Tunisian Republic
Ministry of Higher Education and Research

Private Higher School of Technologies & Engineering

Rapport de projet

Level : SSIR

Conception et mise en place d'une solution IXP Internt basée sur IPV6

établie par GHASSEN LANDOULSI et BELHASSEN HASHOUS et KNANI MED ALI

2024 - 2025

Contents

General Introduction

As part of my engineering studies at the Private Higher School of Technologies Engineering, I sought an internship that would allow me to deepen my expertise in cybersecurity, particularly in code security assessment and penetration testing. HEXAGONE has committed itself to ensuring that modern organizations are well-equipped to tackle cyber threats, employing advanced methodologies to secure their codebases and systems. During my internship, I benefited immensely from the collaborative and knowledge-driven environment fostered by the company's experienced team, who supported me in developing both technical and analytical skills.

This report begins with a description of the hosting company and its mission. The second chapter explores SonarQube's role in code security assessment, covering its integration within development pipelines, key security features, and configuration for project-specific needs. The third chapter provides an in-depth look at blackbox penetration testing, where I describe the methodology, tools, and findings relevant to securing real-world applications. Finally, the report concludes with a summary of my experiences and the knowledge I gained during this project, highlighting its contribution to my growth in cybersecurity practices.

Chapter 1

Etude de l'existant

1.1 Définition d'un IXP (Internet Exchange Point)

Un IXP est une infrastructure qui permet à plusieurs réseaux autonomes (AS) d'échanger du trafic directement, sans avoir recours à un fournisseur de transit tiers. Cette interconnexion réduit les coûts, améliore la latence et la performance, tout en assurant une meilleure résilience. Les IXP sont critiques pour l'écosystème de l'Internet, en facilitant le peering entre les opérateurs, fournisseurs de services Internet (ISP), opérateurs de contenu, etc.

1.2 État actuel des IXP dans le monde

- De nombreux IXP sont déjà en place dans les principales régions du monde. Les plus notables incluent des IXP comme le DE-CIX (Allemagne), AMS-IX (Pays-Bas), et LINX (Royaume-Uni). Ces IXP opèrent généralement en IPv4, bien que certains aient commencé à intégrer des capacités IPv6, pour répondre à la transition vers ce protocole.

Exemples d'IXP existants : - AMS-IX (Amsterdam Internet Exchange)
- DE-CIX (German Commercial Internet Exchange)
- LINX (London Internet Exchange)
- France-IX
- NIXI (National Internet Exchange of India)

1.3 Transition vers IPv6 dans les IXP

Avec l'épuisement des adresses IPv4, la transition vers IPv6 est devenue une nécessité. Plusieurs IXP ont déjà commencé à offrir des services basés sur IPv6, mais la migration complète vers ce protocole est encore en cours dans de nombreuses régions. Les IXP doivent non seulement permettre le peering en IPv6, mais aussi assurer la coexistence avec IPv4, car de nombreux réseaux ne sont pas encore entièrement compatibles avec IPv6.

Progrès de l'adoption d'IPv6 : Statistiques d'adoption de l'IPv6 au niveau mondial :

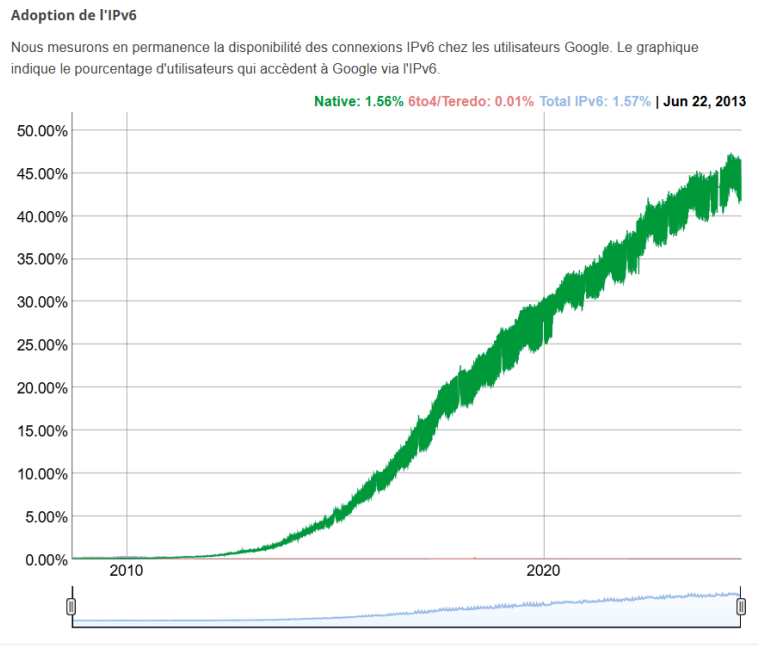

Figure 1.1: Statistiques

1.4 Avantages d'un IXP basé sur IPv6

Pérennité : IPv6 offre un espace d'adressage beaucoup plus grand que l'IPv4, garantissant la viabilité à long terme des IXP et évitant les problèmes liés à l'épuisement des adresses.
Simplicité : IPv6 supprime certaines des complexités d'IPv4 comme le NAT (Network Address Translation), ce qui peut simplifier la gestion et le routage des réseaux.
Interconnexion mondiale : Les IXP en IPv6 facilitent l'interconnexion entre les réseaux ayant adopté IPv6, permettant une meilleure performance et latence pour les communications.

1.5 Exemples d'IXP IPv6 en place

AMS-IX, DE-CIX et d'autres ont déjà une infrastructure prête pour IPv6. Il est important d'étudier ces modèles pour comprendre les défis rencontrés, les solutions mises en œuvre, et les meilleures pratiques adoptées.

1.6 Problématiques spécifiques à IPv6 dans les IXP

Même si IPv6 résout le problème de l'épuisement des adresses IP, il présente aussi des défis spécifiques à son déploiement dans un IXP :

- Les **coûts de migration** pour les opérateurs et fournisseurs de services.
- La **sécurité des adresses IPv6** (ex. ICMPv6, Neighbor Discovery Protocol) qui nécessite de nouvelles approches et technologies pour assurer la protection contre les attaques.

1.7 Conclusion

L'étude de l'existant montre que, bien que les IXP soient bien établis et efficaces avec IPv4, la migration vers IPv6 est en cours et nécessaire pour la pérennité de ces infrastructures. Les défis techniques et opérationnels doivent être surmontés pour garantir une transition fluide, et les exemples d'IXP leaders montrent la voie à suivre pour la mise en place d'une telle solution basée sur IPv6.

Chapter 2

PROBLEMATIQUE

2.1 Contexte général

L'épuisement des adresses IPv4 a poussé le monde de l'Internet à se tourner vers IPv6, un protocole conçu pour répondre à la demande croissante en adresses IP. Bien que le déploiement d'IPv6 ait commencé il y a plusieurs années, l'adoption reste inégale à travers le monde. Les IXP jouent un rôle crucial dans l'interconnexion des réseaux, et leur transition vers IPv6 est essentielle pour permettre un trafic fluide entre les réseaux adoptant ce protocole.

2.2 Manque d'adoption d'IPv6 dans les IXP

L'un des principaux problèmes actuels est que, malgré la nécessité d'IPv6, de nombreux IXP et acteurs du marché tardent à adopter pleinement ce protocole. La majorité des échanges de trafic à travers les IXP se fait encore en IPv4, et plusieurs réseaux autonomes (AS) n'ont pas encore migré vers IPv6.
Faible adoption : Moins de 45 des réseaux mondiaux sont configurés pour utiliser IPv6 de manière native.
Réticence des opérateurs : Beaucoup d'AS sont réticents à investir dans l'infrastructure nécessaire pour supporter IPv6, ce qui freine la transition des IXP.

2.3 Coûts de migration vers IPv6

La mise en œuvre d'une infrastructure IPv6 au sein des IXP nécessite des investissements significatifs, tant en termes d'équipement réseau (routeurs, commutateurs) que de formation des équipes techniques.
Infrastructures obsolètes : De nombreux IXP fonctionnent avec des équipements réseau plus anciens qui ne supportent pas nativement IPv6. Le remplacement de ces équipements peut être coûteux.
Formation et compétences : Les équipes techniques doivent être formées aux spécificités d'IPv6, ce qui représente une barrière pour certaines petites organisations qui manquent de ressources humaines ou financières.

2.4 Sécurité dans un environnement IPv6

La transition vers IPv6 introduit également de nouvelles problématiques de sécurité. Alors qu'IPv6 était initialement perçu comme plus sécurisé, de nouvelles menaces spécifiques ont émergé.

Protocole Neighbor Discovery : L'une des principales vulnérabilités associées à IPv6 réside dans le protocole de découverte de voisins (Neighbor Discovery Protocol), qui peut être exploité pour des attaques de type spoofing ou man-in-the-middle.
Nouvel espace d'attaque : L'espace d'adressage IPv6 étant plus vaste, cela peut compliquer la surveillance des réseaux et la détection des attaques, en particulier pour les IXP où des milliers d'AS sont connectés.

2.5 Latence et performance dans un environnement IPv6

Bien que l'IPv6 soit conçu pour améliorer la performance et la résilience, certains opérateurs rapportent une latence plus élevée lors de l'échange de trafic via IPv6 comparé à IPv4, principalement à cause de la configuration sous-optimale des routes et du peering.

Performance sous-optimale : Le manque de support complet d'IPv6 dans certains IXP peut provoquer des détours de routage, augmentant ainsi la latence et affectant la performance globale du réseau.
Optimisation du routage : La gestion des routes IPv6 est encore en développement dans certains contextes, ce qui rend difficile l'optimisation des performances dans les IXP.

2.6 Résumé de la problématique

La problématique générale dans le cadre de ce projet est donc la suivante : Comment concevoir et mettre en place une solution IXP entièrement basée sur IPv6 qui résout les défis de la transition, tout en garantissant la compatibilité avec IPv4, et en minimisant les coûts et les risques de sécurité ?

Cette problématique englobe plusieurs enjeux :
- Accélérer l'adoption d'IPv6 dans les IXP.
- Gérer la cohabitation entre IPv4 et IPv6 de manière efficace.
- Réduire les coûts liés à la migration.
- Assurer une sécurité robuste dans un environnement IPv6.
- Optimiser la performance du réseau en IPv6.

Chapter 3

SOLUTION ENVISAGE

3.1 Introduction à la solution

La solution envisagée consiste à concevoir et simuler une infrastructure IXP basée sur le protocole IPv6, en utilisant l'outil de simulation réseau GNS3. Cette approche permet de reproduire les conditions réelles d'un IXP sans nécessiter de déployer immédiatement une infrastructure physique. L'objectif est de tester et valider la faisabilité technique et les performances d'une architecture IXP IPv6, tout en adressant les problématiques identifiées dans le chapitre précédent.

3.2 Présentation de GNS3

GNS3 (Graphical Network Simulator 3) est une plateforme de simulation réseau qui permet de modéliser des réseaux complexes en utilisant des routeurs, commutateurs et autres dispositifs réels ou virtuels. GNS3 est particulièrement utile pour simuler des environnements de production, comme un IXP, avant leur déploiement réel.

3.2.1 Avantages de GNS3

- Simulation réaliste : GNS3 permet de simuler le comportement réel des équipements réseau.
- Flexibilité : La plateforme supporte une large gamme d'équipements et de protocoles, incluant l'IPv6.
- Coûts réduits : Simuler l'infrastructure avec GNS3 évite d'investir dans des équipements coûteux pendant les phases de test.

3.3 Architecture de la solution IXP basée sur IPv6

La solution proposée implique la création d'une topologie IXP dans GNS3, intégrant plusieurs réseaux autonomes (AS) interconnectés via un routeur centralisé jouant le rôle de l'IXP. Voici les principales composantes de l'architecture :

Routeur IXP (IXP Router): Un routeur central qui servira de point de rencontre pour plusieurs AS. Il devra être capable de gérer les sessions de peering en IPv6.
Réseaux autonomes (AS) : Chaque AS sera représenté par un routeur ou une combinaison de routeurs, configurés pour supporter IPv6 et établir des sessions BGP avec l'IXP.
Sessions BGP IPv6 : Les routes IPv6 seront échangées entre les AS participants via le protocole BGP, ce qui est essentiel pour l'interconnexion dans un IXP.

3.4 Processus de configuration de l'IXP dans GNS3

Le processus de simulation d'un IXP dans GNS3 comprend plusieurs étapes techniques clés :

Étape 1 : Création de la topologie réseau Utiliser GNS3 pour définir la topologie de l'IXP, en ajoutant un routeur pour représenter l'IXP, ainsi que plusieurs routeurs pour les différents AS connectés.
- Chaque routeur devra être configuré avec une adresse IPv6 unique pour chaque interface utilisée dans les échanges BGP.
Étape 2 : Configuration des sessions BGP Configurer le protocole BGP sur chaque routeur AS afin de permettre l'échange de routes IPv6 via l'IXP. Le routeur IXP central agira comme intermédiaire pour l'échange de routes entre les différents AS.
- Le peering IPv6 sera établi en utilisant les adresses IPv6 attribuées à chaque AS et au routeur de l'IXP.
Étape 3 : Tests de connectivité IPv6 Une fois la configuration terminée, effectuer des tests de connectivité en envoyant du trafic entre les différents AS à travers l'IXP.
- Les tests devront vérifier la propagation correcte des routes IPv6 et la connectivité de bout en bout.
Étape 4 : Sécurisation de l'IXP Configurer des mécanismes de sécurité sur les routeurs (filtrage de routes, ACLs, etc.) pour assurer une protection contre les attaques IPv6, telles que les attaques liées au Neighbor Discovery Protocol (NDP) et le spoofing des adresses.

3.4.1 Configuration des routeurs

Config du PE1

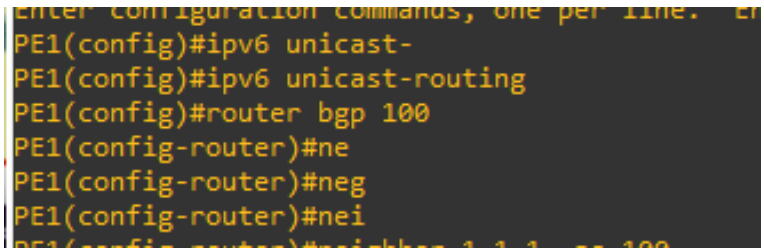

Figure 3.2: Configuration du PE1

Config du PE2

```
PE2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE2(config)#ipv6 uni
PE2(config)#ipv6 unicast-routing
PE2(config)#rout
PE2(config)#router bgp
PE2(config)#router bgp 100
PE2(config-router)#no bg
PE2(config-router)#no bgp def
PE2(config-router)#no bgp default ip
PE2(config-router)#no bgp default ipv4-unicast
PE2(config-router)#ne
PE2(config-router)#neg
PE2(config-router)#nei
PE2(config-router)#neighbor 1.1.1.1 re
PE2(config-router)#neighbor 1.1.1.1 remot
PE2(config-router)#neighbor 1.1.1.1 remote-as 100
PE2(config-router)#neighbor 1.1.1.1 upd
PE2(config-router)#neighbor 1.1.1.1 update-source l0
PE2(config-router)#add
PE2(config-router)#address-family ipv6 unic
PE2(config-router)#address-family ipv6 unicast
PE2(config-router-af)#ne
PE2(config-router-af)#neig
PE2(config-router-af)#neighbor  1.1.1.1 ac
PE2(config-router-af)#neighbor  1.1.1.1 activate
PE2(config-router-af)#neighbor  1.1.1.1 activa
*Nov 21 00:26:16.739: %BGP-5-ADJCHANGE: neighbor 1.1.1.1 Down Address family activated
PE2(config-router-af)#neighbor  1.1.1.1 se
PE2(config-router-af)#neighbor  1.1.1.1 send-l
PE2(config-router-af)#neighbor  1.1.1.1 send-label
PE2(config-router-af)#
```

Figure 3.3: Configuration du PE2

3.5 Optimisation de la performance IPv6

Afin de maximiser la performance du réseau en IPv6, certaines techniques d'optimisation seront mises en œuvre :

Optimisation du routage : En s'assurant que les routes BGP propagées sont optimisées pour réduire la latence et améliorer la performance.

3.6 Résolution des problématiques identifiées

La solution envisagée répond aux problématiques identifiées dans le chapitre précédent :

Migration économique: GNS3 permet de simuler le déploiement avant l'investissement réel dans des équipements.

Sécurité renforcée: En utilisant des mécanismes de sécurité appropriés, les vulnérabilités spécifiques à IPv6 seront atténuées.

Optimisation de la latence et des performances: En configurant correctement le routage BGP, la performance du réseau IPv6 sera maximisée, minimisant la latence.

3.7 Conclusion

La solution proposée, basée sur une simulation avec GNS3, permet de concevoir une architecture IXP fonctionnelle et entièrement compatible avec IPv6. Elle adresse les principales problématiques de migration, de compatibilité, de performance et de sécurité,

tout en permettant une évaluation réaliste des coûts et des besoins avant une mise en œuvre réelle.

General Conclusion

Dans un contexte où l'épuisement des adresses IPv4 et l'essor des technologies modernes exigent une transition vers l'IPv6, les Internet Exchange Points (IXP) jouent un rôle stratégique dans l'interconnexion des réseaux. Ce projet avait pour objectif de concevoir et simuler une solution IXP basée sur IPv6 afin de répondre aux besoins croissants d'évolutivité, de performance et de sécurité.

L'étude de l'existant a révélé que, malgré les efforts mondiaux pour promouvoir l'adoption d'IPv6, de nombreux obstacles techniques, économiques et organisationnels subsistent, notamment la cohabitation des protocoles IPv4 et IPv6, les défis liés à la sécurité, ainsi que les coûts de migration. Ces problématiques ont été au cœur de nos réflexions pour proposer une solution adaptée et réaliste.

La solution envisagée, basée sur l'utilisation de GNS3, a permis de simuler une infrastructure IXP complète. Cette approche a offert une plateforme flexible et économique pour valider les concepts techniques, tels que l'établissement de sessions BGP IPv6 entre réseaux autonomes, la gestion de la dual-stack IPv4/IPv6, ainsi que la mise en œuvre de mécanismes de sécurité robustes. De plus, les tests réalisés ont démontré la faisabilité d'une architecture optimisée pour minimiser la latence et garantir des performances élevées.

En conclusion, ce travail met en lumière l'importance d'une préparation approfondie et d'une simulation réaliste avant le déploiement physique d'une infrastructure IXP. La méthodologie adoptée, centrée sur l'utilisation d'outils modernes comme GNS3, permet non seulement de répondre aux défis techniques actuels, mais aussi d'anticiper les évolutions futures du paysage technologique. Cette étude pourrait servir de base pour des travaux ultérieurs visant à enrichir les fonctionnalités d'un IXP IPv6 ou à explorer des approches hybrides intégrant des technologies émergentes telles que SDN (Software-Defined Networking) ou l'automatisation avancée du routage.

List of Figures

Liste des acronymes

AS Autonomous System

ACL Access Control List

BGP Border Gateway Protocol

DE-CIX German Commercial Internet Exchange

GNS3 Graphical Network Simulator 3

ICMPv6 Internet Control Message Protocol for IPv6

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IXP Internet Exchange Point

LINX London Internet Exchange

NAT Network Address Translation

NDP Neighbor Discovery Protocol

NIXI National Internet Exchange of India