R2(config-rtr)#eigrp router-id 2.2.2.2
R2(config-rtr)#exit
R2(config)#in
R2(config)#interface s2/0
R2(config-if)#ipv6 eigrp 100
R2(config-if)#in
R2(config-if)#interface tunnel 0
R2(config-if)#ipv6 eigrp 100
R2(config-if)#exit
```

FIGURE IV.10 – EIGRP sur R2

```
interface Serial2/0
 ip address 25.0.0.2 255.255.255.0
 ipv6 eigrp 100
 ipv6 eigrp 1
 serial restart-delay 0
 crypto map MY_crypto_map
!
```

FIGURE IV.11 – Activation de EIGRP sur l'interface LAN du R2

```
*Sep 18 11:00:33.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0
, changed state to up
*Sep 18 11:00:36.966: %DUAL-5-NBRCHANGE: EIGRP-IPv6 100: Neighbor FE80::1900:
2 (Tunnel0) is up: new adjacency
```

FIGURE IV.12 – Activation réussi de EIGRP sur les deux extrémités

IV.3.6 Configuration de IPsec

On a implémenté le protocole IPsec afin de sécuriser le trafic qui passe par le tunnel et pour pallier l'attaque d'injection du paquet sur le tunnel comme expliquer dans le chapitre 3,la figure suivante illustre les informations du protocole IPsec sur le Router R2 :

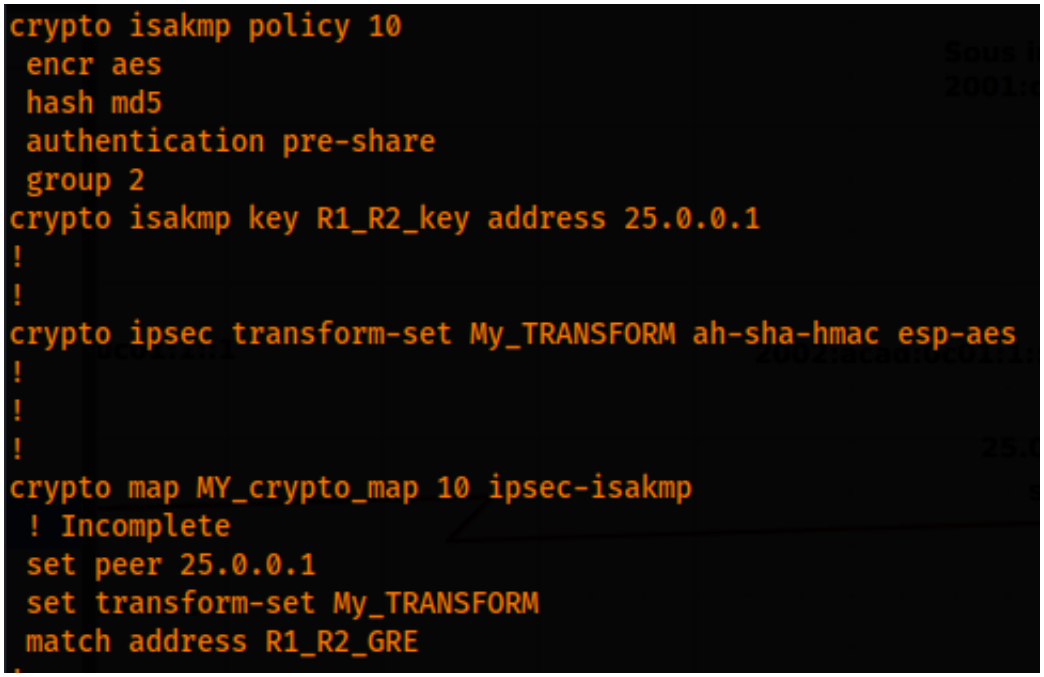


FIGURE IV.13 – Informations sur le protocole IPsec du R2

IV.3.7 Configuration de l'équipement du Président de Tribunal de BEJAIA

La figure suivante montre la configuration de l'hote windows du président de tribunal de BEJAIA :

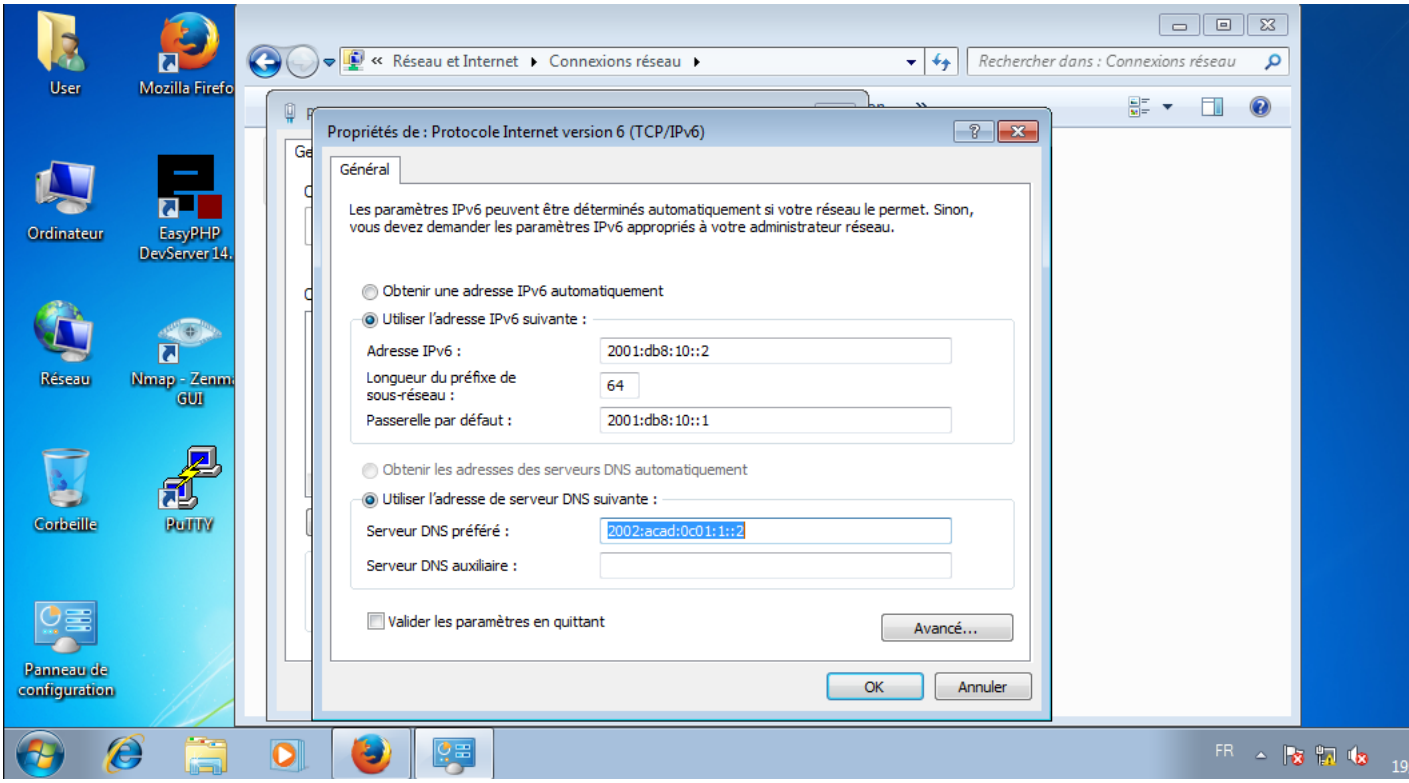


FIGURE IV.14 – Addressage IPv6 sur un hote windows du président de tribunal de BEJAIA

IV.3.8 Configuration du Serveur d'ALGER

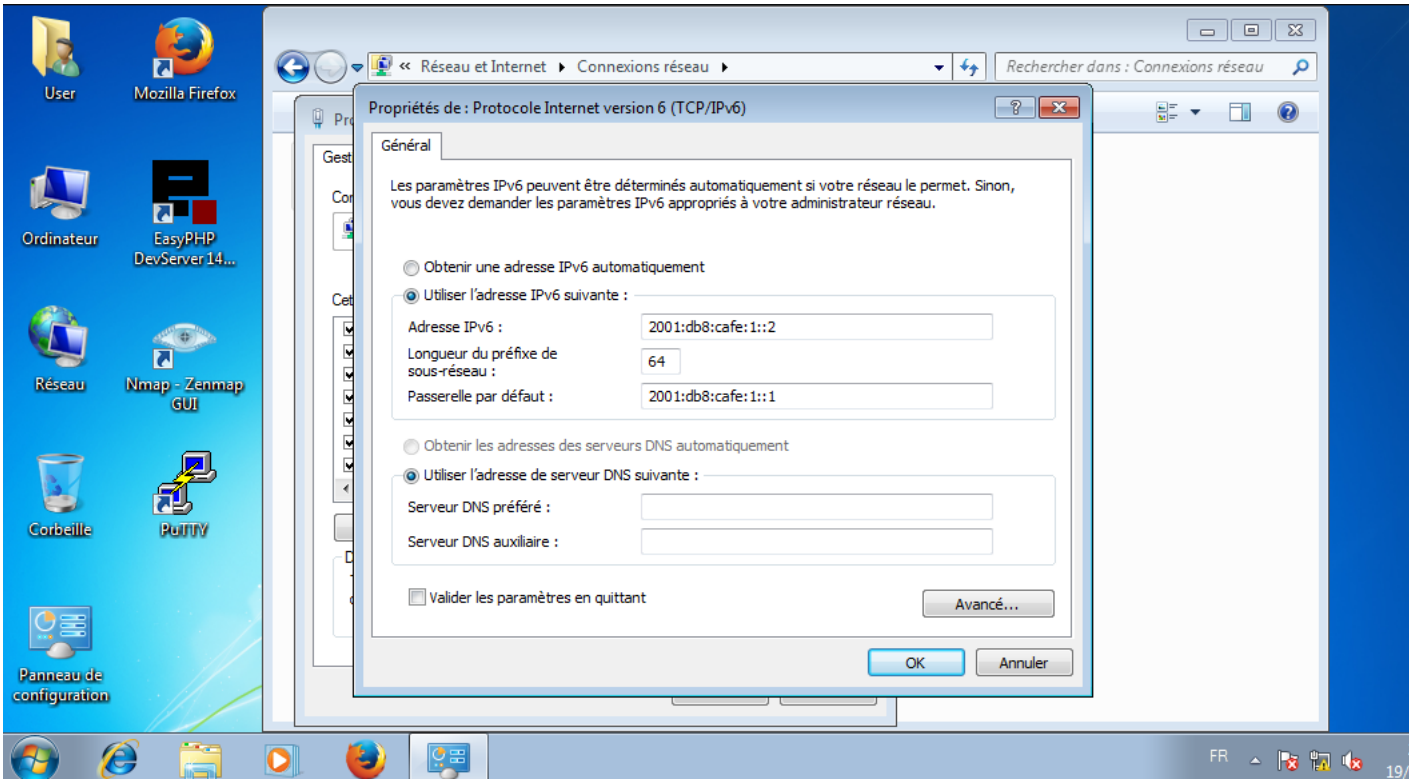


FIGURE IV.15 – Configuration du Serveur situé à ALGER

IV.4 Test de connectivité

IV.4.1 Le président du tribunal de BEJAIA se connecte au Serveur d'ALGER

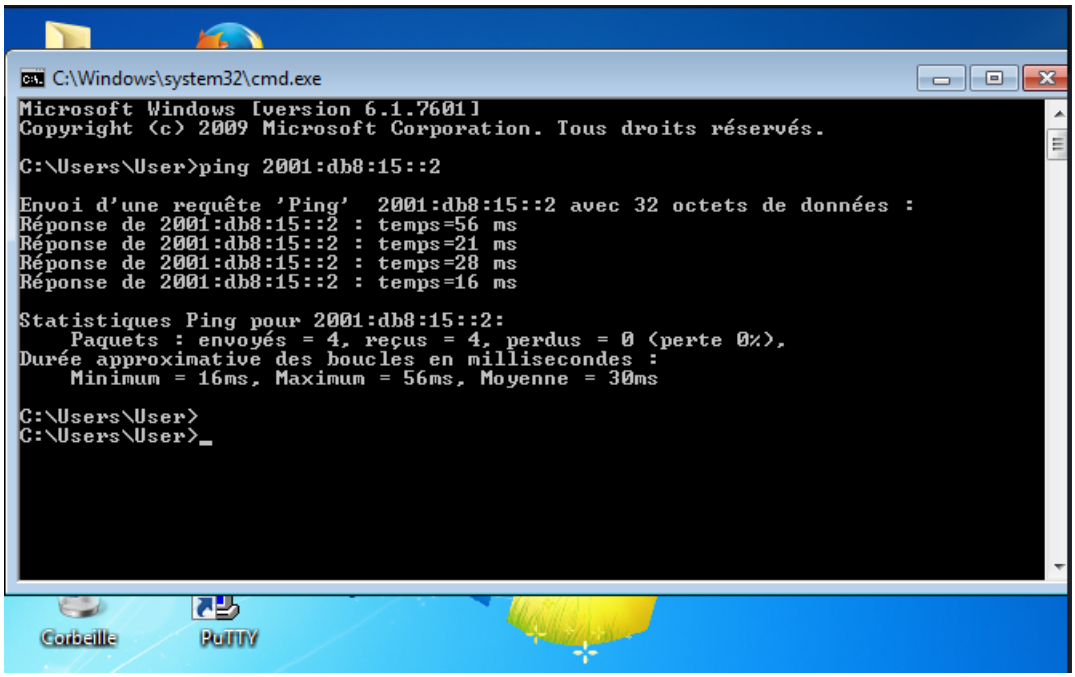


FIGURE IV.16 – Configuration du Serveur situé à ALGER

IV.5 Connexion entre le Président du Tribunal de BEJAIA et celui d'ALGER

IV.5.1 Ping BEJAIA ALGER

La figure suivante montre un test de connectivité entre les deux présidents d'ALGER et de BEJAIA.

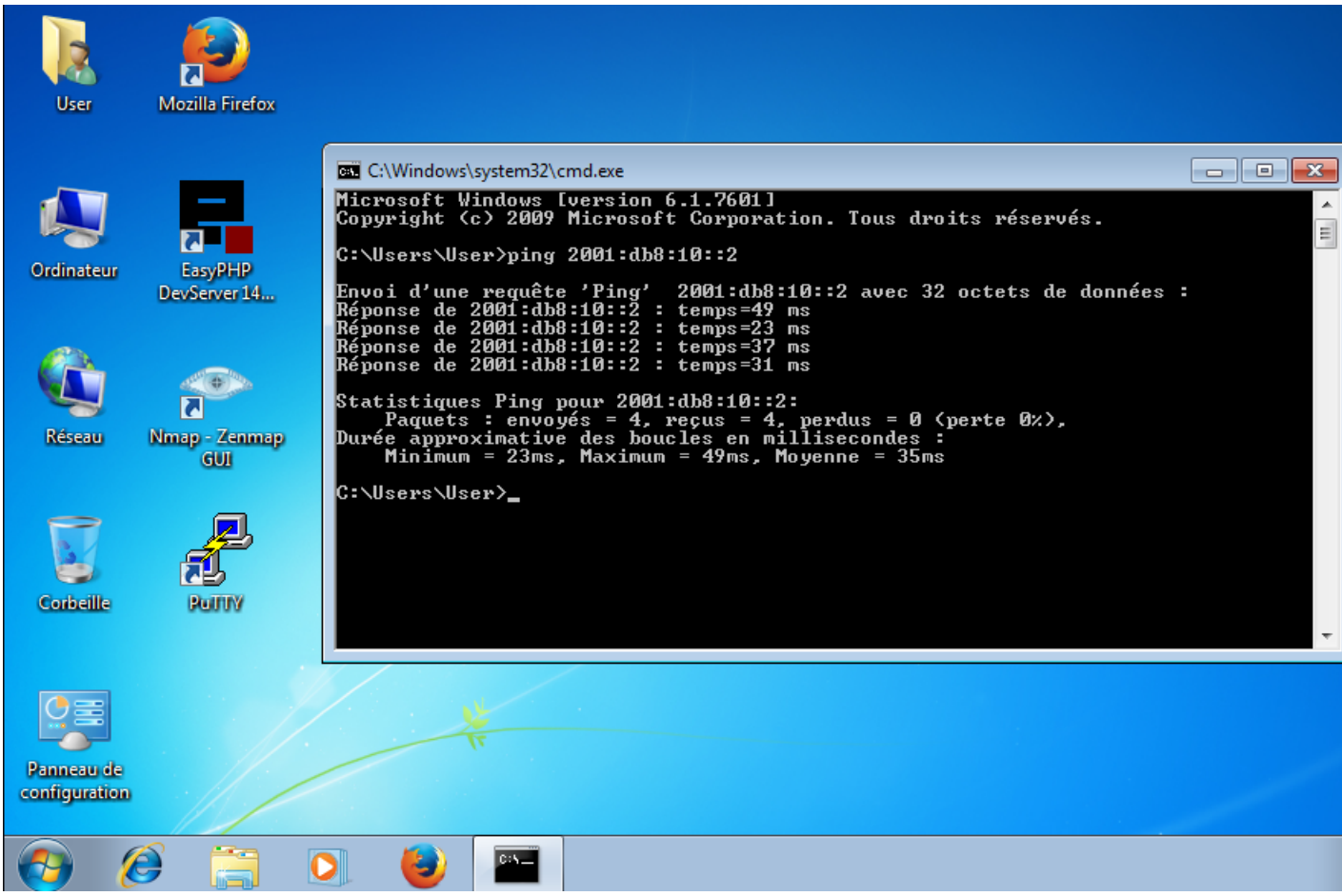


FIGURE IV.17 – Connexion réussi entre les deux hotes.

Conclusion général

Migrer d'IPv4 à IPv6 en un instant est impossible en raison de la taille énorme de l'Internet et du grand nombre d'utilisateurs d'IPv4. De plus, de nombreuses organisations dépendent de plus en plus d'Internet pour leur travail quotidien, et elles ne peuvent donc pas tolérer de temps d'arrêt pour le le remplacement du protocole IP. Par conséquent, Il n'y aura donc pas de jour particulier où IPv4 sera désactivé. Les deux protocoles peuvent coexister sans problème. sans aucun problème.

Acronymes

IPv6 : Internet protocole version 6
IPv4 : Internet protocole version 4
FAI : Fournisseur d'accès à Internet
NAT : Network Address translation
GUA : Global Unicast Address
LLA : Link-Local Address
RFC : Request for Comments
IETF : Internet Engineering Task Force
ICANN : (Internet Committee for Assigned Names and Numbers)
IANA : Internet Assigned Numbers Authority
ID : Identifiant
SLAAC : StateLess Address Auto Configuration
DHCP :Dynamic Host Configuration Pool
DHCPv6 :Dynamic Host Configuration Protocol version 6
EUI : Extended Unique Identifier
MAC : Media Access Control
RA : Router advertisment
RS : Router sollicitation
ICMP : Internet Control Message Protocol
ICMPv6 : Internet Control Message Protocol version 6
DNS : Domain name server
IEEE : Institute of Electrical and Electronics Engineers
OUI : Identifiant unique d'entité
R : Router
(DAD : Duplicate address detection
IP : Internet Protocol
TCP/IP : Transmission Control Protocol / Internet Protocol
ARP : Address Resolution Protocole
IOS : Internetwork Operating System
LAN : Local Area Network
OSPF Open Shortest Path First
NA : Neighbor Advertisment
NS : Neighbor Sollicitation
VPN : virtual private network
URL : Uniform Resource Locator
IPS : Intrusion prevention system
TTL : Time To Live
ISO : International Organization for Standardization
RTT : Round Trip Time
IGMP : Internet Group Management Protocol
OOB : Out Of Band
IRDP : ICMP Router Discovery Protocol
BGP : Border Gateway Protocol
RAM : Random Access Memory
VOIP : Voice over IP
QOS : Quality of service
CPU : Central Processing Unit
DMZ : demilitarized zone
SQL : Structured Query Language
P2P : Poste à Poste
SNMP : Simple Network Management Protocole
DOS : denial-of-service
DDOS : distributed denial-of-service

CSI : Computer Security Institute
IRC : Internet Chats Relais
NDP : Neighbor Discovery Protocol
MTU : Maximum Transmission Unit
MLD : Multicast Listener Discovery
MRD : Multicast Router Discovery
NIQ : Node Information Query
SEND : Secure Neighbor Discovery
UDP : User Datagram Protocol
CBAC : Context-Based Access Control
RR : resource record
AGL : Application Level Gateways
NIDS : Network Intrusion Detection System
NAPT-PT : Network Address Port Translation-Protocol Translation
NAT-PT : User Datagram Protocol
CSA : Cisco Security
GPO : Group Policy Object

Bibliographie

[1] CISCO,CCNA,*Introduction to Network*,Edition 7,année 2021

[2] Cédric Llorens,Laurent Levier,Denis Valois,Benjamin Morin, *Tabeaux de bord de la sécurité réseau*,EDITIONS EYROLLES 61,bd Saint-GERMAIN 75240 Paris cedex 05 www.editions-eyrolles.com.

[3] Eric Vyncke,*IPv6 Security,Scott Hogg, CCIE No. 5133*,Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

[4] Silvia Hagen,*IPv6 Essentials,Third Edition*,Printed in the United States of America.Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

[5] Rick Graziani,*IPv6 Fundamentals,Second Edition*,Straightforward Approach to Understanding IPv6,Cisco Press 800 East 96th Street Indianapolis, IN 46240.

[6] Bob Vachon,*CCNA Security Portable Command Guide,210-260*,Published by :Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.

[7] Prabhu Thiruvasagam and K. Jijo George,*Journal of ICT standardization*,NEC India Private Limited, India.Received 02 December 2018 ; Accepted 06 January 2019.

[8] Chen Su , Renjie Liu ,Xing Li,*Department of Electronic Engineering, Tsinghua University Beijing, China*,2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC 2019).

[9] Hrithik Goyal,Ravi Kumar*School of Electronics Engineering (SENSE) Vellore Institute of Technology Vellore, India*2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN).

[10] Ashis Saklani1 , S. C. Dimri2 *Department of Computer Science, H.N.B Garhwal Central University, Srinagar Garhwal, Uttarakhand, India* International Journal of Science and Research (IJSR), India Online ISSN : 2319-7064 .