REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Domaine : science et technologie

Filière : Télécommunications

Spécialité : Réseaux et **T**élécommunications

Thème :

Mise en place d'un algorithme pour améliorer le QOS dans un réseaux « cas ATM MOBILIS »

Présenter par :

LAICHAOUI AMINA ***SAIDI DIHIA***

Devant le Jury composé de :

Promotrice : Mme Samira Mechid

Président : Mr Akliouat

Examinateur : Mme Haroun

Encadreur : Mr Hassani MOUSSA

Année universitaire:2023/2024

Remerciement

En préambule à ce mémoire nous remercions « ALLAH» de nous avoir aidé et donné la patience et le courage durant ces longues années d'études.

A mon Enseignant

Mme Samira Mechid

Nous tenons à exprimer notre profonde gratitude d'avoir eu l'honneur d'être parmi vos élèves et de bénéficier de votre riche enseignement. Votre reconnaissance envers l'un de nous en le désignant comme l'une de vos étudiantes préférées, avec la phrase touchante "il y a des étudiantes que j'aime spontanément et tu es l'une d'elles", a été une source de motivation extraordinaire pour nous. Vos qualités pédagogiques et humaines sont un modèle qui nous inspire. Votre gentillesse et votre disponibilité permanentes ont toujours suscité notre admiration. Nous tenons à vous remercier sincèrement pour l'immense honneur que vous nous avez fait en acceptant d'encadrer notre travail.

A mon Encadreur

Mr Hassani MOUSSA

Nous tenons à témoigner notre profond respect envers vos compétences exceptionnelles et votre encadrement de qualité. Nous vous exprimons notre sincère gratitude pour votre accueil chaleureux et vos conseils précieux. Par la présente, nous souhaitons vous faire part de notre reconnaissance et de notre estime profonde. Votre présence constante et votre soutien indéfectible jusqu'à la fin du projet ont été d'une valeur inestimable. Vos encouragements inlassables ont été une source de motivation inestimable. Nous sommes conscients que nos mots ne seront jamais suffisants pour exprimer notre gratitude envers vous.

Aux membres du jury

Mme haroune Mr. akliouat

Madame et Monsieur les jurys, vous nous faites un grand honneur en Acceptant de juger ce travail.

On doit des remerciements à tous les enseignants de la faculté technologie UMBB pour leurs qualités scientifiques et pédagogiques

Dédicaces

A la lumière de ma vie, mes très chers parents « BOUALEM & FADILA » Votre amour et votre soutien constants m'ont donné la motivation de vous rendre fiers.

A MA Mère « FADILA », IL est difficile de trouver les mots justes pour exprimer à quel point tu es spéciale dans ma vie. Tu es la lumière qui éclaire mon chemin, la raison qui fait battre mon cœur et la personne qui comble chaque instant de ma vie de bonheur.

A MON Père « BOUALEM », À travers les hauts et les bas, tu as été mon roc, mon soutien inconditionnel et mon inspiration constante. Ta présence réchauffe mon âme et me donne la force de surmonter tous les défis qui se dressent sur notre chemin.

A mon mec Oussama, Avec cette dédicace, je veux te montrer tout l'amour, l'admiration et la gratitude que j'ai pour toi. Tu es mon pilier, mon confident et mon meilleur ami. Je suis tellement reconnaissant de t'avoir à mes côtés dans cette aventure appelée "vie". Votre encouragement, votre conseil et votre présence lors des moments difficiles ont été inestimables

A mes chères frères, Nihad, Mohammed Abdallah, a ma petite princesse ranime a mon frère Youcef vous êtes ma famille précieuse. L'amour et la fraternité qui nous unissent sont une source d'inspiration constante.

À ma binôme DIHIA, pour son partenariat et son dévouement.

Bref, à tous ceux qui m'aiment et que j'aime, a tous mes cousines et mes amies.

A mon oncle « LASOUAOUI Abdelmadjid » pour leur soutien.

A ma belle-famille « KORICHI »

A tout ma famille « LAICHAOUI » ma grand-mère a mes oncles et tantes maternels et paternels

LAICHAOUI AMINA

Dédicaces

À ma mère Hassina et mon père Mouhand Cherif, pour leur amour infini, leur soutien et leurs sacrifices incalculables.

À ma sœur Tinhinan, mon bras droite ma fidèle alliée, pour son soutien constant et ses encouragements

À mes deux frères, Juba et Amazigh, vous représentez un grand amour et respect dans ma vie et je vous souhaite une vie future des plus merveilleuses.

À ma sœur, Lydia, pour son amour et sa fis Chahine mon prince et son mec Lyes,

Pour leur présence constante et leur affection sans limites.

À mes cousines, Chaïma et Fatima, et à mes tantes Djida, Khoukha, Mnana, Naima, Rahima, et leurs enfants, merci pour votre amour et votre soutien. Sans oublier mon oncle Hanafi et sa famille, que j'aime profondément.

À ma meilleure amie Wissam, pour son amitié précieuse et son soutien constant.

À mes chers voisins, Hassiba, Maroua, Meriem, Fatiha, et Khadîdja, merci pour votre amitié et votre soutien.

À mes camarades de la promotion de réseaux et télécommunication 2019/2024, (W.T.N.N.L. A.M.M.) merci pour ces années de partage et de complicité.

À ma binôme Amina, pour son partenariat et son dévouement.

Bref, à tous ceux qui m'aiment et que j'aime, sachez que vos encouragements et votre amour ont été des piliers essentiels dans cette aventure

SAIDI DIHIA

Résumé

Dans un contexte de connectivité croissante, la qualité de service (QoS) des réseaux de télécommunication est cruciale, particulièrement pour ATM MOBILIS à Relizane, Algérie. Ce mémoire se concentre sur l'optimisation de la QoS en développant des algorithmes intelligents pour la vérification de santé et le dépannage des réseaux. Utilisant des outils de simulation comme ENSP et de gestion comme master NCE de Huawei, des configurations complexes telles que IS-IS, MP-BGP, VRF, et MPLS sont déployées sur une topologie simulée. Les algorithmes en Python automatisent la surveillance et la correction des anomalies, réduisant les interventions manuelles et améliorant la stabilité du réseau. Les résultats démontrent une amélioration significative de la QoS, avec une détection rapide des problèmes et une gestion proactive du réseau. L'automatisation contribue à la résilience et à l'efficacité opérationnelle, promettant des développements futurs en intégrant l'intelligence artificielle pour une gestion encore plus robuste et continue du réseau.

Mot-clé : QOS, ISIS, MP-BGP, VRF, MPLS, Ensp, ATM, NCE.

Abstract:

In a context of increasing connectivity, the quality of service (QoS) in telecommunications networks is crucial, particularly for ATM MOBILIS in Relizane, Algeria. This thesis focuses on optimizing QoS by developing intelligent algorithms for network health monitoring and troubleshooting. Using simulation tools like ENSP and management tools like Huawei's master NCE, complex configurations such as IS-IS, MP-BGP, VRF, and MPLS are deployed on a simulated topology. Python algorithms automate the monitoring and correction of anomalies, reducing manual interventions and improving network stability. The results demonstrate a significant improvement in QoS, with rapid problem detection and proactive network management. Automation contributes to resilience and operational efficiency, promising future developments by integrating artificial intelligence.

Keywords: QOS, ISIS, MP-BGP, VRF, MPLS, Ensp, ATM, NCE.

Liste des figures

Chapitre I : Généralité sur les réseaux

Chapitre II : les protocoles de routages

Chapitre III: Simulation et Eude de la topologie de Relizane et L'implémentation des scripts

Liste des tableaux

Chapitre I : Généralités sur les réseaux

Chapitre II : les protocoles de routage

Chapitre III : Simulation et étude de la topologie de Relizane et l'implémentation des scripts

Sommaire

chaptre II : les protocoles de routage

Chapitre III : **Simulation et Eude de la topologie de Relizane et L'implémentation des scripts**

Symboles et abréviations

A

AS	Autonomous System
ASG	
ASBR	Autonomous System Boundary Router
ASG	Aggregation Site/Service Gateway
ATM	Algerie telecom mobile
ABR	Area border router

B

BGP	Border Gateway protocol
BTS	Base transceiver station
BSC	Base station controller

C

C	Customer Edge

Symboles et abréviations

E

EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ELER	Egress Label Edge Router
EBGP	Externel Border Gateway Protocol
E-URTAN	Externel Border Gateway Protocol
ENSP	Enterprise Network Simulation Platform

G

GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GRAN	Generic Radio Access Network

I

ID	Numéro d'identification
IGP	Interior gateway protocol

Symboles et abréviations

IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IP Ran	Internet Protocol Radio Acces Network
IBGP	Internal Border Gateway Protocol
IS-IS	Intermediate system to intermediate system
ISP	Internet service provider

L

LDP	Label distribution protocol
LER	Label Edge Router
LSR	Label Switch Router
LTE	Long Term Evolution

M

MS	Mobile Station
ME	Mobile Equipment
MPLS	MultiProtocol Label Switching

Symboles et abréviations

N

NSAP	Network Service Access Point.µ
Nss	Network Sub System

O

OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

Q

Qos	quality of service

R

RAN	Radio Acces Network
RD	Route Distinguisher
RIP	Routing Information Protocol
RNC	Radio Network Controller
RT	Route target

Symboles et abréviations

T

TCP Transmission Control Protocol

TTL Time to Liv

V

VPN Virtual Private Network

VPNv4 Virtual Private Network Version 4

VRF Virtual Routing and Forwarding

W

WAN Wireless Area Network

WDM Wavelength Division Multiplexing

Introduction générale

Introduction générale

Dans un monde de plus en plus connecté, la fiabilité et la qualité de service (QOS) des réseaux de télécommunication sont essentielles pour assurer une expérience d'utilisateur optimale. La QoS se réfère à la capacité d'un réseau à fournir des services de transmission de données avec des niveaux de performance garantis, tels que la bande passante, le délai et la perte de paquets [28]. Cela est particulièrement critique dans les réseaux IP (Internet Protocol) et RAN (Radio Access Network).

Le réseau télécom de Relizane présente diverses complexités structurelles et opérationnelles qui affectent la qualité du service (QoS). Ces problèmes se traduisent par des interruptions fréquentes, une latence élevée et une gestion inefficace de la bande passante. De plus, les méthodes manuelles de vérification de l'état du réseau et du dépannage pour détecter les erreurs ne sont plus valides et prennent beaucoup de temps, compte tenu de la complexité du réseau et du nombre élevé d'équipements. Face à ces défis, il est crucial de développer des solutions robustes pour améliorer les performances du réseau et offrir une expérience utilisateur fluide et satisfaisante. La nécessité d'optimiser les réseaux de télécommunications pour répondre aux exigences de plus en plus strictes des utilisateurs finaux a motivé le choix de ce sujet. La société ATM MOBILIS, l'un des principaux opérateurs de télécommunications en Algérie, rencontre des difficultés majeures pour assurer une QoS optimale dans la région de Relizane. Notre approche innovante repose sur l'implémentation d'algorithmes intelligents de vérification de santé (check health) et de dépannage (troubleshooting) automatisent la vérification et le dépannage du réseau, réduisant les interventions manuelles et assurant une détection rapide des anomalies pour une meilleure gestion de la QoS.

Pour atteindre cet objectif, ce mémoire propose une méthodologie détaillée incluant l'utilisation. Des outils de simulation comme ENSP et iMaster NCE de Huawei, nous déployons des configurations complexes incluant IS-IS, MP-BGP, VRF, et MPLS, et telnet sur une topologie simulée. Cette approche nous permet de modéliser, étudier et simuler puis améliorer la qualité de service du réseau de la wilaya de Relizane.

Enfin, les algorithmes sont appliqués en Python pour valider ses performances et identifier les améliorations nécessaires.

Chapitre I : Généralités sur les réseaux

Chapitre I : Généralités sur les réseaux

I.1 Introduction :

Afin de bien mener notre travail, il est primordial de bien assimiler les notions de base sur les réseaux de communication. A travers ce chapitre nous allons exposer quelques concepts théoriques sur les réseaux pour mieux comprendre leurs fonctionnements.

Nous commençons par définir un réseau et examinons en détail ses composants. Ensuite, nous explorons l'architecture des réseaux en décrivant les modèles OSI et TCP/IP, ainsi que leur interrelation. Nous poursuivons en explorant les technologies de transmission. Enfin, nous aborderons l'évolution des générations de téléphonie mobile et leurs architectures.

I.2 Définition d'un réseau :

Un réseau désigne un ensemble d'équipements interconnectés pour permettre la communication de données entre applications, quelles que soient les distances qui les séparent.

Un réseau s'appuie sur deux notions fondamentales :

- **L'interconnexion** qui assure la transmission des données d'un nœud à un autre.
- **La communication** qui permet l'échange des données entre processus.**[1]**

I.3 Les composants d'un réseau :

I.3.1 Les équipements finaux :

Un équipement final ne fournit pas de service réseau au sens strict du terme. Soit les données sont destinées à ces équipements, soit ils produisent des données qu'ils doivent faire parvenir à d'autres équipements. En fait, ils ne servent pas à atteindre d'autres équipements, ils ne servent pas d'équipements de transit.

Ces équipements sont fixes ou mobiles, en directe interface avec l'utilisateur ou non. Il y a donc les PC fixes ou mobiles, les téléphones, les tablettes sans fils, les imprimantes, les serveurs, les caméras IP, les terminaux de télé présence, etc. **[2]**

I.3.2 Les équipements intermédiaires :

I.3.2.1 Les Répéteurs :

Les Répéteurs régénèrent le signal et qui permettent ainsi d'étendre la distance maximum de transmission**. [3]**

I.3.2.2 Les Ponts :

Ce type d'équipement, logiciel et matériel, assure une segmentation physique et logique du réseau. Seuls les paquets destinés à un équipement situé de l'autre côté du Bridge le traverse. **[3]**

I.3.2.3 Les concentrateurs :

Les Hubs permettent la connexion de plusieurs nœuds sur un même point d'accès sur le réseau, en se partageant la bande-passante totale**. [3]**

I.3.2.4 Les commutateurs :

Travaille sur les deux premières couches du modèle OSI, c'est-à-dire qu'il distribue les données à chaque machine destinataire, alors que le hub envoie toutes les données à toutes machines qui répondent. **[3]**

I.3.2.5 Les Routeurs :

Un équipement d'interconnexion muni de 2 ports au minimum et ayant une adresse physique et logique pour chacun d'eux**. [3]**

I.3.2.6 Les passerelles :

Ce sont des systèmes matériels et logiciels permettant de faire la liaison entre deux ou plusieurs réseaux travaillant avec des protocoles différents. **[3]**

I.3.3 Les supports de transmission :

Un support de transmission ou canal de transmission est la portion du milieu physique utilisée pour la transmission particulière étudiée au sens de la théorie des communications.

On distingue deux types de support :

I.3.3.1 Supports avec un Guide Physique :

I.3.3.1.1 Une fibre optique :

Est constituée d'un fil de verre très fin. Elle comprend un cœur, dans lequel se propage la lumière émise par une diode électroluminescente ou une source laser et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre. [4]

La figure I-1 ses dessous montre la constituant d'un câble a fibre optique :

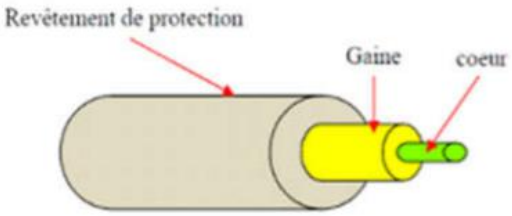


Figure I-1: Constituant d'un câble à fibre optique. *[4]*

I.3.3.2 Supports sans guide physique :

I.3.3.2.1 Les faisceaux hertziens :

La liaison hertzienne est l'une des liaisons les plus utilisées. Cette liaison consiste à relier des équipements radio en se servant des ondes radio

- Les ondes radio servent le plus souvent à relier des ordinateurs distants dans une zone géographique étendue comme une ville.
- Ces ondes radio peuvent atteindre une vitesse de transmission de 11 Mbps. [4]

La figure I- 2 ses dessous montre Les faisceaux hertziens :

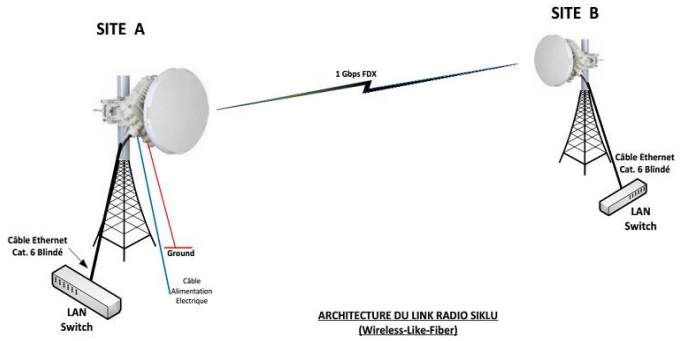


Figure I-2 : les faisceaux hertziens**. [5]**

I.4 Architecture des réseaux :

I.4.1 Modèle OSI :

OSI signifie Open System Interconnections. Ce modèle a été mis en place par l'ISO (International Standard Organisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau. Le modèle OSI est un modèle qui comporte 7 couches [3]:

I.4.1.1 Couche physique :

S'occupe de la connexion physique d'une machine avec le réseau. [3]

I.4.1.2 **Couche liaison** :

S'occupe de l'acheminement de trames de données entre deux équipements voisins. [3]

I.4.1.3 Couche réseau :

Définit l'unité de données de base transférée sur le réseau entre deux sites extrêmes et inclut les concepts d'adressage et de routage. [3]

I.4.1.4 Couche transport :

Assure un contrôle de bout en bout en permettant à un processus destinataire de communiquer directement avec le processus source. [3]

I.4.1.5 Couche session :

Définit la manière dont les protocoles peuvent être organisées pour fournir toutes les fonctionnalités dont les programmes d'applications se servent. [3]

I.4.1.6 Couche présentation :

Est destinée à supporter les fonctions dont beaucoup de programme ont besoin comme la compression de texte ou la conversion d'image graphique. [3]

I.4.1.7 Couche application :

Comprend les programmes qui utilisent le réseau, la messagerie électronique ou le transfert des fichiers. [3]

La figure **I**- 3 montre les couches du modèles OSI :

Figure I-3 : les couches du modèle OSI. *[3]*

I.4.2 Modèle TCP/IP :

TCP/IP représente l'ensemble des règles de communication sur Internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. [3]

TCP/IP est une suite de protocoles. TCP/IP signifie « Transmission Control Protocol/Internet Protocol ». [3]

- **TCP (Transmission Control Protocol)** : Ce protocole a en charge le découpage du message en datagrammes, le réassemblage à l'arrivée avec remise dans le bon ordre, ainsi que la réémission de ce qui a été perdu. [3]
- **IP (Internet Protocol)** : Il assure le routage des datagrammes.

Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle [3]

I.4.2.1 La couche accès réseau :

Est l'interface avec le réseau et est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau. [3]

I.4.2.2 La couche internet ou couche IP :

(Internet Protocol) gère la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi les protocoles ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol). [3]

I.4.2.3 La couche transport :

Assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol) ou non fiable dans le cas de UDP (User Datagram Protocol). [3]

I.4.2.4 La couche application :

Est celle des programmes utilisateurs comme telnet (connexion à un ordinateur distant), FTP (File Transfert Protocol), SMTP (Simple Mail Transfert Protocol), etc. [3]

Le tableau ci-dessous montre le Modèle TCP/IP :

Tableau I-1*:* Modèle TCP/IP [*3]*

APPLICATION : HTTP, FTP
TRANSPORT : TCP, UDP
INTERNET ; IP
Accès réseaux ; WIFI, PPP, ATM

I.4.3 Le modèle TCP/IP et le modèle OSI :

TCP/IP, inspiré du modèle OSI, reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre couches comme est montre dans le Tableau [3]

Tableau I-2 : Comparaison entre OSI et TCP/IP. [3]

Modèle TCP/IP	**Modèle OSI**
Couche Application	Couche Application
	Couche Présentation
	Couche Session
Couche Transport (TCP)	Couche Transport
Couche Internet (IP)	Couche Réseau
Couche Accès réseau	Couche Liaison données
	Couche Physique

Comme on peut le remarquer, les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI. [3]

I.5 Les technologies de transmission.

I.5.1 Système de multiplexage en longueur d'onde WDM :

Le multiplexage en longueur d'onde, souvent appelé WDM (Wavelength Division Multiplexing en anglais), est une technique utilisée en communication optique qui permet d'augmenter le débit sur une fibre optique en faisant circuler plusieurs signaux de longueurs d'onde différentes sur une seule fibre, en les mélangeant à l'entrée à l'aide d'un multiplexeur (Mux) et en les séparant à la sortie au moyen d'un démultiplexeur .[6]

I.5.2 Ethernet :

Ethernet est une technologie universelle qui dominait déjà les réseaux locaux bien avant le développement de l'Internet. La clé de la longévité de cette technologie, c'est sa simplicité. Souvent critiquée, elle a toujours été plus facile à utiliser et à mettre en œuvre que ses concurrentes. Cet article est à la fois une introduction aux normes (IEEE 802.3 - 10 Mbps, Fast Ethernet - 100 Mbps, Gigabit Ethernet - 1 Gbps, 10 Gbps) et une aide à la conception et la réalisation de réseaux locaux.[7]

I.5.3 Présentation des réseaux MPLS :

Est une technologie conçue pour améliorer la vitesse Et l'efficacité du transfert des données au sein de réseaux étendus ou de sites d'Edge computing. Le protocole MPLS permet principalement de lier les différents protocoles du routage de niveau 3 Avec les mécanismes de la commutation de niveau 2 du modèle OSI, on dit que c'est un protocole de couche 2.5. La figure I- 4 montre la localisation de l'en-tête MPLS. [8]

L'idée général de l'MPLS et de rajouter un label aux paquets IP puis le réseau va créer

Figure I-4 : Localisation de l'en-tête MPLS.

un chemin à commutation de label LSP (Label Switching Path) où les routeurs acheminent ces paquets IP. [8]

I.5.3.1 Les Eléments du MPLS :

Le bon fonctionnement de l'MPLS repose sur différents éléments clé qui assurent toutes les principales opérations d'étiquetages et d'acheminement du Traffic de manière fiable et efficace à travers le réseau, Dans cette partie on présente un aperçu détaillé de ces éléments : [8]

- **Ingress Label Edge Router (ILER) :** C'est un routeur périphérique qui impose des paquets d'étiquette (PUSH) et les transferts vers la destination via le domaine.
- **Egress Label Edge Router (ELER)** : est un point de sortie où le paquet de données atteint sa destination. Ce routeur périphérique effectue la suppression des étiquettes.
- **Label Switch Router (LSR) :** Ce routeur reçoit un paquet étiqueté, l'échange avec un sortant et transmet le nouveau paquet à une interface appropriée. En fonction de son emplacement dans le domaine MPLS, ce routeur effectue la disposition, l'imposition ou le remplacement d'étiquette.
- **Label Switch Path (LSP) :** C'est le chemin parcouru par un paquet via un réseau compatible MPLS. Ce chemin est de type simplex ou à sens unique.
- **Label Distribution Protocol (LDP) :** Ce protocole permet de distribuer les labels entre les LSR pour que ces derniers puissent constituer leurs tables de commutation.
- **Forward Equivalence Class (FEC) :** Elle comprend un groupe de paquets d'une application spécifique transmis dans son chemin de commutation sur la même voie.

- **LIB (Label Information Base) :** C'est La première table construite par le routeur MPLS. Elle contient pour chaque sous-réseau la liste des labels affectés par les LSR.
- **LFIB (Label Forwarding Information Base) :** Le routeur construit une table LFIB qui contient que les labels du meilleur prochain saut qui sera utilisée pour commuter les paquets labélisés. [8]

I.6 L'évolution des générations de téléphonie mobile

Depuis plusieurs années, le développement des réseaux mobiles n'a pas cessé d'accroitre, plusieurs générations ont vues le jour (1G, 2G, 3G, 4G et prochainement la 5G) et connues une évolution remarquable, en apportant un débit exceptionnel et qui ne cesse d'augmenter, une bande passante de plus en plus large supportant ainsi de plus en plus d'utilisateurs. [9]

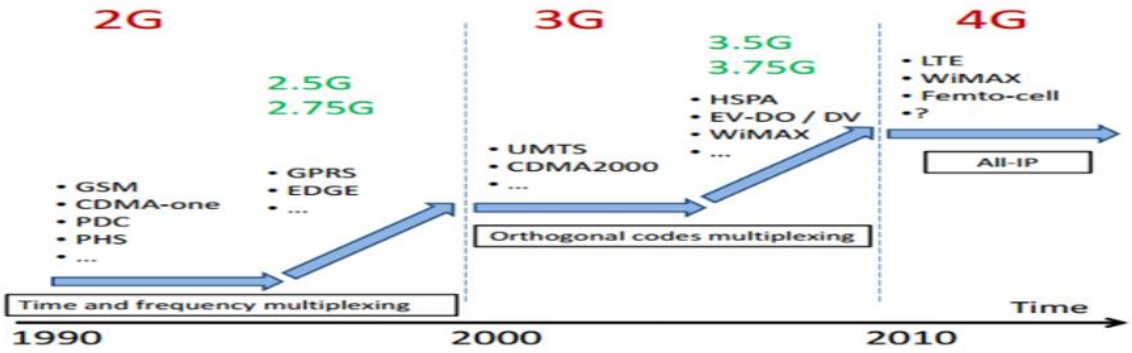


Figure I-5 : l'évolution des réseaux mobile

La Figure ci-dessus montre l'évolution des réseaux mobile.

I.6.1 La Deuxième génération (2G)

La seconde génération de réseaux mobiles a marqué une rupture avec la première génération de téléphones cellulaires grâce au passage de l'analogique vers le numérique. La principale norme 2G utilisé est GSM. Grâce aux réseaux 2G, il est possible de transmettre la voix ainsi que des données numériques de faible volume, notamment des messages textes

(SMS, pour Short Message Service) ou encore des messages multimédias (MMS, pour Multimedia Message Service). [9]

I.6.2 La Troisième génération (3G)

La 3G (troisième génération de téléphonie mobile) s'est implanté au tournant des années 2000. La principale norme 3G utilisée en Europe s'appelle UMTS, Grâce à la vitesse accrue de transmission de données, l'UMTS ouvre la porte à des nouvelles applications et services.

L'UMTS permet en particulier de transférer en temps réel des contenus multimédias tels que les images, le son et les vidéos. [9]

I.6.3 La Quatrième génération (4G LTE)

Généralement commercialisé sous le nom de 4G LTE, développé par 3GPP (3rd Generation Partnership Project), est une norme de communication sans fils de données à haut débit pour les téléphones mobiles et les terminaux de données. Il est basé sur les technologies 2G et 3G, augmentant la capacité et la vitesse en utilisant des différentes interfaces radio, et aussi l'amélioration du réseau de base. [9]

Tableau I-3*:* Les caractéristiques principales des réseaux de téléphonie mobile. [10]

Génération	**1G**	**2G**	**2.5G**	**3G**	**4G**
Standards	NMT, AMPS, TACS	GSM ,1595A	GPRS ,1595 A	UMTS, CDMA2000	LTE
Fréquences	900 MHz	900et 1800MHz	1900-2024MHz 2110-2200MHz	1900-2024MHz 2110-2200MHz	800MHz et 2600MHz
Débits réels	-	9.6kbps	48kbps	384kbps HSPA 14.4 Mbps HSPA+ 42MBPS	150Mbps

Le Tableau ci-dessus montre Les caractéristiques principales des réseaux de téléphonie mobile.

I.7 Architecture d'un réseau mobile :

L'architecture du réseau mobile est composée de trois parties principales :

- MS (Mobile Station), appelé aussi équipement utilisateur, abrégé en UE (User Equipment)
- Le réseau d'accès ou RAN (Radio Access Network) ;

Le réseau cœur ou CN (Core Network) [10]

Comme montre

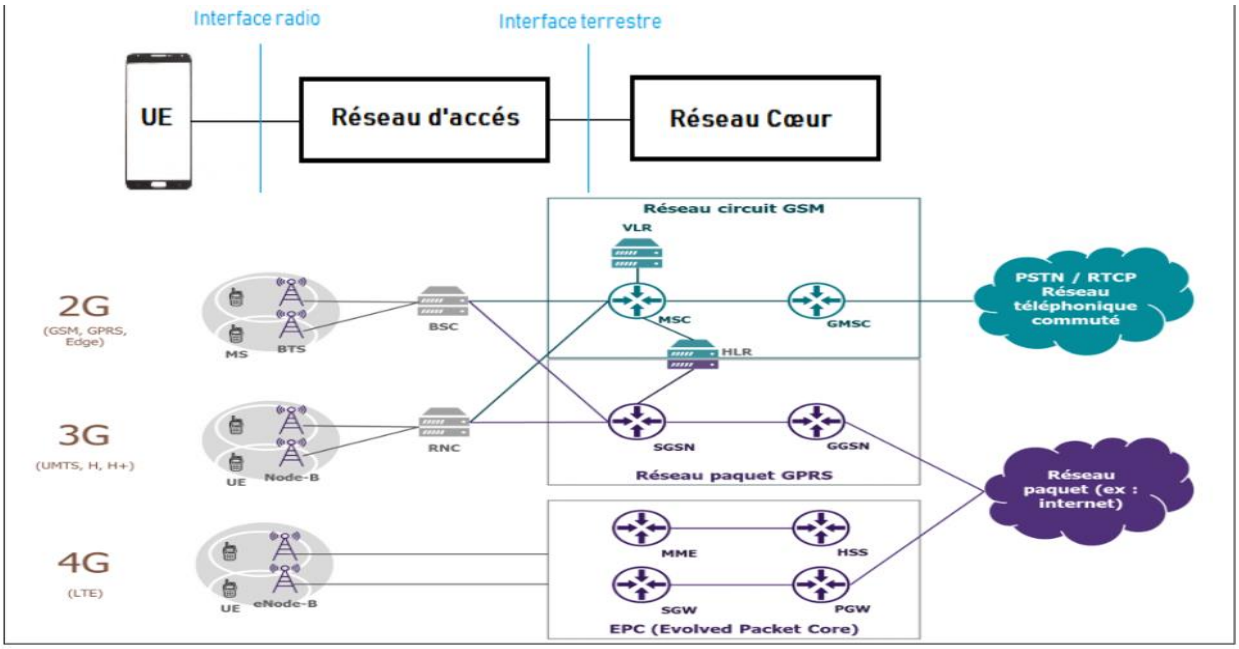


Figure I-6 : l'architecture générale d'un réseau de téléphonie mobile [9]

I.7.1 MS (Mobile Station)

Cette partie est un élément de base d'un système cellulaire de téléphonie mobile, elle est composée de deux éléments :

- **ME** (Mobile Equipment) qui est caractérisé par l'IMEI
- **Carte SIM** (Subscriber Identity Module) qui contient l'identifiant de l'abonné (numéro MSI pour International Mobile Subscriber Identity. [9]

I.7.2 RAN (Radio Access Network) :

Le Radio Access Network (RAN) est la partie radio d'un système de télécommunication mobile. Il met en œuvre une technologie d'accès radio et il assure la connexion entre un terminal tel qu'un téléphone mobile, un ordinateur, ou toute autre machine accessible à distance et le réseau central. Ce réseau se diffère d'une technologie à une autre. [9]

I.7.2.1 GRAN (GSM Radio Access Network)

Il gère la partie radio des communications en GSM et se compose :

- **BTS :** C'est un ensemble d'émetteurs-récepteurs radio, sans grande intelligence. Elle gère la couche physique de l'interface air.
- **BSC :** Il gère les ressources radios (allocation/dés allocation de canal) au niveau des BTS en fonction de l'établissement et de la libération des communications. [9]

I.7.2.2 UTRAN :

Il gère la partie radio des communications en UMTS. Il est composé de :

- **Node B** : C'est un ensemble de stations de base (BS) et de contrôleurs de site qui gèrent la couche physique de l'interface radio.
- **RNC** : C'est un contrôleur de Node B et encore ici l'équivalent du BSC dans le réseau GSM. Le RNC contrôle et gère les ressources radio et le réseau cœur. [9]

I.7.2.3 E-UTRAN

La partie radio du réseau 4G, appelée « E-UTRAN » est simplifiée par rapport à celles des réseaux 2G (BSS) et 3G (UTRAN) par l'intégration dans les stations de base « eNode B ».

- **eNode B :** L'eNode B est la station de base dans le réseau LTE qui est muni à des antennes et peut fonctionner sur une ou plusieurs cellules, et inclut des fonctions de contrôle qui étaient auparavant implémentées dans les RNC (Radio Network Controller). [9]

I.7.3 Le réseau cœur (CN) :

C'est la partie centrale du réseau. Elle prend en charge les fonctions de commutation et de routage. Il est connu par le : [9]

I.7.3.1 Nss (Network Sub System) en 2G:

Il est composé de : [9]

- **MSC (Mobile Switching Center)** : C'est un commutateur qui peut être considéré comme le cœur d'un système cellulaire, car, il est responsable de la gestion des appels et de tout ce qui est lié à l'identité des abonnés, à leurs enregistrements et à leurs localisations.
- **VLR (Visited Location Register) :** Raccordé à un MSC est présent dans une zone géographique donnée, Contient les informations des abonnés présents dans la zone géographique contrôlée par le MSC.
- **EIR (Equipement Identity Register) : C'est** la base de données des abonnés. Elle est consultée pour s'assurer de la légitimité d'un mobile. C'est en particulier dans l'EIR que sont identifiés les mobiles volés et interdits d'accès au réseau.
- **AUC (Authentification Center) :** entité L'AUC est l'unité qui authentifie les mobiles qui détient toutes leurs clés d'authentification. Il est associé au HLR. Le MSC s'adresse à lui lors d'une demande d'inscription pour valider l'accès du mobile au réseau.
- **HLR (Home Location Register) :** c'est la base de données principale qui contient l'information des tous les abonnés présents dans le réseau.

I.7.3.2 CN (Core Network) en 3G :

Il utilise les deux domaines de commutations CS (Circuit Switching) et PS (Packet Switching). De plus des éléments cités en 2G il comprend : [9]

- **SGSN (Serving GPRS Support Node) :** est chargé d'enregistrer les usagers dans une zone géographique dans une zone de routage RA (Routing Area)
- **GGSN (Gateway GPRS Support Node) :** est une passerelle vers les réseaux à commutation de paquets extérieurs tels que l'Internet.

I.7.3.3 EPC (Evolved Packet Core) en 4G:

Il opère avec un seul domaine : commutation par paquet. Il comprend : [9]

- **HSS (Home Suscriber Service) : Base** de données centrale équivalent au HLR

- **MME (Mobility Management Entity) : C'est** l'équivalent au VLR,
- **PGW (Packet Data Network Gateway) :** passerelles d'accès vers les réseaux tiers. Il achemine les données venant des réseaux extérieurs vers les terminaux mobiles concernés à travers le S-GW et les données des terminaux mobiles vers le réseau extérieur.
- **SGW (Serving Gateway) :** est le point de relais entre le réseau d'accès et le réseau cœur, elle permet la collection des paquets de données envoyées par les UE à travers les différents MS et après l'acheminera vers leurs destinations.

I.8 Conclusion :

Après avoir exploré les bases des réseaux de télécommunication, y compris ce qui les compose et comment ils envoient des données, on se concentre maintenant sur la connectivité de ses réseaux et ce qui les rend solides. Le routage IP et Les protocoles de routage sont super importants car ils dirigent les données là où elles doivent aller, ce qui permet aux réseaux de fonctionner de manière fiable. C'est justement le sujet de chapitre suivant.

.

Chapitre II :
Les protocoles de routage

Chapitre II : les protocoles de routage

II.1 Introduction :

Dans le domaine des réseaux informatiques, la communication entre systèmes interconnectés repose sur un ensemble de règles bien définies appelé protocole. Ces règles garantissent la transmission efficace et fiable des données d'un émetteur vers un récepteur. Le chapitre suivant se penche sur le concept fondamental du routage IP, un aspect essentiel de la communication sur Internet et d'autres réseaux similaires. Avant d'explorer les méthodes et les protocoles de routage, il est crucial de comprendre ce qu'est un protocole et les objectifs qu'il cherche à atteindre.

II.2 Définition d'un protocole :

Un protocole est un ensemble de règles de communication respectées par tous les systèmes interconnectés afin de permettre la liaison entre systèmes émetteurs et systèmes récepteurs. [9]

Les objectifs d'un protocole sont :

L'information doit arriver le plus rapidement possible et correcte aux destinations.

- L'expéditeur doit être informé, éventuellement, de la bonne réception par un acquittement.
- Il ne doit pas y avoir de conflit en cas de requêtes simultanées.
- La transparence du réseau pour l'utilisateur. **[1]**

II.3 Routage IP :

II.3.1 Définition de Routage IP

Le routage réseau est le processus de sélection d'un chemin à travers un ou plusieurs réseaux. Les principes de routage peuvent s'appliquer à tous les types de réseaux, des réseaux téléphoniques aux transports publics. Dans les réseaux à commutation de paquets, comme Internet, le routage sélectionne les chemins que doivent emprunter les paquets IP (Internet Protocol) pour se rendre de leur origine à leur destination. Ces décisions de routage Internet sont

prises par des périphériques réseau spécialisés appelés routeurs. Les routeurs s'appuient sur des tables de routage**.[11]**

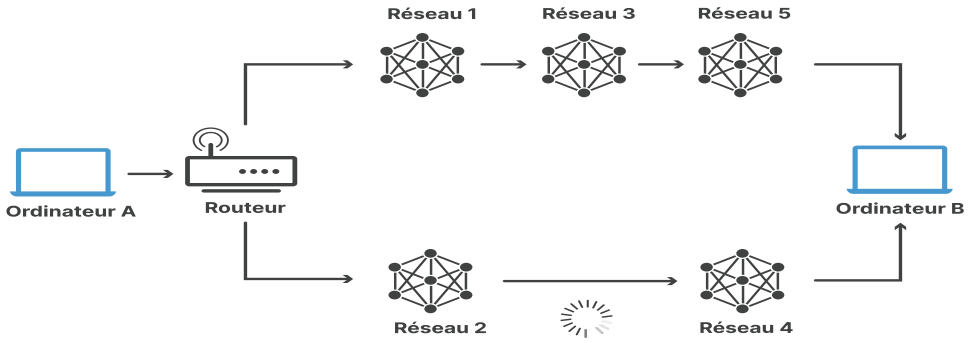


Figure II-1 : Exemple de routage IP[11]

Examinons l'image ci-dessous. Pour qu'un paquet de données puisse se rendre de l'ordinateur A à l'ordinateur B, doit-il passer par les réseaux 1, 3 et 5 ou les réseaux 2 et 4 ? Le paquet empruntera un chemin plus court via les réseaux 2 et 4, mais les réseaux 1, 3 et 5 pourraient s'avérer plus rapides pour acheminer les paquets. C'est là le genre de choix que les routeurs réseau effectuent en permanence. **[11]**

II.3.2 Méthodes de routage IP

II.3.2.1 Routage Direct :

Le routage direct se produit quand la machine de destination se trouve sur le même réseau physique que la machine émettrice. Dans ce cas, un datagramme IP peut être émis directement, sans passer par un routeur, après avoir été en capsulé dans une trame correspondant au type du réseau local. C'est ce qu'on appelle la remise directe. **[12]**

II.3.2.2 Routage Indirect

Si la machine de destination du datagramme ne se trouve pas sur le même réseau que la machine émettrice, il faut passer par un routeur. L'adresse de la première passerelle par laquelle il faut passer pour atteindre la destination est appelée la route indirecte. En effet, la machine émettrice ne s'occupe pas de connaitre le chemin complet jusqu'à la destination, elle doit juste connaitre l'adresse de cette première passerelle. **[13]**

Plusieurs cas de routage indirect peuvent se présentés :

II.3.2.2.1 Routage par table :

Les machines communiquant avec TCP/IP possèdent une table de routage IP. Il s'agit d'un ensemble de correspondances entre une adresse de réseau IP et l'adresse de la première passerelle à emprunter. Quand une machine émet un datagramme, elle vérifie d'abords si l'adresse du réseau de destination est reprise dans cette table. Si c'est le cas, elle peut y lire l'adresse de l'adresse de la passerelle vers laquelle il faut envoyer le datagramme. [12]

Dans La Figure II- 2 ET Tableau II. 2 on définit un exemple de table de routage et analyse le :

Figure II-2 : Example de Table de routage.

Tableau II-1 : Analyse Exemple table de routage [14]

Champs	Signification
D	Indique comment la route a été découverte
10.1.1.0/24	Indique le réseau de destination.
90	Indique la distance administrative (fiabilité) de la source ou de la route.
2170112	Indique la distance à parcourir pour atteindre le réseaux distant
209.165.200.226	Indique l'adresse du traçons suivant parcourir pour atteindre le réseaux distant
00 :00 :05	Indique le temps écouté depuis la découverte de la route
S0/0/0	Indique l'interface de sortie du routeur permettant d'atteindre le réseau de destination

II.3.3 Types de routage :

On classe généralement les protocoles de routage, d'abord en fonction de leur manière de découvrir le réseau, et après dans leur façon d'établir leurs tables de routage. [15]

II.3.3.1 Le routage statique :

Le routage statique est utilisé lorsqu'un administrateur attribue manuellement le chemin de la source au réseau de destination. Il offre plus de sécurité au réseau. [15]

II.3.3.1.1 Avantages :

- Pas de bande passante inutilisée entre les liens.
- Seul l'administrateur peut ajouter des itinéraires. [15]

II.3.3.1.2 Inconvénients :

- L'administrateur doit savoir comment chaque routeur est connecté.
- Chaque fois que la liaison tombe en panne, tout le réseau tombe en panne**. [15]**

II.3.3.2 Le routage dynamique :

Ici, les routes sont calculées et saisies grâce un protocole de routage. Il est utilisé dans les plus gros réseaux. Il est plus difficile à mettre en place, mais plus facile à maintenir. Lorsqu'une route est en panne, il recalcule automatiquement un autre chemin. [15]

II.3.3.2.1 Différenciation :

- ❖ Plus facile à configurer même sur des réseaux plus grands.
- ❖ Il vous aide à équilibrer la charge entre plusieurs liens. [15]

II.3.3.2.2 Désavantage :

- ❖ Les mises à jour sont partagées entre les routeurs, elles consomment donc de la bande passante.
- ❖ Les protocoles de routage imposent une charge supplémentaire au processeur ou à la RAM du routeur. [15]

Tableau II-2 : comparaison entre le routage statique et dynamique **.** [16]

Base de comparaison	Routage statique	Routage dynamique
Configuration	Manuelle	Automatique
Complexité de la configuration	Augmente avec la taille de réseaux	Généralement indépendante de la taille de réseaux
Création d'une table de routage	Les emplacements de routage sont saisis a la main	Les emplacements sont remplis dynamiquement dans le tableau
Routes	Les routes sont définies par l'utilisateur.	Les routes sont mises à jour en fonction de changement de topologie.
Mise en œuvre.	Dans les petits réseaux.	Dans les petits et grands réseaux.
Echec de la liaison.	L'échec de la liaison empêche le réacheminement.	L'échec de la liaison n'affecte pas le réacheminement.
Sécurité	Fournit une haute sécurité.	Moins sécurisé e raison de l'envoi d'émission et de multidiffusions
Protocoles de routage.	Aucun protocole	Les protocoles de routage tels que RIP, EIGRP, OSPF
Utilisation des ressources	Utilisation des microcontrôleurs et bande passante moindre	Utilisation des microcontrôleurs et bande passante grande.

II.3.4 Définition de protocole de routage

Un protocole de routage est un protocole qui permet d'acheminer un paquet envoyé par une source à une destination en respectant certains critères. **[1]**

II.3.5 Les métriques des protocoles de routage :

La métrique est utilisée pour déterminer quel chemin est préférable en présence de plusieurs chemins vers le même réseau distant.

Suivant le protocole de routage utilisé, plusieurs métriques peuvent intervenir lors d'une Décision de routage tel que :

- Longueur du trajet : Définit un critère de décision à partir du nombre de liens qu'un Paquet doit traverser pour se rendre du point d'origine au point de destination.
- Fiabilité : Définit un critère de décision fondé sur la fiabilité de chaque lien du réseau.
- Délai de transmission : Définit un critère de décision fondé sur le temps requis afin D'acheminer un paquet du point d'origine au point de destination.
- Largeur de bande : Définit un critère de décision fondé sur la capacité de Transmission d'un lien.
- Charge : Définit un critère de décision fondé sur les ressources d'un routeur comme le Nombre de paquets traités par seconde, ressource mémoire, etc.
- Coût de la communication : Définit un critère de décision fondé sur un coût appliqué à un lien.**[3]**

II.3.6 Classification des protocoles de routage dynamique :

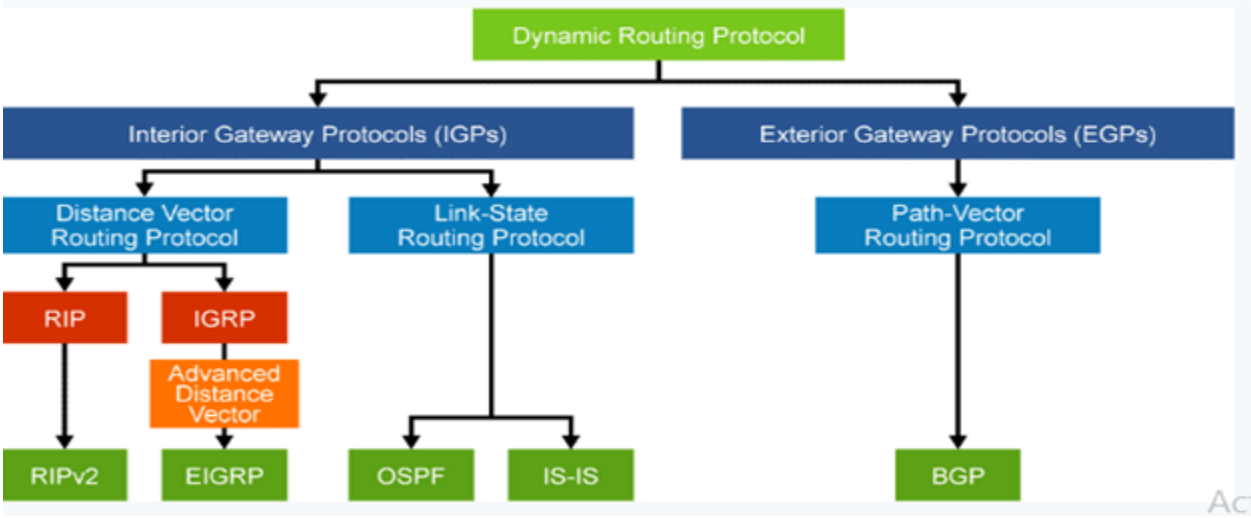


Figure II-3 : Classification des protocoles de routage dynamique [17]

La figure ci-dessus montre Classification des protocoles de routage dynamique.

Il existe deux familles de protocoles de routage :

Les protocoles intra-domaines (system autonome) "IGP" et les protocoles inter-domaines "EGP".

- **Un système autonome** est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage. Les systèmes autonomes (SA) reçoivent des numéros uniques de 1 à 65535, gérés par l'IANA appelé "Autonomes System Nimber ". [19]

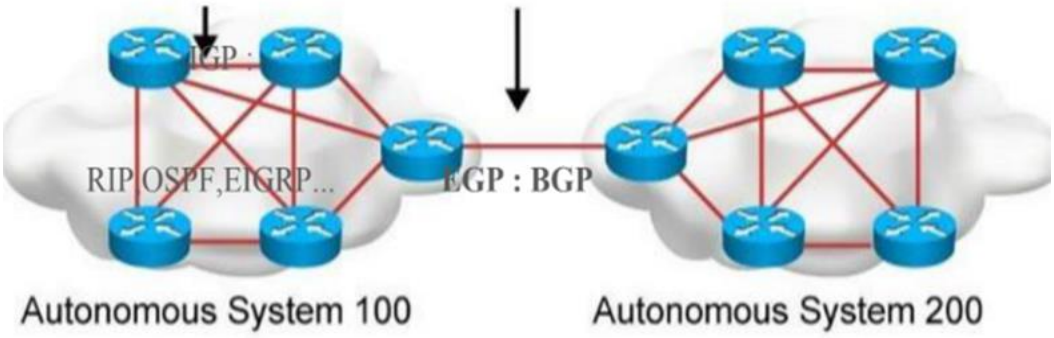


Figure II-4 : Example de deux systèmes autonomes. [18]

II.3.6.1 Protocoles de Routage externes (EGP extérieur Gateway Protocole) :

Le plus utilisé est le **BGP (border Gateway protocole),** c'est un protocole a vecteur de distance, il utilise le TCP comme protocole de transfert ; un échange d'informations s'effectue dès qu'une connexion TCP est établie entre les routeurs voisins (routeurs homologues). Ces informations sont les numéros d'AS de la liste qui doit être suivie pour atteindre une destination.

On distingue plusieurs types de protocole BGP :

- ✓ **I-BGP** : quand le BGP s'exécute entre des routeurs de même AS.
- ✓ **E-BGP** : quand le BGP s'exécute entre des routeurs qui appartiennent à deux AS différents

- ✓ **MP-BGP_** (Multi Protocol BGP) : Une extension de BGP qui permet de transporter des informations de routage pour plusieurs protocoles de couche réseau, tels que IPv6, VPNv4, etc. **[3]**

C'est le protocole utilisé pour aborder les échanges des routes entre les routeurs PE d'un réseau MPLS.Les sous-réseaux annoncés par les routeurs CE aux routeurs PE sont augmentés d'un préfixe de 64 bits, appelé route distinguasse, pour les rendre uniques. Les adresses de 96 bits qui en résultent sont ensuite échangées entre les routeurs PE à l'aide d'une famille d'adresses spéciales de MP-BGP. Le choix de BGP comme Protocole de routage pour le transport de route des VPN est pour les raisons suivantes :

- Le BGP est le protocole de routage qui peut supporter un très grand nombre de routes.
- Sa conception intègre la dimension multi protocole. Il peut transporter des informations de routage pour plusieurs familles d'adresses différentes.
- Il permet les échanges d'informations entre des routeurs non directement connectés. [4]

II.3.6.2 Protocoles de Routage intra-domaine avec IGP (intérieur Gateway protocole) :

Utilisé pour le routage au sein d'un SA. Il est également appelé « routage intra-SA » (RIP, EIGRP et OSPF, IS-IS). [6]

Les protocoles du routage interne peuvent être classés dans deux différentes familles :

II.3.6.2.1 Les protocoles à vecteur de distance :

Les protocoles de routage à vecteur de distances sont des protocoles permettant de construire des tables de routages où aucun routeur ne possède la vision globale du réseau, la diffusion des routes se faisant de proche en proche. Le terme « vecteur de distances » vient du fait que le protocole manipule des vecteurs (des tableaux) de distances vers les autres nœuds du réseau. La distance en question est le nombre de sauts permettant d'atteindre les routeurs voisins. Ces protocoles s'appuient sur l'algorithme de Ford-Bellman**.[12]**

Les protocoles IGP à vecteur de distance incluent les protocoles RIP, EIGRP :

II.3.6.2.1.1 RIP (Routing Information Protocol.) :

Ce premier protocole de routage associé aux réseaux TCP/IP favorisa l'interopérabilité des routeurs. RIP détermine le chemin le plus court à suivre par un paquet pour atteindre sa destination finale à travers des routeurs en comptant le nombre de sauts nécessaires.

Versions de RIP :

Il existe actuellement deux versions à ce jour, RIPv1 ainsi que RIPv2

- ✓ **RIPv1** : Ne prend pas en charge les masques de sous-réseau de longueur variable et l'authentification des routeurs. Les routes sont envoyées en **broadcast**.
- ✓ **RIPv2** : Conçu pour répondre aux contraintes des réseaux actuels (sous-réseaux, authentification, etc.). Les routes sont envoyées à l'adresse **multicast 224.0.0.9. [12]**

II.3.6.2.1.2 IGRP (Interior Gateway Protocol) :

Ce protocole de routage est développé par Cisco pour ses routeurs multi-protocoles. Le désavantage d'IGRP est qu'il est propriétaire et que certaines de ses fonctionnalités sont protégées par des brevets. **[12]**

II.3.6.2.1.2.1 Protocole de routage de passerelle intérieure amélioré (EIGRP) :

EIGRP est un protocole de routage hybride qui fournit des protocoles de routage, des protocoles de routage à vecteur de distance et à état de lien. Le protocole de routage complet EIGRP est amélioré IGRP. Il acheminera les mêmes protocoles que ceux IGRP en utilisant les mêmes métriques composites que IGRP, ce qui aide le réseau à sélectionner la meilleure destination de chemin. **[12]**

II.3.6.2.2 Protocoles à l'états des liens :

Dans cette famille de protocoles chaque routeur communique avec tous les autres routeurs en échangent des informations permettant à chacun de construire une vue complète de la topologie du réseau ainsi qu'une table de routage, prenant en compte les meilleures routes. Tout paquet est transmis sur la meilleure route

. Les métriques utilisées sont :

- La qualité du lien.
- Son encombrement.
- Le type de flux à transmettre.
- Les restrictions de qualité de service appliquées.
- Le coût financier.

Cette méthode de routage permet une construction plus rapide des tables de routage que le routage a vecteur de distance.**[12]**

Les protocoles IGP à l'état de lien incluent les protocoles OSPF et IS-IS :

Nous avons l'intention d'opter pour l'utilisation de protocoles de routage à état de liens (OSPF, IS-IS) pour leur évolutivité supérieure, leur convergence rapide, leur utilisation efficiente de la bande passante et leur capacité à prendre en charge des technologies avancées telles que la QoS et le MPLS. En choisissant ces protocoles, nous visons à garantir la fiabilité, la performance et la flexibilité de notre réseau.

II.3.6.2.2.1 Le protocole OSPF :

II.3.6.2.2.1.1 Définition d'un OSPF :

OSPF, abréviation de (Open Shortest Path First) est un protocole de routage dynamique couramment utilisé dans les réseaux IP à grande échelle. Il fonctionne en déterminant le chemin le plus court pour acheminer les paquets de données entre les routeurs. OSPF calcule ce chemin en fonction de diverses mesures telles que la bande passante de la liaison, le délai et le coût.[22]

II.3.6.2.2.1.2 Versions d'OSPF :

Il existe 3 versions OSPF :

- ❖ OSPF V1 : création du protocole OSPF.
- ❖ OSPF V2 : ajoute de l'authentification.
- ❖ OSPF V3 : pour l'IP version 6.[23]

II.3.6.2.2.1.3 Le fonctionnement d'OSPF :

OSPF (Open Shortest Path First) fonctionne sur la base d'un processus bien défini qui implique la diffusion d'informations de routage au sein d'un réseau et le calcul de chemins de routage optimaux. Le fonctionnement d'OSPF peut être segmenté en phases distinctes, comme détaillé ci-dessous **: [24]**

- **LSA (Link-State Advertisements) :** les routeurs partagent des informations sur leurs connexions directes dans des messages appelés LSA. Cela inclut des informations sur les voisins connectés et le coût pour les atteindre.
- **Inondation de LSA :** chaque routeur OSPF envoie ses LSA à d'autres routeurs de la même zone. Les routeurs mettent ensuite à jour leur base de données Link-State (LSDB) avec les informations reçues, garantissant ainsi que tous les routeurs ont une vue cohérente de la topologie du réseau.
- **Carte topologique :** à l'aide du LSDB, chaque routeur construit une carte de la topologie du réseau, qui montre comment tous les routeurs et réseaux sont interconnectés.
- **Arbre du chemin le plus court :** chaque routeur applique l'algorithme de Dijkstra à sa carte topologique pour calculer le chemin le plus court vers chaque autre nœud du réseau, formant ainsi un arbre du chemin le plus court.
- **Table de routage :** les résultats du calcul de l'arborescence des chemins les plus courts sont utilisés pour remplir la table de routage. Ce tableau aide le routeur à transmettre les paquets de données à venir le long des meilleurs chemins vers leurs destinations.
- **Zones OSPF** : pour gérer les grands réseaux, OSPF divise le réseau en zones qui réduisent la complexité du routage. La zone de base (zone 0) se connecte à d'autres zones et aide à acheminer le trafic entre elles.

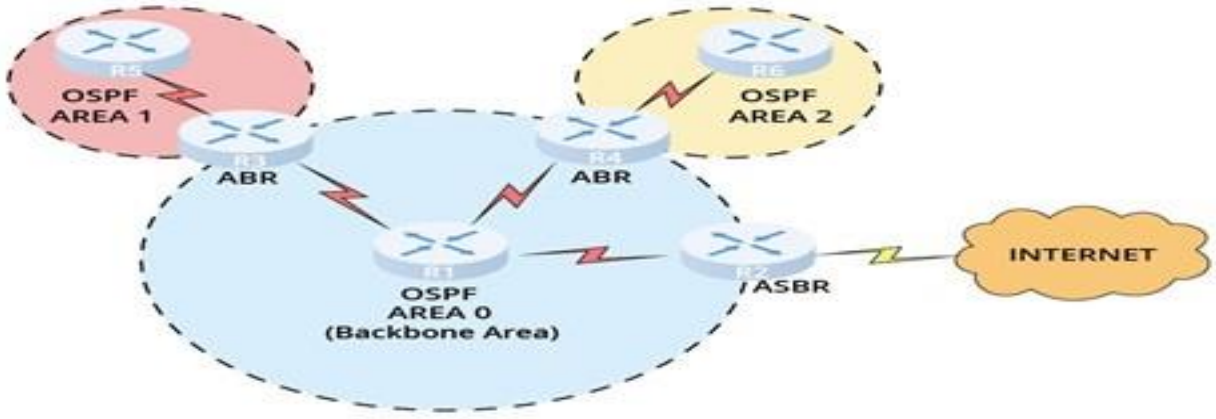


Figure II-5 : les zone de OSPF

- **Types de routeurs :** OSPF utilise différents types de routeurs, tels que des routeurs internes (à l'intérieur d'une zone), des routeurs de frontière de zone (ABR) (connectant deux zones ou plus) et des routeurs de frontière de système autonome (ASBR) (se connectant à différents domaines ou réseaux de routage).
- **Convergence :** OSPF réagit aux changements du réseau en propageant rapidement de nouvelles informations d'itinéraire et en recalculant les chemins, garantissant ainsi que tous les routeurs connaissent l'état actuel du réseau.
- **Protocole Hello :** les routeurs OSPF envoient périodiquement des paquets Hello à leurs voisins pour établir et maintenir des relations de voisinage. Ce processus aide également à détecter les pannes de réseau.[24]

II.3.6.2.2.1.4 Pourquoi en avons-nous besoin :

- Le protocole de routage OSPF est polyvalent et prend en charge les architectures réseau IPv4 et IPv6.
- Il distribue efficacement le trafic réseau pour éviter les surcharges en utilisant des techniques d'équilibrage de charge.
- Le protocole utilise un algorithme qui garantit que le réseau reste exempt de boucles de routage.
  - En raison de sa nature de standard ouvert, OSPF est compatible avec un large éventail de routeurs, sans se limiter à un seul fabricant.
  - Il fonctionne sans restriction de classe, offrant une flexibilité dans la définition des réseaux.

- OSPF dispose d'un nombre illimité de sauts de routeur à sa portée.
- Le protocole excelle dans l'établissement et la mise à jour rapides des informations de routage sur le réseau. [24]

II.3.6.2.3 Intermediate System-to-Intermediate System (IS-IS):

II.3.6.2.3.1 Définition de IS-IS :

IS-IS est un protocole de routage dynamique initialement conçu par l'Organisation internationale de normalisation (ISO) pour son protocole réseau sans connexion (CLNP). Pour prendre en charge le routage IP, le groupe de travail en ingénierie de l'Internet (IETF) étend et modifie IS-IS dans des normes pertinentes, ce qui permet à IS-IS d'être appliqué à la fois aux environnements TCP/IP et Interconnexion de Systèmes Ouverts (OSI). Le nouveau type d'IS-IS s'appelle IS-IS Intégré ou Dual IS-IS. IS-IS utilise l'algorithme SPF pour calculer les routes. Il est caractérisé par une convergence rapide et une grande extensibilité. Fonctionnant au niveau de la couche liaison de données, IS-IS dispose de capacités de protection contre les attaques et peut mettre en œuvre l'interopérabilité sur des réseaux à grande échelle. [25]

II.3.6.2.3.2 Les zone IS-IS et rôles des routeurs :

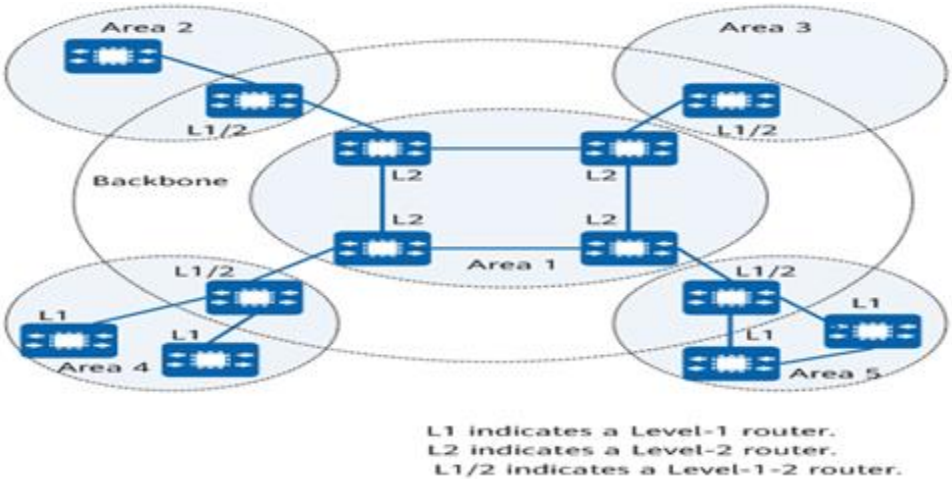


Figure II-6: Example de zone IS-IS [25]

Le réseau IS-IS comprend trois types de routeurs : Niveau 1, Niveau 2 et Niveau 1-2.

- **Routeur de Niveau 1** :

Gère le routage intra-domaine, établissant des relations avec d'autres routeurs de Niveau 1 et Niveau 1-2 dans la même zone. Il maintient une base de données d'état de liaison (LSDB) de Niveau 1 et transfère les paquets vers les routeurs de Niveau 1-2 pour les autres zones. [25]

- **Routeur de Niveau 2** :

Gère le routage inter-domaines, établissant des relations avec d'autres routeurs de Niveau 2 et avec des routeurs de Niveau 1-2 dans d'autres zones. Il maintient une LSDB de Niveau 2 pour les informations de routage inter-domaines. [25]

- **Routeur de Niveau 1-2** :

Appartenant à la fois à une zone de Niveau 1 et à une zone de Niveau 2, il peut établir des relations de voisinage de Niveau 1 et Niveau 2. Il maintient deux LSDB, une pour chaque niveau, pour le routage intra-domaine et inter-domaines respectivement. Les dispositifs de Niveau 1 peuvent accéder à d'autres zones uniquement via des dispositifs de Niveau 1-2.[25]

II.3.6.2.3.3 Adressage IS-IS :

IS-IS utilise des adresses réseau ISO, appelées points d'accès aux services réseau (NSAP), pour identifier les points de connexion au réseau, tels que les interfaces de routeur,

NSAP (network service Access point): contient 20 octet se compose des parties suivantes :

```
49.0001.00a0.c96b.c490.00
49.0001.2081.9716.9018.00
```

Figure II-1 : Adressage IS-IS[]26

- ID de domaine (1 octet) :49
- ID de zone (1-12 octet) :0001
- Système ID (6octet): 2081.9716.9018 , unique dans le réseau, peut-être une adresse MAC ou une adresse IP
- Nsel (network selector) :00 [26]

II.3.6.2.3.4 Les paquets IS-IS :

Sont utilisés pour échanger des informations de protocole et partagent un en-tête commun. Ils incluent plusieurs types de PDUs (paquets) :

- **Bonjour IS-IS (IIH) (hello packet)** : Ces PDUs sont diffusés pour découvrir les systèmes IS-IS voisins et établir les adjacences. Ils ont trois formats différents pour les liaisons point à point, de diffusion de niveau 1 et de diffusion de niveau 2.
- **État de Liaison (LSP)** : Ces PDUs contiennent des informations sur l'état des adjacences des systèmes IS-IS voisins. Ils sont inondés périodiquement dans toute la zone et prennent en charge l'adressage de masque de sous-réseau de longueur variable.
- **Numéro de Séquence Complet (CSP) :** Ces PDUs contiennent une liste complète de tous les LSPs dans la base de données IS-IS. Ils sont envoyés régulièrement sur toutes les liaisons pour maintenir la synchronisation des bases de données.
- **Nombre de Séquences Partielles (PSNP)** : Ces PDUs sont envoyés par un récepteur lorsqu'il détecte des LSPs manquants dans sa base de données locale. Ils demandent les LSPs manquants au système voisin qui a envoyé le CSP.[**25]**

II.3.6.2.3.5 Les topologie IS-IS :

Dans IS-IS il existe deux types de réseaux point à point et diffusion :

II.3.6.2.3.5.1 La topologie point à point :

La topologie point à point dans le protocole IS-IS (Intermediate System-to-Intermediate System) est un type de configuration réseau où chaque connexion est établie directement entre deux nœuds, sans aucun nœud intermédiaire.

Pour les réseaux point à point, les paquets Hello (IIH) point à point sont échangés pour établir la contiguïté. Cela signifie que chaque routeur envoie des paquets IIH pour découvrir et maintenir la communication avec les routeurs voisins directement connectés. Contrairement aux réseaux de diffusion. [25]

II.3.6.2.3.5.2 La topologie de diffusion :

La topologie de diffusion : utilise un concept appelé DIS (Designated Intermediate System) pour optimiser la communication entre les nœuds dans un réseau peer-to-peer. Le DIS est responsable de la réduction de la quantité d'informations d'état de lien (LSDB) échangées entre les nœuds, ce qui améliore l'efficacité et réduit la charge sur le réseau.

Dans un réseau IS-IS, chaque changement d'état d'un routeur est normalement transmis à tous les autres routeurs, ce qui peut gaspiller de la bande passante. Pour résoudre ce problème, le DIS est défini de sorte que tous les routeurs envoient leurs informations au DIS, qui diffuse ensuite les états de lien du réseau. L'utilisation du DIS et des pseudo nœuds simplifie la topologie du réseau et réduit la longueur des LSP (Link State PDU) générés par les routeurs. [25]

II.3.6.2.3.6 La différence entre IS-IS et OSPF :

ISIS et OSPF appartiennent à la même famille de protocoles de routage à état de liaison. Cependant, en les étudiant, vous découvrirez plusieurs différences comment montre le tableau ses dessous : [27]

Tableau II-3 : La différence entre les protocoles OSPF Et IS-IS [27]

Protocole OSPF	Protocole IS-IS
• OSPF fonctionne au-dessus de la couche 3 de modèle OSI • OSPF est un protocole de routage IP • OSPF est plus flexible pour calculer le coût des liens basé sur la vitesse ou la bande passante. • OSPF utilise de nombreux LSAs pour décrire diverses informations de routage, nécessitant plus de mémoire pour la LSDB. • OSPF reste populaire dans les réseaux d'entreprise. • OSPF prend en charge les liens NBMA (Non-Broadcast Multiple Access) et point-à-multipoint, alors qu'ISIS ne les prend pas en charge. • OSPF élit un DR (Designated Router) et un BDR (Backup Designated Router),	• IS-IS fonctionne sur la couche 2 de modèle OSI • IS-IS est à la base un protocole de routage réseau OSI et n'utilise pas IP pour la transmission des messages • IS-IS peut gérer plus de routeurs dans une aire qu'OSPF. • ISIS utilise seulement deux LSPs, ce qui réduit la LSDB et économise de la mémoire • IS-IS est privilégié dans les grands réseaux de fournisseurs de services, • ISIS est plus sécurisée car il fonctionne sur la couche liaison de données, ce qui empêche les attaques de l'IGP (Interior Gateway Protocol) utilisant l'IP, contrairement à OSPF • ISIS élit seulement un DR appelé DIS (Designated Intermediate System).

II.3.6.3 La différence entre les protocoles de routage a état des liens et vecteurs distance :

Le tableau ses dessous montre La différence entre les protocoles de routage a état des liens et vecteurs distance : [3]

Tableau II-4 : La différence entre les protocoles de routage a état des liens et vecteurs distance

Vecteur de distance	**État du lien**
Le protocole vecteur de distance envoie l'intégralité de la table de routage.	Le protocole Link State envoie uniquement des informations sur l'état des liens.
Il est sensible aux boucles de routage.	Il est moins sensible aux boucles de routage.
Les mises à jour sont parfois envoyées par diffusion.	Utilise uniquement la méthode de multidiffusion pour le routage des mises à jour.
C'est simple à configurer.	Il est difficile de configurer ce protocole de routage.
Ne connaît pas la topologie du réseau.	Connaître toute la topologie.
Example RIP, IGRP.	Exemples : OSPF IS-IS.

II.4 Conclusion :

Ce chapitre a permis de présenter une analyse approfondie protocoles de routage, en mettant particulièrement l'accent sur IS-IS et OSPF. Ces protocoles jouent un rôle crucial dans la détermination des chemins optimaux pour les paquets de données dans un réseau. OSPF, largement utilisé dans les réseaux d'entreprises, est reconnu pour sa capacité à s'adapter à des topologies complexes grâce à l'utilisation des zones. En revanche, IS-IS, bien que moins connu, est favorisé dans les environnements de fournisseurs de services et les grands réseaux ce protocole correspond aux attentes de l'opérateur MOBILIS

Nous avons choisi d'opter pour l'utilisation de protocole IS-IS en raison de son évolutivité supérieure, de son utilisation efficiente de la bande passante, et de sa capacité à prendre en charge des technologies avancées telles que la QoS et le MPLS. En choisissant ce protocole, nous visons à garantir la fiabilité, la performance et la flexibilité de notre réseau.

Dans le prochain chapitre, nous aborderons l'aspect pratique en procédant à la configuration de protocole IS-IS et le protocole MP-BGP et MPLS et VPN et VRF, tout en continuant à traiter les différentes problématiques pour optimiser notre infrastructure réseau.

Chapitre III :

Simulation et Eude de la topologie de Relizane et L'implémentation des scripts

Chapitre III : Simulation et étude de la topologie de Relizane et l'implémentation des scripts

III.1 Introduction :

Dans cette étude, nous avons pris la décision d'intégrer des scripts Python dans une topologie IP/RAN simulée pour la wilaya de Relizane, à l'aide de la plateforme ENSP de Huawei. Notre travail se divise en trois parties principales.

La première partie est consacrée à la simulation du réseau IP/RAN en utilisant la plateforme ENSP pour configurer les équipements nécessaires, y compris les équipements et leurs interfaces et les protocoles de routage interne comme IS-IS et MP-BGP. Nous avons également implémenté MPLS pour accélérer le transfert des données et VRF pour optimiser le trafic.

Dans la deuxième partie, nous avons étudié la topologie réelle du réseau de l'ATM Mobilis de la wilaya de Relizane. Grâce à la plateforme de gestion des réseaux iMaster NCE, nous avons examiné la constitution de la topologie, l'adressage, les configurations des routeurs, ainsi que les alarmes et les anomalies. Nous avons également appris à créer de nouveaux sous-réseaux sur NCE.

Enfin, dans la troisième partie, nous avons connecté notre PC à la topologie simulée dans ENSP pour exécuter des scripts de vérification de santé (Check Heath) et de dépannage (trouble shooting) à l'aide de Visual Studio Code. Cela nous a permis d'accéder aux routeurs, d'analyser les configurations de réseau, de détecter et corriger les pannes, et d'optimiser les performances réseau.

III.2 Objectifs de l'étude :

1. Simulation d'un réseau RAN pour une wilaya à l'ENSP :

- Apprendre à configurer un réseau d'accès radio (RAN) en utilisant la plateforme de simulation ENSP.

2. Étude de la topologie réelle du réseau de la wilaya de Relizane :

- Analyser et comprendre la structure actuelle du réseau télécom de la wilaya de Relizane, y compris ses composants et interconnexions.

3. Implémentation d'algorithme de dépannage et troubleshooting dans la topologie de Relizane pour :

- Améliorer la qualité de service (QoS) :
- Développer et intégrer des algorithmes visant à optimiser les performances du réseau et à améliorer la qualité de service pour les utilisateurs de la wilaya de Relizane.

III.3 L'hypothèses :

Le réseau télécom de la wilaya de Relizane présente des complexités structurelles et opérationnelles qui entraînent des problèmes spécifiques de qualité de service (QoS). Ces problèmes incluent des interruptions fréquentes, une latence élevée, et une gestion inefficace de la bande passante. Par conséquent, l'implémentation d'un algorithme de dépannage et troubleshooting est nécessaire pour optimiser les performances du réseau et résoudre les problèmes de QoS, améliorant ainsi l'expérience utilisateur globale.

III.4 Les logiciels utilisés pour notre étude :

III.4.1 Les logiciels utilisé pour la simulation :

Pour la simulation de notre réseau dans la première partie, nous utiliserons le logiciel suivant :

III.4.1.1 eNSP (enterprise Network Simulation Platform):

C'est un logiciel propriétaire de HUAWEI Technologies pour la simulation de réseaux informatiques, semblable à Pocket Tracer, Junosphere ou encore l'alternative libre GNS3

(Graphical Network Simulator), il est considéré comme une plate-forme d'outils de simulation de réseau graphique accessible et extensible.

III.4.1.2 iMaster NCE :

Le logiciel iMaster NCE est une plateforme de gestion de réseau développée par Huawei. Il offre des fonctionnalités avancées pour la surveillance, la configuration et la gestion des réseaux. iMaster NCE permet aux opérateurs de réseau de visualiser et de gérer efficacement leur infrastructure réseau.

III.4.2 Langage de programmation utilisé :

III.4.2.1 Python :

Python est un langage de programmation polyvalent et convivial, largement utilisé dans le développement logiciel et l'analyse de données. Sa syntaxe claire et lisible en fait un choix populaire, même pour les débutants. Python offre de nombreuses fonctionnalités et bibliothèques pour faciliter le développement d'applications dans divers domaines, tels que l'intelligence

Partie 1 : simulation de réseau RAN

III.5 Réalisation du réseau :

III.5.1 Processus de déploiement d'un réseau IP/MPLS MOBILIS :

Pour mettre en œuvre un réseau, l'opérateur de réseau MOBILIS suivent plusieurs étapes clés. Voici une description détaillée et objective de ces étapes :

III.5.1.1 Vérification des besoins en équipements et disponibilité du câblage :

L'opérateur débute par évaluer les besoins en équipements réseau, tels que routeurs, commutateurs et pare-feu, en prenant en compte les spécifications techniques telle que les types des équipements et les performances nécessaires pour répondre aux exigences du réseau. Ils vérifient également la disponibilité et l'état des infrastructures de câblage, y compris la fibre optique, en examinant les chemins de câblage existants et en planifiant de nouvelles installations si besoin.

III.5.1.2 Choix des routeurs :

- **ASBR (Autonomes System Boundary Router)** : Routeur qui connecte un réseau autonome à un autre, échangeant les informations de routage entre les deux systèmes autonomes.
- **ASG (Autonomes System Gateway)** : Routeur servant de point d'entrée/sortie principal pour un réseau autonome, gérant le trafic entrant et sortant.
- **P (Provider Router)** : Routeur au sein du réseau du fournisseur qui gère le routage interne du fournisseur, sans interaction directe avec les routeurs des clients.
- **PE (Provider Edge Router)** : Routeur situé à la frontière du réseau du fournisseur, connectant le réseau du fournisseur aux réseaux des clients et gérant les VPN MPLS.
- **CE (Customer Edge Router)** : Routeur situé à la frontière du réseau du client, connectant le réseau du client au réseau du fournisseur.

III.5.1.3 Installation physique :

III.5.1.3.1 Installation des équipements :

Les équipements sont ensuite installés dans les racks ou les armoires en effectuant les étiquetages. Les connexions physiques, telles que les câbles d'alimentation et les câbles réseau, la sécurité physique sont réalisées.

III.5.1.3.2 Interconnexion des équipements :

Les différents équipements sont interconnectés à l'aide de câbles réseau appropriés. Cette étape inclut la gestion des câbles pour assurer une organisation propre et minimiser les interférences.

III.5.1.4 Configuration et vérification de l'installation :

Les connexions réseau sont configurées sur les équipements, en définissant les interfaces et les protocoles nécessaires pour permettre la communication entre les différents dispositifs.

III.5.1.5 Le Commissioning (côté matériel et logiciel) :

III.5.1.5.1 Tests matériels :

Les équipements installés sont testés pour vérifier leur bon fonctionnement. Cela inclut des vérifications de l'alimentation, des connexions réseau et de la performance des composants matériels.

III.5.1.5.2 Tests logiciels :

L'opérateurs effectue des tests de connectivité en utilisant des commandes telles que "ping" pour vérifier la communication entre les équipements, vérifiant ainsi les paramètres réseau, les protocoles et les services. Ils réalisent également des tests de performance pour évaluer les débits, les latences et la stabilité du réseau.

III.5.1.5.3 Loading de software par un test à vide :

Chargement du logiciel réseau sur les équipements sans générer de trafic réel pour vérifier l'installation correcte et la configuration initiale.

III.5.1.5.4 Loading de software par un test de trafic :

Test du logiciel sous conditions de trafic simulé ou réel pour évaluer les performances, la stabilité et la fiabilité du réseau en situation opérationnelle.

III.5.1.6 Troubleshooting le dépannage (en cas de problèmes) :

III.5.1.6.1 Identification des problèmes :

Si des problèmes sont détectés lors des tests, les opérateurs identifient les causes possibles. Cela peut inclure des analyses de journaux système, des tests de diagnostic et des vérifications de configuration.

III.5.1.6.2 Résolution des problèmes :

Les problèmes identifiés sont résolus en ajustant les configurations, en remplaçant les composants défectueux ou en effectuant d'autres actions correctives nécessaires. Une fois les corrections apportées, de nouveaux tests sont réalisés pour s'assurer que les problèmes ont été résolus.

III.6 Planification du travail :

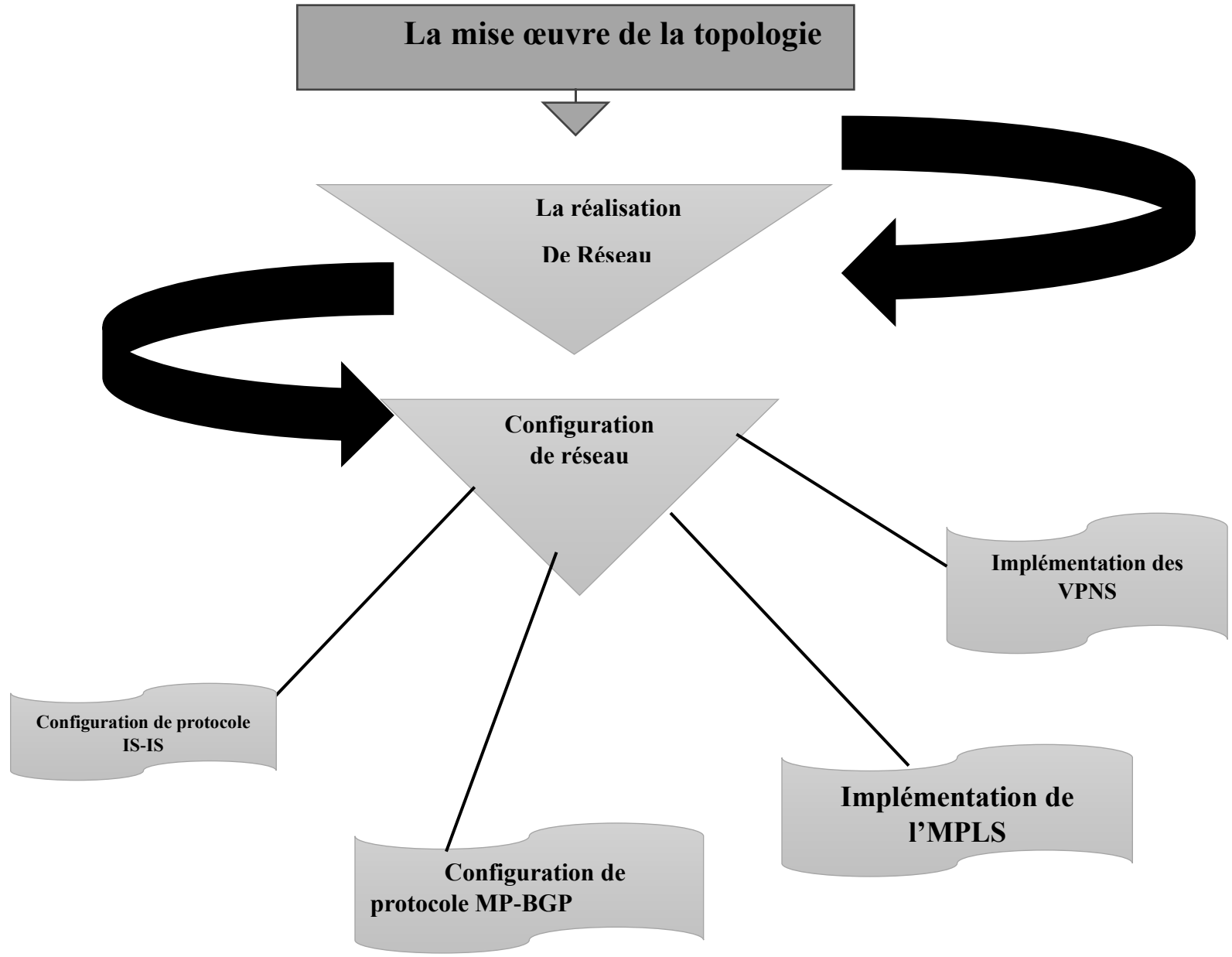


Figure III-1 plan de travail

Le schéma ci-dessus illustre les étapes à suivre dans notre travail pour identifier une topologie optimale et réalisable :

- **Mise en œuvre de la topologie** : Déployer physiquement et logiquement le réseau selon la conception.
- **Configuration de la maquette** : Paramétrer l'environnement de test pour simuler la topologie.
- **Configuration de IS-IS** : Configurer le protocole IS-IS pour la diffusion des informations de routage dans le réseau.
- **Configuration de protocole MP-BGP** : Configurer le protocole MP-BGP pour le routage inter-domaines.
- **Implémentation des VRF** : Déployer les VRF pour la segmentation et l'isolement du réseau.

III.7 La mise en œuvre de la topologie réseau :

Cette section est dédiée à l'infrastructure de la zone de la wilaya de Relizane qui sera mise en place. Ensuite, nous aborderons les aspects liés aux équipements ainsi que les protocoles (IS-IS, MP-BGP, VRF et MPLS) nécessaires pour assurer la connectivité. Nous commencerons par configurer les protocoles intra-domaine IS-IS et BGP, puis nous implémenterons le protocoles MPLS.

III.7.1 Présentation du réseau ;

Afin de mettre en œuvre notre étude, notre réseau comprendra : Provider (P), Provider Edge (PE) et Customer Edge (CE), chacun ayant un rôle essentiel dans la structure et le fonctionnement du réseau, comme décrit ci-dessous :

- Routeurs représentant le cœur MPLS (routeurs P) simulant les routeurs :

  -ASBR1

  -ASBR2

  -ASG2

  -ASG5

- Routeurs représentant l'Edge MPLS (routeurs PE) et simulant les routeurs :
- **- ASG1**
- **-ASG4**
- Routeurs désignant les sites d'un client VPN (routeurs CE) et simulant :
- **-ASG7**
- **-ASG8**
- **-R12**
- **-ASG9**
- **- R13**
- **-R14**
- **-R15**
- **- R17**
- **-R20**

La figure suivante illustre une simulation sur ENSP de réseau RAN définie avant :

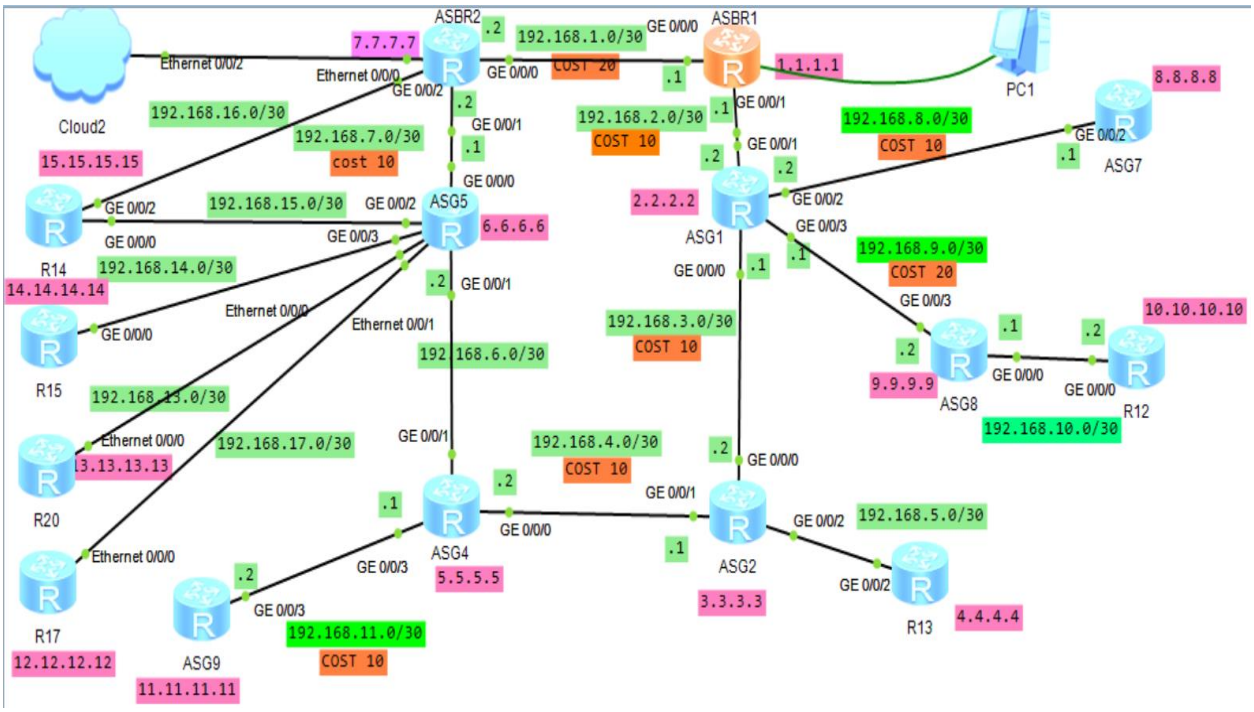


Figure III-2 : Simulation d'architecture approximative de wilaya de Relizane.

III.7.2 Configuration de réseau :

Le tableau ci-dessous montre La répartition des adresses IP attribuées aux interfaces de chaque routeur et les masque est fixée dans le tableau qui suit :

Tableau III-1 : Table d'adressage des routeurs.

Les Routeurs	Interfaces	Adresse IP	Masque
ASBR1	GE 0/0/0	192.168.1.1	255.255.255.252
	GE 0/0/1	192.168.2.1	255.255.255.252
	Loopback0	1.1.1.1	255.255.255.255
ASBR2	GE 0/0/0	192.168.1.2	255.255.255.252
	GE 0/0/1	192.168.7.2	255.255.255.252
	GE 0/0/2	192.168.16.1	255.255.255.252
	Ethernet 0/0/0	192.168.1.2	255.255.255.252
	Loopback0:	7.7.7.7	255.255.255.255
ASG1	GE 0/0/0	192.168.3.1	255.255.255.252
	GE 0/0/1	192.168.2.2	255.255.255.252
	GE 0/0/2	192.168.8.2	255.255.255.252
	GE 0/0/3	192.168.9.1	255.255.255.252
	Loopback0	2.2.2.2.	255.255.255.255
	Loopback1	22.22.22.22	255.255.255.255
ASG2	GE 0/0/0	192.18.3.2	255.255.255.252
	GE 0/0/1	192.16.4.1	255.255.255.252
	GE 0/0/2	192.168.5.1	255.255.255.252
	Loopback0	3.3.3.3	255.255.255.255
R13	GE 0/0/2	192.168.5.2	255.255.255.252
	Loopback0	4.4.4.4	255.255.255.255
ASG5	GE 0/0/0	192.168.7.1	255.255.255.252
	GE 0/0/1	192.168.6.2	255.255.255.252
	GE 0/0/2	192.168.15.1	255.255.255.252
	GE 0/0/3	192.168.14.1	255.255.255.252
	Ethernet0/0/0	192.168.13.1	255.255.255.252

	Ethernet0/0/1	192.168.17.1	255.255.255.252
	Loopback0	6.6.6.6	255.255.255.255
ASG4	GE 0/0/0	192.168.4.2	255.255.255.252
	GE 0/0/1	192.168.6.1	255.255.255.252
	GE 0/0/3	192.168.11.1	255.255.255.252
	Loopback1	5.5.5.6	255.255.255.255
	Loopback0	5.5.5.5	255.255.255.255
ASG7	GE 0/0/2	192.168.8.1	255.255.255.252
	Loopback0	8.8.8.8	255.255.255.255
ASG8	GE 0/0/3	192.168.9.2	255.255.255.252
	GE0/0/0	192.168.10.1	255.255.255.252
	Loopback0	9.9.9.9	255.255.255.255
R12	GE 0/0/0	192.168.10.2	255.255.255.252
	Loopback0	10.10.10.10	255.255.255.255
ASG9	GE 0/0/3	192.168.11.2	255.255.255.252
	Loopback0	11.11.11.11	255.255.255.255
R17	Ethernet0/0/0	192.168.17.2	255.255.255.252
	Loopback 0	12.12.12.12	255.255.255.255
R20	Ethernet0/0/0	192.168.13.2	255.255.255.252
	Loopback0	13.13.13.13	255.255.255.255
R15	GE 0/0/0	192.168.14.2	255.255.255.252
	Loopback0	14.14.14.14	255.255.255.255
R14	GE 0/0/0	192.168.15.2	255.255.255.252
	GE 0/0/2		255.255.255.252
	Loopback0	192.168.16.2	255.255.255.255
		15.15.15.15	

III.7.2.1 Définitions des interfaces :

- **Ethernet** : Une technologie de réseau local (LAN) utilisée pour connecter des dispositifs dans une petite zone géographique, généralement jusqu'à 100 Mbps.
- **Fast Ethernet** : Une version améliorée d'Ethernet offrant des vitesses de transfert de données allant jusqu'à 100 Mbps.
- **Gigabit Ethernet** : Une version encore plus rapide d'Ethernet qui permet des vitesses de transfert de données allant jusqu'à 1 Gbps (1000 Mbps).
- **Port RS-232** : Une interface de communication série utilisée principalement pour la transmission de données sur de courtes distances, généralement jusqu'à 115.2 kbps.

III.7.3 Configuration des différents routeurs :

Cette partie consiste à faire une configuration initiale sur les routeurs en suivant les étapes citées ci-dessous :

-Attribution des noms aux routeurs

- Configuration des interfaces.

- Configuration de routage IGP (le protocole IS-IS).

- Configuration du protocole MPLS.

- Configuration du BGP et les VRF.

III.7.3.1 Attribution des noms aux routeurs :

Cette figure montre la configuration le nom de routeur, tous les routeurs de la topologie sont configurés avec les mêmes étapes :

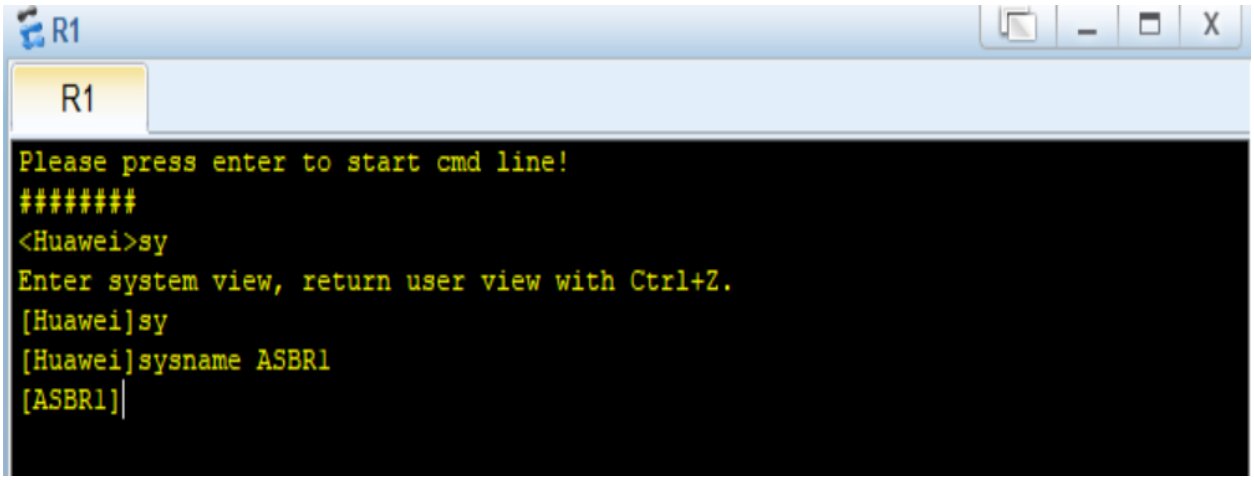


Figure III-3 : Attribution des noms aux routeurs.

III.7.3.2 Configuration des loopbacks :

La loopback est une interface virtuelle dans chaque routeur, pour l'activer on utilise la commande interface loopback Elle permet de remplacer la connexion internet dans un simulateur. La loopback va être configuré avec les mêmes étapes de configuration. La figure ses dessus montre la configuration loopback .

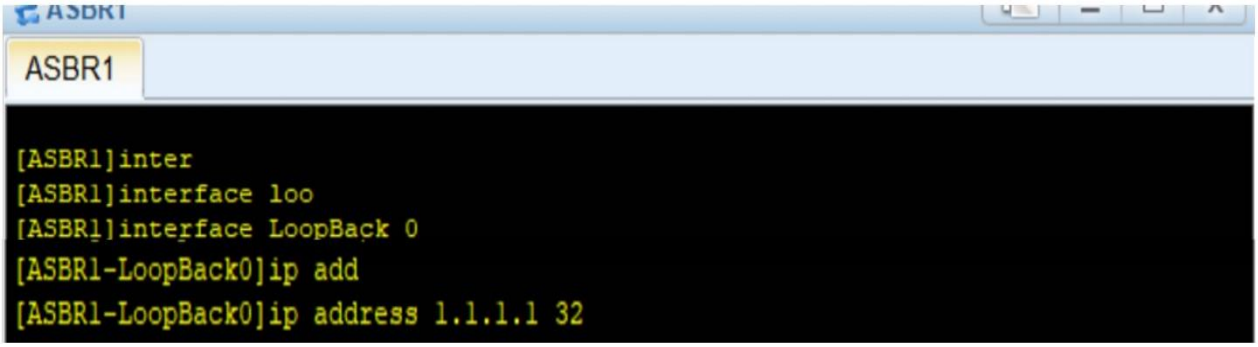


Figure III-4: Configuration d'adresse loopback exemple ASBR1.

III.7.3.3 Configuration de l'adressage pour les interfaces :

On sélectionne chaque interface par la commande **« interface (nom d'interface) »**On attribue à chaque interface une adresse IP et le masque, en utilisant la commande **« IP adresse »** suivie de l'adresse IP et le masque. (Toutes les interfaces des autres routeurs sont configurées de la même manière). Comme montre figure suivante :

ASBR1

```
<ASBR1>
<ASBR1>sy
Enter system view, return user view with Ctrl+Z.
[ASBR1]inter
[ASBR1]interface g
[ASBR1]interface GigabitEthernet0/0/0
[ASBR1-GigabitEthernet0/0/0]ip add
[ASBR1-GigabitEthernet0/0/0]ip address 192.168.1.1 30
[ASBR1-GigabitEthernet0/0/0]Q
[ASBR1]interface GigabitEthernet0/0/1
[ASBR1-GigabitEthernet0/0/1]IP address 192.168.2.1 30
[ASBR1-GigabitEthernet0/0/1]
```

Figure III-5 : Configuration des interfaces de routeur ASBR1.

Vérification des interfaces configuré et activé avec la commande :

« **Display IP interface brief** »

La figure ses dessous montre la Vérification activation Interfaces de ASBR.

```
<ASBR1>display ip interface brief
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 8
The number of interface that is UP in Protocol is 4
The number of interface that is DOWN in Protocol is 8

Interface                         IP Address/Mask      Physical   Protocol
Ethernet0/0/0                     unassigned           down       down
Ethernet0/0/1                     unassigned           down       down
GigabitEthernet0/0/0              192.168.1.1/30       up         up
GigabitEthernet0/0/1              192.168.2.1/30       up         up
GigabitEthernet0/0/2              unassigned           down       down
GigabitEthernet0/0/3              unassigned           down       down
LoopBack0                         1.1.1.1/32           up         up(s)
NULL0                             unassigned           up         up(s)
Serial0/0/0                       unassigned           down       down
Serial0/0/1                       unassigned           down       down
Serial0/0/2                       unassigned           down       down
Serial0/0/3                       unassigned           down       down
<ASBR1>
```

Figure III-6 : Vérification activation Interfaces de ASBR.

III.7.3.4 Configuration du protocol IS-IS (Intermediate System to Intermediate System):

Pour l'activation du routage classique au niveau du backbone, c'est-à-dire entre les PE-Routeurs et les P-Routeurs, Nous avons portés notre choix sur le protocole IS-IS à cause de ses multiples avantages :

- C'est un protocole de routage à états de liens.
- ISIS est bien adaptée aux grandes infrastructures, notamment dans les réseaux de fournisseurs de services.

La configuration IS-IS doit être effectuée sur tous les routeurs du réseau MPLS comme suit :

On active pour chaque routeur le protocole IS-IS, qui permet de créer une table de routage dans chaque routeur, avec les commandes suivantes :

- **La commande « [Huawei] ISIS 1 » :** Cette commande entre dans le mode de configuration ISIS pour le processus 1. Le chiffre 1 est l'identifiant du processus ISIS, similaire à un numéro d'instance unique.
- **[Huawei-isis-1] network-entity 49.0001.0010.0100.1001.00** : Cette commande définit leNetwork Entity Title (NET) pour le processus ISIS. Le NET est une adresse unique pour l'identification du routeur dans le réseau ISIS. Elle est composée de l'identifiant de domaine (49), suivi de l'identifiant du système.
- **[Huawei-isis-1] is-level level-1** : Cette commande configure le routeur pour fonctionner en tant que routeur de niveau 1 dans le réseau ISIS. Les routeurs de niveau 1 communiquent uniquement avec d'autres routeurs de niveau 1 dans la même zone.
- **[Huawei-GigabitEthernet0/0/0] isis enable** 1 Cette commande active le protocole ISIS sur l'interface spécifiée et associe cette interface au processus ISIS 1.
- **[Huawei-GigabitEthernet0/0/0] isis circuit-type p2p** Cette commande configure le type de circuit de l'interface en tant que point à point (point-to-point). Cela est souvent utilisé dans les connexions directes entre deux routeurs pour simplifier la topologie de routage et améliorer la convergence.

les figures III-7 et III- 8 *:* monteront un exemple de la configuration de IS-IS dans le routeur ASBR2 (tous les autres routeurs de topologie sont configurer de même configuration de IS-IS) :

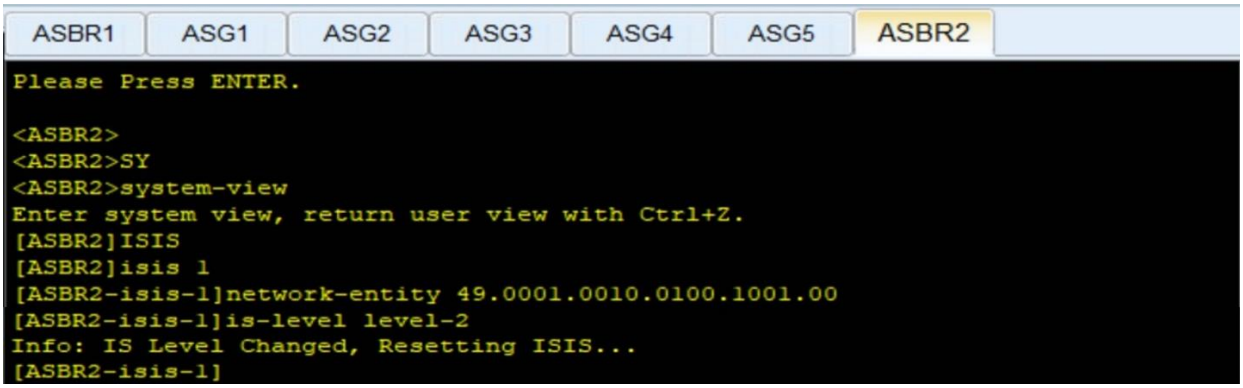


Figure III-7: Exemple de configuration de protocole IS-IS sur ASBR2.

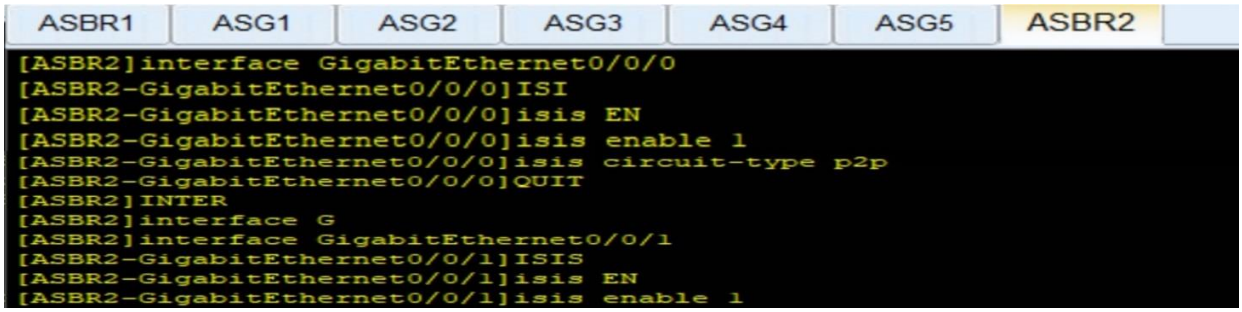


Figure III-8 : Activation de IS-IS dans les interfaces.

Après la configuration et pour tester le bon fonctionnement du protocole IS-IS on exécute la commande :**« DISPLAY IP ROUTING TABLE »** qui nous montre la table de routage comme c'est illustre dans les figures ci-dessous :

ASBR2

ASBR2

```
<ASBR2>DIS IP routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 26        Routes : 26

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  ISIS-L2 15   20          D   192.168.1.1     GigabitEthernet
0/0/0
        2.2.2.2/32  ISIS-L2 15   60          D   192.168.7.1     GigabitEthernet
0/0/1
        3.3.3.3/32  ISIS-L2 15   50          D   192.168.7.1     GigabitEthernet
0/0/1
        4.4.4.4/32  ISIS-L2 15   40          D   192.168.7.1     GigabitEthernet
0/0/1
        5.5.5.5/32  ISIS-L2 15   30          D   192.168.7.1     GigabitEthernet
0/0/1
        6.6.6.6/32  ISIS-L2 15   10          D   192.168.7.1     GigabitEthernet
0/0/1
        7.7.7.7/32  Direct  0    0           D   127.0.0.1       LoopBack0
        8.8.8.8/32  ISIS-L2 15   70          D   192.168.7.1     GigabitEthernet
0/0/1
        9.9.9.9/32  ISIS-L2 15   80          D   192.168.7.1     GigabitEthernet
0/0/1
    10.10.10.10/32  ISIS-L2 15   50          D   192.168.7.1     GigabitEthernet
0/0/1
    11.11.11.11/32  ISIS-L2 15   40          D   192.168.7.1     GigabitEthernet
0/0/1
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/30  Direct  0    0           D   192.168.1.2     GigabitEthernet
0/0/0
    192.168.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
    192.168.2.0/30  ISIS-L2 15   70          D   192.168.7.1     GigabitEthernet
0/0/1
    192.168.3.0/30  ISIS-L2 15   60          D   192.168.7.1     GigabitEthernet
```

Figure III-9 : ROUTES IS-IS.

Afin de vérifier la configuration du protocole ISIS pour ASBR1 on utilise la commande :

« Display current-configuration configuration ISIS »

La figure Montre une capture de cette vérification. De la même manière on vérifie La configuration pour les autres routeurs.

```
return
<ASBR1>display current-configuration configuration ISIS
#
isis 1
 is-level level-2
 network-entity 49.0001.0010.0100.1001.00
#
return
<ASBR1>
```

Figure III-10 : Configuration actuelle du protocole ISIS sur le routeur ASBR1.

Afin de vérifier que le protocole de routage ISIS fonctionne dans le réseau ID 1 on fait un test de ping à partir de ASBR1 vers ASBR2 et de l'ASBR1 vers ASG1. Les résultats de ses pings sont montrés dans les figures :

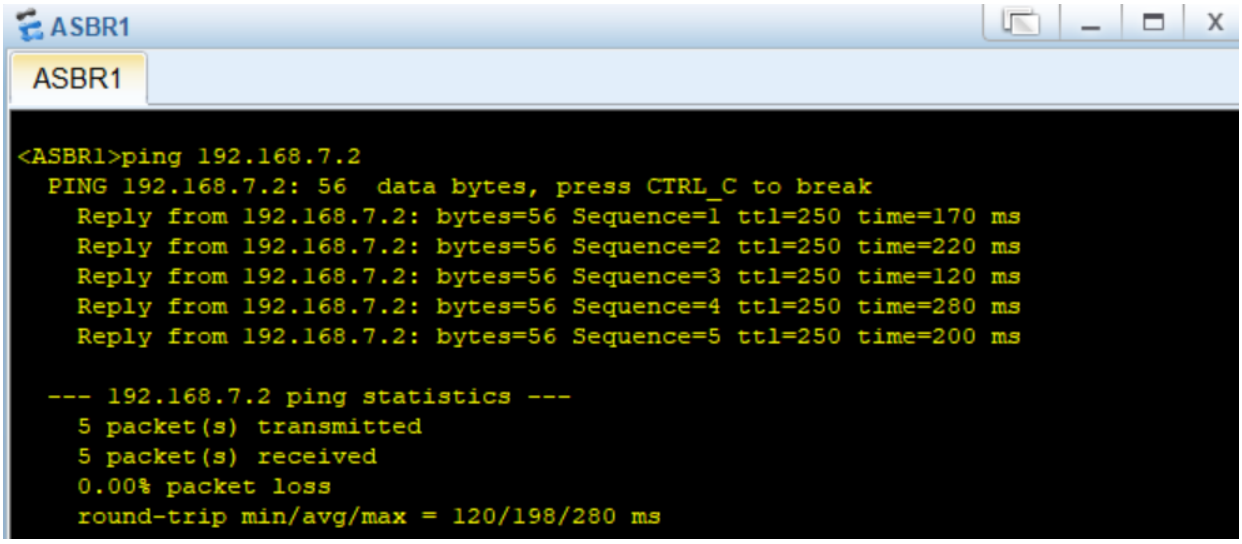


Figure III-11 : Ping de ASBR1 vers ASBR2.

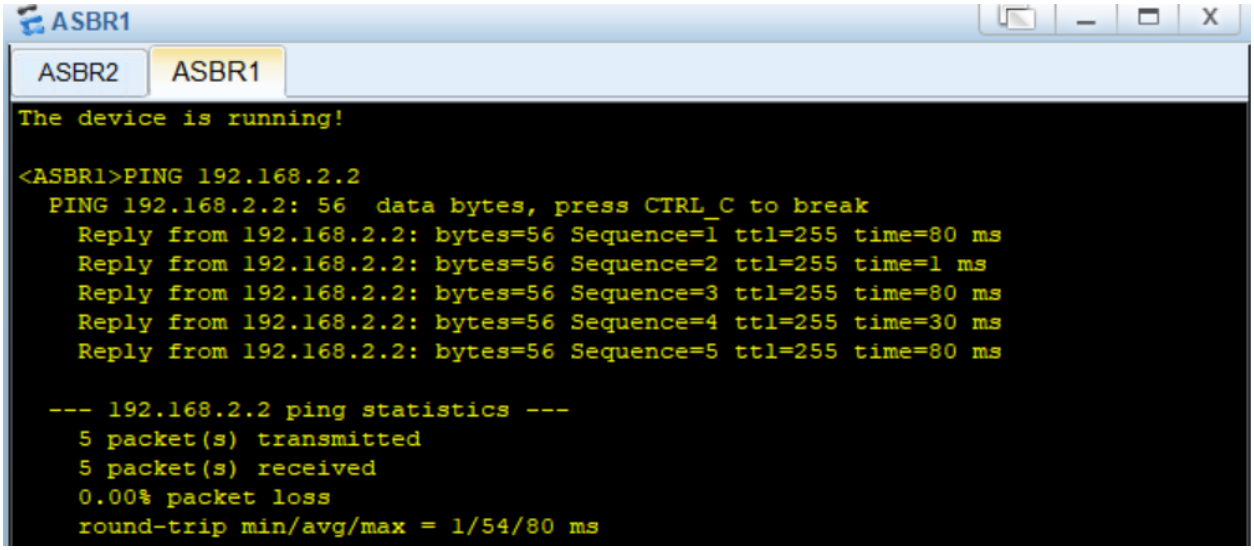


Figure III-12: Ping de ASBR1 vers ASG1.

De la même façon, on vérifie que le protocole ISIS a été installé dans tous les routeurs de l'ID 1. On remarque que la transmission des paquets a été bien reçus par les routeurs destinataires, On conclut que le protocole ISIS a était bien configurer.

III.7.3.5 Configuration de MPLS :

La Configuration des capacités de base MPLS et MPLS LDP pour établir des LSP LDP sur le réseau backbone MPLS.

La configuration de MPLS sur chaque routeur est répartie en 3 étapes :

- Activation du mode MPLS sur les Routeurs.
- Activation du mode MPLS sur les interfaces qu'on souhaite faire participer au domaine MPLS.
- L'activation de protocole LDP dans les routeurs et les interfaces

On active le MPLS sur toutes les retours et les interfaces end to end de notre réseau en utilisant les commandes :

- ✓ **MPLS lSR-id 2.2.2.2 (Ex : adresse loopback0 de l'ASG1) : Cette** commande permet d'identifie un LSR pour chaque routeur afin d'améliorer la fiabilité du réseau.
- ✓ **MPLS :** pour l'activation d'MPLS dans les routeurs et les interfaces
- ✓ **MPLS LDP :** pour l'activation de protocole dans toutes les routeurs et les interfaces.

Configuration de MPLS dans le routeur ASG1 :

ASG1

```
The device is running!

<ASG1>
<ASG1>
<ASG1>
<ASG1>SY
<ASG1>system-view
Enter system view, return user view with Ctrl+Z.
[ASG1]MPL
[ASG1]mpls LS
[ASG1]mpls lsr-id 2.2.2.2
[ASG1-mpls]QUIT
[ASG1]mpls ldp
[ASG1-mpls-ldp]QUIT
```

Figure III-13 : Exemple de Configuration de MPLS dans le routeur ASG1.

La configuration des MPLS dans les interfaces de routeur ASG2 :

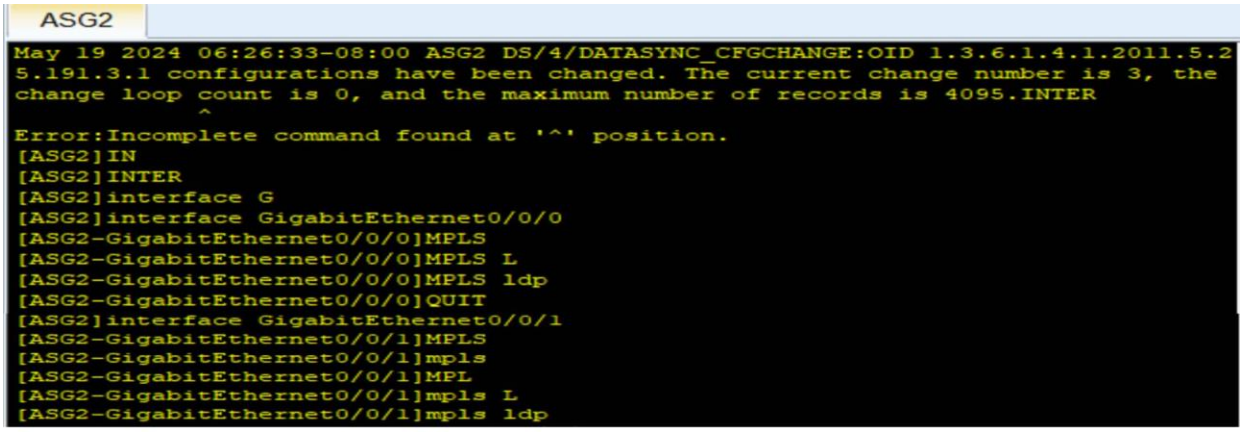


Figure III-14 : Exemple de Configuration de MPLS dans les interfaces de routeur ASG2.

Après avoir terminé les configurations, de MPLS et les sessions LDP sont établies entre les routeurs en exécute la commande « display MPLS LDP session ». La sortie de la commande montre que l'état de la session LDP est opérationnel.

Ensuite, en exécute exécutez la commande « display MPLS LDP LSP ». La sortie de la commande montre qu'un LDP LSP a été établi. L'exemple suivant utilise la sortie de la commande sur le routeur.

ASBR2

```
      ^
Error: Unrecognized command found at '^' position.
<ASBR2>SY
<ASBR2>system-view
Enter system view, return user view with Ctrl+Z.
[ASBR2]display mpls ldp session

 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID            Status      LAM  SsnRole  SsnAge       KASent/Rcv
 ------------------------------------------------------------------------------
 1.1.1.1:0         Operational DU   Active   0000:00:02   10/10
 6.6.6.6:0         Operational DU   Active   0000:00:01   6/6
 ------------------------------------------------------------------------------
 TOTAL: 2 session(s) Found.

[ASBR2]
[ASBR2]display mpls ldp lsp

 LDP LSP Information
 -------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop          OutInterface
 -------------------------------------------------------------------------------

 1.1.1.1/32         NULL/3         -               192.168.1.1      GE0/0/0
 1.1.1.1/32         1024/3         1.1.1.1         192.168.1.1      GE0/0/0
 1.1.1.1/32         1024/3         6.6.6.6         192.168.1.1      GE0/0/0
*1.1.1.1/32         Liberal/1027                   DS/6.6.6.6
```

Figure III-15 : Visualisation de labelling sur le routeur ASG2.

III.7.3.6 Les réseaux privés virtuels :

III.7.3.6.1 Le concept VRF (Virtual Routing and Forwarding):

Les clients (BNP, BNP2, BTS, BTS2 dans notre cas) sont interconnectés à travers les routeurs de périphéries PE (**ASG1, ASG4** dans notre cas) du réseau, qui nécessitent la création de VPN pour chaque client afin de construire des tables de routage séparés. Le concept de VRF permet à un opérateur de créer plusieurs tables de routage dans un même routeur. Ces tables sont étanches entre elles et chacune est généralement associée à un client. Une même adresse IP peut être affectée plusieurs fois à différentes interfaces car celles-ci sont placées dans des VRF différentes.

Configuration des routeurs virtuels (VRF) : Les VRF sont configurées sur les routeurs avec les paramètres suivants (Nom de VRF, RD et RT).

- **Configuration de RD** : c'est un identifiant, codé sur 64 bits, Le route distinguisher permet de distinguer les routes de différents VPNs lorsqu'elles sont propagées à travers le réseau MPLS. Il aide à maintenir l'unicité des routes entre

différents clients ou services. Même si différents clients utilisent les mêmes adresses IP privées, les RDs permettent de les distinguer.

- **Configuration de RT** : Chaque VRF définie sur un PE est configurée pour exporter et importer ses routes. L'import et l'export de routes sont gérés grâce à une communauté étendue BGP appelée RT.

Dans notre topologie en a créer deux VRF nommé BNp et BTS le tableau suivant montre les valeurs affectées aux VRF, RD et RT pour les routeurs PE (ASG1 et ASG2) et les routeur CE (BNP BTS, BNP2, BTS2).

Tableau III-2: Affectation des RT et RD au VRF

Les routeurs	PE- ASG1	PE- ASG1
Distinguisher (RD)	**BNp :** **100 :1**	**BNp :** **200 :1**
	BTS :100 :2	**BTS :200 :2**
La Route Target (RT)	**BNp :111 :1**	**BNp :111 :1**
	BTS :222 :2	BTS :222 :2

Pour la création des VRF en a utilisé les commandes suivantes (exemple de VRF : BTS dans le routeur ASG4) :

- **IP VPN-instance BTS : Créer** un VRF nommée BTS
- **Ipv4-family :** Configurer la famille d'adresses IPv4 pour le VRF BTS, spécifie que cette instance VPN va utiliser des adresses IPv4, préparant ainsi l'instance pour recevoir des routes IPv4.
- **Route-distinguisher 100 :1** : Attribuer un identifiant unique (route distinguisher) à cette instance VPN.
- **Vpn-target 111 :1 both** : Définir un VPN Target pour cette instance VPN, avec l'option "both" (import et export)

La figure suivante montre La création de VRF « BTS » dans le routeur ASG4

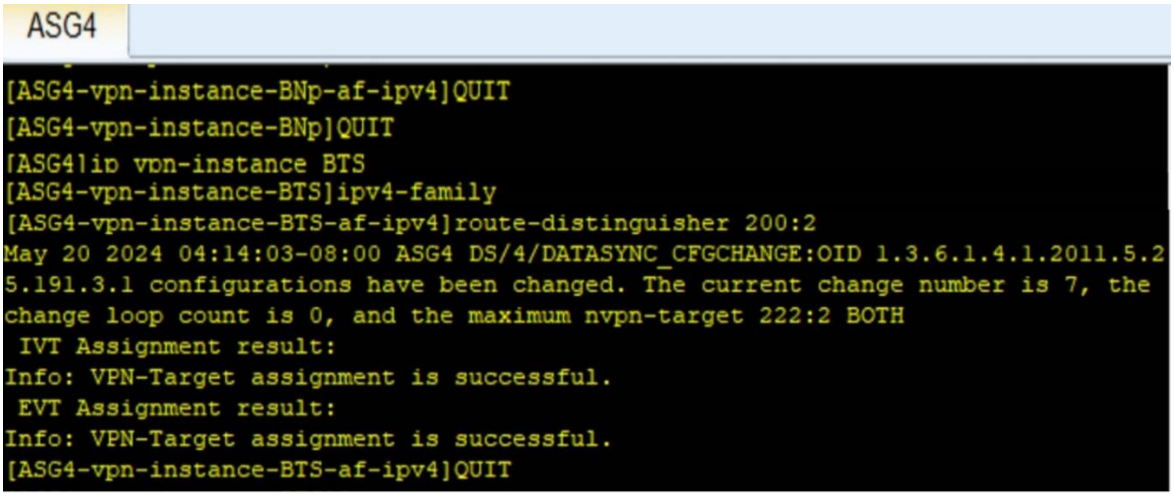


Figure III-16 : Exemple de configuration VRF « BTS » dans le routeur ASG4.

Pour vérifier les configurations des VRF en exécutez la commande **« display IP VPN instance verbose »** sur chaque routeur.

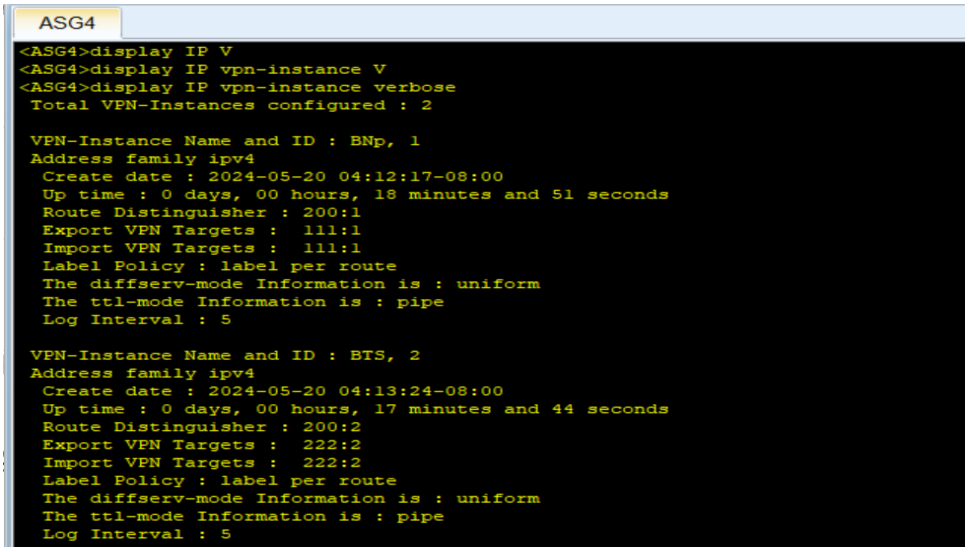


Figure III-17: Vérification de la création de VRF.

III.7.3.7 L'Établissement de sessions MP-BGP VPNv4 :

MP-BGP est configuré pour échanger les routes VPNv4 entre les routeurs PE.

Les routes VPNv4 contiennent les informations nécessaires pour identifier et acheminer les paquets vers les bonnes VRF.

III.7.3.7.1 Rôle de MP-BGP VPNv4 dans un réseau MPLS :

- **Propagation des routes entre les VRF** :

Les VRF créent des tables de routage distinctes pour chaque client sur les routeurs PE (Provider Edge).

MP-BGP VPNv4 permet l'échange de routes entre ces VRF sur différents routeurs PE. Cela signifie que les routes d'un client sur un PE peuvent être propagées aux autres PEs dans le réseau MPLS, permettant la connectivité globale du client.

- **Utilisation de Route Distinguishers (RD) :**

MP-BGP VPNv4 transporte les routes avec leurs RDs, assurant que les préfixes IP sont uniques dans le réseau MPLS.

- **Isolation et sécurité des données :**

En utilisant MP-BGP VPNv4, chaque VRF reste isolée et indépendante. Les routes d'un client ne sont pas mélangées avec celles d'un autre client.

Pour la configuration de MP-BGP en utilise les commandes suivantes (exemple de routeur ASG4) :

- **Bgp 100 :** Initialiser le processus BGP avec le numéro d'AS de PE1.
- **Peer 3.3.3.9 as-number :** Définir le voisin BGP avec l'adresse IP 3.3.3.9 dans le même AS.
- **Peer 3.3.3.9 connect-interface loopback 1 :** Utiliser l'interface loopback pour la session BGP, ce qui assure une connexion stable et continue.
- **Ipv4-family vpnv4 :** Passer à la configuration des routes VPNv4.
- **Peer 3.3.3.9 enable :** Activer l'échange de routes VPNv4 avec le voisin BGP.

```
[ASG4]bgp 100
[ASG4-bgp]peer 2.2.2.2 as-number 100
[ASG4-bgp]peer 2.2.2.2 connect-interface LoopBack 0
[ASG4-bgp]ipv4-family VPNV4
[ASG4-bgp-af-vpnv4]peer 2.2.2.2 en
[ASG4-bgp-af-vpnv4]peer 2.2.2.2 enable
```

Figure III-18 : Exemple de configuration de MP-BGP dans le routeur ASG4

Après avoir terminé les configurations, exécutez la commande « **display BGP vpnv4 all Peer »** sur les PE. La sortie de la commande montre qu'une relation de voisinage BGP a été établie entre les PE et qu'elle est dans l'état Established.

```
<ASG1>dis bgp vpnv4 a
<ASG1>dis bgp vpnv4 all p
<ASG1>dis bgp vpnv4 all pee
<ASG1>dis bgp vpnv4 all peer

 BGP local router ID : 192.168.3.1
 Local AS number : 100
 Total number of peers : 3            Peers in established state : 3

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
fRcv

  5.5.5.5         4         100        3        3     0 00:00:39 Established
   1
  8.8.8.8         4         100        3        3     0 00:00:40 Established
   1
  9.9.9.9         4         100        2        3     0 00:00:40 Established
   0
```

Figure III-19 : État des relations de voisinage BGP entre les PE

Partie 2 : Notre étude sur la zone de Relizane

III.8 Etude de la topologie de Relizane :

III.8.1 La plateforme iMASTER NCE :

D'âpres la plateforme iMASTER NCE pour la gestion de réseau cette interface représente topologie de ATM Mobilis :

Figure III-20 : Topologie IP RAN de ATM Mobilise

Dans Notre travail on sera étudié la région Relizane pour savoir les problèmes et améliorer notre KPI et la qualité de service de réseau à l'aide le système NCE.

III.8.2 La topologie de Relizane :

Notre topologie est définie dans la figure

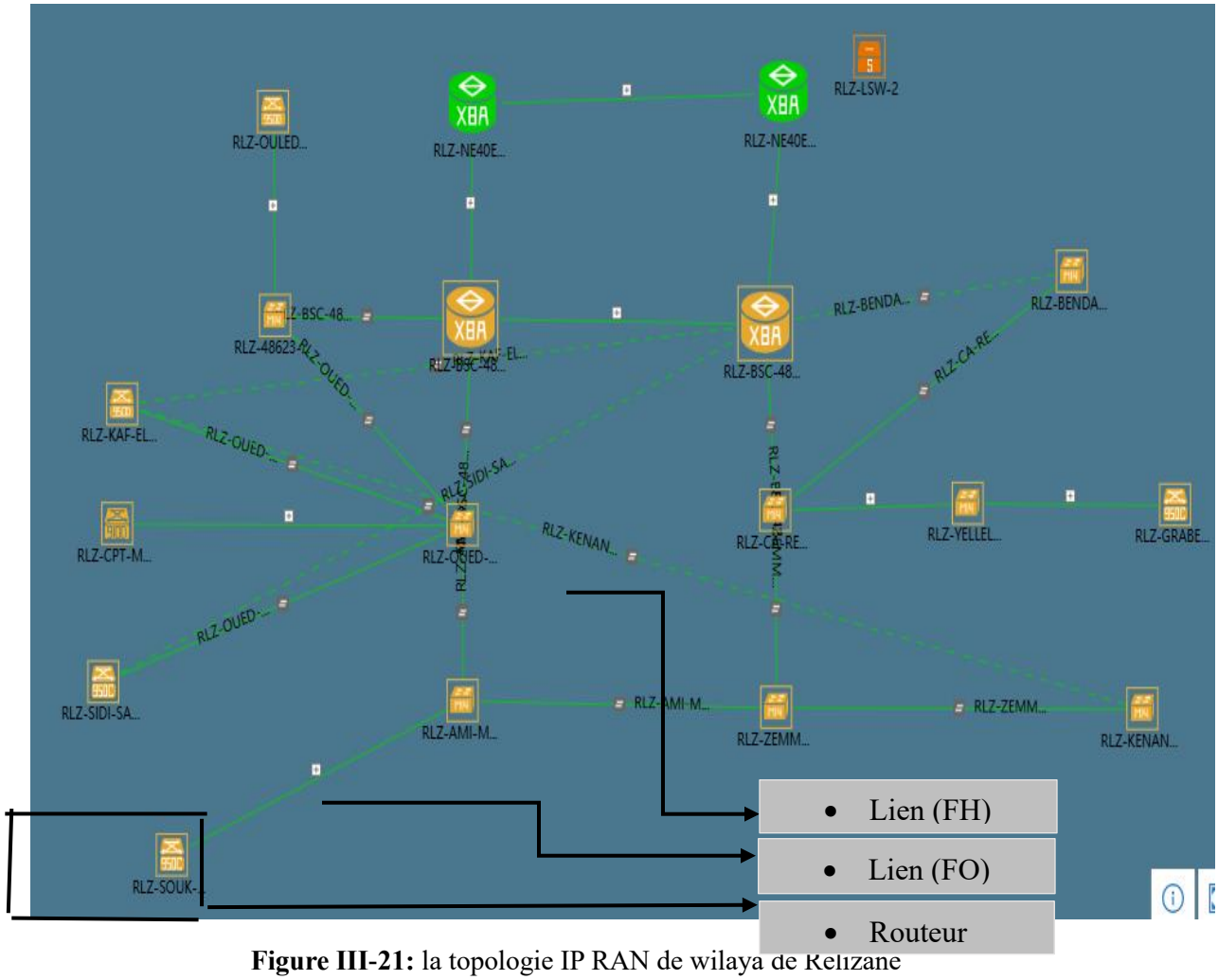


Figure III-21: la topologie IP RAN de wilaya de Relizane

III.8.3 Etude sur la topologie

III.8.3.1 Nombre et Nom des routeurs :

le réseau est composé de 19 Routeur on définit chaque Routeur avec son nom :

Les Noms des Routeur
RLZ_48623_SIDI_KHETAB_ASG_13
RLZ_AMI_MOUSSA_48610_ASG_2
RLZ_BENDAOUD_48657_ASG_9
RLZ_BSC_48001_ASBR_1
RLZ_BSC_48001_ASBR_2
RLZ_CA_RELLIZANE_48101_ASG_6
RLZ_CPT_MAZOUNA_48901_ASG_15
RLZ_GRABES_48205_ASG_8
RLZ_KAF_EL__ABADIA_48102_ASG_12
RLZ_KENANDA_48625_ASG_10
RLZ_LSW_2
RLZ_NE40E_X8A_1
RLZ_NE40E_X8A_2
RLZ_OUED_RHIOU_4803X_ASG_7
RLZ_OULED_SIDI__MIHOUB_4651_ASG_14
RLZ_SIDI_SAID_48904_ASG_3
RLZ_SOUK_ELHAD_48648_ASG_11
RLZ_YELLEL_48201_ASG_7
RLZ_ZEMMOURA_48210_ASG_4

Tableau III 2: Nom des Routeurs

III.8.3.2 Alerte check :

Correspond à une fonctionnalité qui permet de vérifier et de surveiller les alertes dans un système de gestion de réseau. Cette fonctionnalité permet de contrôler et de vérifier l'état des alertes, qu'elles soient liées à des pannes, à des performances dégradées ou à d'autres problèmes au sein du réseau. L'objectif est de détecter rapidement les problèmes potentiels et de prendre les mesures nécessaires pour les résoudre, afin d'assurer un fonctionnement optimal du réseau. En résumé, "Alerte check" dans iMaster NCE se réfère à la vérification et à la surveillance des alertes dans un système de gestion de réseau.

La figure montre les différences alerte reçus :

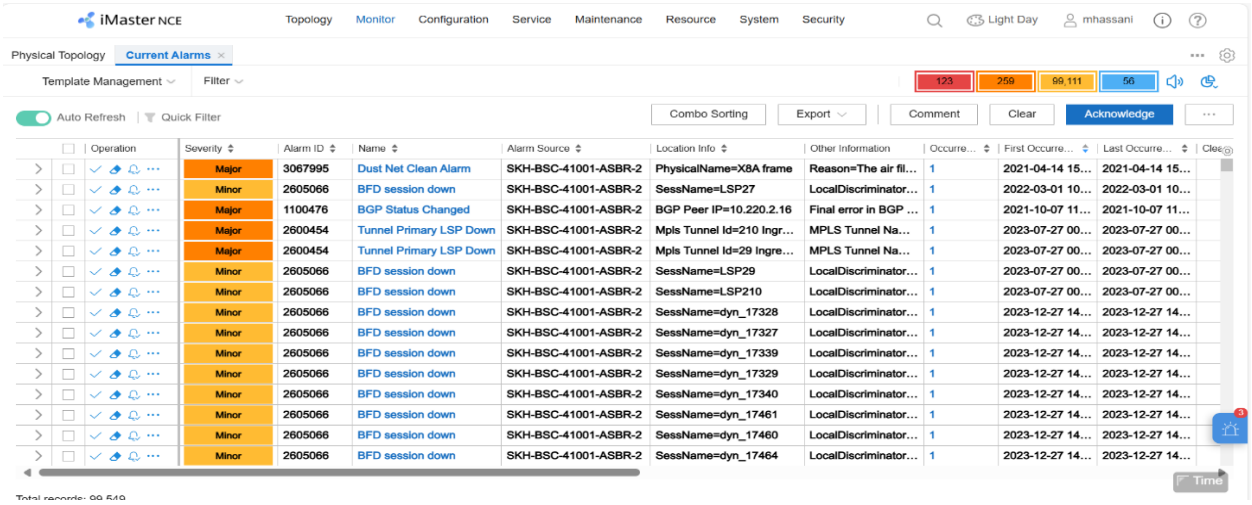


Figure III-22 : Fenêtre des alertes

III.8.3.3 Auto indice trouble short

C'est une fonctionnalité qui automatise la détection et la résolution des problèmes dans un réseau. Elle analyse les indicateurs et les alarmes du réseau, identifie les problèmes potentiels et propose des solutions pour les résoudre, réduisant ainsi les temps d'arrêt et accélérant le processus de dépannage. Comme est montrer dans les figure VI. 1 et VI. 2 ci-dessus :

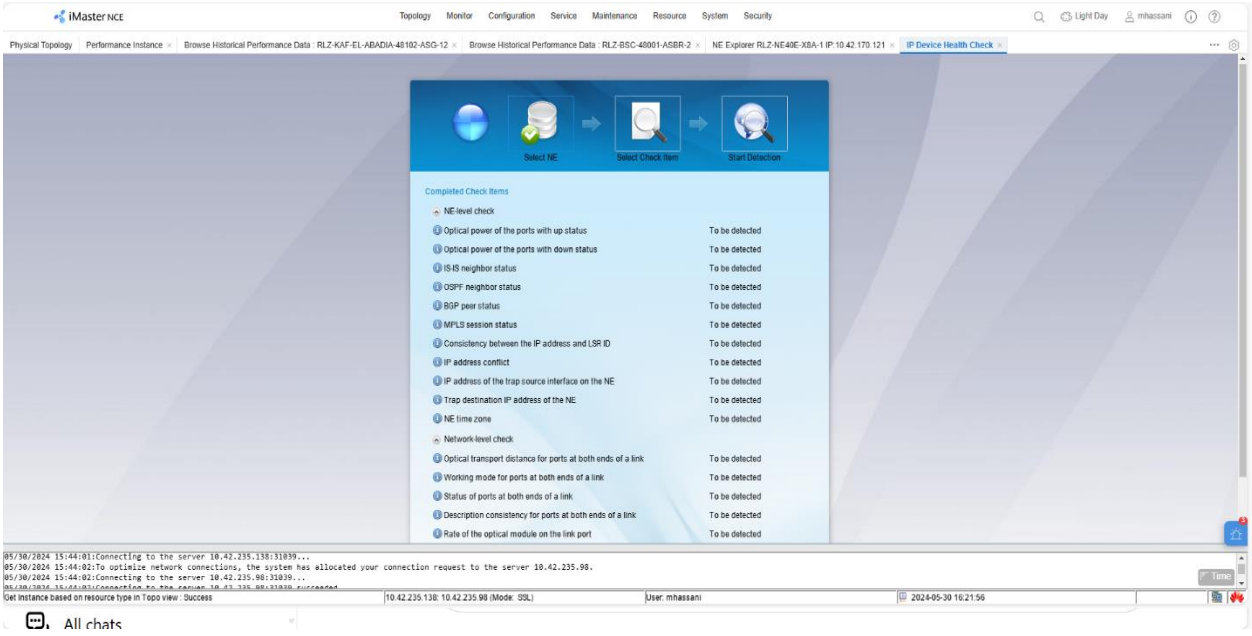
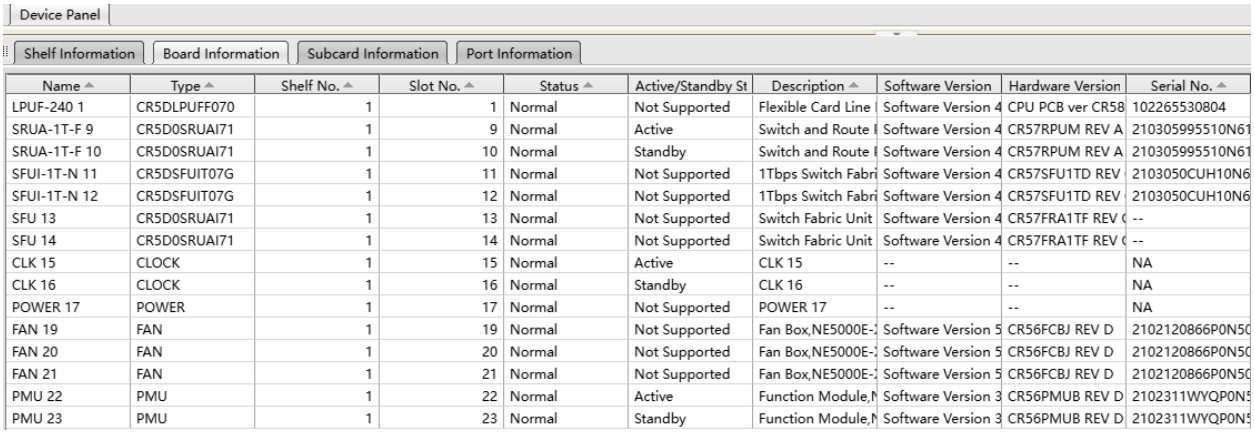


Figure III-23 : fenêtre qui automatise la détection et résolution des problèmes



Name	Type	Shelf No.	Slot No.	Status	Active/Standby St	Description	Software Version	Hardware Version	Serial No.
LPUF-240 1	CR5DLPUFF070	1	1	Normal	Not Supported	Flexible Card Line	Software Version 4	CPU PCB ver CR58	102265530804
SRUA-1T-F 9	CR5D0SRUAI71	1	9	Normal	Active	Switch and Route I	Software Version 4	CR57RPUM REV A	210305995510N61
SRUA-1T-F 10	CR5D0SRUAI71	1	10	Normal	Standby	Switch and Route I	Software Version 4	CR57RPUM REV A	210305995510N61
SFUI-1T-N 11	CR5DSFUIT07G	1	11	Normal	Not Supported	1Tbps Switch Fabri	Software Version 4	CR57SFU1TD REV	2103050CUH10N6
SFUI-1T-N 12	CR5DSFUIT07G	1	12	Normal	Not Supported	1Tbps Switch Fabri	Software Version 4	CR57SFU1TD REV	2103050CUH10N6
SFU 13	CR5D0SRUAI71	1	13	Normal	Not Supported	Switch Fabric Unit	Software Version 4	CR57FRA1TF REV C	--
SFU 14	CR5D0SRUAI71	1	14	Normal	Not Supported	Switch Fabric Unit	Software Version 4	CR57FRA1TF REV C	--
CLK 15	CLOCK	1	15	Normal	Active	CLK 15	--	--	NA
CLK 16	CLOCK	1	16	Normal	Standby	CLK 16	--	--	NA
POWER 17	POWER	1	17	Normal	Not Supported	POWER 17	--	--	NA
FAN 19	FAN	1	19	Normal	Not Supported	Fan Box,NE5000E-1	Software Version 5	CR56FCBJ REV D	2102120866P0N5C
FAN 20	FAN	1	20	Normal	Not Supported	Fan Box,NE5000E-1	Software Version 5	CR56FCBJ REV D	2102120866P0N5C
FAN 21	FAN	1	21	Normal	Not Supported	Fan Box,NE5000E-1	Software Version 5	CR56FCBJ REV D	2102120866P0N5C
PMU 22	PMU	1	22	Normal	Active	Function Module,N	Software Version 3	CR56PMUB REV D	2102311WYQP0N5
PMU 23	PMU	1	23	Normal	Standby	Function Module,N	Software Version 3	CR56PMUB REV D	2102311WYQP0N5

Figure III-24: fenêtre qui automatise la détection et résolution des problèmes

III.8.3.1 Plug and Play :

Simplifie le déploiement et la configuration des nouveaux équipements réseau en automatisant le processus de configuration initiale, ce qui permet d'économiser du temps et d'améliorer l'efficacité lors de l'intégration des équipements au sein du réseau.

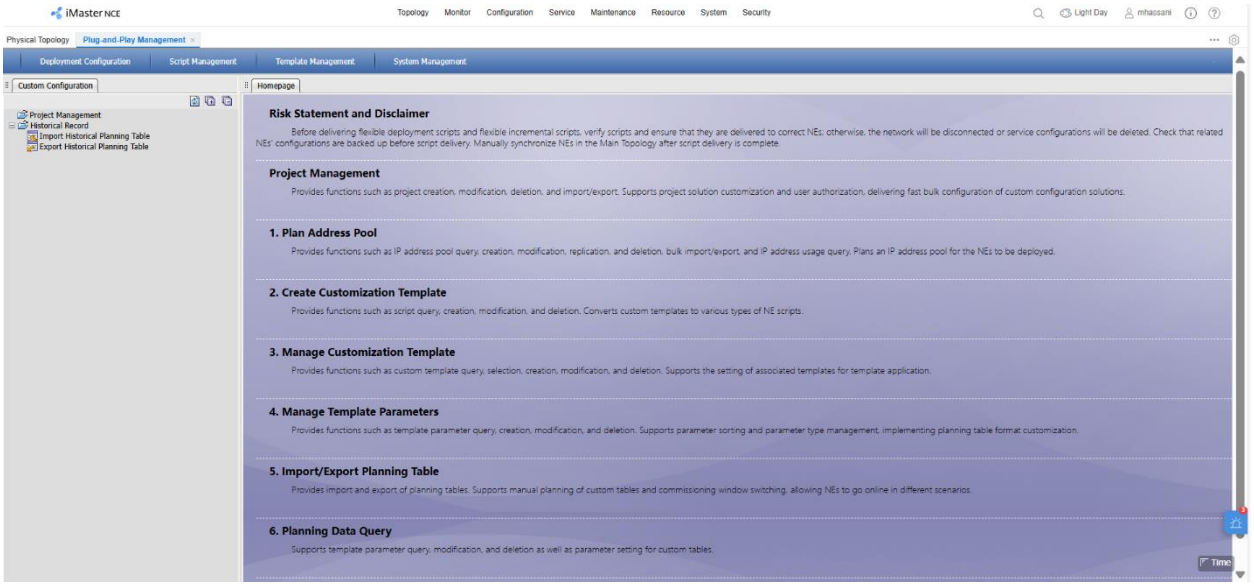


Figure III-25: PLUG AND PLAY

III.8.3.2 Les étapes de configuration des Retours au niveau de NCE :

- Création le sous réseaux (subnet).
- Création des NEs (Network éléments).
- Paramétrages des NEs.
- L'attribution des cartes.
- La mise a jour des NEs.
- Configuration des NEs Source.
- Configuration des NEs Destinations.

III.8.3.2.1 Création le sous réseaux (subnet) :

Nous avons créé le subnet ou on doit mettre les NEs, les étapes de la création du sous réseau sont illustrées dans la figure suivante :

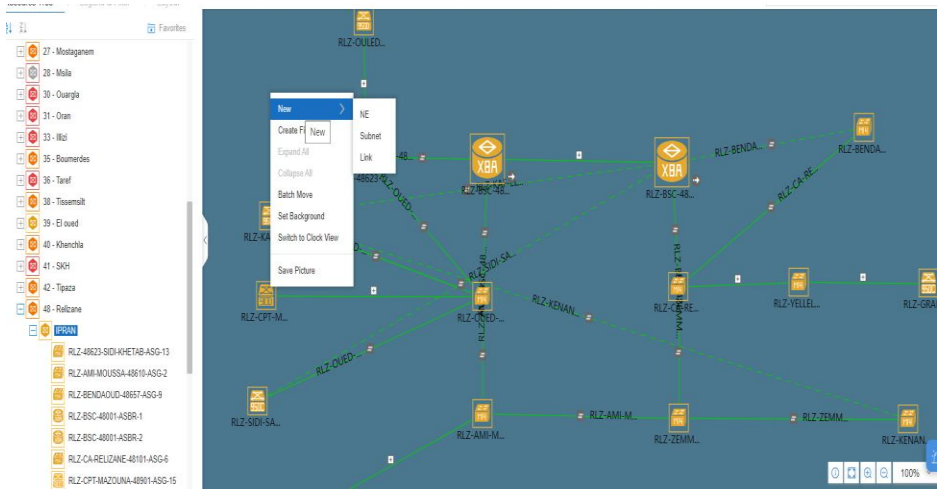


Figure III-26 : Création sous Réseaux (subnet)

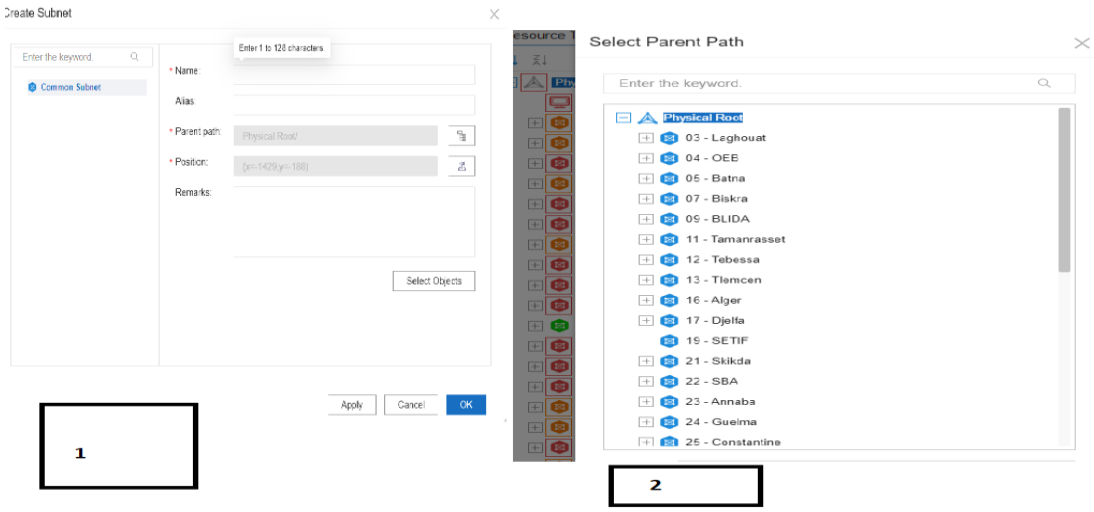


Figure III-27: Création sous Réseaux (subnet)

Après la création de sous réseaux on attribue le nom, le type, et la plage des adresses :

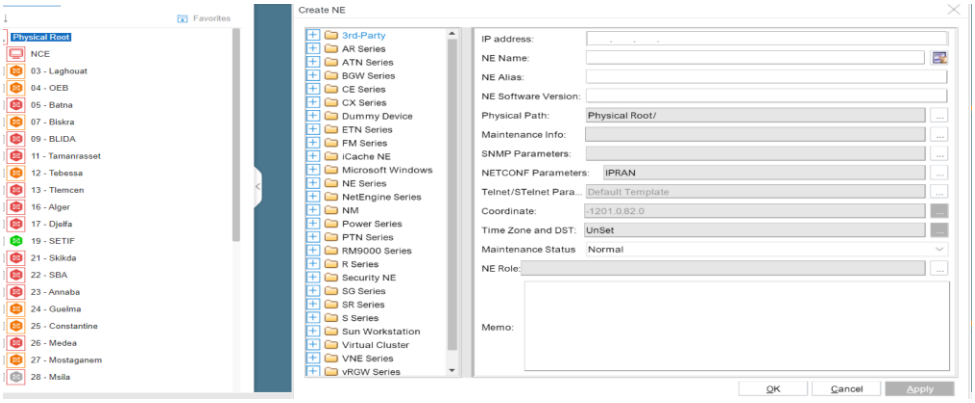
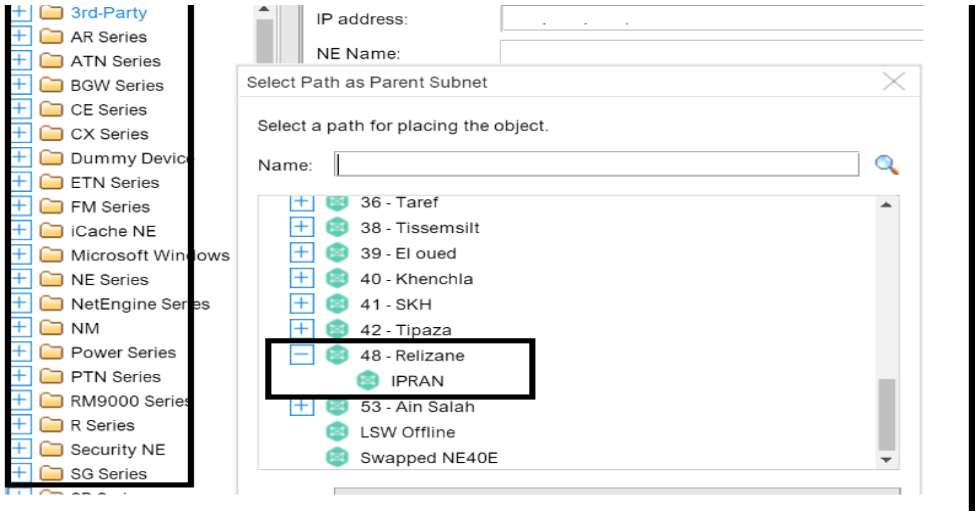


Figure III-28: Paramétrage de sous Réseaux



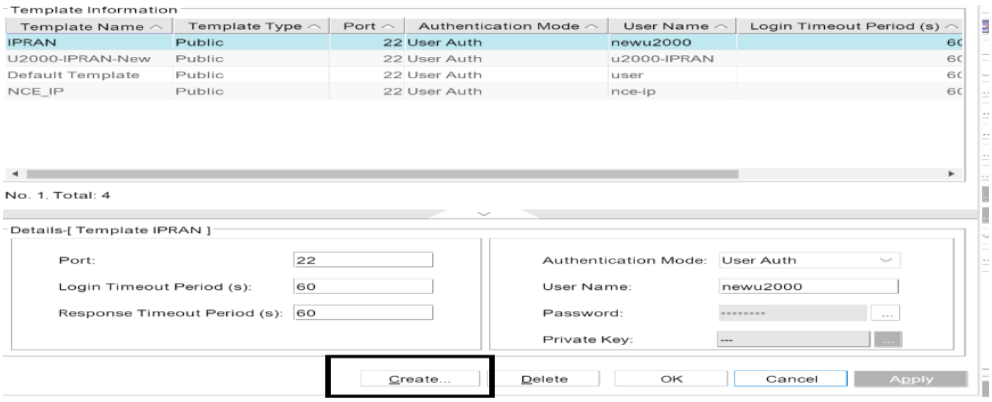


Figure III-29: la creation de subnet

III.8.3.2.2 Création des NEs

Après l'étape de création le sous réseau nous avons créé NEs, les étapes de création des NEs sont illustrées dans la figure suivante

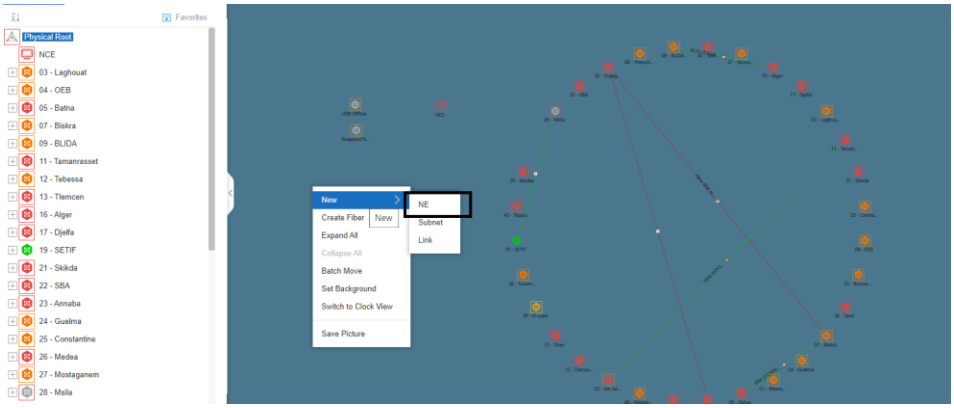


Figure III-30: Les étapes de création les NEs

III.8.3.2.2.1 Paramétrage des NEs

Après la création des NEs, nous avons choisir le type d'équipement ; exemple ASBR, et après nous avons attribué à chaque NE ses paramètres comme le montre la figure suivante :

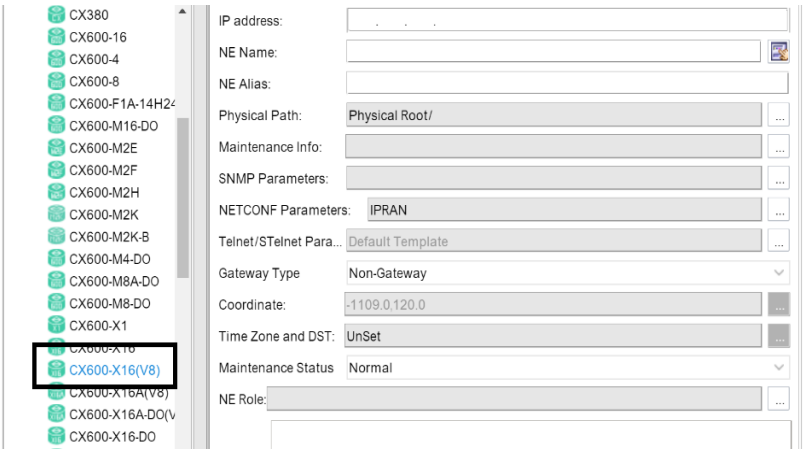


Figure III-31: Les paramètres de configuration des NEs

- **Les différents paramètres d'un NE sont :**

(ID, nom, Gateway, protocole, l'adresse IP, et le nom d'utilisateur et le mot passe). Un ID unique doit être attribué à chaque nœud afin d'identifier les différents nœuds dans le réseau, ce qui permet au gestionnaire NMS d'identifier les différents éléments réseau dans sa base de données, le tableau suivant représente les différents paramètres que nous allons configurer :

Tableau III-3: les paramètres des NEs créées a fin implémentation.

Site	Numéro ID	Protocole	Adresse IP
RLZ_48623_SIDI_KHETAB_ASG_13	59716	IP	10.44.100.187
RLZ_AMI_MOUSSA_48610_ASG_2	61261	IP	10.44.50.126
RLZ_BENDAOUD_48657_ASG_9	57256	IP	10.44.50.133
RLZ_BSC_48001_ASBR_1	58605	IP	10.44.50.123
RLZ_BSC_48001_ASBR_2	58606	IP	10.44.50.124
RLZ_CA_RELLIZANE_48101_ASG_6	55432	IP	10.44.50.130
RLZ_CPT_MAZOUNA_48901_ASG_15	52791	IP	10.44.100.245
RLZ_GRABES_48205_ASG_8	37339	IP	10.44.50.132
RLZ_KAF_EL__ABADIA_48102_ASG_12	59473	IP	10.44.50.182
RLZ_KENANDA_48625_ASG_10	55920	IP	10.44.50.144

RLZ_LSW_2	57253	IP	10.40.92.46
RLZ_NE40E_X8A_1	53794	IP	10.42.170.121
RLZ_NE40E_X8A_2	53664	IP	10.42.170.122
RLZ_OUED_RHIOU_4803X_ASG_7	61210	IP	10.44.50.129
RLZ_OULED_SIDI__MIHOUB_4651_ASG_14	49577	IP	10.44.100.188
RLZ_SIDI_SAID_48904_ASG_3	37410	IP	10.44.50.127
RLZ_SOUK_ELHAD_48648_ASG_11	39213	IP	10.44.100.172
RLZ_YELLEL_48201_ASG_7	55598	IP	10.44.100.187
RLZ_ZEMMOURA_48210_ASG_4	57176	IP	10.44.100.187

III.8.3.3 L'Equipment View :

Offre une visualisation centralisée et détaillée des équipements du réseau, permettant aux administrateurs réseau de surveiller, diagnostiquer, configurer et gérer efficacement les équipements pour assurer un fonctionnement optimal du réseau.

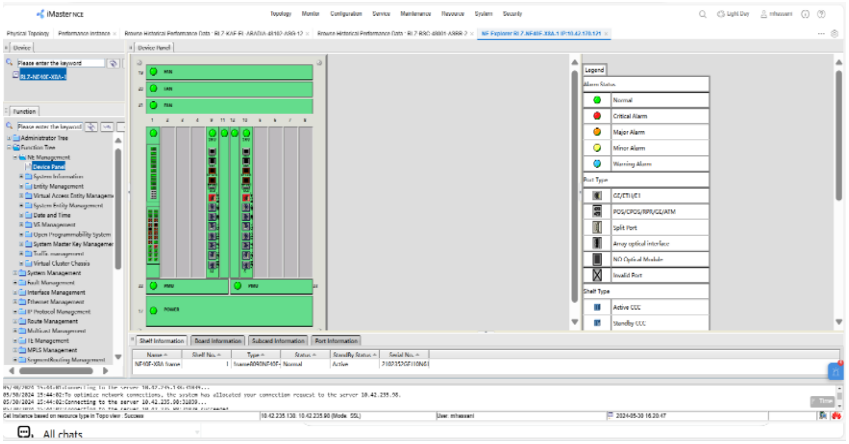


Figure III-32: visualisation centralisée et détaillée de Retour

Partie 3 : l'implémentation des scripts python

III.9 Intégration de l'Algorithme Python dans la Topologie Réseau de Relizane Simulée dans eNSP :

Afin d'intégrer l'algorithme dans notre topologie, nous avons d'abord connecté eNSP à notre PC en suivant ces étapes :

III.9.1 Création d'une Nouvelle carte réseaux Ethernet pour le Test sur le PC

Nous avons créé une nouvelle carte réseaux Ethernet (Ethernet 5) sur notre PC et l'avons configurée statiquement avec une adresse IP, un masque de sous-réseau et une passerelle par défaut.

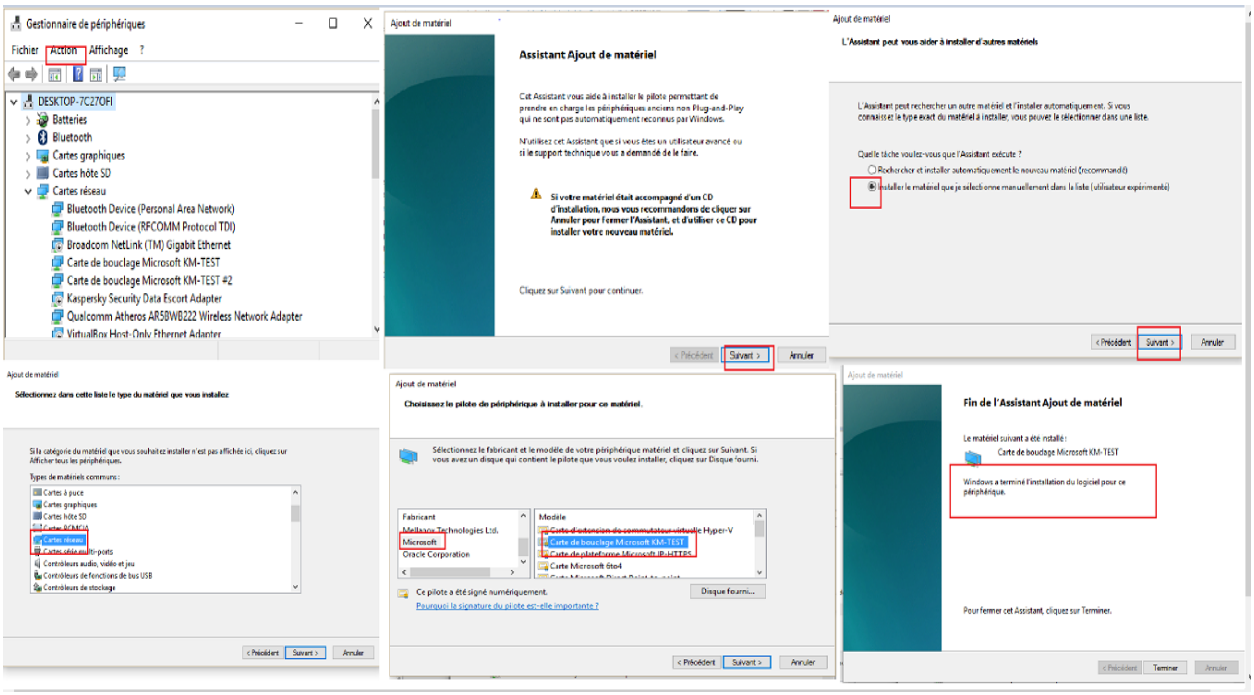


Figure III 40 **: Création d'une nouvelle carte réseaux Ethernet.**

III.9.2 Configuration de la nouvelle Carte Réseau :

Nous avons configuré statiquement l'interface réseau avec une adresse IP, un masque de sous-réseau et une passerelle par défaut

.

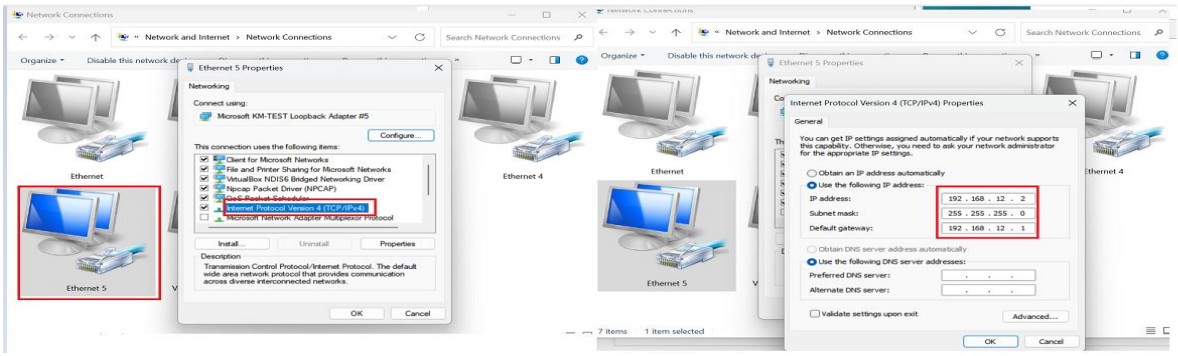


Figure III 41 : Configuration de carte réseaux.

III.9.3 Configuration d'un Cloud dans eNSP

Nous avons configuré un cloud dans eNSP en lui attribuant la même adresse IP que la nouvelle interface physique du PC, soit « 192.168.12.2 ».

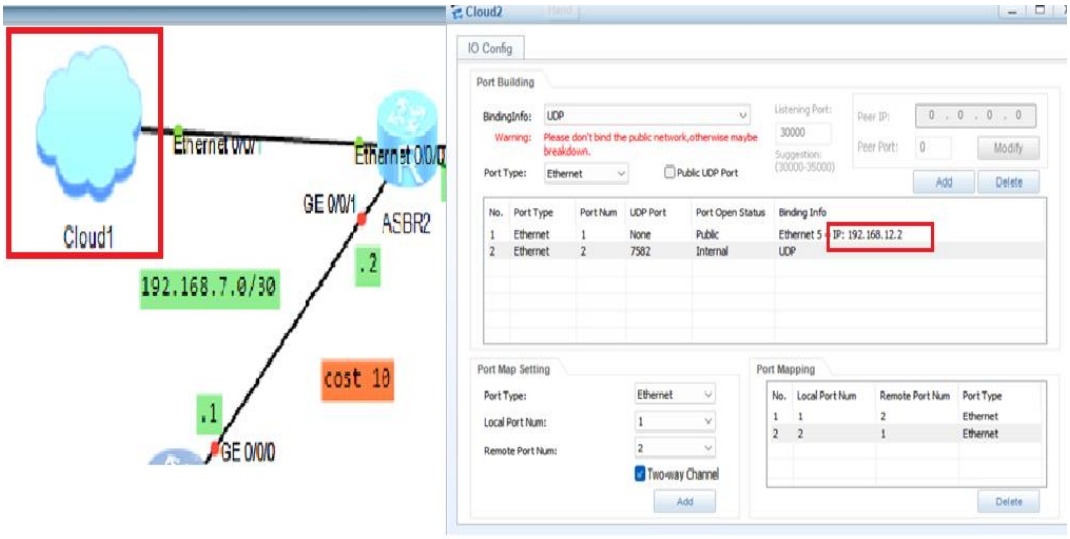


Figure III 42: Configuration d'un Cloud dans eNSP.

III.9.4 Configuration de l'Interface du Routeur ASBR2 Connectée au Cloud :

Nous avons configuré l'interface du routeur ASBR2 comme passerelle par défaut pour le cloud, en lui attribuant la même adresse IP que la passerelle par défaut de notre PC, soit « 192.168.12.1 ».

```
[ASBR2]interface Eth
[ASBR2]interface Ethernet0/0/0
[ASBR2-Ethernet0/0/0]ip add
[ASBR2-Ethernet0/0/0]ip address 192.168.12.1 30
[ASBR2-Ethernet0/0/0]
```

Figure III 43 : Configuration de l'interface du routeur ASBR2 qui relie au cloud.

III.9.5 Test de la Connectivité :

- Nous avons utilisé la commande ping sur le CMD de notre PC pour tester la connectivité avec les routeurs de notre topologie ENSP.

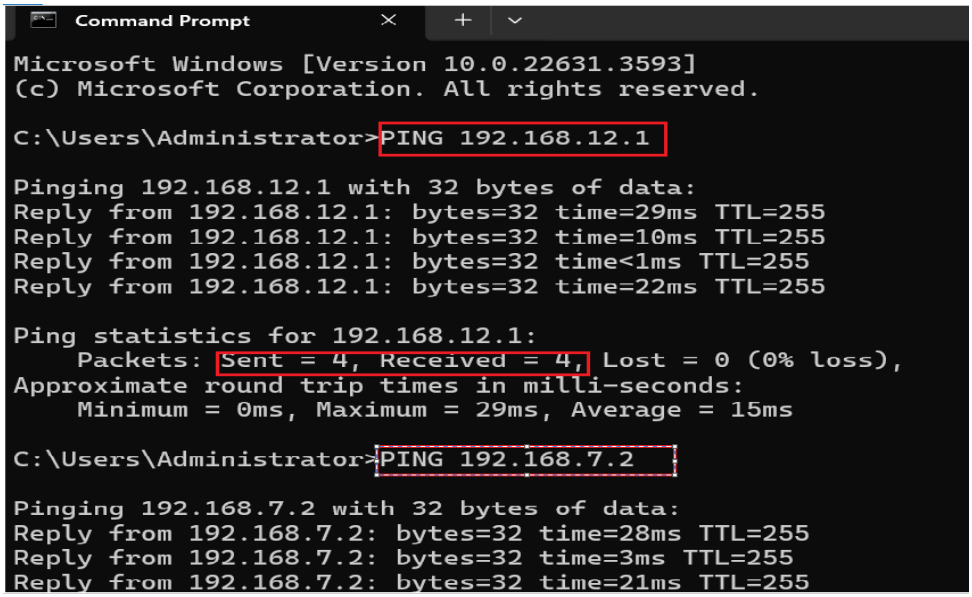


Figure III 44 : test de connectivité entre le pc et les routeurs de notre topologie ENSP.

- Nous avons ping notre pc à travers le routeur ASBR2 de notre topologie de pour tester la connectivité entre les routeurs de notre topologie ENSP et notre pc.

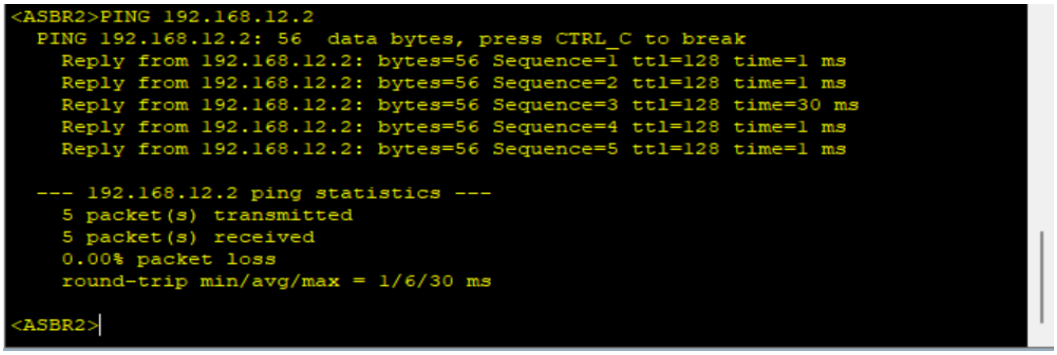


Figure 45 *:* test de connectivité entre le routeur ASBR2 et notre pc.

III.9.6 Configuration du Protocole d'Accès à Distance Telnet :

Nous avons configuré le protocole Telnet sur tous les routeurs de notre topologie pour permettre l'accès à distance. Tous les routeurs sont configurés de la même façon.

```
[ASBR2]telnet server enable
Info: The Telnet server has been enabled.
[ASBR2]
[ASBR2]aaa
[ASBR2-aaa]loc
[ASBR2-aaa]local-user amina pa
[ASBR2-aaa]local-user amina password ci
[ASBR2-aaa]local-user amina password cipher 123
Info: Add a new user.
[ASBR2-aaa]local-user amina service-type telnet
[ASBR2-aaa]local-user amina privilege level 1
[ASBR2]user-interface vty 0 4
[ASBR2-ui-vty0-4]authen
[ASBR2-ui-vty0-4]authentication-mode p
[ASBR2-ui-vty0-4]authentication-mode password 123
[ASBR2-ui-vty0-4]authentication-mode aaa
```

Figure 46 : configuration de telnet

III.9.7 Installation de Tera Term :

Nous avons installé le logiciel Tera Term sur notre PC pour accéder aux routeurs de notre topologie via Telnet. Cela nous a permis de confirmer que le PC peut se connecter aux routeurs via Telnet. Cette étape est essentielle car l'algorithme que nous avons intégré à la topologie utilise Telnet pour accéder aux routeurs et effectuer des modifications.

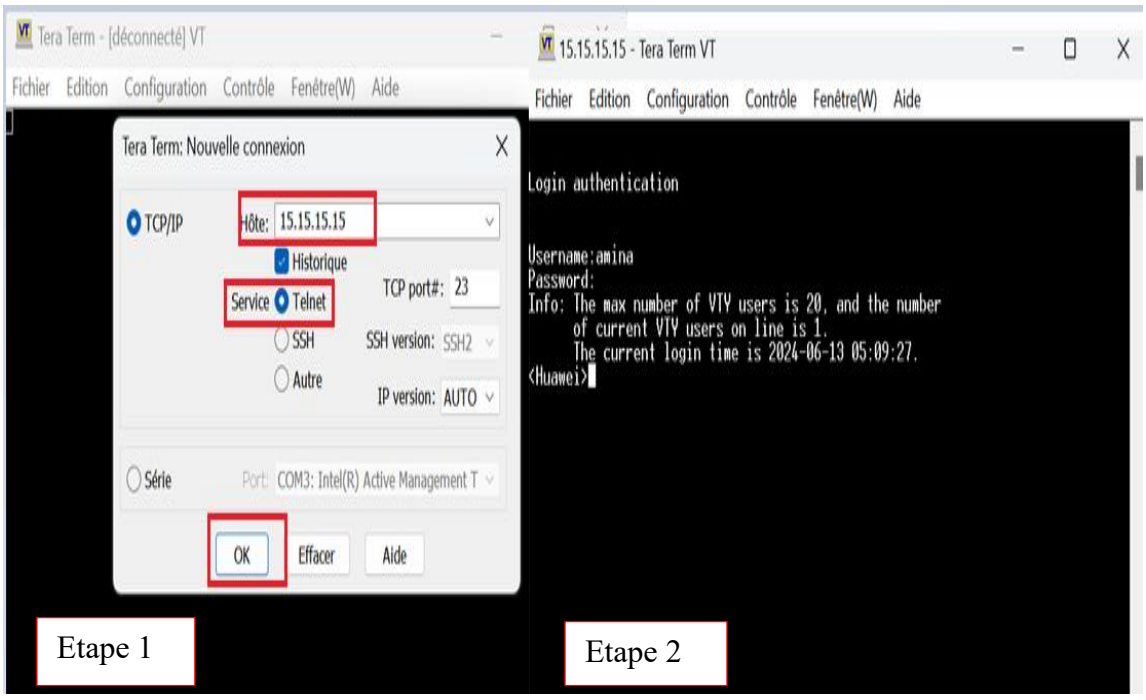


Figure 47 : Accès au routeur avec l'adresse de Loopback « 15.15.15.15 » via telnet en utilisant tera term

III.9.8 Implémentation des scripts :

III.9.8.1 La vérification de santé (Health Check) :

III.9.8.1.1 Définition :

Le Health check, ou vérification de santé, est un processus systématique et automatisé utilisé pour évaluer l'état de fonctionnement des composants d'un réseau de télécommunication. Il consiste en une série de tests et de mesures pour vérifier que chaque élément du réseau fonctionne correctement et que les performances sont optimales.

III.9.8.1.2 Les besoins de vérification de santé :

Les réseaux de télécommunication sont complexes et comportent de nombreux composants, tels que les routeurs, les commutateurs, les liens de communication, etc. Toute défaillance ou sous-performance d'un de ces éléments peut entraîner des interruptions de service, des pertes de données, et une qualité de service (QoS) dégradée. La vérification de santé régulière permet de détecter et corriger ces problèmes avant qu'ils n'affectent les utilisateurs .

III.9.8.1.3 Pourquoi les en utilise dans notre réseau :

- **Prévention des pannes :** En identifiant les signes précurseurs de défaillance, les Health checks permettent de prendre des mesures préventives.
- **Amélioration de la QoS :** En assurant que tous les composants fonctionnent de manière optimale, la QoS globale du réseau est maintenue.
- **Réduction des coûts :** La prévention des pannes et la maintenance proactive réduisent les coûts associés aux interruptions de service non planifiées et aux réparations urgentes.

III.9.8.1.4 Les scripts de la vérification de santé :

Utilisation de se script qui a été présenter dans les figures suivantes est pour :

Automatisation des tâches : Le script permet d'automatiser le processus de connexion aux routeurs et d'exécution des commandes. Au lieu de le faire manuellement pour chaque routeur, le script effectue ces actions de manière répétitive et cohérente. Cela peut vous faire gagner du temps et réduire les erreurs humaines potentielles.

Personnalisation : Le script est conçu de manière à pouvoir être facilement personnalisé. Vous pouvez ajouter ou supprimer des routeurs en modifiant les adresses IP correspondantes. De plus, vous pouvez ajuster les commandes à exécuter sur chaque routeur en modifiant les variables command1, command2 et command3. Cela vous permet d'adapter le script à vos besoins spécifiques.

Collecte de données : Le script enregistre les sorties des commandes exécutées sur les routeurs dans un fichier texte (check.txt). Cela vous permet de collecter et de stocker les informations obtenues à partir des routeurs pour une utilisation future. Vous pouvez analyser ces données ou les utiliser dans d'autres processus.

Flexibilité : Le script utilise des variables pour stocker les informations d'authentification, les adresses IP des routeurs et les commandes à exécuter. Cela rend le script flexible, car vous pouvez facilement les modifier sans avoir à modifier directement le code principal. Vous pouvez également étendre le script en ajoutant d'autres fonctionnalités ou en intégrant d'autres modules selon vos besoins.

Réutilisabilité : Une fois que vous avez écrit et testé le script, vous pouvez le réutiliser chaque fois que vous avez besoin d'exécuter des commandes sur les routeurs. Il vous suffit de fournir les informations d'authentification et les adresses IP appropriées, et le script s'occupera du reste. Cela permet d'économiser du temps et des efforts à long terme.

III.9.8.1.5 Explication de script :

1- Importe les modules telnetlib et datetime :

L'importation des modules telnetlib et datetime permet d'accéder aux fonctionnalités nécessaires pour établir une connexion Telnet et gérer les horaires dans le script.

- **Le module telnetlib** est un module standard de Python qui fournit une interface pour établir des connexions Telnet avec des hôtes distants. Il offre des classes et des méthodes permettant de se connecter, d'envoyer des commandes et de récupérer les réponses des hôtes via Telnet.

- **Le module datetime** est également un module standard de Python qui fournit des classes et des fonctions pour travailler avec des dates et des heures. Dans ce script, nous utilisons la classe datetime du module pour obtenir l'heure actuelle, que nous pouvons ensuite utiliser pour marquer les sorties des commandes avec l'heure à laquelle elles ont été récupérées.

Pour importer ces modules dans le script, nous utilisons la syntaxe import telnetlib et import datetime. Une fois importés, nous pouvons utiliser les fonctionnalités fournies par ces modules en utilisant leurs classes, fonctions et méthodes respectives.

```
1   import telnetlib
2   import datetime
3   import time
4
```

Figure III 48 : les bibliothèques utiliser dans le script

Cela nous permet d'établir une connexion Telnet avec les hôtes distants et de récupérer les sorties de commandes en utilisant le module telnetlib, et d'obtenir l'heure actuelle pour marquer les sorties en utilisant le module datetime.

2- La ligne 5 :

```
4
5   now = datetime.datetime.now()
```

Figure III 49 : fonction de l'heure.

Utilise la fonction **datetime.now ()** pour obtenir l'heure actuelle. Cela permet de marquer les sorties avec l'heure à laquelle elles ont été récupérées.

3-Les lignes hosts :

Définissent les adresses IP des différents hôtes avec lesquels une connexion Telnet sera établie. On a appliqué notre script seulement sur ces hôtes :

```
6   host1 = "1.1.1.1"
7   host2 = "2.2.2.2"
8   host3 = "3.3.3.3"
9   host4 = "5.5.5.5"
10  host6 = "6.6.6.6"
11  host7 = "7.7.7.7"
```

Figure III 50 : les adresses des hôtes utiliser dans le script

4- Accès avec telnet :

Les lignes username = "amina" et password = "123" définissent le nom d'utilisateur et le mot de passe utilisés pour se connecter aux hôtes distants via Telnet.

```
12  username = "amina" # the username
13  password = "123"
```

Figure III 51 : Accès avec telnet

5-Définit les commandes :

Définissent les commandes spécifiques qui seront exécutées sur chaque hôte pour récupérer les informations souhaitées.

La ligne 17 :

Définit une commande supplémentaire pour terminer la session Telnet. Dans cet exemple, il s'agit de la commande "sys".

La ligne 18 :

Ouvre un fichier nommé "check.txt" en mode écriture. Ce fichier sera utilisé pour enregistrer les sorties des commandes exécutées sur les hôtes.

```
14  command1 = "display isis peer"
15  command2 = "dis mpls ldp peer"
16  command3 = "dis bgp peer"
17  fin = "sys"
18  fp = open("check.txt","w")
```

Figure III 52 : les commandes utilisées

6-Les lignes (19 ,20) :

La ligne 19 :

Crée une instance de la classe Telnet du module telnetlib et établit une connexion Telnet avec le premier hôte (host1) sur le port 23 avec un délai de connexion de 6 secondes.

La ligne 20 :

Sont utilisées pour lire et écrire la réponse de l'hôte jusqu'à ce que le script rencontre la chaîne "Username :". Cela permet de se connecter à l'hôte en fournissant le nom d'utilisateur.

Les lignes similaires suivantes (21, 22, 23) :

Sont utilisées pour lire et écrire la réponse de l'hôte jusqu'à ce que le script rencontre la chaîne "Password :" et fournir le mot de passe correspondant.

```
19  tn = telnetlib.Telnet(host1,23,6)
20  tn.read_until(b"Username:")
21  tn.write(username.encode('ascii') + b"\n")
22  tn.read_until(b"Password:")
23  tn.write(password.encode('ascii') +b"\n")
```

Figure III 53 : lire et écrire la réponse de l'hôte

7-La ligne 24 :

Envoyé les commandes spécifiques à l'hôte via la connexion Telnet.

```
24    tn.write(command1.encode('ascii')+b"\n")
25    tn.write(command2.encode('ascii')+b"\n")
```

Figure III 54 : l'Envoi des commandes

8-Les Lignes (28,30,31,32) :

La ligne 28 :

Lit la réponse de l'hôte jusqu'à ce que le script rencontre la chaîne "]". Cela permet de récupérer la sortie des commandes exécutées sur l'hôte.

La ligne 30 :

Affichent la sortie de l'hôte sur la console.

La ligne 31 :

Enregistre la sortie de l'hôte dans le fichier "check.txt" en utilisant fp.write().

La ligne 32 :

Ferme la connexion Telnet avec l'hôte.

Ensuite :

Les étapes 8 à 15 sont répétées pour chaque hôte (host2, host3, etc.) avec les commandes spécifiques correspondantes.

Enfin :

Les lignes fp.close() et tn.close() ferment respectivement le fichier "check.txt" et toutes les connexions Telnet restantes.

III.9.8.1.6 Notre résultat de l'implémentation sur notre topologie approximative de Relizane :

```
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2024-06-25 14:13:50.
<ASBR1>display isis peer

                    Peer information for ISIS(1)

  System Id     Interface          Circuit Id       State HoldTime Type     PRI
------------------------------------------------------------------------------
0010.0100.1007  GE0/0/0            0000000002       Up   28s      L2       --
0010.0100.1002  GE0/0/1            0000000002       Up   28s      L2       --

Total Peer(s): 2
<ASBR1>dis mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0             2.2.2.2            GigabitEthernet0/0/1
 7.7.7.7:0             7.7.7.7            GigabitEthernet0/0/0
 ------------------------------------------------------------------------------
 TOTAL: 2 Peer(s) Found.

<ASBR1>sys
Enter system view, return user view with Ctrl+Z.
[ASBR1]

Info: The max number of VTY users is 20, and the number
```

Figure III 55 : le résultat d'exécution pour ASBR1

```
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2024-06-25 14:13:51.
<ASG1>display isis peer

                    Peer information for ISIS(1)

  System Id     Interface          Circuit Id       State HoldTime Type     PRI
------------------------------------------------------------------------------
0010.0100.1003  GE0/0/0            0000000001       Up   29s      L2       --
0010.0100.1001  GE0/0/1            0000000002       Up   22s      L2       --
0010.0100.1015  GE0/0/2            0000000001       Up   28s      L2       --
0010.0100.1017  GE0/0/3            0000000002       Up   23s      L2       --

Total Peer(s): 4
<ASG1>dis mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 1.1.1.1:0             1.1.1.1            GigabitEthernet0/0/1
 3.3.3.3:0             3.3.3.3            GigabitEthernet0/0/0
 8.8.8.8:0             8.8.8.8            GigabitEthernet0/0/2
 9.9.9.9:0             9.9.9.9            GigabitEthernet0/0/3
 ------------------------------------------------------------------------------
 TOTAL: 4 Peer(s) Found.

<ASG1>dis bgp peer
```

Figure III 56 : le résultat d'exécution pour ASG1

```
<ASG1>dis bgp peer

 BGP local router ID : 192.168.3.1
 Local AS number : 100
 Total number of peers : 3                 Peers in established state : 2

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  5.5.5.5         4         100       75       77     0 01:12:57 Established       0
  8.8.8.8         4         100        0        0     0 01:49:17        Idle       0
  9.9.9.9         4         100       74       76     0 01:12:56 Established       0
<ASG1>sys
Enter system view, return user view with Ctrl+Z.
[ASG1]

Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2024-06-25 14:13:51.
<ASG2>display isis peer

                    Peer information for ISIS(1)

  System Id     Interface          Circuit Id       State HoldTime Type     PRI
------------------------------------------------------------------------------
0010.0100.1002  GE0/0/0            0000000001       Up   29s      L2       --
0010.0100.1005  GE0/0/1            0000000001       Up   22s      L2       --
0010.0100.1019  GE0/0/2            0000000001       Up   23s      L2       --

Total Peer(s): 3
<ASG2>dis mpls ldp peer
```

Figure III 57 : le résultat d'exécution pour ASG1

```
<ASG2>dis mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0             2.2.2.2            GigabitEthernet0/0/0
 4.4.4.4:0             4.4.4.4            GigabitEthernet0/0/2
 5.5.5.5:0             5.5.5.5            GigabitEthernet0/0/1
 ------------------------------------------------------------------------------
 TOTAL: 3 Peer(s) Found.

<ASG2>sys
Enter system view, return user view with Ctrl+Z.
[ASG2]

Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2024-06-25 14:13:52.
<ASG4>display isis peer

                       Peer information for ISIS(1)

  System Id     Interface          Circuit Id       State HoldTime Type     PRI
------------------------------------------------------------------------------
0010.0100.1003  GE0/0/0             0000000002       Up   23s      L2       --
0010.0100.1006  GE0/0/1             0000000004       Up   23s      L2       --
0010.0100.1020  GE0/0/3             0000000001       Up   27s      L2       --

Total Peer(s): 3
```

Figure III 58 : le résultat d'exécution pour ASG2

```
<ASG4>dis mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 3.3.3.3:0             3.3.3.3            GigabitEthernet0/0/0
 6.6.6.6:0             6.6.6.6            GigabitEthernet0/0/1
 11.11.11.11:0         11.11.11.11        GigabitEthernet0/0/3
 ------------------------------------------------------------------------------
 TOTAL: 3 Peer(s) Found.

<ASG4>dis bgp peer

 BGP local router ID : 192.168.4.2
 Local AS number : 100
 Total number of peers : 3              Peers in established state : 2

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  2.2.2.2         4         100       75       75     0 01:12:58 Established       0
  10.10.10.10     4         100        0        0     0 01:49:12     Connect       0
  11.11.11.11     4         100       74       76     0 01:12:57 Established       0
<ASG4>sys
Enter system view, return user view with Ctrl+Z.
[ASG4]

Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2024-06-25 14:13:53.
```

Figure III 59 : le résultat d'exécution pour ASG4

```
<ASG5>display isis peer

                       Peer information for ISIS(1)

  System Id     Interface          Circuit Id       State HoldTime Type     PRI
------------------------------------------------------------------------------
0010.0100.1024  Eth0/0/1           0000000001       Up   28s      L2       --
0010.0100.1007  GE0/0/0            0000000003       Up   27s      L2       --
0010.0100.1005  GE0/0/1            0000000002       Up   28s      L2       --
0010.0100.1022  GE0/0/3            0000000001       Up   23s      L2       --

Total Peer(s): 4
<ASG5>dis mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 5.5.5.5:0             5.5.5.5            GigabitEthernet0/0/1
 7.7.7.7:0             7.7.7.7            GigabitEthernet0/0/0
 12.12.12.12:0         12.12.12.12        Ethernet0/0/1
 14.14.14.14:0         14.14.14.14        GigabitEthernet0/0/3
 15.15.15.15:0         15.15.15.15        GigabitEthernet0/0/2
 ------------------------------------------------------------------------------
 TOTAL: 5 Peer(s) Found.

<ASG5>sys
Enter system view, return user view with Ctrl+Z.
[ASG5]
```

Figure III 60 : le résultat d'exécution pour ASG5

Les résultats d'exécution des figures de notre script de vérification de la santé des routeurs fournissent des informations claires sur l'état de chaque routeur. Ces informations sont essentielles pour notre étude finale et nous avons autorisé le script à accéder aux protocoles ISIS et BGP, ainsi qu'aux protocoles MPLS et LDP. Grâce à ces résultats, nous pouvons évaluer la santé de chaque routeur en termes de pairs ISIS et BGP, ainsi que de la configuration des protocoles MPLS et LDP.

III.9.8.1.7 Une version améliorer pour le script de la vérification de la santé précédant :

Dans cette version du script on a amélioré la version précédant d'après avoir suivons ses étapes :

- On a créé une fonction nommée « check_connectivity » pour gérer la vérification de la connectivité avec les routeurs et modifié le code pour utiliser cette fonction au lieu de répéter le code pour chaque routeur.
- On a ajouté une liste routers « with_issues » pour stocker les routeurs ayant des problèmes de connexion et on a utilisé un bloc try-except pour capturer les exceptions lors de la connexion à chaque routeur. Si une exception se produit, cela signifie qu'il y a un problème de connexion.
- On a aussi ajouté du code pour afficher les routeurs ayant des problèmes de connexion et ajusté le délai d'attente lors de la connexion à 10 secondes pour donner plus de temps à la connexion.
- Enfin, on a passé les paramètres nécessaires à la fonction check_connectivity, y compris la liste des adresses IP des routeurs, le nom d'utilisateur et le mot de passe.

```python
import telnetlib

def check_connectivity(hosts, username, password):
    routers_with_issues = []

    for host in hosts:
        try:
            tn = telnetlib.Telnet(host, 23, 10)  # Augmenter le délai d'attente à 10 secondes
            tn.read_until(b"Username:")
            tn.write(username.encode('ascii') + b"\n")
            tn.read_until(b"Password:")
            tn.write(password.encode('ascii') + b"\n")
            tn.close()

        except Exception as e:
            print(f"Erreur lors de la connexion à {host}: {e}")
            routers_with_issues.append(host)

    if routers_with_issues:
        print("Les routeurs suivants rencontrent des problèmes de connexion:")
        for router in routers_with_issues:
            print(router)
    else:
        print("Tous les routeurs sont accessibles.")
```

Figure III 61 : la version améliorer de script du la vérification de santé

```
24            print("Tous les routeurs sont accessibles.")
25
26    # Paramètres
27    hosts = [
28        "1.1.1.1",
29        "2.2.2.2",
30        "3.3.3.3",
31        "5.5.5.5",
32        "6.6.6.6",
33        "7.7.7.7"
34    ]
35    username = "amina"  # Le nom d'utilisateur
36    password = "123"
37
38    # Vérification de la connectivité avec les routeurs
39    check_connectivity(hosts, username, password)
```

Figure III 62 : La suite de la version améliorer

Dans cette version du script, après avoir lu la sortie jusqu'au prompt du routeur, nous vérifions si la chaîne % Error ou % Error est présente dans la sortie. Si une de ces chaînes est trouvée, cela indique qu'il y a une erreur dans le routeur.

Si une erreur est détectée dans la sortie ou si une exception est levée lors de la connexion Telnet à un routeur, le routeur est ajouté à la liste routers avec ssues.

Après l'exécution du script, il affiche les adresses IP ou les noms d'hôte des routeurs qui rencontrent des problèmes de connexion ou qui ont renvoyé des erreurs. Si tous les routeurs sont accessibles et ne renvoient pas d'erreurs, le script affiche "Tous les routeurs sont accessibles et ne renvoient pas d'erreurs."

III.9.8.1.8 Notre résultat de l'implémentation de la version améliorée de script sur notre topologie approximative de Relizane :

Pour pouvoir exécuter le script et détecter les routeurs ayant des problèmes :

- Nous avons d'abord arrêté le routeur ASG5 avec l'adresse : 6.6.6.6 dans notre topologie. Cela nous permettra de vérifier si le script est capable de détecter ce problème et de signaler l'état défectueux du routeur ASG5.

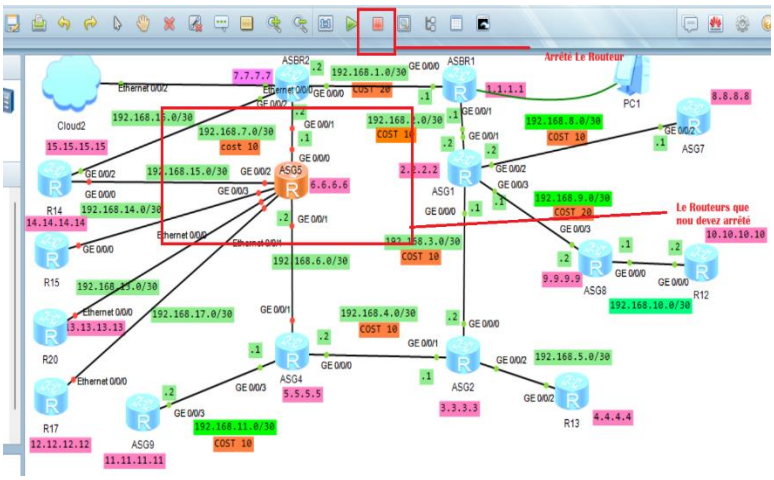


Figure III 63 : Arrêter le routeur de la topologie de Relizane

- Ensuite, ont exécutée le programme pour avoir le résultat comme est montrer dans la figure ses dessous :

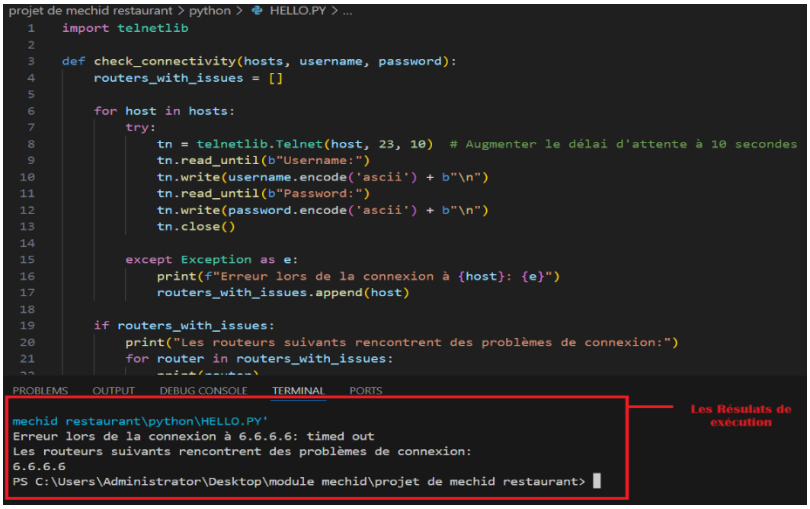


Figure III 64 : le résultat de l'exécution

III.9.8.2 Troubleshooting :

III.9.8.2.1 Définition :

Le troubleshooting, ou dépannage, est le processus d'identification, de diagnostic, et de résolution des problèmes qui surviennent dans un réseau de télécommunication. Il s'agit d'une approche méthodique pour isoler et corriger les anomalies afin de restaurer le service normal le plus rapidement possible.

III.9.8.2.2 Les Besoin de dépannage :

Les réseaux de télécommunication peuvent rencontrer divers types de problèmes tels que des pannes matérielles, des erreurs de configuration, des problèmes de routage, des congestions, etc. Sans une méthode efficace de troubleshooting, ces problèmes peuvent entraîner des interruptions prolongées, affectant les utilisateurs et les services.

III.9.8.2.3 Pourquoi les en utilise le dépannage dans notre réseau :

- **Réduction du temps d'arrêt :** Un dépannage efficace permet de réduire le temps nécessaire pour restaurer le service normal.
- **Documentation des problèmes :** Fournit des données précieuses pour éviter les problèmes similaires à l'avenir.
- **Optimisation continue :** Le troubleshooting permet d'identifier les points faibles du réseau, ouvrant la voie à des améliorations continues.

III.9.8.2.4 Le script de troubleshooting :

Ce programme de dépannage automatiser la connexion Telnet à plusieurs hôtes et exécuter des commandes spécifiques sur chacun d'eux. Cela peut aider à collecter rapidement des informations à partir des hôtes cibles et à diagnostiquer les problèmes.

```
1  import telnetlib
2  import datetime
3  import time
4
5  now = datetime.datetime.now()
6  host1 = "1.1.1.1"
7  host2 = "2.2.2.2"
8  host3 = "3.3.3.3"
9  host4 = "5.5.5.5"
10 host6 = "6.6.6.6"
11 host7 = "7.7.7.7"
12 username = "amina" # the username
13 password = "123"
14 command1 = "dis int des | include " + input("la description")
15 command2 = "Display ip routing-table vpn-instance" + input("vrf")
16 command3 = "dis bgp peer"
17 fin = "sys"
18 fp = open("check.txt","w")
19 tn = telnetlib.Telnet(host1,23,6)
20 tn.read_until(b"Username:")
21 tn.write(username.encode('ascii') + b"\n")
22 tn.read_until(b"Password:")
23 tn.write(password.encode('ascii') +b"\n")
24 tn.write(command1.encode('ascii')+b"\n")
25 tn.write(b"\n")
26 time.sleep(3)
27 tn.write(command2.encode('ascii')+b"\n")
28 tn.write(command3.encode('ascii')+b"\n")
29 tn.write(fin.encode('ascii')+b"\n")
```

Figure III 65 : les commandes utilisées pour troubleshooting

III.9.8.2.5 Explication de script :

En utilisant ce programme dans une approche de dépannage, nous pouvons automatiser la collecte d'informations à partir des hôtes cibles, ce qui peut nous faire gagner du temps et nous aider à identifier rapidement les problèmes potentiels. Nous pouvons ensuite analyser les sorties enregistrées dans le fichier pour trouver des indices sur les problèmes observés.

1- La ligne 14 :

Elle utilise la fonction input () pour demander à l'utilisateur une description spécifique

2- Les autres lignes de codes sont identiques avec le script de check health (ils sont expliqués précédemment).

III.9.8.2.6 Notre résultat de l'implémentation sur notre topologie approximative de Relizane :

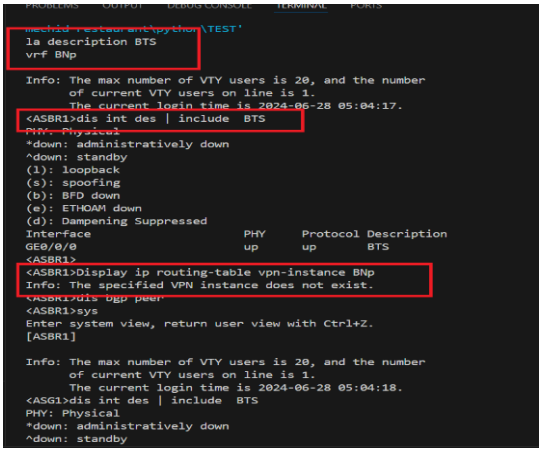


Figure III 66 : le résultat de troubleshooting pour ASBR1

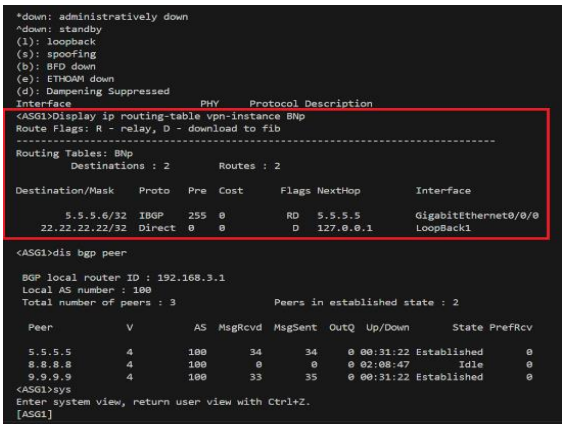


Figure III 67 : le résultat de troubleshooting ASG1

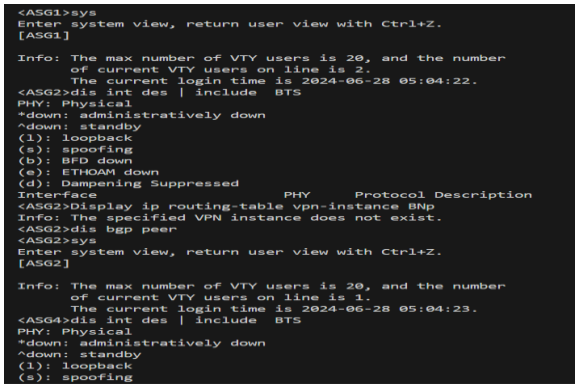


Figure III 68 : le résultat de troubleshooting

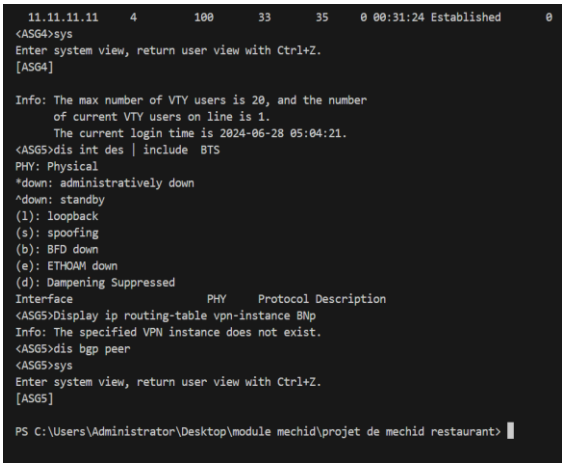


Figure III 69 : le résultat de troubleshooting pour ASG4

III.10 Conclusion

L'objectif de ce chapitre était de développer et d'intégrer des algorithmes de vérification de santé et de dépannage pour automatiser la détection et la résolution des problèmes dans notre réseau IP RAN. Ces algorithmes visaient à améliorer la qualité de service (QoS) en vérifiant les configurations de notre architecture, telles que « MPLS LDP » et « BGP Peer », ainsi qu'en accédant à des interfaces et des VRF spécifiques pour évaluer leur état, et en détectant les erreurs potentielles.

Nous avons effectué des tests de connectivité, affiché les configurations des interfaces et des différents protocoles, puis interprété les résultats obtenus. Cela nous a permis de démontrer comment l'algorithme à accéder aux réseaux et exécute des commandes pour l'analyse de l'ensemble des hôtes du réseau simultanément et faire de dépannage sur des interfaces et des VRF a notre choix.

Conclusion générale

L'objectif principal de ce mémoire est de créer et de mettre en œuvre un algorithme pour améliorer la qualité de service (QoS) dans le réseau IP/RAN de ATM MOBILIS, wilaya de Rélizane. Pour cela, nous utiliserons une méthode stricte avec des tests et des expériences sur notre simulation.

Notre participation active à ce projet nous a permis d'approfondir nos connaissances dans les réseaux de télécommunications. Nous avons étudié les bases des réseaux, leurs composants, et des technologies avancées comme le MPLS. Nous avons aussi exploré l'évolution et l'architecture des réseaux mobiles, en mettant l'accent sur le Réseau d'Accès Radio (RAN), le routage IP et les protocoles de routage essentiels.

Nous avons simulé un réseau IP/RAN avec 19 routeurs, en utilisant des configurations telles que ISIS pour la transmission des paquets, MPLS pour accélérer la transmission, et VRF pour le partage de charge. Nous avons assuré le bon fonctionnement de notre réseau via des tests de connectivité et des vérifications manuelles. En parallèle, nous avons étudié le réseau réel de Rélizane sur la plateforme iMaster NCE pour comprendre les configurations et le trafic de données, et appris à ajouter de nouveaux sous-réseaux.

Enfin, nous avons développé des algorithmes Python pour surveiller la santé du réseau et effectuer le dépannage. Nous les avons connectés à notre topologie simulée sur ENSP via des interfaces réseau de test virtuelles créées sur notre PC, en utilisant le protocole Telnet pour accéder aux routeurs à travers un cloud. Notre programme a exécuté des commandes sur tous les routeurs en même temps, signalant rapidement les divergences de configuration. L'algorithme de vérification de santé a automatisé efficacement les interventions manuelles, détectant rapidement les anomalies. Par exemple, lorsque certaines interfaces de routeurs étaient inaccessibles, le script affichait un message indiquant le problème. Ensuite, avec l'algorithme de dépannage, nous avons accédé spécifiquement aux interfaces des mêmes routeurs présentant des problèmes et avons constaté que ces interfaces étaient désactivées.

Les résultats démontreront l'efficacité de notre solution pour améliore la QOS En assurant une surveillance constante et une détection rapide des problèmes, le script contribue à maintenir.

Un Réseau stable et performant. Les anomalies sont détectées et corrigées avant qu'elles n'affectent les utilisateurs finaux. De plus, l'automatisation des processus de surveillance et de dépannage augmente l'efficacité opérationnelle, réduit les temps d'arrêt et améliore la résilience du réseau.

À l'avenir, nous souhaitons enrichir notre algorithme en intégrant de nouvelles commandes et en développant des algorithmes d'intelligence artificielle capables de réacheminer automatiquement le trafic en cas d'interruption de lien, nous pourrions encore améliorer la résilience et l'efficacité opérationnelle du réseau de Mobilis. Ces développements permettront une gestion proactive et une continuité de service optimale, renforçant ainsi la QoS.

Référence

[1] Meraihi Yacine, « support de cours Les réseaux sans fils, » Faculté de technologie, UNIVERSITE M'HAMED BOUGARA-BOUMERDE, 2016/2017.

[2] https://www.editions-eni.fr/livre/les-reseaux-avec-cisco-connaissances-approfondies-sur-les-reseaux-4e-edition-9782409026690/presentation-des-reseaux . Visité le 20 Mars 2024.

[3] Mr. IBEGHOUCHENE Amar, « Mémoire fin d'étude en réseaux et télécommunication » Université Mouloud Mammeri, TIZI OUZOU, 2011/2012.

[4] HAMMAMI Nadjet, Siham. « Mémoire de fin d'études de Master II en Réseaux et télécommunication, » UNIVERSITE M'HAMED BOUGARA-BOUMERDE, 2020/2021.

[5] Les faisceaux hatriziens sur le site : https://www.google.com/url?sa=i&url=http%3A%2F%2Fwww.stechies.net%2Ffhh%20tml&psig=AOvVaw0PEFfuyFxz1H5SB3cjWwpD&ust=1719528430901000&sourc%20e=images&cd=vfe&opi=89978449&ved=0CBEQjRxqFwoTCJjpqOesoYDFQAAAAAdAAAAABAJ.

Visité le 22 Mars 2024.

[6] le protocole de routage interne sur le site : https://sce1988627bc0958d.jimcontent.com/download/version/1417112964/module/8092788084/name/d227-ch01.pdf Visité le 22 Mars 2024.

[7] https://inetdoc.developpez.com/tutoriels/technologie-ethernet ,Visité le 18 Mars 2024

[8] https://www.futura-sciences.com/tech/definitions/electronique-cable-coaxial-4388/cable coixiale, visité le 30 février 2024.

[9] Https://www.digitalcorner-wavestone.com/2020/01/de-la-2g-a-la-4g, Visité le 18 Mars 2024.

[10] DERRIDJ Kaci, Anis GHERRAS Noureddine : « Mémoire de Fin d'Etudes De MASTER ACADEMIQUE » Télécommunication et Réseaux, 2016.

[11] Https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-routing/, Visité le 29 Mars 2024.

[12] NOUALI. Katia. MOUMOU. Dyhia, « Mémoire fin étude master 2 électronique, » UNIVERSITE MOULOUD MAMMERIE, 2017 /2018.

[13] Https://www.digitalcorner-wavestone.com/2020/01/de-la-2g-a-la-4g/ , visité le : 23 Mars 2024.

[14] https://cisco.ofppt.info/ccna1/course/module6/6.2.2.4/6.2.2.4.html , visité le : 23 Mars 2024.

[15] Https://www.guru99.com/fr/routing-protocol-types.html, visité le : 1 Mai 2024.

[16] BETARZI. Imen, « Mémoire de fin d'études de Master II en Réseaux et télécommunication,» UNIVERSITE M'HAMED BOUGARA-BOUMERDE

[17] https://www.formip.com/pages/blog/ebgp-interdomain-routing visité le : 2 Mai 2024

[18] Mr. GRIM NACIM, Mr. IDIR KAMAL. « Protocoles de routage dynamique à vecteur de distance, » (Doctoral dissertation, Université Mouloud Mammeri TIZI OUZOU, 2011.

[19] Https://fr.linkedin.com/pulse/les-protocole-de-routage-stephane-bergeron, visité le 2 Mai 2024.

[20] H. N. «Mémoire de fin d'études de Master II en Réseaux et télécommunication,» UNIVERSITE M'HAMED BOUGARA-BOUMERDES, 2020/2021.

[21]Https://sce1988627bc0958d.jimcontent.com/download/version/1417112964/module/8092788084/name/d227-ch01.pdf , visité le: 8 Mai 2024.

[22] Https://community.fs.com/article/what-is-ospf-and-why-do-we-need-it.html visité le: 8 Mai 2024.

[23] https://www.it-connect.fr/cours/introduction-au-routage-ospf/ , visité le : 15 Mai 2024

[24] https://info.support.huawei.com/info-finder/encyclopedia/en/IS-IS.html , visité le : 15 Mai 2024.

[25] https://info.support.huawei.com/info-finder/encyclopedia/en/IS-IS.html, , visité le : 17 Mai 2024.

[26] https://www.juniper.net/documentation/fr/fr/software/junos/is-is/topics/concept/is-is-routing-overview.html , visité le : 17 Mai 2024.

[27] https://community.cisco.com/t5/networking-knowledge-base/ospf-and-is-is-differences/ta-p/3126940 , visité le : 20Mai 2024.

[28] https://www.manager-go.com/management-de-la-qualite/qualite-de-service.htm visité le : 20 juin 2024.

ANNEXE

I. Création de Nouvelle Topologie Réseaux sur ENSP

Pour simuler la topologie réseaux de Relizane dans ENSP, nous avons suivi ces étapes :

1. Accès au menu Principal de ENSP

Nous avons d'abord accédé au menu principal pour créer une nouvelle topologie.

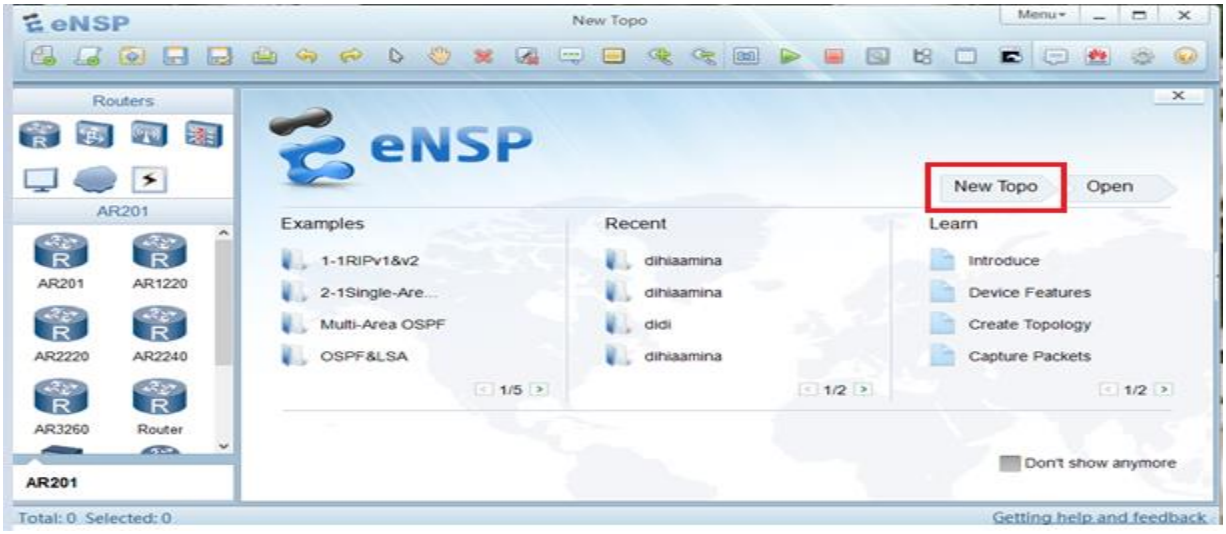


Figure a : Menu principale de ENSP.

2. Accès aux zones de Travail de ENSP

Ensuite, nous avons accédé à la zone de travail, comprenant : La zone principale pour créer et configurer la topologie, La palette des dispositifs à gauche (routeurs, commutateurs, etc.) La barre d'outils avec des options pour démarrer/arrêter des dispositifs

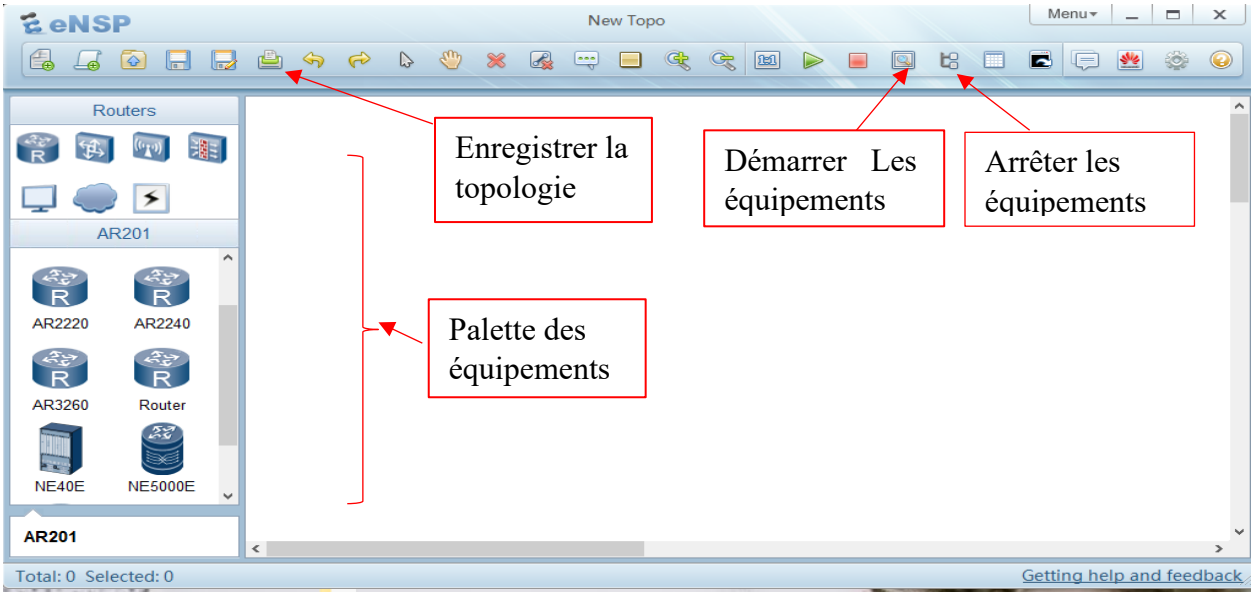


Figure b : La zone de travail de ENSP

3. Intégration des Routeurs :

Nous avons choisi les routeurs pour commencer à les configurer en les intégrant dans la zone de travail d'eNSP, comme le montre la figure ci-dessous.

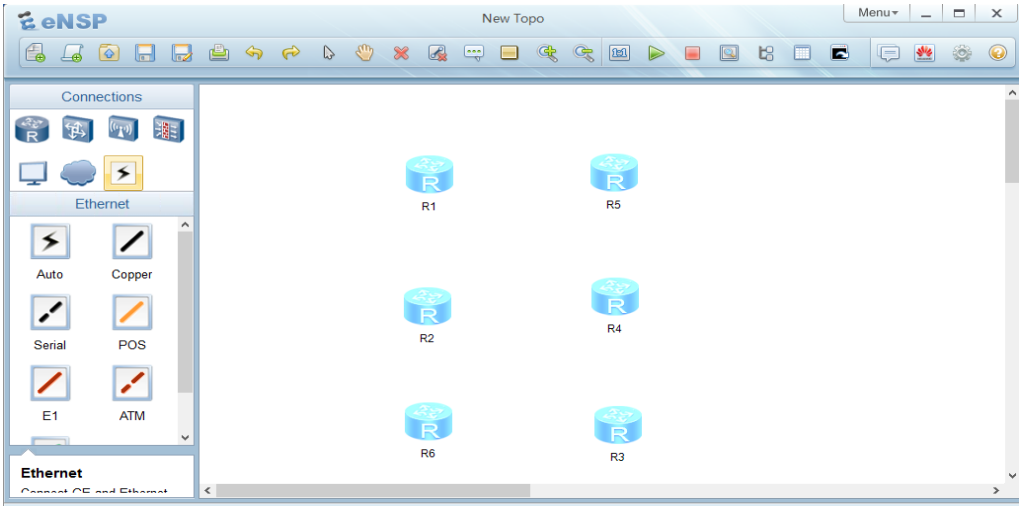


Figure c : Intégration des Routeurs

4. Interconnexion des Routeurs

Pour interconnecter les routeurs, nous avons sélectionné un câble spécifique (comme un câble cuivre), cliqué sur un dispositif, puis sur un autre pour établir la connexion, en spécifiant les interfaces nécessaires (comme Ethernet), comme le montre la figure b.

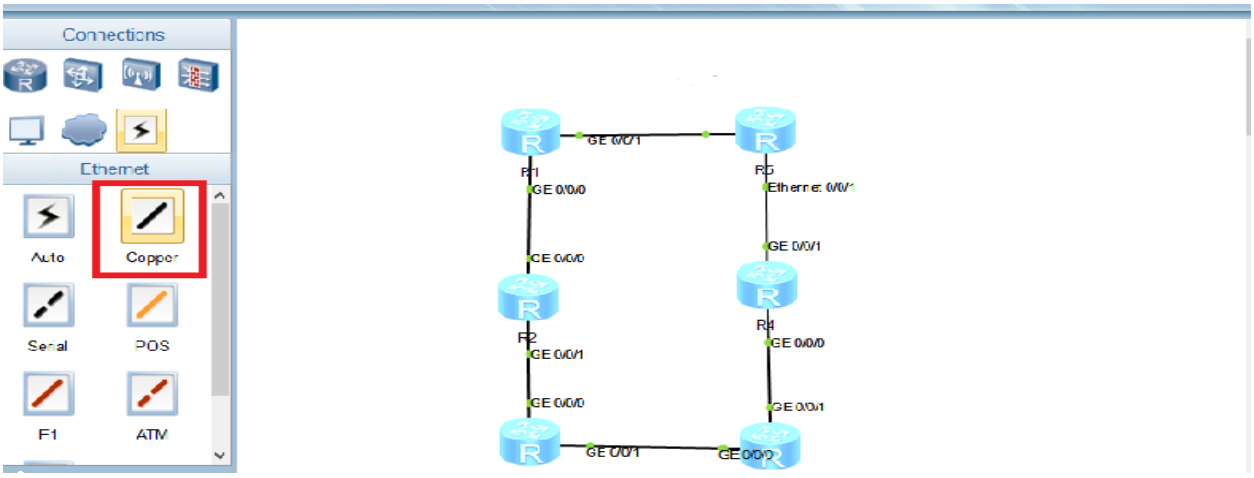


Figure d : Interconnexion des routeurs.