RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 55 02 80 70
https://www.ifri-uac.bj Courriel : contact@ifri.uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Anifath Rèmilèkoun **AMIDOU**

Déploiement sécurisé de l'IPv6 au sein de ISOCEL Telecom: Stratégies de migration et de défense contre les menaces

Sous la supervision :
Ing, M. Victor **OYETOLA**

Membres du jury :

Eugène C. EZIN	Professeur	IFRI-UAC	Président
Abousidikou ODJO	Ingénieur	IFRI-UAC	Examinateur

Année Académique : **2023-2024**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux vii

Liste des acronymes viii

Introduction générale 1

1 Revue de littérature 3

2 Conception et Déploiement 17

3 Résultats et Discussions 35

Conclusion générale et perspectives 42

Bibliographie 43

Webographie 44

Table des matières 46

Dédicace

A ma mère Taibath **KOSSI**,
A mon père Mouftaou **AMIDOU**,
A tous mes frères, sœurs et proches.

Remerciements

Nous tenons tout d'abord à rendre grâce à Dieu pour la bénédiction ainsi que la miséricorde qui nous ont permis de bien terminer.

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui nous voudrons témoigner toute notre reconnaissance. Nous remercions sincèrement :

- Le Professeur Eugène C. EZIN, Directeur de l'Institut de Formation et de Recherche en Informatique, pour ses conseils et son encouragement ;
- Le Professeur Gaston EDAH , le Directeur Adjoint de notre institut ;
- M. Victor OYETOLA, notre maitre de mémoire pour l'encadrement ;
- M. Joey ESQUIBAL. Directeur du système d'Information d'ISOCEL Telecom, pour avoir accepté notre stage ;
- Toute l'administration de l'IFRI ;
- Tous les membres de ISOCEL Telecom qui nous ont soutenu ;
- Tous ceux qui de près ou de loin nous ont apporté leur soutien sous quelque forme que ce soit.

Résumé

Ce mémoire porte sur le déploiement sécurisé de l'IPv6 au sein d'ISOCEL Telecom, en mettant l'accent sur les stratégies de migration et les mécanismes de défense contre les menaces potentielles. La transition vers l'IPv6 est aujourd'hui une nécessité pour les entreprises face à l'épuisement des adresses IPv4. Ce projet a donc consisté à implémenter une architecture Dual-Stack, permettant la coexistence des deux protocoles, tout en assurant une connectivité fluide et sécurisée.

L'étude aborde les défis de migration en analysant les différentes étapes de conception et de configuration du réseau, depuis l'adressage jusqu'à la mise en place des mécanismes de sécurité. Des technologies comme les ACLs, la protection du Neighbor Discovery Protocol (NDP) et la gestion des Neighbor Binding Table ont été intégrées pour renforcer la sécurité du réseau IPv6. Des tests de connectivité ont été réalisés pour vérifier le bon fonctionnement des configurations et garantir une communication entre les nœuds du réseau.

Malgré certaines limitations techniques liées aux outils de simulation, le projet a permis de poser les bases d'un déploiement sécurisé d'IPv6 chez ISOCEL Telecom, en offrant des solutions de protection adaptées à l'évolution du trafic et des menaces. Cette étude constitue une étape importante vers une migration complète et maîtrisée vers l'IPv6.

Mots clés : IPv6, sécurité réseau, migration, dual-stack, ISOCEL Telecom, ACLs, NDP, Neighbor Binding Table.

Abstract

This thesis focuses on the secure deployment of IPv6 at ISOCEL Telecom, emphasizing migration strategies and defense mechanisms against potential threats. The transition to IPv6 is now essential for companies facing the exhaustion of IPv4 addresses. This project involved implementing a dual-stack architecture, enabling the coexistence of both protocols while ensuring seamless and secure connectivity.

The study addresses migration challenges by analyzing the various steps of network design and configuration, from addressing to implementing security mechanisms. Technologies such as ACLs, Neighbor Discovery Protocol (NDP) protection, and Neighbor Binding Table management were integrated to strengthen IPv6 network security. Connectivity tests were conducted to verify the proper functioning of the configurations and ensure communication between the network nodes.

Despite some technical limitations related to simulation tools, the project established the foundation for a secure IPv6 deployment at ISOCEL Telecom, offering protection solutions suited to the evolving traffic and threats. This study is a key step toward a complete and controlled migration to IPv6.

Key words: IPv6, network security, migration, dual-stack, ISOCEL Telecom, ACLs, NDP, Neighbor Binding Table.

Table des figures

1.1 Paquet capturé avec Wireshark 4
1.2 Format d'une adresse IPv6 9
1.3 Entête IPV4 vs Entête IPV6 13
1.4 Principe de fonctionnement du Tunelling 14

2.1 Architecture du réseau de ISOCEL Telecom 17
2.2 Réseau adressé en IPv4. 19
2.3 Configuration OSPF sur RC3 21
2.4 Extrait de la base de données OSPF sur RC3. 22
2.5 Table de routage OSPF sur RC3. 23
2.6 Configuration BGP sur RE1. 24
2.7 Configuration BGP sur RC3. 25
2.8 Configuration BGP sur R1. 26
2.9 Table de routage BGP sur R1. 26
2.10 Adresse IPv6 de l'interface Ethernet0/1 27
2.11 Base de données OSPFv3 sur RC1 28
2.12 Table de routage ospfv3 sur RC1 29
2.13 Configuration BGPv6 sur RC3 30
2.14 Table de routage BGPv6 sur RC3 31
2.15 ACL Implémentés sur R1 sur les interfaces Ethernet 0/0 et Ethernet 0.2 32

3.1 Pingtest PC1-RE1 36
3.2 Pingtest PC1-RC3 36
3.3 Pingtest PC1-RC3 37
3.4 Pingtest Google DNS 37
3.5 Pingtest PC2-RE1 38
3.6 Pingtest PC2-RC3 38
3.7 Pingtest PC2-R1 38
3.8 PC1 vers RC3 39
3.9 Pingtest PC1 vers RC3 40
3.10 Action de l'ACL 40

Liste des tableaux

1.1 Adresses réservées 6
1.2 IPv4 vs IPv6 11

2.1 Illustration du plan d'adressage IPv6. 18
2.2 Adresses de loopback utilisées 21

Liste des acronymes

ACL : Access Control List 31,

CIDR : Classless Inter-Domain Routing 7,

IANA : Internet Assigned Numbers Authority) 4,
IoT : Internet of Things 5,
IPSec : Internet Protocol Security 10,
IPv4 : Internet Protocol version 4 4,
IPv6 : Internet Protocol version 6 8,

MTU : Maximum Transmission Unit 10,

NAT : Network Address Translation 7,
NDP : Neighbor Discovery Protocol 31,

SLAAC : Stateless Address Autoconfiguration

TCP : Transmission Control Protocol 4,
TTL : Time To Live 10,

UDP : User Datagram Protocol 4,

VLSM : Variable Length Subnet Masking 7,
VPN : Virtual Private Network.

Introduction générale

Dans un monde où la connectivité joue un rôle essentiel dans notre vie quotidienne, la transition vers la technologie IPv6 est devenue une priorité pour les entreprises de télécommunications. L'épuisement des adresses IPv4 et l'augmentation exponentielle du nombre d'appareils connectés nécessitent une infrastructure réseau capable de répondre aux besoins actuels et futurs. La technologie IPv6 offre une solution robuste avec un espace d'adressage presque illimité, permettant de soutenir l'expansion des services numériques. ISOCEL Telecom s'engage à déployer IPv6 au sein de son réseau pour améliorer la performance, la sécurité et la fiabilité de ses services, tout en assurant une connectivité continue pour ses clients. Ce déploiement marque une étape cruciale dans l'évolution de son infrastructure et son engagement envers l'innovation technologique.

Problématique

Face à l'épuisement des adresses IPv4 et à la croissance continue des appareils connectés, ISOCEL Telecom doit impérativement migrer vers le protocole IPv6 pour garantir la continuité et la sécurité de ses services. Toutefois, cette migration soulève plusieurs défis techniques et sécuritaires. Comment ISOCEL Telecom peut-elle déployer IPv6 de manière sécurisée tout en assurant une transition fluide pour ses clients ? Quelles stratégies de défense doivent être mises en place pour se prémunir contre les nouvelles menaces inhérentes à ce protocole ?

Contexte et justification

Dans un contexte où l'épuisement des adresses IPv4 et la croissance rapide des appareils connectés nécessitent une infrastructure plus performante, le passage à IPv6 s'impose pour garantir l'avenir des réseaux. Pour ISOCEL Telecom, cette transition est cruciale afin d'assurer la continuité des services tout en améliorant la performance, la sécurité, et la fiabilité de son infrastructure. La justification de ce mémoire repose sur l'importance d'une migration sécurisée vers IPv6. Bien que ce protocole offre des avantages significatifs, il présente aussi des risques spécifiques, comme de nouvelles menaces et vulnérabilités. Ce travail vise donc à explorer des stratégies pour une transition fluide et sécurisée tout en renforçant la défense contre les menaces associées, garantissant ainsi à ISOCEL Telecom une migration réussie sans impact négatif pour ses utilisateurs.

Objectifs

Objectif général

L'objectif global de notre projet est de mettre en œuvre l'architecture IPv6 au sein de la société ISOCEL SA.

Objectifs spécifiques

Il s'agit spécifiquement de :

- **Garantir une connectivité transparente** : garantir que tous les appareils et services de l'entreprise peuvent communiquer de manière transparente, quel que soit le protocole.
- **Soutenir la croissance future** : garantir que l'infrastructure réseau de l'entreprise est prête à prendre en charge la croissance future du nombre d'appareils connectés et de services proposés en adoptant IPv6, qui fournit un espace d'adressage plus grand.
- **Sécurité améliorée** : utilisez les fonctionnalités de sécurité améliorées d'IPv6 pour renforcer la sécurité du réseau d'entreprise, notamment l'authentification et le cryptage des communications. Cela peut conduire à une réduction des coûts associés à la mise en œuvre et à la gestion des solutions de sécurité supplémentaires nécessaires pour IPv4.

Présentation de ISOCEL Telecom

ISOCEL Telecom est un fournisseur d'accès fixe à Internet à très haut débit et services IP utilisant des technologies filaires et sans fil comme la fibre optique, la Boucle Locale Radio (BLR) et le Vsat. Né en 2008 de la vision d'un homme de démocratiser l'accès à Internet pour tous, c'est un leader de service IT qui a pour mission d'offrir un accès haut débit et en volume illimité à tous à des coûts accessibles, à travers un réseau de fibre optique. Son siège est situé à Cotonou au quartier Ganhi.

Organisation du document

Le présent mémoire est composé de 03 chapitres.

- Le premier chapitre aborde la présentation de protocole ipv6 et les généralités qui y sont liées. Il présente les différents mécanismes qui ont trait à IPv6.
- Le deuxième chapitre présente la mise en place pratique et les différentes configurations qui y ont été faites.
- Le dernier chapitre présente les résultats obtenus et les perspectives liés à notre thème.

Chapitre 1

Revue de littérature

Introduction

Dans ce chapitre, nous présenterons la technologie IP en retraçant l'historique d'IPv4, les causes de son épuisement et les mécanismes qui ont permis son maintien. Ensuite, nous aborderons la genèse d'IPv6, ses caractéristiques distinctives, et ses avantages par rapport à IPv4. Une comparaison détaillée entre les deux protocoles sera faite, avant de conclure par le choix du mécanisme de transition au sein de notre projet.

1.1 Généralités

L'Internet Protocol (IP) est au cœur des communications sur Internet, permettant aux dispositifs du monde entier d'échanger des informations. Depuis l'avènement d'IPv4 dans les années 1980, cette technologie a évolué pour répondre aux besoins croissants de l'Internet.

1.1.1 Présentation de la technologie IP

L'Internet Protocol (IP) est conçu pour permettre l'échange de données entre des ordinateurs, des smartphones, des serveurs et d'autres types de dispositifs sur un réseau. Le principe fondamental de l'IP est de diviser les données en petits morceaux appelés **'paquets'** [1]. Chaque paquet contient non seulement **les données utiles** (comme le contenu d'un email ou d'une page Web), mais aussi **des informations de contrôle**, telles que l'adresse IP de l'expéditeur et celle du destinataire.

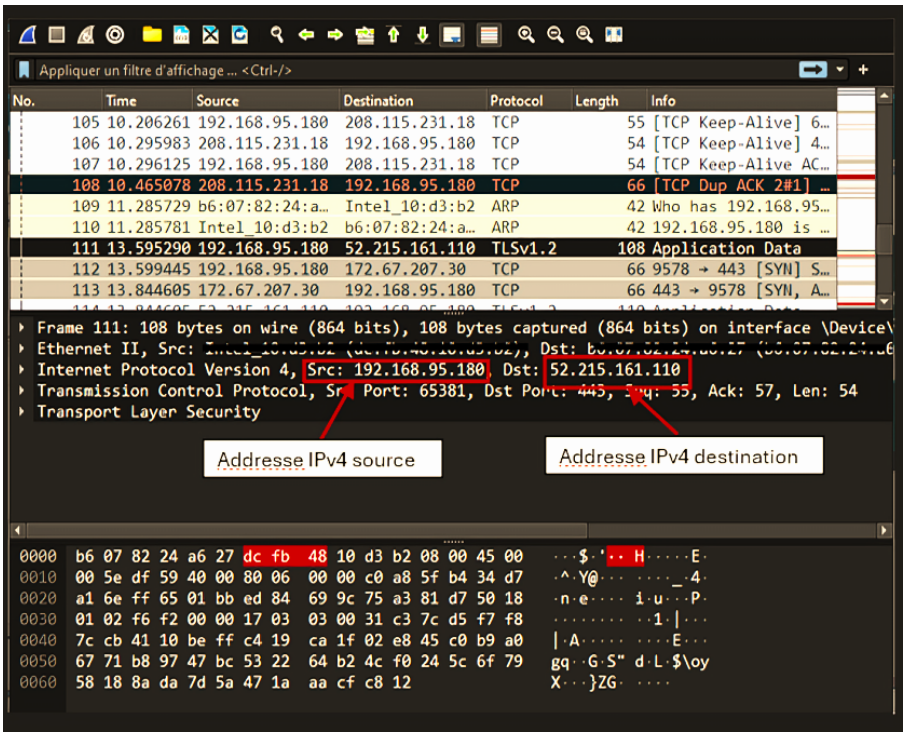


FIGURE 1.1 : Paquet capturé avec Wireshark

Lorsqu'un paquet IP est envoyé, il traverse plusieurs routeurs à travers le réseau, qui décident du meilleur chemin pour l'acheminer à sa destination. Si un paquet est trop gros pour passer sur un lien particulier, il peut être fragmenté en plusieurs morceaux plus petits. Chaque morceau suit le même processus de routage jusqu'à ce que tous les fragments atteignent leur destination, où ils sont ensuite réassemblés.

L'IP fonctionne en coopération avec d'autres protocoles comme TCP ou UDP [1], qui ajoutent des fonctionnalités supplémentaires comme **la fiabilité des transmissions** ou **la gestion des flux de données**.

1.2 Historique de IPv4

IPv4 a été développé dans les années **1970** et décrit pour la première fois dans la **RFC 791** en **septembre 1981** [2] en réponse au besoin croissant d'un protocole standard pour permettre la communication entre réseaux. Il a été conçu pour fournir des adresses uniques à chaque dispositif connecté à un réseau informatique, sous la forme d'adresses **32 bits**.
Le format d'IPv4 permet de créer exactement **4 294 967 296 adresses IP uniques**, ce qui semblait à l'époque largement suffisant pour couvrir les besoins d'Internet, alors principalement utilisé dans les universités et les centres de recherche, quand bien même bon nombre d'entre elles n' étaient pas publiquement utilisables.

Toutefois, avec l'explosion d'Internet dans les années 1990 et 2000 [5], les limitations d'IPv4 sont devenues de plus en plus évidentes. La croissance rapide des appareils connectés (ordinateurs, smartphones, objets connectés) a accéléré l'épuisement des adresses IPv4 disponibles.

En 2011, l'IANA a officiellement attribué le dernier bloc d'adresses IPv4 disponibles, marquant

ainsi la fin des ressources d'adressage IPv4.

1.2.1 Causes de l'épuisement

L'épuisement des adresses IPv4 peut être attribué à plusieurs facteurs. Le principal est l**a croissance exponentielle du nombre d'appareils connectés à Internet** [6].
À l'origine, seuls les ordinateurs utilisaient des adresses IP. Cependant, avec l'avènement des smartphones, des tablettes, des objets connectés et des serveurs cloud, la demande d'adresses IP a explosé. L'IoT a également joué un rôle important. Des appareils tels que les caméras de sécurité, les thermostats, les voitures connectées et même les réfrigérateurs se connectent désormais à Internet, nécessitant chacun une adresse IP unique.
Par ailleurs, la répartition inégale des blocs d'adresses IP, où certaines régions ou organisations ont obtenu des réserves d'adresses disproportionnées, a également contribué à l'épuisement. Plusieurs adresses IP ont également été réservée ;

TABLE 1.1 : Adresses réservées

Block	Adresse de fin	Usage	Référence
0.0.0.0/8	0.255.255.255	Réservé par IETF [7]	RFC 5735, RFC 1122
10.0.0.0/8	10.255.255.255	Adresses privées	RFC 1918
100.64.0.0/10	100.127.255.255	Espace partagé pour **Carrier Grade NAT** [8]	RFC 6598
127.0.0.0/8	127.255.255.255	Adresse de bouclage	RFC 1122
169.254.0.0/16	169.254.255.255	Adresses locales autoconfigurées (APIPA)	RFC 3927
172.16.0.0/12	172.31.255.255	Adresses privées	RFC 1918
192.0.0.0/24	192.0.0.255	Réservé par IETF	RFC 5736
192.0.2.0/24	192.0.2.255	Réseau de test (TEST-NET-1)	RFC 5737
192.88.99.0/24	192.88.99.255	6to4 anycast	RFC 3068
192.168.0.0/16	192.168.255.255	Adresses privées	RFC 1918
192.18.0.0/15	192.19.255.255	Test de performance	RFC 2544
198.51.100.0/24	198.51.100.255	Réseau de test (TEST-NET-2)	RFC 5737
203.0.113.0/24	203.0.113.255	Réseau de test (TEST-NET-3)	RFC 5737
224.0.0.0/4	239.255.255.255	Multicast (Multidiffusion)	RFC 5771
240.0.0.0/4	255.255.255.254	Réservé à un usage ultérieur	RFC 1112
255.255.255.255/32	255.255.255.255	Broadcast limité	RFC 919

1.2.2 Mécanismes de maintien d'IPv4

Pour pallier la pénurie d'adresses IPv4, plusieurs mécanismes ont été mis en place pour optimiser l'allocation et l'utilisation des adresses disponibles.

CIDR (Classless Inter-Domain Routing)

Le CIDR permet de réduire le gaspillage d'adresses IP en offrant une allocation plus flexible des adresses sans tenir compte des classes traditionnelles (A, B, C). Il introduit une notation dite "**sans classe**" [9] qui spécifie précisément le nombre de bits utilisés pour le préfixe réseau. Cela permet d'ajuster plus finement la taille des sous-réseaux en fonction des besoins réels des organisations, améliorant ainsi l'efficacité de l'utilisation des blocs d'adresses IP.

VLSM (Variable Length Subnet Masking)

Le VLSM étend encore davantage cette flexibilité en permettant d'utiliser des sous-réseaux de tailles variées au sein d'un même réseau global. Contrairement à l'allocation fixe des classes IP, VLSM permet de diviser un réseau en sous-réseaux [9] adaptés aux besoins spécifiques de chaque segment. Par exemple, un sous-réseau pour un service avec peu d'appareils peut utiliser une plus petite plage d'adresses, tandis qu'un sous-réseau plus grand peut être dédié à des services avec plus de besoins.

RFC 1918 (Adresses IP privées)

Le document **RFC 1918** [3], publié par l'**Internet Engineering Task Force (IETF)**, définit trois plages d'adresses IP réservées à l'usage privé au sein des réseaux locaux. Ces adresses ne sont pas routées sur Internet, ce qui permet leur réutilisation dans de nombreux réseaux privés sans risque de conflit. Les plages d'adresses privées définies par RFC 1918 sont :

```
10.0.0.0 à 10.255.255.255
172.16.0.0 à 172.31.255.255
192.168.0.0 à 192.168.255.255
```

Ces adresses permettent aux organisations d'étendre leurs réseaux locaux sans consommer d'adresses IP publiques, précieuses et limitées.

NAT (Network Address Translation)

Le NAT est une technique qui permet à un ensemble d'appareils dans un réseau local privé d'accéder à Internet en partageant une seule adresse IP publique. Il joue un rôle de passerelle entre le réseau local privé et le réseau public (Internet). Le NAT fonctionne en modifiant les adresses IP dans l'en-tête des paquets sortants : lorsqu'un appareil envoie un paquet vers Internet, le routeur NAT remplace l'adresse IP source privée par son adresse IP publique.

De plus, le routeur NAT conserve une table de traduction (NAT table) [9] où il enregistre les correspondances entre les adresses IP privées et l'adresse publique qu'il utilise pour chaque connexion. Ainsi, lorsqu'une réponse revient depuis Internet, le NAT peut rediriger le paquet vers l'appareil privé approprié.

1.3 Genèse d'IPv6

1.3.1 Présentation d'IPv6

Le protocole **IPv6** est la réponse aux défis de l'évolution constante de l'Internet, notamment pour permettre une connectivité sans restriction dans un monde de plus en plus interconnecté.
Conçu pour remplacer IPv4, IPv6 apporte des solutions durables qui anticipent les futurs besoins de l'Internet, comme **l'augmentation des dispositifs connectés**, **la mobilité accrue** et **la sécurité**.

IPv6 n'a pas pour seul objectif de répondre à une pénurie d'adresses, mais il vise aussi à introduire de nouvelles capacités qui faciliteront l'expansion des réseaux et l'amélioration des performances. Le protocole a été conçu pour **offrir une évolutivité massive**, mais aussi pour **simplifier la gestion des réseaux** et **améliorer la sécurité native**.
Parmi les avancées majeures d'IPv6, on retrouve :

- **L'extension des adresses à 128 bits**, permettant non seulement de répondre aux besoins actuels, mais aussi de garantir une infrastructure prête pour l'avenir, où des milliards de dispositifs peuvent se connecter sans contraintes.
- **L'automatisation des configurations** à travers des mécanismes comme **SLAAC (Stateless Address Autoconfiguration)** [10] , qui permet aux dispositifs de s'autoconfigurer sans dépendre de serveurs externes, rendant ainsi les réseaux plus dynamiques et résilients.

L'adoption d'IPv6 est aujourd'hui incontournable pour permettre l'expansion des réseaux tout en offrant une meilleure gestion, des communications sécurisées, et une compatibilité avec les environnements modernes de plus en plus connectés.

1.3.2 Caractéristiques d'IPv6

IPv6 apporte de nombreuses améliorations et innovations techniques par rapport à IPv4, non seulement en termes d'espace d'adressage, mais aussi dans la gestion des réseaux, la sécurité, et la performance. Voici les caractéristiques détaillées qui font d'IPv6 une solution incontournable pour l'avenir d'Internet :

1. **Taille des adresses : 128 bits**

   L'une des innovations majeures d'IPv6 est l'augmentation de la taille des adresses IP de 32 bits (en IPv4) à 128 bits. Cela permet de créer environ **340 undecillions d'adresses uniques**, soit 3.4×10^{38}. Pour donner une idée de l'échelle, cela permettrait à chaque grain de sable sur Terre d'avoir sa propre adresse IP unique, plusieurs fois.

   Les adresses IPv6 sont représentées sous forme de groupes de 16 bits, séparés par des deux-points. Voici un exemple d'adresse IPv6 [11] :

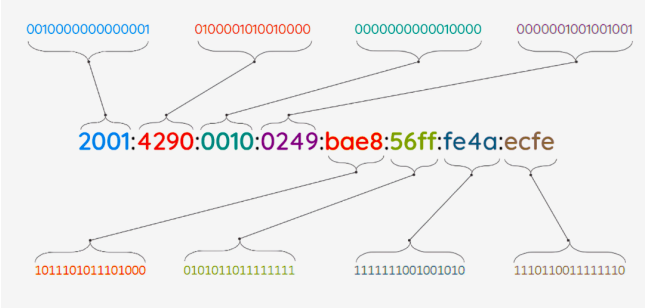


FIGURE 1.2 : Format d'une adresse IPv6

Chaque partie de l'adresse est exprimée en hexadécimal (0-9, a-f), et les séquences de zéros contigus peuvent être abrégées par **' : :'**

Cette vaste capacité d'adressage permet à chaque dispositif connecté (ordinateurs, smartphones, objets connectés, etc.) de posséder une adresse publique unique sans avoir recours à des mécanismes tels que NAT (Network Address Translation).

2. **Autoconfiguration d'adresses avec SLAAC (Stateless Address Autoconfiguration)**

   IPv6 introduit une fonctionnalité puissante appelée **SLAAC** [10] qui permet à un appareil de **générer automatiquement sa propre adresse IP** sans l'intervention d'un serveur DHCP (Dynamic Host Configuration Protocol), comme c'est souvent le cas en IPv4.

   Le processus de SLAAC fonctionne ainsi :

   - Lorsqu'un dispositif se connecte à un réseau, il envoie une requête Router Solicitation (RS) pour découvrir le routeur local.
   - Le routeur répond avec un message Router Advertisement (RA) qui contient le préfixe réseau (généralement les 64 premiers bits de l'adresse).
   - L'appareil combine ce préfixe réseau avec son identifiant d'interface (souvent dérivé de son adresse MAC via le mécanisme EUI-64) pour générer une adresse IPv6 complète.

   Cela permet de configurer les réseaux de manière plus flexible et efficace, sans avoir besoin de serveurs DHCP dans des environnements dynamiques où les dispositifs se connectent et se déconnectent fréquemment.

3. **En-tête simplifié et optimisé pour le routage**

   L'un des défis d'IPv4 est la complexité des en-têtes de paquets, qui comportent des champs nombreux et parfois peu utilisés, ralentissant le processus de traitement par les routeurs. IPv6 résout ce problème [12] en simplifiant l'en-tête des paquets, en réduisant le nombre de champs obligatoires et en facilitant le traitement des données.

   L'en-tête IPv6 se compose de 40 octets et inclut les champs essentiels tels que :

   - **Version (4 bits)** : indique la version du protocole (IPv6).
   - **Classe de trafic (8 bits)** : permet de spécifier la priorité du paquet pour le Quality of Service (QoS).
   - **Étiquette de flux (20 bits)** : identifie des flux de paquets nécessitant un traitement spécifique.

- **Longueur des données (16 bits)** : indique la taille des données utiles (payload) contenues dans le paquet.
- **Prochain en-tête (8 bits)** : pointe vers les en-têtes d'extension optionnels (pour des fonctions comme IPsec ou fragmentation).
- **Limite de saut (Hop Limit) (8 bits)** : équivalent du champ TTL d'IPv4, limite le nombre de routeurs que le paquet peut traverser.

En supprimant ou externalisant des champs non critiques comme la fragmentation (voir ci-dessous), IPv6 rend le traitement plus efficace et rapide. Cela est crucial dans un réseau global où les routeurs doivent gérer des millions de paquets chaque seconde.

4. **Gestion de la fragmentation**

   En IPv6, la fragmentation des paquets ne se produit plus au niveau des routeurs intermédiaires, contrairement à IPv4. Seul l'expéditeur du paquet peut fragmenter les données. Cela permet aux routeurs de se concentrer sur le routage pur sans avoir à gérer des processus coûteux de fragmentation et de réassemblage.

   Pour cela, IPv6 introduit un mécanisme appelé **Path MTU Discovery (PMTUD)**, où l'expéditeur détermine la taille maximale des paquets (MTU) autorisée sur un chemin réseau donné, en envoyant des paquets test et en recevant des réponses indiquant si le paquet est trop grand pour passer à travers les routeurs [13]. Si nécessaire, l'expéditeur ajuste la taille de ses paquets pour correspondre à la MTU minimale des liens réseau.

5. **Sécurité intégrée : IPsec natif**

   Une des lacunes d'IPv4 est l'absence d'un mécanisme de sécurité standardisé pour garantir **la confidentialité, l'intégrité et l'authenticité des données échangées sur Internet**. IPv6 inclut dès sa conception la prise en charge de **IPSec**.

   IPsec est un ensemble de protocoles qui sécurisent les communications réseau via deux fonctionnalités principales :

   - **Authentification de l'en-tête (AH)** : vérifie l'intégrité des paquets et l'identité de l'expéditeur.
   - **Encapsulation de la charge utile (ESP)** : fournit la confidentialité des données en chiffrant le contenu du paquet [14].

   Bien que IPsec soit également disponible en option sous IPv4, il est **obligatoire** dans l'architecture IPv6, offrant ainsi une base plus sécurisée pour les communications de bout en bout, **un atout essentiel dans un monde de plus en plus préoccupé par la cybersécurité.**

6. **Suppression du NAT (Network Address Translation)**

   L'implémentation d'IPv6 élimine la nécessité du NAT grâce à la vaste capacité d'adressage.

   En IPv4, les réseaux privés utilisent le NAT pour partager une seule adresse IP publique entre plusieurs dispositifs, ce qui complique souvent les communications de bout en bout (par exemple, dans le cas des applications peer-to-peer ou des jeux en ligne).

Avec IPv6, chaque appareil peut avoir **sa propre adresse IP publique**, permettant ainsi une communication directe avec n'importe quel autre appareil sur Internet sans les limitations imposées par le NAT. Cela simplifie la gestion du réseau, réduit la latence et améliore la performance des applications.

1.4 Comparaison entre IPv4 et IPv6

IPv4 et IPv6 sont deux versions du même protocole Internet, mais ils diffèrent fondamentalement dans leur conception, leurs capacités et leurs applications. Bien que les deux protocoles servent à identifier les dispositifs sur Internet, leurs caractéristiques techniques varient considérablement. Voici une comparaison détaillée des deux :

TABLE 1.2 : IPv4 vs IPv6

Caractéristique	IPv4	IPv6
Espace d'adressage	Adresse de **32 bits**, avec 4 294 967 296 adresses uniques. L'épuisement des adresses IPv4 a conduit à l'adoption de mécanismes comme **le NAT** et **le CIDR** pour prolonger la durée de vie du protocole.	Adresse de **128 bits**, offrant une capacité d'adressage de 340×10^{38} adresses. Cette ampleur d'adressage permet de répondre aux besoins croissants d'Internet, notamment avec l'explosion du nombre de dispositifs connectés (IoT, smartphones, etc.).
Notation des adresses	Les adresses sont écrites en notation décimale pointée, divisées en quatre octets. (ex. : 192.168.1.1).	Les adresses sont écrites en notation hexadécimale et sont séparées par des deux-points[1.2], avec des groupes de quatre chiffres hexadécimaux. Les zéros peuvent être omis pour simplifier l'écriture (ex. 2001 :db8 : :1).

Caractéristique	IPv4	IPv6
Gestion des adresses	Utilise des **classes d'adresses (A, B, C)** pour déterminer les plages d'adresses. La gestion des adresses est parfois complexe, en particulier avec l'utilisation de NAT pour partager une adresse publique entre plusieurs dispositifs internes.	N'a pas de classes d'adresses, et la gestion des adresses est plus flexible grâce à CIDR. Permet une allocation directe d'adresses publiques uniques à chaque appareil, éliminant ainsi la nécessité du NAT.
Performance et Complexité des en-têtes	L'en-tête IPv4 comporte **14 champs**, et certains d'entre eux sont rarement utilisés, ce qui alourdit le traitement des paquets.[1.3]	L'en-tête IPv6 est simplifié avec **8 champs principaux**[1.3], et certains processus comme la fragmentation ont été déplacés hors des routeurs pour alléger leur charge.
Sécurité	La sécurité **(IPsec)** est optionnelle en IPv4 et nécessite une configuration supplémentaire pour être activée.	La sécurité est intégrée nativement avec **IPsec**, et est une composante essentielle du protocole, ce qui rend les communications sur IPv6 plus sûres par défaut.
Configuration des dispositifs	Les dispositifs doivent souvent être configurés manuellement ou via un serveur DHCP pour obtenir une adresse IP.	Permet une autoconfiguration grâce à SLAAC, où les dispositifs peuvent s'attribuer une adresse IP automatiquement sans nécessiter un serveur externe.
Fragmentation des paquets	La fragmentation peut être effectuée par les routeurs intermédiaires si un paquet dépasse la MTU (Maximum Transmission Unit).	La fragmentation est effectuée uniquement par l'expéditeur, ce qui améliore les performances du réseau en réduisant la charge des routeurs.

Caractéristique	IPv4	IPv6
Temps de transition	Très largement déployé et utilisé dans le monde entier, mais son espace d'adressage est saturé.	En déploiement progressif, mais nécessaire pour l'avenir d'Internet. La transition entre IPv4 et IPv6 se fait progressivement grâce à des mécanismes comme le Dual Stack.

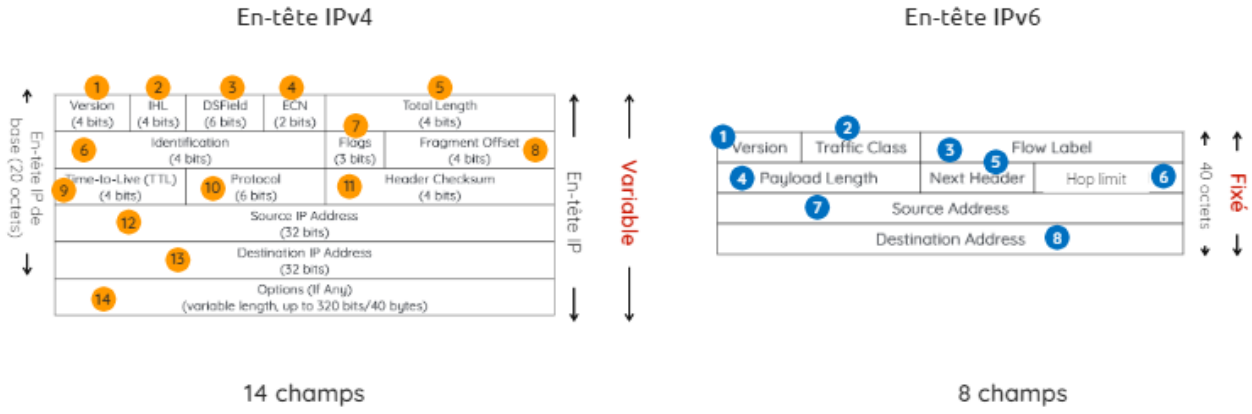


FIGURE 1.3 : Entête IPV4 vs Entête IPV6

1.5 Mécanismes de Transition vers IPv6

La transition de l'IPv4 vers l'IPv6 pose des défis pour maintenir l'interopérabilité et la connectivité avec les réseaux existants tout en adoptant le nouveau protocole. Pour faciliter cette transition, plusieurs mécanismes ont été mis en place [4], les plus courants étant le Dual Stack, le Tunneling, et le NAT64. Ces solutions permettent de faire coexister les deux protocoles, chacun offrant des avantages particuliers selon le contexte.

1.5.1 Dual Stack

Le concept de Dual Stack fait référence à l'implémentation simultanée des deux versions du protocole Internet, IPv4 et IPv6, sur un même réseau. Cela permet une transition en douceur de IPv4 à IPv6, tout en assurant la compatibilité avec les réseaux existants qui ne supportent que IPv4.

1.5.1.1 Avantages du Dual Stack

- **Compatibilité ascendante et descendante** : Le Dual Stack permet aux dispositifs d'être compatibles à la fois avec les réseaux existants basés sur IPv4 et avec les nouveaux réseaux IPv6. Cela évite les ruptures de communication lors de la migration.

- **Flexibilité de transition** : En permettant de fonctionner avec IPv4 et IPv6 simultanément, le Dual Stack permet aux réseaux d'effectuer une transition progressive, sans avoir à migrer complètement d'un protocole à l'autre du jour au lendemain.
- **Support des applications** : Les applications qui ne sont pas encore compatibles avec IPv6 peuvent toujours fonctionner en utilisant IPv4, tandis que celles qui sont prêtes pour IPv6 peuvent communiquer directement via ce protocole.

1.5.1.2 Inconvénients du Dual Stack

- **Gestion complexe** : La gestion de deux protocoles différents sur un même réseau peut rendre l'administration plus complexe, en particulier lors de la configuration des dispositifs ou des services.
- **Routage et interopérabilité** : Bien que les réseaux IPv4 et IPv6 puissent coexister, les mécanismes de routage et les intermédiaires (comme les passerelles) doivent être configurés pour gérer le trafic des deux protocoles, ce qui peut compliquer la gestion du réseau.

1.5.2 Tunneling

Le Tunneling encapsule les paquets IPv6 dans des paquets IPv4 pour les faire transiter sur des infrastructures qui ne supportent pas IPv6. Cette méthode est couramment utilisée pour connecter des îlots IPv6 isolés à travers des réseaux IPv4.
Ci dessous une image simplifiée montrant clairement le principe du tunelling.

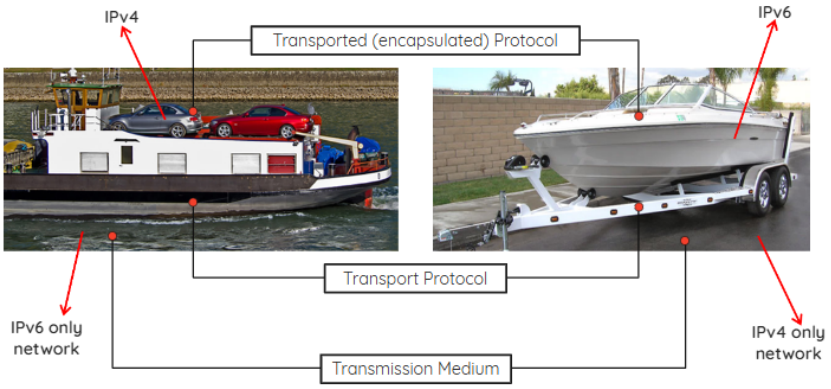


FIGURE 1.4 : Principe de fonctionnement du Tunelling

1.5.2.1 Avantages du Tunelling

- **Aucun changement physique nécessaire** : Le Tunneling permet de faire passer du trafic IPv6 sur une infrastructure IPv4 existante, sans nécessiter d'importantes modifications matérielles.
- **Connectivité pour des réseaux partiels** : Utile pour connecter des segments IPv6 séparés, comme des bureaux distants ou des sites qui n'ont pas de connexion IPv6 directe.
- **Flexibilité de configuration** : Les solutions de tunneling, telles que 6to4, ISATAP, et Teredo, offrent des options pour différentes configurations et cas d'usage, ce qui permet d'adapter le tunnel aux besoins spécifiques du réseau.

1.5.2.2 Inconvénients du Tunneling

- **Latence accrue** : Le tunneling ajoute un niveau supplémentaire d'encapsulation, ce qui peut augmenter la latence et affecter les performances du réseau.
- **Difficulté de diagnostic** : Le diagnostic et le dépannage des réseaux utilisant le tunneling peuvent être complexes, car les paquets encapsulés rendent la surveillance et le débogage plus difficiles.
- **Failles de sécurité potentielles** : Certains mécanismes de tunneling, en particulier les tunnels non sécurisés, peuvent être vulnérables aux attaques, comme les attaques par injection ou le spoofing, ce qui nécessite des configurations de sécurité supplémentaires.

1.5.3 NAT64

Le NAT64 permet aux hôtes IPv6 d'accéder aux services disponibles uniquement en IPv4 en traduisant les adresses et les en-têtes de paquets entre les deux protocoles. Il est particulièrement utile lorsque les réseaux et les applications doivent opérer principalement en IPv6, mais avec un accès ponctuel aux ressources IPv4.

1.5.3.1 Avantages du NAT64

- **Réduction de la demande en adresses IPv4** : Les utilisateurs et dispositifs IPv6 peuvent partager une seule adresse IPv4, ce qui réduit le besoin d'adresses IPv4 publiques pour chaque hôte.
- **Interconnexion des réseaux IPv6 et IPv4** : Permet aux réseaux IPv6 d'accéder aux services IPv4 sans nécessiter de déploiement d'IPv4 dans tout le réseau.
- **Simplicité pour les réseaux IPv6-only** : Dans les environnements qui migrent complètement vers IPv6, NAT64 permet de se passer de Dual Stack tout en assurant une connectivité vers les services IPv4 externes.

1.5.3.2 Inconvénients du NAT64

- **Problèmes de compatibilité d'applications** : Certaines applications nécessitent des communications de bout en bout sans traduction d'adresses (ex : certaines applications VoIP), ce qui peut être limité par NAT64.
- **Perte de transparence réseau** : Le NAT64 introduit un intermédiaire dans la communication, ce qui peut compliquer la gestion des sessions, surtout pour des services qui reposent sur les adresses IP pour des règles de sécurité ou de routage.
- **Dégradation des performances** : La traduction en temps réel des paquets peut ralentir la transmission de données et introduire de la latence, ce qui affecte les performances globales du réseau.

1.5.4 Choix du Dual Stack

Dans le cadre de ce projet, le Dual Stack a été choisi comme mécanisme de transition, car il offre une compatibilité native entre IPv4 et IPv6, assurant une connectivité fluide avec les réseaux et applications existants tout en intégrant progressivement IPv6. Cette approche garantit une interopérabilité sans recours à la traduction d'adresses ou à l'encapsulation, simplifiant la gestion et les diagnostics réseau. Le Dual Stack représente une solution durable et stable pour ISOCEL Telecom dans sa transition sécurisée vers l'IPv6.

Conclusion

La transition de l'IPv4 vers l'IPv6 est une nécessité incontournable pour l'avenir d'Internet en raison de l'épuisement des adresses IPv4 et des limitations inhérentes à ce protocole. IPv6, avec son espace d'adressage immense, ses capacités de sécurité intégrées et sa flexibilité dans la gestion des réseaux, répond aux défis actuels et futurs de l'expansion d'Internet. Le Dual Stack, en permettant une cohabitation des deux protocoles, offre une solution pratique pour assurer une transition progressive et sans heurts, garantissant ainsi la compatibilité avec les systèmes existants tout en facilitant l'adoption d'IPv6.

Chapitre 2

Conception et Déploiement

Introduction

Dans ce chapitre, nous aborderons la conception et le déploiement de la solution réseau, en détaillant l'architecture choisie et le plan d'adressage mis en place pour la transition vers IPv6. Nous présenterons également les différentes étapes de l'implémentation pratique, suivies des tests de sécurité et des audits effectués afin de garantir que l'infrastructure déployée réponde aux exigences en matière de performance et de sécurité. Ces étapes sont essentielles pour assurer une migration fluide et sécurisée vers IPv6.

2.1 Présentation de l'architecture réseau de ISOCEL Telecom

L'architecture réseau présentée dans ce projet suit une structure en plusieurs couches, chacune jouant un rôle spécifique dans la gestion du trafic réseau et la transition vers IPv6.

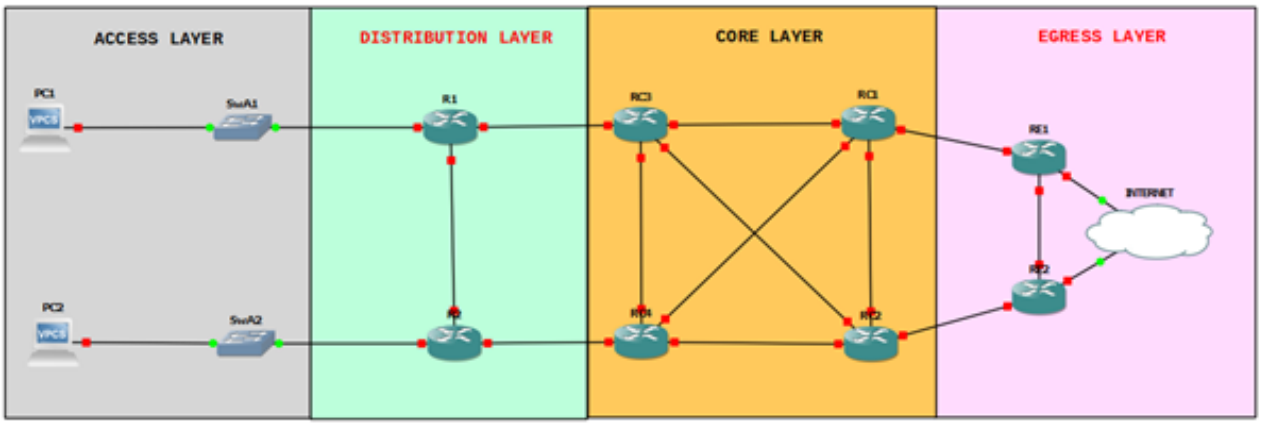


FIGURE 2.1 : Architecture du réseau de ISOCEL Telecom

La couche d'accès ou Access layer connecte les terminaux utilisateurs au réseau via des commutateurs. Cette couche utilise le plan d'adressage IPv4 et IPv6 pour fournir une connectivité dual stack aux utilisateurs finaux.

La couche de distribution relie la couche d'accès à la couche cœur, jouant un rôle clé dans le routage des paquets et l'application des politiques réseau.

La couche cœur forme la colonne vertébrale du réseau, reliant plusieurs routeurs centraux. Ces routeurs sont configurés pour assurer une redondance et une haute disponibilité grâce à des connexions inter-routeurs multiples, garantissant une faible latence et une résilience accrue.

La couche Egress (sortie vers l'internet) est assurée par les routeurs RE1 et RE2, qui connectent le réseau interne à Internet tout en appliquant des mesures de sécurité et des filtres pour assurer une transition sécurisée vers IPv6.

Chaque interface et chaque lien entre les équipements est adressé précisément en IPv4 et en IPv6, facilitant ainsi la transition vers IPv6 tout en assurant une compatibilité continue avec IPv4.

2.2 Mise en place du plan d'adressage

TABLE 2.1 : Illustration du plan d'adressage IPv6.

LAYERS	INITIAL ADDRESS RANGE	SUBNET RANGE	NUMBER OF HOSTS	IP RANGE
EGRESS	2001:db8:5678::/64	2001:db8:5678::/117	2048	2001:db8:5678:0:0:0:0:0 -- 2001:db8:5678:0:0:ffff:ffff:ffff
CORE	2001:db8:5678::/64	2001:db8:5678::800/117	2048	2001:db8:5678:0:0:0:0:800 -- 2001:db8:5678:0:0:0:0:fff
DISTRIBUTION	2001:db8:5678::/64	2001:db8:5678::1000/117	2048	2001:db8:5678:0:0:0:0:1000 -- 2001:db8:5678:0:0:0:0:17ff
ACCESS	2001:db8:5678::/64	2001:db8:5678:0:1::/80	2^48	2001:db8:5678:0:1:0:0:0 -- 2001:db8:5678:0:1:ffff:ffff:ffff

La conception du plan d'adressage IPv6 repose sur une hiérarchisation claire en fonction des différentes couches de l'architecture réseau [15], permettant ainsi une gestion optimisée des adresses et facilitant l'administration et la sécurité du réseau. Le schéma d'adressage respecte les bonnes pratiques en matière de segmentation et de structuration des sous-réseaux, assurant à la fois une évolutivité et une efficacité dans l'allocation des adresses IP.

Pour ce projet, la plage d'adresses globale **2001 :db8 :5678 : :/64** a été subdivisée en plusieurs sous-réseaux, chaque couche du réseau se voyant attribuer une plage dédiée.

2.3 Implémentation pratique

Dans cette section, nous détaillons les étapes d'implémentation des protocoles IPv4 et IPv6 au sein du réseau simulé. Cette implémentation est effectuée dans un environnement virtualisé à l'aide de **GNS3**, et elle a permis de configurer les sous-réseaux ainsi que la connectivité entre les différents équipements.

2.3.1 Configuration IPv4

Afin d'assurer une communication fluide entre les équipements du réseau tout en respectant le principe du Dual-Stack, nous avons commencé par la configuration de l'adressage IPv4 sur l'ensemble des équipements. Cette étape est primordiale, car elle garantit que les systèmes existants qui fonctionnent encore majoritairement en IPv4 pourront continuer à échanger des données de manière optimale tout en préparant la transition vers IPv6.

2.3.1.1 Adressage du réseau en IPv4

La première étape pour configurer l'IPv4 a été de définir le plan d'adressage adéquat pour chaque sous-réseau et chaque lien point-à-point. Pour ce faire, nous avons attribué des adresses IP correspondant à chaque interface d'équipement, en tenant compte de la topologie réseau, des sous-réseaux à utiliser, et des besoins en termes de connectivité ; puis nous avions utilisé le **DHCP** pour les interfaces connectées à Internet, afin d'obtenir des adresses dynamiques pour la connectivité extérieure.

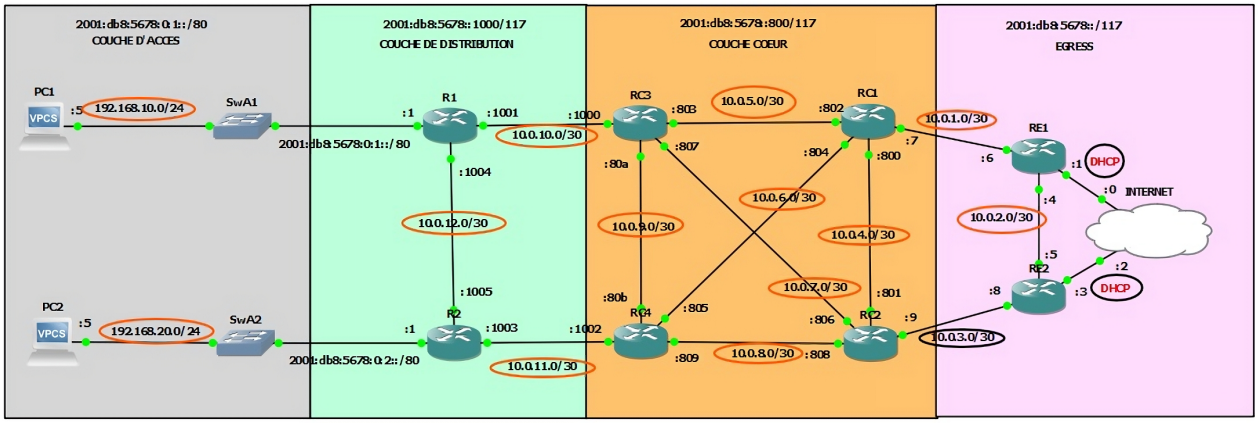


FIGURE 2.2 : Réseau adressé en IPv4.

Chaque équipement, qu'il s'agisse de routeurs ou de terminaux, a été associé à une adresse IPv4. Les sous-réseaux utilisés respectent une allocation précise afin d'optimiser l'utilisation des adresses IP et de limiter le gaspillage. Voici quelques points clés de l'adressage mis en place :

a. Plages d'adresses IPv4

Pour chaque liaison point-à-point entre les routeurs, nous avons utilisé un masque de sous-réseau de /30. Ce masque permet de définir un sous-réseau avec deux adresses IP utilisables, ce qui est optimal pour les liaisons entre deux équipements. Cette approche permet une gestion efficace des adresses IP et réduit la surface d'attaque potentielle.

b. Liaisons avec les équipements utilisateurs

Pour les équipements terminaux tels que les PC connectés aux switches de la couche d'accès, nous avons attribué des adresses IPv4 à partir de sous-réseaux plus larges (192.168.10.0/24 et 192.168.20.0/24). Cela permet de connecter jusqu'à 254 équipements par sous-réseau.

c. Interfaces connectées à internet

Les interfaces des routeurs connectées à Internet ont été configurées pour obtenir leurs adresses IP dynamiquement via **DHCP (Dynamic Host Configuration Protocol)**. Cela permet une **gestion flexible de l'adressage** et **évite une configuration statique** sur les interfaces exposées aux réseaux externes.

2.3.1.2 Utilisation des interfaces de loopback

En plus de l'adressage sur les interfaces physiques, nous avons également mis en place des **interfaces Loopback** sur chaque routeur pour IPv4 et IPv6. Ces interfaces jouent un rôle important dans la stabilité du réseau, car elles fournissent des adresses IP qui ne dépendent pas de l'état des interfaces physiques.
Les interfaces Loopback sont des interfaces logiques qui restent actives tant que le routeur fonctionne, quel que soit l'état des autres interfaces. Voici les avantages de leur utilisation :

- **Disponibilité élevée** : Contrairement aux interfaces physiques qui peuvent être sujettes à des pannes (câble déconnecté, lien inactif), une interface Loopback reste accessible tant que le routeur est opérationnel.
- **Utilisation dans les protocoles de routage** : Les interfaces Loopback sont souvent utilisées comme adresses source pour les protocoles de routage, tels que OSPF et BGP, car elles garantissent une stabilité et une continuité de la connectivité, ce qui est adapté pour nos configurations.
- **Facilitation des configurations d'accès** : Les Loopbacks simplifient les configurations pour l'administration à distance (comme SSH ou SNMP), puisque l'interface est toujours accessible.

TABLE 2.2 : Adresses de loopback utilisées

Routeurs	Adresse de loopback utilisée	
-	IPv4	IPv6
RE1	172.16.255.1/32	2001:db8:5678:100::1/128
RE2	172.16.255.2/32	2001:db8:5678:100::2/128
RC1	172.16.255.3/32	2001:db8:5678:100::3/128
RC2	172.16.255.4/32	2001:db8:5678:100::4/128
RC3	172.16.255.5/32	2001:db8:5678:100::5/128
RC4	172.16.255.6/32	2001:db8:5678:100::6/128
R1	172.16.255.7/32	2001:db8:5678:100::7/128
R2	172.16.255.8/32	2001:db8:5678:100::8/128

2.3.1.3 Protocole de routage IPv4 : OSPF et BGP

Pour assurer un échange optimal des routes au sein du réseau, deux protocoles de routage ont été mis en place : OSPF (Open Shortest Path First) pour le routage interne et BGP (Border Gateway Protocol) pour l'échange de routes avec l'extérieur [16].

1. **OSPF (Open Shortest Path First)** : OSPF a été choisi comme protocole de routage interne (IGP) pour assurer une convergence rapide des routes et la découverte automatique des sous-réseaux. Le processus OSPF est configuré sur tous les routeurs pour permettre une propagation efficace des routes à travers le réseau. De plus, les interfaces Loopback sont utilisées comme adresses sources pour échanger les paquets OSPF, garantissant ainsi la stabilité et la disponibilité des sessions de routage, même en cas de défaillance d'une interface physique.

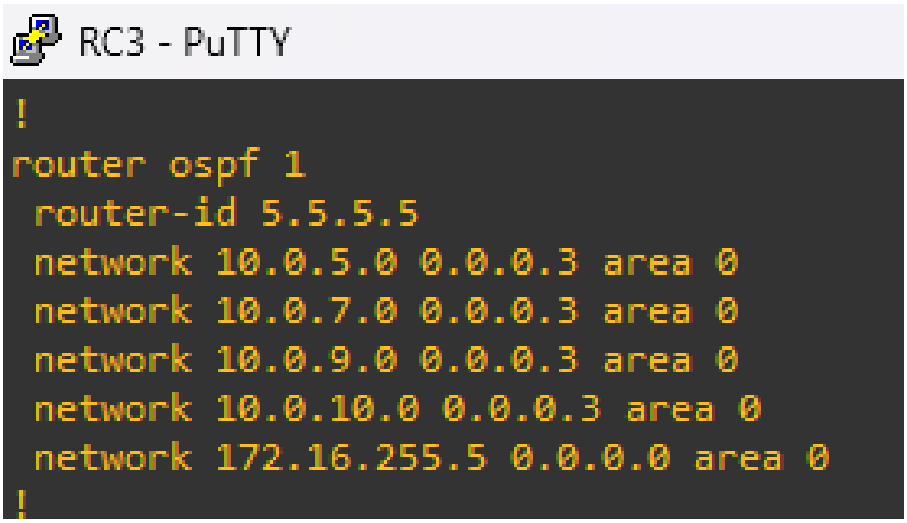


FIGURE 2.3 : Configuration OSPF sur RC3

Cette configuration a été répliquée sur les autres routeurs, avec des adaptations au niveau des sous-réseaux locaux. Chaque routeur a été configuré pour **propager ses interfaces internes via OSPF.**

Afin de donner une vue d'ensemble du fonctionnement OSPF, nous avons extrait la base de données OSPF et les routes calculées sur RC3, montrant ainsi l'ensemble des routes interconnectées et apprises par OSPF :

- **Extrait de la base de données OSPF sur RC3**

```
RC3#
RC3#show ip ospf database

            OSPF Router with ID (5.5.5.5) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         513         0x80000003 0x00F5C5 3
2.2.2.2         2.2.2.2         492         0x80000005 0x006246 3
3.3.3.3         3.3.3.3         526         0x80000005 0x00AE79 5
4.4.4.4         4.4.4.4         506         0x80000004 0x008E81 5
5.5.5.5         5.5.5.5         494         0x80000005 0x00539D 5
6.6.6.6         6.6.6.6         512         0x80000005 0x00528B 5
7.7.7.7         7.7.7.7         519         0x80000004 0x0063E7 3
9.9.9.9         9.9.9.9         533         0x80000004 0x006FC0 3

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.0.1.2        3.3.3.3         526         0x80000002 0x0028EA
10.0.2.2        2.2.2.2         491         0x80000002 0x001901
10.0.3.2        4.4.4.4         503         0x80000002 0x0048BC
10.0.4.2        4.4.4.4         506         0x80000002 0x006F90
10.0.5.2        5.5.5.5         494         0x80000002 0x00688E
10.0.6.2        6.6.6.6         510         0x80000002 0x00618C
10.0.7.2        5.5.5.5         494         0x80000002 0x00846C
10.0.8.2        6.6.6.6         512         0x80000002 0x007D6A
10.0.9.2        6.6.6.6         510         0x80000002 0x00A43E
10.0.10.2       7.7.7.7         519         0x80000002 0x009D3C
10.0.11.2       9.9.9.9         533         0x80000002 0x00CCF7
10.0.12.2       9.9.9.9         533         0x80000002 0x00F3CB

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         513         0x8000000A 0x000B9A 1
192.168.10.0    7.7.7.7         519         0x80000002 0x00F21D 0
192.168.20.0    9.9.9.9         533         0x80000002 0x0048B5 0
RC3#
```

FIGURE 2.4 : Extrait de la base de données OSPF sur RC3.

- **Table de routage OSPF sur RC3**

RC3 - PuTTY

```
RC3#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.7.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.0.7.1, 01:24:35, Ethernet0/1
      10.0.0.0/8 is variably subnetted, 16 subnets, 2 masks
O        10.0.1.0/30 [110/20] via 10.0.5.1, 01:24:35, Ethernet0/0
O        10.0.2.0/30 [110/30] via 10.0.7.1, 01:24:35, Ethernet0/1
                     [110/30] via 10.0.5.1, 01:24:35, Ethernet0/0
O        10.0.3.0/30 [110/20] via 10.0.7.1, 01:24:35, Ethernet0/1
O        10.0.4.0/30 [110/20] via 10.0.7.1, 01:24:35, Ethernet0/1
                     [110/20] via 10.0.5.1, 01:24:35, Ethernet0/0
O        10.0.6.0/30 [110/20] via 10.0.9.2, 01:24:30, Ethernet0/2
                     [110/20] via 10.0.5.1, 01:24:35, Ethernet0/0
O        10.0.8.0/30 [110/20] via 10.0.9.2, 01:24:30, Ethernet0/2
                     [110/20] via 10.0.7.1, 01:24:30, Ethernet0/1
O        10.0.11.0/30 [110/20] via 10.0.9.2, 01:24:30, Ethernet0/2
O        10.0.12.0/30 [110/20] via 10.0.10.2, 01:24:30, Ethernet0/3
      172.16.0.0/32 is subnetted, 8 subnets
O        172.16.255.1 [110/21] via 10.0.5.1, 01:24:35, Ethernet0/0
O        172.16.255.2 [110/21] via 10.0.7.1, 01:24:35, Ethernet0/1
O        172.16.255.3 [110/11] via 10.0.5.1, 01:24:35, Ethernet0/0
O        172.16.255.4 [110/11] via 10.0.7.1, 01:24:35, Ethernet0/1
O        172.16.255.6 [110/11] via 10.0.9.2, 01:24:30, Ethernet0/2
O        172.16.255.7 [110/11] via 10.0.10.2, 01:24:30, Ethernet0/3
O        172.16.255.8 [110/21] via 10.0.10.2, 01:24:30, Ethernet0/3
                      [110/21] via 10.0.9.2, 01:24:30, Ethernet0/2
O E2  192.168.10.0/24 [110/20] via 10.0.10.2, 01:24:30, Ethernet0/3
O E2  192.168.20.0/24 [110/20] via 10.0.10.2, 01:24:30, Ethernet0/3
                      [110/20] via 10.0.9.2, 01:24:30, Ethernet0/2
RC3#
```

FIGURE 2.5 : Table de routage OSPF sur RC3.

Pour les routeurs directement connectés aux clients, R1 et R2, une configuration spéciale a été mise en place pour redistribuer les réseaux connectés. Cela permet aux autres routeurs de connaître les sous-réseaux des clients afin de les inclure dans la table de routage globale.

La commande : "**`redistribute connected subnets`**" a été utilisée pour s'assurer que les réseaux directement connectés aux routeurs R1 et R2 (notamment les sous-réseaux des PC clients) soient connus par les autres routeurs du réseau via OSPF.

1.1. **Injection de la route par défaut via RE1 et RE2**

Pour permettre à l'ensemble du réseau d'accéder à Internet, les routeurs RE1 et RE2 (connectés à des fournisseurs d'accès via DHCP) ont été configurés pour injecter une route par défaut vers l'extérieur du réseau.

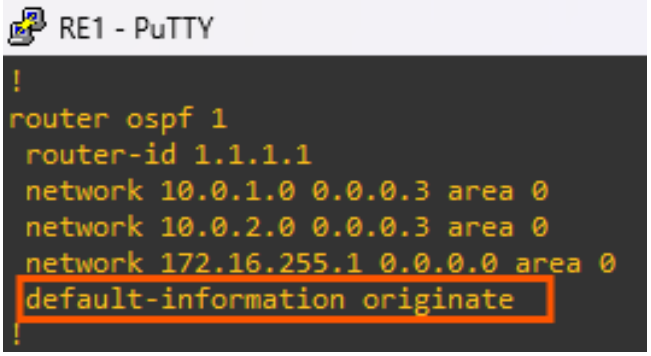


FIGURE 2.6 : Configuration BGP sur RE1.

La commande "**`default-information originate`**" permet de propager une route par défaut (0.0.0.0/0) à tous les autres routeurs, leur indiquant que tout le trafic destiné à l'extérieur du réseau doit être redirigé vers RE1 ou RE2, selon leur proximité et les coûts OSPF.

Cela permet à tous les équipements du réseau de communiquer avec des adresses externes telles que 8.8.8.8 (Google DNS).

2. **BGP (Border Gateway Protocol) :** En complément d'OSPF pour le routage interne, BGP a été mis en place pour permettre à notre réseau d'échanger des routes avec des réseaux externes et de propager les routes entre les routeurs au sein de l'AS (Autonomous System). Le routeur RC3 a été configuré comme Route Reflector (RR), tandis que tous les autres routeurs sont des clients RR, leur seul voisin étant RC3.

   - **Configuration BGP sur RC3 (Route Reflector)**

   Cette configuration montre que RC3 joue le rôle de **Route Reflector**, centralisant ainsi les informations de routage et éliminant la nécessité de configurer un full-mesh entre tous les routeurs BGP. Chacun des routeurs n'a qu'un seul voisin BGP, RC3, facilitant ainsi la gestion du routage dans l'AS.

```
RC3#
RC3#sh run | section bgp
router bgp 65001
 bgp log-neighbor-changes
 neighbor 172.16.255.1 remote-as 65001
 neighbor 172.16.255.1 update-source Loopback0
 neighbor 172.16.255.2 remote-as 65001
 neighbor 172.16.255.2 update-source Loopback0
 neighbor 172.16.255.3 remote-as 65001
 neighbor 172.16.255.3 update-source Loopback0
 neighbor 172.16.255.4 remote-as 65001
 neighbor 172.16.255.4 update-source Loopback0
 neighbor 172.16.255.6 remote-as 65001
 neighbor 172.16.255.6 update-source Loopback0
 neighbor 172.16.255.7 remote-as 65001
 neighbor 172.16.255.7 update-source Loopback0
 neighbor 172.16.255.8 remote-as 65001
 neighbor 172.16.255.8 update-source Loopback0
 !
 address-family ipv4
  network 10.0.5.0 mask 255.255.255.252
  network 10.0.7.0 mask 255.255.255.252
  network 10.0.9.0 mask 255.255.255.252
  network 10.0.10.0 mask 255.255.255.252
  network 172.16.255.5 mask 255.255.255.255
  no neighbor 2001:DB8:5678:100::1 activate
  no neighbor 2001:DB8:5678:100::2 activate
  no neighbor 2001:DB8:5678:100::3 activate
  no neighbor 2001:DB8:5678:100::4 activate
  no neighbor 2001:DB8:5678:100::6 activate
  no neighbor 2001:DB8:5678:100::7 activate
  no neighbor 2001:DB8:5678:100::8 activate
  neighbor 172.16.255.1 activate
  neighbor 172.16.255.1 route-reflector-client
  neighbor 172.16.255.2 activate
  neighbor 172.16.255.2 route-reflector-client
  neighbor 172.16.255.3 activate
  neighbor 172.16.255.3 route-reflector-client
  neighbor 172.16.255.4 activate
  neighbor 172.16.255.4 route-reflector-client
  neighbor 172.16.255.6 activate
  neighbor 172.16.255.6 route-reflector-client
  neighbor 172.16.255.7 activate
  neighbor 172.16.255.7 route-reflector-client
  neighbor 172.16.255.8 activate
  neighbor 172.16.255.8 route-reflector-client
 exit-address-family
 !
```

FIGURE 2.7 : Configuration BGP sur RC3.

Les figures 2.8 et 2.9 présentent la configuration BGP, sur le routeur R1, ainsi que la table de routage associée. Cette configuration est la même sur tous les autres routeurs clients du Route reflector.

R1 - PuTTY

```
router bgp 65001
 bgp log-neighbor-changes
 neighbor 2001:DB8:5678:100::5 remote-as 65001
 neighbor 2001:DB8:5678:100::5 update-source Loopback0
 neighbor 172.16.255.5 remote-as 65001
 neighbor 172.16.255.5 update-source Loopback0
 !
 address-family ipv4
  network 10.0.10.0 mask 255.255.255.252
  network 10.0.12.0 mask 255.255.255.252
  network 172.16.255.7 mask 255.255.255.255
  no neighbor 2001:DB8:5678:100::5 activate
  neighbor 172.16.255.5 activate
 exit-address-family
 !
```

FIGURE 2.8 : Configuration BGP sur R1.

R1 - PuTTY

```
R1#sh ip bgp
BGP table version is 21, local router ID is 172.16.255.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 r>i 10.0.1.0/30      172.16.255.3             0    100      0 i
 r>i 10.0.2.0/30      172.16.255.1             0    100      0 i
 r>i 10.0.3.0/30      172.16.255.4             0    100      0 i
 r>i 10.0.4.0/30      172.16.255.3             0    100      0 i
 r>i 10.0.5.0/30      172.16.255.5             0    100      0 i
 r>i 10.0.6.0/30      172.16.255.3             0    100      0 i
 r>i 10.0.7.0/30      172.16.255.5             0    100      0 i
 r>i 10.0.8.0/30      172.16.255.4             0    100      0 i
 r>i 10.0.9.0/30      172.16.255.5             0    100      0 i
 * i 10.0.10.0/30     172.16.255.5             0    100      0 i
 *>                   0.0.0.0                  0         32768 i
 r>i 10.0.11.0/30     172.16.255.6             0    100      0 i
 *>  10.0.12.0/30     0.0.0.0                  0         32768 i
 r>i 172.16.255.1/32  172.16.255.1             0    100      0 i
     Network          Next Hop            Metric LocPrf Weight Path
 r>i 172.16.255.2/32  172.16.255.2             0    100      0 i
 r>i 172.16.255.3/32  172.16.255.3             0    100      0 i
 r>i 172.16.255.4/32  172.16.255.4             0    100      0 i
 r>i 172.16.255.5/32  172.16.255.5             0    100      0 i
 r>i 172.16.255.6/32  172.16.255.6             0    100      0 i
 *>  172.16.255.7/32  0.0.0.0                  0         32768 i
 r>i 172.16.255.8/32  172.16.255.8             0    100      0 i
R1#
```

FIGURE 2.9 : Table de routage BGP sur R1.

Les sessions BGP sont établies sur les interfaces Loopback, garantissant la résilience en cas de panne d'une interface physique. Cela assure une stabilité accrue dans les échanges de routes.

2.3.2 Implémentation IPv6

Afin d'assurer une transition fluide entre IPv4 et IPv6, et en accord avec les recommandations de déploiement modernes, l'implémentation de l'IPv6 s'est faite en **Dual Stack**. Cela signifie que chaque équipement de notre réseau fonctionne **simultanément avec IPv4 et IPv6**, permettant une communication transparente avec les réseaux IPv4 existants tout en profitant des avantages de l'IPv6.

2.3.2.1 Configuration des adresses IPv6 sur les interfaces

Chaque routeur a été configuré avec une adresse IPv6 globale unique (GUAs) pour assurer une connectivité complète sur le réseau. Les interfaces point-à-point ont été configurées avec des préfixes en **/127** pour optimiser l'utilisation de l'espace d'adressage, sauf pour les interfaces reliant les PC et routeurs, où des préfixes plus larges ont été utilisés.

Voici un exemple de la configuration IPv6 d'une interface sur un des routeurs :

```
interface GigabitEthernet0/0
 ipv6 address 2001:db8:5678::1/127
 no shutdown
```

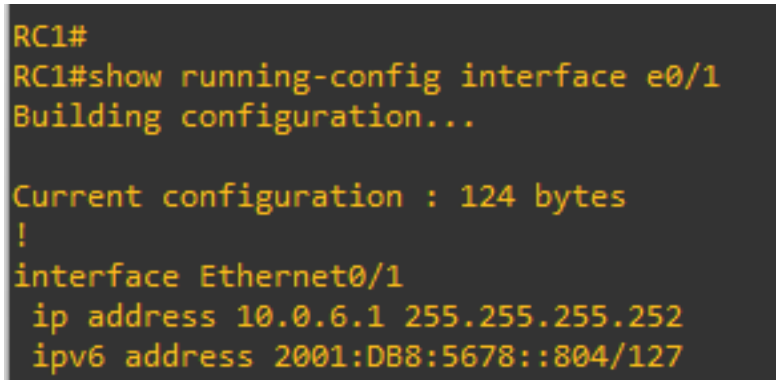


FIGURE 2.10 : Adresse IPv6 de l'interface Ethernet0/1

2.3.2.2 Implémentation du routage OSPFv3 et BGPv6

Dans cette implémentation, deux protocoles de routage ont été déployés pour assurer la propagation des routes IPv6 au sein du réseau : OSPFv3 pour le routage interne (IGP) et BGPv6 pour l'échange de routes externes avec des réseaux distants.

OSPFv3

Le protocole OSPFv3 a été activé sur tous les routeurs internes afin de découvrir les sous-réseaux IPv6 et de calculer les chemins optimaux pour acheminer le trafic à travers le réseau. De manière similaire à OSPF pour IPv4, OSPFv3 utilise les interfaces Loopback comme source des paquets OSPF, garantissant ainsi une identification unique et stable des routeurs à travers leurs adresses de Loopback.

L'activation d'OSPFv3 permet une meilleure convergence des routes dans le réseau interne en IPv6, tout en s'appuyant sur les mêmes principes de fonctionnement qu'OSPF pour IPv4, tels que **l'utilisation de la base de données d'état de liens (LSDB)** pour construire la topologie du réseau [17].

Le router-id en OSPFv3, bien qu'il s'agisse d'un protocole IPv6, reste exprimé en format IPv4 pour des raisons de compatibilité avec les versions précédentes d'OSPF.

Voici un exemple de la configuration OSPFv3 sur un routeur :

```
ipv6 router ospf 1
 router-id 20.20.20.20
 int Ethernet0/2
 ipv6 ospf 10 area 0
```

Cette configuration de base a été répliquée sur tous les autres routeurs du réseau, avec une adaptation du router-id et au niveau de l'interface pour chaque équipement. Chaque routeur participant à OSPFv3 utilise cette configuration pour échanger ses informations de routage et ses états de liens avec les autres routeurs.

Configuration OSPFv3 sur le routeur RC1

- Base de données OSPFv3 sur RC1

RC1 - PuTTY

```
RC1#
RC1#show ipv6 ospf database

            OSPFv3 Router with ID (30.30.30.30) (Process ID 10)

                Router Link States (Area 0)

ADV Router       Age         Seq#       Fragment ID  Link count  Bits
 10.10.10.10     272         0x80000003  0           2           None
 20.20.20.20     273         0x80000003  0           2           None
 30.30.30.30     271         0x80000003  0           4           None
 40.40.40.40     275         0x80000003  0           4           None
 50.50.50.50     275         0x80000003  0           4           None
 60.60.60.60     272         0x80000003  0           4           None
 70.70.70.70     278         0x80000002  0           2           None
 90.90.90.90     273         0x80000003  0           2           None

                Net Link States (Area 0)

ADV Router       Age         Seq#       Link ID    Rtr count
 20.20.20.20     278         0x80000001  8          2
 30.30.30.30     274         0x80000001  7          2
 40.40.40.40     275         0x80000001  3          2
 40.40.40.40     275         0x80000001  7          2
 50.50.50.50     275         0x80000001  3          2
 50.50.50.50     281         0x80000001  4          2
 60.60.60.60     277         0x80000001  3          2
 60.60.60.60     277         0x80000001  4          2
 60.60.60.60     277         0x80000001  5          2
 70.70.70.70     279         0x80000001  3          2
 90.90.90.90     273         0x80000001  3          2
 90.90.90.90     280         0x80000001  4          2

                Link (Type-8) Link States (Area 0)

ADV Router       Age         Seq#       Link ID    Interface
 10.10.10.10     313         0x80000002  7          Et1/0
 30.30.30.30     314         0x80000002  7          Et1/0
 30.30.30.30     314         0x80000002  5          Et0/2
 50.50.50.50     315         0x80000002  3          Et0/2
 30.30.30.30     314         0x80000002  4          Et0/1
 60.60.60.60     312         0x80000002  4          Et0/1
 30.30.30.30     314         0x80000002  3          Et0/0
 40.40.40.40     314         0x80000002  3          Et0/0
```

FIGURE 2.11 : Base de données OSPFv3 sur RC1

La base de données OSPFv3 sur RC1 stocke les informations de topologie collectées via les

paquets d'état de lien (LSA), permettant au routeur de construire une carte complète du réseau et de calculer les chemins les plus courts.

- **Table de routage ospfv3 sur RC1**

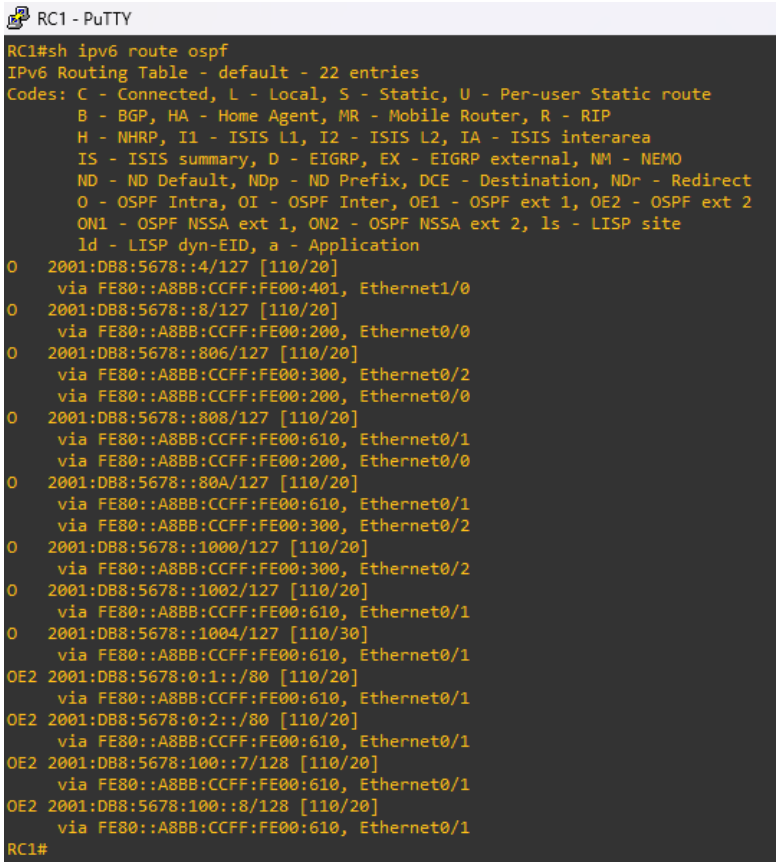


FIGURE 2.12 : Table de routage ospfv3 sur RC1

La table de routage OSPFv3 contient les routes apprises via OSPFv3, permettant au routeur de déterminer le chemin optimal pour chaque destination IPv6 dans le réseau. Chaque entrée de la table de routage indique le prochain saut pour atteindre un sous-réseau donné, basé sur l'algorithme de plus court chemin (SPF).

Pour les routeurs reliés aux clients, une configuration similaire a été appliquée. Cependant, une commande supplémentaire a été introduite pour redistribuer les routes connectées directement à ces routeurs dans OSPFv3. Cette redistribution assure que les sous-réseaux connectés aux interfaces clients sont également annoncés dans la topologie globale OSPFv3.

La commande spécifique utilisée est :

```
1    redistribute connected
```

Cette approche garantit que tous les sous-réseaux clients sont correctement propagés à travers le réseau OSPFv3, offrant ainsi une visibilité complète de la topologie et permettant une acheminement efficace du trafic.

BGPv6

Le BGPv6 (Border Gateway Protocol version 6) a été mis en œuvre pour l'échange de routes IPv6 avec des réseaux externes, jouant ainsi le rôle de protocole de routage externe (EGP) [18]. Alors que OSPFv3 est utilisé pour la gestion des routes à l'intérieur du réseau interne, BGPv6 permet de maintenir les relations de peering avec les autres systèmes autonomes (AS) afin de s'assurer que les routes IPv6 peuvent être échangées entre différents réseaux à grande échelle.

BGPv6 se base sur les mêmes principes que BGP pour IPv4, mais avec quelques modifications pour supporter le routage des adresses IPv6. Il est configuré au niveau des routeurs des frontières qui connectent le réseau à des systèmes externes. BGPv6 gère l'énorme espace d'adressage IPv6 et facilite l'échange de tables de routage massives entre différents AS, garantissant que chaque réseau puisse connaître les chemins vers les autres réseaux IPv6.

Configuration BGPv6 sur le routeur RC3



FIGURE 2.13 : Configuration BGPv6 sur RC3

Table de routage BGPv6

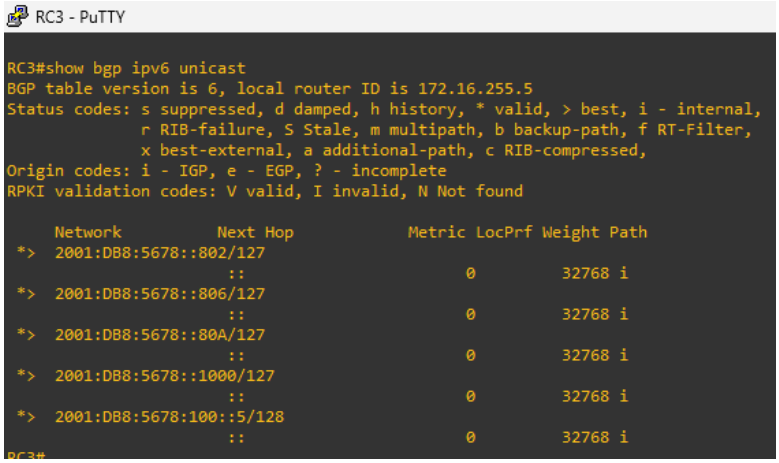


FIGURE 2.14 : Table de routage BGPv6 sur RC3

2.3.3 Configuration de sécurité de base pour IPv6

Dans le cadre de la transition vers IPv6, la sécurité est un aspect primordial pour protéger l'infrastructure réseau d'ISOCEL Telecom contre les menaces émergentes. La mise en œuvre de mécanismes de sécurité avancés vise à assurer une protection efficace contre les attaques courantes liées à IPv6, tout en maintenant une connectivité fluide. Les principales mesures de sécurité appliquées incluent la configuration des Access Control Lists (ACL) [19], la protection du Neighbor Discovery Protocol (NDP) et la sécurisation des interfaces locales [20].

2.3.3.1 Configuration des ACLs (Access Control Lists) IPv6

Les listes de contrôle d'accès (ACLs) sont essentielles pour restreindre le trafic non autorisé dans le réseau IPv6. Contrairement à IPv4, **IPv6 dispose de ses propres ACLs spécifiques** qui permettent de **contrôler le trafic à un niveau plus granulaire**.
Dans ce projet, les ACLs IPv6 ont été configurées pour bloquer le trafic non autorisé entre les différents segments du réseau tout en permettant les communications légitimes.

Voici un exemple de configuration d'ACL IPv6 appliquée sur le routeur R1 :

```
ipv6 access-list BLOCK_UNAUTHORIZED
permit ipv6 2001:db8:5678:0:1::/80 any
permit ipv6 2001:db8:5678:0:2::/80 any
deny ipv6 any 2001:db8:5678:800::/117
deny ipv6 any any log
!
interface Ethernet0/0
ipv6 traffic-filter BLOCK_UNAUTHORIZED in
```

Cette configuration permet de bloquer tout le trafic IPv6 non autorisé en provenance ou à destination du segment réseau associé

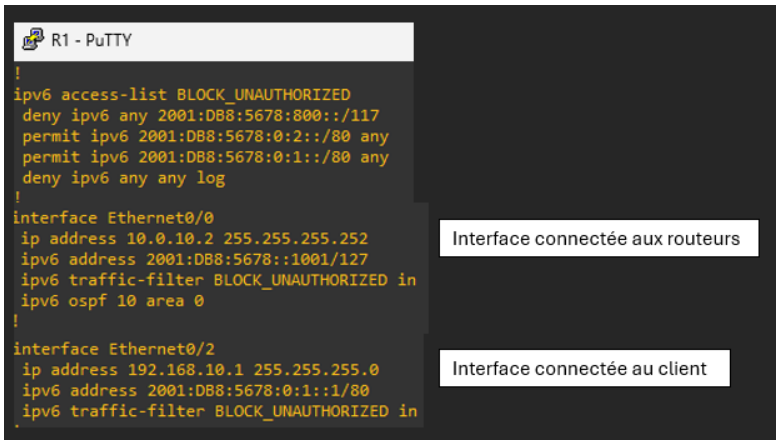


FIGURE 2.15 : ACL Implémentés sur R1 sur les interfaces Ethernet 0/0 et Ethernet 0.2

2.3.3.2 Protection du Neighbor Discovery Protocol (NDP)

Le Neighbor Discovery Protocol (NDP) joue un rôle crucial dans la communication au sein des réseaux IPv6, en gérant des fonctions essentielles telles que **la découverte des routeurs voisins**, **la résolution d'adresses** et **la détection des adresses dupliquées (DAD)**.
Cependant, le NDP présente des vulnérabilités intrinsèques qui peuvent être exploitées pour diverses attaques, notamment **l'usurpation d'identité (spoofing)**, **l'empoisonnement des tables de voisins**, ou encore les attaques de type **"Denial of Service" (DoS)**.
Ces vulnérabilités peuvent permettre à des attaquants de perturber ou de détourner le trafic réseau. Pour contrer ces menaces, plusieurs mécanismes de protection peuvent être mis en place. Deux des solutions les plus efficaces sont le RA (Router Advertisement) Guard et le DHCPv6 Guard. Ces fonctionnalités permettent de filtrer et bloquer les messages non autorisés qui circulent au sein du réseau, renforçant ainsi la sécurité du NDP.

1. **RA Guard.**

   RA Guard est une fonctionnalité de sécurité conçue pour empêcher les attaques par usurpation des annonces de routeurs (**Router Advertisements ou RA**). Ces annonces sont utilisées pour informer les appareils clients sur le réseau de la présence de routeurs disponibles et des paramètres de configuration d'adresse IPv6. Un attaquant pourrait, en envoyant de fausses annonces RA, rediriger le trafic ou causer des interruptions du service. RA Guard bloque ces annonces non autorisées sur les interfaces, limitant ainsi les attaques potentielles.

   Fonctionnement :

   - RA Guard vérifie les annonces de routeur qui transitent sur une interface réseau et autorise uniquement celles provenant de routeurs légitimes configurés par l'administrateur.
   - Les annonces envoyées par des sources non autorisées sont bloquées, empêchant les attaques de type "rogue RA" ou les configurations malveillantes sur le réseau.

2. **DHCPv6 Guard**

   Le DHCPv6 Guard est un autre mécanisme de protection qui bloque les messages DHCPv6 illégitimes. Le protocole DHCPv6 est utilisé par les clients pour obtenir dynamiquement des adresses IPv6 et des informations de configuration réseau. Un attaquant pourrait usurper un

serveur DHCPv6 légitime et envoyer des réponses malveillantes, ce qui pourrait entraîner la distribution d'adresses incorrectes ou malveillantes aux clients.

Fonctionnement :

- DHCPv6 Guard identifie les réponses DHCPv6 provenant des serveurs autorisés et filtre toutes les autres réponses non conformes.
- Les interfaces configurées avec DHCPv6 Guard sont protégées contre les serveurs DHCPv6 illicites, empêchant ainsi des attaques par empoisonnement DHCP.

3. **Configuration de RA Guard et DHCPv6 Guard**

   Pour mettre en place ces protections, il est nécessaire de configurer les interfaces concernées sur les routeurs. Dans notre implémentation réseau, l'objectif est de protéger les interfaces sensibles, notamment celles exposées au trafic provenant de sources non fiables.

   Voici un exemple de configuration qui pourrait être utilisée pour sécuriser une interface sur nos routeurs contre les attaques RA et DHCPv6 :

```
interface tEthernet0/0
ipv6 nd ra guard
ipv6 dhcp guard policy DHCPV6_PROTECT
```

2.3.3.3 Sécurisation des interfaces locales

Une autre mesure de sécurité consiste à sécuriser les interfaces locales pour empêcher l'exploitation des annonces ICMPv6 et bloquer les messages potentiellement malveillants. Un filtrage des paquets ICMPv6 est mis en place via les ACLs afin de bloquer certaines annonces tout en autorisant les paquets légitimes comme les pings.

Exemple de configuration sur R1 pour bloquer les annonces ICMPv6 indésirables :

```
ipv6 access-list BLOCK_MALICIOUS_ICMP
deny icmp any any router-advertisement
permit icmp any any echo-request
!
interface GigabitEthernet0/1
ipv6 traffic-filter BLOCK_MALICIOUS_ICMP in
```

Conclusion

En somme, la conception et le déploiement du réseau dual-stack d'ISOCEL Telecom ont permis de mettre en place une architecture intégrant efficacement IPv4 et IPv6. Les différentes configurations d'adressage, de routage et de sécurité, comme l'implémentation des ACLs et la protection du Neighbor Discovery Protocol (NDP), ont permis d'assurer une connectivité fluide et sécurisée. Ce déploiement pose les bases d'une transition progressive et contrôlée vers l'IPv6, assurant ainsi la pérennité et la fiabilité du réseau face aux besoins futurs.

Chapitre 3

Résultats et Discussions

Introduction

Dans cette section, nous présenterons et analyserons les résultats obtenus à partir des tests effectués sur le réseau que nous avons configuré. Notre objectif est d'évaluer la connectivité et la sécurité du réseau afin de confirmer que les équipements et les configurations déployés respectent les exigences de communication et de sécurité attendues.

3.1 Test de connectivité

La première étape des tests a consisté à vérifier la connectivité globale au sein du réseau pour s'assurer que toutes les configurations appliquées, aussi bien pour IPv4 que pour IPv6, permettent aux différents nœuds de communiquer efficacement. Nous avons utilisé des tests de ping pour valider la connectivité entre les différents équipements du réseau (routeurs, commutateurs, serveurs, et postes clients). Ces tests ont été effectués sur l'ensemble des sous-réseaux configurés, à la fois pour les adresses IPv4 et IPv6.

Pour IPv4, nous avons vérifié si les hôtes étaient capables de joindre les autres machines via les adresses IP, y compris à travers le NAT pour l'accès à Internet. Chaque segment de réseau a fait l'objet d'un test de connectivité bidirectionnelle afin de garantir l'intégrité des routes configurées.

Test de connectivité entre PC1 - RE1

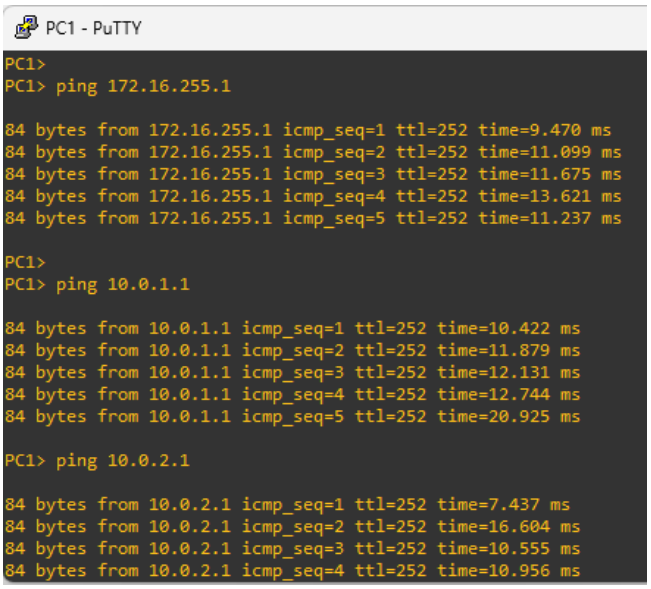


FIGURE 3.1 : Pingtest PC1-RE1

Test de connectivité entre PC1 - RC3

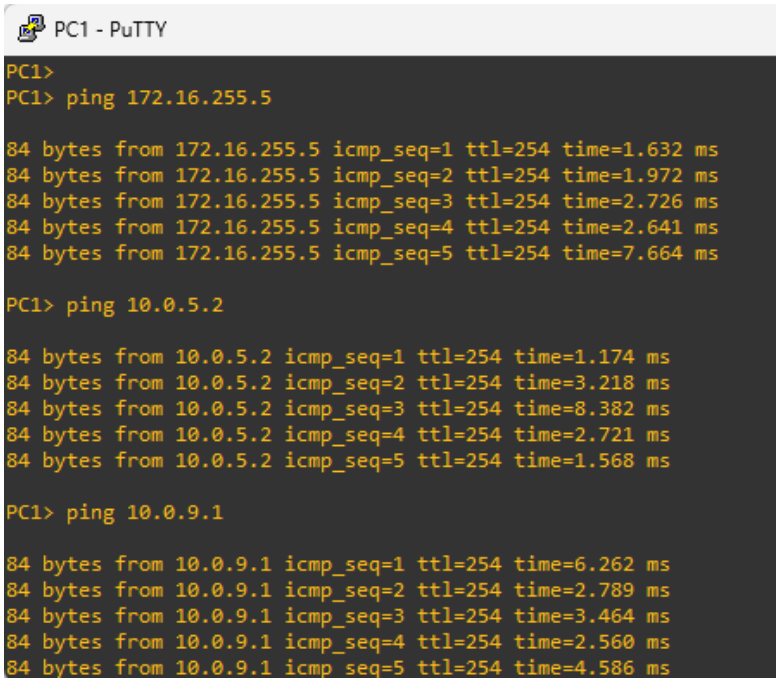


FIGURE 3.2 : Pingtest PC1-RC3

Test de connectivité entre PC1 - R1

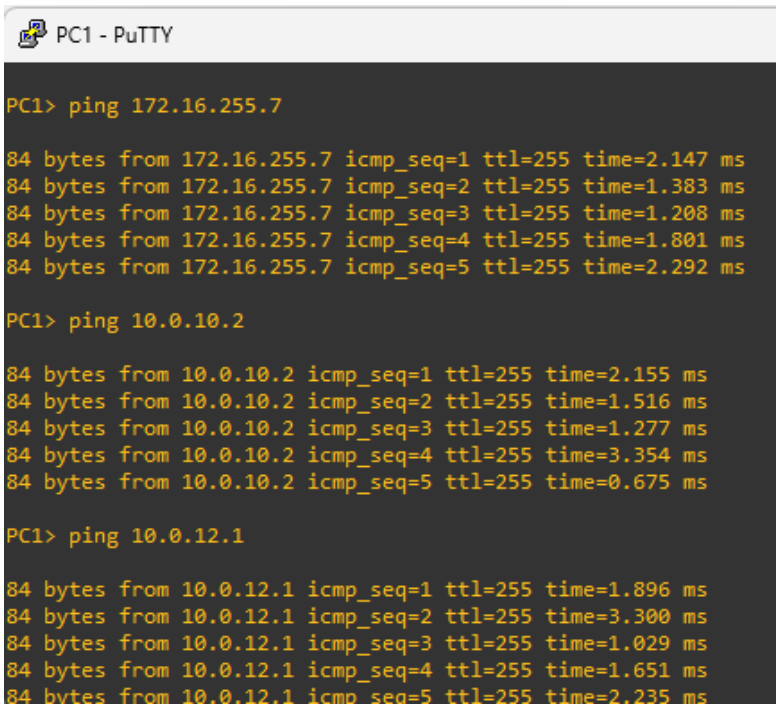


FIGURE 3.3 : Pingtest PC1-RC3

Test de connectivité vers internet

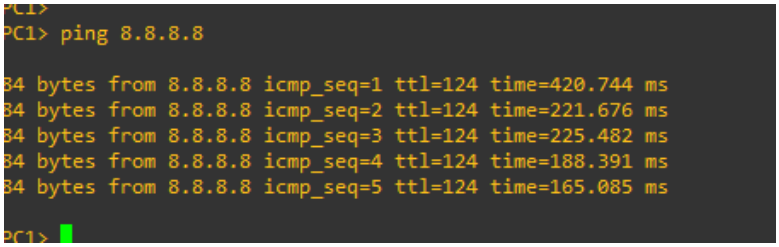


FIGURE 3.4 : Pingtest Google DNS

Du côté **IPv6**, nous avons évalué la connectivité en réalisant des pingtests entre les clients et les différents routeurs du réseau. Ce test a permis de vérifier si les adresses IPv6 globales assignées étaient correctement routées à travers le réseau et si les hôtes étaient capables de communiquer au-delà de leur sous-réseau local.
Une attention particulière a été portée à la compatibilité Dual-Stack, garantissant que les machines peuvent communiquer simultanément en IPv4 et en IPv6 sans conflit.

Test de connectivité entre IPv6 entre PC2 et RE1

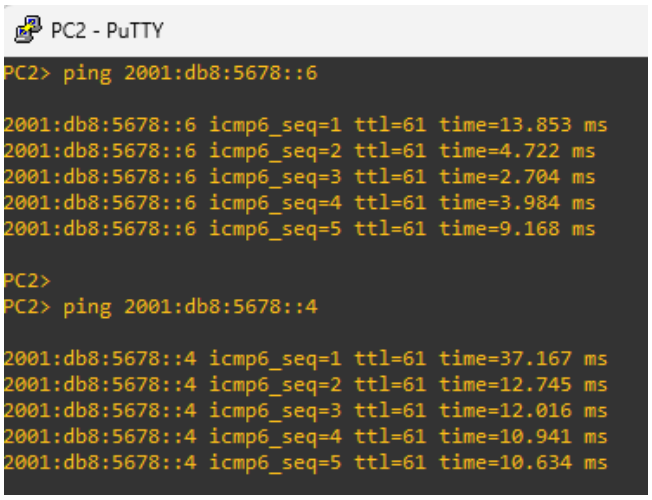


FIGURE 3.5 : Pingtest PC2-RE1

Test de connectivité entre IPv6 entre PC2-RC3

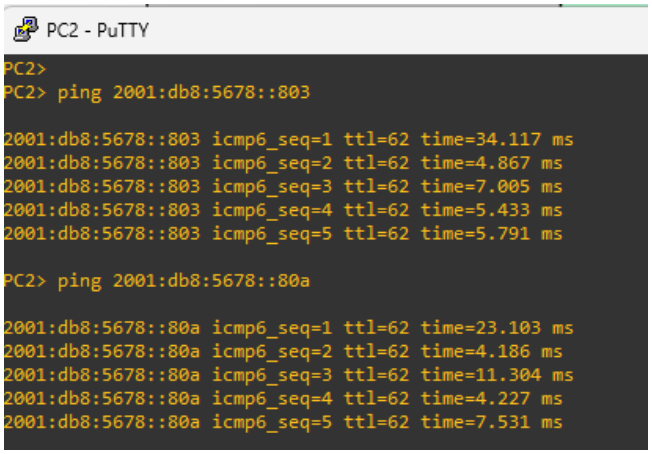


FIGURE 3.6 : Pingtest PC2-RC3

Test de connectivité entre IPv6 entre PC2 - R1

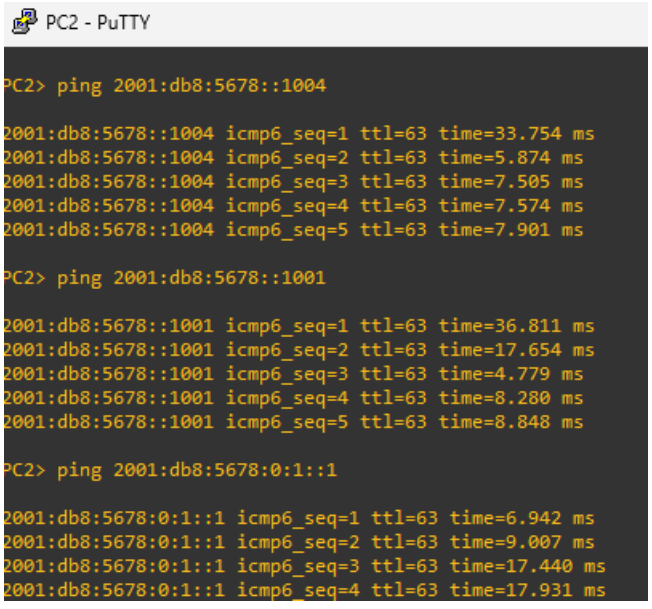


FIGURE 3.7 : Pingtest PC2-R1

3.2 Test de Sécurité

De manière générale, il est impératif que les clients ne puissent pas établir de communication directe avec les routeurs du cœur de réseau (core routers), afin de préserver la sécurité et l'intégrité de l'infrastructure. Pour assurer cette séparation, des listes de contrôle d'accès (Access Control Lists - ACLs) ont été déployées sur le routeur R1. Ces ACLs permettent de filtrer le trafic et de restreindre les communications des clients uniquement aux équipements autorisés. Grâce à cette configuration, les clients ne peuvent interagir qu'avec les services et les équipements pour lesquels ils disposent de l'autorisation nécessaire, bloquant ainsi tout accès non sollicité vers les routeurs de cœur.

Pour illustrer l'efficacité des ACLs mises en place, nous avons effectué une série de tests de connectivité, notamment entre PC1 et RC3. Sans ces ACLs, PC1 serait théoriquement capable d'envoyer des requêtes et de recevoir des réponses de la part de RC3. Cependant, suite à la mise en place des ACLs sur R1, le trafic indésirable entre ces deux éléments est bloqué.

Les résultats de cette configuration sont présentés ci-dessous, démontrant que les tentatives de communication directe entre PC1 et RC3 sont bloquées, conformément aux règles de filtrage définies.

Connectivité PC1-RC3 suite à la mise en place des ACL

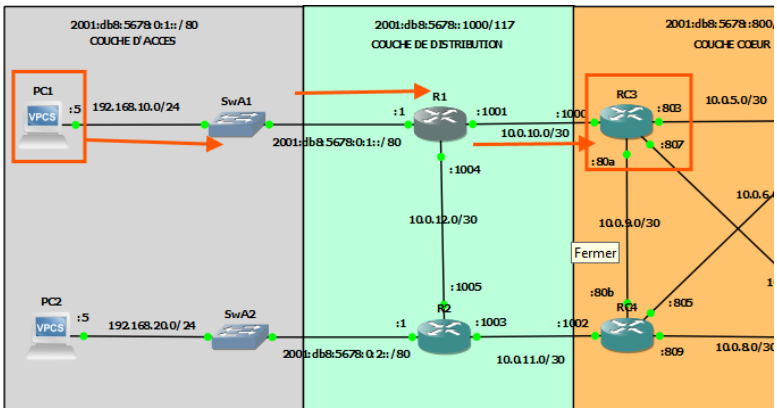


FIGURE 3.8 : PC1 vers RC3



FIGURE 3.9 : Pingtest PC1 vers RC3

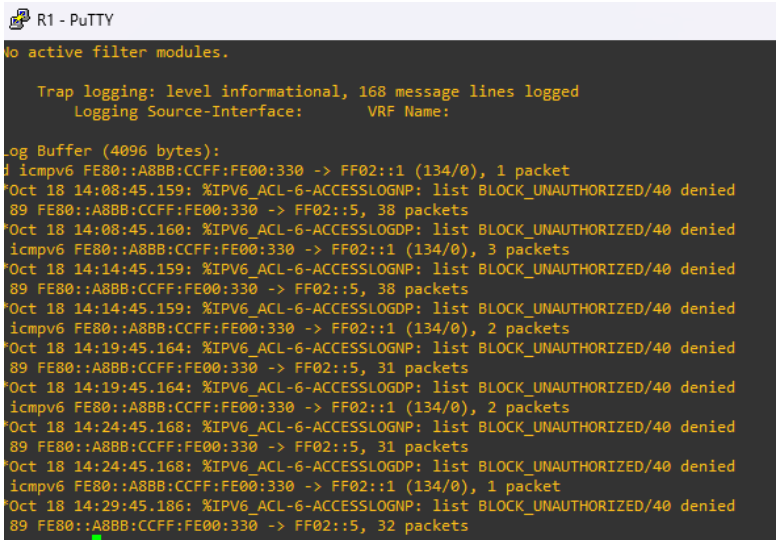


FIGURE 3.10 : Action de l'ACL

il était prévu de mener des tests approfondis de sécurité sur le réseau dual-stack (IPv4/IPv6). Ces tests avaient pour but de valider la robustesse du réseau face à des attaques potentielles et à des comportements non désirés. Les configurations de sécurité suivantes devaient être testées :

- **Protection du Neighbor Discovery Protocol (NDP)** : Étant donné que NDP est un protocole clé en IPv6 pour la découverte des voisins [21], sa protection est cruciale pour prévenir les attaques de type Neighbor Solicitation/Advertisement Spoofing.
- **RA Guard** : Ce mécanisme permet de bloquer les annonces de routeur malveillantes . L'activation du RA Guard [22] sur les interfaces locales devait permettre de sécuriser le réseau contre les faux routeurs IPv6.
- **Sécurisation des tables de binding (SLAAC)** : L'objectif était d'empêcher les manipulations non autorisées des adresses autoconfigurées à travers le Stateless Address AutoConfiguration (SLAAC).

Dans un environnement réel, il est primordial d'intégrer ces mécanismes de sécurité dès le déploiement initial du réseau IPv6.

Ces contrôles permettent de limiter les risques liés à des **attaques spécifiques à IPv6**, comme les attaques par **spoofing du Neighbor Discovery Protocol (NDP)**, ou encore les attaques de type **rogue router advertisement**.

De plus, la mise en place d'ACLs rigoureuses et la segmentation du réseau permettraient de restreindre les accès non autorisés aux ressources internes

3.3 Discussions

Bien que le réseau IPv6 ait été correctement configuré pour les tests de connectivité, certaines limitations inhérentes à l'outil de simulation **GNS3** ont empêché l'implémentation complète des mécanismes de sécurité prévus, tels que **la protection du Neighbor Discovery Protocol (NDP)** et la **configuration des RA Guard**.

Ces fonctionnalités, bien que configurables dans un environnement de production réel, n'ont pas pu être simulées avec précision dans notre environnement de laboratoire.

Cependant, nous avons pu mettre en place certaines **Access Control Lists (ACLs)** et tester leur efficacité sur le réseau dual-stack, ce qui constitue un premier niveau de sécurité.

Conclusion

La mise en œuvre des protocoles IPv4 et IPv6 au sein du réseau simulé a permis de démontrer les possibilités et les défis inhérents à la coexistence de ces deux technologies dans une architecture dual-stack. À travers les tests de connectivité, nous avons validé la capacité des différents nœuds à communiquer entre eux, assurant une transition fluide entre les deux protocoles. En parallèle, l'application des mécanismes de sécurité, notamment à travers les listes d'accès (ACL), a renforcé la protection des équipements critiques du réseau, bloquant les tentatives de communication non autorisées tout en maintenant un accès contrôlé aux services nécessaires.

Conclusion générale et perspectives

Dans le présent mémoire, nous avons abordé le déploiement sécurisé de l'IPv6 au sein d'ISOCEL Telecom. Cela nous a permis d'explorer les enjeux techniques et sécuritaires liés à la transition vers cette nouvelle technologie.

En mettant en place un réseau dual-stack, nous avons assuré la continuité du service tout en introduisant progressivement IPv6. Sur le plan sécuritaire, l'utilisation d'ACLs, la protection du Neighbor Discovery Protocol (NDP) et la gestion des Neighbor Binding Table permettront de renforcer la sécurité du réseau de ISOCEL Telecom et de protéger les équipements critiques. Ce projet constitue une base solide pour la future intégration complète d'IPv6 chez ISOCEL Telecom, tout en posant les fondations pour une architecture réseau prête à affronter les défis de demain.

Parmis les perspectives futures envisagées pour ce projet, il est essentiel de renforcer la sécurité IPv6 au sein de réseau ainsi que d'optimiser les services IPv6 pour les clients en leur offranr des services IPv6 natifs.

Bibliographie

[1] Philippe Latu. Adressage ipv4. Présentation du fonctionnement de la technologie IP.

[2] Jon Postel. Internet protocol. 1981. 44 pages.

[3] Y. Rekhter. Address Allocation for Private Internets. 1996. describes address allocation for private internets.

[4] Najib ELKAMOUN Rachid HILAL Khalid EL KHADIRI, Ouidad LABOUIDYA. Etude comparative des mécanismes de transition de l'ipv4 à l'ipv6. *Mediterranean Telecommunications Journal*, 2017.

Webographie

[5] Wikipédia. Histoire d'internet. https://fr.wikipedia.org/wiki/Histoire_d%27Internet. Explosion de l'internet dans les années 1990 et 2000.

[6] APNic. Ipv4 exhaustion and address space management. https://blog.apnic.net. Explications sur la pénurie d'adresses IPv4 et les solutions mises en place pour y remédier.

[7] Wikipédia. Plages d'adresses ip spéciales. https://fr.wikipedia.org/wiki/Adresse_IP. adresses IP réservées à un usage particulier (RFC 5735).

[8] Wikipédia. Carrier-grade nat. https://fr.wikipedia.org/wiki/Carrier-grade_NAT. Explication de ce qu'est le Carrier Grade NAT.

[9] trouver ip.info. l'épuisement des adresses ipv4 : Comprendre les enjeux et explorer les solutions. https://trouver-ip.info/enjeux-solutions-epuisement-adresses-ipv4/. Enjeux et solutions par rapport à l'épuisement des adresses IPv4.

[10] Netwoek academy.io. Ipv6 stateless address auto-configuration (slaac). https://www.networkacademy.io/ccna/ipv6/stateless-address-autoconfiguration-slaac. describes address allocation for private internets.

[11] Advantages and features of ipv6. http://www.ipv6.com. Un aperçu des avantages, des fonctionnalités et des caractéristiques principales du protocole IPv6.

[12] ISolution. Ipv6 - caractéristiques. https://isolution.pro/fr/t/ipv6/ipv6-features/ipv6-caracteristiques. Caractéristiques du protocole IPv6.

[13] Wikipédia. Path mtu discovery. https://fr.wikipedia.org/wiki/Path_MTU_discovery. Explication du Path MTU discovery.

[14] Ipv6 security challenges and acls. https://www.sans.org. Articles traitant des défis de sécurité dans les environnements IPv6 et des meilleures pratiques pour les ACLs.

[15] AFRINIC Academy. Ipv6 addressing plans. https://academy.afrinic.net. Formation et documentation sur la planification des adresses IPv6 dans les réseaux.

[16] Juniper Networks. Ospf and bgp configuration for ipv4 and ipv6. https://www.juniper.net. Documentation sur la configuration du routage OSPF et BGP dans les environnements IPv4/IPv6.

[17] IETF RFC 5340. Ospf for ipv6 (ospfv3). https://tools.ietf.org/html/rfc5340. Guide sur le protocole OSPFv3 pour le routage IPv6.

[18] BGPv6. Bgpv6. https://bgpv6.com/. Tout sur le protocole BGPv6.

[19] SANS Institute. Ipv6 security challenges and acls. https://www.sans.org. Articles traitant des défis de sécurité dans les environnements IPv6 et des meilleures pratiques pour les ACLs.

[20] IETF RFC 6583. Mitigating neighbor discovery attacks on ipv6 networks. https://tools.ietf.org/html/rfc6583. Méthodes pour protéger le protocole de découverte de voisins (NDP) dans les réseaux IPv6.

[21] cbtnuggets. What is neighbor discovery protocol (ndp)? https://www.cbtnuggets.com/blog/technology/networking/what-is-neighbor-discovery-protocol-ndp. Tout sur le NDP.

[22] Jerome Durand. Se protéger des routeurs advertisements (ra) non désirés. https://gblogs.cisco.com/fr/reseaux/se-proteger-des-routeurs-advertisements-ra-non-desires/. Se protéger des RA non désirés.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux vii

Liste des acronymes viii

Introduction générale 1

1 Revue de littérature 3

Introduction . . . 3

1.1 Généralités . . . 3

1.1.1 Présentation de la technologie IP . . . 3

1.2 Historique de IPv4 . . . 4

1.2.1 Causes de l'épuisement . . . 5

1.2.2 Mécanismes de maintien d'IPv4 . . . 6

1.3 Genèse d'IPv6 . . . 8

1.3.1 Présentation d'IPv6 . . . 8

1.3.2 Caractéristiques d'IPv6 . . . 8

1.4 Comparaison entre IPv4 et IPv6 . . . 11

1.5 Mécanismes de Transition vers IPv6 . . . 13

1.5.1 Dual Stack . . . 13

1.5.1.1 Avantages du Dual Stack . . . 13

1.5.1.2 Inconvénients du Dual Stack . . . 14

1.5.2 Tunneling . . . 14

1.5.2.1 Avantages du Tunelling . . . 14

1.5.2.2 Inconvénients du Tunneling . . . 15

1.5.3 NAT64 . . . 15

1.5.3.1 Avantages du NAT64 . . . 15

1.5.3.2 Inconvénients du NAT64 . . . 15

1.5.4 Choix du Dual Stack . . . 16

2 Conception et Déploiement **17**
Introduction . . . 17
2.1 Présentation de l'architecture réseau de ISOCEL Telecom . . . 17
2.2 Mise en place du plan d'adressage . . . 18
2.3 Implémentation pratique . . . 19
2.3.1 Configuration IPv4 . . . 19
2.3.1.1 Adressage du réseau en IPv4 . . . 19
2.3.1.2 Utilisation des interfaces de loopback . . . 20
2.3.1.3 Protocole de routage IPv4 : OSPF et BGP . . . 21
2.3.2 Implémentation IPv6 . . . 26
2.3.2.1 Configuration des adresses IPv6 sur les interfaces . . . 27
2.3.2.2 Implémentation du routage OSPFv3 et BGPv6 . . . 27
2.3.3 Configuration de sécurité de base pour IPv6 . . . 31
2.3.3.1 Configuration des ACLs (Access Control Lists) IPv6 . . . 31
2.3.3.2 **Protection du Neighbor Discovery Protocol (NDP)** . . . 32
2.3.3.3 Sécurisation des interfaces locales . . . 33

3 Résultats et Discussions **35**
Introduction . . . 35
3.1 Test de connectivité . . . 35
3.2 Test de Sécurité . . . 39
3.3 Discussions . . . 41

Conclusion générale et perspectives **42**

Bibliographie **43**

Webographie **44**

Table des matières **46**