RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ A. MIRA-BEJAIA

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

FACULTÉ DES SCIENCES EXACTES

DÉPARTEMENT D'INFORMATIQUE

MÈMOIRE

EN VUE DE L'OBTENTION DU DIPLÔME DE

MASTER PROFESSIONNEL

Domaine : Mathématiques et Informatique **Filière :** Informatique

Spécialité : Administration et Sécurité des Réseaux

Présenté par

Mlle. AYOUZ Selma

Mlle. BOUBADRA Melissa

Thème

Amélioration du réseau de Sonelgaz via la migration IPv4-IPv6 : Étude de cas et implémentation

Soutenu le 03 Juillet 2024. **Devant le jury composé de :**

Nom et Prénom	Grade		
M. AMROUN Kamal	Professeur	Université de Béjaia	Président
M. MOKTEFI Mohand	MCB	Université de Béjaia	Raporteur
Mlle. HOUHA Amel	MAA	Université de Béjaia	Examinatrice

Année Universitaire : 2023/2024

⁕ Remerciements ⁕

Ce travail a été réalisé au sein du département Informatique, à l'Université Abderrehamne Mira campus Targua Ouzmour, Béjaia.

On aimerait en premier lieu remercier Dieu qui nous a donné la volonté et le courage pour la réalisation de ce travail.

On tiens à remercier tout d'abord notre encadrant M. Moktefi Mohand, grâce à qui on a appris beaucoup de choses au cours de la réalisation de ce travail, pour la proposition du thème de ce mémoire ainsi que sa présence et son enseignement, sa critique et ses conseils nous ont été précieux.

Nous souhaitons aussi exprimer nos sincéres remerciements á notre encadrant, M. Idri Bachir, au sein de l'Entreprise Nationale SONELGAZ. Sa présence, son enseignement et son suivi tout au long de ce travail ont été d'une valeur inestimable pour nous.

On voudrait également remercier les membres du jury d'avoir accepter d'évaluer ce travail et pour toutes leurs remarques et critiques, ainsi que tous ceux qui nous ont enseigné durant toutes nos études, en particulier nos enseignants des deux années de Master.

On tient à remercier également le personnel administratif du département Informatique de l'université de Béjaia.

Enfin on adresse nos sincères remerciement à nos parents, nos frères et nos soeurs, nos amis et à tous ceux qui ont contribué de prés ou de loin à l'élaboration de ce travail.

⁕ *Dédicaces* ⁕

Je dédie ce travail :

Á mes parents, qui ont illuminé mon chemin tout au long de ma vie , pour leur soutien indéfectible et leurs encouragements constants. Que ce travail soit le témoignage de ma profonde reconnaissance envers eux.

Á mes sœurs, d'une valeur inestimable pour moi, ainsi qu'á mon unique et cher petit frère. Vous m'avez chaleureusement soutenue et aidée, partageant avec moi chaque moment émotionnel lors de la réalisation de ce modeste travail. Je vous serai éternellement reconnaissante.

À mes amies, qui ont fait preuve d'une disponibilité sans faille, en particulier á mon cher ami depuis le lycée. Merci du fond du cœur á tous.

Á mes camarades de la promotion 2019-2024, spécialement á ma binome qui est mon amie, á qui je souhaite un immense succés dans leurs parcours et leurs vies futures.

Ayouz Selma

⁕ *Dédicaces* ⁕

Je dédie ce travail :

Á mes chers parents,

Aucune dédicace ne pourrait pleinement exprimer l'amour profond, la gratitude immense et le respect sincère que je vous porte. Aujourd'hui, je tiens à vous exprimer ma plus profonde reconnaissance pour votre soutien inébranlable et vos encouragements constants tout au long de mon parcours académique. Grâce à vous, j'ai surmonté les défis et persévéré dans la réalisation de mes rêves. Ce travail est le fruit de votre dévouement et de vos sacrifices, pour lesquels je vous serai éternellement reconnaissante.

Á mes chers frères et ma précieuse sœur,

Mes bras forts et mon cœur tendre. Chaque jour passé avec vous est un cadeau précieux que je chérirai toujours.

Á mon fiancé,

Mon pilier à travers les hauts et les bas de mon parcours. tu es mon compagnon de route le plus précieux.

Ámes amies et camarades de la promotion 2019-2024 ,

spécialement á ma binome qui est bien plus qu'une partenaire académique mais une amie précieuse, á qui je souhaite un immense succés dans leurs parcours et leurs vies futures.

BOUBADRA Melissa

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

Liste des acronymes

ACK Acknowledgment

ACL Access Control List

ALG Application Layer Gateway

ARP Address Resolution Protocol

CDB Concession de Distribution Bejaïa

CIDR Classless Inter-Domain Routing

DAD Duplicate Address Detection

DHCPv6 Dynamic Host Configuration Protocol version 6

DMZ Demilitarized Zone

DNS Domain Name System

DoS Denial of Service

DTP Dynamic Trunking Protocol

EIGRP Enhanced Interior Gateway Routing Protocol

EUI Extended Unique Identifier

FTP File Transfer Protocol

GRE Generic Routing Encapsulation

GNS3 Graphical Network Simulator-3

GUA Global Unicast Address

HSRP Hot Standby Router Protocol

HTTP HyperText Transfer Protocol

ICANN Internet Corporation for Assigned Names and Numbers

IANA Internet Assigned Numbers Authority

ICMP Internet Control Message Protocol

IDS/IPS Intrusion Detection System/Intrusion Prevention System

IAX Inter-Asterisk eXchange

IRDP Internet Router Discovery Protocol

IoT Internet of Things

IPSec Internet Protocol Security

ISATAP Intra-Site Automatic Tunnel Addressing Protocol

ISO International Organization for Standardization

LAN Local Area Network

LLA Link-Local Address

MITM Man-in-the-Middle

NAT Network Address Translation

NAT-PT Network Address Translation - Protocol Translation

NDP Neighbor Discovery Protocol

NS Neighbor Solicitation

OSI Open Systems Interconnection

OSPF Open Shortest Path First

PPTP Point-to-Point Tunneling Protocol

QoS Quality of Service

RA Router Advertisement

RFC Request for Comments

RIPng Routing Information Protocol next generation

RS Router Solicitation

SIP Session Initiation Protocol

SIIT Stateless IP/ICMP Translation

SLAAC Stateless Address Autoconfiguration

SMTP Simple Mail Transfer Protocol

SSH Secure Shell

SYN Synchronize

TCP Transmission Control Protocol

TTL Time To Live

TLS Transport Layer Security

UDP User Datagram Protocol

VPN Virtual Private Network

VoIP Voice over IP

WAN Wide Area Network

INTRODUCTION GÉNÉRALE

Au cours des trois derniers siècles, les avancées technologiques ont profondément transformé notre monde. Le XVIIIe siècle a vu l'émergence des grands systèmes mécaniques issus de la révolution industrielle. Le XIXe siècle a été marqué par des innovations telles que la locomotive à vapeur, symbole de l'essor de l'industrialisation. Le XXe siècle, quant à lui, a été dominé par la collecte, le traitement et la distribution de l'information, avec des développements significatifs comme les réseaux téléphoniques mondiaux, la radio, la télévision, l'essor de l'industrie informatique, les communications par satellite et l'émergence d'Internet.

Cependant, avec les progrès technologiques rapides du XXIe siècle, les domaines de la collecte, du transport, du stockage et du traitement de l'information convergent rapidement, effaçant progressivement les frontières entre ces activités. Cette transformation a également impacté l'industrie informatique, qui a connu des avancées spectaculaires en peu de temps. Les ordinateurs, autrefois centralisés, sont désormais omniprésents et connectés, offrant des capacités de traitement sans précédent.

Un défi majeur émerge dans ce contexte de transformation : la pénurie d'adresses IPv4. Ce problème critique, dû à l'explosion du nombre de dispositifs connectés, a incité ingénieurs et chercheurs à développer une nouvelle version du protocole Internet, IPv6, pour surmonter les limitations d'IPv4 et répondre aux besoins croissants d'adressage IP. IPv6 offre une solution plus évolutive et résiliente, ouvrant la voie à un Internet capable de soutenir une croissance continue.

Ce mémoire se propose d'explorer en profondeur les différences entre IPv4 et IPv6 et de mettre en lumière les défis et les solutions liés à la migration vers IPv6.

Le premier chapitre sera consacré à l'adressage IPv4 et IPv6, en examinant les caractéristiques et les limites de chaque protocole. Nous y analyserons les problèmes rencontrés avec IPv4, notamment la pénurie d'adresses IP et les limitations de son format d'en-tête, ainsi que les avantages offerts par IPv6 pour résoudre ces défis.

Dans le deuxième chapitre, nous aborderons les mécanismes de transition de IPv4 vers IPv6. Nous examinerons les différentes stratégies et techniques permettant de faciliter cette transition, tout en assurant la continuité et la compatibilité des services existants.

Le troisième chapitre, qui constitue le cœur de notre étude, présentera une étude préalable et le contexte de travail, basé sur un rapport de stage réalisé à Sonelgaz. Nous y décrirons comment la transition vers IPv6 peut être appliquée au réseau informatique de Sonelgaz, en mettant en œuvre des règles de sécurité adaptées. Ce chapitre détaillera les étapes pratiques de la migration, les défis rencontrés et les solutions adoptées pour garantir une transition efficace et sécurisée.

Ainsi, ce mémoire vise à fournir une compréhension approfondie des enjeux liés à l'épuisement des adresses IPv4 et à démontrer comment la migration vers IPv6 constitue une réponse nécessaire et efficace pour assurer la continuité et la croissance de l'Internet, illustrée par une application pratique chez Sonelgaz.

CHAPITRE

1

ADRESSAGE ET SÉCURITÉ

1.1 Introduction

Dans ce chapitre, il y a deux parties distinctes. Dans la première partie nous nous pencherons sur les mécanismes d'adressage utilisés dans les réseaux informatiques, en mettant l'accent sur les protocoles IPv4 et IPv6. Nous explorerons les caractéristiques et les structures de ces deux types d'adressage, leurs avantages respectifs, ainsi que les défis associés à leur mise en œuvre et leur gestion. De plus, nous examinerons les raisons qui ont conduit à la transition progressive de l'IPv4 vers l'IPv6 et les implications de cette transition pour les infrastructures réseaux actuelles et futures.

Alors que IPv6 apporte des améliorations significatives en termes d'efficacité, de fonctionnalités et de performances, il introduit également de nouvelles vulnérabilités et des défis uniques en matière de sécurité. Ce qui nous amène à la deuxième partie de ce chapitre qui se concentre sur une analyse approfondie des enjeux de sécurité liés à IPv6, en mettant en évidence les défis spécifiques, les meilleures pratiques et les stratégies de sécurisation des réseaux IPv6. Nous examinerons en détail les attaques possible associées à IPv6, les protocoles spécifiques d'IPv6, ainsi que les vulnérabilités inhérentes à ce protocole. Nous aborderons également les méthodes recommandées pour atténuer ces risques de sécurité. De plus, nous discuterons des technologies de sécurité spécifiques à IPv6, notamment les pare-feu et les VPNs, et nous explorerons les mécanismes de surveillance et de détection des intrusions adaptés à l'environnement IPv6.

1.2 Modèle TCP/IP

Le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) est une suite de protocoles de communication utilisés pour interconnecter les périphériques réseaux sur Internet, développé originellement par le ministère de la Défense américaine en 1981, propose l'évolution de concepts déjà utilisés en partie pour le réseau historique ARPAnet (1972), et est employé en très forte proportion sur le réseau internet. Au-delà de son aspect historique, TCP/IP doit aussi son succès à son indépendance vis-à-vis de tout constructrice informatique [28].
TCP/IP spécifie la manière dont les données sont échangées sur Internet en fournissant des communications de bout en bout qui identifient la manière dont elles doivent être divisées en paquets, adressées, transmises, acheminées et reçues à la destination [31].

1.2.1 Couches du modèle TCP/IP

1. **Couche d'application** : Représente la couche supérieure, fournis aux applications un échange de données standardisé. Un grand nombre de protocoles divers de haut niveau permettent d'assurer les services de cette couche :
   — **Telnet** : Ouverture de session à distance .
   — **File Transfer Protocol (FTP)** : Protocole de transfert de fichiers .
   — **HyperText Transfer Protocol (HTTP)** : Protocole de transfert de l'hypertexte .
   — **Simple Mail Transfer Protocol (SMTP)** : Protocole simple de transfert de courrier.
   — **Domain Name System (DNS)** : Système de nom de domaine .
2. **Couche de transport** : Responsable du maintien des communications de bout en bout sur le réseau. Les deux principaux protocoles pouvant assurer les services de cette couche sont les suivants :
   — **Transmission Control Protocol (TCP)** : Est un protocole fiable, assurant une communication sans erreur par un mécanisme question /réponse /confirmation /synchronisation (orienté connexion) .
   — **User Datagram Protocol (UDP)** : Est un protocole non-fiable, assurant une communication rapide mais pouvant contenir des erreurs en utilisant un mécanisme question/réponse (sans connexion).
3. **Couche Internet/couche réseau** : S'occupe de l'acheminement à destination. Des paquets de données indépendamment les uns des autres, soit donc de leur routage à travers les différents nœuds par rapport au trafic et à la congestion du réseau.

   Les protocoles de couche réseau sont :
   — **Le protocole IP** : Assure intégralement les services de cette couche, et constitue donc

l'un des points-clefs du modèle TCP/IP. Le format et la structure des paquets IP sont précisément définis.

— **Internet Control Message Protocol (ICMP)** : Est un protocole de rapport d'erreurs utilisé par les périphériques réseau tels que les routeurs.

4. **Couche hôte-réseau** : Intègre les services des couches physiques et prend en charge la communication avec l'interface physique afin de transmettre ou de récupérer les paquets de données qui lui sont transmis de la couche supérieure.

1.3 Protocole IP

Le protocole IP (Internet Protocol), assure le service attendu de la couche réseau du modèle TCP/IP. Son rôle est donc de gérer l'acheminement des paquets (issus de la couche transport) entre les nœuds de manière totalement indépendante, même dans le cas où les paquets ont les mêmes nœuds source et destination. Ce protocole offre un fonctionnement non-fiable et sans connexion.

1.3.1 Protocole IP version 4 (IPv4)

La première version d'internet Protocol (IP) largement déployée est appelée IPv4 (Internet Protocole Version 4 avec la valeur 4 pour le numéro de version), il a été créé dans les années 70, et mis en application en 1980. Les adresses IPv4 sont codées sur 32 bits ce qui permet d'attribuer environ 4.3 milliards d'adresses. Elles sont sous la forme de quatre chiffres compris entre 0 et 255. Une adresse IPv4 est constituée d'une partie réseau identifiant le réseau et d'une partie hôte désignant l'interface correspondante [15].

Datagramme IPv4

Un datagramme IP, aussi appelé paquet IP lorsqu'il est fragmenté, correspond aux données émises de la couche supérieure (généralement issues du protocole TCP ou UDP) encapsulées dans une trame.

Comme on peut le voir dans la Figure suivante, un paquet IP comprend un ensemble de champs où chacun a une fonctionnalité bien déterminée.

— **Version (4)** : C'est un champ codé sur 4 bits et représente la version du protocole IP.

— **Header Length (IHL)** : Dans l'en-tête IPv4 est utilisé pour indiquer la longueur totale de l'en-tête IP en mots de 32 bits. Ce champ est stocké sur 4 bits et permet de déterminer la taille de l'en-tête IP, qui peut varier en fonction des options ajoutées. La valeur maximale possible est de 15, ce qui correspond à une longueur totale de 60 octets.

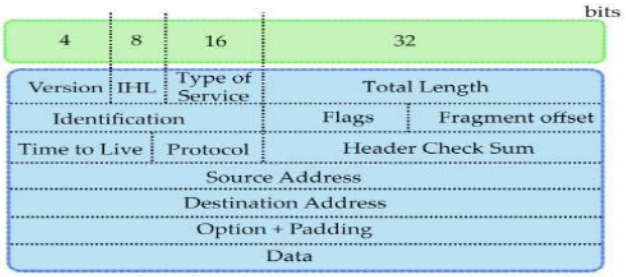

FIGURE 1.1 – En-tête IPv4.

— **Type of service** : C'est un champ codé sur 8 bits. Il est utilisé pour des raisons de qualité de service. Il stipule comment la couche transport aimerait voir ses datagrammes traités et assigne un degré d'importance différent à chacun d'entre eux.

— **Total length** : C'est un champ codé sur 16 bits qui représente la longueur totale du paquet en octets (en-tête + donnée.).

— **Identification** : C'est un champ codé sur 16 bits, contient un entier qui identifie le datagramme actuel. Ce champ est spécifié par l'émetteur afin d'aider le récepteur à réassembler les fragments de datagrammes.

— **Flag** : C'est un champ codé sur 3 bits dont les deux bits de poids faible contrôlent la fragmentation.

— **Fragment offset** : C'est un champ codé sur 13 bits et qui indique la position du fragment dans le datagramme original. Cela permet au processus IP destinataire de reconstruire le datagramme correctement.

— **Time to live (TTL**) : C'est un champ codé sur 8 bits et qui indique la durée de vie maximale d'un paquet. Cette valeur est décrémentée d'un ''1'' à chaque fois qu'un paquet transite par un routeur. Ceci évite ainsi que le paquet ne circule en boucle à l'infini.

— **Protocol** : C'est un champ codé sur 8 bits qui représente le protocole de couche transport auquel le paquet doit être transmis une fois arrivé à destination.

— **Checksum** : C'est un champ codé sur 16 bits qui représente le code détecteur d'erreurs, ce qui permet de vérifier l'intégrité du paquet.

— **Source (32bits) /Destination (32 bits) adresses** : Adresse IPv4 des hôtes émettrices et destinatrices du paquet.

— **Option** : Il est possible de positionner des options avant le champ de données. Ce champ permet au protocole IP de supporter différentes options.

— **Data** : Ce champ représente les données [15].

Fragmentation

La fragmentation est un processus de l'Internet Protocol (IP) qui permet de diviser un paquet IP en plusieurs fragments plus petits pour qu'ils puissent passer par des liens avec une unité de transmission maximale (MTU) plus petite que la taille du paquet original. Les fragments sont ensuite reassemblés par l'hôte de réception.

Si la MTU d'un réseau est suffisamment grande pour accepter le datagramme ou le fragment, ce dernier sera encapsulé sans être fragmenté. Le ré-assemblage des fragments s'opère quoi qu'il arrive au niveau du nœud destination, et jamais au niveau des routeurs intermédiaires, même si les réseaux traversés autoriseraient des fragments plus grands.

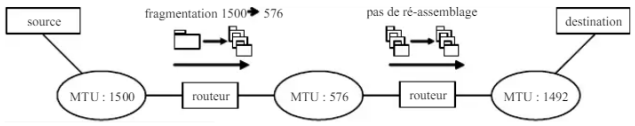

FIGURE 1.2 – Fragmentation de datagramme.

À l'arrivée du premier fragment d'un datagramme, le nœud destinataire active un compte à rebours, utilisé conjointement avec le champ TTL de chaque fragment, qui détermine ainsi le délai laissé à tous les autres fragments pour arriver. Si ce délai arrive à expiration, les fragments reçus sont néanmoins détruits et le datagramme n'est donc pas traité. De plus, un message ICMP est envoyé à l'émetteur pour lui transmettre l'erreur de transmission [15].

Adressage IPv4

— Une adresse IPv4 est une identification unique pour un hôte sur un réseau IP.

— Une adresse IP est de 32 bits, représentés par 4 valeurs décimales pointées chacune a un poids de 8 bits (1 octet) prenant des valeurs décimales de 0 à 255 séparées par des points. La notation est aussi connue sous le nom de "décimale pointée".

Identification de la classe d'adresse

À l'origine d'IPv4, on distingue une organisation en classes d'adresses dont les quatre premiers bits indiquent la classe (RFC 791).

— Les adresses de **Classe A** commencent par 0xxx en binaire, ou 0 à 127 en décimal.

— Les adresses de **Classe B** commencent par 10xx en binaire, ou 128 à 191 en décimal.

— Les adresses de **Classe C** commencent par 110x en binaire, ou 192 à 223 en décimal.

— Les adresses de **Classe D** commencent par 1110 en binaire, ou 224 à 239 en décimal.

— Les adresses de **Classe E** commencent par 1111 en binaire, ou 240 à 255 en décimal

Notes sur les Classes d'adresses

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

Adresses spécifiques

- Les adresses commençant de 127.0.0.0 à 127.255.255.255 sont réservées pour le **bouclage (loopback)**.
- Adresses privées non routables vers l'Internet (RFC 1918) :
  - Pour la **classe A** : de 10.0.0.0 à 10.255.255.255
  - Pour la **classe B** : de 172.16.0.0 à 172.31.255.255
  - Pour la **classe C** : de 192.168.0.0 à 192.168.255.255

Distinction de la partie réseau de la partie hôte

- La partie réseau des adresses de Classe A portera sur le premier octet et la partie hôte sur les trois derniers $2^{24} = 16\,777\,216$ hôtes possibles par réseau).
- La partie réseau des adresses de Classe B portera sur les deux premiers octets et la partie hôte sur les deux derniers $2^{16} = 65\,536$ hôtes possibles par réseau.
- La partie réseau des adresses de Classe C portera sur les trois premiers octets et la partie hôte sur le dernier $2^8 = 256$ hôtes possibles par réseau[4].

Type d'adresses IP

Les adresses IP permettent d'identifier de manière unique les hôtes d'origine et de destination. Les routeurs se chargent d'acheminer les paquets à travers les liaisons intermédiaires [4].

Il existe plusieurs types d'adresses qui correspondent à plusieurs usages.

On trouve trois grandes catégories :

- **les adresses Unicast** : à destination d'un seul hôte .
- **les adresses Broadcast** : à destination de tous les hôtes du réseau .
- **les adresses Multicast** : à destination de certains hôtes du réseau.

Limites d'IPv4

- **La pénurie d'adresse IP(2^{32} adresses)** : La population mondiale actuelle s'élève à environ 7,6 milliards. Cependant, IPv4 n'offre qu'environ 4 milliards d'adresses publiques. De plus, avec l'avènement de l'IoT ou de nombreux équipements (montres, voitures, lunettes, frigo...) sont connectés, on se rend très vite compte que le nombre d'adresses fourni par IPv4 est insuffisant.

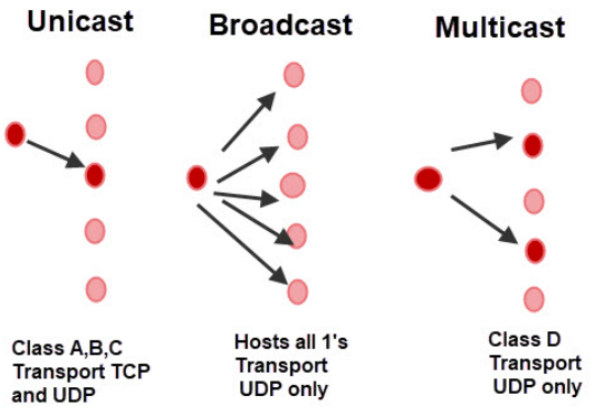

FIGURE 1.3 – Type d'adresses IP.

— **La croissance des tables de routage** : Plus on a d'adresses IP, plus le nombre de routes augmente, et cela consomme beaucoup de ressources au routeur.

— **Les difficultés pour les connexions de bout en bout** : L'adresse publique d'un hôte est partagée tandis que l'adresse privée est masquée, ce qui peut causer un problème de connectivité de bout en bout [29].

Modèle OSI (Open Systems Interconnection)

Le modèle de référence Open Systems Interconnection (OSI), développé par l'organisation Internationale de Normalisation (International Organization for Standardization (ISO)) en 1984, est un cadre de référence qui explique le processus de transmission de données entre ordinateurs. Il est divisé en sept couches, chacune permettant de communiquer avec celles qui sont directement au-dessus et en dessous d'elle (couches adjacentes). La couche inférieure fournit les services dont a besoin la couche actuelle, tandis que la couche actuelle fournit les services à la couche supérieure pour remplir sa fonction.

Une représentation graphique peut être employée pour clarifier ce concept d'échanges entre couches :

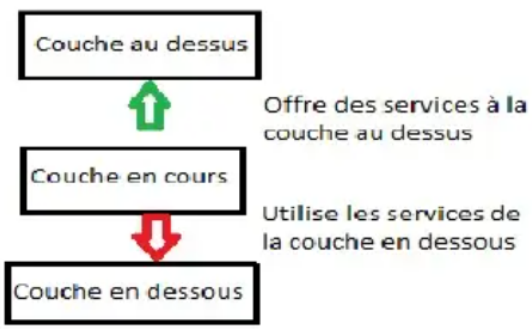

FIGURE 1.4 – Liaison entre les couches.

Couches du modèle OSI

1. **Couche physique** : C'est la couche la plus basse du modèle de référence OSI. Elle assure la réception des trames de données provenant de la couche de liaison de données et de leur transformation en une suite de bits qui seront ensuite transmis sur le support de communication. Cette couche offre également des services essentiels tels que la détection de collisions, le multiplexage et la modulation pour assurer un échange de données efficace et fiable.
2. **Couche de liaison de données (DLL)** : Responsable de la transmission du message d'un nœud à un autre. La fonction principale de cette couche est de garantir que le transfert de données sans erreur d'un nœud à un autre, elle offre des mécanismes de détection et de correction d'erreurs pour garantir l'intégrité des données lors de leur transmission. La couche liaison de données est divisée en deux sous-couches :
   — Contrôle de liaison logique (LLC).
   — Contrôle d'accès aux médias (MAC).
3. **Couche réseau** : Assure la transmission des données d'un hôte à l'autre situé dans différents réseaux. Il s'occupe également du routage des paquets , c'est-à-dire de la sélection du chemin le plus court pour transmettre le paquet, parmi le nombre de routes disponibles et en s'assurant que les paquets de données sont acheminés de manière efficace de l'émetteur au récepteur.
4. **Couche de transport** : Fournit des services à la couche application et prend les services de la couche réseau. Responsable de la livraison de bout en bout du message complet, fournit également un accusé de réception de la transmission réussie des données et retransmet les données si une erreur est détectée. Elle s'occupe également de ré-assembler le message à la réception des différentes parties. Les données de la couche de transport sont appelées Segments.
5. **Couche de session** : Responsable de l'établissement de la connexion, de la maintenance des sessions, de l'authentification et assure également la sécurité.
6. **Couche de présentation** : Également appelée couche de traduction, car elle effectue la conversion des fichiers d'un format codé en EBCDIC à un format ASCII si nécessaire afin de fournir à la couche application des données dans un format qu'elle peut comprendre.
7. **Couche d'application** : Fournit les services de base offerts par le réseau tels que le transfert de fichiers, la rédaction des e-mails, l'établissement de sessions à distance, la visualisation de pages web, etc. C'est là où l'utilisateur interagit directement avec le réseau.

Dans l'ensemble, le modèle OSI fournit une approche normalisée pour le développement et la mise en œuvre de protocoles de communication en réseau qui permettent d'améliorer l'interopérabilité

entre des systèmes de réseau hétérogènes.

1.3.2 Protocole IP version 6 (IPv6)

Formats d'adresse IPv6

Les adresses IPv6 sont des identifiants de 128 bits, elle est représentée en notation hexadécimale. Divisés en huit segments de 16 bits chacun, chaque quartet peut prendre une valeur comprise entre 0 (4 bits à ZÉRO) et F (4 bits à UN) séparés par des deux-points (:).

Format préféré

Le format préféré d'une adresse IPv6 est représenté par x :x :x :x :x :x :x :x, où chaque x correspond à une valeur en hexadécimale [19]. Pour simplifier la notation, deux règles sont appliquées :

1. **Omettre les zéros en début de segment** La première règle pour simplifier la notation des adresses IPv6 est de supprimer les zéros (0) au début d'une section de 16 bits. Voici quelques exemples illustrant cette règle :
   (a) **Adresse IPv6 complète :** 2001 :0db8 :0000 :0000 :0000 :0000 :1428 :57ab
   — **Adresse IPv6 réduite :** 2001 :db8 : :1428 :57ab
   (b) **Adresse IPv6 complète :** 2001 :0db8 :00a0 :0000 :0000 :00c0 :1a2f :1a2b
   — **Adresse IPv6 réduite :** 2001 :db8 :a0 : :c0 :1a2f :1a2b
2. **Double deux-points :** La deuxième règle consiste, l'utilisation du double deux-points (: :) en IPv6 stipule qu'une suite de deux fois deux points peut remplacer toute chaîne de zéros consécutifs dans une adresse IPv6. Cependant, cette notation ne peut être utilisée qu'une seule fois par adresse pour éviter toute ambiguïté. Si elle était utilisée plusieurs fois, cela pourrait conduire à des adresses IPv6 différentes. Voici un exemple :
   (a) **Adresse IPv6 complète :** 2001 :0db8 :3c4d :0015 :0000 :0000 :1a2f :1a2b
   — **Adresse IPv6 réduite :** 2001 :db8 :3c4d :15 : :1a2f :1a2b

Longueur de préfixe IPv6

— La longueur du préfixe IPv6 peut varier de 0 à 128 bits, avec une longueur standard de /64 pour les réseaux locaux et la plupart des autres réseaux. Cette notation représente la partie réseau de l'adresse IPv6.
— Pour indiquer la longueur du préfixe en bits, la notation Classless Inter-Domain Routing (CIDR) est utilisée, avec un slash (/) suivi du nombre de bits.

Par exemple, une adresse IPv6 avec un préfixe de 64 bits serait notée comme adresse-ipv6/64. Les préfixes IPv6 sont représentés avec la notation **adresse-ipv6/longueur-du-préfixe-en-bits**.

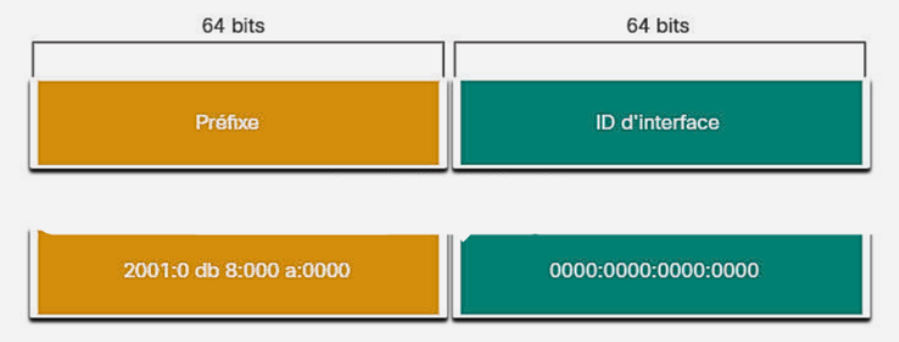

FIGURE 1.5 – Préfixe IPv6.

— La configuration automatique d'adresse sans état (Stateless Address Autoconfiguration (SLAAC)) utilise 64 bits pour l'ID d'interface. Il facilite également la création et la gestion des sous-réseaux.

Types d'adresses IPv6

Les premiers bits d'une adresse IPv6 définissent le type de cette adresse, et ces bits sont regroupés dans ce qu'on appelle "préfixe de format". Une adresse IPv6 unicast se compose de deux parties distinctes : le préfixe de l'adresse et l'identificateur de l'interface. Pour exprimer de manière concise cette combinaison, on utilise la notation suivante : **ipv6-address/prefix-length.** En fait, il existe trois grandes catégories d'adresses ipv6 :

1. **Adresse à diffusion unique (Mono-diffusion) :** Une adresse de mono-diffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique. Un paquet envoyé à une adresse de mono-diffusion 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 mono-diffusion. L'adresse IPv6 de destination peut quant à elle être une adresse de mono-diffusion ou de multidiffusion [4].

   Il existe six types d'adresse de mono-diffusion IPv6.

   — **Mono-diffusion Globale Global Unicast Address (GUA) :** Une adresse de mono-diffusion globale ressemble à une adresse IPv4 publique. Ces adresses sont uniques à travers le monde et peuvent être routées sur Internet. Elles peuvent être configurées de manière statique ou attribuées dynamiquement.

   — L'Internet Corporation for Assigned Names and Numbers (ICANN), opérateur de l'Internet Assigned Numbers Authority (IANA), attribue des blocs d'adresses IPv6 aux cinq organismes d'enregistrement Internet locaux. Actuellement, seules des adresses de mono-diffusion globale dont les premiers bits sont 001 ou 2000 : :/3 sont attribuées.

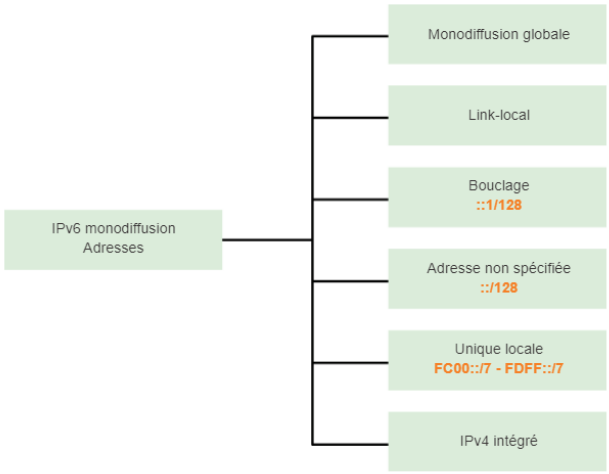

FIGURE 1.6 – Adresses mono-diffusion.

— **Lien local Link-Local Address (LLA) :** Les adresses de type lien-local sont employées pour l'échange de données avec d'autres équipements sur la même liaison locale. En IPv6, le concept de "lien" désigne un sous-réseau spécifique. Les adresses lien-local sont restreintes à une seule liaison et leur unicité est valide uniquement à l'intérieur de cette liaison, car elles ne sont pas routables au-delà de celle-ci. En conséquence, les routeurs ne dirigent aucun paquet comportant une adresse lien-local en tant qu'adresse source ou destination.

— **Bouclage :** L'adresse de bouclage est employée par un périphérique pour s'envoyer des paquets à lui-même. Contrairement à une adresse physique, elle ne peut être assignée à une interface matérielle. Tout comme avec une adresse de bouclage IPv4, une requête ping peut être envoyée à une adresse de bouclage IPv6 pour tester la configuration TCP/IP de l'hôte local. L'adresse de bouclage IPv6 est composée uniquement de zéros, à l'exception du dernier bit, et est représentée par : :1/128, ou simplement : :1 en format compressé.

— **Adresse non spécifiée :** Une adresse non spécifiée est une adresse composée exclusivement de zéros, représentée par : :/128 ou simplement : : en format compressé. Elle ne peut être assignée à une interface et est réservée pour être utilisée uniquement comme adresse source dans un paquet IPv6. Cette adresse est employée lorsque le périphérique n'a pas encore obtenu d'adresse IPv6 permanente ou lorsque l'adresse source du paquet n'est pas critique pour la destination.

— **Adresse locale unique :** Les adresses IPv6 locales uniques présentent des similitudes avec les adresses privées Request for Comments (RFC) 1918 de l'IPv4, mais elles se distinguent également sur certains aspects. Utilisées pour l'adressage local à l'intérieur d'un site ou entre un nombre restreint de sites. Ces adresses ne sont pas conçues pour être routées sur Internet. Elles sont définies dans la plage comprise entre FC00 : :/7 et FDFF : :/7.

— **IPv4 intégré :** Le dernier type d'adresse de mono-diffusion est l'adresse IPv4 intégrée. Ces

adresses sont utilisées pour faciliter la transition de l'IPv4 vers l'IPv6.

2. **Adresses de multidiffusion (Multicast) :** Les adresses de multidiffusion servent à identifier un ensemble d'interfaces, souvent situées sur des nœuds différents. Lorsqu'un paquet est envoyé à cette adresse, il est distribué à toutes les interfaces identifiées par cette adresse. Ces adresses remplacent les adresses de diffusion IPv4.
3. **Adresses anycast :** Les adresses anycast sont utilisées pour identifier un ensemble d'interfaces, généralement sur des nœuds distincts. Lorsqu'un paquet est envoyé à cette adresse, il est distribué uniquement à l'interface la plus proche, déterminée par les métriques de routage. Contrairement aux adresses de multidiffusion, les adresses anycast sont tirées de l'espace d'adressage de mono-diffusion et ne peuvent être différenciées par leur syntaxe. La distinction entre les adresses de mono-diffusion et les adresses anycast est réalisée au niveau de la configuration de l'interface concernée.

Structure de Global Unicast Adress IPv6 (GUA)

La structure d'une adresse IPv6 Global Unicast Address (GUA) est composée de trois parties distinctes :

Préfixe de routage global

Ce préfixe est attribué par un fournisseur, tel qu'un ISP ou FAI, à un client ou à un site. Actuellement, les RIR attribuent un préfixe de routage global de /48 aux clients, fournissant un espace d'adressage adéquat. Ce préfixe identifie le réseau ou le site.

Identifiant de sous-réseau

L'ID de sous-réseau est utilisé par une organisation pour identifier les sous-réseaux au sein de son site. Il est placé entre le préfixe de routage global et l'ID d'interface.

Identifiant d'interface

L'ID de l'interface IPv6 est similaire à la partie hôte d'une adresse IPv4. Chaque hôte peut avoir plusieurs interfaces, chacune ayant une ou plusieurs adresses IPv6. Il est recommandé d'utiliser des sous-réseaux /64, ce qui génère un ID de 64 bits.

Link-Local Address LLA

La plage d'adresses réservée aux adresses de LLA est définie dans le préfixe **fe80 : :/10**. Ces adresses sont générées automatiquement par les équipements IPv6 en l'absence d'autres méthodes

d'attribution d'adresse telles que la configuration manuelle ou l'utilisation de DHCPv6. Les LLAs sont destinées aux communications locales au sein d'un même segment de réseau, notamment pour la découverte des voisins, les protocoles de configuration automatique des adresses, et d'autres fonctions réseau qui ne requiert pas de connectivité externe.

Les méthodes d'obtention d'une LLA

Un périphérique peut obtenir une adresse de lien local IPv6 (LLA) de deux manières principales :

— **Configuration Statique :** Cette méthode implique la configuration manuelle de LLA sur le périphérique, généralement basé sur l'adresse MAC.

— **Configuration Dynamique :** Les routeurs génèrent automatiquement une adresse link-local IPv6 dès qu'une adresse de diffusion globale est attribuée. En utilisant la méthode Extended Unique Identifier (EUI)-64 par défaut, les routeurs calculent l'identifiant de l'interface pour ces adresses link-local.

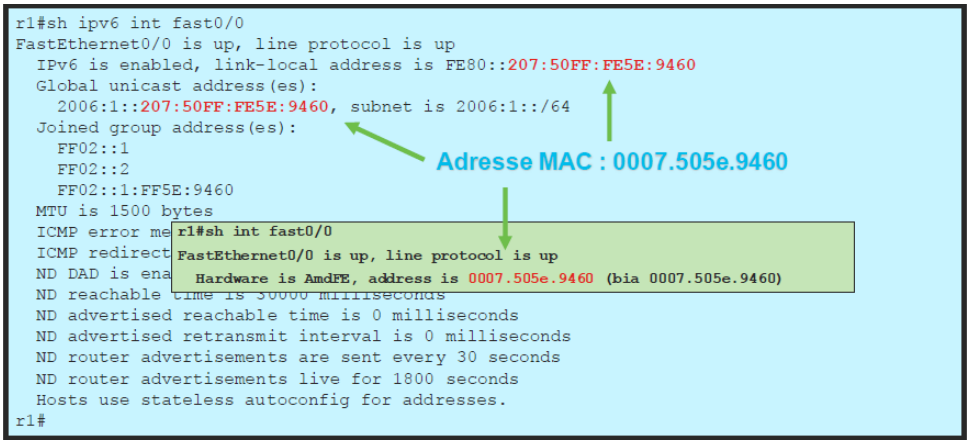

FIGURE 1.7 – Identifiant d'interface EUI-64.

— Bien que le DHCPv6 soit principalement utilisé pour la configuration des adresses IPv6 globales, il peut également être utilisé pour distribuer des informations supplémentaires, y compris des adresses de lien local. Dans ce cas, le serveur DHCPv6 peut attribuer une adresse de lien local à un périphérique en réponse à une demande DHCPv6.

En-tête IPv6

Les champs d'en-tête de paquet IPv6 incluent [4] :

— **Version** – contient une valeur binaire de 4 bits indiquant la version du paquet IP. Pour les paquets IPv6, ce champ est toujours 0110.

— **Classe de trafic** – ce champ de 8 bits est équivalent au champ de services différenciés pour l'IPv4. Il contient également une valeur de 6 bits utilisée pour classer les paquets, et une valeur de notification explicite de congestion de 2 bits utilisée pour contrôler l'encombrement.

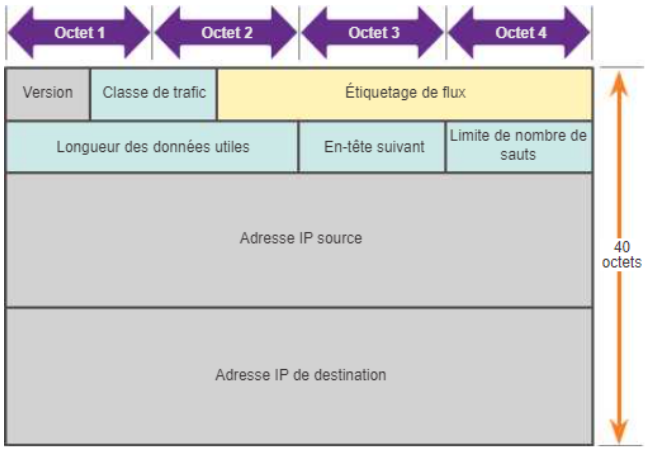

FIGURE 1.8 – En-tête IPv6.

— **Étiquetage de flux** – ce champ de 20 bits fournit un service spécifique pour les applications en temps réel. Ce champ peut être utilisé pour indiquer aux routeurs et aux commutateurs de conserver le même chemin pour le flux de paquets, de telle sorte que l'ordre des paquets ne soit pas modifié.

— **Longueur des données utiles** – ce champ de 16 bits est équivalent au champ de longueur totale de l'en-tête IPv4. Il définit la taille globale du paquet (fragment), y compris l'en-tête et les extensions facultatives.

— **En-tête suivant** – ce champ de 8 bits est équivalent au champ de protocole de l'IPv4. Il indique le type de données utiles transportées par le paquet, permettant ainsi à la couche réseau de transmettre les données au protocole de couche supérieure approprié. Ce champ est également utilisé s'il existe des en-têtes d'extension ajoutés au paquet IPv6.

— **Limite de nombre de sauts** – ce champ de 8 bits remplace le champ de durée de vie (Time To Live (TTL)) de l'IPv4. Cette valeur est réduite à chaque fois qu'un routeur transmet le paquet. Lorsque le compteur atteint 0, le paquet est rejeté et un message ICMPv6 est transféré à l'hôte émetteur, indiquant que le paquet n'a pas atteint sa destination.

— **Adresse source** – ce champ de 128 bits identifie l'adresse IPv6 de l'hôte émetteur.

— **Adresse de destination** – ce champ de 128 bits indique l'adresse IPv6 de l'hôte récepteur.

Un paquet IPv6 peut contenir des en-têtes d'extension, qui offrent des informations supplémentaires de couche réseau. Ces en-têtes sont facultatifs et sont insérés entre l'en-tête IPv6 et les données réelles du paquet. Ils servent à différentes fonctions telles que la fragmentation, la sécurité, le support de la mobilité, entre autres.

En-têtes IPv6 d'extension

Les en-têtes d'extension IPv6 sont des structures de données facultatives qui peuvent être ajoutées aux datagrammes IPv6 pour fournir des fonctionnalités supplémentaires au protocole. Contraire-

ment à l'en-tête principal IPv6, qui est obligatoire pour chaque datagramme, les en-têtes d'extension sont facultatifs et peuvent être inclus ou omis en fonction des besoins spécifiques de la communication [16].

Il existe plusieurs types d'en-têtes d'extension IPv6, chacun offrant des fonctionnalités différentes pour répondre à divers besoins de communication. Voici quelques-uns des en-têtes d'extension IPv6 les plus courants :

1. **En-tête d'extension Hop-by-Hop :** Cet en-tête est utilisé pour spécifier les options de traitement qui doivent être examinées par chaque nœud sur le chemin du datagramme. Il est généralement utilisé pour des options telles que le marquage de paquets ou la définition de politiques de routage.
2. **En-tête d'extension Routage :** L'en-tête d'extension Routage est utilisé pour spécifier un chemin explicite que le datagramme doit suivre. Il peut également être utilisé pour spécifier plusieurs sauts intermédiaires à travers lesquels le datagramme doit être routé.
3. **En-tête de Fragmentation :** Cet en-tête est utilisé pour fragmenter un datagramme IPv6 en plusieurs fragments lorsqu'il est trop grand pour être transmis sur le réseau. Chaque fragment contient une partie des données d'origine, ainsi que des informations de contrôle permettant au destinataire de reconstituer le datagramme d'origine.
4. **En-tête de Destination Optionnelle :** Cet en-tête contient des options spécifiques à la destination, telles que des informations sur la qualité de service ou des paramètres de sécurité, qui ne sont pas nécessaires pour tous les nœuds sur le chemin du datagramme.

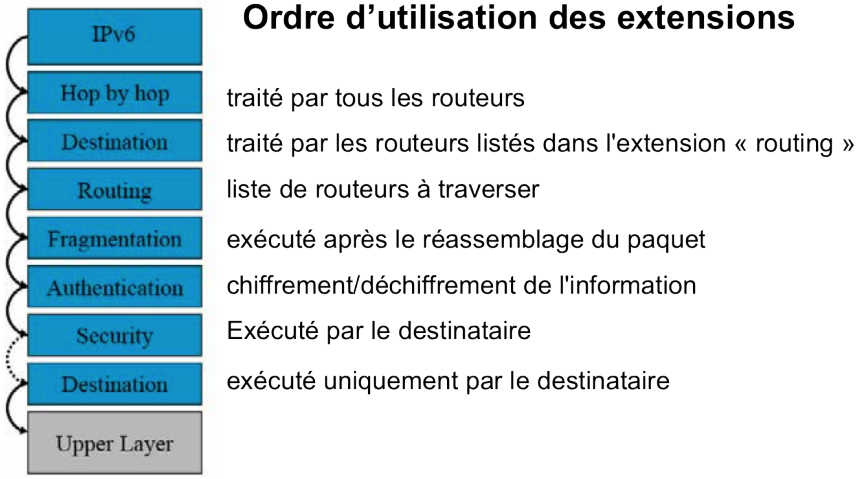

FIGURE 1.9 – Utilisation d'extensions en ordre.

Ces en-têtes d'extension permettent d'ajouter des fonctionnalités supplémentaires au protocole IPv6 tout en conservant une certaine flexibilité dans la manière dont les données sont transmises et traitées sur le réseau. Ils sont essentiels pour prendre en charge des fonctionnalités avancées telles que le routage dynamique, la qualité de service et la sécurité des communications IPv6.

Découverte du MTU

La découverte de la MTU dans IPv6, également appelée découverte de la MTU de chemin, est un processus dynamique permettant à un nœud de déterminer la taille maximale des paquets qu'il peut envoyer sans fragmentation sur un chemin de communication spécifique.

— Le processus commence par l'envoi de paquets IPv6 avec le bit de fragmentation "Don't Fragment" (DF) activé. Lorsque ces paquets rencontrent un routeur dont la MTU est inférieure à la taille du paquet, ce dernier ne peut être fragmenté et est donc rejeté. En réponse, le routeur envoie un message ICMPv6 de type "Packet too Big" à l'émetteur, indiquant la MTU maximale autorisée sur le chemin.

— L'émetteur ajuste alors la taille de ses paquets en conséquence pour garantir qu'ils ne dépassent pas la MTU maximale autorisée. Ce processus se poursuit jusqu'à ce que la taille des paquets envoyés par l'émetteur soit inférieure ou égale à la MTU maximale autorisée sur tout le chemin de communication.

La découverte de la MTU de chemin est un processus facultatif dans IPv6, mais elle est fortement recommandée pour garantir des performances optimales du réseau.

Remarque :

— Il convient de noter que les pare-feu peuvent parfois bloquer les messages ICMPv6 "paquet trop gros", ce qui peut entraîner des problèmes de connectivité. Afin de garantir une découverte précise de la MTU de chemin, il est conseillé de configurer les pare-feu pour autoriser ces messages, évitant ainsi les potentiels obstacles à une communication fluide et efficace sur les réseaux IPv6.

Comparaison des champs d'en-tête IPv6 et IPv4 : Changements, Suppressions et Ajouts

Dans l'en-tête IPv6, plusieurs champs ont été retirés par rapport à l'en-tête IPv4 :

— Longueur de l'en-tête ;

— Identification ;

— Drapeaux ;

— Décalage de fragment ;

— Somme de contrôle de l'en-tête.

Tandis que d'autres ont été ajoutés ou modifiés.

Tout d'abord, la longueur de l'en-tête a été supprimée en IPv6. Contrairement à IPv4 qui permet une longueur d'en-tête variable avec des options pouvant étendre cette longueur jusqu'à 60 octets, IPv6 a une longueur d'en-tête fixe de 40 octets. Ainsi, la spécification de la longueur totale de l'en-tête devient superflue en IPv6.

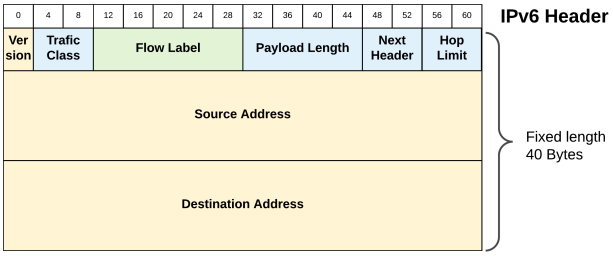

FIGURE 1.10 – En-tête IPv6.

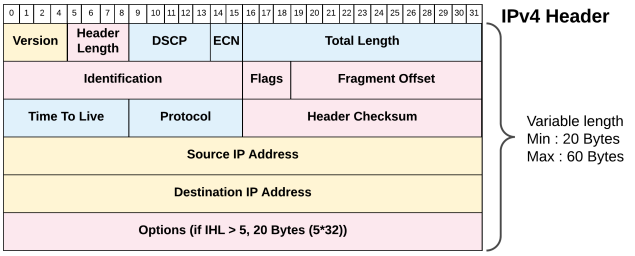

FIGURE 1.11 – En-tête IPv4.

Ensuite, les champs Identification, Drapeaux et Décalage de fragment ont été retirés en IPv6. Ces champs étaient utilisés pour gérer la fragmentation des paquets en IPv4. La fragmentation se produit lorsque des paquets doivent être envoyés sur un réseau ne supportant que des tailles de paquets plus petites. En IPv6, cette fonctionnalité est gérée différemment, l'hôte apprend la taille de l'unité de transmission maximale (MTU) du chemin à travers une procédure appelée découverte du MTU du chemin, qui a été définie dans le RFC 1981. Les routeurs IPv6 ne fournissent pas de fragmentation comme c'était le cas avec IPv4, mais renvoient un message ICMP avec "Paquet trop grand" au nœud source si nécessaire.

De plus, le champ Somme de contrôle de l'en-tête a été supprimé en IPv6 pour améliorer la vitesse de traitement. Cette vérification n'est plus nécessaire à ce niveau, car les risques d'erreurs non détectées ou de paquets mal acheminés sont considérablement réduits dans les infrastructures modernes.

modifications et ajouts :

— Le champ **Classe de trafic** remplace le champ "Type de service" en IPv4. IPv6 introduit également un nouveau mécanisme pour gérer les préférences.

— Le champ Type de protocole en IPv4 est renommé en **champ Prochain en-tête**.

— Le champ Temps de vie (TTL) devient **la Limite de saut**.

— Un **champ d'étiquette de flux** a été ajouté pour améliorer la qualité de service et la gestion du trafic dans les réseaux IPv6.

Segmenter un réseau IPv6 en sous-réseaux

Segmenter le réseau en sous-réseaux a l'aide d'ID de sous-réseau

Dans IPv4, la segmentation en sous-réseaux nécessite l'emprunt de bits de la partie hôte, car l'idée de sous-réseau n'était pas initialement prise en compte dans la conception de ce protocole. Cependant, avec IPv6, la segmentation en sous-réseaux est un processus plus pratique et efficace, car ce protocole a été conçu en tenant compte de cette fonctionnalité.

IPv6 dispose d'un champ d'ID de sous-réseau distinct dans l'adresse globale unique (GUA) IPv6, qui permet de créer des sous-réseaux. Cette conception permet d'augmenter la sécurité, les perfor-

mances et l'évolutivité du réseau, car chaque sous-réseau peut être associé à un lien matériel unique et l'ID de sous-réseau définit un sous-réseau administratif du réseau.

— La longueur de l'ID de sous-réseau est de 16 bits maximum, et l'assignation d'un ID de sous-réseau fait partie de la configuration de réseau IPv6. Les hôtes IPv6 peuvent utiliser le protocole de détection de voisins pour générer automatiquement leurs propres ID d'interface, en fonction de l'adresse MAC ou EUI-64 de l'interface de l'hôte. Vous pouvez également attribuer manuellement les ID d'interface, ce qui est recommandé pour les routeurs IPv6 et les serveurs compatibles IPv6.

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 [3] :

— **ID de sous-réseau 16 bits** : Crée jusqu'à 65536 sous-réseaux.

— **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).

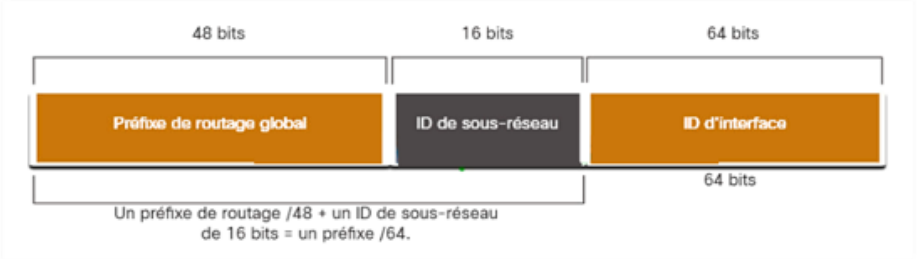

FIGURE 1.12 – GUA avec un ID de sous-réseau 16 bits.

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, puisque'aucune conversion en binaire n'est requise.

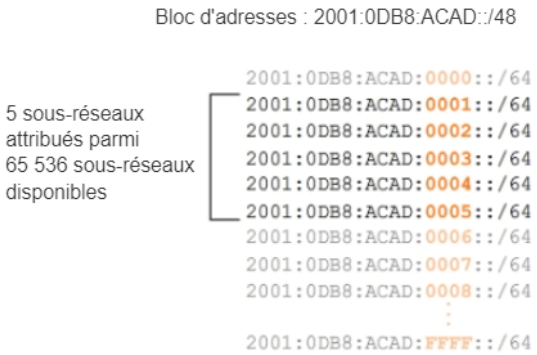

FIGURE 1.13 – Sous-réseau IPv6.

1.4 Sécurité Réseau

1.4.1 Protocole ARP

L'ARP est un protocole qui se situe sur la couche 3 du modèle OSI. ARP traduit l'adresse MAC d'un ordinateur en adresse IP, ce qui est crucial pour le bon fonctionnement des réseaux. Ce protocole est utilisé pour retrouver l'adresse MAC d'un destinataire à partir de son adresse IP, assurant ainsi la transmission efficace des données. ARP est nécessaire car il permet aux hôtes d'un réseau de connaître l'adresse matérielle des autres hôtes, ce qui est fondamental pour l'acheminement des paquets de données.

Anomalies de ARP

1. **Address Resolution Protocol (ARP) Spoofing** : Cette anomalie survie lorsqu'un attaquant envoie de fausses réponses ARP dans le but de lier sa propre adresse MAC à l'adresse IP d'une autre machine sur le réseau. Cela peut être utilisé pour intercepter le trafic réseau, effectuer des attaques de type "man-in-the-middle" ou compromettre la sécurité du réseau.

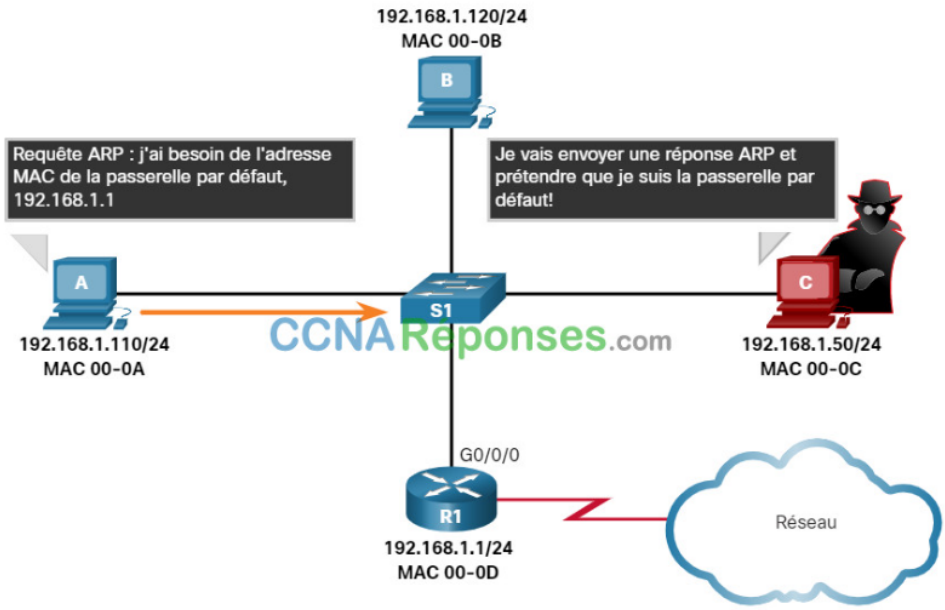

FIGURE 1.14 – Arp spoofing.

2. **ARP Cache Poisoning :** Dans ce scénario, des informations ARP incorrectes ou malveillantes sont introduites dans la table de cache ARP d'un périphérique. Cela peut entraîner un routage incorrect du trafic, des interruptions de connectivité ou des attaques ciblées sur des systèmes spécifiques.
3. **ARP Storms :** Les tempêtes ARP surviennent lorsqu'un grand nombre de demandes ARP ou

de réponses ARP sont diffusées simultanément sur le réseau. Cela peut entraîner une congestion du réseau, des ralentissements ou une défaillance complète du réseau.

4. **ARP Table Overflow :** Les tables ARP ont une capacité limitée pour stocker les entrées ARP. Lorsque cette limite est dépassée, cela peut entraîner un dépassement de capacité ou un "overflow", et peut potentiellement être exploité par des attaquants pour perturber le fonctionnement du réseau.
5. **ARP Broadcast Storms :** Des tempêtes de diffusion ARP se produisent lorsqu'un grand nombre de demandes ARP sont diffusées sur le réseau, souvent en raison d'une mauvaise configuration ou d'un dysfonctionnement d'un périphérique. Cela peut entraîner une utilisation excessive de la bande passante et une dégradation des performances du réseau.

Mesures protectrices

1. Utilisation des entrées ARP statiques pour les systèmes critiques, mais peu extensible dans de grands réseaux.
2. Mise en œuvre de l'inspection ARP dynamique sur les commutateurs pour prévenir les attaques par usurpation d'adresse ARP.
3. Segmentation du réseau en segments plus petits pour limiter les problèmes liés à l'ARP et faciliter l'isolation des problèmes.
4. Configuration des périphériques réseau pour limiter la taille de leur table ARP et éviter les risques de débordement.
5. Configuration de filtres de paquets ou de pare-feu pour bloquer les paquets ARP provenant de l'extérieur du réseau local.
6. Utilisation de VPN et d'autres méthodes de cryptage pour protéger les données contre les attaques ARP spoofing.
7. Sensibilisation des utilisateurs aux risques des attaques ARP et aux meilleures pratiques en matière de sécurité réseau.
8. Surveillance continue du trafic réseau pour détecter toute activité ARP anormale et conservation des enregistrements pour analyse.
9. Maintien à jour du micro-logiciel et du logiciel des appareils réseau pour atténuer les vulnérabilités et améliorer la sécurité.

Projection dans un monde IPv6

IPv6 intègre ces fonctions à l'adresse IP elle-même dans le cadre des algorithmes de configuration automatique sans état et de reconnaissance de voisins à l'aide ICMPv6. Par conséquent, **il n'existe**

pas de ARP pour IPv6 [20].

1.4.2 Attaques permettant de dévoiler le réseau

Attaque par cartographie du réseau

Les attaques visant à établir la cartographie d'un réseau ont pour but de dresser les artères de communication des futurs systèmes cibles.

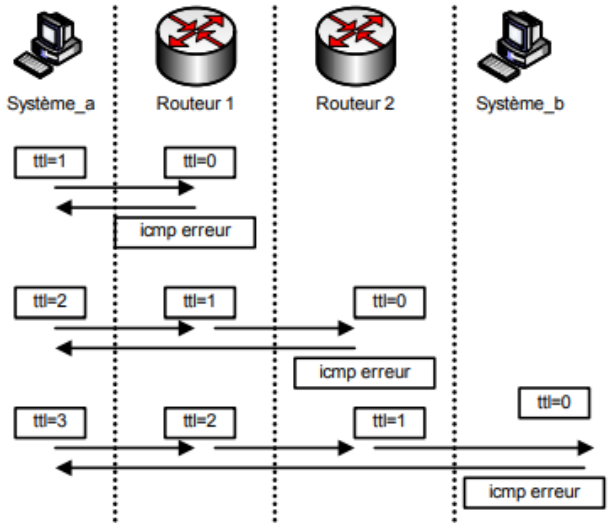

FIGURE 1.15 – Fonctionnement de l'outil Traceroute.

Projection dans un monde IPv6 Une adresse IPv6 est codée sur 128 bits, contre 32 bits pour une adresse IPv4 [22].

À titre d'exemple :

— En IPv4, on trouve des tailles de sous-réseaux de l'ordre de 28 ou 216. Elles représentent de 256 à 65 536 adresses, qui peuvent facilement faire l'objet d'une cartographie complète et avec de balayage de réseau ZMap et un ordinateur de connexion Gigabit on peut scanner l'ensemble d'espace d'adresse IPv4 en quelques minutes(45 min) .

— 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.

1.4.3 Attaques par identification des systèmes réseau

Ce type d'attaques vise à identifier tous les systèmes d'un réseau afin de dresser les futurs moyens de pénétration du réseau ou des systèmes qui le composent, les outils qui ont fait leurs preuves dans le suivi des ports déverrouillés sont appelés balayeurs de ports. Il existe pour cela différentes techniques de balayage des systèmes :

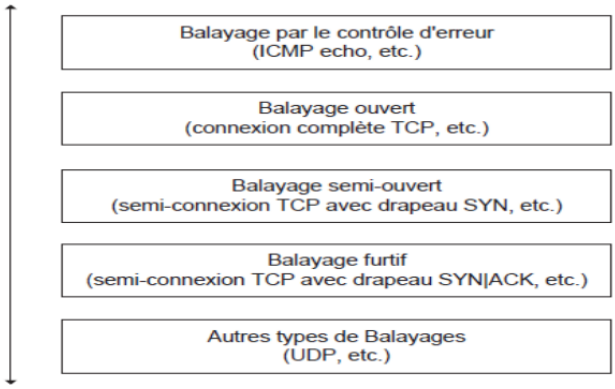

FIGURE 1.16 – Différents types de balayages.

Attaque par balayage ICMP

Il existe trois méthodes différentes de balayage utilisant le protocole ICMP pour découvrir les hôtes actifs dans un réseau [30] :

1. **ICMP Scanning (le balayage par ICMP) :** consiste à faire des Ping, c'est-à-dire envoyer un paquet ICMP Echo Request à la cible et si cette dernière est active, elle va répondre par un paquet ICMP Echo Reply.

   Il aide à déterminer les périphériques qui sont actifs dans un réseau et à savoir si les paquets ICMP sont autorisés à passer à travers un pare-feu.

2. **PING SWEEP (le balayage par PING :)** permet de détecter les hôtes allumés en utilisant une plage d'adresses IP.

   Cela consiste à envoyer un Ping et les hôtes allumés vont répondre. Alors l'attaquant va utiliser le masque de sous-réseau pour calculer le nombre d'hôtes présents dans le réseau.

3. **ICMP ECHO SCANNING (le balayage par ICMP ECHO) :** ICMP ne se base pas sur les numéros de port. A la base, ce type de balayage ne permet pas de savoir les ports qui sont actifs sur un hôte, mais il est fait pour déterminer les hôtes actifs dans un réseau. Mais en plus de ça, il peut afficher les ports ouverts sur chaque hôte actif dans le réseau ciblé.

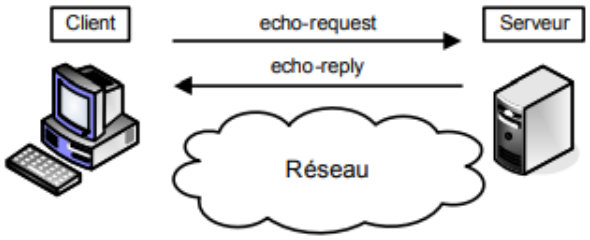

FIGURE 1.17 – Fonctions de la commande ping.

Projection dans un monde IPv6 : Le protocole ICMP, qui était confiné à la remontée d'erreurs, de tests et de découverte en IPV4, est fortement étendu en IPv6, puisqu'il intègre notamment les fonctionnalités suivantes :

— découverte des voisins ;
— découverte des routeurs ;
— remontée des erreurs et ping ;
— découverte des préfixes utilisés sur le réseau (pour s'auto-configurer) et des adresses dupliquées ;
— 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 [22].

Attaque par balayage TCP

C'est en partant du principe que le flux réseau toujours accessible au pirate est celui qui est destiné à être accessible au public que la technique du balayage TCP a été inventée.Similaire au balayage ICMP, sa spécificité est de s'appuyer sur le protocole TCP. Le client envoie un paquet SYN vers un port réseau particulier de l'adresse IP du serveur. Si le port est en écoute, un paquet Synchronize (SYN)/Acknowledgment (ACK) est reçu en retour. Sinon, la réception d'un paquet RST signifie qu'il n'y a pas de service en écoute sur le port. Le client envoie en réponse un paquet RST pour terminer la connexion, comme l'illustre la figure ci dessous :

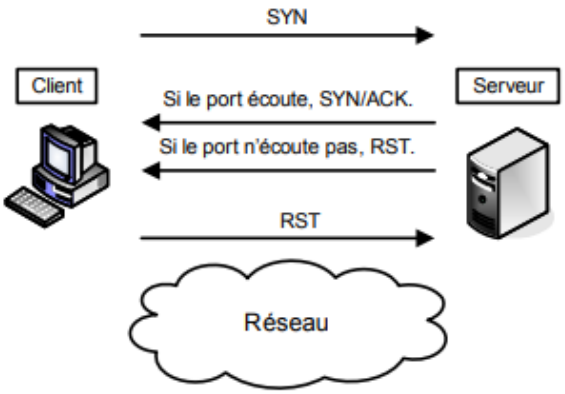

FIGURE 1.18 – Balayage TCP.

Si aucune réponse n'est reçue en retour, c'est qu'il existe un équipement filtrant entre le serveur et le client ou qu'il n'y a aucune machine derrière l'adresse IP visée.
Cette technique est cependant si peu discrète, que des variantes ont été élaborées pour améliorer le balayage en jouant sur le principe de fonctionnement de la pile TCP/IP [22].

Projection dans un monde IPv6 : Dans un environnement IPv6, les attaquants peuvent utiliser des outils et des techniques pour scanner les adresses IPv6 et les ports TCP correspondants. Cela peut être réalisé en envoyant des paquets TCP SYN à différentes adresses IPv6 avec différents numéros de port, et en écoutant les réponses pour déterminer quels ports sont ouverts.

1.4.4 Attaque par identification des routeurs

— L'écoute de réseau permet 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.

— Le lancement des requêtes qui ont pour but de forcer ces routeurs à répondre. Par exemple, des requêtes peuvent s'appuyer sur une demande ICMP de découverte de routeur (ICMP router discovery) ou des requêtes de routage (OSPF, BGP, etc.).

— Un pirate peut aussi envoyer des requêtes Internet Router Discovery Protocol (IRDP) (ICMP Router Discovery Protocol), également appelées sollicitations de routeur (router solicitations), vers l'adresse de broadcast afin de connaître la route par défaut du réseau.

1.4.5 Attaque par traversée des équipements filtrants

Quand un pirate désire établir la cartographie d'un réseau généralement, il rencontre sur son chemin un équipement filtrant (pare-feu ou un routeur avec des règles de filtrage). On y trouve donc des attaques comme :

Attaque par modification du port source

Lorsqu'un pare-feu n'est qu'un simple routeur utilisant des listes de contrôle d'accès (ACL) ou un pare-feu qui ne peut détecter qu'un flux correspond au trafic retour d'une session sortante déjà initiée (le pare-feu est alors dit "stateful"), il est possible de passer outre les règles de filtrage appliquées en usurpant (spoofing) le port source du paquet émis (source porting).

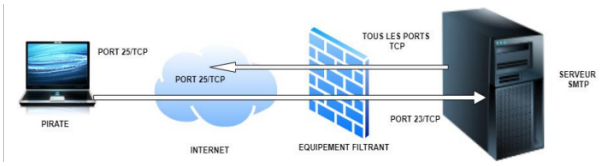

FIGURE 1.19 – Traversée d'un pare-feu en fixant le port source.

Attaques par fragmentation des paquets IP

Deux techniques permettent de jouer sur la fragmentation des paquets : celle dite par **Tiny Fragments** et celle par **Fragment Overlapping**.

1. **Attaque par Tiny Fragments :** Consiste à fragmenter sur deux paquets IP une demande de connexion TCP ou d'autres demandes sur une machine cible 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'entête TCP, c'est-à-dire 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, de même que tous les fragments associés, sans avantage de contrôle sur les autres fragments. Lors de la défragmentation au niveau IP de la machine cible, le paquet de demandes de connexion était reconstitué et passé à la couche TCP. La connexion s'établissait alors malgré le filtre IP.

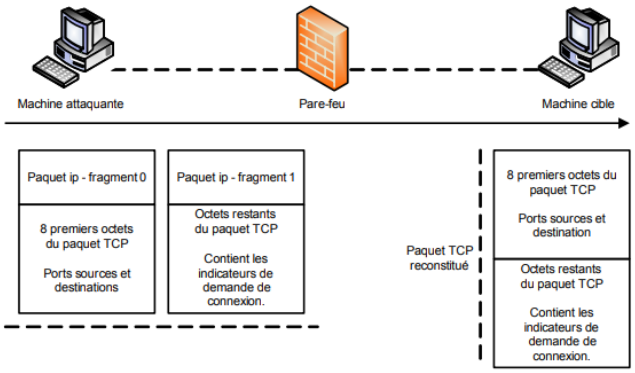

FIGURE 1.20 – Attaque de Tiny Fragments.

2. **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 autre 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) [22].

Projection dans un monde IPv6 : En IPv6, seule la machine émettrice peut fragmenter les paquets, permettant par conséquence aux sauts IP de ne pas avoir à analyser, et donc de ne pas être vulnérables aux attaques par fragmentation. Cependant, il reste à la charge du destinataire du trafic de se prémunir contre ses attaques (il doit défragmenter les paquets.).

Pour protéger les destinataires IPv6 de ce type d'attaque, les équipements de sécurité de protection du périmètre doivent être en mesure de contrôler la fragmentation des paquets en transit.

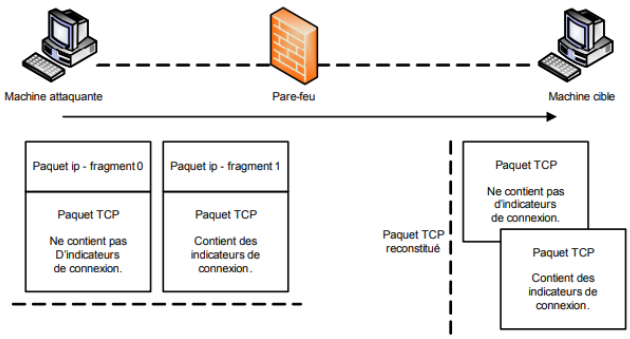

FIGURE 1.21 – Attaque par Fragment Overlapping.

1.4.6 Attaques permettant d'écouter le trafic réseau

Attaque par sniffing

Il est important de savoir qu'un sniffer est un magnifique outil permettant d'étudier le trafic d'un réseau quelconque. De nos jours malheureusement, comme tous les outils d'administration, le sniffer peut également servir à une personne malveillante ayant un accès physique au réseau pour collecter des informations confidentielles.

Attaque de commutateur

Compte tenu de nombreux types d'attaques VLAN dans les réseaux commutés modernes. Grâce à la simplification des architectures, VLAN permet d'améliorer les performances, elle peut également ouvrir la voie aux excès. Il est primordial de comprendre la méthodologie générale sous-tendant ces attaques et les principales approches permettant de les limiter.

Pour voir le trafic en prévenance d'un autre VLAN, le saut de VLAN permet à un VLAN de le voir, par exemple, l'usurpation de commutateur qui tire parti d'un port trunk configuré de manière incorrecte. Les ports trunk par défaut ont accès à tous les VLAN et acheminent le trafic de plusieurs VLAN sur une même liaison physique, c'est généralement entre des commutateurs.

- Désactiver le trunking sur tous les ports, est le meilleur moyen d'éviter une attaque de base d'usurpation de commutateur, sauf ceux qui le requièrent spécifiquement sur les ports de trunking requis, désactivez Dynamic Trunking Protocol (DTP), puis activez manuellement trunk.

1.4.7 Protocoles Utilisés dans IPv6

ICMPv6

Le protocole ICMPv6 est un protocole de la couche Internet du modèle TCP/IP qui est défini dans la RFC 4443, il est plus puissant que son prédécesseur ICMPv4.

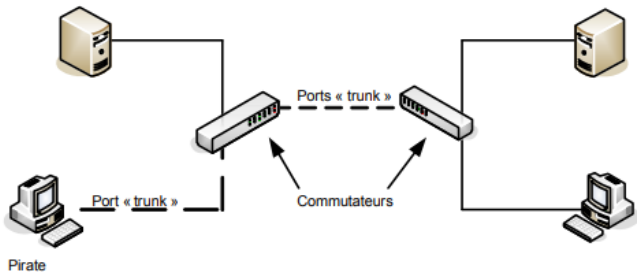

FIGURE 1.22 – Attaque VLAN Hopping.

Fonctionnalités

ICMPv6 permet de véhiculer non pas des données utilisateur mais des informations permettant de gérer les communications entre les différents composants d'un réseau (postes, routeurs, imprimantes, switchs...) [2] [16].

Types des messages ICMPv6

Il existe deux catégories des messages :

— les messages d'erreur, pour lesquels la valeur du champ Type est inférieure ou égale à 127.

— les messages d'information,pour lesquels la valeur du champ Type est supérieure à 127.

L'en-tête du message ICMPv6 a la même structure que celui du message ICMPv4,la seule différence provient du mode de calcul du champ Checksum qui est effectué en prenant en compte le pseudo en-tête [1].

	Type	Code	Description
ERROR MESSAGES	Destination Unreachable (Type 1)	0	Destination Unreachable
		1	Source Quence
		2	Redirection
		3	Time Exceeded
		4	Parameter Problem
	Packet Too Big	0	Time Exceeded
	Time Exceed	0	Hop limit exceeded
		1	Fragment reassembly time exceeded
	Parameter Problem	0	Erroneous header field encountered
		1	Unrecognized next header type encountered
		2	Unrecognized IPv6 option encountered

FIGURE 1.23 – Champ Type de l'en-tête ICMPv6.

NDP

Le protocole Neighbor Discovery Protocol (NDP) permet à un équipement de s'intégrer dans l'environnement d'un réseau local, c'est-à-dire le lien sur lequel sont physiquement transmis les paquets IPv6[12].
NDP s'appuie essentiellement sur la couche ICMPv6 et n'utilise que cinq messages pour cette couche. Ces messages sont :

- **Sollicitation de routeur (Router Solicitation (RS)) :** Lorsqu'une interface est activée, les hôtes peuvent envoyer des RS demandant aux routeurs de générer des annonces de routeur (Router Advertisement (RA)) immédiatement plutôt qu'à l'heure programmée suivante.
  Le champ Type de l'en-tête ICMPv6 a une valeur égale à 133.
- **Annonce de routeur (RA)** Les routeurs annoncent leur présence ainsi que divers paramètres de liaison et Internet, soit périodiquement, soit en réponse à un message RS. Les RA contiennent des préfixes qui sont utilisés pour déterminer si une autre adresse partage la même liaison (détermination sur liaison) et/ou configuration d'adresse, une valeur limite de saut suggérée, etc [17].
- **Neighbor Solicitation (Neighbor Solicitation (NS))** : est utilisé pour déterminer l'adresse MAC d'un voisin,il permet également de détecter la duplication des adresses IPv6 via la fonction Duplicate Address Detection (DAD).
- **Neighbor Advertisement (NA)** : c'est la réponse au message NS,Un nœud peut également envoyer des NA non sollicités pour annoncer un changement d'adresse de couche liaison.
- **Redirection** : Les redirections sont utilisées par les routeurs pour informer les hôtes d'un meilleur premier saut pour une destination.

HSRP : Protocole de Routeur en Veille Active

Le protocole Hot Standby Router Protocol (HSRP) est un mécanisme essentiel pour garantir la redondance et la haute disponibilité des routeurs dans les réseaux d'entreprise. Il permet de créer des groupes de routeurs actifs et en veille, assurant ainsi la continuité du service en cas de défaillance d'un routeur (en permettant à plusieurs routeurs de fonctionner ensemble comme un seul routeur virtuel) [18].

Mise en œuvre du protocole HSRP

- Configuration des routeurs en groupes HSRP avec un routeur actif et un ou plusieurs routeurs en veille.
- Définition des priorités et des adresses virtuelles pour chaque groupe HSRP.
- Surveillance et gestion des groupes HSRP pour s'assurer de leur bon fonctionnement.

DNSv6

Le DNS (Domain Name System) permet l'obtention d'un nom plus lisible à partir d'une adresse et inversement à partir du moment où ce nom a été enregistré dans une hiérarchie de serveur DNS. Le format des adresses IPv6 étant naturellement plus long, la question d'une mise à jour du DNS était évidente. En IPv4, la transformation nom DNS vers adresse IP est définie par un enregistrement nommé A.

En IPv6, la taille des adresses étant 4 fois plus importante le quadruplé AAAA est utilisé.

DHCPv6

Dynamic Host Configuration Protocol version 6 (DHCPv6) est une méthode qui permet d'attribuer automatiquement les adresses IPv6 aux clients du réseau. Lorsque vous activez le protocole IPv6 pour une interface approuvée ou facultative, vous avez la possibilité d'activer le serveur DHCPv6 sur l'interface, pour attribuer des adresses IPv6 aux clients qui se connectent [33].

Structure des messages DHCPv6

Le message DHCPv6 présente deux structures selon les deux cas suivants :

— **Cas 1** : le client et le serveur appartiennent au même réseau.le message DHCPv6 contient les champs de la figure suivante :

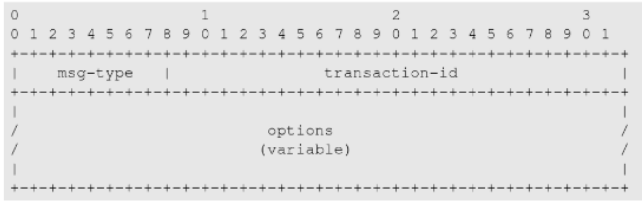

FIGURE 1.24 – Format du message DHCPv6 cas n°1.

Le tableau suivant dresse la correspondance avec les types de messages DHCPv4 :

— **Cas 2** : le client et le serveur n'appartiennent pas au même réseau.
  — Lorsque le routeur effectue le relayage du message DHCPv6, le client et le serveur étant localisés dans des réseaux différents, il encapsule le message original dans un nouveau message RELAY-FORW transmis au serveur.
  — Le serveur répond avec un message original encapsulé dans un nouveau message RELAY-REPL. L'en-tête du nouveau message sera retiré par le routeur lorsqu'il transfère le message original vers le client.
  — Le relayage des messages DHCPv6 peut également être mis en œuvre lors du renouvellement du bail, si le serveur DHCP n'a pas fourni son adresse IPv6 au client.

Messages DHCPv4	Messages DHCPv6
DHCPDISCOVER	SOLICIT
DHCPOFFER	ADVERTISE
DHCPREQUEST	REQUEST/RENEW/REBIND
DHCPACK/DHCPNAK	REPLY
DHCPRELEASE	RELEASE
DHCPDECLINE	DECLINE
DHCPFORCERENEW	RECONFIGURE
DHCPINFORM	INFORMATION-REQUEST

TABLE 1.1 – Correspondance entre les types de messages DHCPv4 et DHCPv6.

— A la différence du protocole DHCPv4, le routeur reste transparent aux données échangées entre le client et le serveur et n'apporte aucune modification [1].

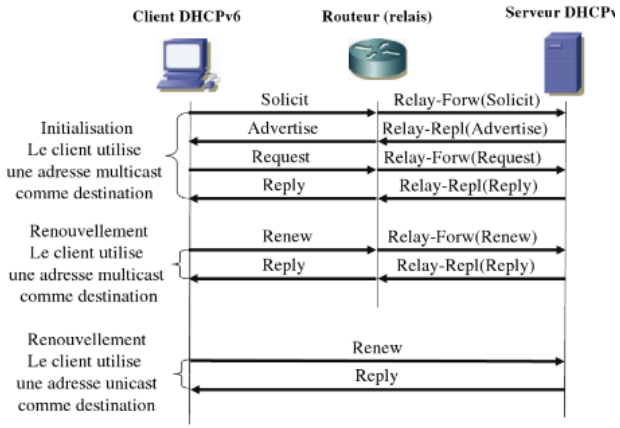

FIGURE 1.25 – Relayage des messages DHCPv6.

— L'en-tête du nouveau message comprend les champs de la figure suivante :

Attaques de DHCP

1. **Attaque DHCP Spoofing (Usurpation d'identité DHCP)** : Se produit lorsqu'un attaquant tente de répondre aux demandes DHCP et tente de se faire passer (spoof) pour la passerelle (Gateway) ou le serveur DNS par défaut, ce qui déclenche une attaque de l'homme du milieu (Man In The Middle ou Man-in-the-Middle (MITM)). Il est donc possible qu'ils puissent intercepter le trafic des utilisateurs avant de le rediriger vers la passerelle réelle ou effectuer des Denial of Service (DoS) (Denial of Service Attack, Attaque par déni de service en français) en inondant le serveur DHCP réel de demandes visant à effectuer les ressources en adresses IP [6].

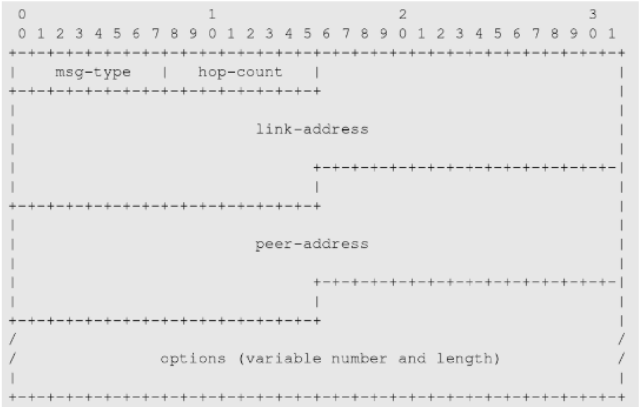

FIGURE 1.26 – Format du message DHCPv6.

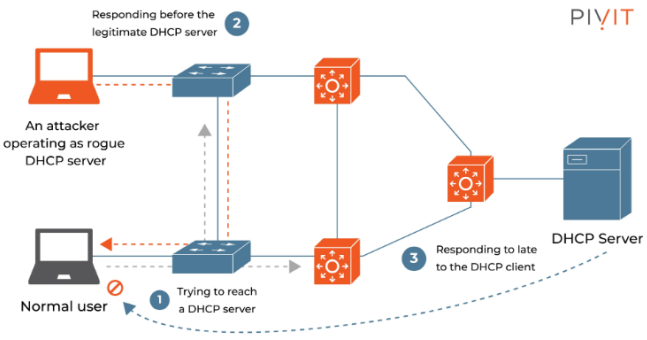

FIGURE 1.27 – DHCP spoofing.

2. **Attaque DHCP Starvation (attaque par épuisement de ressources / Famine)** : Cible généralement les serveurs DHCP du réseau, dans le but d'inonder le serveur DHCP autorisé de messages de demandes DHCP REQUEST en utilisant des adresses MAC source spoofées. Le serveur DHCP répondra à toutes les demandes, sans savoir qu'il s'agit d'une attaque, en lui attribuant les adresses IP disponibles, entraînant ainsi l'épuisement du stock DHCP. Les vrais clients ne pourront plus obtenir d'adresse IP : le trafic réseau sera paralysé [6]. Une attaque par déni de service (DoS) ou une attaque de l'homme du milieu peut être déclenchée.

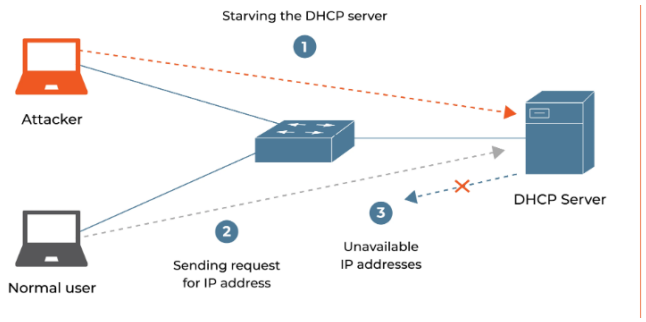

FIGURE 1.28 – Famine DHCP.

3. **Attaque de Rogue (serveur DHCP malveillant) :** Le pirate informatique configure un serveur DHCP malveillant et crée un conflit d'adresses IP en diffusant une adresse IP en double. Les pirates infiltrent un réseau en attaquant le routeur sans fil, ce qu'ils font avec un empoisonnement ARP afin d'injecter des paquets malveillants dans le flux de données traité par le routeur. Ce hack ingénieux donne aux pirates un accès continu aux réseaux via des serveurs proxy et des courriers indésirables, ce qui rend difficile pour les professionnels de l'informatique d'arrêter ou même de détecter une cyberattaque. Le pirate informatique écoute ensuite les connexions entrantes et répond de manière sélective avec des messages malveillants tels que de fausses demandes d'authentification ou des virus qui font des ravages sur les appareils des utilisateurs sans méfiance [13].

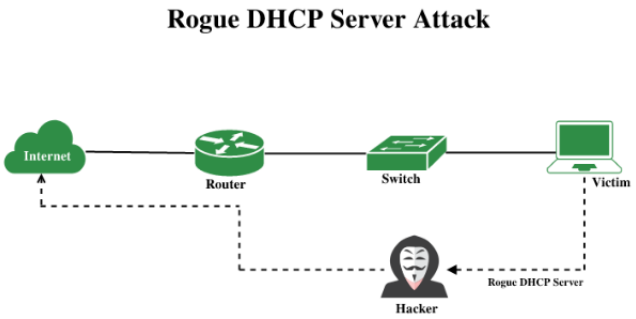

FIGURE 1.29 – DHCP Rogue.

Mesure de sécurité pour contrôler le trafic DHCP

Citons quelques mesures de sécurité pour contrôler le trafic DHCP sur un réseau :

— **DHCP Snooping** : Est une technologie de sécurité de couche 2 du modèle OSI intégrée dans le système d'exploitation d'un commutateur réseau capable qui connecte les clients aux serveurs DHCP et supprime le trafic DHCP jugé inacceptable. Il empêche les serveurs DHCP non autorisés de distribuer des adresses IP aux clients DHCP.

  La fonction DHCP Snooping permet d'effectuer les actions suivantes :

  — Valide les messages DHCP provenant de sources non fiables et filtre les messages invalides.
  — Construit et maintient la base de données de liaison DHCP Snooping, qui contient des informations sur les hôtes non fiables avec des adresses IP louées.
  — Utilise la base de données de liaison DHCP Snooping pour valider les requêtes ultérieures des hôtes non fiables [6].

— Utilisation des mécanismes d'authentification DHCP tels que DHCPv4 Authentification ou DHCPv6 Authentification pour valider l'identité des serveurs DHCP et des clients DHCP.

— Limitation de nombre de ports sur lesquels un serveur DHCP peut fonctionner.

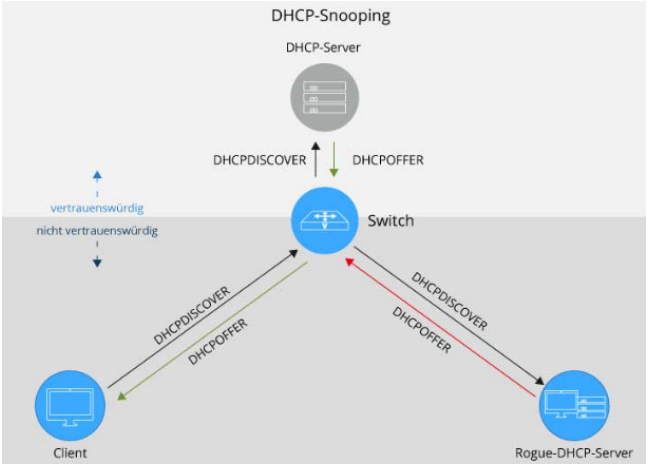

FIGURE 1.30 – DHCP snooping.

1.4.8 Vulnérabilités d'IPv6

Les caractéristiques de sécurité d'IPv6 ont été mentionnées dans RFC 2401, RFC 2402 et RFC 2406, mais nous allons décrire les vulnérabilités d'IPv6 dans cette partie .

Espace d'adressage large

L'espace d'adressage d'IPv6 est extrêmement vaste, ce qui offre des avantages en termes d'adressage, mais peut aussi créer des difficultés majeures en termes de gestion d'un tel volume d'adresses. Par exemple, une mauvaise gestion des adresses pourrait permettre à des dispositifs non autorisés de gagner l'accès à travers des adresses IP valides et compromettre la sécurité du réseau.
Les attaquants peuvent cibler les vulnérabilités d'espace d'adressage pour effectuer des attaques sur le réseau.

Méthodes d'attaque possibles liées à l'espace d'adressage étendu d'IPv6

Attaque par Scanning d'adresses IPv6

Est une méthode sophistiquée utilisée par les experts en sécurité informatique pour effectuer une reconnaissance détaillée et exhaustive d'un réseau IPv6 spécifique. Cette technique vise à identifier et à analyser de manière systématique les adresses IPv6 actives au sein d'un réseau donné.
En raison de la vaste plage d'adresses, les attaquants peuvent exploiter cette vulnérabilité pour effectuer un scan afin d'identifier les hôtes actifs et vulnérables sur le réseau.

Attaques par auto-configuration

La technologie IPv6 permet aux dispositifs de configurer leur adresse sans avoir besoin d'un serveur DHCP.
En raison de la vaste plage d'adresses, les attaquants pourraient exploiter ce processus pour générer de nouvelles adresses IP et accéder au réseau de manière indésirable.

Attaque de l'Internet des objets (Internet of Things (IoT))

C'est un paradigme technologique et conceptuel qui rend les objets simples des objets intelligents capable de transférer des données sur un réseau sans interaction humaine.
En raison de la vaste plage d'adresses,Les attaquants peuvent explorer cette dernière pour trouver des objets connectés et vulnérables [7].

1.4.9 Méthodes d'atténuation de la sécurité IPv6

1. **Antivirus** : A pour mission la détection, prévention et élimination des logiciels malveillants sur les appareils informatiques contre toutes les menaces extérieures. Il est principalement utilisé pour protéger les systèmes contre les virus et les logiciels malveillants, il peut également jouer un rôle dans la sécurisation des réseaux IPv6 en détectant les menaces potentielles au niveau des appareils.
2. **Nessus** : Est un outil de sécurité permettant de scanner des vulnérabilités utilisé pour identifier les failles de sécurité dans les systèmes informatiques. Bien qu'il ne soit pas directement lié à la sécurité des réseaux IPv6, il peut être utilisé pour évaluer la sécurité des périphériques et des services IPv6, ce qui en fait un outil utile dans le processus d'atténuation des vulnérabilités et fait gagner un temps incroyable.
3. **Tunneling** : Permet de créer des connexions sécurisées entre des réseaux IPv6 via des réseaux IPv4 non sécurisés. Afin que le tunneling puisse améliorer la connectivité et la confidentialité des données sur les réseaux IPv6, il peut également introduire des vulnérabilités potentielles en raison de la complexité de la mise en œuvre et des risques associés à la traversée de réseaux non sécurisés.

Pare-feu

Un pare-feu est un dispositif utilisé pour empêcher les accès non autorisés à un réseau. Sa fonction est double : renforcer une politique de sécurité et journaliser un trafic réseau. Le renforcement d'une politique de sécurité consiste à décider s'il faut accepter ou rejeter une connexion selon des règles spécifiques de filtrage permettant de forcer un réseau à se conformer à une politique donnée.

La journalisation quant à elle, consiste à enregistrer tous les aspects du trafic afin de pouvoir mieux l'analyser. Un pare-feu est donc un composant clé pour la conception d'un réseau sécurisé. Cependant, étant un point de passage pour tout le trafic réseau, un pare-feu peut aussi être un unique point de défaillance. Par conséquent, son choix ainsi que son emplacement sont d'importantes tâches pour la sécurité des infrastructures réseau [10].

Types de pare-feu

1. **Filtrage de paquets (packet-filtering firewall)** : Un pare-feu de filtrage de paquets opère au niveau de la couche réseau. Il examine le contenu des paquets IP et filtre le trafic en fonction des adresses, ports et autres options des paquets. Le fait d'opérer au niveau réseau lui procure une performance assez élevée car le trafic réseau passe sans délai notable. Ce type de pare-feu est alors une excellente solution lorsque la performance est une exigence importante. Par exemple, la conception d'un réseau qui doit accueillir une application Web telle qu'un site de e-commerce.
2. **Circuit de passerelles (circuit gateway firewall)** : un pare-feu à circuit de passerelle opère au niveau de la couche transport. Il filtre également le trafic en fonction des adresses. Son principal objectif est de créer un circuit virtuel entre les hôtes source et destination afin d'avoir une connexion plus transparente. Cependant, sa mise en oeuvre requiert des "Sockets" pour garder une trace des connexions séparées. Ce qui nécessite un "Socket-client" compatible sur le système de l'hôte source.
3. **Application proxy (application-proxy firewall)** : Un pare-feu d'application de proxy œuvre au niveau application et contrôle toutes les connexions entrantes et sortantes du réseau. Si une connexion est autorisée, l'application-proxy l'initie vers l'hôte destination au nom de l'hôte source. Ce type de pare-feu est capable de s'assurer que le trafic qui le traverse est conforme à la politique de sécurité et que les fonctions au sein d'un protocole ou d'une application sont conformes aux politiques spécifiées [10].

Règles de filtrage

- Un pare-feu est un système qui permet de filtrer les communications qui lui parviennent : il peut les autoriser si elles remplissent certaines conditions (ou les rejeter sinon). Ces conditions sont exprimées selon un certain nombre de règles reflétées par la configuration du pare-feu.
- Les critères de filtrage sont spécifiés selon des règles de type : **SI condition ALORS action** ou des **tables** qui énumèrent les sources et les destinations acceptables.
  - **Condition** : Le trafic pouvant être analysé selon plusieurs critères comme :
    - L'origine et/ou la destination des paquets (l'adresse source, l'adresse destination, le port source, le port destination, le protocole réseau (TCP ou UDP), le protocole appli-

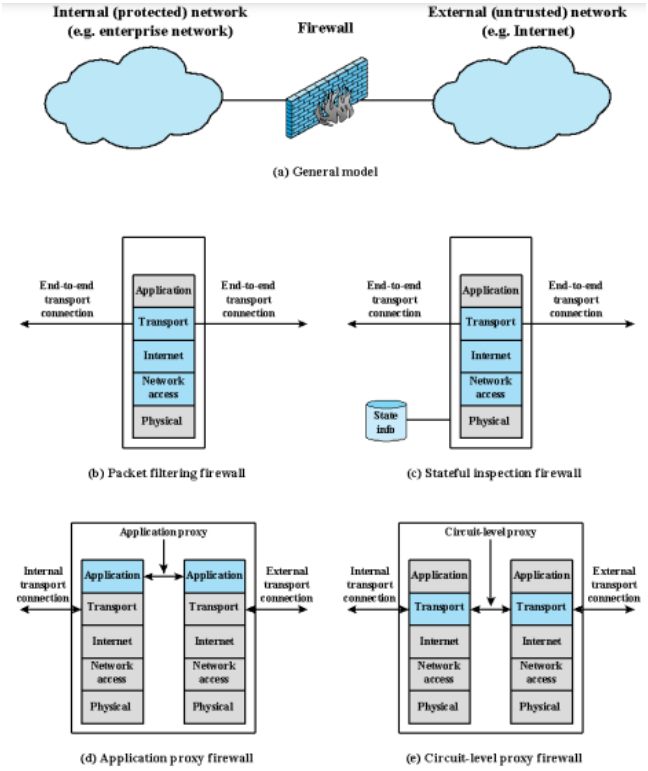

FIGURE 1.31 – Types de pare-feu.

catif (HTTP, ...), les interfaces réseau).

- La structure des données (la taille, la segmentation, la nature de chaque fragment, etc.).
- Les données et les utilisateurs.

— **Action :** L'action à prendre peut être :

- Permission.
- Interdiction.

Listes de contrôle d'accès (ACL)

Les Access Control List (ACL) sont des règles appliquées aux trafics transitant via les interfaces du routeur que ce soit en entrée (in) ou en sortie (out). LesACL filtrent le trafic en demandant aux interfaces d'acheminer ou non les paquets qui y transitent. Pour ce faire, le routeur lit l'en-tête de chaque paquet afin de déterminer s'il doit être acheminé ou non en fonction des conditions définies dans la liste de contrôle d'accès ACLs.

Utilité des ACLs

- Contrôler l'accès au réseau, en définissant les sources, destinations, services ou types de trafic autorisés à traverser les périphériques réseau.
- Optimiser les performances du réseau en limitant le trafic autorisé, réduisant ainsi la congestion et utilisant efficacement les ressources disponibles.
- Renforcer la sécurité en filtrant le trafic et en bloquant l'accès non autorisé ainsi que les at-

taques potentielles.

— Optimiser le réseau à d'autres fins que la sécurité, par exemple pour contrôler la bande-passante, restreindre le contenu des mises à jour de routage ou identifier et classer le trafic par fonctionnalités de qualité de service (Quality of Service (QoS)).

Types d'ACL

1. **ACL standard :** Dans ce type, l'ACL ne peut être liée qu'à l'adresse IP source du paquet. Ces ACL sont identifiables par un identifiant correspondant à un nombre allant de 1 à 99 ou 1300 à 1999.
2. **ACL étendue :** En plus des ACL standard l'ACL étendue peut être liée à l'adresse IP source, à l'adresse IP de destination, au type de protocole, aux ports TCP ou UDP source et destination, etc. Ces ACL sont identifiables par un identifiant correspondant à un nombre allant de 100 à 199 ou 2000 à 2699.

Remarque : Contrairement aux ACL IPv4, les ACL IPv6 ne disposent que d'un seul type, **l'ACL étendue nommée**, qui permet de spécifier des critères détaillés tels que les adresses source et destination, les types de protocole, les ports source et destination, etc.

— Les ACL étendues IPv6 sont généralement identifiables par un identifiant correspondant à un nombre allant de 2000 à 2699, en suivant une convention similaire à celle des ACL IPv4 étendues.

Gestion et Maintenance : Il est impératif de maintenir régulièrement à jour les ACL afin de les aligner avec les évolutions du réseau et les exigences de sécurité en constante évolution. Avant leur déploiement en production, il est essentiel de soumettre les ACL à des tests rigoureux pour prévenir tout risque d'erreur de configuration susceptible de compromettre la connectivité ou la sécurité du réseau. De plus, une documentation détaillée des ACL est indispensable pour faciliter leur gestion et leur maintenance à long terme.

VPN

Réseau privé virtuel (noté RPV ou Virtual Private Network (VPN)) : est une technique permettant à un ou plusieurs postes distants de communiquer de manière sûre. C'est un environnement de communication, dans lequel l'accès est contrôlé, afin de permettre des connexions entre une communauté d'intérêt seulement.

— Ce réseau est dit virtuel car il relie deux réseaux (physiques) (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données .

Types des VPN

1. VPN d'accès distant (Remote Access VPN).
2. VPN de site à site (Site-to-Site VPN).
3. VPN d'accès mobile (Mobile VPN).
4. VPN basé sur le protocole (Protocol-Based VPN).
5. VPN basé sur le cloud (Cloud VPN).
6. VPN MPLS (Multiprotocol Label Switching VPN).

Le choix de VPN dépend des besoins spécifiques en matière de connectivité, de sécurité et de performance de l'utilisateur ou de l'entreprise.

IPSec

Internet Protocol Security (IPSec) introduit des mécanismes de sécurité au niveau du protocole IP, de telle sorte qu'il y ait indépendance vis-à-vis du protocole de transport. Le rôle de ce protocole de sécurité est de garantir l'intégrité, l'authentification, la confidentialité et la protection contre les attaques. L'utilisation des propriétés d'IPsec est optionnelle dans IPv4 et obligatoire dans IPv6 [27].

1.5 Conclusion

En conclusion, l'étude de l'adressage IPv4 et IPv6, ainsi que la sécurité des réseaux, a mis en lumière des éléments cruciaux pour le fonctionnement et la protection des infrastructures réseau. L'IPv6, avec son espace d'adressage étendu, représente la réponse aux limitations de l'IPv4. Parallèlement, la mise en place de solides mesures de sécurité est indispensable pour prévenir les diverses menaces qui pèsent sur les réseaux informatiques. En identifiant les vulnérabilités potentielles et en proposant des stratégies d'atténuation, nous avons éclairé les stratégies potentielles pour une migration transparente vers IPv6.

La maîtrise de ces deux domaines est essentielle pour garantir des réseaux performants et sécurisés, capables de répondre aux défis actuels et futurs.

CHAPITRE

2

MÉCANISMES DE TRANSITIONS

2.1 Introduction

La transition vers le protocole IPv6 est devenue une nécessité incontournable pour faire face à l'épuisement des adresses IPv4. Avec la prolifération des appareils connectés et l'essor de l'Internet des objets, le nombre d'adresses IPv4 disponibles n'est plus suffisant. IPv6 offre une solution pérenne avec un espace d'adressage beaucoup plus vaste, permettant d'accueillir des milliards de nouveaux appareils.

Bien que les avantages d'IPv6 soient nombreux, la transition représente un défi technique important pour de nombreuses organisations. Les réseaux existants doivent être adaptés pour supporter IPv6 tout en maintenant la compatibilité avec IPv4. Cela nécessite la mise en place de techniques de transition spécifiques afin d'assurer une migration en douceur.

Ce chapitre a pour objectif de présenter les principales techniques de transition IPv6 à mettre en œuvre pour faciliter le passage d'IPv4 à IPv6. Nous aborderons les méthodes d'activation progressive d'IPv6 tel que le Tunneling, les mécanismes de double pile IPv4/IPv6 et les solutions de traduction entre les deux protocoles.

2.2 Techniques de transitions IPv4 vers IPv6

Un mécanisme de transition est une méthode ou un procédé pour connecter des hôtes/réseaux utilisant les mêmes ou des protocoles IP différents. La transition de l'IPv4 à l'IPv6 ne peut se faire

que d'une manière progressive qui va s'étaler sur une longue période en raison de la complexité de la taille de l'internet et du nombre énorme de dispositifs connectés au temps actuel. Pour cette raison qu'il existe de nombreuses techniques de transition pour migrer de l'IPv4 à l'IPv6, que l'on peut regrouper en trois catégories :

2.2.1 Dual Stack (double pile)

Est la préférée des techniques de transition, car elle ne fait intervenir aucun mécanisme de tunneling ou de translation d'adresse. Cela signifie que les deux protocoles IPv4 et IPv6 fonctionnent côte à côte sur la même infrastructure et sur tous les équipements connectés au réseau [21].

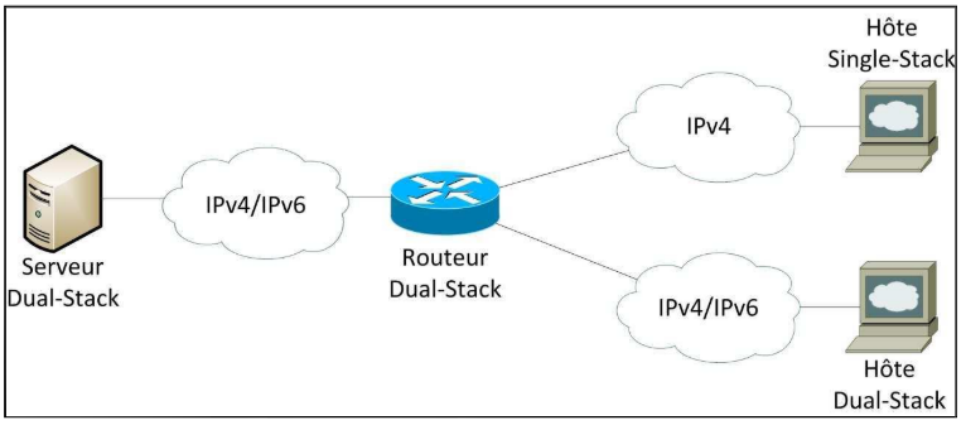

FIGURE 2.1 – IPv4-IPv6 Dual-stack.

Cette technique consiste à déployer simultanément les piles IPv4 et IPv6 sur les équipements réseau. Concrètement, chaque nœud du réseau est doté de deux piles réseau, une pour IPv4 et une pour IPv6, lui permettant de communiquer avec d'autres nœuds via les deux protocoles.

Cette approche offre une coexistence transparente des deux protocoles pendant la phase de transition vers IPv6. Les nœuds peuvent ainsi continuer à utiliser IPv4 pour communiquer avec des équipements non encore migrés, tout en étant en mesure de communiquer en IPv6 avec les nœuds ayant déjà effectué la transition.

Avantage

— L'avantage principal de cette méthode est de pouvoir se connecter aux applications IPv4 existantes via IPv4, tout en ayant accès aux applications IPv6 via le réseau IPv6. Cela peut-être coûteux en termes de performance et d'utilisation CPU.

— Les équipements réseau équipés de dual stack peuvent interagir avec les infrastructures IPv4 et IPv6 sans modification majeure.

— Facilite la coexistence des deux protocoles pendant la phase de transition.

Inconvénient

— Il ne résout pas le problème de pénurie d'adresses.

— Les routeurs doivent acheminer les deux types de paquets, ce qui réduit leur performance.

— Les applications doivent être recompilées.

Remarque et clarification : Lorsqu'une application ou un service cherche à établir une connexion au réseau sur un système configuré en dual stack, c'est-à-dire avec les piles IPv4 et IPv6 activées simultanément, le choix entre l'utilisation d'IPv4 ou d'IPv6 est souvent effectué automatiquement par le système d'exploitation, ce choix prend en compte plusieurs facteurs avec une préférence généralement accordée à l'utilisation d'IPv6 lorsque c'est possible.

Cette préférence s'explique par la nécessité de promouvoir l'adoption d'IPv6 afin de répondre à l'épuisement des adresses IPv4. De plus, IPv6 offre des avantages significatifs en termes de sécurité, de performances et de fonctionnalités par rapport à IPv4.

Ainsi, lorsque les deux options sont disponibles, les systèmes modernes configurés en dual stack optent souvent pour une connexion IPv6 pour une expérience réseau optimale. Ce processus automatique permet une transition fluide entre les deux protocoles, garantissant une connectivité efficace tout en favorisant l'évolution vers des technologies réseau plus avancées.

2.2.2 Tunneling (Les tunnels)

Bien que l'adoption d'IPv6 progresse, une grande partie du réseau Internet demeure encore en IPv4. Cette coexistence des deux protocoles a créé un besoin d'interconnecter les îlots IPv6 qui se déploient à travers le réseau IPv4 encore largement présent. C'est dans ce contexte que les techniques de tunneling ont été développées. Le tunneling consiste à encapsuler des paquets IPv6 dans des paquets IPv4 permettant ainsi leur acheminement à travers le réseau IPv4, cela se traduit par l'ajout d'un en-tête IPv4 autour du paquet IPv6 en créant ainsi un tunnel virtuel pour le faire transiter sur l'infrastructure IPv4 existante.

Cette approche offre une solution pragmatique pour interconnecter les îlots IPv6 au sein du réseau IPv4 encore dominant, facilitant ainsi la transition progressive vers IPv6. Le tunneling joue donc un rôle essentiel dans la coexistence et l'interopérabilité des deux protocoles pendant la phase de migration.

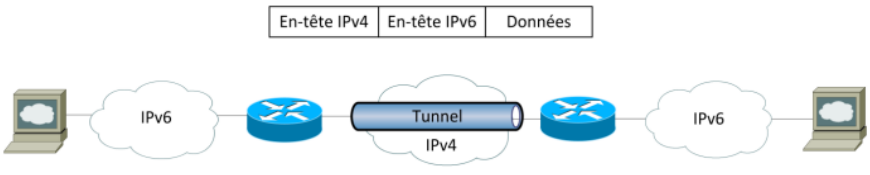

FIGURE 2.2 – Tunnel d'un paquet IPv6 à l'intérieur d'IPv4.

Il existe une variété de tunnels, chacun étant utilisé à des fins spécifiques. Certaines utilisations dépendent des points de terminaison (hôte ou routeur), de leur nombre, et parfois de la version du système d'exploitation [23]. Les types de tunnels incluent :

— **Routeur à routeur** : Les routeurs connectés à l'infrastructure réseau IPv4 peuvent transporter des paquets IPv6 en les encapsulant dans un en-tête IPv4 [23], comme illustré dans la Figure 2.3 .

— **Hôte à routeur** : Un hôte peut créer un tunnel vers un routeur ayant une connectivité IPv6. Le paquet sera envoyé en IPv6 natif depuis le routeur jusqu'à sa destination [8].

FIGURE 2.3 – Tunnel hôte à routeur.

— **Hôte à Hôte** : le tunnel existe entre deux ou plusieurs hôtes. Les hôtes IPv6/IPv4 utilisent ce tunnel pour communiquer en encapsulant les paquets IPv6 dans un en-tête IPv4 [23].

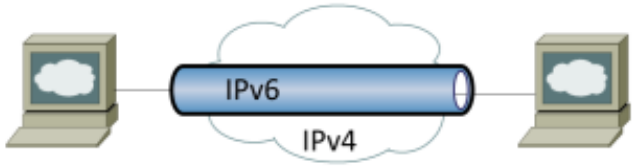

FIGURE 2.4 – Tunnel hôte à hôte.

La complexité de configuration est également un critère de classement, on peut identifier :

— Les tunnels configurés manuellement (Generic Routing Encapsulation (GRE)).

— Les tunnels configurés semi-automatiquement (Tunnel broker).

— Les tunnels configurés automatiquement (6to4, ISATAP, Teredo, etc.).

IPv6 over IPv4 GRE tunnel

Ce tunnel encapsule des paquets IPv6 à l'intérieur de paquets IPv4 à l'aide du protocole GRE. Cela permet aux réseaux IPv6 de communiquer entre eux sur une infrastructure IPv4 existante. Utile lors de la transition vers IPv6, permettant de supporter IPv6 sans remplacer immédiatement le réseau IPv4 sous-jacent. Elle est utilisée pour encapsuler des données IPv4 contenant une adresse privée de destination ou pour encapsuler le trafic d'autres protocoles comme AppleTalk sur le réseau IPv4. L'adresse de destination encapsulée n'était donc pas routable. En pratique, les données IPv6 sont encapsulées à l'intérieur d'un tunnel fournissant une connexion point-à-point entre deux routeurs [8].

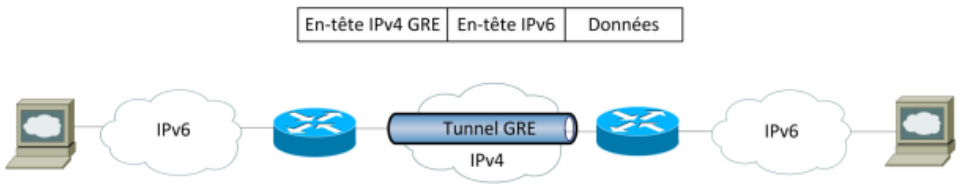

FIGURE 2.5 – Tunnel IPv6 sur IPv4 GRE.

Avantages

- Encapsulation de données IPv6.
- Connexion point-à-point.
- Compatibilité entre IPv4 et IPv6 .

Inconvénients

- Non-évolutif si le nombre de sites augmente.
- Configuration manuelle.
- Difficultés de dépannage en raison de sa configuration manuelle et de son manque de scalabilité .

Tunnel broker

Décrit dans la RFC 3053, permet la configuration semi-automatique de tunnels pour connecter des ordinateurs ou des sites de petites entreprises en IPv4 à l'IPv6. Un tunnel broker est un service qui fournit des connexions IPv6 à des utilisateurs ou des organisations sur des réseaux IPv4 en configurant automatiquement des tunnels IPv6-over-IPv4. Ces tunnels permettent aux utilisateurs d'envoyer et de recevoir du trafic IPv6 même si leur fournisseur d'accès Internet ne prend pas en charge IPv6.

En pratique, le tunnel broker configure un des routeurs pour établir le tunnel et envoie un script à exécuter sur la machine qui souhaite utiliser le tunnel afin de configurer correctement les paramètres réseau. La machine est ensuite connectée à l'IPv6 via le service du tunnel broker [8]. Les étapes mentionnées sont illustrées à la Figure 2.6.

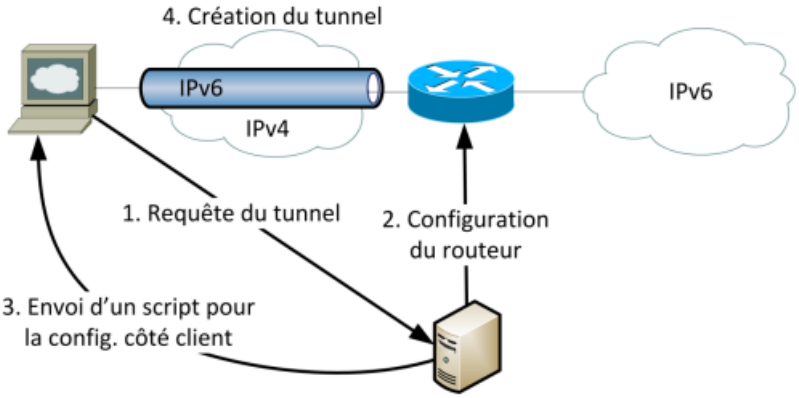

FIGURE 2.6 – Mise en place automatique d'un tunnel à l'aide d'un tunnel broker.

Avantages

- Facilité d'accès.
- Gestion centralisée.
- Configuration simplifiée.
- Support technique en cas de problème avec le tunnel ou la configuration réseau.

Inconvénients

- Le routeur du tunnel broker doit accepter des modifications de configuration depuis un serveur distant, ce qui peut présenter un risque en termes de sécurité du réseau.
- En fonction de l'emplacement géographique du tunnel broker et de la qualité de son infrastructure, il peut y avoir une latence supplémentaire dans la communication réseau.

6to4 tunnel

Le tunnel 6to4 décrit dans la RFC 3056 est un mécanisme de tunnel automatique permettant aux domaines IPv6 isolés de s'interconnecter via le réseau IPv4. Contrairement aux autres mécanismes, les tunnels 6to4 sont multipoint plutôt que point-à-point.

De plus, ce n'est pas un tunnel à proprement parler, il utilise le préfixe réservé 2002 : :/16 suivi de l'adresse IPv4 du routeur 6to4 auquel l'hôte est connecté, comme illustré à la Figure 2.7. Les 16 bits désignent un sous-réseau et les 64 derniers bits identifient l'interface de l'hôte (adresse MAC). Les routeurs 6to4 extraient l'adresse IPv4 du routeur de destination à partir de l'adresse IPv6 de destination et encapsulent le paquet IPv6 [8].

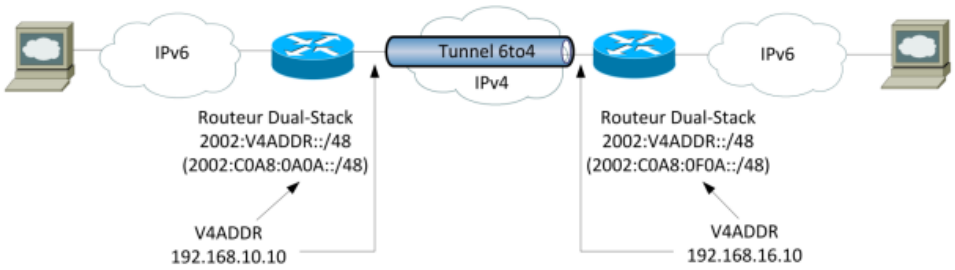

FIGURE 2.7 – Interconnexion de domaines 6to4.

Avantages

— Connectivité automatique des hôtes ou des sites IPv6 entre eux via le réseau IPv4 existant.

— Utilisation des adresses IPv4 existantes pour encapsuler les paquets IPv6.

— Extension de la connéctivité IPv6 à des domaines isolés ou des sites qui ne disposent pas encore d'un accès natif à IPv6.

Inconvénients

— Limitée par le nombre d'adresses IPv4 publiques, puisqu'il est obligatoire pour un routeur d'en posséder une.

— Elle ne supporte pas qu'un NAT soit sur le chemin.

— Elle ne supporte pas l'utilisation du multicast.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

ISATAP est un mécanisme automatique de tunneling défini dans la RFC 5214, permettant la communication entre hôtes IPv6 à l'intérieur d'un même site en utilisant l'infrastructure IPv4 existante. Ceci est illustré à la Figure 2.8. L'adresse ISATAP est formée d'un préfixe IPv6 global ou lien-local d'une longueur de 64 bits, de l'identificateur propre 0000 :5efe et enfin des 32 bits de l'adresse IPv4 identifiant l'interface. Il faut toutefois noter qu'ISATAP ne supporte pas le NAT, ni le multicast [8].

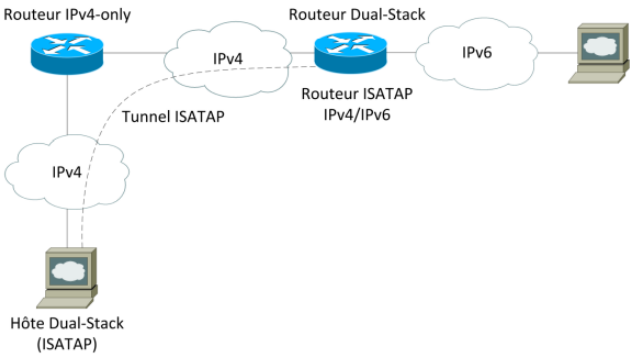

FIGURE 2.8 – Création d'un tunnel ISATAP.

Avantages

— Utilisation de l'infrastructure IPv4 existante qui réduit les coûts de déploiement et facilite la transition vers IPv6.

— ISATAP facilite la communication entre les hôtes IPv6 au sein d'un même site, ce qui peut être utile dans les réseaux d'entreprise et les environnements locaux.

— Automatisation du tunneling pour simplifie la configuration et la gestion des réseaux.

Inconvénients

— Ne résout pas le problème de la pénurie des adresses IP.

— ISATAP ne prend pas en charge le Network Address Translation (NAT) ni le multicast, ce qui peut limiter ses capacités dans certains scénarios réseau.

— la configuration et la gestion d'ISATAP peuvent être complexes dans certains cas, en particulier dans les réseaux de grande taille.

Teredo

Teredo est une technologie d'adressage et de tunneling automatique définie dans la RFC 4380, établissant une connexion IPv6 au moyen du réseau IPv4. Son point fort est sa capacité de traverser la plupart des NAT sur un ou plusieurs niveaux, en encapsulant le paquet IPv6 dans un paquet UDP IPv4. Ce paquet sera donc constitué d'un en-tête IPv4 suivi d'un en-tête UDP puis d'un en-tête IPv6, et enfin des données IPv6. Une adresse Teredo commence toujours par le préfixe 2001 : :/32. Il faut noter que ce protocole développé par Microsoft, s'adapte automatiquement au type de Nat qu'il doit traverser [8].

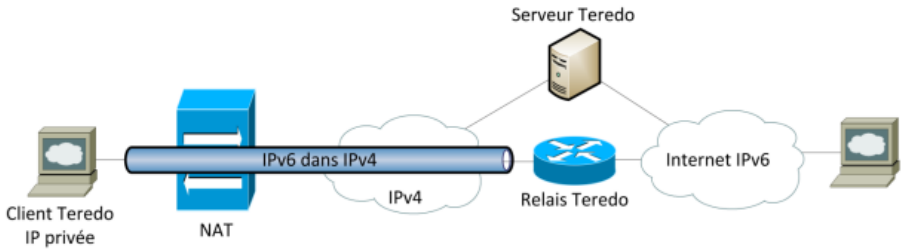

FIGURE 2.9 – Infrastructure Teredo.

L'infrastructure Teredo est composée d'un client, d'un relais et d'un serveur Teredo, comme illustré à la Figure 2.9. Le serveur Teredo aide le client dans sa configuration d'adresse en découvrant son adresse et son port, ce qui facilite la communication entre clients Teredo. Le relais Teredo transmet les paquets à un hôte IPv6. Il existe encore un relais host-specific dual-stack, qui peut communiquer directement avec les clients Teredo.

Avantages

— Adaptabilité aux différents types de NAT.

— Teredo rend la mise en place d'une connexion IPv6 sur un réseau IPv4 plus facile grâce à son processus automatique.

— Teredo permet de passer à travers les pare-feus NAT en enveloppant les données IPv6 dans des paquets UDP IPv4.

Inconvénients

— L'ajout d'en-têtes supplémentaires peut ralentir les performances du réseau.

— Teredo est sensible aux limitations et aux problèmes du protocole UDP.

— La configuration peut être complexe, en particulier lors du passage à travers des pare-feu ou d'autres dispositifs de sécurité réseau.

2.2.3 Translation (Traduction)

Également connue sous le nom de **Network Address Translation - Protocol Translation (NAT-PT)** , est l'une des techniques utilisées pour faciliter la communication entre les réseaux IPv4 et IPv6 pendant la phase de transition. Cette méthode consiste à traduire dynamiquement les en-têtes IP et les protocoles de transport entre les deux versions du protocole IP. Ainsi, les nœuds IPv4 peuvent communiquer avec des nœuds IPv6, et vice versa, grâce à cette passerelle de traduction.

Remarque : La RFC 2766 définit deux types de NAT-PT, le NAT-PT traditionnel, qui permet aux terminaux IPv6 d'initier la communication avec les terminaux IPv4, et le NAT-PT bidirectionnel, qui permet également aux terminaux IPv4 d'initier des sessions de communication avec le réseau IPv6. En se basant sur l'algorithme Stateless IP/ICMP Translation (SIIT) (Stateless IP/ICMP Translator) [21].

L'algorithme SIIT : est un mécanisme de traduction d'adresses IP qui permet aux réseaux IPv4 et IPv6 de communiquer entre eux sans nécessiter de modifications sur les hôtes eux-mêmes. Il est défini dans la RFC 6145 et est utilisé pour résoudre le problème de la compatibilité entre les réseaux IPv4 et IPv6.

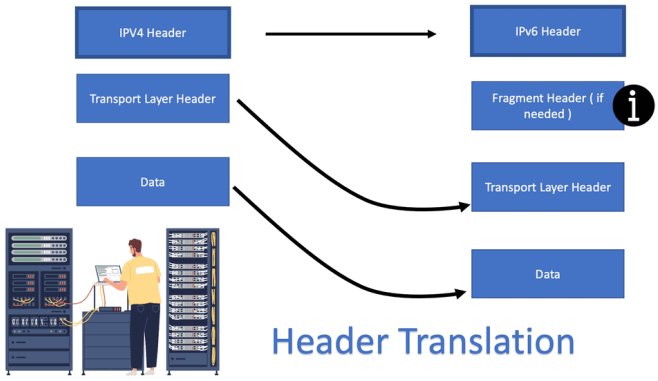

FIGURE 2.10 – Utilisation de SIIT pour NAT46 sans état, En-tête.

Le principe de la traduction NAT-PT repose sur deux éléments clés :

1. **Traduction d'adresses (Network Address Translation (NAT)) :** Pour les paquets IPv6 à destination d'un nœud IPv4, le NAT-PT utilise généralement un préfixe/96 prédéfini. Ce préfixe est combiné avec les 32 bits de l'adresse IPv4 de destination pour former une adresse IPv6 de 128 bits. Le processus inverse est appliqué pour les paquets IPv4 à destination d'un nœud IPv6.
2. **Traduction de protocole (PT) :** Cette opération concerne la conversion entre les en-têtes IPv4 et IPv6 y compris l'en-tête ICMP. La majorité des champs sont traduits mais pas tous, selon des règles de traduction spécifiques.

Limitations

— NAT-PT présente certaines limitations. Lors de la traduction, l'adresse dans la charge utile reste inchangée, ce qui peut poser des problèmes de compatibilité pour certaines applications. De plus, le NAT-PT nécessite une configuration de routage spécifique avec un préfixe /96 réservé pour le fonctionnement de cette technique.
— Problèmes potentiels de performances et de fiabilité.
— Complexité de mise en œuvre et de maintenance.
— Risque de perte d'informations lors de la traduction.

En bref, la traduction NAT-PT est une solution de transition temporaire pour interconnecter les réseaux IPv4 et IPv6, mais qui présente des limitations techniques et de mise en œuvre qui ont conduit au développement de mécanismes plus récent et performants.

NAT64

Le NAT64 décrit dans la RFC 6146, est le successeur du NAT-PT. Il permet à des clients IPv6-only de contacter un serveur IPv4, comme on peut le voir à la Figure 2.12.

Il faut noter que la communication ne peut s'initier que dans ce sens. En complétant le NAT64 avec un DNS 64, aucun changement de configuration n'est nécessaire, ni du côté de l'hôte IPv6, ni du côté du serveur IPv4 [8].

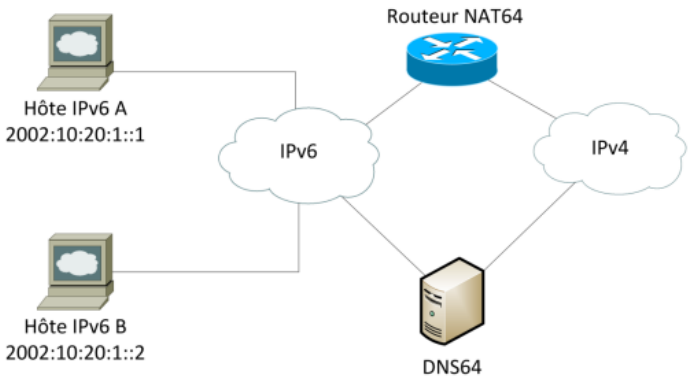

FIGURE 2.11 – NAT64 et DNS 64.

L'association d'un DNS64 à un NAT64 permet à des hôtes IPv6 d'accéder dynamiquement aux services d'un serveur IPv4. L'inverse n'est possible qu'avec une translation statique d'adresses.

Exemple

Dans cette architecture, le DNS64 fournit l'adresse IPv6 du NAT64 dans laquelle les 4 derniers octets correspondent à l'adresse IPv4 de l'hôte recherché :

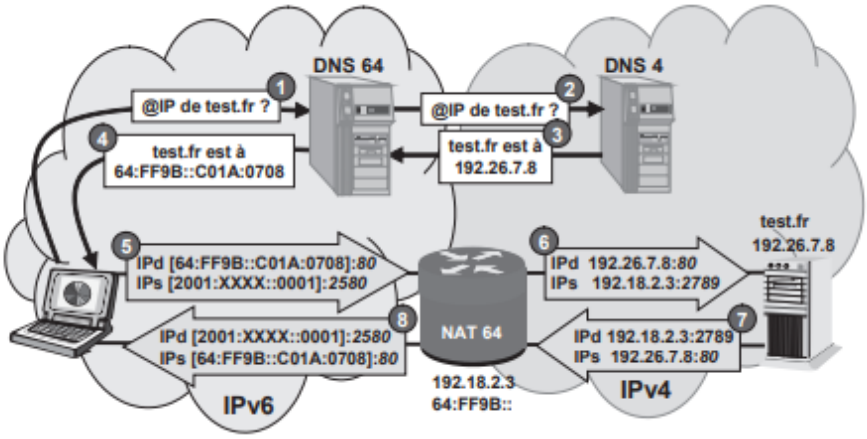

FIGURE 2.12 – Architecture du NAT64/DNS64.

1. Le client devant joindre « test.fr » sollicite le DNS64 pour en obtenir l'adresse.
2. Le DNS 64, ne disposant pas de réponse @IPv6 pour cette requête, formule une demande itérative vers un DNS4.
3. Le DNS4 fournit au DNS64 l'adresse IPv4 du serveur recherché.
4. Le DNS64 à partir du préfixe réservé au NAT64 « 64 :FF9B : :/96 » et de l'adresse IPv4 (« 192.26.7.8 » soit « C01A :0708 » en notation IPv6) construit une adresse qui correspond au domaine de réponse du NAT64.
5. L'hôte adresse donc ses messages au NAT64 qui, dans ce cas, fait office de proxy vis-à-vis du serveur test.fr. Notons que le service http est bien appelé au port 80 et que le port source du demandeur est, dans ce cas, 2580.
6. Le NAT crée une entrée dans sa table, assigne un nouveau numéro de port source1 (translation de port2), et transmet la requête à l'hôte final(test.fr).
7. La réponse de l'hôte n'appelle aucun commentaire.
8. Le NAT64 transfère cette réponse au client en restituant le port source (devenu destination) d'origine.

La translation d'adresses n'est pas la seule opération à réaliser par le NAT. En effet, passant du monde IPv4 et IPv6, le NAT doit gérer la fragmentation notamment en assurant le ré-assemblage en garantissant l'ordonnancement. Le système est un système à état, celui-ci doit être détruit en fin de session, ce qui est assez commode avec TCP (message « Fin »), mais présente une difficulté avec UDP [9].

Contrôleur wifi IPv6

Un contrôleur de réseau local sans fil ou un contrôleur wifi (ou en anglais un wireless LAN controller WLC) est un composant de réseau qui gère les points d'accès au réseau sans fil en utilisant le protocole IPv6, permet aux appareils sans fil de se connecter au réseau. Il fournit un contrôle central sur les éléments du réseau, augmente la visibilité du réseau et simplifie grandement la surveillance des composants individuels [5].

Fonctionnement

— **Attribution d'adresses IPv6** aux périphériques du réseau via le protocole DHCPv6 ou bien avec un mécanisme d'attribution automatique d'adresses, tels que l'autoconfiguration sans état SLAAC.
— **Configuration des tables de routage IPv6** pour diriger le trafic entre les différents sous-réseaux IPv6 du réseau.

— **Gestion de la qualité de service (QoS)** pour prioriser certains types de trafic sur d'autres, en fonction des besoins du réseau.
— **Renforcement de la sécurité** en mettant en place des mesures de sécurité tel que les listes de contrôle d'accès IPv6 (ACLs), le filtrage des paquets, le chiffrement des communications et la détection d'intrusion [25].
— **Détection des pannes et correction (dépannage)**.
— **Gestion des fonctionnalités avancées** comme la mobilité IPv6, le multicast IPv6, etc [4].

Bump-in-the-Host

Bump-in-the-Host, décrit dans la RFC 6535 est un mécanisme de translation côté hôte, permettant à une application IPv4-only fonctionnant derrière un NAT de communiquer avec un serveur IPv6-only. C'est à la fois le successeur et une combinaison de Bump-in-the-stack (RFC 2767) et Bump-in-theAPI (RFC 3338). BIH peut être implémenté au niveau de l'API de la socket, en traduisant les appels aux fonctions, ou au niveau de la couche réseau, en convertissant les paquets IPv4 en IPv6 en utilisant le Stateless IP/ICMP Translation Algorithm (RFC 6145) [8].

Application Level Gateway (ALG)

Un Application Layer Gateway (ALG) est actif à la couche applicative du modèle OSI, il inspecte en détail le contenu des paquets lui étant adressés. Cette machine est placée en général entre le serveur application interne et le lien à internet. Pour l'utilisateur se connectant depuis internet, il est vu comme le but des paquets, mais en réalité, l'ALG inspecte, interprète et traduit si nécessaire chaque requête, avant de la transmettre au serveur applicatif concerné. Le même processus se déroule lorsqu'il reçoit la réponse du serveur applicatif.
Comme système de translation, un ALG peut être utilisé pour effectuer la traduction entre IPv6 et IPv4. Pour ce faire, il inspecte les paquets, et s'ils sont conformes aux règles établies, l'ALG remplace les adresses et numéros de port IPv4 par de l'IPv6, et inversement [8].

Reverse proxy

Dans le but de faciliter la communication entre hôtes ou entre applications utilisant une version différente du protocole internet, il est possible d'utiliser un reverse proxy. Cela permet donc à un utilisateur de se connecter en IPv6 au proxy, qui lui va chercher la page demandée sur le serveur web en IPv4, et la retourne en IPv6 au client, comme on peut le voir à la Figure 2.14 [8].
Cela reste la méthode la plus simple, la moins coûteuse, et la plus performante afin de pourvoir activer IPv6 sur les services Web.

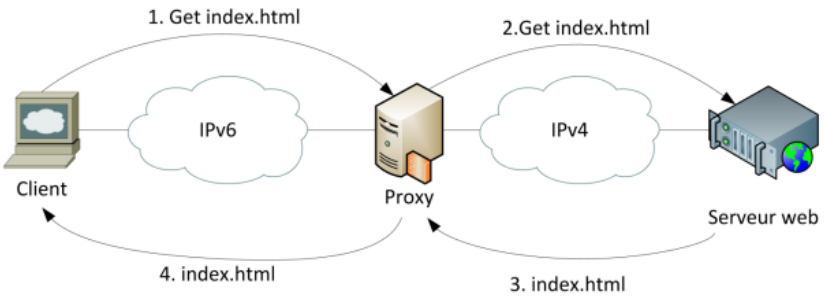

FIGURE 2.13 – Fonctionnement d'un proxy.

2.3 Conclusion

Dans ce chapitre crucial, nous avons examiné les différentes techniques et technologies de transition IPv4 vers IPv6.Ce chapitre a présenté les principales techniques de transition IPv6 à mettre en œuvre pour faciliter ce passage :

— Les tunnels IPv6 over IPv4 GRE permettent d'interconnecter des réseaux IPv6 isolés à travers une infrastructure IPv4 existante. Ils offrent une solution de transition flexible en attendant le déploiement natif d'IPv6.

— Les mécanismes de double pile IPv4/IPv6 autorisent le fonctionnement simultané des deux protocoles sur un même réseau, facilitant une migration progressive.

— Les solutions de traduction IPv4-IPv6 assurent la communication entre des hôtes IPv4 et IPv6, évitant ainsi l'isolement des équipements ne supportant pas nativement IPv6.

La transition vers IPv6 est un défi de taille, mais essentielle pour assurer la pérennité et la croissance future de l'Internet. En mettant en œuvre les bonnes pratiques et les solutions de transition appropriées, les entreprises pourront réussir cette migration stratégique.

CHAPITRE

3

ÉTUDE PRÉALABLE ET CONTEXTE DE TRAVAIL ET IMPLÉMENTATION

3.1 Introduction

Sonelgaz, établi en 1969, joue un rôle prépondérant en tant qu'opérateur historique dans le secteur de la fourniture d'électricité et de gaz en Algérie. Pendant cinquante ans, Sonelgaz s'est dévoué à fournir une source énergétique vitale pour le quotidien des Algériens.

Avec une couverture électrique de plus de 99 % et une pénétration du gaz dépassant les 62 %, Sonelgaz a considérablement amélioré la qualité de vie des familles algériennes, leur permettant de bénéficier des avantages du monde moderne.

Après la dissolution de l'EGA, Sonelgaz a relevé d'importants défis, devenant un acteur majeur dans le paysage industriel algérien. L'essor économique, le développement industriel, la croissance démographique et l'amélioration du niveau de vie ont propulsé Sonelgaz au statut de groupe industriel de premier plan.

Grâce à ses réalisations, Sonelgaz a mis en œuvre d'ambitieux programmes d'investissement, allant de l'électrification des zones rurales aux énergies renouvelables, en passant par la distribution publique du gaz dans toutes les régions, y compris les plus éloignées. Cela témoigne de son engagement en tant qu'entreprise citoyenne et de son rôle crucial dans la fourniture de services publics essentiels.

Dans ce chapitre, nous allons examiner la sécurité du réseau de la Direction de Distribution de l'électricité et du gaz de Béjaïa. Nous commencerons par identifier les vulnérabilités présentes dans le réseau. Ensuite, nous proposerons des solutions concrètes pour renforcer la protection du réseau contre les menaces internes et externes, avec une attention particulière sera accordée à l'implémentation d'IPv6 comme protocole de nouvelle génération. Bien que le déploiement d'IPv6 ne soit pas encore généralisé en Algérie, nous étudierons comment son adoption peut améliorer la sécurité du réseau de la Direction de Distribution de Béjaïa.

3.2 Organisme générale de la direction de distribution de l'électricité et de gaz de Bejaia

La Direction de Distribution de Béjaïa, filiale de la Société Algérienne de l'Electricité et du Gaz (SONELGAZ), est chargée de la distribution de l'électricité et du gaz naturel dans la wilaya de Béjaïa. Son organigramme détaille l'organisation interne et la répartition des responsabilités au sein de cette entité stratégique pour l'approvisionnement énergétique de la région.

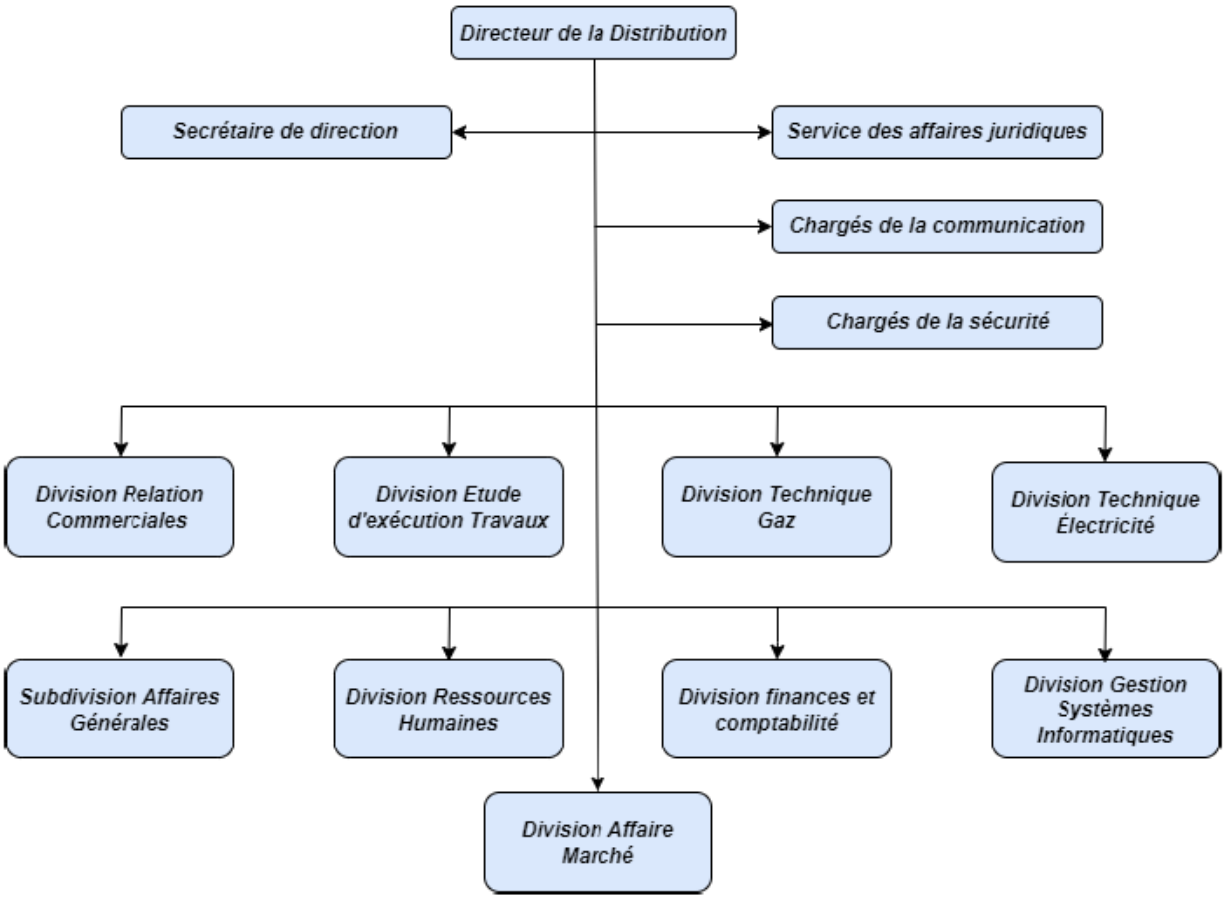

FIGURE 3.1 – Organisme de la direction de distribution de Béjaia.

Concession de distribution de Bejaïa

La direction de distribution de Bejaïa alimente les clients résidant sur le territoire de la wilaya.

Siège social : Cité Tobal - Bejaïa.

Nombre de clients électricité : 312 143 clients.

Nombre de clients gaz : 106 000 clients.

Concession de distribution de Bejaïa contient :

10 agences commerciales chargées de la prise en charge de la clientèle, qui sont :

— Bejaïa, Seddouk, Kherrata, Aokas, Amizour, El Kseur, Sidi-Aïch, Tazmalt, Akbou et les Quatre

Chemins.

5 districts d'électricité chargés du développement et de la maintenance du réseau électrique, qui sont :

— Bejaïa, Kherrata, Amizour, Sidi-Aïch, Akbou.

5 districts du gaz chargés du développement et de la maintenance du réseau de gaz, qui sont :

— Bejaïa, Kherrata, Amizour, Sidi-Aïch, Akbou.

Présentation des filiales métiers du groupe SONELGAZ

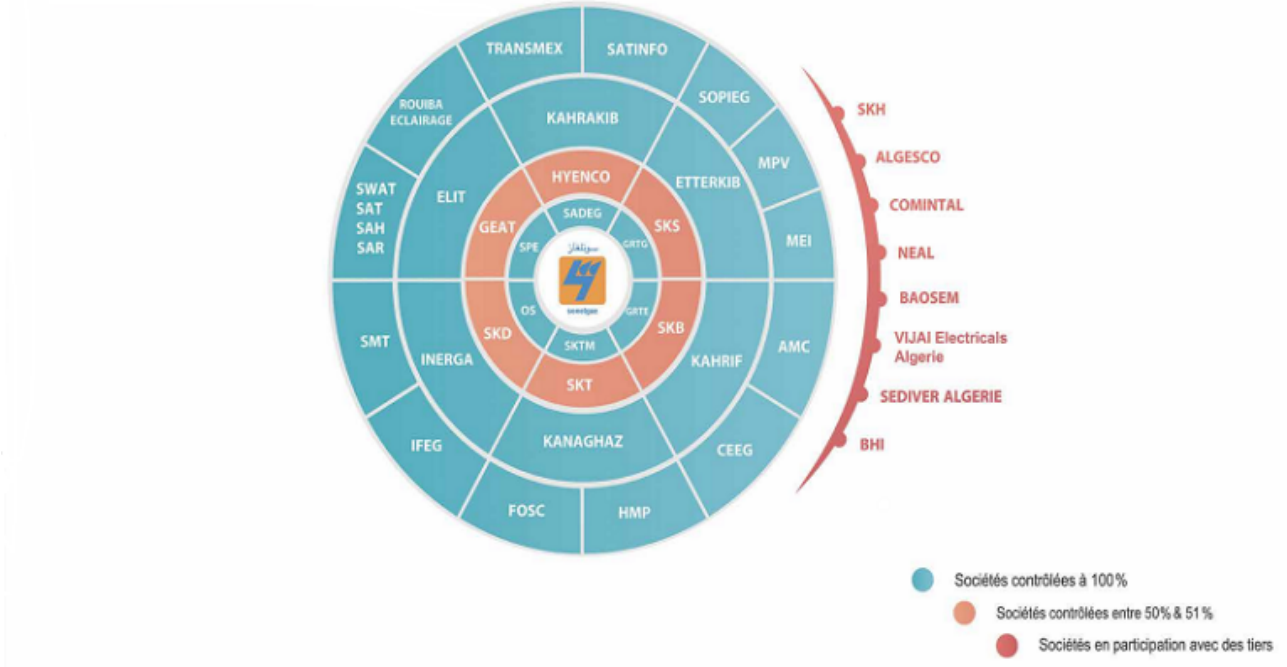

FIGURE 3.2 – Filiale Sonelgaz.

Filiale SPE

SPE gère la maintenance et l'exploitation du plus grand parc de production d'électricité en Algérie, totalisant plus de 18 GW de puissance installée, et visant à atteindre environ 23 GW d'ici 2030. Sonelgaz - Production de l'Electricité investit massivement dans la maintenance lourde pour devenir un leader sur le marché des services de maintenance à moyen terme.

Filiale GRTE

Le GRTG est chargé de l'exploitation, de la maintenance et du développement du réseau de transport du gaz, en vue de garantir une capacité adéquate par rapport aux besoins de transit et de réserve.

Filiale GRTG

La Société Algérienne de Gestion du Réseau de Transport du Gaz, assure l'acheminement du gaz naturel haute pression à travers un réseau de plus de 22 000 km. Les canalisations de Transport du Gaz sont enterrées et repérées par des balises.

Filiale SADEG

Société Algérienne de Distribution de l'Electricité et du Gaz, est le résultat de la fusion - absorption des sociétés SDC, SDE, SDO et SDA.

- **Filiale SDC** La Société de Distribution d'électricité et de gaz du Centre gère la distribution et la commercialisation d'électricité dans les wilayas du centre de l'Algérie. C'est donc la SDC qui entretient les lignes électriques et les compteurs d'électricité des foyers et des entreprises raccordés.
- **Filiale SDA** La société de distribution d'électricité et de gaz d'Alger, assure l'entretien et le développement du réseau de gaz et d'électricité ainsi que des compteurs dans la wilaya d'Alger.
- **Filiale SDE** Société de Distribution de l'EST.
- **Filiale SDO** Société de Distribution de l'Ouest.

Filiale d'OS

L'Opérateur système électrique , chargée de la conduite du système de production et de transport de l'électricité.

Infrastructure du réseau de concession de distribution Béjaïa

Le système informatique interne de la Direction de la Distribution à Béjaïa est configuré comme suit :

1. Deux armoires informatiques :
   - Armoire rez-de-chaussée, contenant 3 switchs stackés qu'on illustrera par la suite par un seul switch. Elle couvre les divisions : informatique, commerciale, électricité.
   - Armoire premier étage, comportant 5 switchs stackés, couvrant les bureaux du deuxième et du troisième étage.
2. Un routeur cisco 2600.
3. Téléphonie IP.
4. Des serveurs de base de données, de gestion des fichiers...

Ce réseau est structuré selon un modèle hiérarchique, ce qui signifie qu'il est organisé en trois couches distinctes, à savoir :

1. **Couche d'accès :**
   - **Contrôle d'accès** : Elle régule les droits d'accès aux ressources et aux services du réseau, en déterminant quels périphériques sont autorisés à communiquer entre eux.
   - **Gestion du trafic local** : Chargée de la distribution du trafic réseau à travers les différents appareils, comme les commutateurs et les ponts, garantissant ainsi une communication fluide entre les périphériques finaux.
   - **Isolation des flux de données** : Elle s'assure que les données échangées entre les périphériques finaux ne perturbent pas le fonctionnement des autres couches du réseau, préservant ainsi l'intégrité de la communication globale.
2. **Couche de distribution :**
   - **Filtrage** : Elle applique des règles de filtrage pour limiter ou autoriser le trafic sur les réseaux locaux, offrant ainsi un niveau supplémentaire de sécurité.
   - **Connectivité** : Elle facilite l'interconnexion des différents réseaux locaux et sous-réseaux, permettant ainsi une communication transparente entre les utilisateurs et les applications.
   - **Contrôle de la qualité de service (QoS)** : Assure la priorisation du trafic en fonction des besoins des applications, garantissant des performances optimales pour les flux de données importants.
3. **Couche coeur du réseau :**
   - **Adressage** : Elle assigne des adresses IP uniques à chaque périphérique connecté au réseau, permettant ainsi leur identification et leur localisation.
   - **Contrôle de congestion** : Elle gère la congestion du réseau en surveillant le flux de données et en ajustant la quantité de trafic envoyée pour éviter la saturation.
   - **Fiabilité** : Elle assure la fiabilité des communications en gérant les erreurs de transmission et en garantissant que les paquets arrivent dans le bon ordre à destination.

Plan d'Adressage

La concession de distribution de Béjaia détient une adresse de réseau de classe A, qui est **10.65.0.0/19** (avec un masque de sous-réseau de 255.255.224.0).

Pour une segmentation en VLANs, cette adresse a été divisée en 32 sous-réseaux distincts, chacun allant de 10.65.0.x à 10.65.31.x. Cela signifie que le nouvel adressage est désormais 10.65.0.0/24 (avec un masque de sous-réseau de 255.255.255.0).

Le tableau ci-après représente la liste des VLANs créés, leurs adresses IP et masque de sous réseau :

Vlan	Nom 2	Adressage
Vlan 100	Serveur	10.65.0.0/24
Vlan 111	DATA1	10.65.11.0/24
Vlan 112	DATA2	10.65.12.0/24
Vlan 113	DATA3	10.65.13.0/24
Vlan 200	Voix	10.65.20.0/24

TABLE 3.1 – Infrastructure réseau réalisée sous GNS3.

3.3 Description de l'environnement de travail

3.3.1 GNS

Pour se rapprocher au maximum de la mise en place d'une architecture réseau réelle, nous avons choisi d'utiliser Graphical Network Simulator-3 (GNS3) 2.2.31. Ce logiciel open source et multi-plateforme (Windows, Linux, Mac OS) fonctionne à la fois comme un simulateur et un émulateur. En tant que simulateur, il modélise le comportement des réseaux LAN et WAN, tandis qu'en tant qu'émulateur, il exécute directement le système d'exploitation des équipements, notamment les routeurs et pare-feu CISCO. Cette double fonctionnalité permet de reproduire fidèlement les conditions et les résultats observés dans un environnement réel [14].

3.3.2 VMware Workstation 16.2.2

Pour l'émulation de notre réseau, nous avons opté pour VMware Workstation 10.2.2. Cet outil permet la création de multiples machines virtuelles sur un même système d'exploitation, chacune pouvant être connectée au réseau local avec une adresse IP distincte, tout en résidant sur la même machine physique. Cette solution offre la possibilité d'exécuter simultanément plusieurs machines virtuelles, la seule limite étant les performances du matériel hôte [32].

3.3.3 Pfsense

Le projet pfSense est une distribution de pare-feu réseau gratuite, basée sur le système d'exploitation FreeBSD avec un noyau personnalisé et intégrant des logiciels libres. pfSense offre la gestion de divers services, activables ou désactivables via une interface graphique conviviale [24]. Voici une liste des services proposés par pfSense :

— VPN client Point-to-Point Tunneling Protocol (PPTP), VPN site à site, OpenVPN et IPSec.

— Gestion des VLAN.

— Filtrage d'URL.
— Serveur DHCP.
— Partage de bande passante (Traffic Shaper), permettant de réguler le flux et d'optimiser ou garantir les performances du réseau.
— Répartition de charge (LoadBalancer).
— Système de détection et de prévention d'intrusion (Intrusion Detection System/Intrusion Prevention System (IDS/IPS)) avec Snort.

3.3.4 Wireshark

Wireshark est l'un des outils d'analyse de paquets les plus puissants et robustes disponibles gratuitement. Ce logiciel permet de surveiller et d'inspecter les paquets de données au sein d'un réseau. Compatible avec Windows, Mac et Linux, et doté d'une interface en français, Wireshark peut analyser et détecter plusieurs centaines de protocoles réseau, facilitant ainsi l'identification et la résolution des éventuels dysfonctionnements [34].

3.3.5 Asterisk

Asterisk est un logiciel libre et open-source qui permet la création de systèmes de téléphonie IP. Basé sur une architecture modulaire, il offre une vaste gamme de fonctionnalités pour la gestion des communications, telles que la messagerie vocale, les conférences téléphoniques, les centres d'appels, et la gestion des appels entrants et sortants. Il est compatible avec de nombreux protocoles de communication, notamment Session Initiation Protocol (SIP) et Inter-Asterisk eXchange (IAX), ce qui le rend extrêmement flexible et adaptable à divers besoins de téléphonie [26].

3.3.6 Snort

C'est un système de détection des intrusions (IDS) et un système de prévention des intrusions (IPS) open source qui fournit une analyse du trafic réseau et un enregistrement des paquets de données en temps réel. SNORT utilise un langage basé sur des règles qui combine des méthodes d'inspection des anomalies, des protocoles et des signatures pour détecter les activités potentiellement malveillantes [11].

3.4 Topologie Actuelle du Réseau SONELGAZ

La Figure suivante illustre la topologie de la Concession de Distribution Bejaïa(Concession de Distribution Bejaïa (CDB)) qui alimente en énergie électrique et gazière les clients résidant sur le territoire de la wilaya.

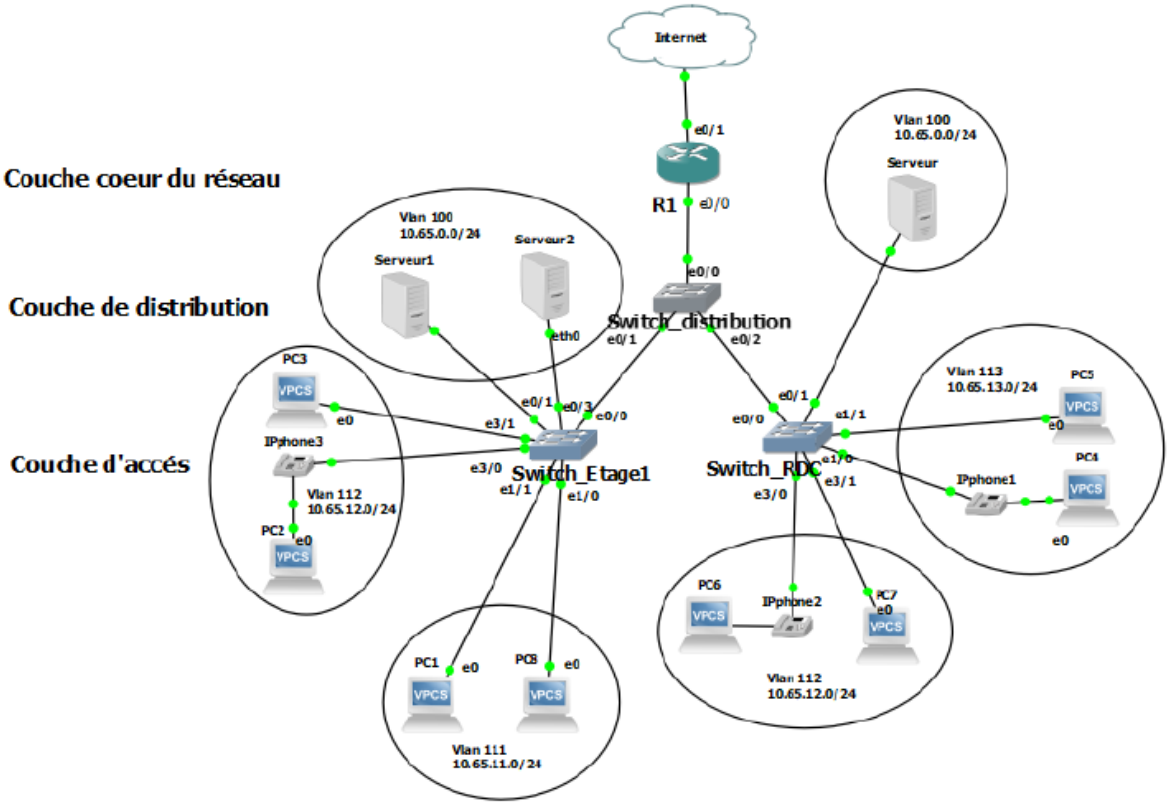

FIGURE 3.3 – Infrastructure réseau de la CDB.

Failles de sécurité du réseau existant

L'examen des attaques sur le réseau a révélé des vulnérabilités critiques dans la configuration et l'architecture, qui seront identifiées et décrites dans la section suivante :

Failles dans l'architecture

Point unique de défaillance : La dépendance sur un seul routeur central crée un risque majeur d'interruption totale des communications et de la connexion Internet en cas de défaillance du routeur.

1. **Absence de système de défense** : Le réseau manque de pare-feu ou de proxy, ce qui le rend vulnérable aux attaques comme le "reverse tunneling".
2. **Utilisation de protocoles à texte clair (ClearText)** : Les protocoles non chiffrés comme Telnet et HTTP sont utilisés pour la gestion du réseau, exposant les identifiants, mots de passe et commandes de configuration à des interceptions.
3. **Une attaque par écoute sur les appels Voice over IP (VoIP)** : Cela expose les utilisateurs à des risques importants de violation de la confidentialité et de divulgation d'informations sensibles échangées lors de leurs communications.

3.5 Solutions Proposées pour l'Amélioration du Réseau SONELGAZ

Nous proposons une solution réseau avancée conçue pour optimiser la sécurité, la performance et la résilience des infrastructures réseau. Cette solution intègre les technologies et protocoles les plus récents, notamment IPv6, tunneling, dual stack pare-feu, Zone Demilitarized Zone (DMZ) pour les serveurs, ACL, HSRP, SSH, DNS local et DHCPv6.

Tout en utilisant :

— Un routeur **IOU** .

— Trois switches **Cisco IOSvL3**.

— Un pare-feu **FreeBSD version 10**.

— Trois serveurs **Windows Server 2016**.

— Plusieurs machines virtuelles **Windows 7** .

— Asterisk pour la **voix ip**.

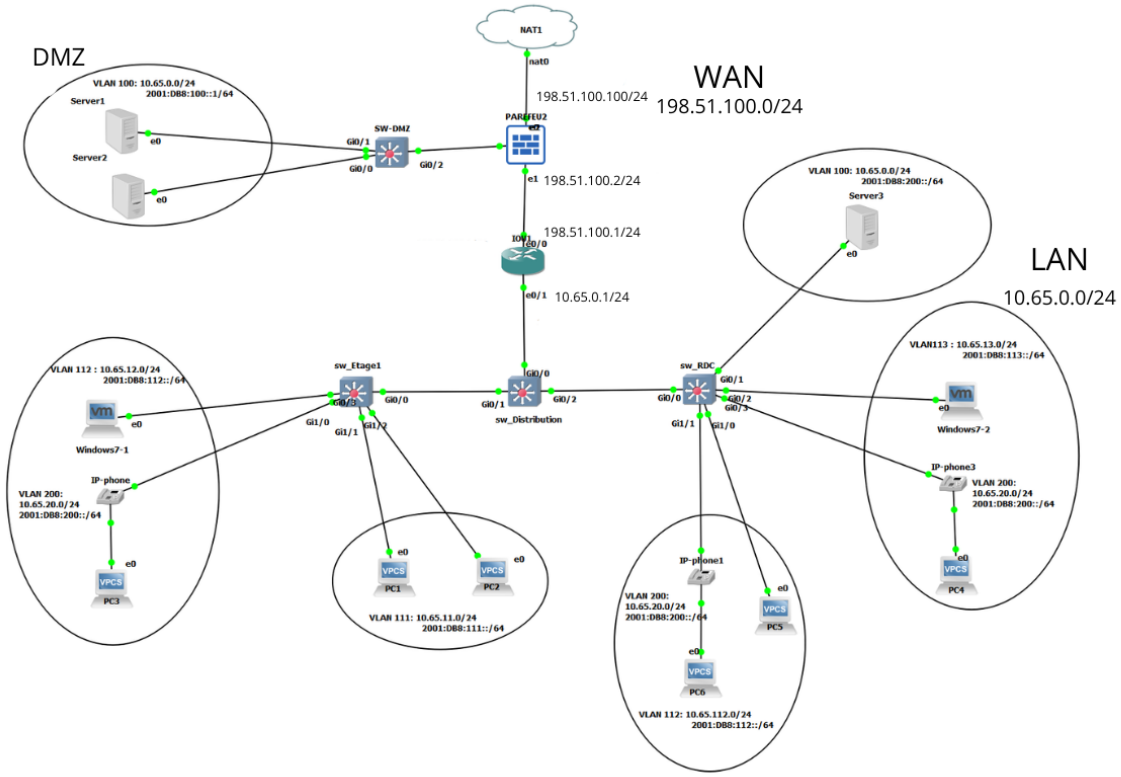

FIGURE 3.4 – Topologie du réseau Sonelgaz Améliorer.

Dans le réseau LAN, nous avons mis en œuvre une configuration Dual Stack, permettant aux équipements de fonctionner simultanément avec IPv4 et IPv6. Cette approche assure une transition fluide entre les deux protocoles, offrant une compatibilité rétroactive avec les dispositifs et applications plus anciens qui ne supportent que l'IPv4, tout en permettant l'utilisation des adresses IPv6

plus récentes et abondantes. La mise en œuvre du Dual Stack améliore la flexibilité et la robustesse du réseau interne, facilitant la gestion des adresses IP et la résolution des noms. En dehors du réseau LAN, seule la connectivité IPv6 est utilisée, grâce à la technique du tunneling 6to4 que nous avons configurée, offrant une meilleure performance, une sécurité améliorée et une future compatibilité avec les nouvelles technologies. Cette configuration garantit que notre infrastructure réseau est prête pour les défis de demain, tout en maintenant une continuité de service avec les technologies actuelles.

3.6 Mise en œuvre de la nouvelle topologie Réseau : étapes et configurations

3.6.1 Configuration du routeur

Configuration du tunnel : Voici la configuration du tunnel avec la méthode 6 to4 dans l'extrémité du routeur.

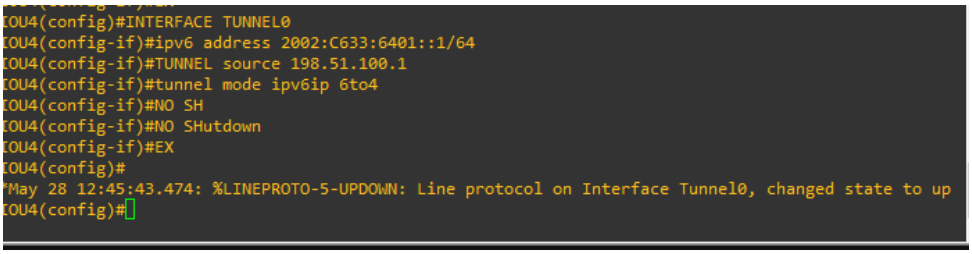

FIGURE 3.5 – Tunnel 6to4.

Création des sous interfaces du routeur avec les adresses IPv6 : La figure suivante illustre la configuration des VLANs en utilisant le protocole 802.1Q sur un routeur Cisco.

```
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
IOU4(dhcp-config)#IN
IOU4(dhcp-config)#EX
IOU4(config)#IN
IOU4(config)#INterface F
IOU4(config)#INterface FA
IOU4(config)#INterface FAS
IOU4(config)#INterface E
IOU4(config)#INterface Ethernet 0/1.10
IOU4(config-subif)#EN
IOU4(config-subif)#ENcapsulation DO
IOU4(config-subif)#ENcapsulation DOt1Q 100
IOU4(config-subif)#IP ADD
IOU4(config-subif)#IP ADDress 10.65.0.1 255.255.255.0
IOU4(config-subif)#EX
IOU4(config)#INterface Ethernet 0/1.20
IOU4(config-subif)#ENcapsulation DOt1Q 111
IOU4(config-subif)#IP ADDress 10.65.11.1 255.255.255.0
IOU4(config-subif)#EX
IOU4(config)#INterface Ethernet 0/1.30
IOU4(config-subif)#ENcapsulation DOt1Q 112
IOU4(config-subif)#IP ADDress 10.65.12.1 255.255.255.0
IOU4(config-subif)#EX
IOU4(config)#INterface Ethernet 0/1.40
IOU4(config-subif)#ENcapsulation DOt1Q 113
IOU4(config-subif)#IP ADDress 10.65.13.1 255.255.255.0
IOU4(config-subif)#EX
IOU4(config)#INterface Ethernet 0/1.50
IOU4(config-subif)#ENcapsulation DOt1Q 200
IOU4(config-subif)#IP ADDress 10.65.20.1 255.255.255.0
IOU4(config-subif)#EX
IOU4(config)#DO WR
Building configuration...
[OK]
IOU4(config)#
```

FIGURE 3.6 – Implementation du protocole DOT.1Q

Configuration d'adresses IPv6 sur les interfaces et les sous-interfaces du routeur Cisco, avec **DHCPv6** pour distribuer des adresses IPv6 à plusieurs sous-réseaux. Cette configuration est essentielle pour permettre la communication sur des réseaux utilisant le protocole IPv6.

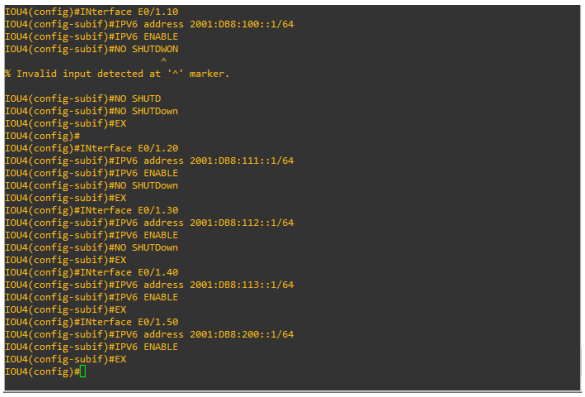

FIGURE 3.7 – Configuration des adresses IPv6.

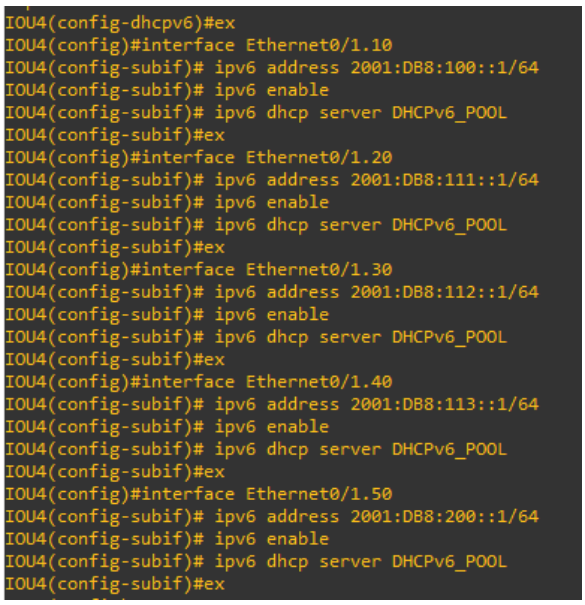

FIGURE 3.8 – Configuration de DHCPv6.

Protocole de routage

1. **Open Shortest Path First (OSPF)v3 sur le routeur :** adaptée pour les adresses IPv6 ,permet de gérer le routage dans les réseaux.

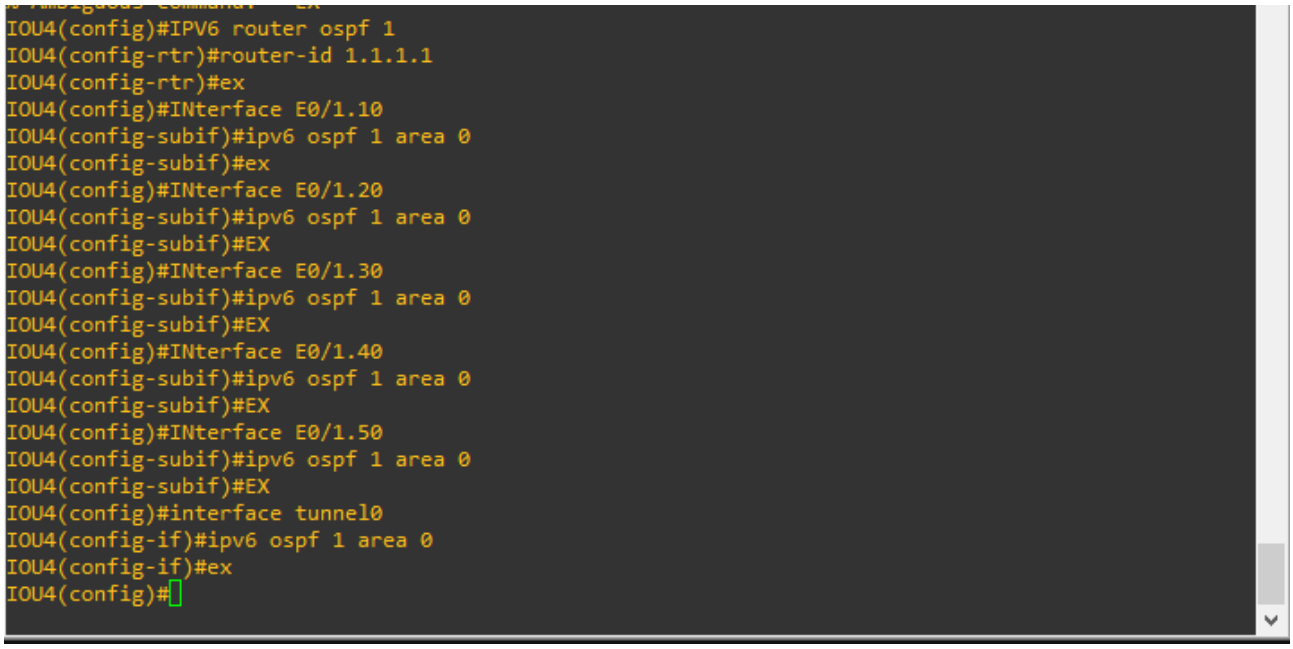

FIGURE 3.9 – OSPFv3 pour IPv6 sur Routeur.

2. **Enhanced Interior Gateway Routing Protocol (EIGRP) :** Pour les switches car c'est un protocole de routage avancé qui permet une convergence rapide et une utilisation efficace de la bande passante.
3. **Routing Information Protocol next generation (RIPng) :** Qui est un protocole de routage à

vecteur de distance adapté aux réseaux plus simples. Il envoie des mises à jour de routage toutes les 30 secondes.

Autre protocole

1. **Protocole HSRP :** pour assurer une redondance au niveau du routage et améliorer la disponibilité de notre réseau, nous allons configurer le protocole HSRP sur notre routeur.

```
!
interface Ethernet0/1.10
 encapsulation dot1Q 100
 ip address 10.65.0.1 255.255.255.0
 standby version 2
 standby 1 ip 10.65.0.150
 standby 1 priority 110
 standby 1 preempt
 ipv6 address 2001:DB8:100::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

FIGURE 3.10 – Récapitulatif d'une sous-interface routeur et exemple sur le protocole HSRP.

2. **Secure Shell (SSH) :** la configuration de SSH pour IPv6 sur les équipements Cisco du réseau permet d'améliorer la sécurité des connexions distantes et d'assurer la compatibilité avec les adresses IPv6.

```
IOU1(config)#crypto key generate rsa
% You already have RSA keys defined named IOU1.ASR.local.
% Do you really want to replace them? [yes/no]: y
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
*Jun  6 14:06:40.527: %SSH-5-DISABLED: SSH 1.5 has been disabled
1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

IOU1(config)#
*Jun  6 14:06:47.032: %SSH-5-ENABLED: SSH 1.99 has been enabled
IOU1(config)#
IOU1(config)#ip ssh v
IOU1(config)#ip ssh version 2
IOU1(config)#ip ssh tim
IOU1(config)#ip ssh time-out 60
IOU1(config)#IP SSH AU
IOU1(config)#IP SSH AUthentication-retries 2
IOU1(config)#USERNAME cisco  privilege 15 secret cisco
IOU1(config)#line vty 0 4
IOU1(config-line)#login local
IOU1(config-line)#transport input ssh
IOU1(config-line)#ipv6 access-class SSh-ipv6 in
IOU1(config-line)#
```

FIGURE 3.11 – Configuration de SSH.

3.6.2 Configuration des Switchs

La configuration des switches (commutateurs) constitue une étape essentielle dans la mise en place d'un réseau informatique fiable et performant.

Déclaration et la configuration des différents Vlans

```
Switch(config-if)#ex
Switch(config)#vlan 100
Switch(config-vlan)#name Serveur
Switch(config-vlan)#vlan 111
Switch(config-vlan)#name DATA1
Switch(config-vlan)#vlan 112
Switch(config-vlan)#NAME DATA2
Switch(config-vlan)#VLAN 113
Switch(config-vlan)#NAME DATA3
Switch(config-vlan)#VLAN 200
Switch(config-vlan)#NAME voix
Switch(config-vlan)#do wr
Building configuration...
Compressed configuration from 3530 bytes to 1578 bytes[OK]
Switch(config-vlan)#
Switch(config-vlan)#
*May 12 12:01:15.702: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*May 12 12:01:16.582: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
Switch(config-vlan)#ex
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#SWitchport access vlan 100
Switch(config-if)#switchport mode access
Switch(config-if)#ex
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#SWitchport access vlan 113
Switch(config-if)#switchport mode access
Switch(config-if)#EX
Switch(config)#interface gigabitEthernet 0/3
Switch(config-if)#SWitchport access vlan 113
Switch(config-if)#switchport mode access
Switch(config-if)#SW
Switch(config-if)#SWitchport voice vlan 200
Switch(config-if)#ex
Switch(config)#interface gigabitEthernet 1/0
Switch(config-if)#SWitchport access vlan 112
Switch(config-if)#switchport mode access
Switch(config-if)#ex
Switch(config)#interface gigabitEthernet 1/1
Switch(config-if)#SWitchport access vlan 112
Switch(config-if)#switchport mode access
Switch(config-if)#SWitchport voice vlan 200
Switch(config-if)#
```

FIGURE 3.12 – Configurations des vlans sur les Switchs.

De plus, j'ai configuré plusieurs interfaces en tant que 'Trusted' avec ***DHCP Snooping***[1], ce qui signifie qu'elles sont considérées comme fiables et autorisées à recevoir des offres DHCP. Cela garantit que les appareils légitimes connectés à ces interfaces peuvent obtenir des adresses IP de manière sécurisée et fiable.

```
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 ipv6 eigrp 100
 ip dhcp snooping trust
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 ipv6 eigrp 100
 ip dhcp snooping trust
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 ipv6 eigrp 100
 ip dhcp snooping trust
!
interface GigabitEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 ipv6 eigrp 100
!
```

FIGURE 3.13 – Sw-Distribution avec Protocole DHCP Snooping.

3.6.3 Configuration des équipements

les figures suivante montre la configuration d'hôte Windows de CDB et celle de Astrisk pour la voix ip :

1. DHCP Snooping est une fonctionnalité de sécurité qui permet de contrôler et de filtrer le trafic DHCP en autorisant uniquement le trafic DHCP provenant de sources fiables.

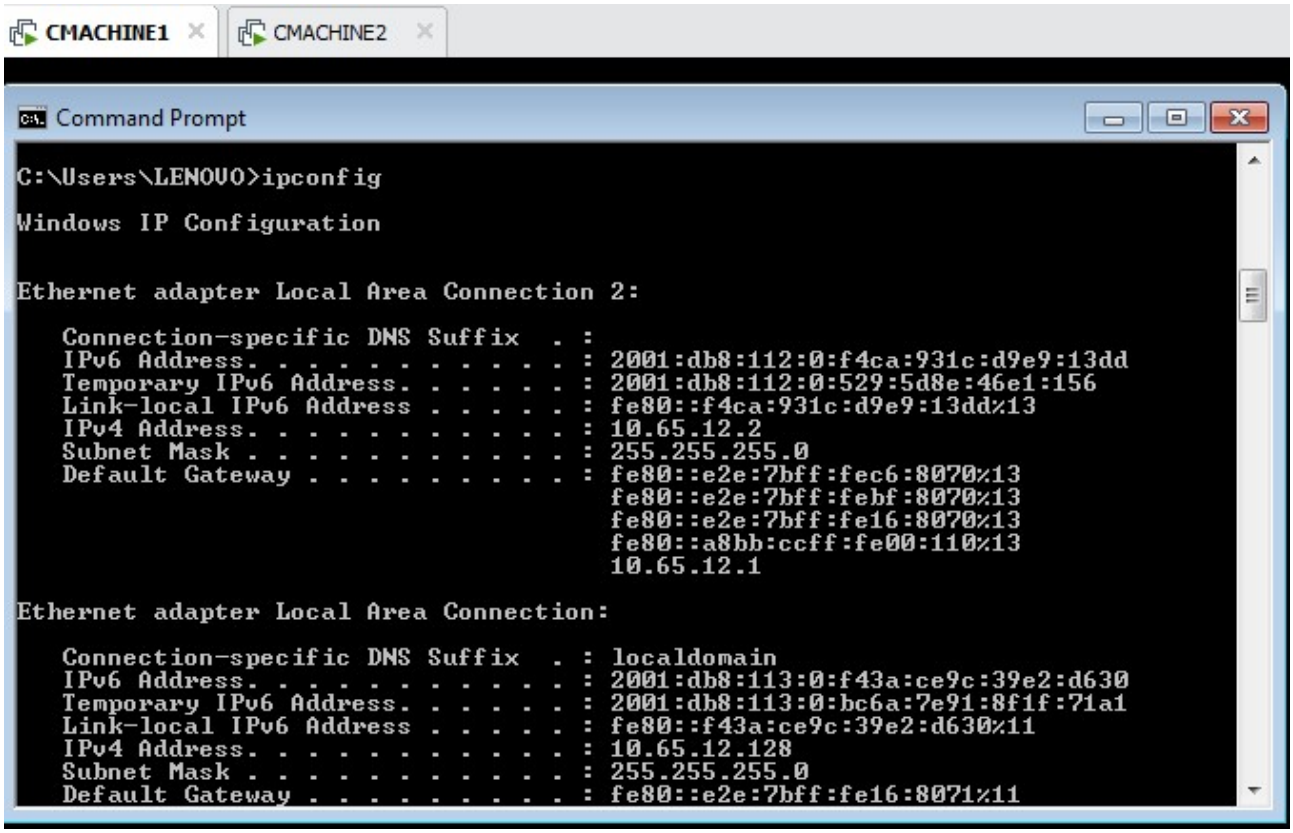

FIGURE 3.14 – Configuration d'une machine client sur VLAN 112.

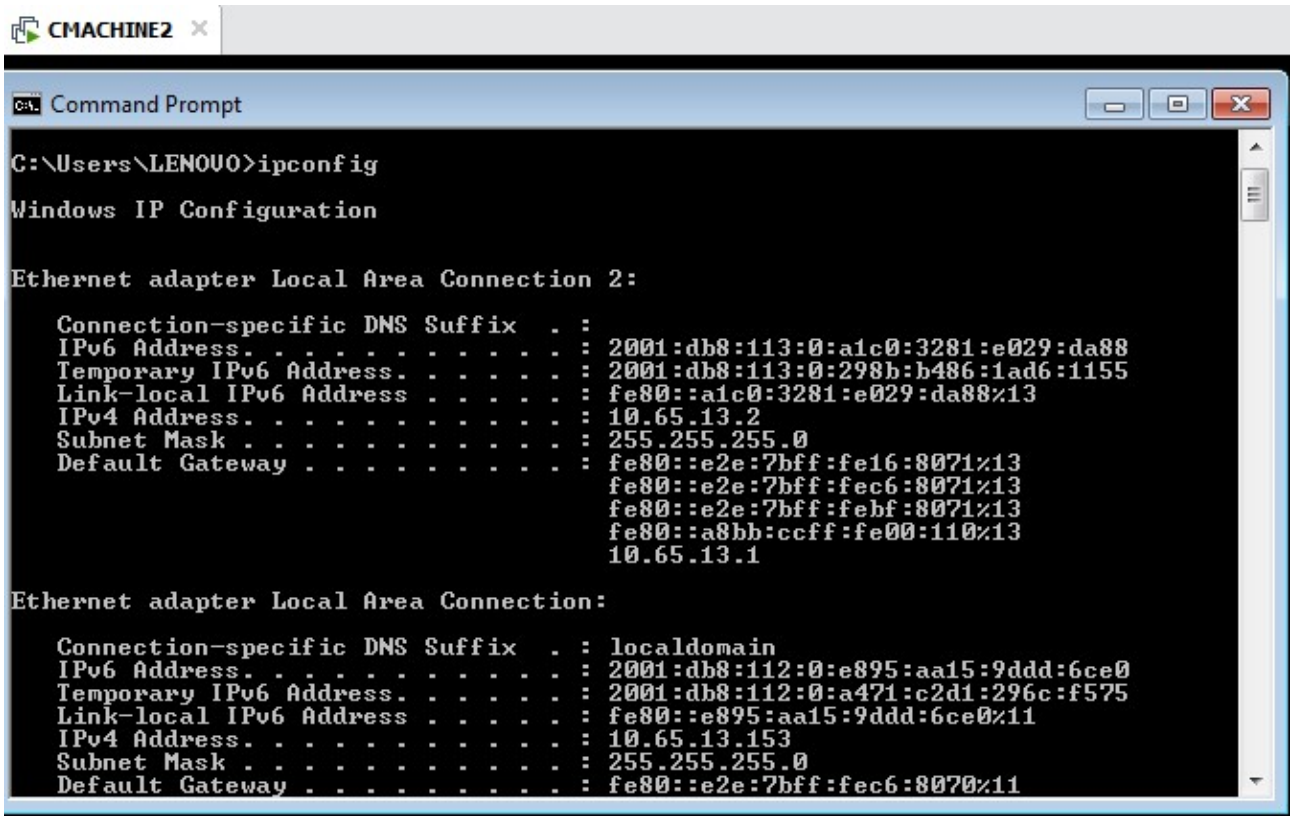

FIGURE 3.15 – Configuration d'une machine client sur VLAN 113.

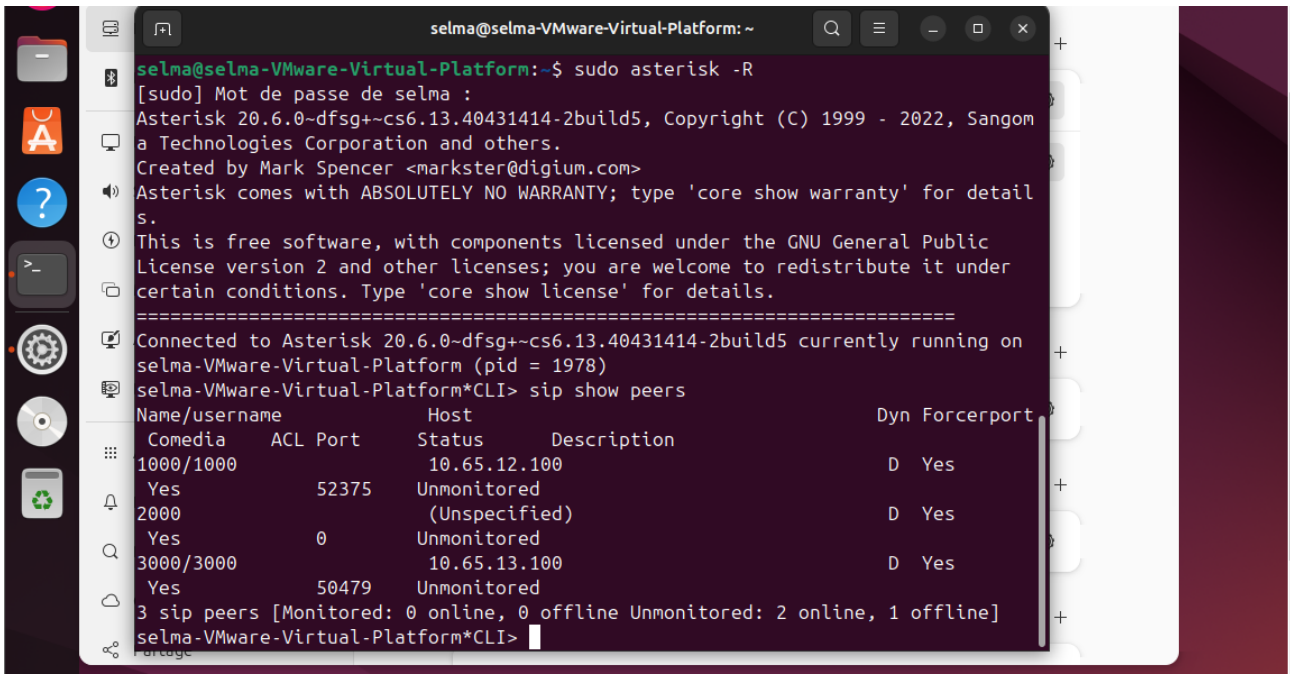

FIGURE 3.16 – Configuration des Téléphones pour la VoixIP.

Test de connectivité

Nous allons maintenant tester la connectivité entre le sous-réseau du VLAN 112 et celui du VLAN 113.

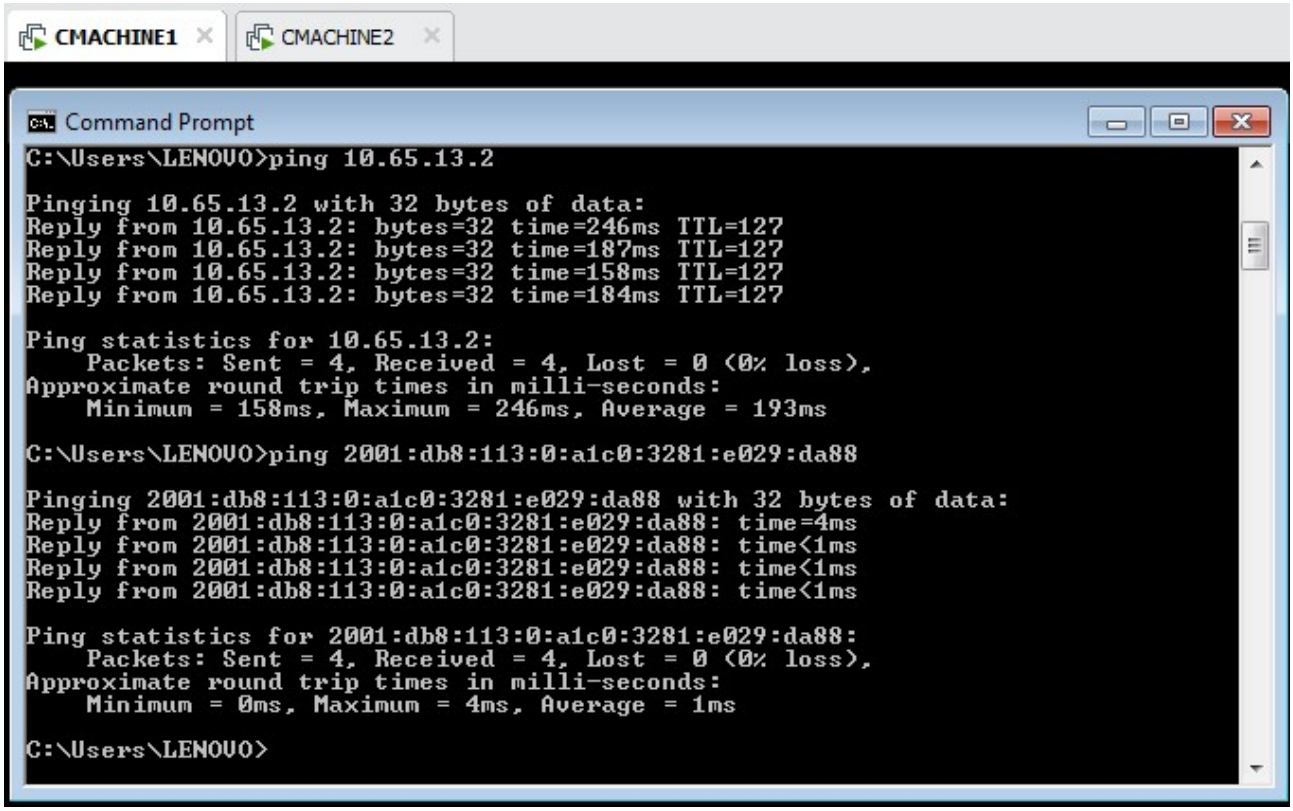

FIGURE 3.17 – Cammande Ping de la machine vlan 112 vers vlan 113

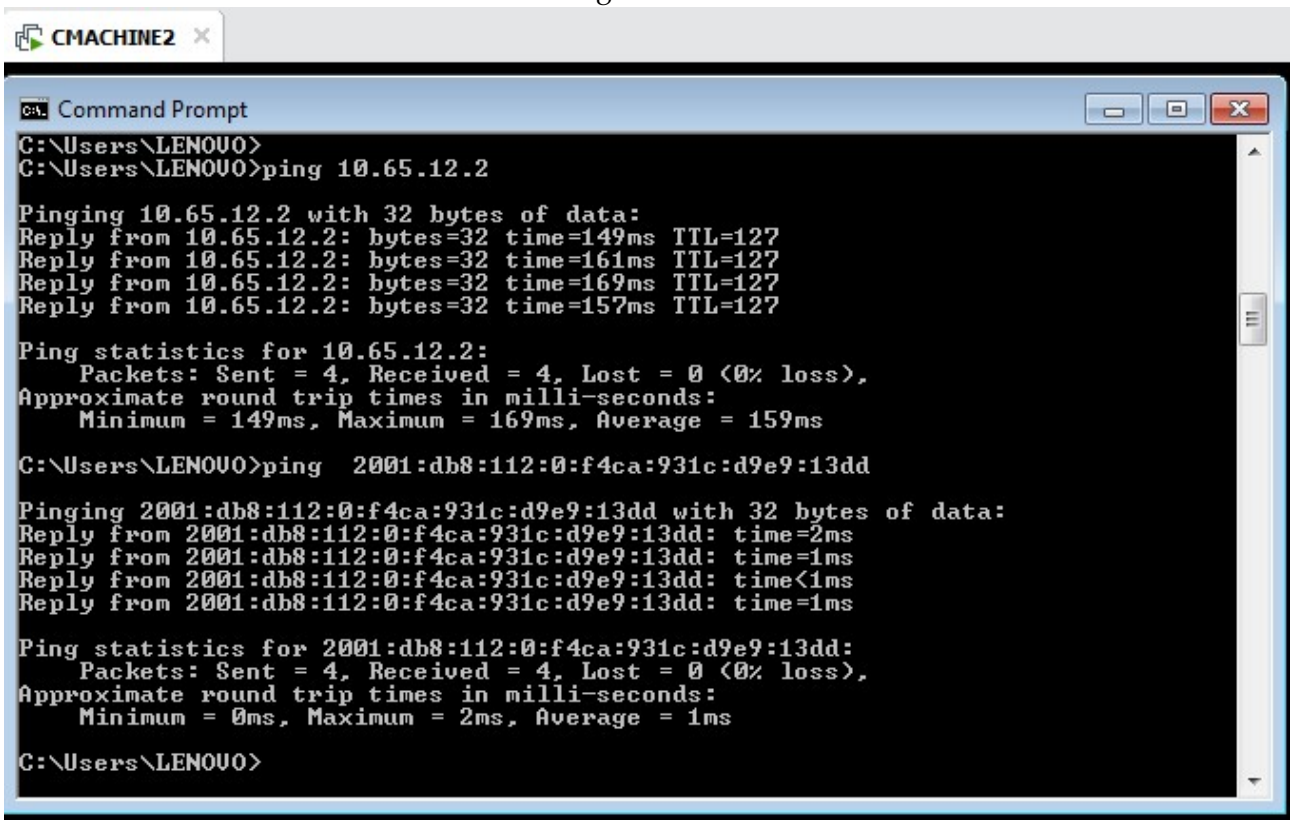

FIGURE 3.18 – Cammande Ping a partir de la machine du vlan 113 vers vlan 112

3.7 Renforcement de la sécurité du réseau : intégration de nouvelles fonctionnalités sur les équipements

3.7.1 Ajout d'une Zone DMZ

L'ajout d'une zone DMZ permet d'isoler les serveurs publics des serveurs internes, renforçant la sécurité en limitant l'accès aux services critiques et en protégeant les données sensibles du réseau.

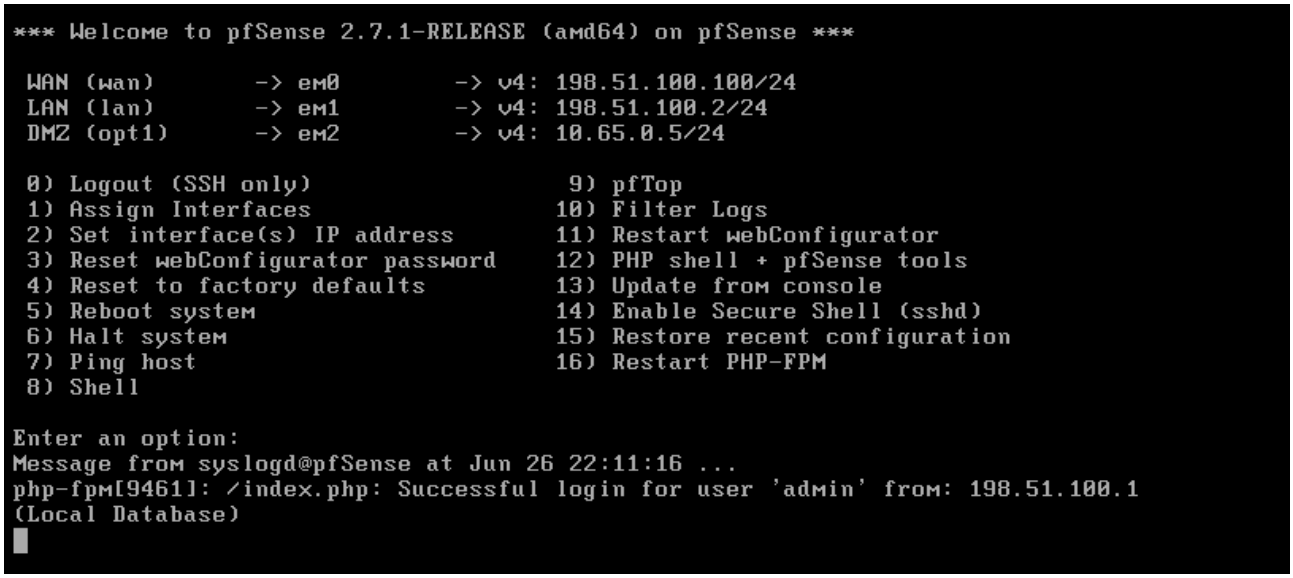

FIGURE 3.19 – Interfaces active sur pfSense.

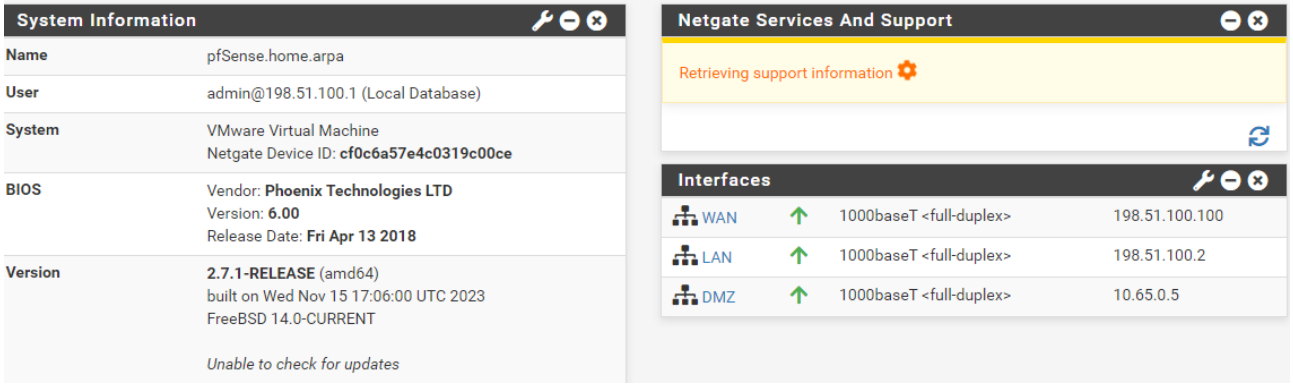

FIGURE 3.20 – Interfaces active sur pfSense.

3.7.2 Règles de filtrage configurées sur le pare-feu

Les règles de filtrage sur les interfaces Local Area Network (LAN), Wide Area Network (WAN) et DMZ dans pfSense servent à contrôler et à sécuriser le trafic réseau qui entre et sort dans un réseau.

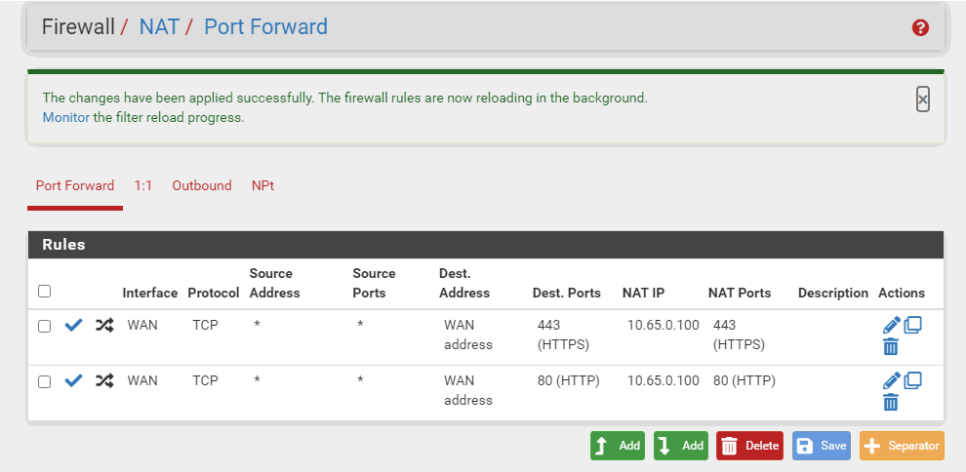

FIGURE 3.21 – Configuration de la table NAT.

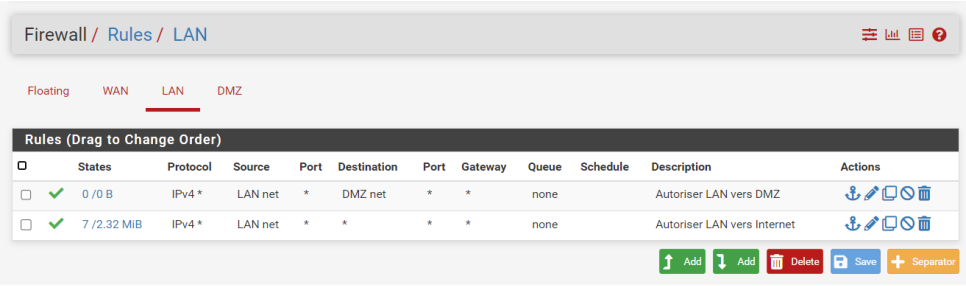

FIGURE 3.22 – Interface LAN.

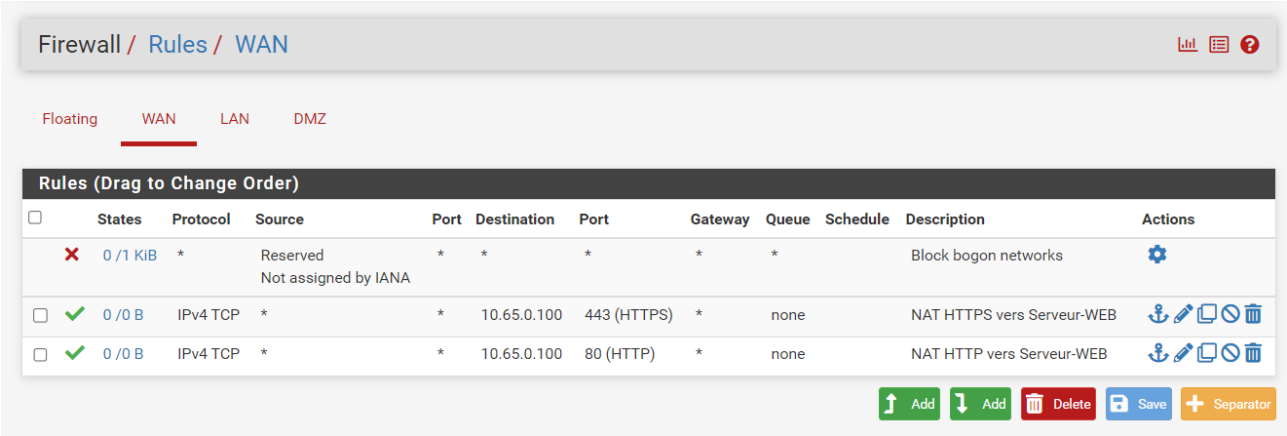

FIGURE 3.23 – Interface WAN.

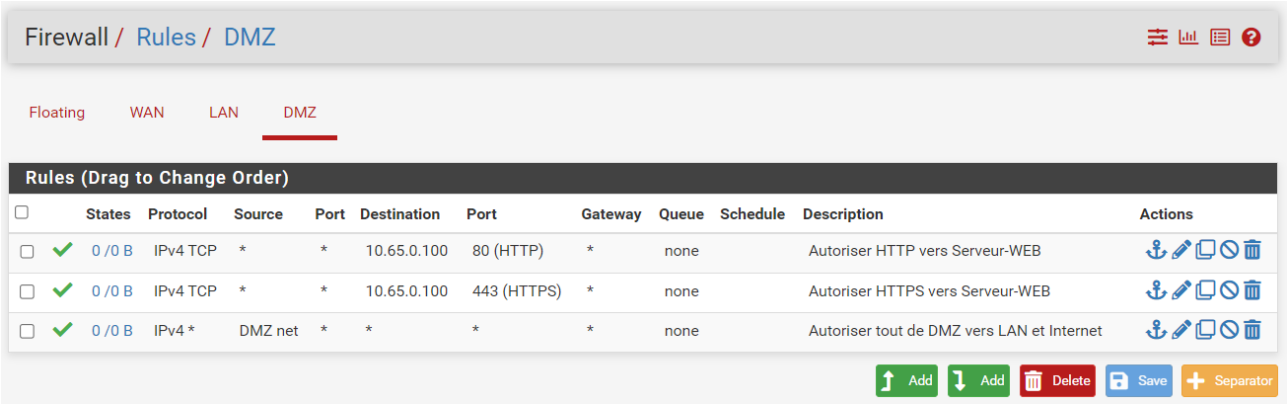

FIGURE 3.24 – Interface DMZ.

3.7.3 Configuration d'Active Directory

L'ajout d'Active Directory sur un serveur Windows 2016 permet de centraliser la gestion des utilisateurs et des ressources du réseau, facilitant ainsi l'administration et la sécurité.

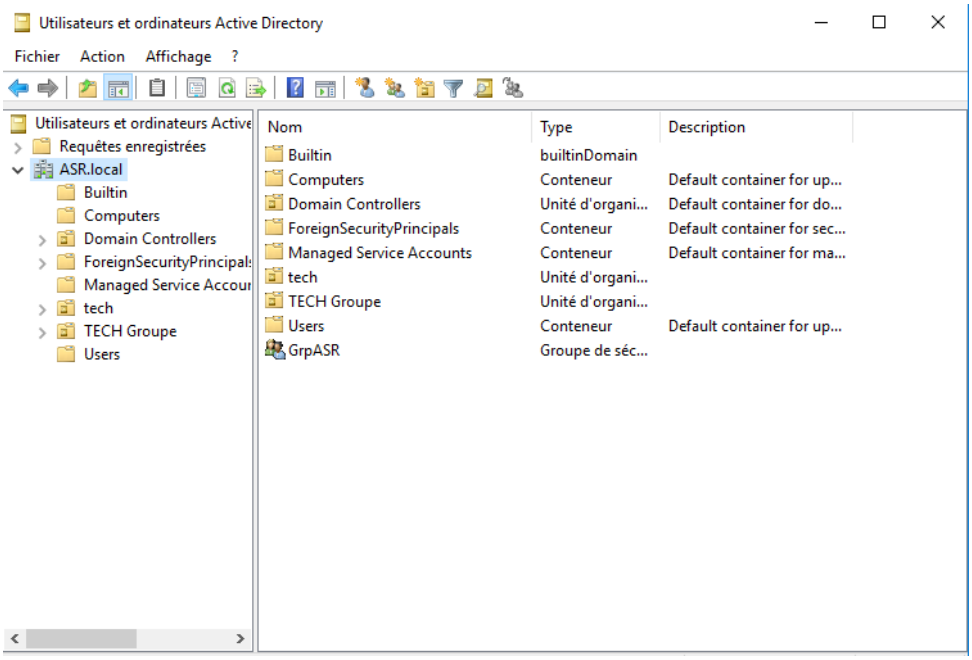

FIGURE 3.25 – Active Directory sur Serveur Windows 2016.

3.7.4 Configuration d'un DNS Local

La configuration d'un DNS local avec le domaine **ASR.local** permet de faciliter la résolution des noms de domaine à l'intérieur du réseau local, améliorant ainsi l'efficacité et la rapidité des communications internes.

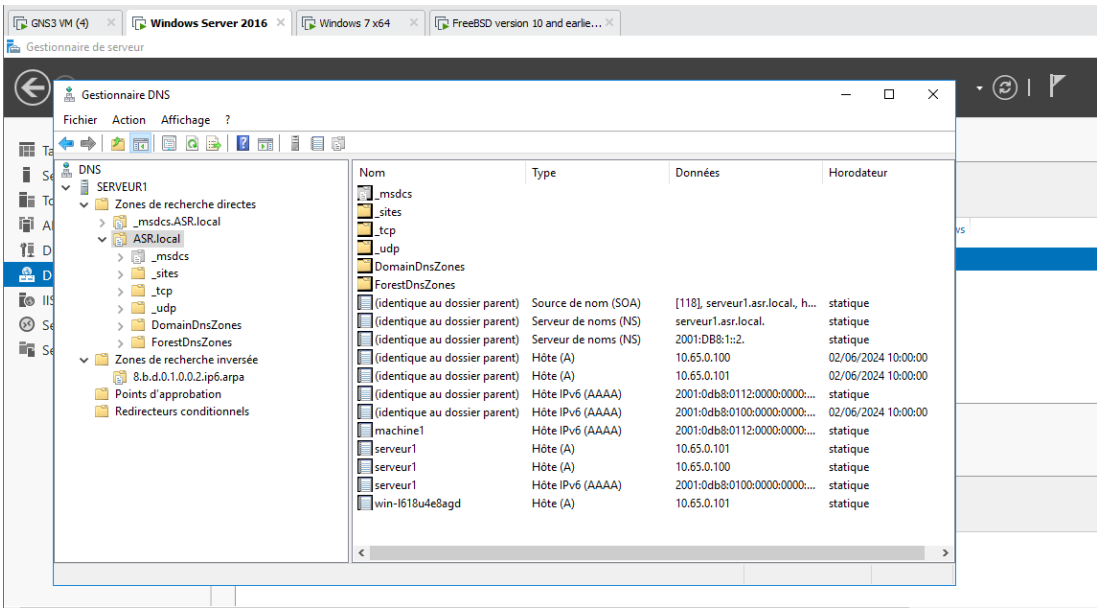

FIGURE 3.26 – DNS Local.

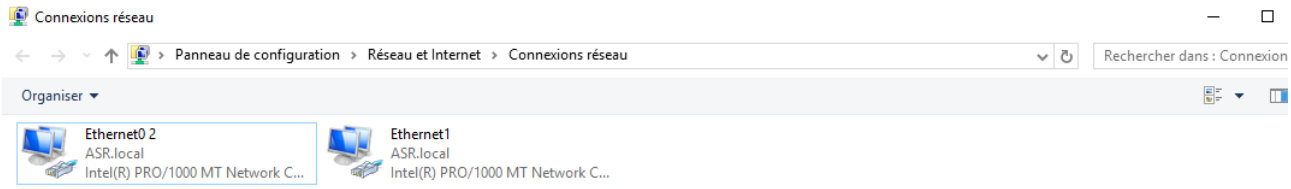

FIGURE 3.27 – DNS Local.

3.7.5 Configuration des ACLsV6

Pour sécuriser notre réseau IPv6, nous avons implémenté des listes de contrôle d'accès pour ce protocole, visant à réguler le trafic entrant et sortant sur diverses interfaces.

```
IOU4(config)#ipv6 access-list WAN-INBOUND-IPv6
IOU4(config-ipv6-acl)# permit tcp any any eq www
IOU4(config-ipv6-acl)# permit tcp any any eq 443
IOU4(config-ipv6-acl)# deny ipv6 any any log
IOU4(config-ipv6-acl)#EX
IOU4(config)#interface Ethernet0/0
IOU4(config-if)# ipv6 traffic-filter WAN-INBOUND-IPv6 in
IOU4(config-if)#EX
```

FIGURE 3.28 – Configuration des ACLsv6 sur le WAN.

```
IOU4(config)#interface E0/0.113
IOU4(config-subif)# ipv6 traffic-filter LAN-ACCESS in
IOU4(config-subif)#EX
IOU4(config)#interface E0/0.112
IOU4(config-subif)# ipv6 traffic-filter LAN-ACCESS in
IOU4(config-subif)#EX
IOU4(config)#interface E0/0.113
IOU4(config-subif)# ipv6 traffic-filter LAN-ACCESS in
IOU4(config-subif)#EX
IOU4(config)#
```

FIGURE 3.29 – Configuration des ACLsv6 sur les interfaces.

```
IOU4(config)#ipv6 access-list LAN-ACCESS
IOU4(config-ipv6-acl)#permit ipv6 2001:DB8:111::/64 2001:DB8:112::/64
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:112::/64 2001:DB8:113::/64
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:113::/64 2001:DB8:111::/64
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:111::/64 any
IOU4(config-ipv6-acl)#permit ipv6 2001:DB8:112::/64 any
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:113::/64 any
IOU4(config-ipv6-acl)#EX
```

FIGURE 3.30 – Configuration des ACLsv6 sur le LAN.

```
IOU4(config)#ipv6 access-list DMZ-ACCESS
IOU4(config-ipv6-acl)# permit tcp any host 2001:DB8::100 eq 80
IOU4(config-ipv6-acl)#permit tcp any host 2001:DB8::100 eq 443
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:111::/64 host 2001:DB8::100
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:111::/64 host 2001:DB8::101
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:112::/64 host 2001:DB8::100
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:112::/64 host 2001:DB8::101
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:113::/64 host 2001:DB8::100
IOU4(config-ipv6-acl)# permit ipv6 2001:DB8:113::/64 host 2001:DB8::101
IOU4(config-ipv6-acl)#INT E0/2
IOU4(config-if)# ipv6 traffic-filter DMZ-ACCESS in
IOU4(config-if)#EXIT
```

FIGURE 3.31 – Configuration des ACLsv6 sur la DMZ.

3.8 Analyse des menaces : identifier les attaques potentielles sur le réseau

Écoute des Appels sur le réseau (voixIp)

1. **Interception de l'Audio :** Les données audio des appels VoIP peuvent être capturées en interceptant les paquets de données sur le réseau. Ces paquets contiennent les fragments de la conversation en cours.
2. **Enregistrement de l'Appel :** Une fois interceptées, les données audio peuvent être enregistrées par l'attaquant. Cet enregistrement permet de conserver la conversation pour un accès futur et le réécouté. Cela permet à l'attaquant de récupérer des informations sensibles échangées lors de la conversation, compromettant ainsi la confidentialité de la communication.

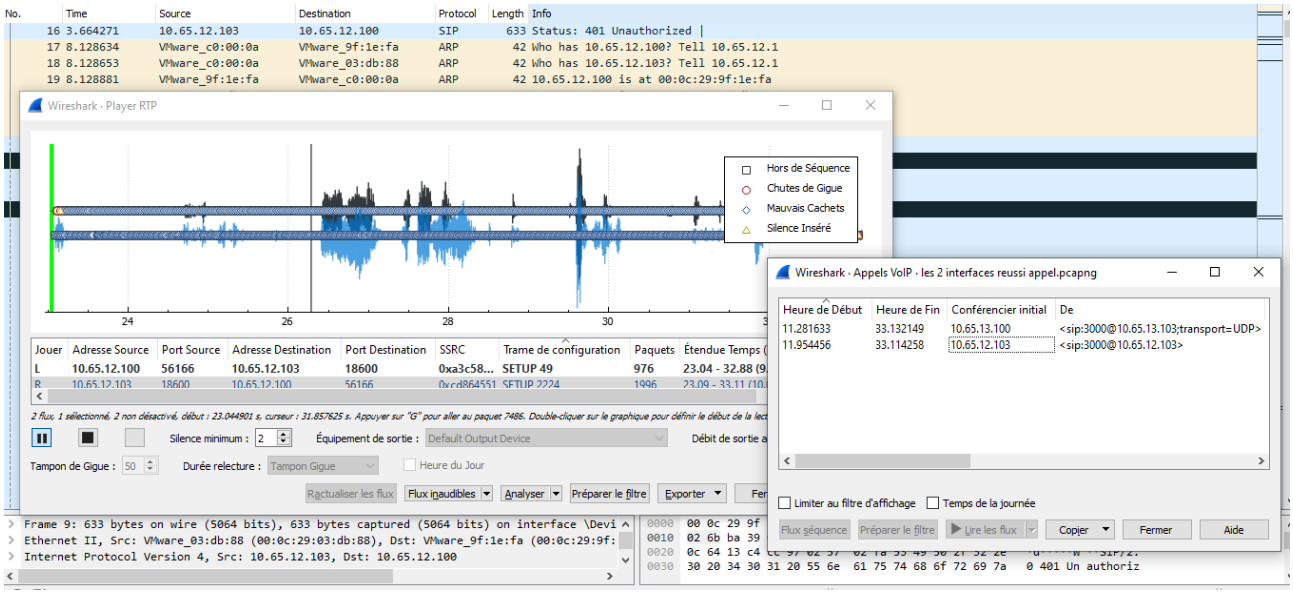

FIGURE 3.32 – Attaque sur la voixIP.

Attaque Bombardement par des paquets SIP (inviteflood) : L'attaque de bombardement par des paquets SIP consiste à envoyer un grand nombre de requêtes SIP INVITE à un serveur cible. Cette méthode vise à surcharger le serveur, provoquant un déni de service (DoS).

```
┌──(root㉿kali)-[/home/kali]
└─# inviteflood eth0 1000 10.65.12.50 10.65.12.103 70707070

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port    = 10.65.12.129:9
dest   IPv4 addr:port    = 10.65.12.103:5060
targeted UA              = 1000@10.65.12.50

Flooding destination with 70707070 packets
sent: 1229389
```

FIGURE 3.33 – Attaque Bombardement par des paquets SIP.

Attaque Bruteforce sur les mots de passe SIP (svcrack) : L'attaque de bruteforce sur les mots de passe SIP (Session Initiation Protocol) consiste à essayer toutes les combinaisons possibles de noms d'utilisateur et de mots de passe jusqu'à ce que l'une d'elles soit correcte. Cette méthode exploite la faiblesse des mots de passe peu sécurisés.

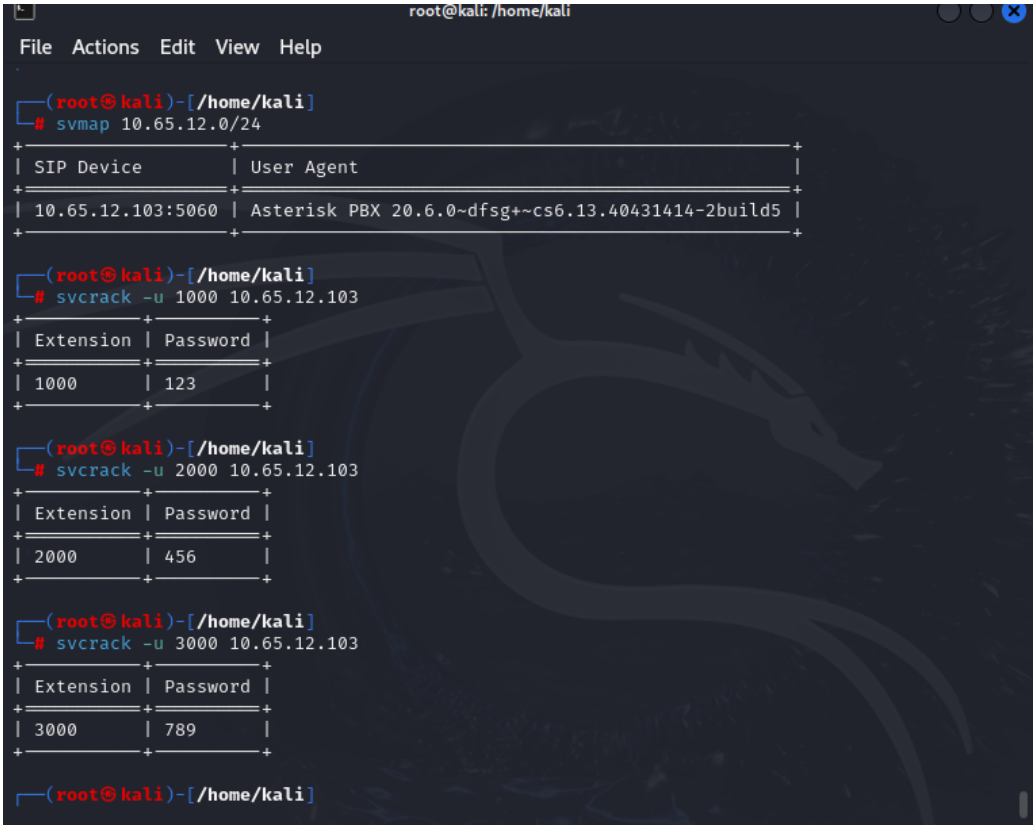

FIGURE 3.34 – Attaque Bruteforce.

3.9 Stratégies proposées pour l'élimination des menaces et des attaques potentielles

- Pour sécurisé les appels par voix ip, nous proposant le protocole :

Transport Layer Security (TLS)

Est un protocole de sécurité utilisé pour chiffrer les communications sur les réseaux. Lorsqu'il est appliqué au SIP, il garantit la confidentialité, l'intégrité et l'authentification des messages SIP.

- Pour prévenir toutes sorte d'attaques, nous proposons une solution basée sur pfSense et les systèmes de prévention et détection d'intrusion (IPS/IDS).

Systèmes de Détection et de Prévention d'Intrusion (IDS/IPS)

IDS (Intrusion Detection System)

Un IDS surveille le trafic réseau en temps réel pour détecter des activités suspectes ou malveillantes. Il analyse les paquets de données, compare le trafic avec une base de signatures d'attaques connues, et alerte les administrateurs en cas de détection d'anomalies.

IPS (Intrusion Prevention System)

Un IPS offre les mêmes fonctionnalités de détection qu'un IDS, mais va plus loin en prenant des mesures pour bloquer ou prévenir les activités malveillantes. Lorsqu'une menace est détectée, l'IPS peut automatiquement bloquer le trafic suspect.

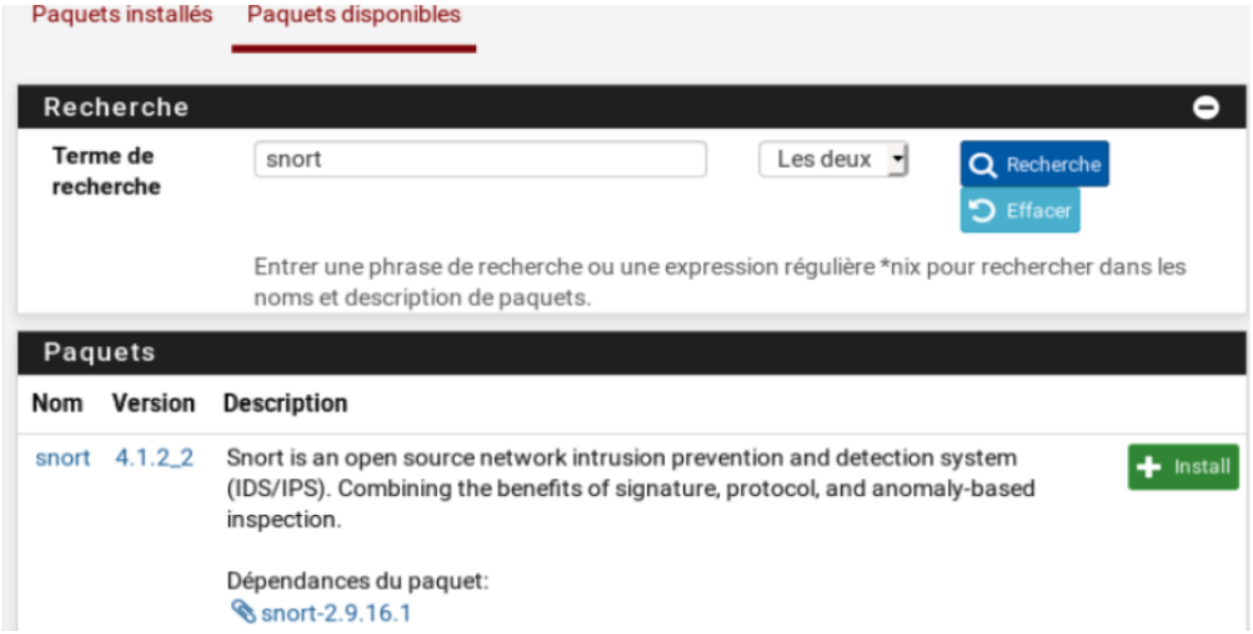

FIGURE 3.35 – Installation de Snort.

Implémentation de Snort sur pfSense

pfSense supporte l'installation de plusieurs packages IDS/IPS, parmi lesquels Snort et Suricata sont les plus populaires.

la figure suivante illustre les interfaces activées pour la détection des intrusions :

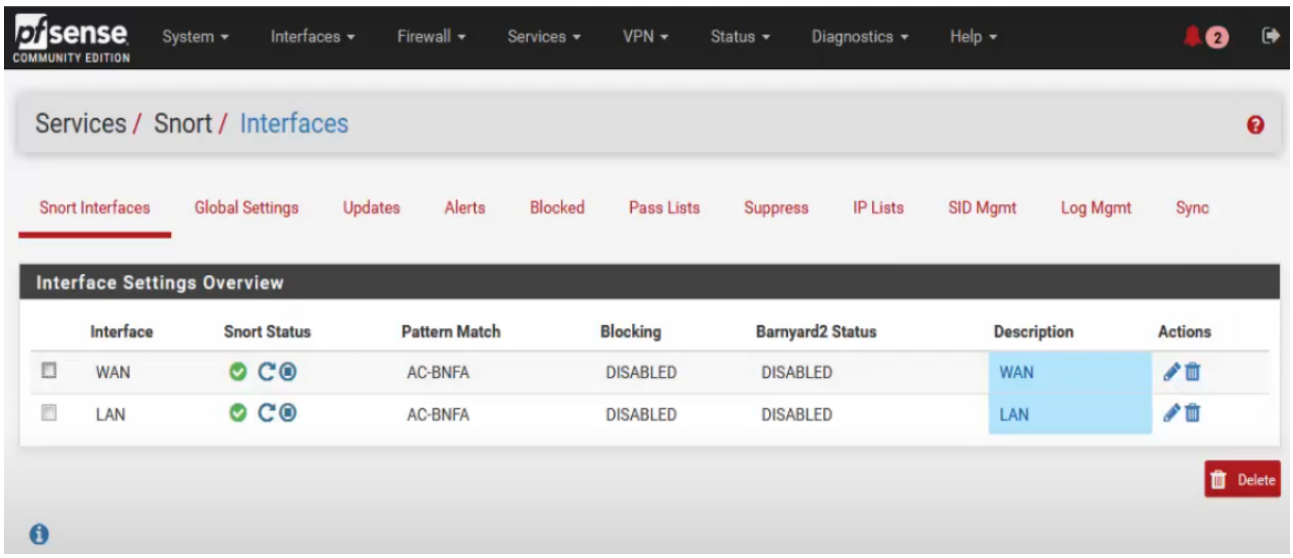

FIGURE 3.36 – Interfaces du Snort.

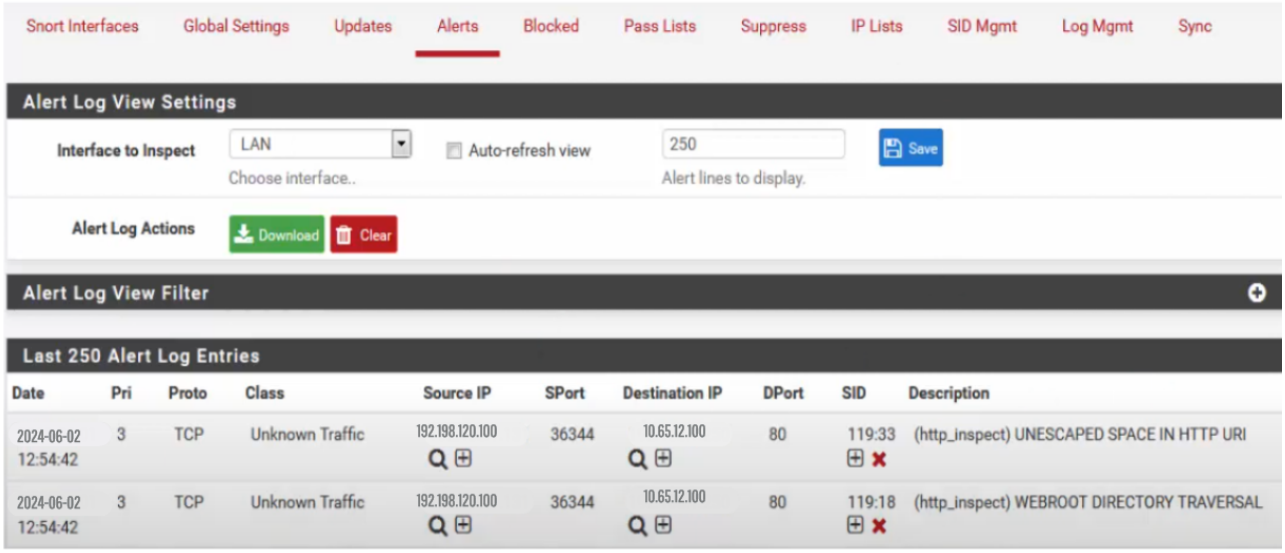

FIGURE 3.37 – Exemple d'alerte Snort.

3.10 Conclusion

L'objectif de ce chapitre était de renforcer la sécurité du réseau local de la CDB. Pour y parvenir, nous avons analysé ses vulnérabilités et évalué sa résilience. Afin de combler les lacunes sécuritaires, nous avons révisé l'architecture réseau en intégrant un pare-feu configuré et supervisé par l'interface pfSense, combiné aux fonctionnalités IDS/IPS de Snort, et en isolant les serveurs web du LAN pour créer une DMZ. De plus, nous avons implémenté le chiffrement RSA via le protocole SSH pour sécuriser les données en transit. Des tests ont été menés pour valider ces améliorations, avec des résultats satisfaisants. Tout en déployant efficacement la transition IPv6 au sein de leur organisation, en choisissant les techniques les plus adaptées à leur contexte.

CONCLUSION GÉNÉRALE

La migration d'IPv4 vers IPv6 est une étape cruciale pour garantir la croissance durable des réseaux et répondre à la pénurie croissante d'adresses IP. Le protocole IPv6 offre des solutions essentielles en termes de capacité d'adressage, de performance et de sécurité .

Cependant, la transition comporte des défis importants en raison de l'incompatibilité directe entre les deux protocoles. Une approche stratégique et méthodique est essentielle, impliquant une planification minutieuse, la sensibilisation du personnel et l'adoption de bonnes pratiques de sécurité .

Les mécanismes de transition tels que le tunneling ISATAP, le dual stack et les tunnels 6to4 jouent un rôle crucial pour faciliter cette transition en douceur . L'utilisation intensive de protocoles de sécurité comme les IDS, IPS et les pare-feu configurés avec des ACLs renforcent également la sécurité du réseau IPv6 .

L'étude pratique menée à Sonelgaz a démontré avec succès l'application concrète de ces principes, illustrant qu'une migration efficace est réalisable grâce à une planification rigoureuse et à l'adoption des meilleures pratiques .

Bien que la transition vers IPv6 comporte des défis, elle demeure essentielle pour répondre à la demande croissante en adressage IP et soutenir l'expansion continue d'Internet. Une approche proactive et collaborative entre les acteurs de l'industrie est cruciale pour surmonter ces défis et exploiter pleinement les avantages offerts par IPv6 .

BIBLIOGRAPHIE

[1] PÉREZ André. *Les technologies IPv4 et IPv6 : protocoles et transitions*. Lavoisier, 2012.

[2] Jean-Paul Archier. *IPv6 : Principes et mise en œuvre*. Maison d'édition, 2012.

[3] CCNA Réponses (Fictif). Introduction aux réseaux - modules 1&2 : Adressage ipv6. https://ccnareponses.com/introduction-aux-reseaux-modules-12-adressage-ipv6/. Consulté le 18 avril 2024.

[4] Cisco. Adressage ipv4. https://cisco.goffinet.org/ccna/ipv4/adressage-ipv4/, 2020.

[5] CityPassenger. *Un contrôleur WiFi, c'est quoi et à quoi ça sert ?*, 2024. https://citypassenger.com/un-controleur-wifi-cest-quoi-et-a-quoi-ca-sert/.

[6] FS Community. What is dhcp snooping and how it works. *FS Community*, n.d. https://community.fs.com/fr/article/what-is-dhcp-snooping-and-how-it-works.html.

[7] H. Dawood. Ipv6 security vulnerabilities. *International Journal of Information Security Science*, 2012. https://dergipark.org.tr/en/pub/ijiss/issue/16066/167874#article_cite.

[8] Simon Dunand. Publication de services web ipv4 sur internet ipv6, 2012. https://www.stephan-robert.ch/wp-content/uploads/2015/07/Rapport-Final-S-DUNAND.pdf.

[9] Dunod. *Aide-mémoire Réseaux et télécoms(Claude Servin)*.

[10] Marfall N'Diaga Fall. Sécurisation formelle et optimisée de réseaux informatiques. Mémoire de maîtrise, Université Laval, Québec, octobre 2010. http://central.bac-lac.gc.ca/.redirect?app=laccat&id=716957890&lang=fra.

[11] Fortinet. Snort - cyber glossary. https://www.fortinet.com/fr/resources/cyberglossary/snort.

[12] G6 Asso. *Protocole de Découverte des Voisins*, s.d. https://livre.g6.asso.fr.

[13] GeeksforGeeks. What is rogue dhcp server attack? *GeeksforGeeks*, n.d. https://www.geeksforgeeks.org/what-is-rogue-dhcp-server-attack/.

[14] GNS3 Documentation. *Getting Started with GNS3*. GNS3, 2024. https://docs.gns3.com/docs/.

[15] François Goffinet. https://www.scribd.com/document/170031503/Rsx-OSI-TCPIP-cours-pdf.

[16] Silvia Hagen. *IPv6 Essentials : Integrating IPv6 into Your IPv4 Network*. O'Reilly Media, 3rd edition, 2014.

[17] Christian Huitema. *IPv6 : The New Internet Protocol*. Prentice Hall, 2nd edition, 1997. https://www.pearson.com/store/p/ipv6-the-new-internet-protocol/P100000203258.

[18] IA. *IA Perplexity*, n.d. https://www.perplexity.ai/ 01/05/2024.

[19] Ibm ipv6 address formats. https://www.ibm.com/docs/fr/i/7.5?topic=concepts-ipv6-address-formats.

[20] Comparaison entre ipv4 et ipv6. https://www.ibm.com/docs/fr/i/7.5?topic=6-comparison-ipv4-ipv6.

[21] Mohammed Amine Ait Lafkih and Ahmed Mousayer. Stratégies de migration d'ipv4 vers ipv6. Rapport de projet, 2018. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.academia.edu{STRATGIESDEMIGRATIOND'IPv4VERSIPv6.},.

[22] Cédric Llorens, Laurent Levier, and Denis Valois. *Tableaux de bord de la sécurité réseau*. Groupe Eyrolles, 3 edition, 2010. https://www.eyrolles.com/download/9782212128215/Llorens-web.pdf.

[23] Shannon McFarland, Muninder Sambi, Nikhil Sharma, and Sanjay Hooda. *IPv6 pour les réseaux d'entreprise*. Cisco Press, 800 East 96th Street Indianapolis, IN 46240 États-Unis, 2011. https://www.ciscopress.com/store/ipv6-for-enterprise-networks-9780132731980Copyright © 2011 Cisco Systems, Inc. Tous droits réservés.

[24] Netgate. *pfSense Documentation*. https://docs.netgate.com/pfsense/en/latest/.

[25] Juniper Networks. *What is IPv4 vs IPv6?*, n.d. https://www.juniper.net/fr/fr/research-topics/what-is-ipv4-vs-ipv6.html.

[26] Asterisk Project. *Asterisk Documentation*, 2024. url https ://docs.asterisk.org/Getting-Started/.

[27] Guy Pujolle. *Les Réseaux*. Eyrolles, 5ème edition, 2009.

[28] RSX - OSI TCP/IP cours. Rsx - osi tcp/ip cours. https://fr.scribd.com/document/309697340/Rsx-OSI-TCPIP-cours.

[29] Scribd. Expose-2-protocole-ipv4, 2022. https://fr.scribd.com/document/490923896/Expose-2-Protocole-IPv4.

[30] Techno Skills. Le balayage (scanning) : Le guide complet. https://techno-skills.com/securite/cyber-securite-ethical-hacking/le-balayage-scanning/.

[31] TechTarget. Tcp/ip. https://www.techtarget.com/searchnetworking/definition/TCP-IP.

[32] VMware, Inc. *VMware Workstation 16.2.2*, 2024. https://www.vmware.com/products/workstation-pro.html.

[33] WatchGuard (Fictif). *Configurer le serveur DHCPv6*. https://www.watchguard.com/help/docs/fireware/12/fr-FR/Content/fr-FR/networksetup/ipv6_dhcp_server_c.html, urldate = 2024-03-23.

[34] Wireshark Foundation. *Wireshark User's Guide*, 2024. https://www.wireshark.org/docs/.

RÉSUMÉ

Ce mémoire explore la transition de l'Internet Protocol version 4 (IPv4) vers l'Internet Protocol version 6 (IPv6) afin de répondre à la croissance des dispositifs connectés et à l'épuisement des adresses IPv4. L'étude analyse les défis et opportunités liés à cette migration, en mettant en évidence les avantages d'IPv6, tels qu'un espace d'adressage élargi, des améliorations de sécurité avec IPsec intégré et des fonctionnalités avancées d'auto-configuration. En examinant les protocoles de transition comme Dual Stack et Tunneling, ainsi que les impacts économiques et techniques, ce mémoire démontre que malgré les défis initiaux, les bénéfices à long terme de l'adoption d'IPv6 surpassent largement les obstacles. Une planification rigoureuse et des stratégies de formation sont essentielles pour une transition fluide, assurant ainsi la durabilité et l'efficacité du réseau Internet.

Mots clés : IPv4 , IPv6 , Migration Transition , Dual Stack , Tunneling , Translation .

ABSTRACT

This thesis explores the transition from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6) in response to the growth of connected devices and the depletion of IPv4 addresses. The study analyzes the challenges and opportunities associated with this migration, highlighting the advantages of IPv6 such as expanded address space, enhanced security with integrated IPsec, and advanced auto-configuration capabilities. By examining transition protocols like Dual Stack and Tunneling, as well as economic and technical impacts, this thesis demonstrates that despite initial challenges, the long-term benefits of adopting IPv6 outweigh the obstacles. Rigorous planning and training strategies are crucial for a smooth transition, ensuring the sustainability and efficiency of the Internet network.

Mots clés : IPv4 , IPv6 , Migration Transition , Dual Stack , Tunneling , Translation .