REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université M'Hamed BOUGARA –BOUMERDES

FACULTE DE TECHNOLOGIE

Département Ingénierie des Systèmes Electriques

Mémoire de Master

Présenté par :

M^elle NASRI Rafika

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

THEME

Etude et intégration du protocole MPLS dans le réseau core network au niveau de l'opérateur Djezzy

Soutenus le 18/06/2023 devant le jury composé de :

Mr RAHMOUNE	Fayçal	Prof	Université de Boumerdès	Président
Mme BELKACEM	Samia	MCA	Université de Boumerdès	Encadreur
Mr RIAL	Ahmed	Ing	Optimum Télécom Algérie S.P.A	Co-Encadreur
Mme HOCINE	Faiza	MCB	Université de Boumerdès	Examinateur

2022/2023

Remerciements

Notre parfaite gratitude et nos remerciements sont tout d'abord à Allah, le clément et le miséricordieux, qui nous a donné la force, le courage et la volonté pour mener à bien ce modeste travail.

C'est avec une profonde reconnaissance et une considération particulière, que nous remercions notre encadreur Dr BELKACEM Samia de nous avoir accordé sa confiance pour réaliser ce travail, ainsi que pour son aide et son suivi permanent. On la remercie également pour sa patience, ses encouragements et ses précieux conseils.

Un grand merci pour notre co-encadreur Mr Riyal Ahmed, qui nous a donné cette opportunité de travailler au sein de l'entreprise DJEZZY, ainsi que les moyens qu'il a mis à notre disposition. On le remercie également pour sa patience, ses encouragements et ses précieux conseils.

Nos vifs remerciements s'adressent également à tous les membres du jury qui nous ont honorés par leurs présences et d'avoir acceptés d'examiner et d'évaluer notre modeste travail.

Nos sincères remerciements et notre gratitude pour l'ensemble des enseignants du département Ingénierie des Systèmes Electriques, dont nous avons eu l'honneur d'être parmi ses étudiants

A tous ceux qui nous ont aidés de près ou de loin pour la réalisation de ce projet de fin d'études, qu'ils trouvent ici, l'expression de nos sincères remerciements.

Un grand merci également à tous ceux qui ont partagés avec nous, nos années d'études, « étudiants et amis ».

Merci à tous nos proches, nos familles, de nous avoir encouragés tout au long de nos études et ce travail.

Nous réservons cette dernière ligne pour nos chers parents, nous leurs dirons tout simplement merci pour votre «amour qui nous a aidé tout au long de ces années à franchir des caps bien difficiles».

Dédicace

C'est avec une grande émotion que nous dédions ce modeste travail à des personnes très chères à mes yeux :

Mes chers parents, dont les mots ne sauraient exprimer l'immense et le profond respect, reconnaissance et gratitude que nous leurs témoignons, pour leurs précieux soutiens et leurs patiences, ainsi que pour leurs réconforts et leurs sacrifices qui nous ont permis

D'atteindre cette étape dans notre vie.

« Que Dieu les gardes et les protèges ».

Mes très chères sœurs, et mon adorable frère, à qui me souhaitons, pleins de succès et de réussites.

Mon cher fiancé, pour son amour, son assistance morale et ses conseils.

Toutes mes familles et surtout mes très chères grands-parents que Dieu les protèges.

Tous ceux qui ont participés de près ou de loin à la réalisation de ce modeste travail.

Tous mes enseignants tout au long de nos études.

RAFIKA

ملخص

MPLS (تبديل ملصقات متعدد البروتوكولات) هو بروتوكول مصمم لتحسين وتسريع حركة مرور الشبكة الآمنة. في هذا المشروع ، نعطي المفاهيم الأساسية لشبكات IP وبروتوكولات التوجيه الثابتة والديناميكية المختلفة (RIP، OSPF) المقدمة. كما تمت مناقشة مبدأ تقنية MPLS وتطبيقاتها المختلفة والبروتوكولات النشطة التي استخدمناها في هذا المشروع.

الهدف من مشروعنا هو فصل حركة المرور بين كيانين وإعادة توجيه حركة المرور. وهذا يشمل ضمان حركة المرور بين موقع تيزي وزو والجزائر العاصمة وبين موقع البليدة والمدية مع فصل حركة تيزي والجزائر مع البليدة والمدية. تم تنفيذ بروتوكولات OSPF و BGP على محاكي GNS3. أكدت النتائج التي تم الحصول عليها الأداء الجيد للشبكة أثناء الإرسال للحزم المرسلة.

كلمات مفتاحية : شبكات IP ، تقنية MPLS ، التوجيه ، OSPF، BGP، GNS3.

Abstract

MPLS (Multi-Protocol Label Switching) is a protocol designed to optimise and accelerate secure network traffic. In this project, we cover the basic concepts of IP networks and the various static and dynamic routing protocols (RIP, OSPF) that are presented. The principle of MPLS technology, its various applications, and the active protocols we have used in this project are also discussed.

The objective of our project is to separate the traffic between two entities and to forward the traffic. This involves ensuring traffic between the Tizi-Ouzou site and Algiers and between the Blida site and Médéa with a separation of Tizi and Algiers traffic with Blida and Médéa. The OSPF and BGP protocols were implemented on the GNS3 simulator. The results obtained confirmed the good performance of the network during transmission for the packets transmitted.

Keywords : IP networks, MPLS technology, Routing, OSPF, BGP, GNS3.

Résumé

MPLS (Multi-Protocol Label Switching) est un protocole conçu pour optimiser, accélérer et sécuriser le trafic du réseau. Dans ce projet, on a abordé les concepts de base des réseaux IP et les différents protocoles de routage statiques et dynamiques (RIP, OSPF) qui sont présentés. Le principe de la technologie MPLS, ses différentes applications, et les protocoles actifs que nous avons utilisés dans ce Projet sont expliqués aussi.

L'objectif de notre projet est de séparer le trafic entre deux entités et forwarding le trafic. Il s'agit d'assurer le trafic entre le site de Tizi-Ouzou et Alger et entre site Blida et Médéa avec une séparation de trafic Tizi et Alger avec Blida et Médéa. Une implémentation du protocole OSPF et BGP sur le simulateur GNS3 est effectuée. Les résultats obtenus ont confirmé la bonne performance du réseau en cours de transmission pour les paquets transmis.

Mots clés : Réseaux IP, Technologie MPLS, Routage, OSPF, BGP, GNS3.

Table des matières

Liste des abréviations

A

ATM: Asynchronous Transfer Mode

ARP: Address Resolution Protocol

B

BGP: Border Gateway Protocol

C

CAN: Campus Area Network

Cos: Classe of Service

F

FEC: Forwarding Equivalent Class

FAI : fournisseurs d'accès Internet

FIB: Forwarding Information Base

G

GNS3: Graphical Network Simulator

H

HDLC: High-level Data Link Control

I

ICMP: Internet Control Message Protocol

IGP: Interior Gateway Protocol

IP : Internet Protocol

L

LAN: Local Area Network

LSR: Label Switch Router

LER : Label Edge Router

LDP : Label Distribution Protocol

L'ISO : Organisation Internationale de Normalisation

l'OSPF: Open Shortest Path First

LFIB: Label Forwarding Information Base

LIB: Label Information Base

LSP: Label Switched Path

M

MAN: Metropolitan Area Network

MPLS: Multi-Protocol Label Switching

MPLS – TE: Trafic Engineering

N

NFS: Network File System

O

OSI: en anglais Open System Interconnexion

P

PoS: Packet over Sonet/SDH

Q

QOS: Quality of service

R

RLE: Réseau Local d'Entreprise

RPC: Remote Procedure Call

RSVP TE: Resource Reservation Protocol Traffic Engineering

RD: Route Ditinguisher

RT: Route Target

S

SNMP: Simple Network Management Protocol

SCTP: Stream control transmission Protocol

SQL: Structured Query Language

T

TAN: Tiny Area Network

TLS: Transport Layer Secutrity

TCP: Transport Control Protocol

TE : l'ingénierie de trafic

U

UDP: User Datagram Protocol

V

VRF: Virtual Routing and Forwarding

VPN: Virtual Private Network

W

WAN: Wide Area Network

Liste *des figures*

Liste des tableaux

Introduction générale

Aujourd'hui, Internet est largement utilisé dans le monde et est plus orienté métier. Les organismes offrant la connexion Internet sont intéressés par la tarification où les clients payent pour les ressources qu'ils consomment. (William, 2009)

Les réseaux IP représentent désormais une part importante des infrastructures de télécommunications, transportant de nombreux services avec leurs contraintes de disponibilité. Des incidents, tels que des pannes matérielles, la perte de liens de transmission, des bugs logiciels ou des opérations de maintenance, réduisent leur disponibilité. Des solutions permettent cependant de réduire les impacts de ces incidents sur le trafic existent. (NATAF, 2007).

Au fur et à mesure que les réseaux s'étendent, les routeurs sont très occupés à travailler avec des tables de routage basées sur les préfixes IP. En outre, les routeurs décident du chemin le plus court entre la source et la destination. Destination, et lorsque tout le trafic est envoyé par le chemin le plus court, cela peut créer une congestion dans le réseau. Pour y remédier, de nouveaux mécanismes sont nécessaires pour améliorer les réseaux. (DELMI, 2020)

Avec l'arrivée de la technologie MPLS et les modèles de gestion de la qualité de service, une nouvelle approche est considérée (MPLS pour l'augmentation des performances des équipements réseaux, les notions de trafic engineering et les VPN et la gestion de qualité de service pour le traitement de la congestion, la classification des trafics et la garantie de service). (HAMAMI, 2021)

Ce principe de commutation intégré au routage IP vise à améliorer la vitesse et la portée du réseau IP réduisant de manière significative les exigences de traitement des paquets. L'intérêt des MPLS est aussi pour les différents services proposés. Le rôle du MPLS est d'acheminer et de commuter les paquets à travers les réseaux de nouvelle génération pour répondre aux besoins des utilisateurs du réseau et des services.

L'objectif de notre projet est d'implémenter un réseau IP/MPLS avec GNS3 dans le réseau DJEZZY.

Notre mémoire est divisé en trois chapitres comme suit :

Dans le premier chapitre, des généralités sur les réseaux informatiques et de ses différents composants, classés et traités par IP, modèle OSI et TCP/IP sont présentés.

Le deuxième chapitre est consacré à la présentation des réseaux MPLS, de leur architecture fonctionnelle et de leurs applications, s'intitule LDP label expansion Protocol et BGP Border Gateway Protocol, pour présenter les routeurs virtuels (VRF) et les réseaux privés virtuels (VPN).

Le chapitre troisième contient les résultats de la production de modèles standard à l'aide du dispositif GNS3, ainsi que des tests de validation de configuration globale.

Notre mémoire s'est terminé par une conclusion générale, avec perspectives.

Chapitre 1 : Généralités sur les réseaux IP

1. Introduction

Dans ce chapitre, nous allons donner des généralités sur le réseau internet, et d'étudier les réseaux LAN et WAN. Par la suite, nous discutons le modèle OSI avec l'explication de ses sept couches, le fonctionnement des réseaux IP, l'adressage dans les réseaux IP, et enfin les protocoles de routage IP.

2. Réseau Internet

Internet est le plus grand réseau mondial. Il connecte des millions d'utilisateurs à travers le monde. Les paquets sont routés de la source à la destination à travers plusieurs sous-réseaux connectés sur un support physique de différentes capacités. (BENISSE, 2009)

Un réseau informatique, est un ensemble d'équipements matériels et logiciels interconnectés les uns avec les autres dans le but de partager des ressources (données). Ces équipements peuvent être éloignés ou rapprochés. Suivant l'éloignement entre ces équipements, on distingue les réseaux suivants : (BOUDOUR, 2017)

– Le réseau LAN (Local Area Network) à l'intérieur d'un immeuble, ou d'une superficie inférieure à 10 Kilomètres.

– Le réseau MAN (Metropolitan Area Network) circoncis à une ville, comme par exemple, le réseau du métro.

– Le réseau WAN (Wide Area Network) a au moins la dimension d'un pays, et ils englobent souvent la planète entière.

– Le réseau CAN (Campus Area Network) pour les campus universitaires (plusieurs immeubles, mais une surface de terrain limitée).

– Le réseau TAN (Tiny Area Network) est une expression inventée par un journaliste américain, Cheryl Currid, pour désigner les réseaux domestiques, à la maison.

– Le réseau RLE (Réseau Local d'Entreprise).

2.1. Définition des réseaux LAN et WAN

Dans cette section nous donnons la définition des réseaux LAN et WAN.

2.1.1 Réseau WAN

Un WAN, qui signifie Wide Area Network, est un réseau de communication de données qui fonctionne au-delà d'un réseau local LAN. Ce sont dans Les WAN qu'on retrouve les fournisseurs de services ou les opérateurs. C'est eux qui relient les différentes entreprises, les services externes, ou bien directement des utilisateurs distants. Les WAN comportent différents types de trafic tels que la voix, les données et la vidéo. Il existe plusieurs raisons pour lesquelles les WAN sont nécessaires pour une entreprise. Par exemple, les salariés d'une entreprise situés en province dans un petit office doivent pouvoir communiquer avec leur siège social. Ou même, pourquoi pas, communiquer avec d'autres organisations. On peut aussi retrouver des utilisateurs qui se déplacent dans plusieurs offices de l'entreprise, et qui ont besoin d'accéder à l'ensemble du réseau. Comme il n'est pas possible de connecter des périphériques dans le monde entier de la même manière que dans un environnement LAN, par exemple avec des câbles, et bien, différentes technologies existent pour pouvoir faire cela. Par exemple, Internet est utilisé de plus en plus, comme une alternative peu couteuse pour faire du WAN d'entreprise avec certaines applications (Soulages, 2023). Il est constitué d'un ensemble de réseaux d'opérateurs interconnectés entre eux (réseaux de réseaux) (MEGRI, 2015), comme le montre la figure (1.1).

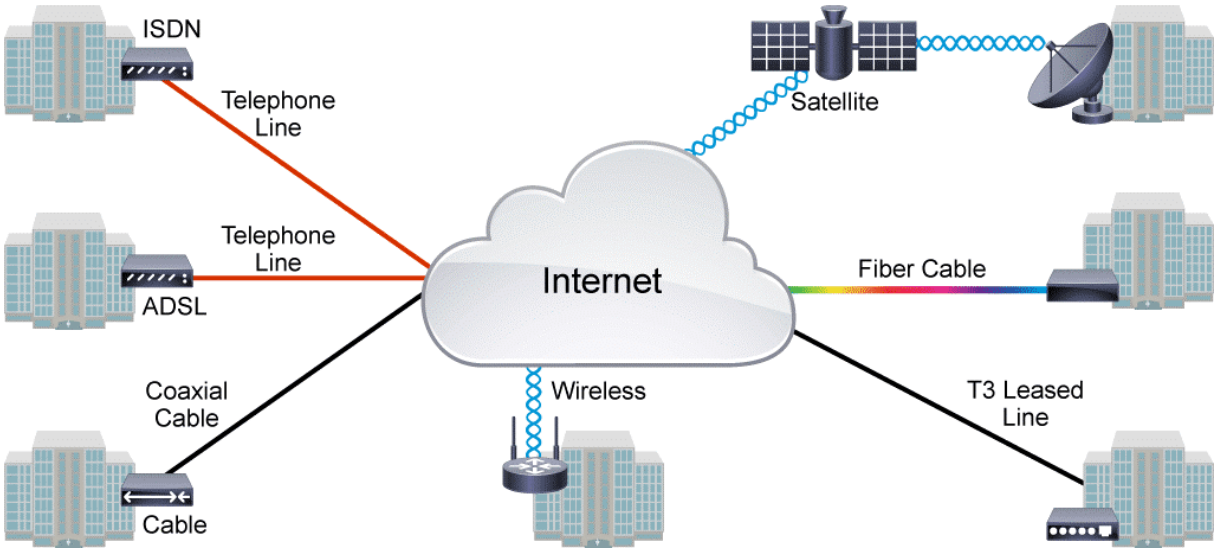

Figure 1. 1 : WAN (Wide Area Network) (Soulages, 2023)

2.1.2 Réseau LAN

Ce sont des réseaux de taille plus ou moins modeste, complexes, qui permettent l'échange de données informatiques et le partage de ressources (données, disques durs, périphériques divers, etc.). L'étendue géographique des réseaux locaux ne dépasse pas 10 km (ex. : pour un immeuble ou un campus). Le débit, ou la vitesse de communication, varie de quelques Mbps à 100 Mbps. Le nombre de stations ne dépasse généralement pas 1 000. (ATROUNE, 2021)

Englobe un ensemble de techniques allant de celles nécessaires à la communication de plusieurs machines appartenant à une même organisation et reliés entre eux dans une petite aire géographique, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet) (MEGRI, 2015), comme l'indique la figure (1.2).

Figure 1. 2 : Réseau local LAN

3. Le modèle OSI

Le modèle OSI (en anglais Open System Interconnexion), est un modèle de communication entre ordinateur proposé par l'ISO (Organisation Internationale de Normalisation) afin d'établir des normes de communication entre les ordinateurs du réseau. La norme complète, de référence ISO7498 est globalement intitulée « Modèle Basique de référence pour l'interconnexion des systèmes ouvertes (OSI) ». Il est devisé en sept couches numérotées comme le montre la Figure (1.3). (ATROUNE, 2021)

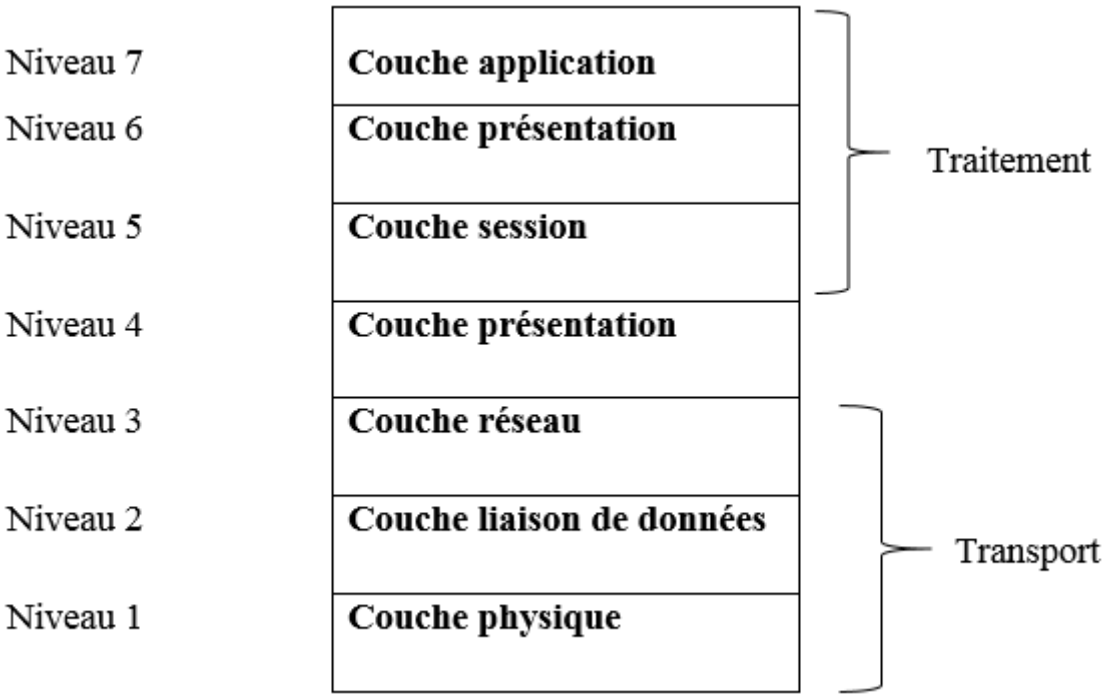

Figure 1. 3 : Les différentes couches du modèle OSI [BERKANI, 2018]

3.1 Couche1 : La couche physique

Décrit des caractéristiques électriques (niveaux de tension, signaux…), mécaniques (forme des connecteurs, caractéristiques des câbles…), physiques (distances maximales de transmission…) et logiques (débit, codage…) de connexion du poste au réseau. Elle fait en sorte que physiquement, l'émission d'un bit à 1 (bit « brut » en bande de base ou signal analogique…) ne soit pas considérée à la réception comme un bit 0. Elle gère le type de transmission (synchrone/asynchrone) et procède éventuellement à la modulation/démodulation du signal. L'unité d'échange à ce niveau est le bit. Comme La paire torsadée, les connecteurs RJ45 et la carte réseau Ethernet travaillent en couche 1 OSI. (ZOUAOUI ,2012)

3.1.1 Les supports de transmission

Les supports permettant de transporter des données sous forme de signaux peuvent être classés en deux types (TEBINA, 2020) :

Supports avec un guide physique : paire téléphonique classique, paire téléphonique torsadée, câble coaxial en télévision, fibre optique,

Supports sans guide physique : faisceaux hertziens, faisceaux lasers…etc.

3.1.2 Topologie

La topologie d'un réseau constitue l'organisation ou la relation des périphériques réseaux et les interconnexions existantes entre eux comprennent deux types de topologies différentes utilisées pour décrire les réseaux, la topologie physique et la topologie logique (électrique). (ATROUNE, 2021)

3.1.2.1 La Topologie physique

La topologie physique c'est la configuration spatiale, visible, du réseau. Elle décrit la mise en pratique du réseau logique (câblage etc.) (Santos, 2013) ; Il existe quatre types : En bus, en étoile, en anneau et en étoile répartie. Ces éléments de base sont combinés pour former des réseaux complexes. (GADOUM, 2012)

3.1.2.1.1 Topologie en bus

Le bus, est un segment central où circulent les informations, s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinatrice peut les récupérer. Une seule station peut émettre à la fois. En, bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre. L'avantage du bus est qu'une station en panne ne perturbe pas le reste du réseau. Elle est, de plus, très facile à mettre en place. Par contre, en cas de rupture du bus, le réseau devient inutilisable. Notons également que le signal n'est jamais régénéré, ce qui limite la longueur des câbles. (BELAID, 2011)

Et pour communiquer entre eux, l'appareil envoie un message de diffusion sur le fil que tous les autres appareils voient, mais seul le destinataire prévu accepte et traite réellement le message. (ATROUNE, 2021) comme le montre la figure ci-dessous :

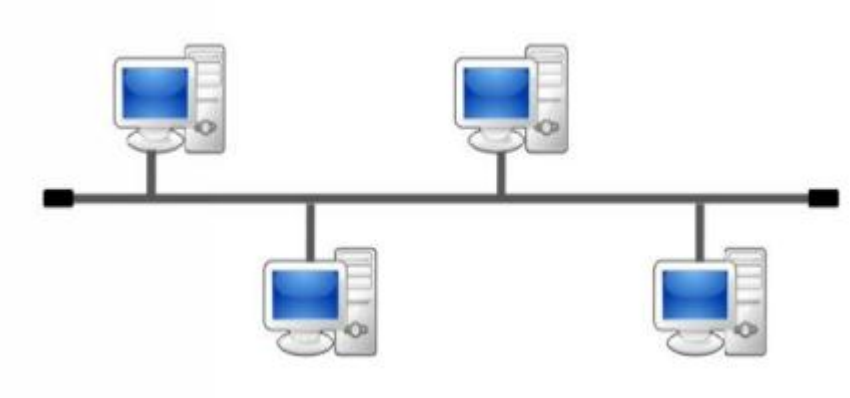

Figure 1. 4 : Topologie en bus

3.1.2.1.2 La topologie en étoile

C'est la topologie la plus courante, notamment avec les réseaux Ethernet RJ45. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet vers le concentrateur, celui-ci envoie les données à toutes les autres machines (hub) ou uniquement au destinataire (Switch). Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Par contre, il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est anéanti. De plus, le débit pratique est moins bon que pour les autres topologies. (BELAID, 2011)

Tous les ordinateurs sont reliés à l'aide d'un câble à un concentrateur. Si l'un des câbles se rompt seul l'ordinateur relié à ce câble en est affecté, toutefois, si le concentrateur tombe en panne, l'ensemble des ordinateurs ne peut plus communiquer. (SAFI, 2010), comme le montre la figure (1.5).

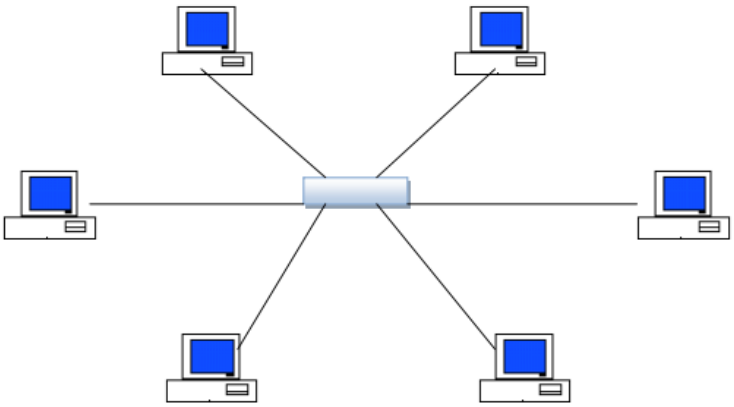

Figure 1. 5 : Topologie en étoile

3.1.2.1.3 La topologie en étoile répartie

C'est une méthode dérivée de la topologie en étoile. On peut relier plusieurs concentrateurs sur un seul câble. (GADOUM, 2012) les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur. Comme le montre la figure (1.6).

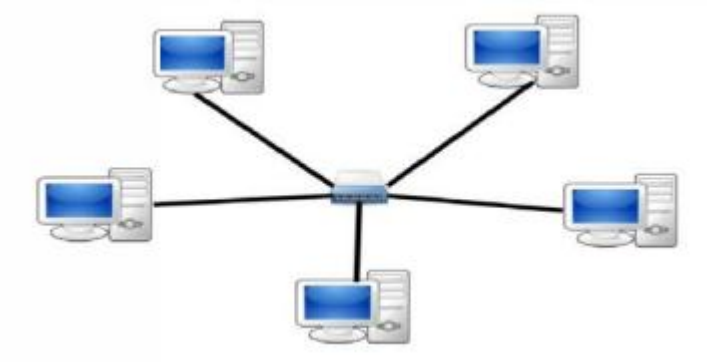

Figure 1. 6 : Topologie en étoile répartie

3.1.2.1.4 La topologie en anneau

Dans cette topologie, les machines sont reliées en anneau unidirectionnel ou bidirectionnel formant une succession de liaisons point à point circulaire. Tous les coupleurs doivent être en état de fonctionnement sinon tout le réseau est bloqué. L'utilisation d'un double anneau augmente la sécurité. (GADOUM, 2012)

Les ordinateurs sont reliés à un seul câble en anneau, les signaux transitent dans une seule direction, chaque ordinateur joue le rôle de répéteur, régénérant le signal (SAFI, 2010), comme l'indique la Figure (1.7).

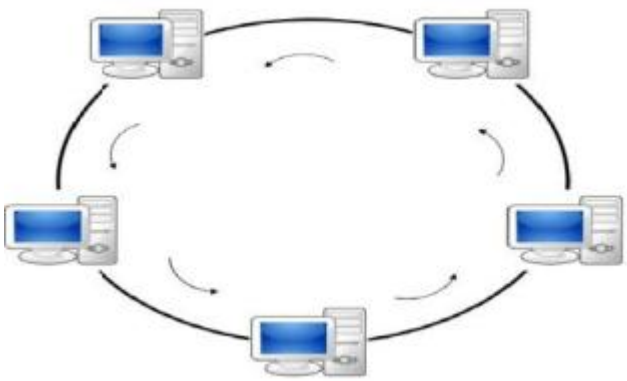

Figure 1. 7 : Topologie en anneau

3.1.2.2 La Topologie logique

Une topologie logique est la structure logique d'une topologie physique, c'est à dire que la topologie logique nous renseigne sur le mode de communication et l'échange des messages dans le réseau. (BERKANI, 2018)

3.2 Couche 2 : la couche liaison de données

Cette couche reçoit les données brutes de la couche physique, elle les organise en trames, elle détecte les erreurs, elle retransmet les trames erronées, elle gère les acquittements (ACK) qui indiquent si les données sont bien transmises Une fois ceci fait, elle transmet ses données formatées à la couche réseau. Cette couche travaille aussi avec la couche qui la précède à savoir la couche physique (couche 1). L'unité de données est la trame (data frame) et les informations qui circulent sur le réseau sont donc structurées en trames, Elle transforme les paquets fournis par la couche réseau (couche 3) en trame. La carte réseau (en partie – adresse MAC), le protocole HDLC (High-level Data Link Control) travaillent au niveau 2. (ZOUAOUI, 2012)

3.3 Couche 3 : la couche réseau

Son rôle est chargé de l'acheminement des paquets de données qui transitent sur l'ensemble du réseau, elle doit utiliser des informations d'adressage. Ces paquets seront sans doute amenés à traverser des nœuds intermédiaires, un routage est donc nécessaire (c'est-à-dire que la couche réseau doit déterminer le meilleur chemin de communication c'est le routage). Si un nœud est surchargé ou hors service, le contrôle de flux doit éviter les congestions en régulant la charge du trafic ou en déroutant les paquets vers un autre nœud. L'unité de données est le paquet. La couche réseau assure également un service de traduction des adresses logiques (adresse IP) en adresses physiques (adresse MAC). (ZOUAOUI, 2012)

3.3.1 Adresse IP

Sur internet, les ordinateurs communiquent entre eux grâce au protocole TCP/IP qui utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8bits),on le note donc sous la forme xxx.xxx.xxx.xxx, ou chaque xxx représente un entier de 0 à 255.Ces numéros servent aux ordinateurs du réseau pour se reconnaitre, aussi il ne doit pas exister deux ordinateurs sur le réseau ayant la même adresse IP. Par exemple, 194.153.205.26 est une adresse TCP/IP donnée sous une forme technique. C'est l'IANA (Internet Assigned Numbers Agency) qui est chargée d'attribuer ces numéros. (BELAID, 2011)

3.3.1.1 Les classes

Il existe cinq classes d'adresses IP, chaque classe est identifiée par une lettre allant de A à E. L'adresse IP type utilisée : w. x. y. z. Ces différentes classes ont chacune leurs spécificités en termes de répartition du nombre d'octet servant à identifier le réseau ou les ordinateurs sont connectés à ce réseau (BERKANI, 2018). Sur le tableau (1.1) on montre les classe d'adresse IP.

Tableau 1. 1 : Les classes d'adresses IP

Classes	Adresses IP	Id réseau	Id d'hôte	Minimum	Maximum
A	W.X.Y.Z	W	X.Y.Z	0	126
B	W.X.Y.Z	W.X	Y.Z	127	191
C	W.X.Y.Z	W.X.Y	Z	192	223
D	W.X.Y.Z	Adresses IP Particulières	-	224	239
E	W.X.Y.Z	Adresses IP Particulières	-	240	254

3.3.1.2 Les types d'adresses IP

Dans cette section nous allons décrire les différents types d'adresse IP :

3.3.1.2.1 Adresses publiques

Ces adresses sont utilisées dans les réseaux externes ou internes. Elles sont routables dans les différents routeurs dans le réseau, ainsi, les fournisseurs d'accès à internet les attribuent à leurs clients.

3.3.1.2.2 Adresses privées

Une classe privée est une portée d'adresses IP d'une certaine classe publique (A, B, C), mais réservée pour un usage particulier par des standards ou conventions. Le tableau ci- dessous montre les plages d'adresses privées : (BOUDERRA, 2021). Sur le tableau (1.2) on montre les adresses IP privées.

Tableau 1. 2 : Adresses IP privées en classes A, B et C.

Classe	Adresses privées	Nombre maximal de machines
A	De 10.0.0.0 à 255.255 (masque/8)	(256*256*256)-2=16 777 214
B	De 172.16.0.0 à 172.31.255.255 (masque/12)	(15*256*256)-2=1 048 574
C	De 192.168.0.0 à 192.168.255256=65534.255 (masque/16)	(256*256)=65534

3.3.1.3 Adresse particulière

Le protocole IP définit un certain nombre d'adresses particulières. Dans cette section nous allons donner un aperçu sur les adresses particulières :

3.3.1.3.1 L'adresse zéro

En IP v4, l'adresse zéro (0.0.0.0) signifie "tout le réseau". Il s'agit en fait d'une adresse réseau. En IP v6, l'adresse zéro (::) indique une adresse indéfinie, c'est à dire une absence d'adresse. (Sébastien, 2023)

3.3.1.3.2 L'adresse de bouclage (loopback)

Une adresse de bouclage (loopback en anglais) est une adresse utilisée par une interface pour s'envoyer un message à elle-même. Elle peut, par exemple, être utilisée lors de tests.

En IP v4, il s'agit de l'adresse 127.0.0.1. En IP v6, il s'agit de l'adresse ::1.

3.3.2 Routage IP

Le routage est un processus qui permet de sélectionner des chemins dans un réseau pour transmettre des données (paquets) d'un routeur (réseau) à un autre grâce à des adresses IP depuis un expéditeur jusqu'à un ou plusieurs destinataires. Dans les premiers réseaux, les tables de routage étaient statiques et donc maintenues à jour manuellement. Avec l'évolutivité et l'augmentation de la taille des réseaux, Des protocoles de routage dynamiques échangent les informations de routage d'autres systèmes du réseau afin de mettre à jour les tables de routage. (BERKANI, 2018)

3.3.3 Les protocoles ARP, ICMP, SNMP

Dans cette section nous décrivons les protocoles ARP, ICMP, SNMP (GADOUM, 2012):

3.3.3.1 Les protocoles ARP (Address Resolution Protocol)

L'objectif d'ARP est de résoudre une adresse physique par l'intermédiaire de l'adresse IP correspondante d'un host distant. Il permet d'obtenir l'adresse physique (MAC) d'une machine connaissant son adresse IP (logique).

3.3.3.2 Les protocoles ICMP (Internet Control Message Protocol)

Le protocole ICMP (Internet Control Message Protocol) permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des Datagrammes en erreurs.

3.3.3.3 Les protocoles *SNMP*

SNMP (Simple Network Management Protocol) est un protocole de couche d'application utilisé pour la surveillance et la gestion des périphériques réseau sur les réseaux TCP/IP.

Il fournit une interface unifiée pour mettre en œuvre une gestion unifiée sur différents appareils (tels que switch réseau, routeur, pare-feu, imprimantes, etc.) de différents fournisseurs, ce qui simplifie considérablement la gestion du réseau. Nous expliquerons dans cet article leurs principes de fonctionnement et comment configurer le protocole SNMP. (Howard, 2023)

3.4 Couche 4 : La couche transport

Dans la couche de transport, nous pouvons trouver toutes les règles de fonctionnement. Cela peut assurer la transparence du réseau vis-à-vis des couches supérieures. Elle traite principalement l'adressage, l'établissement des connexions ainsi que la fiabilité du transport. (ZAIDI, 2022)

3.4.1 Protocole TCP (Transport Control Protocol)

Le protocole TCP est un protocole de la couche transport. TCP est l'acronyme de « Transmission Control Protocol ». Il est décrit dans la RFC 793 (Postel, 1981). Le protocole TCP permet un transport fiable et en ordre des données de bout en bout grâce à son mécanisme d'acquittement et de l'utilisation de numéros de séquence. TCP est un protocole orienté connexion, les applications communiquent alors entre elles comme si elles étaient physiquement connectées. Avant que les deux applications puissent s'échanger des informations, elles doivent établir une connexion entre elles ; cet établissement est connu sous le nom de « Three-way handshake ». Cette phase d'établissement permet aux deux applications d'échanger et d'initialiser plusieurs paramètres du protocole. Une fois la connexion établie, les deux applications peuvent commencer à envoyer leurs données. TCP fournit un service de contrôle de flux afin de s'assurer que le transmetteur n'envoie pas à un taux que le récepteur ne peut pas supporter et cause ainsi un dépassement de mémoire au niveau du tampon. Pour assurer

ce contrôle de flux, TCP utilise une variable nommée « Receive Window » qui indique au transmetteur l'espace disponible dans le tampon du récepteur. (ZIED, 2010)

3.4.2 Protocole UDP (User Datagram Protocol)

Le protocole UDP (User Datagram Protocol) est un protocole simple et moins fiable pour la transmission paquets ou datagrammes. Ce protocole est non orienté connexion et transmet les données sans l'établissement de connexion. Le protocole UDP est utilisé dans les applications en temps réel comme les jeux informatiques, streaming et les vidéoconférences donc il est utilisé dans le cas où le retard de paquet est plus sérieux que la perte de paquet (BOUDERRA, 2021). Il fournit juste les fonctions de base pour la transmission. Comme le montre la figure ci-dessous (BERKANI, 2018):

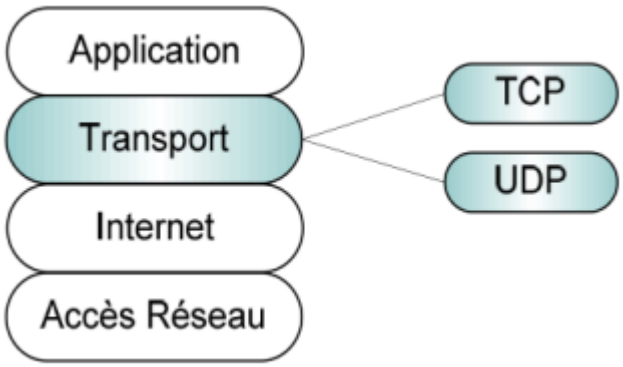

Figure1.5: TCP et UDP dans le modèle TCP/IP (BERKANI, 2018))

3.4.3 Protocole SCTP

Le SCTP (Stream control transmission Protocol) est un protocole de transport fiable de la suite des protocoles Internet permettant la transmission de messages de télécommunication à travers des réseaux IP. Il réunit plusieurs caractéristiques des protocoles TCP (orienté connexion) et UDP (sans connexion) servant également au transfert des données, et comprend notamment des mécanismes de gestion des congestions (Congestion Control) et d'amélioration de la tolérance aux erreurs lors de l'envoi des paquets. Grâce à sa grande flexibilité, le SCTP est également utilisé dans d'autres applications (par exemple pour la gestion et l'administration de pools de serveurs). (Know, 2023)

3.5 Couche 5 : La couche session

La couche session est la première couche orientée traitement. Elle permet l'ouverture et la fermeture d'une session de travail entre systèmes distants et assure la synchronisation du

dialogue. C'est à ce niveau que l'on décide également du mode de transmission (simplex, half-duplex, full-duplex). La synchronisation du dialogue se fait au moyen de points de contrôle ainsi, lorsqu'un problème se produit, seules les données émises après le dernier point de Contrôle correctement reçu seront réexpédiées. Le langage de requête SQL (Structured Query Language), le système de partage de fichiers NFS (Network File System) TLS (Transport Layer Secutrity), RPC (Remote Procedure Call) … travaillent au niveau 5. (ZOUAOUI, 2012)

3.6 Couche 6 : La couche présentation

Cette couche permet de coder les données en un langage connu par la couche supérieure. (BERKANI, 2018)

3.7 Couche 7 : La couche application

Elle s'agit de la source et la destination de toutes les informations à transporter, la couche application comprend toutes les applications éprouvant le besoin de communiquer par le réseau : transfert de fichiers messagerie électronique, gestionnaire de bases de données, etc. (ZAIDI, 2022).

4.Les protocoles de routage

Le but de tous les protocoles de routage est de maintenir la table de routage des différents routeurs. Pour cette fin, le protocole diffuse des informations de routage vers d'autres systèmes du réseau afin que les modifications de la table de routage sont tenues en compte pour la mise à jour des différentes tables de routage. Les protocoles de routage sont conçus pour améliorer la vitesse de routage, pas besoin de configurer manuellement toutes les routes, économisant ainsi du temps sur chaque routeur, améliorez la stabilité du réseau en sélectionnant à chaque fois le meilleur itinéraire. Les protocoles de routage peuvent être divisés en deux catégories (Belgherbi, 2020):

– Les protocoles à vecteur de distance.

– Les protocoles à état de liens.

4.1. Les protocoles à vecteur de distance

Le protocole de routage à vecteur de distance utilise un algorithme de routage qui ajoute les distances pour trouver le meilleur itinéraire (Bellman-Ford). Habituellement, chaque routeur

envoie sa table de routage entière à ses voisins. Ils sont très sensibles aux boucles de routage. Ce type de méthode compte le nombre de sauts entre deux endroits, et en fonction de ce nombre de sauts, il choisira l'itinéraire le plus court. Nous citerons RIP et IGRP.

• RIP : Routing Information Protocol, qui est un protocole à vecteur de distance, c'est-à-dire la distance de communication entre chaque routeur et les autres routeurs (le nombre de sauts entre eux). Par conséquent, lorsque le routeur reçoit l'un de ces messages, il augmentera cette distance de un et transmettra le message au routeur directement accessible. Par conséquent, le routeur peut maintenir le meilleur itinéraire du message de cette manière en stockant l'adresse du routeur suivant dans la table de routage, minimisant ainsi le nombre de sauts vers le réseau.

• IGRP : (Interior Gatway Routing Protocol) est un protocole propriétaire développé par Cisco Systems, qui est plus robuste et moins restrictif que RIP. EIGRP (Extended Interior Gateway Routing Protocol) est une version avancée de IGRP.

4.2. Les protocoles à état de liens

Le protocole de routage d'état de liaison utilise un algorithme plus efficace (Dijkstra ou chemin le plus court en premier). Le routeur collecte tous les coûts de liaison de son point de vue et construit une arborescence de tous les chemins. Intégrez ensuite le meilleur itinéraire dans la table de routage. L'avantage de ces algorithmes est qu'ils fournissent une convergence rapide sans boucle ni multiacheminement. Nous citerons OSPF.

• OSPF : (Open Shortest Path First), Il est plus efficace que RIP, il le remplace donc progressivement. Contrairement à RIP, ce protocole n'envoie pas le nombre de sauts entre eux, aux routeurs voisins, mais leur envoie l'état de la liaison. De cette manière, chaque routeur peut mapper l'état du réseau, afin de pouvoir choisir à tout moment la route la plus appropriée pour le message. De plus, ce protocole peut empêcher les routeurs intermédiaires d'augmenter le nombre de sauts, réduisant ainsi la génération d'informations, obtenant ainsi une meilleure bande passante disponible que RIP.

4.3. Protocoles de routage externe EGP

Les protocoles EGP sont conçus pour gérer le routage externe d'un réseau (entre systèmes Autonomes). Avec des objectifs de convergence et d'optimisation de nouvelles routes injectées

dans les tables de routage du réseau. Le protocole EGP utilisés de nos jours, c'est le protocole de routage BGPv4 (Border Gateway Protocol). (BERKANI, 2018)

- BGPv4 : permet d'échanger des informations de routage entre les AS. Lorsqu'un routeur BGP reçoit des mises à jour en provenance de plusieurs systèmes autonomes décrivant différents chemins vers une même destination, il choisit alors le nœud et le système autonome qui doivent traversés pour atteindre la destination

- BGP : (Border Gateway Protocol) Le protocole BGP est utilisé par les Fournisseur d'Accès Internet (FAI) pour communiquer entre eux ou avec des sociétés appartiennant aux différents AS. BGP est constitué de deux parties :

- Les sessions de routage entre deux routeurs au sein du même système autonome sont appelées sessions iBGP (intenal BGP).

- Les sessions de routage entre système autonome différents sont appelées sessions eBGP (external BGP).

Conclusion

Dans ce chapitre, nous avons donné des généralités sur les réseaux d'internet IP et le modèle OSI ainsi que les limitations de cette technologie.

Dans le chapitre suivant, nous allons aborder d'une manière détaillée l'évolution d'IP vers la technologie MPLS.

Chapitre 2 : Etude de la technologie MPLS

1. Introduction

MPLS est une technique réseau en cours de normalisation à l'IETF (Internet Engineering Task Force). Son rôle principal est de combiner les concepts de routage IP niveau 3 et les mécanismes de la commutation niveau 2 implémentées dans ATM (Asynchronous Transmission Mode) ou Frame Relay. Au début, il avait pour but de commuter plus rapidement le trafic IP en ajoutant des labels aux paquets afin d'accélérer les traitements dans les commutateurs. Aujourd'hui, avec l'arrivée des commutateurs capables de traiter les en-têtes IP, MPLS ne réside plus dans sa rapidité d'effectuer les traitements. Il est désormais utilisé comme un outil d'ingénierie de trafic dans les réseaux dorsaux IP. (RAVOAVAHY, 2013)

Dans ce chapitre, nous allons voir l'évolution de l'adresse IP vers la technologie MPLS, les principes de fonctionnement de MPLS, les labels, et protocole de distribution de labels LDP, les applications de la technologie MPLS, structure fonctionnelles du MPLS, enfin nous donnons des aperçus sur les routeurs virtuels (VRF).

2. L'évolution d'IP vers MPLS

Dans le cadre du routage traditionnel, chaque routeur maintient un algorithme de routage de couche 3. Lorsqu'un paquet de données traverse le réseau, chaque routeur décide indépendamment d'envoyer le paquet de données. Le routeur utilise les informations contenues dans l'en-tête de paquet et les informations de routage obtenues à partir de la table de routage construite, pour sélectionner un "Next-Hop" avant d'envoyer le paquet. Dans un réseau IP, ce processus consiste à faire correspondre l'adresse IP de destination stockée dans l'en-tête de chaque paquet avec le chemin le plus spécifique obtenue à partir de la table de routage IP. Dans un environnement traditionnel sans connexion, cette activité se reproduit à chaque nœud le long du chemin de bout en bout. L'analyse et la classification des en-têtes de couche 3 peuvent être gourmandes en ressources processeur.

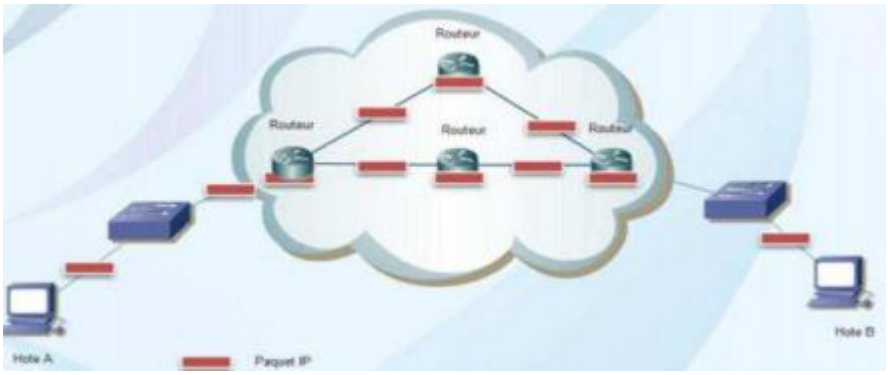

Figure 2. 1 : Modèle de routage IP (MOKHTARI, 2021)

Par conséquent, il est essentiel de trouver une méthode de transmission de paquets plus efficace. La technologie MPLS est une technologie qui détermine à l'avance le meilleur chemin à travers le réseau. Ensuite, lorsque le paquet de données est envoyé dans le réseau MPLS, le dispositif à la périphérie du réseau utilise les informations de l'en-tête de couche 3 pour attribuer le paquet de données à l'un des chemins prédéterminés. Cette affectation est utilisée pour ajouter des balises (également appelées étiquette, référence ou libellé). Lorsque le paquet de données traverse le réseau, le label sera envoyé avec le paquet de données. Le routeur dans le chemin du paquet utilise les informations du label pour déterminer le routeur de saut suivant.

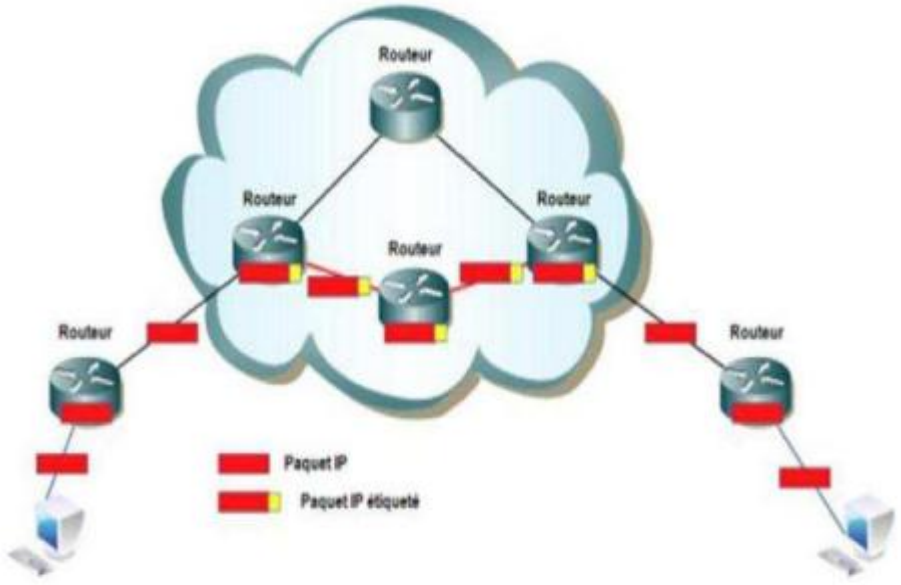

Figure 2. 2 : Routage IP où MPLS est appliqué (ZERROUKI, 2019)

L'insertion de label se fait au dispositif à la périphérie du réseau, parce que le processus d'analyse et de classification de l'en-tête de la troisième couche se produit uniquement aux points d'entrée et de sortie de l'environnement MPLS. (ZERROUKI, 2019)

2.1 Présentation des réseaux MPLS

L'objectif principal du groupe de projet MPLS est de normaliser une technologie de base qu'intègre le paradigme de la transmission par commutation de labels avec le routage de couche réseau. Cette technologie (la commutation de labels) est destinée à améliorer le ratio coût/performance du routage de couche réseau, à accroître l'évolutivité de la couche réseau et à fournir une plus grande souplesse dans la remise des (nouveaux) services de routage, tout en permettant l'ajout de nouveaux services de routage sans modification du paradigme de transmission. L'architecture MPLS repose sur des mécanismes de commutation de labels associant la couche 2 du modèle OSI (commutation) avec la couche 3 du modèle OSI (routage). De plus, la commutation réalisée au niveau de la couche 2 est indépendante de la technologie utilisée. En effet, le transport des données au sein d'une architecture MPLS peut être par exemple effectué à l'aide de paquets ou de cellules à travers des réseaux Frame Relay ou des réseaux ATM. Cette commutation, indépendante des technologies utilisées est possible grâce à l'insertion dans les unités de données (cellules ou paquets) d'un label. Ce petit label de taille fixe indique à chaque nœud MPLS la manière dont ils doivent traiter et transmettre les données. L'originalité de MPLS par rapport aux technologies WAN déjà existantes est la possibilité pour un paquet de transporter une pile de labels et la manière dont ceux-ci sont attribués.

L'implémentation des piles de labels permet une meilleure gestion de l'ingénierie de trafic et des VPN notamment en offrant la possibilité de rediriger rapidement un paquet vers un autre chemin lorsqu'une liaison est défaillante. Les réseaux actuels utilisent l'analyse des en-têtes de couche 3 du modèle OSI pour prendre des décisions sur la transmission des paquets. MPLS quant à lui repose sur deux composants distincts pour prendre ses décisions : le plan de contrôle (control plane) et le plan des données. Le plan des données permet de transmettre des paquets de données en fonction des labels que ceux-ci transportent en se basant sur une base de données de transmission de labels maintenue par un commutateur de labels. Le plan de contrôle quant à lui créé et maintient les informations de transmission des labels destinées à des groupes de commutateurs de labels. Du point de vue, chaque nœud MPLS est un routeur IP qui doit par conséquent utiliser des protocoles de routage IP afin d'échanger ses tables de routage IP avec les routeurs voisins. (William, 2009). La figure suivante, indique clairement l'emplacement du protocole MPLS dans le modèle OSI:

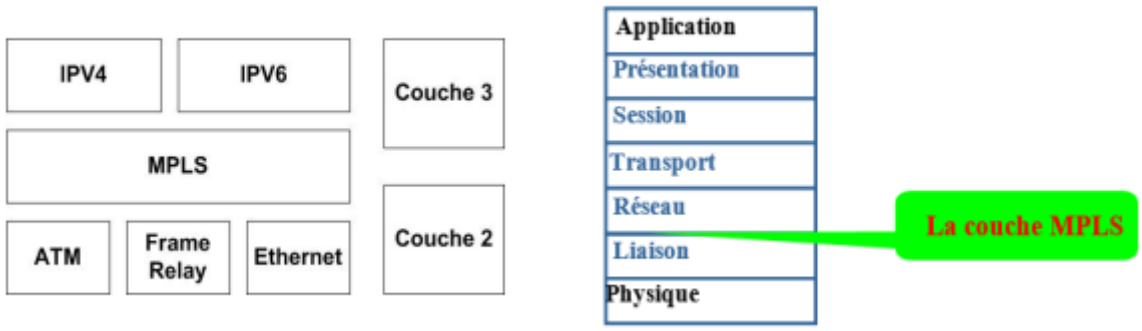

Figure 2. 3 : La couche MPLS. ((BELAID, 2018)

2.2 Les composants de l'architecture MPLS

L'architecture du réseau MPLS utilise des LSR (Label Switch Router) et des LSP (Label Switched Path), et FEC (Forwarding Equivalent Class). (RAMAHAROBANDRO, 2013)

2.2.1. Label Switching Router (LSR)

Le LSR est un équipement de cœur du réseau MPLS de type routeur, ou commutateur qui effectue la commutation sur les labels et qui participe à la mise en place du chemin par lequel les paquets sont acheminés. Lorsque le routeur LSR reçoit un paquet labélisé, il le permute avec un autre label de sortie et expédie le nouveau paquet labélisé sur l'interface de sortie appropriée. Le routeur LSR, peut jouer plusieurs rôles à savoir : (RAMAHAROBANDRO, 2013)

1) L'échange d'informations de routage ;
2) L'échange des labels ;
3) L'acheminement des paquets.

2.2.2. Label Switched Path (LSP)

Est un chemin commuté d'entrée-sortie construit par les nœuds MPLS pour transmettre les paquets encapsulés MPLS d'une FEC particulière à l'aide du mécanisme de transfert d'échange d'étiquettes. Il est similaire au concept de canaux virtuels dans un contexte ATM.4

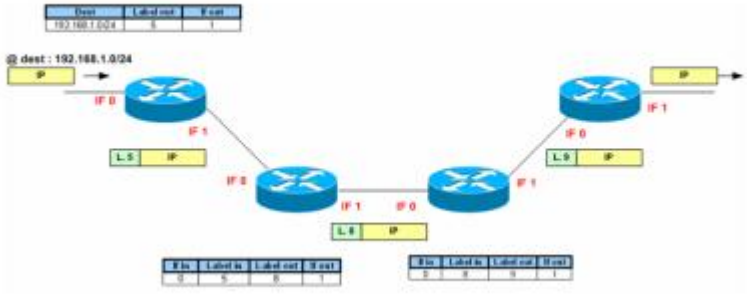

Figure 2. 4 : Principe de fonctionnement du MPLS.4

Dans le mariage du routage IP classique et de la commutation de paquets est né un nouveau système appelé commutation de labels. Un label, est un petit paquet de données qui va, dans l'architecture de base, s'intercaler entre l'entête de niveau 2 et l'entête de niveau 3. La Fig. 2.3 illustre le mécanisme. Dans cette figure nous que les labels sont déjà enregistrés dans chacun des routeurs. Nous aborderons le mécanisme qui conduit à cette topologie dans la suite. Soit un paquet IP arrivant à destination de l'adresse réseau 192.168.1.0/24. Le routeur d'entrée va utiliser l'adresse de destination pour retrouver le label à associer au paquet. Il voit par exemple ici que cette adresse de destination est associée au label #5 et qu'il doit être recopié sur l'interface1. Ce routeur va donc ajouter le label après l'entête de niveau 3. Ce label sera conservé tout au long de la traversée du réseau à commutation de labels. A chaque intermédiaire, le label va être échangé par les routeurs intermédiaires. C'est ce que l'on appelé le Label Swapping. Pour le deuxième routeur, celui-ci va utiliser le label entrant comme index dans la table de commutation, et modifier le label par celui de sortie spécifié dans sa table. Lors de l'arrivée du paquet au dernier routeur, celui-ci va retirer le label et transmettre le paquet à sa couche de niveau 3 qui va se charger du routage "classique" du paquet. Ces opérations d'ajout et suppression des labels sont primordiales, car elles vont conditionner l'interopérabilité des réseaux à commutation de labels avec les autres types de réseaux basés sur IP. (Bouziane, 2021)

2.2.3. Forwarding Equivalent Class (FEC)

Est un ensemble de paquets traités de manière identique par un routeur, c'est-à-dire transmis par la même interface avec les mêmes sauts et étiquettes, et affectés à la même classe de service. Lorsqu'un paquet entre dans le domaine MPLS au niveau du nœud d'entrée, il est mappé dans une FEC. Le mappage peut être effectué en fonction d'un certain nombre de facteurs, à savoir le préfixe d'adresse, la paire d'adresses source / destination ou l'interface

d'entrée. Au moment actuel, il existe trois éléments FEC définis, un préfixe d'adresse, un identifiant de routeur et un flux (port source / de destination et adresses IP). Un groupe de paquets IP qui sont transmis sur le même chemin et traités de la même manière et qui peuvent être mappés sur une seule étiquette par un LSR, comme le montre la figure suivante : (GHANIA, 2019)

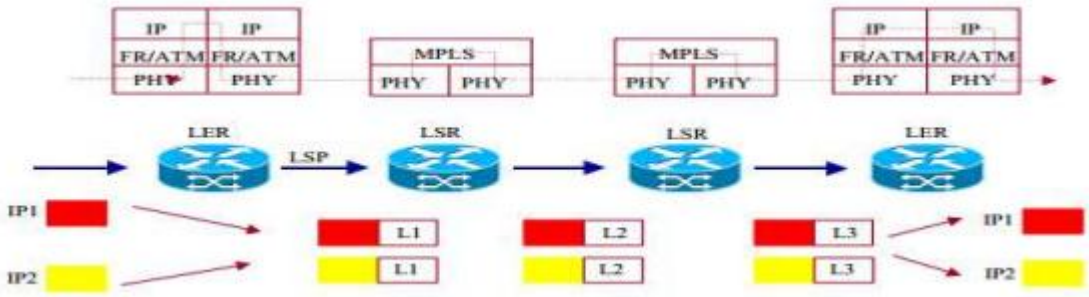

Figure 2. 5 : Forwarding Equivalence Classes

2.3 Format du Label MPLS

Le label est un index codé de 32 bits inséré par le LER, qui identifie le chemin que le paquet de données doit suivre une fois qu'il entre dans le nuage MPLS. Le label est directement encapsulée et transmise dans le paquet de données, puis insérée entre l'en-tête de niveau 2 (adresse MAC) et l'en-tête de niveau 3 (adresse IP). Chaque paquet de données doit suivre le processus basé sur le changement d'étiquette.

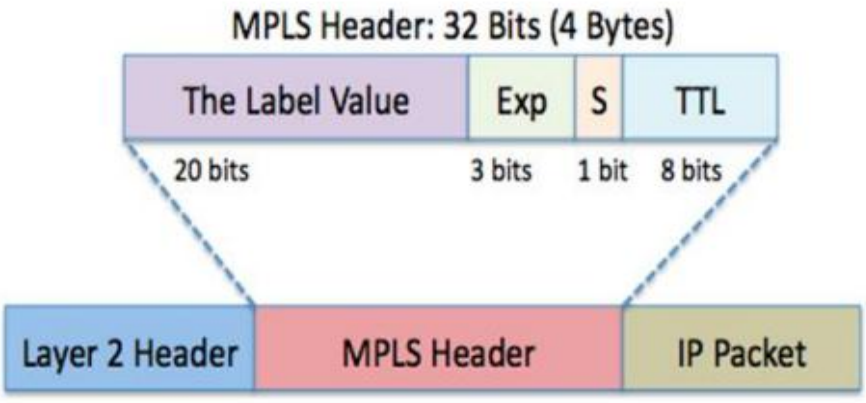

Figure 2. 6 : Format générique d'une étiquette MPLS

• LABEL : A 20 bits, c'est le code binaire du label à convertir dans le domaine MPLS. La valeur attribuée au label correspond à la classe d'équivalence de transmission (FEC).

• EXP : Sur 3 bits, c'est un champ expérimental, qui n'a pas encore été normalisé et peut être utilisé pour gérer la qualité de service afin de coder le numéro de service.

• STACK : ce bit est utilisé pour spécifier si la balise est la dernière de la liste, parce que les étiquettes peuvent être empilées dans le même emballage. Par conséquent, il est nécessaire d'indiquer au routeur s'il y a d'autres balises à lire. Dans le cas courant d'une seule label, le bit sera positionné à 1.

• TTL : Sur 8 bits, le TTL représente le cycle de vie des paquets de données dans le nuage MPLS. Le TTL permet d'éviter les boucles sur le réseau D'après le type de protocole de niveau 2 porté dans le paquet de données, le label est implémenté de différentes manières : (MOKHTARI, 2021)

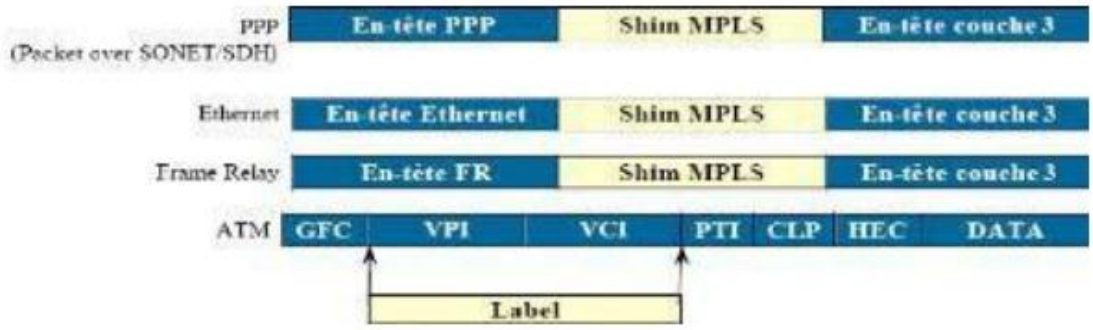

Figure 2. 7 : Encapsulation des labels dans des différentes trames

Pour ATM, le label n'est pas inséré entre les en-têtes de niveau 2 et de niveau 3, mais Directement dans le champ VPI / VCI de la trame ATM. FRAME RELAY, le principe est le même que ATM, le label est le même Inséré dans le champ DLCI de l'en-tête FR Pour les protocoles Ethernet, HDLC et PPP contrairement aux protocoles ATM et FR, le label occupe un champ séparé et est ajoutée à la trame susmentionnée entre l'en-tête de deuxième niveau et le en-tête de troisième niveau.

3. Principes de fonctionnement de MPLS

Le principe de base de MPLS est la commutation des labels. C'est un protocole situé au niveau 2,5 du modèle OSI car il associe les protocoles des couches 2 et 3. MPLS rend le concept de commutation générique car il peut fonctionner sur tout type de protocole de niveau 2.

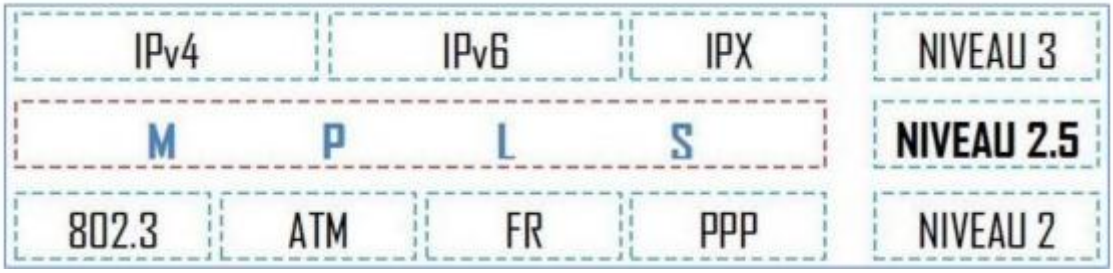

Figure 2. 8 : MPLS au niveau des couches

Les routeurs MPLS, à l'intérieur du Backbone, permutent les labels tout au long du réseau jusqu'à destination sans consultation de l'entête IP et la table de routage. La commutation MPLS est une technique orientée connexion. (RAJONIAINA, 2018)

3.1 Acheminement des paquets dans un réseau IP

Dans un réseau IP classique, il y a une mise en œuvre d'un protocole de routage (RIP, OSPF, ISIS, etc.). Ce protocole sera exécuté indépendamment par chaque nœud. A la convergence du protocole de routage, chaque nœud aura une vision plus ou moins complète du réseau et pourra calculer une table de routage contenant l'ensemble des destinations. Chaque destination sera associée à un "prochain saut" ou "Next Hop". Le routage IP classique distingue les paquets en se basant seulement sur les adresses réseaux de destination. (RAVOAVAHY, 2013)

3.2 Acheminement des paquets dans un réseau MPLS

La mise en œuvre de MPLS se repose sur la détermination des caractéristiques communes à un ensemble de paquets et dont dépendra l'acheminement de ces derniers. Cette notion de caractéristiques communes est appelée FEC (Forwarding Equivalence Class). Une FEC est la représentation d'un ensemble de paquets. Ces derniers suivent le même chemin et ont la même priorité. MPLS constitue les FEC selon de nombreux critères : adresse destination, adresse source, application, QoS, etc.

Quand un paquet IP arrive à un « Ingress LER », il sera associé à une FEC. Exactement comme dans le cas d'un routage IP classique, un protocole de routage sera mis en œuvre pour découvrir un chemin jusqu'à l'« Egress LER » (voir figure 2.8, la flèche en bleue). A la différence d'un routage IP classique, cette opération ne se réalise qu'une seule fois. Ensuite, tous les paquets appartenant à la même FEC seront acheminés suivant ce chemin qu'on appellera LSP (Label Switched Path). Ainsi on a eu la séparation entre fonction de routage et fonction de commutation : le routage se fait uniquement à la première étape. Ensuite, tous les paquets appartenant à la même FEC subiront une commutation simple à travers le chemin découvert.

Pour que les LSR puissent commuter correctement les paquets, l'« Ingress LER » affecte un label à ces paquets. Cette opération s'appelle « label imposition » ou « label pushing ». Si on prend l'exemple de la figure 2.8 : Le LSR1 saura en consultant sa table de commutation que tout paquet entrant ayant le label L=18 appartient à telle FEC et donc doit être commuté sur telle sortie en lui attribuant un nouveau label L=21. Ce processus s'appelle « label swapping ». Ce dernier sera exécuté par tous les LSR du LSP jusqu'à l'« Egress LER ». Enfin, le LER supprimera le label et routera le paquet de nouveau dans le monde IP de façon traditionnelle. Cette opération s'appelle « label popping » ou « label disposition ».

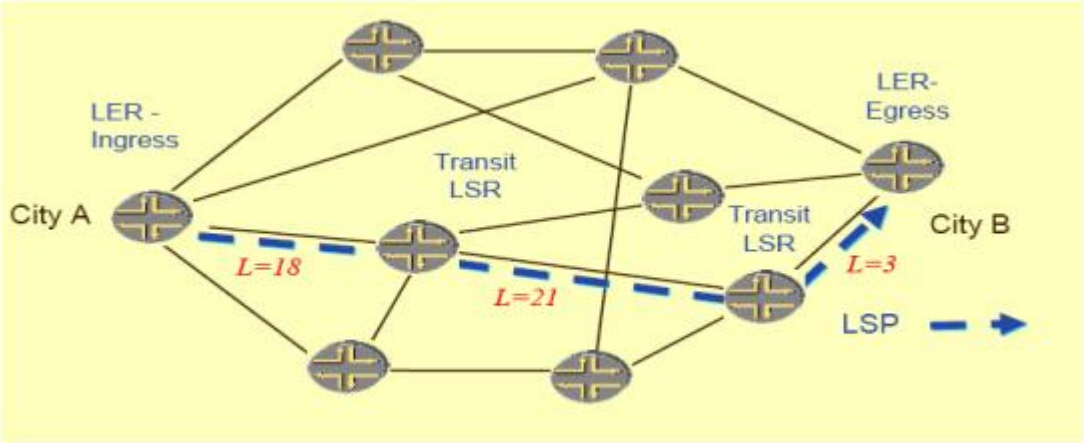

Figure 2. 9 : Exemple d'un réseau MPLS

L'acheminement des paquets dans le domaine MPLS ne se fait pas à base d'adresse IP mais de label. Il est clair qu'après la découverte du chemin (par le protocole de routage), il faut mettre en œuvre un protocole qui permet de distribuer les labels entre les LSR. Ces derniers constituent leurs tables de commutation adéquate à chaque paquet entrant. Cette tâche est effectuée par un protocole de distribution de label, tel que LDP (Label Distribution Protocol) ou RSVP TE (Resource Reservation Protocol Traffic Engineering). Les opérations « label pushing » et «

label popping » peuvent être le résultat d'une classification en FEC aussi complexe qu'on veut. Ainsi on aura placé toute la complexité aux extrémités du réseau MPLS alors que le cœur du réseau exécutera seulement la fonction simple « label swapping » en consultant la table de commutation.

4. Labels

Un label a une signification locale entre 2 LSR adjacents et mappe le flux de trafic entre le LSR amont et la LSR aval. A chaque bond le long du LSP, un label est utilisé pour chercher les informations de routage (next hop, lien de sortie, encapsulation, queueing et scheduling) et les actions à réaliser sur le label : insérer, changer ou retirer. La figure ci-dessous, décrit la mise en œuvre des labels dans les différentes technologies ATM, Frame Relay, PPP, Ethernet et HDLC. Pour les réseaux Ethernet, un champ appelé shim a été introduit entre la couche 2 et la couche 3. Sur 32 bits, il a une signification d'identificateur local d'une FEC. 20 bits contiennent le label, un champ de 3 bits appelé Classe of Service (CoS) sert actuellement pour la QoS, un bit S pour indiquer s'il y a empilement de labels et un dernier champ, le TTL sur 8 bits (même signification que pour IP). L'empilement des labels permet en particulier d'associer plusieurs contrats de service à un flux au cours de sa traversé du réseau MPLS. (FRAMEIP, 2023)

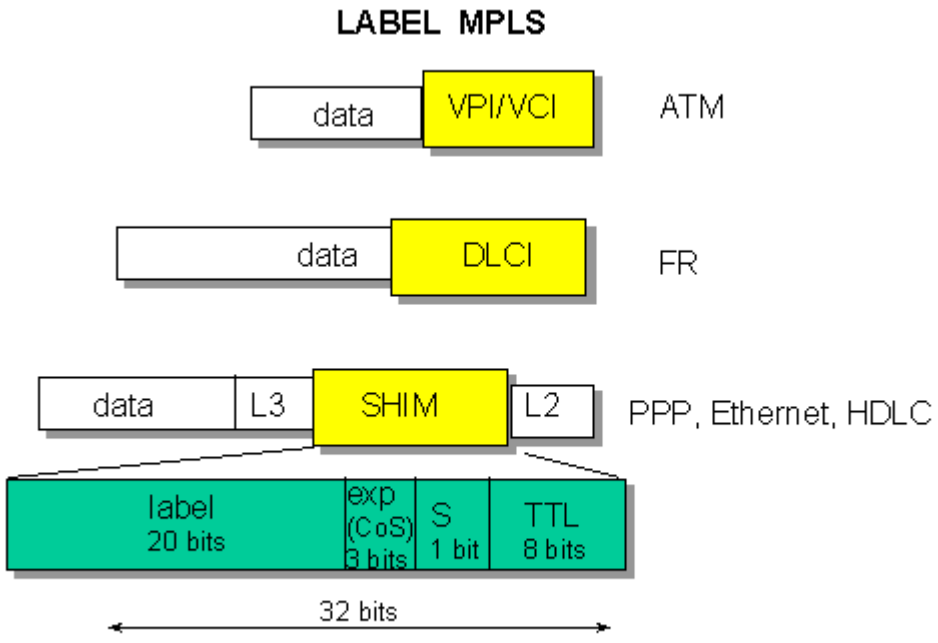

Figure 2. 10 : Label MPLS

5. Protocole de distribution de labels LDP

LDP définit une suite de procédures et de messages utilisés par les LSR pour s'informer mutuellement du mapping entre les labels et le flux. Une connexion LDP peut être établie entre deux LSR directement ou indirectement connectés.

5.1 Principe de connexion du LDP

¬ Deux routeurs adjacents vont s'échanger des messages UDP de type "HELLO" pour s'informer mutuellement de leur présence.

¬ Une connexion TCP va s'établir entre les deux routeurs voisins par l'échange des messages "TCP Open", et comme réponse, le message "Initialisation" est renvoyé pour initialiser le transport des messages d'annonce des labels.

¬ LDP commence la distribution des labels : (HAMAMI, 2021)

¬ Avec le mode sollicité : un message "Label Request" est envoyé par l'Ingress LER vers l'Egress LER, ce dernier répond par un message "Label Mapping" qui contient un label.

¬ Avec le mode non sollicité : l'Egress LER distribue directement les labels avec le message "Label Mapping", sans demande de l'Ingress LER par un message "Label Request".

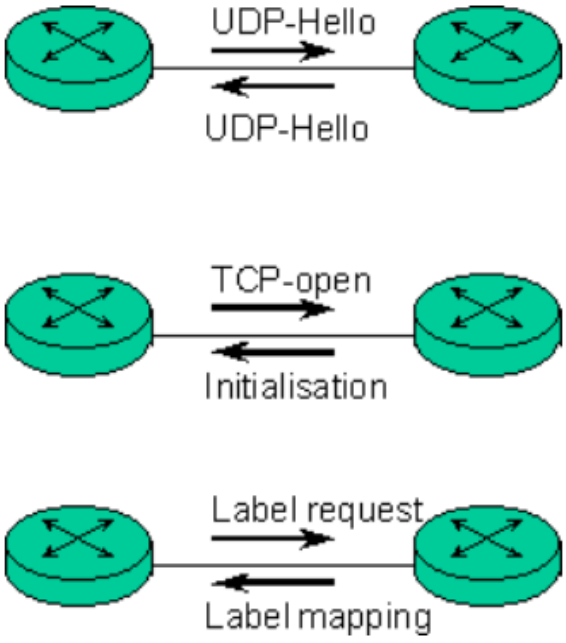

Figure 2. 11 : Etablissement d'une connexion LDP

5.2 Les différents modes de distribution de labels

Il existe deux modes de distribution de labels : le mode downstream on demand et le mode unsolicited downstream. Dans le premier mode, lorsqu'un routeur upstream va découvrir une nouvelle FEC il va établir une connexion avec un routeur downstream et lui demander un label pour la FEC découverte. En revanche, dans le second mode, dès lors qu'un routeur va découvrir une nouvelle FEC et mettre à jour ses labels, il va en informer le routeur upstream pour que ce dernier mettre à jour sa table de commutation. (Marot, 2023)

6. Les applications de la technologie MPLS

Les principales applications de la technologie MPLS sont les réseaux privés virtuels (VPN), la qualité de service (QoS) et l'ingénierie de trafic (TE). (RAJONIAINA, 2018)

6.1 VPN/MPLS (MPLS Virtual Private Network)

Cette application est populaire parmi les fournisseurs de services. Tout client peut disposer d'un réseau virtuel via le réseau MPLS et connecter tous les sites clients, même si les sites sont connectés à différents fournisseurs de services. Le client conserve ainsi sa vie privée et sécurise ses informations. (GHANIA, 2019)

6.2 MPLS – TE (Trafic Engineering)

Cette application est utilisée pour fournir un niveau de service spécifique aux clients, notamment pour garantir la qualité du son et des images et pour assurer une certaine bande passante au client. Cette application permet aux routeurs de connaître la bande passante disponible et de déterminer s'il existe une congestion entre les expéditeurs et les destinataires. (GHANIA, 2019)

6.3 QoS (Quality of service)

Avec la technologie MPLS et la définition des classes disposant chacune d'un niveau de priorité, il est possible de garantir une qualité de service adaptée à chacun des flux utilisant la solution VPN/MPLS. La QoS est un élément crucial pour un réseau d'opérateur. En effet, l'opérateur doit pouvoir garantir à ses clients le transport de leurs flux en garantissant différentes contraintes, comme par exemple : Débit minimal garanti, Débit maximal, Latence, Gigue. Ainsi cette solution permet de véhiculer la voix sur IP (VoIP) et de mettre en place des

applications de visioconférence dans des conditions excellentes sur des réseaux VPN/MPLS à forts taux d'utilisation. (RAJONIAINA, 2018)

7. Structure fonctionnelle du MPLS

Cette structure repose sur deux plans principaux pour la commutation des labels dans le réseau, qui sont illustrés dans la figure suivante : (BELAID, 2018)

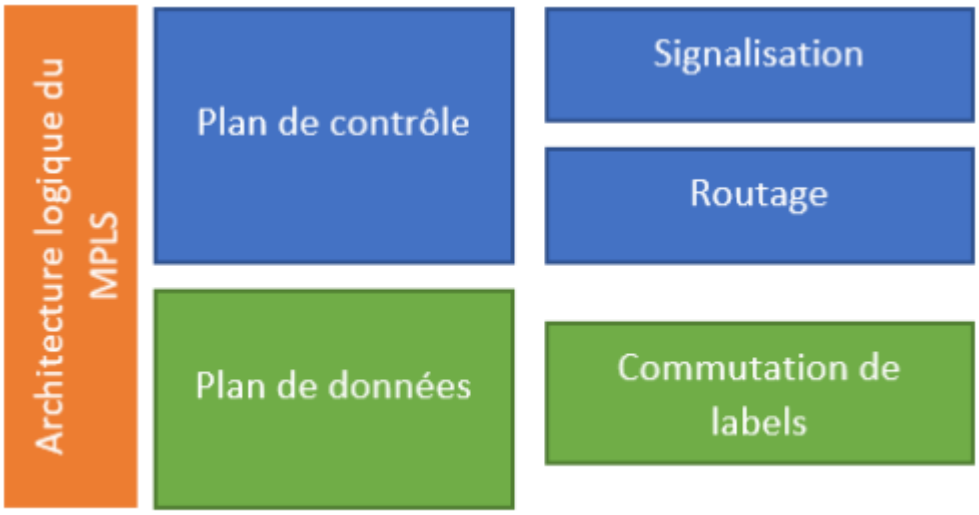

Figure 2. 12 : Structure fonctionnelle du réseau MPLS.

7.1 Le plan de contrôle (control plane)

Ce plan est composé de deux parties : la partie routage et la partie signalisation.

La partie routage utilise des protocoles de routage IGP (Interior Gateway Protocol) classiques, tels que l'OSPF (Open Shortest Path First), dans le but d'avoir une vision globale de la topologie du réseau MPLS (création de la table de routage).

La partie signalisation s'occupe de la distribution des labels et la création des chemins LSP (Label Switch Path), grâce à des protocoles de signalisation spécialement développés pour le réseau MPLS comme le LDP (Label Ditribution Protocol). La construction des LSP se fait de deux manières : par le routage implicite et le routage explicite (développé par la suite).

7.2 Le plan de données (data plane)

Il est indépendant des protocoles de routage et de distribution des labels, il permet d'acheminer les paquets labélisés à travers le réseau MPLS, en se basant sur une table de commutation appelée LFIB (Label Forwarding Information Base). La LFIB permet de

commuter des paquets de la source vers la destination, en utilisant les bons labels pour avoir le meilleur chemin (LSP) possible. Les LSR construisent deux tables, la LFIB et la LIB (Label Information Base) à partir des informations apprises par le protocole LDP. La LFIB est un sous ensemble de la base LIB.

Figure 2. 13 : Plan de contrôle et plan de données.

8. Routeurs virtuels (VRF)

Le VRF (Virtual Routing and Forwarding) est une technologie incluse dans les routeurs de réseau IP (Internet Protocol) qui permet à plusieurs instances d'une table de routage de coexister dans un routeur et de travailler simultanément.

La fonctionnalité réseau est alors améliorée, car les chemins réseau peuvent être segmentés sans faire appel à plusieurs routeurs. Dans la mesure où le trafic est automatiquement isolé, le VRF permet aussi d'accroître la sécurité du réseau et d'éviter le chiffrement et l'authentification. Les fournisseurs d'accès Internet (FAI) s'appuient souvent sur le concept VRF pour créer des réseaux privés virtuels (VPN) distincts pour chaque client. C'est pourquoi on fait également référence à cette technologie sous l'appellation Routage et transfert VPN. (REDACTION, 2023 a)

8.1 Table de transmission VRF

La table virtuelle de routage et de transfert (VRF) est un élément clé de la technologie VPN MPLS. VRF ou VPN Routing and Forwarding Table est une table de routage associée à un VPN qui donne les routes vers les réseaux IP faisant partie de ce VPN. Permet de virtualiser une partie du routeur car un opérateur a plusieurs clients sur le même PE. Par exemple, un

routeur qui doit traiter le trafic de plusieurs AS ayant le même adressage, afin de ne pas les mélanger, mettra chaque AS dans une VRF. Constituée d'une table de routage, d'une FIB (Forwarding Information Base) et d'une table CEF spécifiques, indépendantes des autres VRF et de la table de routage globale. Chaque VRF est désignée par un nom sur les routeurs PE. Les noms sont affectés localement, et n'ont aucune signification vis-à-vis des autres routeurs. Chaque interface de PE reliée à un site client est rattachée à une VRF particulière. (RAHANTANIRINA, 2016)

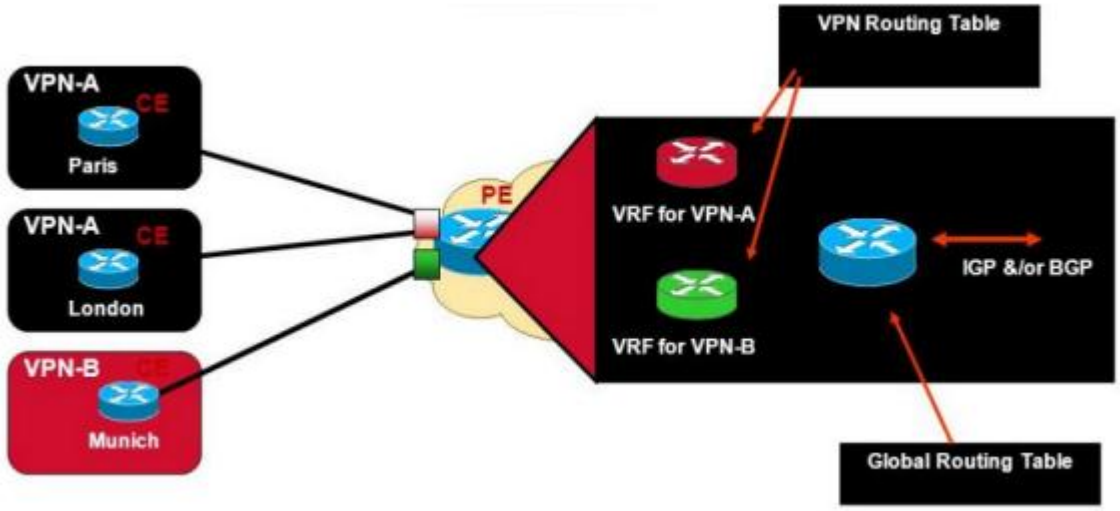

Figure 2. 14 :La table de transmission VRF

8.2 Propagation des informations du routage VPN

• MP-BGP (Multi-Protocol BGP): il s'agit d'une extension du protocole BGP qui permet à BGP de transporter des informations de routage pour plusieurs couches réseau et familles d'adresses. MP-BGP prend en charge les routes IPv4 monodiffusion/multidiffusion, IPv6 monodiffusion/multidiffusion et VPNv4.

• Notion de RD (Route Ditinguisher) : La fonction de RD est de rendre les routes appartenant à différents VRF uniques dans le noyau MPLS. Pour ce faire, nous devons annoncer les routes VPNv4 et nous accomplissons cette tâche en utilisant MP-BGP (Multi-Protocol BGP).

• Notion de RT (Route Target) : Maintenant, pour obtenir un routage correct sur un VPN MPLS, nous devons discuter des Route Targets (RT). Les RT définissent l'appartenance VPN

car ils permettent au routeur de contrôler l'importation et l'exportation de routes entre différents VRF. Ainsi, disons que si le client A situé dans la succursale X souhaite avoir une connectivité avec le client A situé dans la succursale Y, les RT devront être importés et exportés entre les VRF respectifs. (RAHIL, 2022)

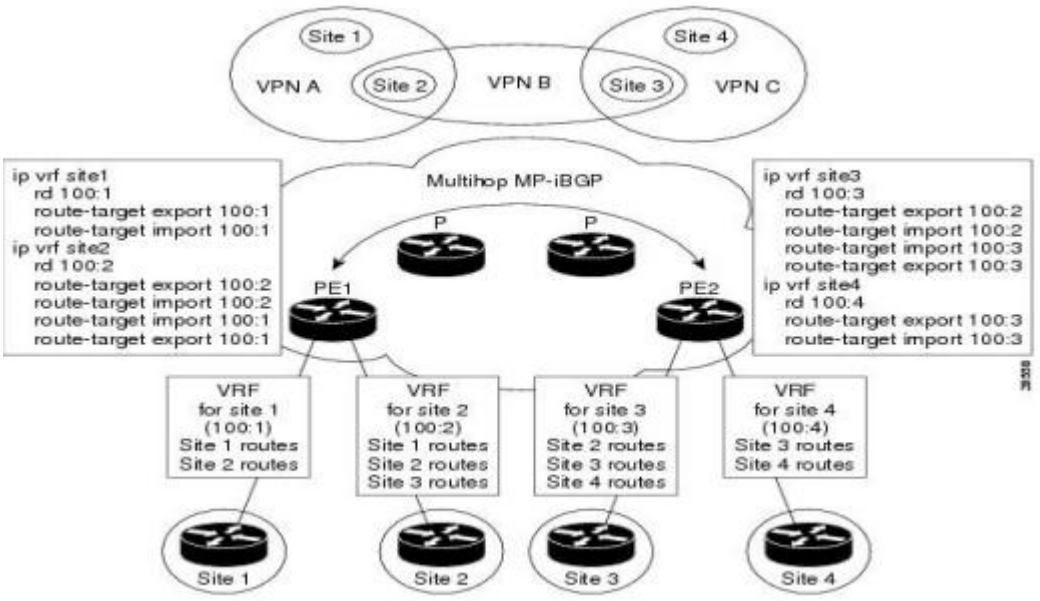

Figure 2. 15 : VRF pour les sites dans plusieurs VPNs

8.3 Propagation des étiquettes VPN

La deuxième étiquette est exigée pour l'opération appropriée de MPLS VPN, Cette étiquette a été assignée par le routeur PE de sortie. Cette étiquette doit être propagée du routeur PE de sortie aux routeurs PE d'entrée pour permettre la transmission de paquet approprié.

MP-BGP a été choisi comme mécanisme de propagation. Chaque mise à jour MP-BGP porte ainsi une étiquette assignée par le routeur PE de sortie ainsi que le préfixe VPNv4 de 96 bit.

La propagation d'étiquette VPN doit suivre les étapes suivantes : (AMINE, 2010)

- Etape1 : le routeur PE de sortie assigne une étiquette à chaque route VPN reçu des routeurs CE attachés et à chaque route, il la récapitule à l'intérieur du routeur PE. Cette étiquette est alors employée comme la deuxième étiquette dans la pile d'étiquette de MPLS par les routeurs PE d'entrée en marquant des paquets VPN.

- Etape 2 : Les étiquettes de VPN assignées par les routeurs PE de sortie sont annoncées à tous autres routeurs PE ainsi que le préfixe VPNv4 dans les mises à jour MP-BGP.

- Etape 3 : le routeur PE d'entrée a deux étiquettes liées à une route VPN distante, une étiquette pour le prochain saut de BGP assigné par le prochain saut du routeur P par l'intermédiaire de LDP aussi bien que l'étiquette assignée par le routeur distant PE et propagée par l'intermédiaire de la mise à jour MP-BGP. Les deux étiquettes sont combinées dans une pile d'étiquette et installées dans la table VRF.

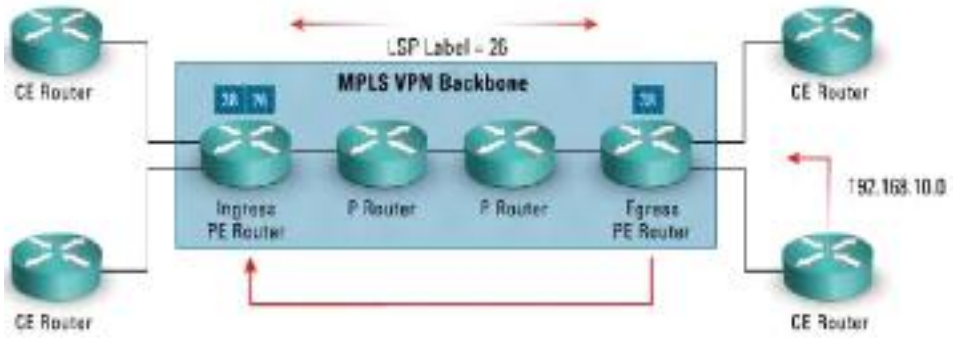

Figure 2. 16 : Propagation d'étiquette VPN.

Pour configurée la propagation d'étiquette VPN en suivre les étapes suivant :

- Mise en place du protocole de routage intra-nuage (OSPF).
- Mise en place du protocole de découverte des voisins MPLS (LDP).
- Configuration de l'authentification des voisins (MDS) 1010.
- Mise en place des VRFs et des interfaces.
- Mise en place du protocole de routage CE-PE (RIP v2, OSPF).
- Mise en place du protocole MP-BGP ; Gestion de redistribution des préfixes.

9. Conclusion

Grace à des mécanismes avancés de commutation facile en place sur des réseaux déjà existants, MPLS est devenu une technologie de pointe du futur, combinant flexibilité, évolutivité et performance à faible cout.

Dans ce chapitre, nous avons étudié la technologie MPLS et son principe de fonctionnement, ainsi que leurs application dans les réseaux télécom.

Chapitre 3 : Réalisation d'un réseau MPLS

1. Introduction

Dans ce chapitre, nous allons expliquer le but de cette étude, et de montrer les résultats de l'implémentation des protocoles OSPF et BGP dans le réseau MPLS. Ce chapitre consiste à valider notre projet, en inférant les différentes configurations qu'il est important d'implémenter sur notre architecture, basée sur l'émulateur GNS3. Pour cela, nous présentons les configurations que nous avons réalisées, nous avons utilisé des captures d'écran montrant les étapes de configuration nécessaires et les tests que nous avons effectués.

2. Organigramme de djezzy

Structure de Djezzy : l'organisation d'optimum télécom Algérie S.P.A qui a une partie de manageant qui décompose en six parties et chaque partie et a ait décomposé.

Le département de manageant est constitué de plusieurs services comme le montre Structure, il est charge : (MEGRI, 2015)

- Du contrôle des transactions.
- De la surveillance des incidents.
- De la charge d'un réseau local ou interconnecté.
- L'administration du réseau.
- La mise en œuvre des nouveaux services.
- l'administration des accès et de la bande passante.

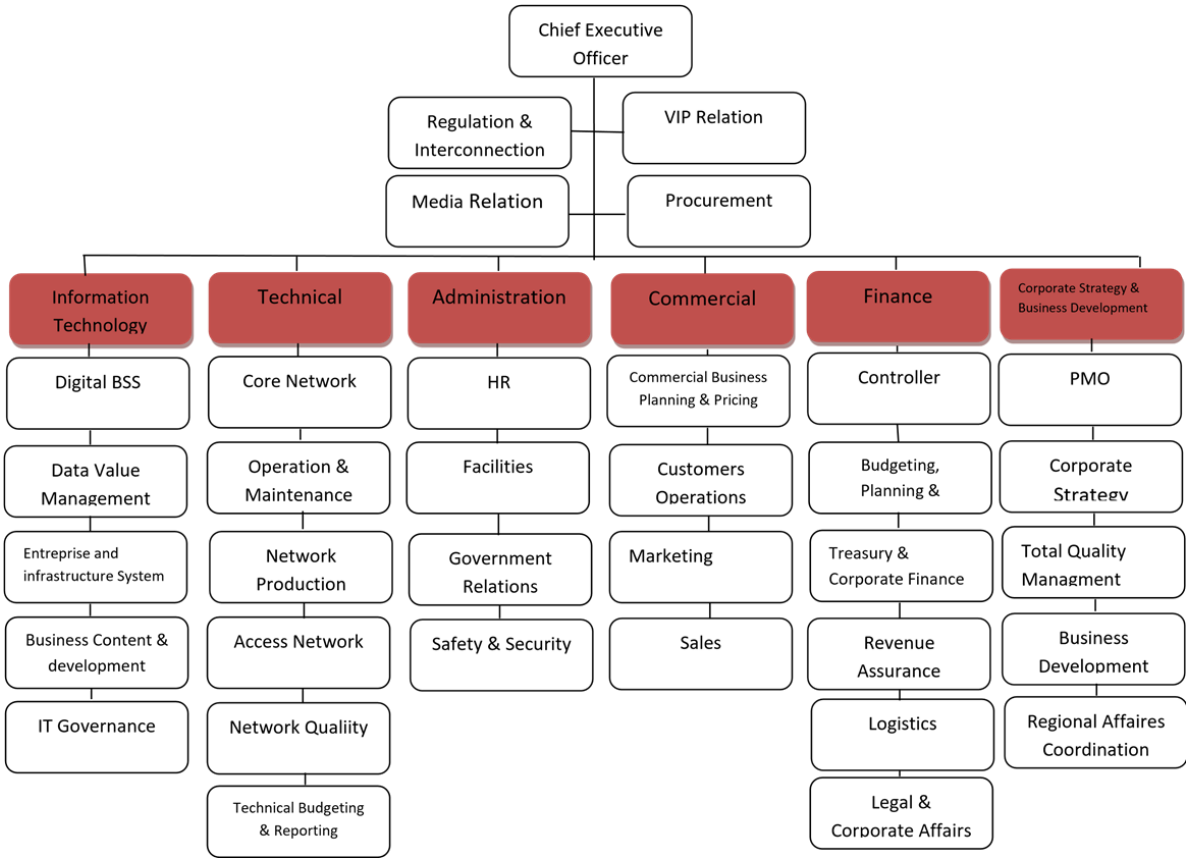

Figure 3. 1 : Structure de Djezzy

2.1 Zoom sur le service network dans lequel nous trouvons

Nous avons réalisé ce stage au service du Core Network qui se compose en cinq parties qui sont :

- Core planning & integration CS&PS
- Core Data Network
- Core Environnement &Power
- Budget & Core Project
- Core Infrastructure & Virtualisation

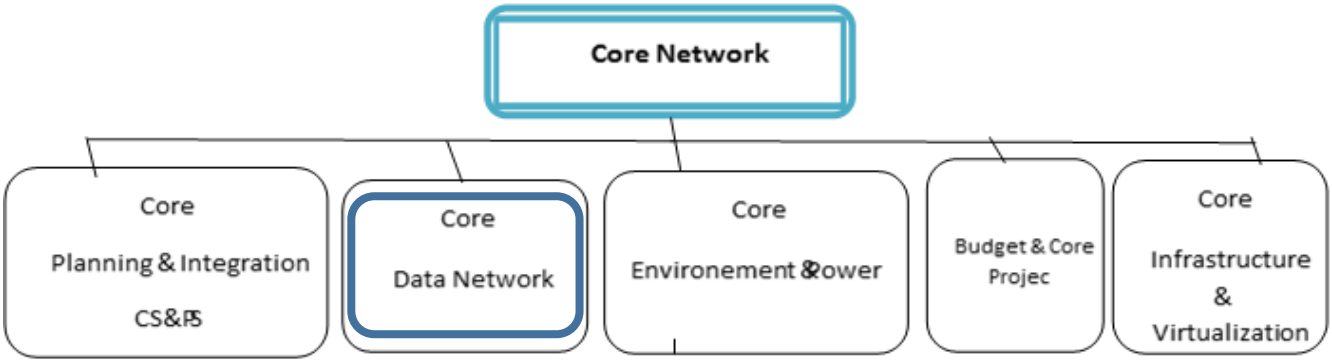

Figure 3. 2 : Zoom sur le service Core Network dans lequel nous nous trouvons

3. Le but du projet

Notre projet consiste a étudié les technologies du routage IP au sein du réseau DJEZZY d'une façon générale et d'une façon détaille le Protocol de routage MPLS.

Dans ce projet on a utilisé deux couches ; les deux couches sont : la couche liaison et la couche réseaux.

La couche liaison de données : qui reçoit les données brutes de la couche physique, elle les organise en trames, et détecte les erreurs.

La couche réseau (IP) : assure également un service de traduction des adresses logiques (adresse IP) en adresses physiques (adresse MAC). Dans cette couche on a étudié les adresse IP et le routage IP.

Le but de notre projet est de séparer le trafic entre deux entités et forwarding du trafic.

Il s'agit d'assurer le trafic entre le site de Tizi-Ouzou & Alger et entre site Blida & Médéa avec une séparation de trafic Tizi & Alger avec Blida &Médéa.

4. Réalisation du réseau

Dans cette partie, nous allons présenter le réseau utilisé et ses différentes configurations :

4.1 Présentation du réseau

Nous avons utilisé 10 routeurs dont :

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

- R3 ; R4 ; R5 ; R6

• Routeurs représentant l'Edge MPLS (routeurs PE : provider Edge) et simulant les routeurs :

- R7 ; R8

• Routeurs désignant les sites d'un client (routeurs CE) et simulant :

- R9 ; R10 ; R11 ; R12

Les routeurs PE et P utilisent la version IOS :

Pour le 7200 : << c7200-adventerprisek9-mz.152 -4.S5.bin>>

Et de type Cisco avec les caractéristiques ci-dessous :

- RAM : 512 MB.
- NVRAM : 512 KB.
- SLOT0 : une carte d'une interface FE.
- SLOT 1-5 : une carte d'une interface GE par SLOT.
- SLOT 6 : une carte de deux (02) interfaces FE.

Les routeurs CE utilisent la version IOS :

Pour le 3725 : << c3725-adventerprisek9-mz124-15.bin>>

Et de type Cisco avec les caractéristiques ci-dessous :

- RAM : 128 MB.
- NVRAM : 256 KB.
- SLOT 0 : une carte deux (02) interfaces FE.

Nous utilisons le GNS3 comme un simulateur pour simuler notre architecteur. GNS3 est un programme qui permet de simuler des réseaux de routeur et de commutateur qui tournent sous IOS (le système d'exploitation des routeurs et switch Cisco).

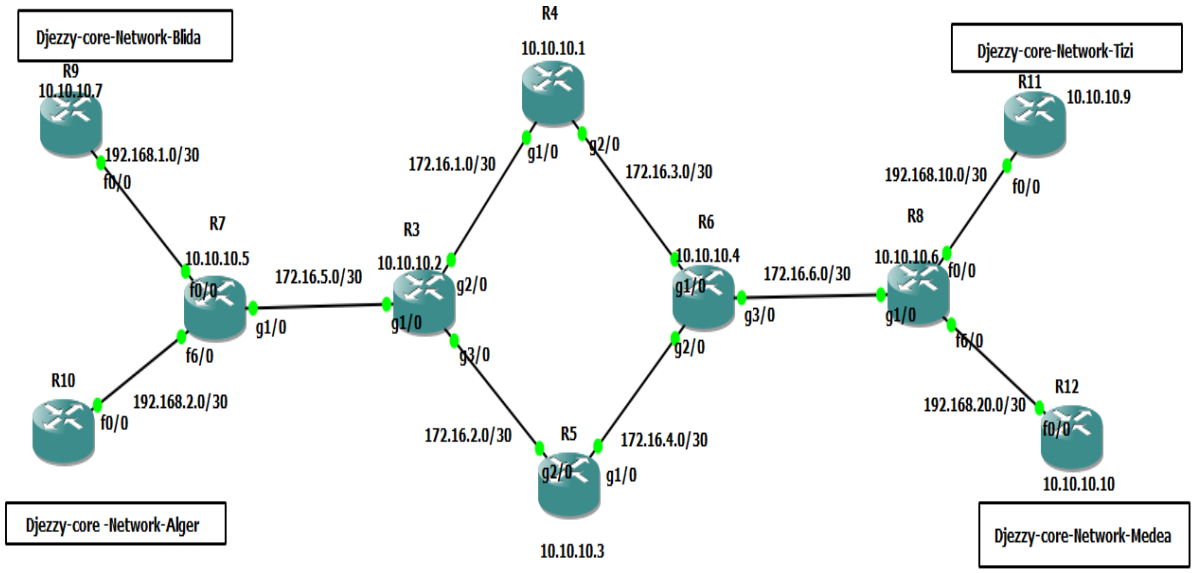

Figure 3. 3 : Architecture du réseau

4.2 Configuration du réseau

Les différentes étapes de la configuration du réseau seront montrées dans cette section :

4.2.1 Table d'adressage

La configuration des adresses IP attribuées aux interfaces de chaque routeur est illustrée dans le tableau suivant :

Tableau 3. 1 : Configuration des adresses IP

Equipement	Interface	Adresse	Masque	Gateway
R7	Fats Ethernet 0/0	192.168.1.1	255.255.255.252	R9
	Fats Ethernet 6/0	192.168.2.1	255.255.255.252	R10
	Gigabit Ethernet 1/0	172.16.5.2	255.255.255.252	R3
	Loopback	10.10.10.5	255.255.255.255	-
R8	Fats Ethernet 0/0	192.168.10.1	255.255.255.252	R11
	Fats Ethernet 6/0	192.168.20.1	255.255.255.252	R12
	Gigabit Ethernet 1/0	172.16.6.2	255.255.255.252	R6
	Loopback	10.10.10.6	255.255.255.255	-
R3	Gigabit Ethernet 1/0	172.16.5.1	255.255.255.252	R7
	Gigabit Ethernet 2/0	172.16.1.1	255.255.255.252	R4
	Gigabit Ethernet 3/0	172.16.2.1	255.255.255.252	R5
	Loopback	10.10.10.2	255.255.255.255	-
R4	Gigabit Ethernet 1/0	172.16.1.2	255.255.255.252	R3
	Gigabit Ethernet 2/0	172.16.3.1	255.255.255.252	R6
	Loopback	10.10.10.1	255.255.255.255	-
R5	Gigabit Ethernet 1/0	172.16.4.1	255.255.255.252	R6
	Gigabit Ethernet 2/0	172.16.2.2	255.255.255.252	R3
	Loopback	10.10.10.3	255.255.255.255	-

R6	Gigabit Ethernet 1/0	172.16.3.2	255.255.255.252	R4
	Gigabit Ethernet 2/0	172.16.4.2	255.255.255.252	R5
	Gigabit Ethernet 3/0	172.16.6.1	255.255.255.252	R8
	Loopback	10.10.10.4	255.255.255.255	-
R9	Fats Ethernet 0/0	192.168.1.2	255.255.255.252	R7
	Loopback	10.10.10.7	255.255.255.255	-
R10	Fats Ethernet 0/0	192.168.2.2	255.255.255.252	R7
	Loopback	10.10.10.8	255.255.255.255	-
R11	Fats Ethernet 0/0	192.168.10.2	255.255.255.252	R8
	Loopback	10.10.10.9	255.255.255.255	-
R12	Fats Ethernet 0/0	192.168.20.2	255.255.255.252	R8
	Loopback	10.10.10.10	255.255.255.255	-

3.2.2 Configuration des différents routeurs

Cette partie consiste à effectuer une configuration initiale sur les routeurs primaires (réseau) en suivant les étapes mentionnées ci-dessous :

- Configuration de l'adressage ; Configuration des interfaces ; Configuration de routage IGP (le protocole OSPF) ; Configuration du protocole MPLS ; Configuration du BGP et les VRF.

3.2.3 Intégration des routeurs

Nous sélectionnons des routeurs pour les configurer et les intégrer dans la partie centrale de GNS3 comme le montre la figure suivante :

Figure 3. 4 : Intégration des routeurs

3.2.4 Interconnexion des routeurs

On connecte les routeurs aux câbles, et quand la plateforme est prête, on active la topologie avec l'icône sur la barre de menu en haut. Est montrée sur la figure ci-dessous :

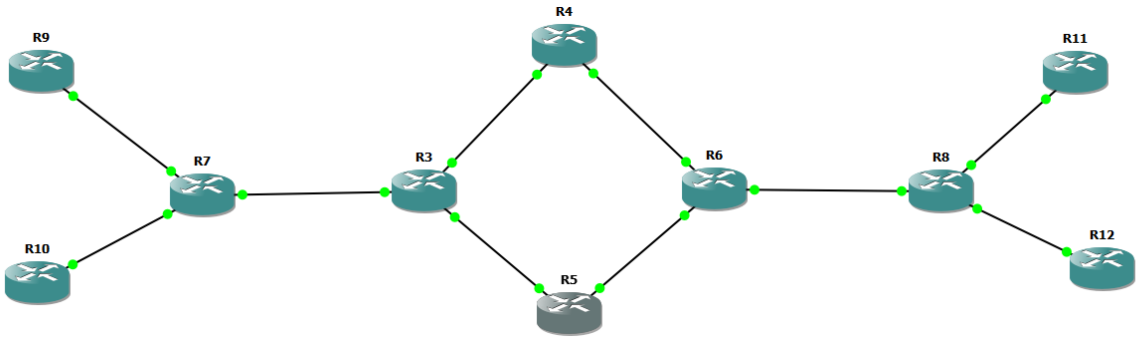

Figure 3. 5 : Liaison des routeurs

4.2.5 Configuration des interfaces loopback

Interface loopback : est une interface virtuelle, cette interface est perçue comme une interface physique, pour activée cette interface en utilisée cette commande « **interface loopback** », en suit utilisant la commande **« Ip Address »** ; comme le montre la figure suivante :

```
R7(config)#interface loopback 5
R7(config-if)#ip address 10.10.10.5 255.255.255.255
R7(config-if)#
*May 30 12:38:02.847: %TCP-6-BADAUTH: Invalid MD5 digest from 10.10.10.2(646) to 172.16.5.2(25239) (RST) tableid - 0
R7(config-if)#ip address 10.10.10.5 255.255.255.255
*May 30 12:38:04.663: %TCP-6-BADAUTH: Invalid MD5 digest from 10.10.10.2(646) to 172.16.5.2(25239) (RST) tableid - 0
R7(config-if)#exit
R7(config)#
```

Figure 3. 6 : Configuration loopback

Pour voire l'interface de loopback, nous utilisons la commande « **show runing-config** », comme le montre la figure suivante:

```
interface Loopback1
 ip address 10.10.10.2 255.255.255.255
 ip ospf 1 area 0
!
```

```
interface Loopback2
 ip address 10.10.10.1 255.255.255.255
 ip ospf 2 area 0
!
```

```
interface Loopback3
 ip address 10.10.10.3 255.255.255.255
 ip ospf 3 area 0
!
```

```
interface Loopback4
 ip address 10.10.10.4 255.255.255.255
 ip ospf 4 area 0
!
```

```
interface Loopback5
 ip address 10.10.10.5 255.255.255.255
 ip ospf 5 area 0
!
```

```
interface Loopback6
 ip address 10.10.10.6 255.255.255.255
!
```

```
interface Loopback7
 ip address 10.10.10.7 255.255.255.255
!
```

```
interface Loopback8
 ip address 10.10.10.8 255.255.255.255
 ip ospf 8 area 0
!
```

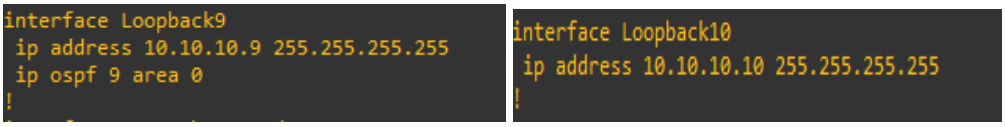

Figure 3. 7 : Loopback activé

4.2.6 Configuration de l'adressage pour les interfaces

Nous configurons chaque interface par la commande « **interface Fats Ethernet X/Y** » ou bien avec « **interface Gigabit Ethernet X/Y** ».

Nous attribuons une IP à chaque interface, en utilisant la commande « **ip address** », ensuite on les active avec la commande « **no shutdown** ». Comme le montre la figure ci-dessous :

```
R7(config)#interface Gi
R7(config)#interface GigabitEthernet 1/0
R7(config-if)#ip add
R7(config-if)#ip address 172.16.5.2 255.255.255.252
R7(config-if)#no s
R7(config-if)#no sh
R7(config-if)#no shutdown
R7(config-if)#
*May 30 15:58:13.523: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*May 30 15:58:14.523: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
R7(config-if)#interface f
R7(config-if)#interface fa
R7(config-if)#interface fas
R7(config-if)#interface fast
R7(config-if)#int
R7(config-if)#intr
R7(config-if)#int
R7(config-if)#int
R7(config-if)#intrf
R7(config-if)#exit
R7(config)#int
R7(config)#interface f
R7(config)#interface fa
R7(config)#interface fastEthernet 0/0
R7(config-if)#ip add
R7(config-if)#ip address 192.168.1.1 255.255.255.252
R7(config-if)#no sh
R7(config-if)#no shutdown
R7(config-if)#EXIT
*May 30 15:59:57.163: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*May 30 15:59:58.163: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R7(config-if)#EXIT
R7(config)#int
R7(config)#interface fa
R7(config)#interface fastEthernet 6/0
R7(config-if)#ip add
R7(config-if)#ip address 192.168.2.1 255.255.255.252
R7(config-if)#no sh
```

```
R8(config)#interface GigabitEthernet 1/0
R8(config-if)#ip add
R8(config-if)#ip address 172.16.6.2 255.255.255.252
R8(config-if)#no sh
R8(config-if)#no shutdown
R8(config-if)#exit
R8(config)#
*May 30 16:03:11.675: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*May 30 16:03:12.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
R8(config)#int
R8(config)#interface fa
R8(config)#interface fastEthernet 0/0
R8(config-if)#ip add
R8(config-if)#ip address 192.168.10.1 255.255.255.252
R8(config-if)#no sh
R8(config-if)#no shutdown
R8(config-if)#exi
*May 30 16:03:49.343: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*May 30 16:03:50.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R8(config-if)#exit
R8(config)#int
R8(config)#interface fa
R8(config)#interface fastEthernet 6/0
R8(config-if)#ip add
R8(config-if)#ip address 192.168.20.1 255.255.255.252
R8(config-if)#no sh
R8(config-if)#no shutdown
R8(config-if)#exit
R8(config)#
*May 30 16:04:24.959: %LINK-3-UPDOWN: Interface FastEthernet6/0, changed state to up
R8(config)#
*May 30 16:04:25.959: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet6/0, changed state to up
R8(config)#
```

Figure 3. 8 : Configuration des interfaces de R7 et R8

L'étape de la vérification des interfaces qu'on a activées avec la commande « **show ip interfaces brief** » dans le consol est montré sur la figure ci-dessous :

```
R8#sh
R8#show int
R8#show ip int
R8#show ip interface b
R8#show ip interface br
R8#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES NVRAM  up                    up
GigabitEthernet1/0     172.16.6.2      YES NVRAM  up                    up
GigabitEthernet2/0     unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0     unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0     unassigned      YES NVRAM  administratively down down
FastEthernet5/0        unassigned      YES NVRAM  administratively down down
FastEthernet5/1        unassigned      YES NVRAM  administratively down down
FastEthernet6/0        192.168.20.1    YES NVRAM  up                    up
FastEthernet6/1        unassigned      YES NVRAM  administratively down down
Loopback4              unassigned      YES unset  up                    up
Loopback6              10.10.10.6      YES NVRAM  up                    up
R8#

R9#sh
R9#show ip int
R9#show ip interface br
R9#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.2     YES NVRAM  up                    up
FastEthernet0/1            192.168.100.1   YES NVRAM  up                    up
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
FastEthernet2/0            unassigned      YES NVRAM  administratively down down
Loopback5                  unassigned      YES NVRAM  up                    up
Loopback7                  10.10.10.7      YES NVRAM  up                    up
R9#

R7#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
GigabitEthernet1/0     172.16.5.2      YES manual up                    up
GigabitEthernet2/0     unassigned      YES unset  administratively down down
GigabitEthernet3/0     unassigned      YES unset  administratively down down
GigabitEthernet4/0     unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
FastEthernet5/1        unassigned      YES unset  administratively down down
FastEthernet6/0        192.168.2.1     YES manual up                    up
FastEthernet6/1        unassigned      YES unset  administratively down down
R7#
```

Figure 3. 9 : Interfaces activées de R8 et R7 et R9 après configuration.

Dans Figure (3.9), nous voyons l'activation des interfaces 0/0 et l'interface 0/1 et l'interface de loopback 7 dans le Edge 7.

Vérification des adresses qui activée. En présentée dans la figure suivant :

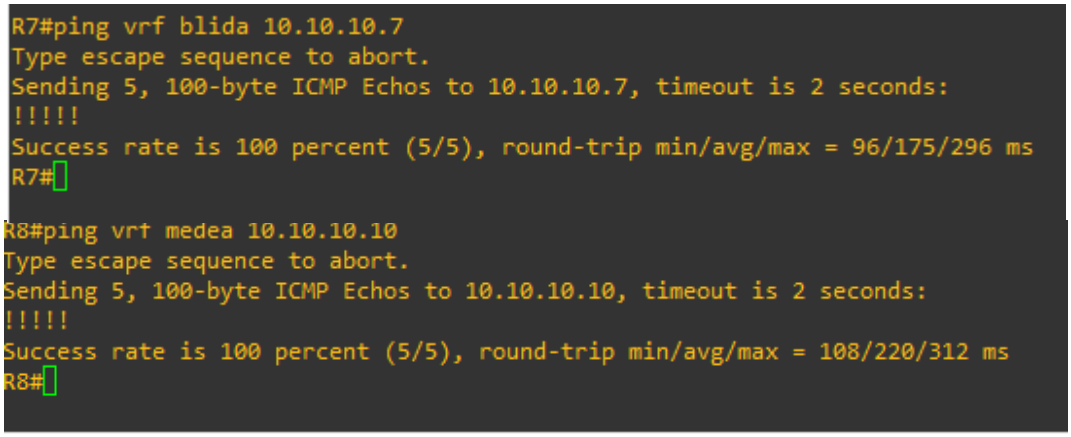

Figure 3. 10 : Vérification des adresses

4.2.7 Configuration du protocole RIP

Le protocole RIP (Routing Information Protocol) est utilisé pour gérer les informations du routeur dans un réseau autonome, par exemple un réseau local d'entreprise (LAN) ou un réseau étendu privé (WAN). (Fireware, 2023)

- « **router rip** » : pour déclencher le processus RIP.

- « **network** » : pour déclarer et spécifier le réseau participant au processus RIP.

- « **exit** » : pour sortir du mode configuration.

Est montrée sur la figure ci-dessous :

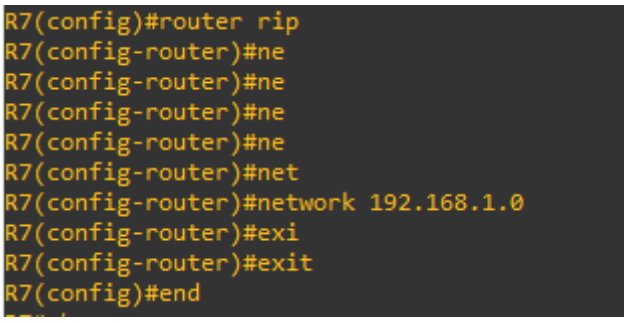

Figure 3. 11 : Activation de RIP.

Après la configuration, nous testons l'activation de protocole RIP avec la commande **« show ip route vrf blida** » dans le routeur 7 et «**show ip route vrf medea »** dans le routeur 8 qui nous montre la table de routage. Est montrée sur la figure ci-dessous :

```
R7#show ip route vrf blida

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

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 2 subnets
R        10.10.10.7 [120/1] via 192.168.1.2, 00:00:46, FastEthernet0/0
B        10.10.10.10 [200/1] via 10.10.10.6, 00:02:13
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, FastEthernet0/0
L        192.168.1.1/32 is directly connected, FastEthernet0/0
      192.168.20.0/30 is subnetted, 1 subnets
B        192.168.20.0 [200/0] via 10.10.10.6, 00:02:13
R7#
```

```
R8#show ip route vrf medea

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

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 2 subnets
B        10.10.10.7 [200/1] via 10.10.10.5, 00:05:17
R        10.10.10.10 [120/1] via 192.168.20.2, 00:01:35, FastEthernet6/0
      192.168.1.0/30 is subnetted, 1 subnets
B        192.168.1.0 [200/0] via 10.10.10.5, 00:05:17
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/30 is directly connected, FastEthernet6/0
L        192.168.20.1/32 is directly connected, FastEthernet6/0
R8#
```

Figure 3. 12 : Router RIP

Dans cette figure nous montrons que le protocole RIP est actif dans l'interface de loopback 7 via l'interface 0/0 dans Edge 7, dans Edge 8 est activée à l'interface de loopback 10 via l'interface 6/0.

4.2.8 Configuration du protocole OSPF

Est un protocole servant à déterminer le meilleur chemin que peuvent emprunter des paquets pour transiter par une série de réseaux connectés (REDACTION, 2023 b). L'utilité d'OSPF pour établir session OSPF plus rapide de RIP et utilise les loopback pour un réseau plus stable en se trouver dans la table publique.

Nous configurons OSPF sur tous les routeurs du réseau MPLS comme suit :

« **router ospf 5** » : pour déclencher le processus ospf, le numéro 5 représente l'identifiant du routeur.

- « **network** » : pour déclarer et spécifier le réseau participant au processus ospf.

- « **exit** » : pour sortir du mode configuration

Est montrée sur la figure ci-dessous :

```
R7(config)#router ospf 5
R7(config-router)#net
R7(config-router)#network 172.16.5.2 0.0.0.3 ar
R7(config-router)#network 172.16.5.2 0.0.0.3 area 0
R7(config-router)#exit
R7(config)#
```

```
R10(config)#router ospf 10
R10(config-router)#ne
R10(config-router)#net
R10(config-router)#network 192.168.2.0 0.0.0.3 ar
R10(config-router)#network 192.168.2.0 0.0.0.3 area 0
R10(config-router)#no sh
R10(config-router)#ex
R10(config-router)#exit
R10(config)#
```

Figure 3. 13 : Activation d'OSPF

Après la configuration, en teste l'activation de protocole OSPF avec la commande **« show ip route OSPF** » qui nous montre la table de routage. Est montrée sur la figure ci-dessous :

```
      172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O        172.16.1.0/30 [110/2] via 172.16.5.1, 00:24:14, GigabitEthernet1/0
O        172.16.2.0/30 [110/2] via 172.16.5.1, 00:24:14, GigabitEthernet1/0
O        172.16.3.0/30 [110/3] via 172.16.5.1, 00:24:14, GigabitEthernet1/0
O        172.16.4.0/30 [110/3] via 172.16.5.1, 00:24:14, GigabitEthernet1/0
C        172.16.5.0/30 is directly connected, GigabitEthernet1/0
L        172.16.5.2/32 is directly connected, GigabitEthernet1/0
O        172.16.6.0/30 [110/4] via 172.16.5.1, 00:24:14, GigabitEthernet1/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, FastEthernet0/0
L        192.168.1.1/32 is directly connected, FastEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/30 is directly connected, FastEthernet6/0
L        192.168.2.1/32 is directly connected, FastEthernet6/0
      192.168.10.0/30 is subnetted, 1 subnets
O        192.168.10.0 [110/5] via 172.16.5.1, 00:21:11, GigabitEthernet1/0
      192.168.20.0/30 is subnetted, 1 subnets
O        192.168.20.0 [110/5] via 172.16.5.1, 00:20:45, GigabitEthernet1/0
R7#
```

```
      172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O        172.16.1.0/30 [110/3] via 172.16.6.1, 00:23:02, GigabitEthernet1/0
O        172.16.2.0/30 [110/3] via 172.16.6.1, 00:23:02, GigabitEthernet1/0
O        172.16.3.0/30 [110/2] via 172.16.6.1, 00:23:02, GigabitEthernet1/0
O        172.16.4.0/30 [110/2] via 172.16.6.1, 00:23:02, GigabitEthernet1/0
O        172.16.5.0/30 [110/4] via 172.16.6.1, 00:23:02, GigabitEthernet1/0
C        172.16.6.0/30 is directly connected, GigabitEthernet1/0
L        172.16.6.2/32 is directly connected, GigabitEthernet1/0
      192.168.1.0/30 is subnetted, 1 subnets
O        192.168.1.0 [110/5] via 172.16.6.1, 00:23:02, GigabitEthernet1/0
      192.168.2.0/30 is subnetted, 1 subnets
O        192.168.2.0 [110/5] via 172.16.6.1, 00:23:02, GigabitEthernet1/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/30 is directly connected, FastEthernet0/0
L        192.168.10.1/32 is directly connected, FastEthernet0/0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/30 is directly connected, FastEthernet6/0
L        192.168.20.1/32 is directly connected, FastEthernet6/0
R8#
R8#
```

```
      192.168.10.0/30 is subnetted, 1 subnets
O        192.168.10.0 [110/15] via 192.168.1.1, 00:00:00, FastEthernet0/0
      172.16.0.0/30 is subnetted, 6 subnets
O        172.16.4.0 [110/13] via 192.168.1.1, 00:00:00, FastEthernet0/0
O        172.16.5.0 [110/11] via 192.168.1.1, 00:00:00, FastEthernet0/0
O        172.16.6.0 [110/14] via 192.168.1.1, 00:00:00, FastEthernet0/0
O        172.16.1.0 [110/12] via 192.168.1.1, 00:00:00, FastEthernet0/0
O        172.16.2.0 [110/12] via 192.168.1.1, 00:00:00, FastEthernet0/0
O        172.16.3.0 [110/13] via 192.168.1.1, 00:00:09, FastEthernet0/0
      192.168.20.0/30 is subnetted, 1 subnets
O        192.168.20.0 [110/15] via 192.168.1.1, 00:00:09, FastEthernet0/0
      192.168.1.0/30 is subnetted, 1 subnets
C        192.168.1.0 is directly connected, FastEthernet0/0
      192.168.2.0/30 is subnetted, 1 subnets
O        192.168.2.0 [110/11] via 192.168.1.1, 00:04:26, FastEthernet0/0
R9#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 744/995/1420 ms
R9#
```

Figure 3. 14 : Routes OSPF

Dans cette figure nous voyons qu'OSF a été activée dans les interfaces 1/0 dans les Edge 7 et 8.

4.2.9 Configuration de MPLS

Est une technologie conçue pour améliore la vitesse et l'efficacité du transfert des données ; en utilisée MPLS pour offre une meilleur rapidité de commutation des paquets en effet la décision de routage se fait en analysant un label insérée par le protocole MPLS entre couche 2 et couche 3. Ainsi chaque routeur possédé une table associant un port / label d'entrée à un port / label de sortie.

La configuration de MPLS sur chaque routeur se fait en 3 étapes :

- en activée MPLS sur les Routeurs ; en activée MPLS sur les interfaces qu'on veut participer au domaine MPLS ; Le protocole LDP est activé par défaut dans cette version.

Cette partie se concentre sur la configuration des routeurs (P et PE), car elle donne les étapes nécessaires à suivre pour configurer MPLS sur notre réseau.

Dans les routeurs P, nous avons travaillé avec MPLS réside sur toutes les interfaces qui se connectent directement aux routeurs P. La configuration est la même pour les routeurs restants.

Nous devrons donc faire les commandes suivantes sur chaque routeur (interfaces backbone uniquement) du réseau backbone :

- « **mpls ip** »: pour l'activation d'MPLS.

- « **interface** » : pour l'activation d'MPLS sur l'interface

Sur la figure ci-dessous, nous montrons la configuration de MPLS :

```
R7(config)#interface GigabitEthernet 1/0
R7(config-if)#mpl
R7(config-if)#mpls ip
R7(config-if)#mpls ip
R7(config-if)#no sh
R7(config-if)#no shutdown
R7(config-if)#exit
R7(config)#
```

Figure 3. 15 : Configuration de MPLS

4.2.9.1 Interfaces MPLS après configuration

On met la commande « **Show mpls interfaces** » afin de voir les interfaces activées comme indiqué dans le document suivant :

```
interface GigabitEthernet1/0
 ip address 172.16.3.2 255.255.255.252
 negotiation auto
 mpls ip
!
interface GigabitEthernet2/0
 ip address 172.16.4.2 255.255.255.252
 negotiation auto
 mpls ip
!
interface GigabitEthernet3/0
 ip address 172.16.6.1 255.255.255.252
 negotiation auto
 mpls ip
!
```

Figure 3. 16 : Interfaces MPLS

Dans Figure (3.16), nous voyons l'activation des MPLS via l'interface 1/0 et l'interface 2/0, l'interface 3/0.

4.2.9.2 Vérification du fonctionnement du MPLS

Confirmer les sessions faites par LDP entre routeurs voisins à l'aide de la commande « **show tcp brief** » qui permet de vérifier les sessions LDP. Comme indiqué dans le document suivant :

```
R7#show tcp brief
TCB        Local Address               Foreign Address             (state)
68A9EAD4   10.10.10.5.55988           10.10.10.6.179               ESTAB
68A47B18   10.10.10.5.22579           10.10.10.2.646               ESTAB
R7#
```

```
R8#show tcp brief
TCB        Local Address               Foreign Address             (state)
68A48240   10.10.10.6.46196           10.10.10.4.646               ESTAB
68AAD04C   10.10.10.6.179             10.10.10.5.55988             ESTAB
R8#
```

Figure 3. 17 : Vérification des sessions LDP

Pour vérifier le fonctionnement du protocole MPLS/IP on utilise les deux commandes suivantes : La commande « **show mpls ldp neighbor** » et « **Show mpls forwardingtable** »

La première commande : « **Show mpls ldp neighbor** » qui découvrir les voisins crée par le protocole MPLS. Comme le montre la figure suivante :

```
R7#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.2:0; Local LDP Ident 10.10.10.5:0
        TCP connection: 10.10.10.2.646 - 10.10.10.5.22579
        State: Oper; Msgs sent/rcvd: 30/30; Downstream
        Up time: 00:13:56
        LDP discovery sources:
          GigabitEthernet1/0, Src IP addr: 172.16.5.1
        Addresses bound to peer LDP Ident:
          10.10.10.2      172.16.5.1      172.16.1.1      172.16.2.1
R7#
```

```
R8#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.4:0; Local LDP Ident 10.10.10.6:0
        TCP connection: 10.10.10.4.646 - 10.10.10.6.46196
        State: Oper; Msgs sent/rcvd: 31/30; Downstream
        Up time: 00:14:06
        LDP discovery sources:
          GigabitEthernet1/0, Src IP addr: 172.16.6.1
        Addresses bound to peer LDP Ident:
          10.10.10.4      172.16.3.2      172.16.4.2      172.16.6.1
R8#
```

Figure 3. 18 : Résultat du Voisinage MPLS

Pour la deuxième commande de protocole MPLS « **Show mpls forwardingtable** » qui voir l'affectation des labels aux adresses qui se trouvent dans la table FEC. Comme le montre la figure (3.19) :

```
R7#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  10.10.10.2/32    0             Gi1/0      172.16.5.1
17         Pop Label  172.16.1.0/30    0             Gi1/0      172.16.5.1
18         Pop Label  172.16.2.0/30    0             Gi1/0      172.16.5.1
19         19         10.10.10.4/32    0             Gi1/0      172.16.5.1
20         17         10.10.10.3/32    0             Gi1/0      172.16.5.1
21         20         172.16.6.0/30    0             Gi1/0      172.16.5.1
22         21         172.16.3.0/30    0             Gi1/0      172.16.5.1
23         18         172.16.4.0/30    0             Gi1/0      172.16.5.1
24         22         10.10.10.1/32    0             Gi1/0      172.16.5.1
25         23         10.10.10.6/32    0             Gi1/0      172.16.5.1
26         No Label   192.168.2.0/30[V]   \
                                       0             aggregate/alger
27         No Label   192.168.1.0/30[V]   \
                                       0             aggregate/blida
29         No Label   10.10.10.8/32[V] 0             Fa6/0      192.168.2.2
R7#
```

```
R8#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         16         10.10.10.5/32    0             Gi1/0      172.16.6.1
17         Pop Label  10.10.10.4/32    0             Gi1/0      172.16.6.1
18         17         10.10.10.3/32    0             Gi1/0      172.16.6.1
19         18         10.10.10.2/32    0             Gi1/0      172.16.6.1
20         22         10.10.10.1/32    0             Gi1/0      172.16.6.1
21         20         172.16.5.0/30    0             Gi1/0      172.16.6.1
22         21         172.16.2.0/30    0             Gi1/0      172.16.6.1
23         19         172.16.1.0/30    0             Gi1/0      172.16.6.1
24         Pop Label  172.16.3.0/30    0             Gi1/0      172.16.6.1
25         Pop Label  172.16.4.0/30    0             Gi1/0      172.16.6.1
26         No Label   192.168.10.0/30[V]   \
                                       0             aggregate/tizi
27         No Label   192.168.20.0/30[V]   \
                                       0             aggregate/medea
28         No Label   10.10.10.9/32[V] 0             Fa0/0      192.168.10.2
30         No Label   10.10.10.10/32[V]   \
                                       0             Fa6/0      192.168.20.2
R8#
```

Figure 3. 19 : Correspondance entre les labels et les Adresses IP

« **Show mpls ldp bindings** » la commande de vérification qui indique les labels affectés aux adresses réseau pour qu'ils puissent circuler dans le réseau IP-MPLS. Comme indiqué dans la figure suivant :

```
R7#show MPls LDp BIndings
  lib entry: 10.10.10.1/32, rev 22
        local binding:  label: 24
        remote binding: lsr: 10.10.10.2:0, label: 22
  lib entry: 10.10.10.2/32, rev 6
        local binding:  label: 16
        remote binding: lsr: 10.10.10.2:0, label: imp-null
  lib entry: 10.10.10.3/32, rev 15
        local binding:  label: 20
        remote binding: lsr: 10.10.10.2:0, label: 17
  lib entry: 10.10.10.4/32, rev 14
        local binding:  label: 19
        remote binding: lsr: 10.10.10.2:0, label: 19
  lib entry: 10.10.10.5/32, rev 2
        local binding:  label: imp-null
        remote binding: lsr: 10.10.10.2:0, label: 16
  lib entry: 10.10.10.6/32, rev 24
        local binding:  label: 25
        remote binding: lsr: 10.10.10.2:0, label: 23
  lib entry: 172.16.1.0/30, rev 8
        local binding:  label: 17
        remote binding: lsr: 10.10.10.2:0, label: imp-null
  lib entry: 172.16.2.0/30, rev 10
        local binding:  label: 18
        remote binding: lsr: 10.10.10.2:0, label: imp-null
  lib entry: 172.16.3.0/30, rev 19
        local binding:  label: 22
        remote binding: lsr: 10.10.10.2:0, label: 21
  lib entry: 172.16.4.0/30, rev 20
        local binding:  label: 23
        remote binding: lsr: 10.10.10.2:0, label: 18
  lib entry: 172.16.5.0/30, rev 4
        local binding:  label: imp-null
        remote binding: lsr: 10.10.10.2:0, label: imp-null
  lib entry: 172.16.6.0/30, rev 17
        local binding:  label: 21
        remote binding: lsr: 10.10.10.2:0, label: 20
R7#
```

```
R8#show mpls ldp bindings
  lib entry: 10.10.10.1/32, rev 14
        local binding:  label: 20
        remote binding: lsr: 10.10.10.4:0, label: 22
  lib entry: 10.10.10.2/32, rev 12
        local binding:  label: 19
        remote binding: lsr: 10.10.10.4:0, label: 18
  lib entry: 10.10.10.3/32, rev 10
        local binding:  label: 18
        remote binding: lsr: 10.10.10.4:0, label: 17
  lib entry: 10.10.10.4/32, rev 8
        local binding:  label: 17
        remote binding: lsr: 10.10.10.4:0, label: imp-null
  lib entry: 10.10.10.5/32, rev 6
        local binding:  label: 16
        remote binding: lsr: 10.10.10.4:0, label: 16
  lib entry: 10.10.10.6/32, rev 4
        local binding:  label: imp-null
        remote binding: lsr: 10.10.10.4:0, label: 23
  lib entry: 172.16.1.0/30, rev 20
        local binding:  label: 23
        remote binding: lsr: 10.10.10.4:0, label: 19
  lib entry: 172.16.2.0/30, rev 18
        local binding:  label: 22
        remote binding: lsr: 10.10.10.4:0, label: 21
  lib entry: 172.16.3.0/30, rev 22
        local binding:  label: 24
        remote binding: lsr: 10.10.10.4:0, label: imp-null
  lib entry: 172.16.4.0/30, rev 24
        local binding:  label: 25
        remote binding: lsr: 10.10.10.4:0, label: imp-null
  lib entry: 172.16.5.0/30, rev 16
        local binding:  label: 21
        remote binding: lsr: 10.10.10.4:0, label: 20
  lib entry: 172.16.6.0/30, rev 2
        local binding:  label: imp-null
        remote binding: lsr: 10.10.10.4:0, label: imp-null
R8#
```

Figure 3. 20 : Allocation des labels pour les réseaux

4.2.10 Réseaux privés virtuels

Dans cette section, nous allons créer, configurer et tester la table VRF.

4.2.10.1 Le concept VRF (Virtual Routing and Forwarding)

Les clients sont connectés les uns aux autres via des routeurs network Edge (PE) qui créent des réseaux VPN pour chaque client en créant des tables de routage distinctes. VRF permet de créer plusieurs tables de routage dans un seul routeur. Ces derniers sont scellés entre eux et chacun d'eux est généralement associé au client. Il est possible d'attribuer plusieurs fois la même adresse IP à différentes interfaces mettez-les dans différents VRF.

4.2.10.2 Création de VRF

Dans cette partie nous montrons les commandes nécessaires à la création de la table VRF.

```
R6(config)#mpls ldp password required
R6(config)#
*May 16 12:27:53.511: %LDP-5-NBRCHG: LDP Neighbor 192.168.20.1:0 (2) is DOWN (Session's MD5 password changed)
*May 16 12:27:53.515: %LDP-5-NBRCHG: LDP Neighbor 172.16.4.1:0 (3) is DOWN (Session's MD5 password changed)
R6(config)#mpl
R6(config)#mpls
*May 16 12:27:56.591: %LDP-4-PWD: MD5 protection is required for peer 172.16.3.1:0, no password configured
R6(config)#mpls ld
R6(config)#mpls ldp ne
R6(config)#mpls ldp neighbor 172.16.4.1 pa
R6(config)#mpls ldp neighbor 172.16.4.1 password 1010
R6(config)#
*May 16 12:28:24.707: %TCP-6-BADAUTH: No MD5 digest from 172.16.4.1(646) to 172.16.6.1(65027) tableid - 0
R6(config)#
*May 16 12:28:26.607: %TCP-6-BADAUTH: No MD5 digest from 172.16.4.1(646) to 172.16.6.1(65027) tableid - 0
*May 16 12:28:26.775: %TCP-6-BADAUTH: No MD5 digest from 172.16.4.1(646) to 172.16.6.1(65027) tableid - 0
R6(config)#
*May 16 12:28:26.903: %LDP-4-PWD: MD5 protection is required for peer 192.168.20.1:0, no password configured
R6(config)#
*May 16 12:28:32.887: %TCP-6-BADAUTH: No MD5 digest from 172.16.4.1(646) to 172.16.6.1(36900) tableid - 0
R6(config)#
*May 16 12:28:33.987: %TCP-6-BADAUTH: No MD5 digest from 172.16.4.1(646) to 172.16.6.1(36900) tableid - 0
*May 16 12:28:34.879: %TCP-6-BADAUTH: Invalid MD5 digest from 172.16.4.1(646) to 172.16.6.1(36900) (RST) tableid - 0
R6(config)#
*May 16 12:28:41.391: %TCP-6-BADAUTH: No MD5 digest from 172.16.4.1(646) to 172.16.6.1(57750) tableid - 0
R6(config)#
*May 16 12:28:43.459: %TCP-6-BADAUTH: No MD5 digest from 172.16.4.1(646) to 172.16.6.1(57750) tableid - 0
*May 16 12:28:43.463: %TCP-6-BADAUTH: No MD5 digest from 172.16.4.1(646) to 172.16.6.1(57750) tableid - 0
R6(config)#
```

Figure 3. 21 : Création de VRF

4.2.10.3 Configuration VRF coté PE-R7 et PE- R8

La configuration des VRF pour les clients (R9, R10, R11, R12) sur les routeurs PE-R7 et PE-R8, avec la command « **show running-config** ». Comme indiqué dans la figure suivant :

```
ip vrf alger
 rd 111:111
 route-target export 111:111
 route-target import 111:111
!
ip vrf blida
 rd 222:222
 route-target export 222:222
 route-target import 222:222
```

```
ip vrf medea
 rd 222:222
 route-target export 222:222
 route-target import 222:222
!
ip vrf tizi
 rd 111:111
 route-target export 111:111
 route-target import 111:111
```

Figure 3. 22 : Configuration des VRF de R7 et R8

Dans cette figure nous montrons que route-Target export et import entre Alger et tizi et entre blida et medea.

Rd : c'est les paramètres qui sont utilisées pour taguer les messages.

4.2.10.4 Vérification des VRF

La figure suivante présente la vérification des VRF dans les router R7 et R8, avec la commande « **show ip VRF** »

```
R7#show ip vrf
  Name                              Default RD          Interfaces
  alger                             111:111             Fa6/0
  blida                             222:222             Fa0/0
R7#
```

```
R8#show ip vrf
  Name                              Default RD          Interfaces
  medea                             222:222             Fa6/0
  tizi                              111:111             Fa0/0
R8#
```

Figure 3. 23 : Vérification des VRF pour R7 et R8

Dans la figure (3.23) nous montrons que dans le Edge 7, VRF Alger et activée via l'interface 6/0 et VRF Blida est activée via l'interface 0/0.

4.2.10.5 Tests Vérification de VRF

Sur la figure suivante nous montrons le Ping de tests de vérification de VRF tizi et medea.

```
R8#ping vrf tizi 10.10.10.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 196/519/1568 ms
R8#ping vrf 10 medea 10.10.10.10
vrf 10 does not exist
Translating "vrf"
```

Figure 3. 24 : Tests de vérification de VRF

Nous remarquons sur cette figure, la moyenne de ce Ping est transmis en 0.5 secondes.

4.2.11 Le concept MPLS – VPN

Pour assurer une connexion externe aux routeurs du réseau, le concept MPLS-VPN est configuré, mis en œuvre par l'autorité de protocole BGP.

4.2.11.1 Configuration de MP-BGP

Nous présentons la configuration de MP-BGP dans cette figure.

```
router rip
 version 2
 no auto-summary
 !
 address-family ipv4 vrf blida
  redistribute bgp 1 metric transparent
  network 192.168.1.0
  no auto-summary
 exit-address-family
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 10.10.10.6 remote-as 1
 neighbor 10.10.10.6 update-source Loopback5
 neighbor 10.10.10.6 next-hop-self
 !
 address-family vpnv4
  neighbor 10.10.10.6 activate
  neighbor 10.10.10.6 send-community both
 exit-address-family
 !
 address-family ipv4 vrf blida
  redistribute rip
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback5 force
!
!
control-plane
 --More--
```

Figure 3. 25 : Configuration de MP-BGP

4.3 Tests

Dans cette section nous donnons les tests de vérification de notre implémentation.

4.3.1 Vérification du fonctionnement de MP-BGP

Les commandes de test de performance appropriées doivent être appliquées au processus suivant :

« **Show ip bgp vpnv4 all** » : pour avoir les tables VPN-BGP qui sont directement liés au processus VRF et les routes empruntées par MP-BGP.

La Table de VPN-BGP pour R7 et R8 vérifiée, qui permet d'avoir le résultat suivant dans cette figure :

```
R7#show ip bgp vpnv4 all
BGP table version is 11, local router ID is 10.10.10.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 111:111 (default for vrf alger)
 *>  10.10.10.8/32    192.168.2.2              2         32768 ?
 *>i 10.10.10.9/32    10.10.10.6               2    100      0 ?
 *>  192.168.2.0/30   0.0.0.0                  0         32768 ?
 *>i 192.168.10.0/30  10.10.10.6               0    100      0 ?
Route Distinguisher: 222:222 (default for vrf blida)
 *>  10.10.10.7/32    192.168.1.2              1         32768 ?
 *>  192.168.1.0/30   0.0.0.0                  0         32768 ?
 *>i 192.168.20.0/30  10.10.10.6               0    100      0 ?
R7#
```

```
R8#show ip bgp vpnv4 all
BGP table version is 12, local router ID is 10.10.10.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 111:111 (default for vrf tizi)
 *>i 10.10.10.8/32    10.10.10.5               2    100      0 ?
 *>  10.10.10.9/32    192.168.10.2             2         32768 ?
 *>i 192.168.2.0/30   10.10.10.5               0    100      0 ?
 *>  192.168.10.0/30  0.0.0.0                  0         32768 ?
Route Distinguisher: 222:222 (default for vrf medea)
 *>i 10.10.10.7/32    10.10.10.5               1    100      0 ?
 *>i 192.168.1.0/30   10.10.10.5               0    100      0 ?
 *>  192.168.20.0/30  0.0.0.0                  0         32768 ?
R8#
```

Figure 3. 26 : Table de routage BGP VPNv4 pour R7 et R8

4.3.2 La table de routage VRF de R7 et R8

La table de routage du VRF de R7 avec la commande « **show ip route VRF blida** »

La table de routage du VRF de R8 avec la commande « **show ip route VRF medea** »

Comme indique dans les figures suivant :

```
R7#show ip route vrf bilda
% IP routing table vrf bilda does not exist
R7#show ip route vrf medea
% IP routing table vrf medea does not exist
R7#show ip route vrf blida

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

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 1 subnets
R        10.10.10.7 [120/1] via 192.168.1.2, 00:01:01, FastEthernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, FastEthernet0/0
L        192.168.1.1/32 is directly connected, FastEthernet0/0
      192.168.20.0/30 is subnetted, 1 subnets
B        192.168.20.0 [200/0] via 10.10.10.6, 00:05:33
R7#
```

```
R8#show ip route vrf medea

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

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 1 subnets
B        10.10.10.7 [200/1] via 10.10.10.5, 00:08:00
      192.168.1.0/30 is subnetted, 1 subnets
B        192.168.1.0 [200/0] via 10.10.10.5, 00:08:00
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/30 is directly connected, FastEthernet6/0
L        192.168.20.1/32 is directly connected, FastEthernet6/0
R8#
```

Figure 3. 27 : Résultat de la table de routage VRF client 9 pour PE-R7 et client 12 pour PE-R8

Le test des performances réseau appropriées peut être compensé en exécutant un test Ping client 11 à client 9 et client 11 à client 10, comme l'indique la figure suivante :

```
R11#
R11#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 736/1008/1248 ms
R11#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 864/1060/1200 ms
R11#
```

Figure 3. 28 : Résultats du test

Les résultats obtenus ont confirmé la bonne performance du réseau en cours de transmission pour les paquets transmis.

Ping : ce sont des paquets qui sont envoyés entre la source vers la destination pour vérifier la connectivité.

5. Conclusion

Dans ce chapitre, nous avons abordés le routage MPLS au sein du réseau DJEZZY par la simulation et la configuration du protocole MPLS via le simulateur GNS3 et mettre l'accent sur les concepts qui s'y rattachent selon les protocoles de routage internes et externes BGP, OSPF et RIP.

Tout au long de ce projet, nous avons effectué des contrôles et des tests entre les clients par les fonctions **Ping** et **traceroute** (Protocol ICMP) pour vérifie te confirmer le bon fonctionnement de la configuration sur les retours.

Conclusion générale

Le développement technologique a augmenté la capacité et la fonctionnalité des réseaux. MPLS est devenu une solution phare qui facilite l'intégration des technologies existantes dans le réseau fédérateur, permettant à l'administrateur de gérer entièrement le réseau.

Une étude biographique des concepts de base est faite dans le premier et le deuxième chapitre, ce qui nous permet de fournir une description des équipements de base du réseau informatique, des différents protocoles de routage, et des concepts de la technologie IP/MPLS, ce qui a aidé à comprendre et étudier le MPLS.

Le dernier chapitre est consacré à la mise en œuvre de ce réseau en configurant et en activant les protocoles OSPF et MPLS sur les interfaces de routeur respectives, puis en passant à la configuration de VRF sur le routeur de périphérie.

A la fin de notre projet, pour assurer la connexion externe des routeurs, MPLS-VPN est configuré sous l'autorité du protocole BGP. Nous avons testé le Ping entre les clients d'un site ver un site distant. Nous avons conclu que le trafic est correctement propagé en fonction des libellés.

Nous cherchons à améliorer notre réseau MPLS avec l'utilisation de nouvelles technologies de réseau, qui réduisent la congestion et la complexité et accélèrent le déploiement des services.

Enfin, nous pouvons dire que l'application MPLS est parfaite pour notre projet, mais ce n'est pas une solution idéale pour améliorer notre réseau, nous pouvons ouvrir de nouvelles voies de recherche. Soit de créer un autre protocole pouvant le remplacé, ou bien de configurer MPLS avec une autre application et améliorer la qualité de service (QoS).

Bibliographie

(AMINE, 2010) : Amine Amine, « Mise en œuvre d'un cœur de réseau IP/MPLS », Mémoire d'Ingéniorat, Université de Bechar, 2010.

(ATROUNE, 2021) : ATROUNE Sofia, AMER Salma « Mise en place d'une solution VPN », Mémoire Master, Université Akli Mohand Oulhadj Bouira, 2021.

(BELAID, 2011) : BELAID Nassima, ARKOUB Chabha, « Services d'accélération des applications et optimisation des liens WAN (WAAS : Wide Area Application services) au niveau de la CNAS d'Alger », Mémoire Master, UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU, 2011.

(BERKANI, 2018) : Randa BERKANI, « Etude et simulation d'un réseau IP-MPLS sous GNS3 », Mémoire Master, Université Mouloud Mammeri de Tizi-Ouzou, 2018.

(BENISSE, 2009) : Mohamed Taib BENISSE, « TRANSMISSION MÉDIA SUR LES RÉSEAUX IP EN UTILISANT LES PROTOCOLES SIP ET IAX », Mémoire de Maîtrise Electronique, UNIVERSITÉ DU QUÉBEC, 2009.

(BOUDOUR ,2017) : BOUDOUR Ouissem-eddine Amir, « Conception et implémentation d'un outil de simulation de la QoS dans un réseau IP », Mémoire Master, UNIVERSITE MOHAMED BOUDIAF - M'SILA, 2017.

(BOUZIANE, 2021) : Dalila Bouziane & Halima Baoudj, « Etude et modélisation des congestions dans les réseaux MPLS », Mémoire Master, UNIVERSITE KASDI-MERBAH OUARGLA, 2021.

(BELAID, 2018) : BELAID El-Hadi, BENEDINE Mahdi, « Extension du réseau MPLS via la technologie VSAT », Mémoire Master, Université Mouloud Mammeri de Tizi-Ouzou, 2018.

(BELGHERBI, 2020) Belgherbi Zineddine, Simulation sous GNS3 d'une Solution Réseau Intégrée Application à l'université 8 Mai 1945, Guelma, Mémoire Master, Université de Guelma, 2020.

(BOUDERRA, 2021) : BOUDERRA Nesrine, BOUARRACHE Wisseme, « Evaluation de la Qualité de Service de la Voix IP sur un réseau MPLS », Mémoire Master, UNIVERSITE M'HAMED BOUGARA-BOUMERDES, 2021.

(DELMI, 2020) : DELMI Youssouf, « MPLS (Multi prortocol Label Switching) Applications », Mémoire Master, Université Abdelhamid Ibn Badis Mostaganem, 2020.

(FRAMEIP, 2023) : FRAMEIP.COM Partage des connaissances du monde TCP/IP. Lien : https://www.frameip.com/mpls/ [en ligne] : 01/06/2023.

(Fireware, 2023) : A propos du Protocole RIP et RIPng (Routing Information Protocol), Fireware help, lien: https://www.watchguard.com/help/docs/fireware/12/fr-FR/Content/frFR/dynamicrouting/rip_about_c.html#:~:text=Le%20protocole%20RIP%20(Routing%20Information,r%C3%A9seau%20%C3%A9tendu%20priv%C3%A9%20(WAN). [en ligne] : 13/06/2023.

(GADOUM, 2012) : GADOUM Karim, AZOUAOUI Sofiane, Mémoire Master, « Mise en place d'une solution VoIP à base de serveur Asterisk », UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU, 2012.

(GHANIA, 2019) : Mohammed Nafaa GHANIA, Mohamed Redha KORICHI, Mémoire Master, « Vers algorithme optimal pour la gestion de la congestion dans les réseaux MPLS», UNIVERSITE KASDI-MERBAH OUARGLA, 2019.

(HAMAMI, 2021) : HAMAMI Nadjet, BOUKSANI Siham, Mémoire Master, « Etude et simulation d'un réseau IP-MPLS sous GNS3 », UNIVERSITE M'HAMED BOUGARA-BOUMERDES,2021.

(Howard ,2023) : Howard, Qu'est-ce que le Protocole SNMP et Comment Ça Marche ?, FS.com, Lien : https://community.fs.com/fr/blog/understanding-snmp.html [en ligne]: 01/06/2023.

(KNOW, 2023) : Know-how, SCTP (Stream control transmission protocol) : le protocole de transport fiable axé sur les messages, Produits IONOS. Lien : https://www.ionos.fr/digitalguide/serveur/know-how/sctp/ [en linge] : 01/06/2023.

(Marot, 2023): R. Marot, Architecture MPLS, Dominique Revuz, Consulté en 2023 :Lien : http://igm.univ-mlv.fr/~dr/XPOSE2006/marot/architecture.html#:~:text=Il%20existe%20deux%20modes%20de,label%20pour%20la%20FEC%20d%C3%A9couverte.

(MEGRI, 2015) : MEGRI Hmanou, SALHI Noureddine, « Etude, Conception et Evaluation d'une Architecture MPLS/VPN Désignée pour une Infrastructure Operateur », Mémoire Master, Université A. MIRA – BEJAIA, 2015.

(MOKHTARI, 2021) : Mokhtari Abdelghani Issam Eddine, Bessam Wassim Ibrahim, Mémoire Master, « Implémentation de la VoIP sur une architecture MPLS/VPN», Université – Ain Temouchent- Belhadj Bouchaib, 2021.

(NATAF, 2007) : Sarah Nataf, Bruno Decraene « Haute disponibilité dans les réseaux IP», Technique de l'ingénieur, 2007.

(OLIVIER, 2006) : OLIVIER TRUONGr, « Etude et développement d'outils d'optimisation de gestion de services dans les réseaux MPLS», Mémoire Master, ÉCOLE DE TECHNOLOGIE SUPÉRIEURE UNIVERSITÉ DU QUÉBEC, 2006.

(Rachdi ,2007) : Mohamed Anouar Rachdi, «Optimisation des ressources de réseaux hétérogène avec cœur de réseau MPLS », Thèse de Doctorat,- LAAS-CNRS à Toulouse, 2007.

(RAHANTANIRINA, 2016): RAHANTANIRINA Odile Samoella, «PERFORMANCE VPN – MPLS, RAHAN », Mémoire de Licence, UNIVERSITE D'ANTANANARIVO, 2016.

(RAHIL, 2022) : D.S. RAHIL, « Routage de segments sur un réseau IP-MPLS », Mémoire Master, UNIVERSITE M'HAMED BOUGARA-BOUMERDES, 2022.

(RAVOAVAHY, 2013) : RAVOAVAHY Andriamparany Arnaud, « ANALYSE DE PERFORMANCE DE LA VOIP SUR UN BACKBONE MPLS AVEC TRAFFIC ENGINEERING », Mémoire Master, UNIVERSITE D'ANTANANARIVO, ECOLE SUPERIEURE POLYTECHNIQUE, 2013.

(Ramaharobandro, 2013) : Ramaharobandro Rahasina Fenomanjato Mariah, « ETUDE DES PERFORMANCES DES MECANISMES DE QUALITE DE SERVICE DANS UN

RESEAU MPLS AVEC TRAFFIC ENGINEERING», Mémoire Master, UNIVERSITE D'ANTANANARIVO, 2013.

(RAJONIAINA, 2018) : RAJONIAINA Léonard Ismaël, « CONTRIBUTION A LA MODELISATION DES ROUTEURS MPLS PAR LES RESEAUX DE PETRI », Mémoire Master, UNIVERSITE D'ANTANANARIVO, 2018.

(REDACTION, 2023 a): La Rédaction TechTarget, DEFINITION Routage et transfert virtuels (virtual routing and forwarding, VRF), TechTarget. Lien: https://www.lemagit.fr/definition/Routage-et-transfert-virtuels-virtual-routing-and-forwarding-VRF [en ligne]: 01/04/2023.

(REDACTION, 2023 b) : La Rédaction TechTarget, DEFINITION OSPF, TechTarget. Lien :

https://www.lemagit.fr/definition/OSPF#:~:text=Si%20les%20routeurs%20connectent%20des,une%20s%C3%A9rie%20de%20r%C3%A9seaux%20connect%C3%A9s [en linge] : 01/04/2023.

(SAFI, 2010) Safi Mohamed, Djamila Sahraoui, Filtrage des paquets TCP/IP, Mémoire Licence, Université de Tlemcen, 2010.

(SANTOS, 2013) : Santos Hugo Antonio da Costa Dias dos, Jeremias Sara Caridade Maria, « Conception et réalisation d'une application de surveillance réseau basée sur SNMP », Mémoire Master, Université Mouloud Mammeri Tizi-Ouzou, 2013.

(SEBASTIEN, 2023) : Sébastien Adam, Les adresses particulières, lien : https://www.sebastienadam.be/connaissances/cours/adressage_ip/les_adresses_particulieres.php [en linge]: 01/06/2023.

(SOULAGES, 2023) D. Soulages, Introduction WAN (Wide Area Network), Plateforme de formation certifiante, en ligne et présentielle, . Lien : https://formip.com/introduction-wan-wide-area-network/ [en ligne] :31/05/2023

(TEBINA, 2020) : TEBINA Randa, Mémoire Master, « Conception d'une interface graphique sous Python en vue du choix d'un support de transmission », Université Mohamed Khider de Biskra, 2020.

(WILLIAM, 2009) : William Landry SIME SIME, « Mise en place d'une architecture VPN MPLS avec gestion du temps de connexion et de la bande passante utilisateur », Mémoire Master, Institut d'ingénierie d'informatique de Limoge, Administration systèmes réseaux 2009.

(ZAIDI, 2022) : ZAIDI Mohamed Arysse, « Mise en place d'un réseau IP/MPLS et l'intégration d'une plateforme Web pour la gestion et l'exploitation du réseau d'accès 2G 3G 4G», Mémoire d'ingéniorat, Ecole Nationale Polytechnique, 2022.

(ZIED, 2010) : ZIED NAAS, « ÉTUDE DE L'ÉQUITÉ DU PROTOCOLE TCP DANS LES RÉSEAUX MULTI-SAUT», MAÎTRISE EN GÉNIE CONCENTRATION RÉSEAUX DE TÉLÉCOMMUNICATIONS, UNIVERSITÉ DU QUÉBEC, 2010.

(ZERROUKI, 2019): ZERROUKI.H ADJABI.M, Utilisation de la technologie MPLS dans le réseau 4G, Mémoire Master, UNIVRESITE ZIANE ACHOUR DJELFA 2019.

(ZOUAOUI, 2012) : Siham ZOUAOUI, « Implémentation et validation de la pile TCP/IP de Micro chip sur un dsPIC », Mémoire Master, UNIVERSITE DE M'SILA, 2012.