République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université de M'hamed Bougara de Boumerdes

Faculté des sciences

Département d'informatique

Mémoire de fin d'études en vue de l'obtention du diplôme de Master

Spécialité : Ingénierie du logiciel et traitement de l'information / Technologies de l'information

Thème :

Étude et implémentation du Segment Routing sur un réseau IP/MPLS

Auteurs :

Amina GRINE

Radia BOURAIB

Soutenu le 16/11/2020 devant le jury composé de :

Président : M. Cheikh Salmi

Examinateur : M. Redouane Siaci

Encadreur : M. Abdelhak Mesbah

Promoteur : M. Rochdi Benlaksira

Année universitaire : 2019/2020

« La vraie nouveauté naît toujours dans le retour aux sources. »

Edgar Morin

Résumé

Les évolutions technologiques ont entraîné une explosion de données et une grande variabilité des trafics ce qui a amené les opérateurs à suivre le développement pour profiter des meilleures technologies et offrir ainsi un meilleur service à leurs abonnés.

La nouvelle technologie du Segment Routing gagne en popularité notamment grâce à sa capacité d'optimiser le réseau avec les différentes applications qu'elle propose en termes de protection rapide de lien ou de noeud, d'ingénierie de trafic, d'équilibrage de charge, d'établissement de tunnels VPN et de simplification du plan de contrôle.

Elle vise principalement à surmonter les limitations imposées par les protocoles de signalisation du MPLS en réduisant considérablement les informations d'état dans les nœuds car elle est basée sur le concept de routage source, où les nœuds d'entrée programment le chemin que les paquets doivent suivre en insérant une séquence d'instructions appelées segments dans l'en-tête des paquets, éliminant ainsi le besoin de créer et maintenir des états sur les autres noeuds du réseau.

Dans le cadre de ce travail, il est question d'étudier, réaliser et démontrer une migration sans impact du réseau MPLS de l'opérateur mobile Mobilis vers le Segment Routing puis d'introduire un contrôleur SDN et le combiner avec le Segment Routing pour résoudre les problèmes d'ingénierie de trafic dont souffrait le MPLS et permettre ainsi d'utiliser optimalement les liens du réseau et avoir plus de contrôle et de visibilité du réseau à l'ère du déluge de données.

Mots clés : Segment Routing, MPLS, Ingénierie de trafic, SDN, VPN, TI-LFA.

Abstract

Technological developments are generating an explosion of data and a high traffic variability which led operators to follow the development in order to benefit of the best technologies and offer better service to their clients.

Segment Routing is gaining popularity especially thanks to its ability to optimize the network with the various applications it offers in terms of rapid link or node protection, traffic engineering, load balancing, establishment of VPN tunnels and control plane simplification.

The first goal of Segment Routing is to overcome the limitations imposed by MPLS signaling protocols by drastically reducing state information in nodes because it's based on the concept of source routing where ingress nodes direct packets through paths using a sequence of instructions called segments placed in the header of the packet, eliminating the need to create and maintain states on the other nodes of the network.

As part of this work, we studied, implemented and demonstrated a smooth migration from the MPLS network of the mobile operator Mobilis to the Segment Routing. We also introduced an SDN controller in the network and combined it with Segment Routing to solve the traffic engineering problems suffered by MPLS and thus allow optimal use of the links and have more control and visibility of the netowrk in the era of data deluge.

Keywords : Segment Routing, MPLS, Traffic Engineering, SDN, VPN, TI-LFA.

Remerciements

Nous tenons à exprimer toute notre reconnaissance et notre gratitude à notre promoteur Monsieur Rochdi Benlaksira pour nous avoir proposé ce sujet de mémoire et pour nous avoir permis de réaliser l'ensemble de ces travaux dans d'excellentes conditions.

Nous tenons à remercier vivement notre encadreur Monsieur Abdelhak Mesbah pour ses précieux conseils et remarques, la qualité de son encadrement et sa disponibilité pendant toute la durée de la préparation du mémoire.

Nous tenons également à remercier tout particulièrement Monsieur Kamel Hassani pour tout le temps qu'il nous a consacré, son orientation, son soutien infallible et ses importantes contributions qui ont fait de ce travail ce qu'il est aujourd'hui.

Nous remercions enfin tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Dédicaces

Je dédie ce travail à mes chers parents, qui sont les personnes qui m'inspirent le plus. Aucun mot ne suffit pour exprimer mon incommensurable amour et ma gratitude envers eux, je leur serais éternellement reconnaissante pour leur éducation, pour tout ce qu'ils m'ont appris, pour les valeurs qu'ils m'ont transmises, pour les efforts et les sacrifices qu'ils ont fait, pour leur soutien sans failles que qui me pousse à croire en mes rêves et pour me donner toujours de la force pour persévérer.

Je le dédie aussi à mon frère Abdelkrim qui occupe une place unique dans ma vie ainsi qu'à ma très chère grand-mère et à la mémoire de mes grands-parents et à toute ma famille que j'aime énormément.

Je le dédie également à ma binôme Radia qui mérite le titre de la meilleure binôme du monde. La collaboration avec elle a été absolument agréable, efficace, productive, organisée et d'une fluidité remarquable grâce à ses impressionnantes et particulières compétences.

Amina

Dédicaces

Je dédie ce modeste et humble travail ;

A mes très chers parents qui m'ont toujours encouragée à aller de l'avant. Pour leurs patience, présence, amour et bienveillance. Aucun hommage ne serait suffisant pour exprimer mon respect et ma gratitude pour les sacrifices qu'ils ont consentis pour mon parcours d'éducation et mon contentement. Que Dieu le tout puissant vous garde, vous protège et puisse vous accorder longue vie, bonheur et santé.

A mon frère Billel et ma sœur Yasmine. Pour leurs soutient, présence et patience.

Je tiens à le dédier plus particulièrement à ma binôme Amina, que je n'aurais pas pu espérer mieux qu'elle pour m'assister dans cet accomplissement et sans qui ce travail n'aurait jamais été pareil.

A ma famille et à toute personne qui m'est chère.

Radia

Table des matières

Table des figures

Liste des tableaux

Acronymes

ABR Area Border Router.

API Application Programming Interface.

ARPA Advanced Research Projects Agency.

AS Autonomous System.

ASBR Autonomous System Boundary Router.

ATM Asynchronous Transfer Mode.

BDR Backup Designated Route.

BFD Bidirectional Forwarding Detection.

BGP Border Gateway Protocol.

BR Backbone Router.

CE Customer Edge.

CLNP Connectionless Network Protocol.

CR-LDP Constraint-Based LSP Setup using LDP.

CSPF Constrained Shortest Path First.

DLCI Data Link Connection Identifier.

DNS Domain Name System.

DR Designated Router.

E-BGP External Border Gateway Protocol.

ECMP Equal Cost Multiple Path.

EGP Exterior Gateway Protocol.

EVE-NG Emulated Virtual Environment Next Generation.

FEC Forward Equivalent Class.

FIB Forwarding Information Base.

FRR Fast ReRoute.

FTP File Transfer Protocol.

HTTP Hypertext Transfer Protocol.

I-BGP Internal Border Gateway Protocol.

ICMP Internet Control Message Protocol.

IETF Internet Engineering Task Force.

IGP Interior Gateway Protocol.

IP Internet Protocol.

IR Internal Router.

IS-IS Intermediate System to Intermediate System.

ISO International Organization for Standardization.

LAN Local Area Network.

LDP Label Distribution Protocol.

LER Label Edge Router.

LFA Loop free Alternate.

LFIB Label Forwarding Information Base.

LIB Label Information Base.

LSA Link State Advertisement.

LSDB Link-State Database.

LSP Label Switching Path.

LSR Label-switching router.

MAC Media Access Control.

MAN Metropolitan Area Network.

MPLS Multi Protocol Label Switching.

NETCONF Network Configuration.

NFV Network Function Virtualization.

NLRI Network Layer Reachability Information.

OSI Open Systems Interconnection.

OSPF Open Shortest Path First.

PCC Path Computation Client.

PCE Path Computation Element.

PCEP Path Computation Element Communication Protocol.

PHP Penultimate Hop Popping.

PVC Permanent virtual circuits.

QoS Quality of Service.

RD Route Distinguisher.

RIB Routing Information Base.

RIP Routing Information Protocol.

RLFA Remote Loop free Alternate.

RSVP-TE Resource Reservation Protocol Traffic Engineering.

RTT Round Trip Time.

S-BFC Seamless Bidirectional Forwarding Detection.

SDN Software-defined Networking.

SFC Service Function Chaining.

SID Segment Identifier.

SMPT Simple Mail Transfer Protocol.

SNMP Simple Network Management Protocol.

SPF Shortest Path First.

SPRING (Source Packet Routing in Networking.

SR Segment Routing.

SR-TE Segment Routing - Traffic Engineering.

SRGB Segment Routing Global Block.

SRLB Segment Routing Local Block.

SSH Secure Shell.

SUD Southbound Application Protocols.

SVC Switched virtual circuits.

TCP Transport Control Protocol.

TED Traffic Engineering Database.

TI-LFA Topology Independent-Loop-Free Alternate.

TTL Time to Live.

UDP User Datagram Protoco.

VCC Virtual Channel Connection.

VLSM Variable Length Subnet Mask.

VNI Visual Networking Index.

VPN Virtual Private Network.

VRF Virtual Routing and Forwarding.

WAN Wide Area Network.

Introduction générale

L'une des évolutions les plus passionnantes du 21e siècle est la révolution numérique. Avec la montée en puissance d'une génération férue de technologies tels que le streaming, le cloud, l'IoT, le big data, l'IPTV et la 5G, les opérateurs font face à une complexe équation dictée par un rythme effréné de l'augmentation du nombre d'internautes ce qui entraîne une forte variabilité des trafics et une explosion des données.

Les opérateurs algériens n'y échappent pas, les algériens sont de plus en plus connectés et exigent constamment un meilleur service réseau. Ainsi, une concurrence féroce s'est installée poussant les opérateurs à améliorer la qualité de leur réseau tout en cherchant à simplifier son fonctionnement et sa gestion sans pour autant flamber les coûts d'investissements.

La technologie du MPLS largement déployée et qui avait révolutionné les réseaux des opérateurs principalement grâce aux services qu'elle octroie notamment en terme de qualité de services et d'ingénierie de trafic, tend à arriver à ses limites, particulièrement à cause de la complexité des protocoles qu'elle utilise et des problèmes d'évolutivité liés.

D'autant plus, il est plus judicieux pour les opérateurs de se tourner vers une architecture centralisée et introduire un contrôleur qui constitue une brique essentielle de la structure des réseaux modernes. Il permet de pousser le niveau de l'intelligence du réseau et de le rendre plus agile, évolutif, programmable et dynamique.

Pour ces raisons, la nouvelle technologie Segment Routing a été conçue. Cette solution révolutionne en profondeur la conception du réseau des opérateurs en facilitant l'intégration du contrôleur SDN et en augmentant la capacité du réseau tout en rentabilisant l'utilisation des ressources existantes. En effet le Segment Routing peut être déployé sur deux plans de transfert existants à savoir MPLS et IPv6 ce qui protège les investissements d'hier et répond aux défis de demain.

Il s'appuie sur le routage source où le chemin que les paquets doivent suivre est spécifié à l'entrée du réseau sous forme d'une liste de segments, chaque segment contient une instruction que les routeurs du réseau doivent exécuter afin d'acheminer le paquet. Ils n'auront donc pas besoin de protocoles de signalisation et à calculer des étiquettes ou des tunnels et conserver leur état comme était le cas avec le MPLS.

Le travail présenté dans ce mémoire est né de la curiosité qu'a suscitée chez nous l'apparition

du Segment Routing dans le domaine des réseaux et c'est ce qui éclaire la raison de notre choix d'effectuer notre stage au sein de l'opérateur Mobilis qui justement s'intéresse à passer au Segment Routing afin de pallier les problèmes posés par le MPLS notamment la création de dizaines de milliers de chemins LSP difficiles à maintenir et qui consomment énormément de ressources, divulgués par la demande croissante et diverse des données.

L'objectif de ce mémoire est d'étudier en profondeur les technologies MPLS et Segment Routing puis de migrer du MPLS vers le Segment Routing et exploiter ses différentes applications qui permettront l'équilibrage de charge pour répartir le flux de données sur l'ensemble des liaisons disponibles, le calcul rapide des chemins en cas de panne d'un noeud ou d'un lien, la mise en place de VPN et l'ingénierie de trafic en introduisant un contrôleur SDN afin d'optimiser le calcul et l'utilisation des chemins pour éviter la saturation des liens tandis que d'autres liens sont soit sous-utilisé ou pas du tout utilisés. Et cela, sans la complexité des protocoles d'ingénierie de trafic du MPLS.

De plus, nous cherchons à migrer vers un réseau plus moderne et le Segment routing constitue la pierre angulaire des nouvelles technologies des réseaux de nouvelle génération.

Ce mémoire est subdivisé en quatre chapitres, le premier chapitre est dédié à la présentation de l'organisme d'accueil, à l'étude de l'existant, à la problématique et aux solutions retenues.

Le deuxième chapitre est relatif à la présentation des généralités sur les réseaux informatiques et à une étude fondamentale du MPLS, son architecture ainsi que les applications que propose cette technologie.

Le troisième chapitre est consacré à l'étude des concepts et du fonctionnement du Segment Routing avec une étude comparative avec le MPLS puis nous mettons les points sur les bénéfices qu'elle apporte pour les fournisseurs de service.

A partir des informations obtenues au cours de l'étude théorique, nous procédons à la phase de conception et d'implémentation de l'architecture du réseau qu'on détaillera en quatrième chapitre. Nous confirmerons l'efficacité de notre migration par une étude des résultats des performances du réseau obtenus avant et après la migration vers le Segment Routing.

Enfin, ce mémoire se termine par une conclusion générale qui dresse le bilan de notre contribution tout en proposant des perspectives d'avenir à notre travail.

Chapitre 1

Étude préalable

1.1 Introduction

Pour commencer ce mémoire et situer notre contexte d'étude, nous présentons, dans un premier temps, l'organisme d'accueil Mobilis, qui est l'un des principaux opérateurs mobiles en Algérie. Ensuite, nous étudions l'existant puis nous exposons la problématique en fonction de ce que nous aurons analysé ainsi que les solutions retenues qui répondront aux problèmes notés.

1.2 Présentation de l'organisme d'accueil

ATM (Algerie Telecom Mobile) Mobilis, filiale de l'opérateur de téléphonie Algérie Telecom, est le premier opérateur de téléphonie mobile en Algérie, il a vu le jour suite à l'ouverture du secteur des postes et des télécommunications en Algérie stipulée par la loi 2000-03 du 5 août 2000. Il est devenu ensuite autonome en août 2003.

Mobilis est le leader du marché de la téléphonie mobile en Algérie avec 18,1 millions d'abonnés et avec une part de 39,93 % en 2019. Il propose différents types de services tel que la téléphonie Mobile, l'internet Mobile, et les solutions pour les entreprises. La 4G de Mobilis couvre 32 Wilayas de l'Algérie, la 3G et la 2G couvrent 48 Wilayas. Il possède plus de 9000 stations de base, 178 agences, plus de 15000 points de vente agréés Mobilis et plus de 60.000 points de vente indirecte.

1.3 Étude de l'existant

Nous effectuons notre stage dans la sous-direction MPLS qui est chargée de gérer, maintenir et améliorer le réseau IP/MPLS de Mobilis et de définir et de piloter sa stratégie d'évolution.

Nous allons analyser et étudier le réseau IP/MPLS existant, dont l'architecture est illustrée

dans la figure 1.1, afin de déterminer les problèmes actuels et proposer les solutions adéquates.

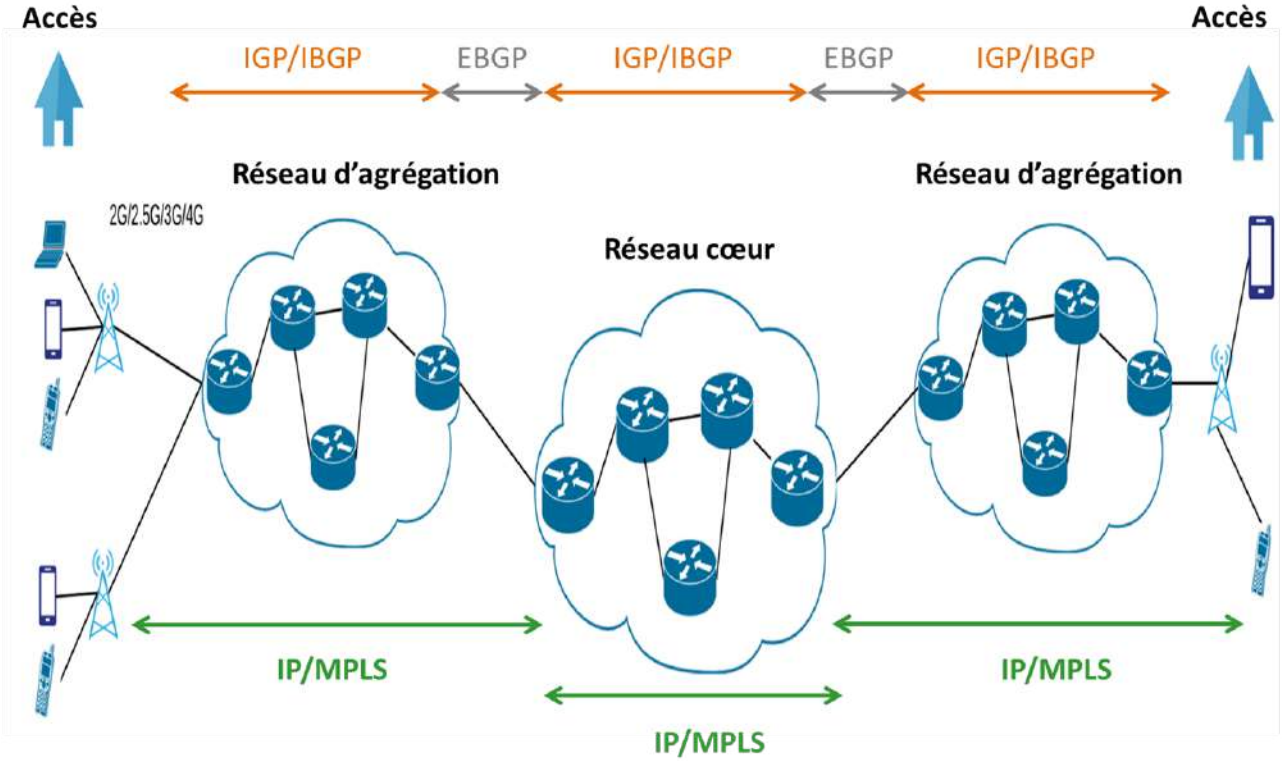


FIGURE 1.1 – Architecture du réseau de Mobilis

La hiérarchie du réseau de Mobilis comprend trois niveaux différents, chacun d'eux ayant une conception spécifique. Le premier niveau est le réseau d'accès qui représente la partie du réseau qui relie Mobilis à l'abonné. Il se charge de collecter le flux total d'informations provenant des abonnés connectés via la 2G, 2,5G, 3G ou 4G, puis de son transfert vers le réseau d'agrégation. Le deuxième niveau est le réseau d'agrégation, il regroupe l'ensemble du trafic d'une wilaya puis transfère cela au réseau cœur. Il y a donc 48 réseaux d'agrégation et ils constituent l'interface entre le réseau cœur et le réseau d'accès. Le troisième niveau est le réseau cœur, il est unique et mutualisé pour tous les autres réseaux, il représente le nœud central du réseau et fournit les nombreux services aux abonnés connectés via le réseau d'accès.

Les réseaux d'agrégation et le réseau coeur utilisent Open Shortest Path First (OSPF) et Intermediate System to Intermediate System (IS-IS) comme protocoles de routage interne, ainsi que le Internal Border Gateway Protocol (I-BGP). le Border Gateway Protocol (BGP) est utilisé comme protocole de routage externe, plus spécifiquement le External Border Gateway Protocol (E-BGP) qui permet aux différents AS de s'échanger les données. Le Multi Protocol Label Switching (MPLS) est utilisé comme protocole d'acheminement de données, ce qui permet à l'opérateur de créer des Virtual Private Network (VPN) pour les clients, d'assurer la qualité de service et d'utiliser l'ingénierie de traffic. Le Label Distribution Protocol (LDP) est utilisé comme protocole de distribution d'étiquettes MPLS et le Resource Reservation Protocol

Traffic Engineering (RSVP-TE) est utilisé comme protocole de distribution d'étiquettes pour l'ingénierie de trafic. Tous les termes introduits ci-dessus seront expliqués dans le chapitre 2 afin de détailler davantage les concepts.

1.4 Problématique

La technologie IP/MPLS utilisée actuellement au sein du réseau de MOBILS, se définit comme une technologie innovante dans le domaine des réseaux. Cependant cette technologie se voie comme étant complexe, difficile à mettre en place et réduite en terme d'évolutivité du fait qu'elle utilise des protocoles de signalisation lourds tels que RSVP-TE et LDP.
En effet, LDP ne permet pas l'ingénierie de trafic, de se fait lorsqu'un un lien est surchargé, il est quand même choisi pour transporter les données car c'est le chemin le plus court, en plus qu'il lui faut un temps non négligeable pour sa synchronisation avec IGP, entraînant ainsi une perte de paquets. De plus, la gestion des milliers d'étiquettes dans les bases de données LDP est complexe. De même, la configuration et la gestion des milliers de tunnels de RSVP-TE est encore plus complexe, RSVP-TE consomme une quantité non des moindres des ressources des nœuds notamment en stockage mémoire et cela pour maintenir les différents états des liens. Cela entraîne une congestion des noeuds après un redémarrage. Par conséquent le réseau ne peut être étendu étant donné que la capacité de mémoire d'un noeud est limitée. D'autant plus que ce protocole ne permet l'équilibrage de charge.

Avec l'ère du temps, Mobilis voit son nombre d'abonné en hausse continue, entraînant une augmentation exponentielle de la quantité de données que doit transporter le réseau, mais encore, des services de nouvelle génération sont apparues, tel que le streaming vidéo qui ne tolère guère des délais et des erreurs de transmissions et nécessite un réseau stable pour l'acheminement des paquets. Ces nouvelles contraintes mettent Mobilis devant de réelles difficultés. Les routeurs ont besoin de plus de puissance et multiplier leur nombre inflige des dépenses excessives avec une gestion complexe du réseau. De plus, la forte variabilité des trafics et la diversité de services nécessite une issue efficace pour assurer une qualité de service et une ingénierie de trafic plus fiables.

D'autre part, avec l'évènement imminent de la 5G, Mobilis doit optimiser son infrastructure et utiliser des solutions qui accompagnent une telle technologie. Dès lors, l'adoption du Software-defined Networking (SDN) qui est l'une des principales technologies qui structurent la 5G, est incontestablement inévitable.
Cela dit, pour fidéliser leurs clientèles et attirer un plus grand nombre, Mobilis se voit dans l'obligation de trouver une solution afin de subvenir à leurs besoins sans pour autant apporter de grande modification dans le réseau opérationnel afin de le simplifier tout en garantissant une meilleur qualité de service et sans pour autant perturber ou créer des points de vulnérabilité.

1.5 Solutions

Afin de pouvoir satisfaire les besoins des abonnés de Mobilis et de répondre à un grand nombre d'exigences et d'attentes plus élevées en matière de qualité tout en rentabilisant les ressources existantes, ce qui passe nécessairement par une optimisation du routage des trafics, nous utiliserons la technologie du Segment Routing qui permet d'optimiser et d'accroître les capacités du réseau. Elle peut être implémentée sur le plan de donnés MPLS existant sans changement matériel et elle simplifie le déploiement et la configuration de services tels que le réacheminement rapide, le Traffic engineering et les VPN, en supprimant les protocoles de distributions d'étiquettes LDP et RSVP-TE, éliminant ainsi toutes les complications liées. Dès lors, son principe est d'éviter autant que possible de déployer de nouveaux protocoles et d'étendre les protocoles déjà déployés (OSPF, ISIS et BGP)

De surcroît, le Segment Routing offre une architecture qui facilite l'intégration du contrôleur SDN qui est l'une des pièces maîtresses qui permettront aux opérateurs d'exploiter le potentiel de l'infrastructure et permettre d'optimiser les débits au maximum tout en gardant une importante visibilité sur le comportement de leurs équipements réseau.

Nous concluons que la solution choisie correspond aux exigences citées dans la problématique pour les raisons suivantes :

- Ne nécessite aucun changement matériel, elle est donc pas coûteuse.
- Diminue le nombre de protocoles utilisés.
- Élimine les millions d'étiquettes LDP et les millions de tunnels RSVP-TE.
- Permet une ingénierie de traffic plus appropriée.
- Assure un réacheminement ultra rapide.
- Prend en charge l'équilibrage de charge.
- Propose d'autres applications intéressantes pour les réseaux modernes tel que le Service Function Chaining (SFC)

Au cours de ce projet, il serait question de migrer d'un réseau IP/MPLS vers un réseau Segment Routing (SR) puis d'introduire un contrôleur SDN qui calcule les chemins selon l'état du réseau et les contraintes en temps réel, en plus de configurer le réacheminement rapide et le ECMP et les VPN.

Or, il serait intéressant de vérifier la pertinence de cette solution, pour cette raison, nous comparerons les performances du réseau avant et après l'adoption du SR.

Notre projet se situe donc dans le domaine du IP/MPLS, de la QoS, de l'Ingénierie de Trafic et plus particulièrement de la technologie Segment Routing.

1.6 Conclusion

Au cours de ce chapitre nous avons présenté notre cadre d'étude, étudié l'existant, posé la problématique et retenu des solutions pour pouvoir passer à l'étape de l'état de l'art dans le chapitre suivant.

Chapitre 2

Réseaux IP/MPLS

2.1 Introduction

Les réseaux ne cessent d'évoluer, notamment dans cette dernière décennie. Cependant cette évolution n'est pas radicale, les réseaux s'appuient toujours sur leurs bases et principes. Nous allons présenter dans ce chapitre des notions essentielles sur les réseaux, nécessaires à la compréhension des travaux présentés dans ce mémoire.

Nous commençons par un tour d'horizon sur les principales notions du réseau après nous poursuivons avec la présentation des deux protocoles de routage dynamique à savoir Interior Gateway Protocol (IGP) et Exterior Gateway Protocol (EGP), qui vont être régulièrement employés dans la suite du mémoire. Ensuite nous évoquons les réseaux étendus puis nous nous concentrons sur la technologie MPLS, en expliquant son principe de fonctionnement et en détaillant les protocoles de distribution d'étiquettes LDP et RSVP-TE. Nous abordons par la suite quelques notions primordiales sur le traffic engineering et la qualité de service dans les réseaux.

2.2 Généralités sur les réseaux

2.2.1 Définition d'un réseau

Un réseau est un graphe dirigé T (N, E) constitué d'un ensemble de nœuds N et d'un ensemble d'arcs dirigés E. Chaque arc (u, v) $\in$ E est associé à une capacité c. Les nœuds et les arcs représentent respectivement les routeurs et les liaisons de ce réseau. La capacité d'un arc est sa bande passante, c'est-à-dire la quantité maximale de bits que la liaison peut fournir par seconde.

En d'autres termes, un réseau connecte des périphériques afin qu'ils puissent communiquer entre eux. Il est composé de périphériques de terminaison qui sont des éléments en bout de chaîne comme des serveurs, des PC, des capteurs ou des imprimantes et de périphériques d'in-

terconnexion qui sont les composantes qui connectent les équipements sur le réseau. Il permet de faire circuler des données sous forme binaire et ainsi d'échanger du texte, des images, de la vidéo ou du son entre chaque équipement selon des règles et des protocoles [1]bien définis.

2.2.2 Le modèle OSI

2.2.2.1 Définition

Au début, le développent des réseaux était chaotique, chaque fournisseur avait sa propre solution propriétaire, le soucis avec ça c'était que la solution d'un fournisseur n'était pas compatible avec celle d'un autre fournisseur, et c'est là que l'idée du modèle OSI est née.
Le modèle OSI ou communication entre systèmes ouverts a été établit par International Organization for Standardization (ISO) en 1984 [2]. Il fournit des règles et des standards internationaux qui permettent à n'importe quel système qui obéit à ces protocoles de communiquer avec n'importe quels autres systèmes les utilisant aussi. Dans le modèle OSI, ces règles sont séparées en sept couches communicantes, chaque couche s'occupe d'un aspect différent de la communication.

2.2.2.2 Les couches du modèle OSI

1. **Couche physique** permet la connexion physique entre deux instances communicantes. Autrement dit, elle gère la communication avec l'interface physique afin de faire transiter ou récupérer des données sur le support de transmission.
2. **Couche liaison de données** s'occupe de la bonne transmission de l'information entre les noeuds via le support, en assurant la gestion des erreurs de transmission et la synchronisation des données, et c'est à ce niveau qu'a lieu les adresses physique Media Access Control (MAC) et les trames Ethernet.
3. **Couche réseau** gère l'adressage logique Internet Protocol (IP) des terminaux et le routage sur le réseau, elle est chargée de déterminer le choix de la route entre les noeuds afin de transmettre de façon indépendante l'information ou les différents paquets la constituants en prenant en compte en temps réel le trafic, elle assure aussi un certain nombre de contrôle de congestion qui ne sont pas assurer par la couche liaison.
4. **Couche transport** supervise le découpage et le ré-assemblage de l'information en paquets, contrôlant ainsi la cohérence de la transmission de l'information, de l'émetteur vers le destinataire, c'est ici qu'a lieu les protocoles Transport Control Protocol (TCP) et User Datagram Protoco (UDP).

1. Un protocole est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

5. **Couche session** prend en charge l'établissent, la gestion et la terminaison des sessions entre deux hôtes, permettant ainsi un réel suivie de dialogue.
6. **Couche présentation** veille à ce que les informations soient lisibles pour la couche application, elle assure ainsi de bien structurer et de convertir les données échangées ainsi que leur syntaxe, afin de garantir la communication entre les noeuds.
7. **Couche application** concerne toutes les applications que l'on utilise tel que le courrier électronique, le transfert de fichier..etc. C'est le point d'accès des applications aux réseaux. Parmi les protocoles de couche application les plus connus on trouve : Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMPT), Telnet, Domain Name System (DNS), Simple Network Management Protocol (SNMP)...

2.2.3 Le modèle TCP/IP

2.2.3.1 Définition

Le modèle TCP/IP a été conçu et développé par Advanced Research Projects Agency (ARPA) l'agence de recherche du ministère américain de la défense dans les années 70 [4]. C'est une version abrégée du modèle OSI, lui aussi sépare la communication en plusieurs couches sauf qu'il ne comprend que quatre.

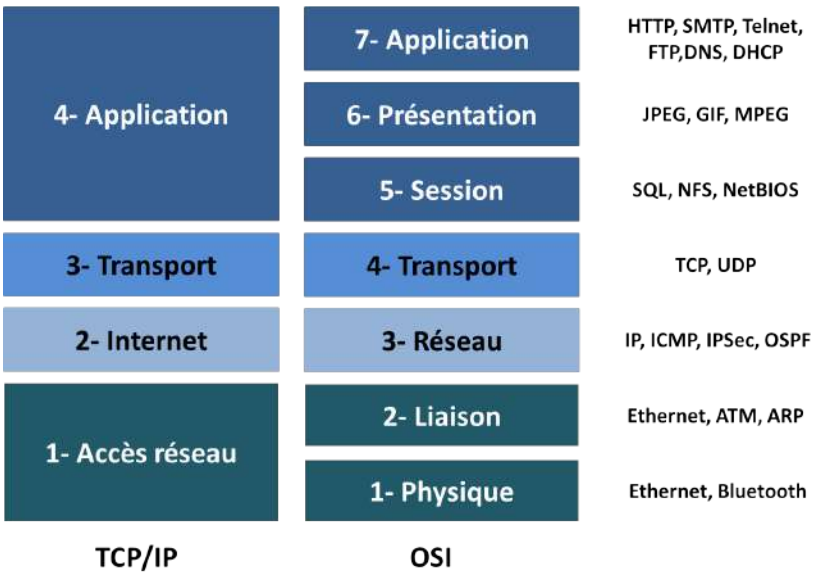


FIGURE 2.1 – Modèles OSI et TCP/IP

2.2.3.2 Les couches du modèle TCP/IP

1. **Couche accès réseau** ou couche liaison, elle est équivalente aux couches physique et liaison du modèle OSI.

2. **Couche internet**, elle correspond à la couche réseau du modèle OSI.
3. **Couche transport**, elle correspond à la couche transport du modèle OSI.
4. **Couche application**, elle regroupe les couches session, présentation et application du modèle OSI.

La figure 2.1 représente les deux modèles OSI et TCP/IP ainsi que certains des protocoles de chaque couche. Au cours de ce mémoire nous utiliserons le modèle OSI comme référence.

2.3 Protocole IP et Routage

2.3.1 Le protocole IP

Le protocole IP est un protocole qui réside dans la couche réseau et qui constitue la base fondamentale d'internet avec le protocole de transport TCP. Il définit une structure qui résume les informations sur la source et la destination des données à envoyer et il est principalement responsable de l'adressage et de la fragmentation des paquets.

Le paquet IP est formé de deux parties, la première est un en-tête d'une taille variable où sont inscrites les informations nécessaires à la transmission du paquet et la seconde est le champ de données.

Le protocole IP transmet le paquet en utilisant l'adresse de destination. Il est parfois nécessaire de diviser le paquet s'il est trop long pour être transmis en un seul paquet puis rassemblé à son arrivée. Mais le flux de données ne suit pas forcement le même ordre que celui dans lequel il a été envoyé, c'est donc un protocole non orienté connexion [36].

IPv4 est la version la plus utilisée de IP et IPv6 est son successeur en cours de déploiement.

2.3.2 Le routage

Le routage désigne le processus selon lequel les systèmes identifient et déterminent le meilleur chemin que suivent les paquets envoyés à une adresse selon une métrique qui peut être le nombre de sauts, le coût, le délai, ou autre. Ensuite le processus d'acheminement se charge de conduire les paquets selon le chemin obtenu grâce au routage.
Pour effectuer le routage un matériel réseau appelé routeur est utilisé, il rassemble et conserve les informations de routage dans une table de routage avec une entrée pour chaque route identifiée, le routeur s'appuie sur cette table pour savoir par quelle interface transmettre les paquets.

La figure 2.2 montre un exemple typique de ce à quoi pourrait ressembler une table de routage sur un routeur et les champs de ses colonnes sont expliqués en ce qui suit :

— **Destination réseau :** Affiche l'adresse IP des réseaux de destination.
— **Masque réseau :** Indique le masque de sous-réseau de destination.
— **Adresse passerelle :** L'adresse du routeur qui sera traversée par le paquet avant d'atteindre sa destination.

Destination	Masque	Passerelle	Interface	Métrique
10.0.0.0	255.255.255.0	10.1.1.1	eth0/0	4000
192.168.0.0	255.255.0.0	10.2.2.2	eth0/1	4001
10.8.8.0	255.255.255.0	10.3.3.3	eth1/0	4002

FIGURE 2.2 – Table de routage

— **Interface :** Interface réseau de sortie que le dispositif doit utiliser pour envoyer le paquet vers le saut suivant.
— **Métrique :** Représente une échelle de mesure, il s'agit de l'élément qui permettra au routeur de choisir une route plutôt qu'une autre. Plus cet indice est faible, plus la route semblera fiable pour le routeur.

2.3.3 Routage statique

Dans le routage statique, les tables de routage doivent être maintenues et mises à jour manuellement par l'administrateur réseau chaque fois qu'un changement de topologie du réseau intervient.

2.3.4 Routage Dynamique

Dans le routage dynamique, une table de routage est bâtie et maintenue automatiquement par le protocole de routage administré par l'administrateur. Ces protocoles sont notamment utilisés pour établir et maintenir les routes entre les nœuds, découvrir de nouveaux réseaux distants, actualiser les informations de routage et choisir le meilleur chemin vers les destinations. La figure 2.3 classifie les protocoles de routages qui seront décrits par la suite.

2.3.5 Système autonome

Avant d'aborder les protocoles de routages, nous allons définir la notion de système autonome Autonomous System (AS), également appelé « domaine de routage » qui est un ensemble de réseaux IP au sein d'une administration commune avec une politique de routage cohérente. Autrement dit, Un grand réseau est découpé en domaines idéntifiés appelés AS.

Ce découpage a mené à définir deux types de protocoles de routage, des protocoles internes qui assurent la communication au sein d'un AS et des protocoles externes qui permettent le routage entres les AS.

Nous évoquons dans ce qui suit les spécificités des principaux protocoles utilisés.

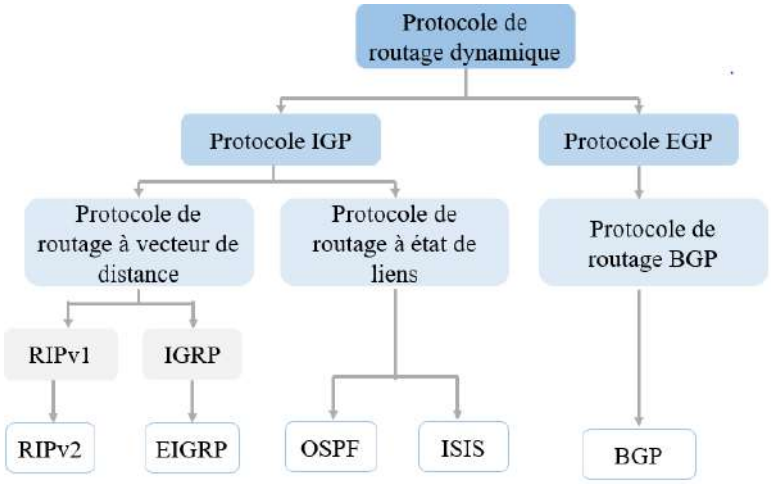


FIGURE 2.3 – Classification des protocoles de routage

2.3.6 Routage intra-domaine avec IGP

Utilisé pour le routage au sein d'un AS, les entreprises, les organisations et les fournisseurs de services utilisent un protocole IGP sur leurs réseaux internes. Il existe deux types de protocoles IGP que nous abordons dans ce qui suit.

2.3.6.1 Les protocoles de routage à vecteur de distance

Soit V(D,C,S) un vecteur de distance, il est composé d'une destination D, d'un coût C et d'un prochain saut S. La distance peut être le nombre de sauts, le coût, la bande passante, le délai ou autres. Le principe des protocoles de routage à vecteur de distance est d'annoncer les routes à travers une liste de distances estimée à chaque destination. Les routeurs ne connaissent pas le chemin complet vers la destination, ils connaissent uniquement l'estimation de distance sur une interface donnée.
L'un des protocoles les plus connus est Routing Information Protocol (RIP).

RIP est un Protocole qui s'appuie sur le calcul probabiliste de Bellman-Ford, moyennant l'utilisation d'une métrique particulière, le nombre de sauts (Maximum 15 sauts). Les transferts se font à l'aide de datagrammes UDP émis toutes les 30 secondes [37]. C'est l'un des plus vieux protocole de routage et n'est que très rarement utilisé. Le protocole RIP ne répond pas de manière favorable aux critères des réseaux IP cœur sur lesquels reposent des architectures MPLS assez grandes et supportent des applications nécessitant des temps de convergence rapides. La plupart de ces réseaux reposent sur des protocoles de routage internes à état de liens comme OSPF ou IS-IS.

2.3.6.2 Les protocoles de routage à état de liens

Ils sont basés sur la connaissance complète de la topologie du réseau. Chaque routeur découvre ses voisins à travers l'échange de messages HELLO, il construit des paquets contenants des informations sur les voisins, puis il les diffuse à ses voisins, ces derniers stockent les informations et les diffusent à leur tour à leur voisins. Ainsi tous les routeurs auront les mêmes visions globale du réseau. Nous présentons ici les protocole OSPF et IS-IS qui sont les plus répandus dans cette catégorie.

OSPF C'est un protocole de routage à état de lien qui fut originellement crée par l'Internet Engineering Task Force (IETF) pour remplacer le protocole RIP à la fin des années 80 [24]. En 1997 ils ont lancé la version OSPFv2 [31]. Il existe aussi une version OPSFv3 pour l'IPv6. [2] Ce protocole possède deux caractéristiques essentielles :
- Il est ouvert : C'est le sens du terme Open de OSPF, son fonctionnement est connu de tous.
- Il utilise l'algorithme Shortest Path First (SPF), plus connu sous le nom d'algorithme de Dijkstra, afin d'élire la meilleure route vers une destination donnée. La longueur d'un chemin est définie comme la somme des longueurs des liens parcourus, tandis que la longueur d'un lien, que l'on nomme également métrique ou poids peut-être fixée arbitrairement par le gestionnaire du réseau à la seule condition d'être un nombre entier positif.

Fonctionnement de OSPF Chaque routeur découvre ses voisins en envoyant des messages HELLO puis il leur envoie la liste des réseaux auxquels il est connecté à travers des messages Link State Advertisement (LSA). L'ensemble de ces LSA forme une base de données de l'état des liens appelée Link-State Database (LSDB).
Puis, en se basant sur la LSBD et sur l'algorithme de Dijkstra, chaque routeur calcule un arbre des plus courts chemins vers les autres destinations. C'est ce qui sera utilisé pour construire la table de routage du routeur.
Contrairement à RIP, OSPF a été pensé pour supporter un très grand réseau et afin d'éviter l'engloutissement de la bande passante, il introduit le concept de zone (area) qui permet de hiérarchiser le réseau en le divisant en plusieurs zone de routage, afin de diminuer la taille de la topologie à mémoriser sur chaque routeur. Chaque zone, identifiée par un numéro, possède sa propre topologie et ne connaît pas la topologie des autres zones et chaque routeur appartenant à une zone ne connaît que les routeurs de sa propre zone ainsi que la façon d'atteindre une zone particulière, la zone 0. L'OSPF est composé de [30] :

- Une zone 0 ou backbone area : C'est la zone centrale connectée à toutes les autres zones, elle est chargée de diffuser les informations de routage qu'elle reçoit aux autres zones.
- Backbone Router (BR) : C'est un routeur appartenant à la zone 0.
- Internal Router (IR) : C'est un nœud interne à une seule zone, sa fonction est de main-

2. OSPFv3 est défini dans la RFC 5340 `https://tools.ietf.org/html/rfc5340`

tenir à jour sa base de données d'état des liens avec tous les réseaux de sa zone.
- Area Border Router (ABR) : Ce sont des points de sortie pour les zones, Il connecte au moins deux zones différentes.
- Autonomous System Boundary Router (ASBR) : il est chargé de l'échange d'informations entre les systèmes autonomes.

Dans une zone OSPF, un routeur Designated Router (DR) doit être désigné qui servira de référent pour la base de données topologique [37]. Ainsi qu'un autre routeur de secours Backup Designated Route (BDR).

L'OSPF supporte entièrement le Variable Length Subnet Mask (VLSM) qui est une extension du découpage en sous-réseaux permettant d'optimiser l'attribution d'adresses IP et il supporte également l'agrégation de plusieurs routes en une seule.

IS-IS C'est un protocole à état de liens utilisé à l'intérieur d'un AS. Il a été initialement conçu pour le protocole Connectionless Network Protocol (CLNP) ou le protocole de couche réseau sans connexion [24]. Ensuite, il fut adapté pour transporter des préfixes IP, en plus des paquets CLNP.

Il est conceptuellement similaire au protocole OSPF étant donné qu'il découvre ses voisins à l'aide des messages HELLO, c'est un standard ouvert, il échange des paquets d'état de lien, il exécute l'algorithme SPF de Djikstra pour trouver le meilleur chemin qui est installé dans la table de routage LSDB, il définit des zones et il supporte le VLSM et l'agrégation des routes en plus d'être hautement évolutif.

Cependant, il possède des caractéristiques bien propres à lui listés ci-dessous :
- Il s'exécute sur la couche 2 du modèle OSI, la transmission des paquets n'est pas effectué avec le protocole IP mais directement dans des trames niveau 2.
- Il possède des extensions IPv6.
- Il supporte le CLNP
- Il est indépendant du protocole, offrant plus flexibilité.
- Il diffère dans la manière dont les zones sont définies et routés.

Fonctionnement d'IS-IS Tout comme OSPF, IS-IS diffuse des paquets HELLO pour découvrir ses voisins et pour déterminer s'ils sont de niveau 1 ou de niveau 2. Aussi le réseau AS est divisé en zones organisées de manière hiérarchique, cette organisation est accomplie en configurant les systèmes intermédiaires de niveau 1 et de niveau 2. Le niveau 1 pour le routage interne à une zone, il permet de découvrir le réseau et d'effectuer le routage, le niveau 2 pour le routage extérieur à une zone, il permet l'agrégation des routes, l'apprentissage des adresses des autres routes et la topologie pour le routage entre zones. Les routeurs IS-IS peuvent agir

à la fois comme des routeurs de niveau 1 et de niveau 2 partageant des routes intra-zone avec d'autres routeurs de niveau 1 et des routes inter-zones avec d'autres routeurs de niveau 2.

Tous les routeurs d'un niveau conservent une base de données d'état des liens complète de tous les autres routeurs du même niveau. Chaque routeur utilise ensuite l'algorithme Dijkstra pour déterminer le chemin le plus court entre le routeur local et les autres routeurs de la base de données d'état des liens.
IS-IS, comme OSPF, permet de calculer des chemins de secours en cas de panne d'un lien ou d'un nœud grâce au Loop free Alternate (LFA) Fast ReRoute (FRR)

La figure 2.4 illustre un exemple d'une topologie IS-IS qui donne un bon aperçu des zones et des routeurs de différents niveaux. En effet, nous avons un réseau IS-IS composé de 4 zones, les routeurs de niveau 1 (L1) savent uniquement communiquer à l'interieur de leur zone, s'ils veulent communiquer avec une autre zone ils utilisent un routeur de niveau 1-2 (L1-L2). Nous remarquons que la zone 4 est composé d'un seul routeur de niveau 2, il n'y a pas de routeur de niveau 1 donc on aura pas besoin de routeur L1-L2

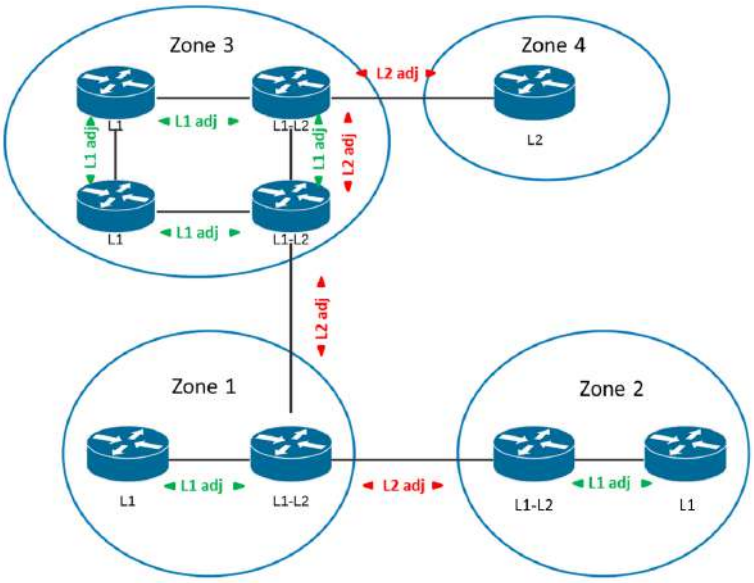


FIGURE 2.4 – Topologie d'un réseau IS-IS

2.3.7 Routage inter-domaine avec EGP

Les EGP assurent le routage entre les AS. Le BGP est le seul protocole EGP actuellement viable et responsable de la propagation des routes Internet à l'échelle mondiale.

BGP Le BGP est utilisé par les routeurs de bord des AS pour qu'ils échangent toutes les informations sur leurs réseaux et sur les réseaux qu'ils connaissent, dès leur première connexion

en utilisant le protocole TCP, puis seules les éventuelles mises à jours sont transmises [37].

Les routeurs qui implémentent BGP s'échangent des informations d'accessibilité de la couche réseau (NLRI) via des messages UPDATE. Les NLRI contiennent les informations suivantes : l'adresse du réseau, les attributs spécifiques au chemin et la liste des systèmes autonomes que le chemin doit transiter pour atteindre la destination.

BGP présente les caractéristiques suivantes :

— les informations échangées entre routeurs de différents AS ne contiennent aucun renseignement relatif à l'utilisation d'une métrique ou à la valorisation d'un coût particulier.

— les informations échangées entre routeurs de différents AS sont des informations qui décrivent un ensemble de routes qui permettent d'atteindre un ensemble de réseaux en termes de systèmes autonomes traversés par chaque route pour atteindre une destination donnée.

Fonctionnement de BGP Un réseau qui veut se faire connaître informe ses voisins BGP de son existence. Les voisins peuvent soit ignorer ou prendre en compte cette information. Dans le cas où un voisin la prend en compte, il l'annoncera à tous ses voisins et il s'engage à accepter le trafic vers cette destination. Sinon il ne l'annonce pas.

BGP possède la possibilité de l'agrégation des routes afin de diminuer la taille de la table de routage. Au sein d'un AS, le i-BGP est chargé des communications entre les routeurs internes, et entre les routeurs externes des différents AS le e-BGP est chargé de gérer la communication entre eux.

Comme le montre la figure 2.5 où les cercles gris en pointillés représentent les domaines AS. Les routeurs BGP sont représentés par des petits cercles non pointillés. Les flèches bleues représentent les e-BGP et les flèches rouges représentent les i-BGP.

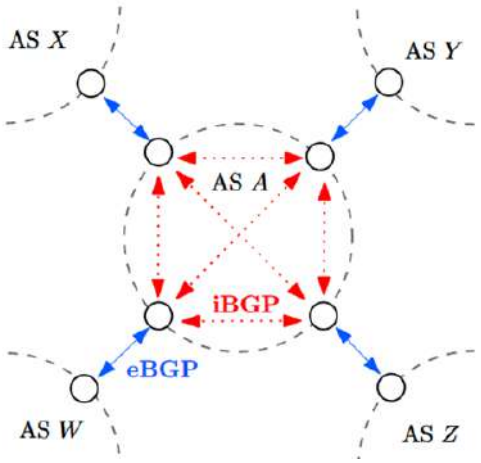


FIGURE 2.5 – Présentation de I-BGP et E-BGP

Le i-BGP, comme le IGP, sont deux protocoles qui s'effectuent au sein d'un même AS. Cependant, les IGP ne sont pas adaptés pour l'échange d'un trop grand nombre de routes,

ils restent donc limités à l'échanges des préfixes internes, d'où l'intérêt du i-BGP qui permet l'annonce des routes externes entre les routeurs.

2.4 Réseaux étendus

Les réseaux étendus WAN inter connectent plusieurs réseaux locaux à travers de grandes distances géographique, souvent utilisés par les grandes entreprises pour connecter leurs sites distants. Nous allons découvrir à travers cette section les protocoles ATM et Frame Relay.

2.4.1 Frame Relay

2.4.1.1 Définition

Frame Relay ou relais de trames est un protocole de commutation de paquets de couche liaison de données, successeur du protocole X.25 qui présentait des inconvénients tels que le faible débit de données et le manque de contrôle des erreurs.
Le Frame Relay utilise un circuit virtuel pour établir une connexion entre l'émetteur et le récepteur et transférer les données sous forme de paquets à une vitesse raisonnable et à un coût abordable. Il peut etre de type permanent Permanent virtual circuits (PVC) ou temporaire établi à la demande Switched virtual circuits (SVC). Un identifiant unique Data Link Connection Identifier (DLCI) identifie la connexion virtuelle [36].

2.4.1.2 Avantages et inconvénients

Avantages

— Ses trames sont de longueur variable et sa faible surcharge fournissent un excellent débit réseau et un faible retard de données.
— La bande passante peut être allouée dynamiquement selon les besoins.
— Il offre un débit plus élevé que X.25. Ceci est dû au fait qu'aucune détection d'erreur n'est incorporée et donc la surcharge est moindre.
— Il fonctionne sur la couche physique et liaison de données, il est donc facile de l'intégrer avec des périphériques ayant des fonctionnalités de couche 3 réseau.
— Il y a peu de surcharge du réseau en raison de l'incorporation du mécanisme de contrôle de la congestion.
— Il est moins cher que les autres technologies WAN.
— Il fournit une connexion sécurisée car il est difficile d'intercepter des circuits PVC entre les DTE.

— Il offre un débit et un délai garantis.

Inconvénients

— Le contrôle de flux et le contrôle d'erreur ne sont pas disponibles dans le relais de trame. Cela devrait être pris en charge par les protocoles de couches supérieures.
— Ses trames sont de longueur variable et ça peut donc créer des retards variables pour différents utilisateurs.
— En raison du retard variable, il n'est pas approprié d'envoyer des données sensibles comme la voix ou la vidéo en temps réel.
— Les paquets subissent un délai supplémentaire avec chaque nœud qu'ils traversent. Cela implique une surcharge de données et une surcharge de traitement avec chaque paquet

2.4.2 ATM

2.4.2.1 Définition

Asynchronous Transfer Mode (ATM) ou mode de transfert asynchrone est une technologie de commutation et de multiplexage orientée connexion, elle a été conçue pour prendre en charge un mélange de trafic tout en garantissant la qualité de service contrairement à la technologie Frame Relay.

Une connexion, appelée Virtual Channel Connection (VCC) ou circuit virtuel, est établie entre les deux points d'extrémité avant le début de l'échange de données, puis ATM utilise des paquets appelés cellules de longueur fixe 53 octets dont 48 octets de données et 5 octets d'informations d'en-tête [36].

2.4.2.2 Avantages et inconvénients

Avantages

— Communication à haut débit et commutation rapide.
— Il est facile à intégrer avec tout type de réseaux Local Area Network (LAN), Metropolitan Area Network (MAN) et Wide Area Network (WAN).
— Il est oritenté qualité de service. Il permet de transporter de manière fiable la voix, les données et la vidéo simultanément et de gérer la bande passante en fonction de la priorité du service requis.

Inconvénients

— Coût élevé, les connexions au réseau ATM et les équipements ATM sont très chers.
— ATM ne supporte pas la Notification Explicite de congestion avancée disponible dans Frame Relay ou le réacheminement automatique trouvé dans les réseaux modernes IP.
— Surcharge de l'en-tête de cellule (5 octets par cellule)

— Complexité des mécanismes pour atteindre la QoS.

2.5 MPLS

Comme nous l'avons vu dans la section précédente, malgré les avantages considérables qu'offrent Frame Relay et ATM, ils constituent un échec quant à leurs nombreux inconvénients. Nous avons aussi vu que le protocole IP fonctionne en mode non connecté, l'émetteur d'un paquet ne peut pas prévoir le chemin qui sera emprunté par ce dernier alors que les opérateurs ont besoin de plus de certitude quant au routage du trafic et ils ont besoin d'optimiser l'utilisation des liens et mettre en place des contraintes d'acheminement des paquets. Pour résoudre ces problèmes et répondre aux besoins du réseau IP tout en bénéficiant des avantages des technologies Frame Relay et ATM, la technologie MPLS a été mise en place. Nous aborderons cette technologie dans la section suivante.

2.5.1 Définition

Le protocole MPLS est défini et normalisé par IETF en 1997 [32]. Il fait partie intégrante de la plupart des réseaux de fournisseurs de services. Son but est de donner aux routeurs une plus grande puissance de commutation. Il apporte à l'IP un mode connecté car la transmission des paquets est réalisée en commutant les paquets en fonction d'étiquettes, sans avoir à consulter l'adresse IP et la table de routage.

Il combine donc les principes du routage IP avec les principes de la commutation (ATM, Frame Relay). Il est appelé Multi Protocol car il est indépendant du protocole utilisé pour la couche inférieure et il est appelé Label Switching car la commutation est faite en fonction d'une étiquette attachée à un paquet.

Un réseau MPLS est composé des éléments suivantes :

— **Des routeurs Label-switching router (LSR) :** Ce sont des routeurs cœur capables de supporter le MPLS, ils prennent les décisions de transfert des paquets en se basant sur des étiquettes et non pas sur l'adresse IP [32]. Ils effectuent les opérations SWAP ou bien POP sur les labels.
— **Des routeurs Customer Edge (CE) :** Ce sont les routeurs des clients.
— **Des routeurs Label Edge Router (LER) :** Ils se trouvent au bord du réseau MPLS, ils permettent de faire la transition entre le réseau MPLS et les réseaux externes [32]. Ils se divisent en deux type :

  - **Ingress LER :** Ce sont des LER qui gèrent le trafic qui entre dans un réseau MPLS, ils effectuent l'opération PUSH sur les labels.
  - **Egress LER :** Ce sont des LER qui gèrent le trafic qui sort d'un réseau MPLS, ils effectuent l'opération POP sur les labels.
- **Des chemins Label Switching Path (LSP) :** Ou chemins à commutation d'étiquette, ce sont des chemins unidirectionnels construits à base d'échange d'étiquettes d'un routeur d'entrée vers un routeur de sortie en passant par des routeurs LSR [32].
- **Forward Equivalent Class (FEC) :** Dans le MPLS le routage s'effectue par l'intermédiaire de classe d'équivalence (FEC) [34]. Chaque paquet est associé à une FEC, qui permet de les regrouper selon des propriétés communes (Champs label et Exp identiques). Ensuite tous les paquets appartenant à la même FEC reçoivent le même traitement au cours de leur acheminement.

2.5.2 Structure de l'en-tête MPLS

A l'entrée du paquet IP, un en-tête MPLS de 32 bits est inséré entre l'en-tête de couche 2 et l'en-tête de couche 3 [32]. L'en-tête MPLS est composé de quatre champs [28] illustrés dans la figure 2.6 et décrits ci-dessous :

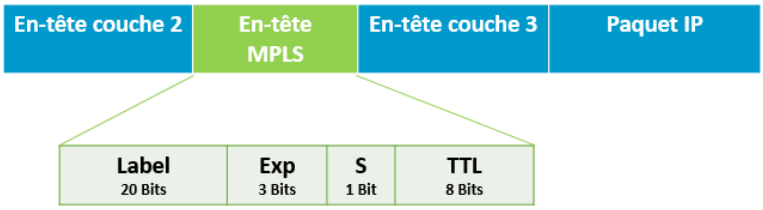


FIGURE 2.6 – Structure d'un entête MPLS

- **Label ou étiquette :** Cette valeur identifie un LSP et change à chaque saut. Elle est codée sur 20 bits.
- **EXP :** Il est codé sur 3 bits et permet d'inclure des informations sur la classe de service, la Quality of Service (QoS).
- **Bottom of stack (S) :** Ce champ est codé sur un bit. Sur un paquet IP, plusieurs label peuvent être empilés, et ce champ permet de savoir si il reste des labels dans le paquet. La valeur 1 indique que c'est la dernière étiquette associée au paquet et la valeur 0 pour informer le routeur que d'autres labels suivront.
- **Time to Live (TTL) :** Ce champ de 8 bits indique la durée de vie du paquet de données. À cette fin, il limite le nombre de sauts qu'un paquet étiqueté peut parcourir. La limite est de 255 routeurs, et à chaque passage de routeur il sera décrémenté d'une unité, une fois que le TTL est à 0 et qu'il n'a pas encore atteint sa destination, le paquet est détruit et un message d'erreur sera envoyer par le routeur en charge en utilisant un paquet ICMP. La fonctionnalité par défaut du passage de l'IP vers le MPLS consiste à

copier la valeur TTL de l'en-tête IP vers l'en-tête MPLS au niveau du routeur d'entrée, et vis versa à la sortie, la valeur TTL de l'en-tête MPLS est copiée vers l'en-tête IP par le routeur de sortie.

2.5.3 Opérations sur les labels

Trois opérations PUSH, POP et SWAP sont implémentées sur les routeurs MPLS.

— **PUSH :** C'est une opération d'insertion, elle va permettre d'insérer le label entre les couches deux et trois. Cette opération est utilisée lorsqu'un paquet pure IP est transmit à l'entrée d'une interface réseau MPLS.

— **POP :** C'est une opération de suppression. Elle est réalisée à la sortie d'un réseau pure MPLS vers un réseau pure IP, soit par le routeur de sortie LER, soit par le dernier routeur LSR afin d'éviter d'effectuer deux recherches dans la table de routage du routeur de sortie et dans ce cas, l'opération est appelée Penultimate Hop Popping (PHP) utilisée dans le cas du VPN.

— **SWAP :** C'est une opération de changement, elle permet de remplacer un label par un autre qui pourra être interpréter par le routeur suivant afin de transmettre le paquet vers sa destination. Elle est utilisée à la sortie d'un routeur vers un autre au sein d'un réseau MPLS.

2.5.4 Architecture du protocole MPLS

Pour fournir plus de flexibilité, l'architecture MPLS illustrée dans la figure 2.7 est composée de deux plans pour séparer les données du contrôle et permettre la commutation d'étiquettes [5] :

2.5.4.1 Plan de contrôle

Il permet de créer et de distribuer des chemins LSP et des étiquettes. Il est donc responsable du contrôle des informations de routage, de commutation et de distribution des labels. Il existe deux méthodes pour créer et distribuer des étiquettes :

— Implicit Routing : Consiste à créer des labels en exécutant des protocoles de routage classique internes tel que OSPF.

— Explicit routing : Consiste à ne construire de route que lorsqu'un flux de données est susceptible de l'utiliser afin d'utiliser efficacement les ressources du réseau. Cette méthode utilise le routage RSVP-TE et permet le Traffic Engineering qui est expliqué par la suite.

La table Routing Information Base (RIB) située dans le plan de contrôle stocke les informations nécessaires pour atteindre le réseau IP de destinations. Ces informations sont transférées vers la table Forwarding Information Base (FIB) située dans le plan de données. [33] La table Label

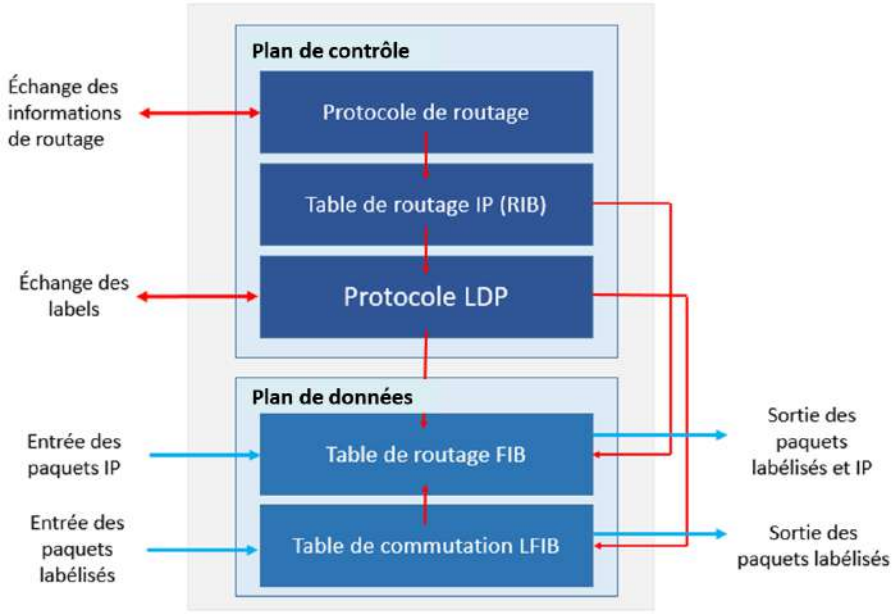


FIGURE 2.7 – Architecture MPLS

Information Base (LIB) illustrée dans la figure 2.8 appartient au plan de contrôle, elle est générée par les protocoles de signalisations et constitue la liste des labels transmis par les LSR voisins pour chaque sous-réseau IP qui constituent la table de routage, lui permettant ainsi de connaître tous les chemins pour atteindre une destination. [20]

Destination	Router	Label
10.0.0.0	Local	20

FIGURE 2.8 – Table LIB

2.5.4.2 Plan de données

Appelé aussi plan de transfert, il permet d'assurer la transmission des données en se basant sur la commutation des étiquettes expliquée dans la sous-section suivante. Les informations de transfert sont conservées dans des tables et elles sont pilotées depuis le plan de contrôle.
Le plan de données est indépendant des protocoles de routage et il utilise des tables de commutations. FIB, table de transfert IP, illustrée dans la figure 2.9 est utilisée pour le mappage des paquets non étiquetés, elle est construite à partir de la table de routage RIB. A partir de

Destination	Next hop	Interface
10.0.0.0	10.1.1.1	eth 0/0

FIGURE 2.9 – Table FIB

la table LIB et FIB [33], chaque routeur construit la table Label Forwarding Information Base (LFIB), illustrée dans la figure 2.10, qu'il utilisera pour commuter les paquets étiquetés. La table LFIB fournit le mappage en destination d'un réseau ainsi que l'opération à effectuer sur chaque étiquette.

Destination	Local label	Outgoing label	Next hop	Interface
10.0.0.0	20	Pop	10.1.1.1	eth 0/0

FIGURE 2.10 – Table LFIB

Nous allons expliquer dans ce qui suit le fonctionnement du protocole MPLS.

2.5.5 Acheminement des paquets par commutation d'étiquettes

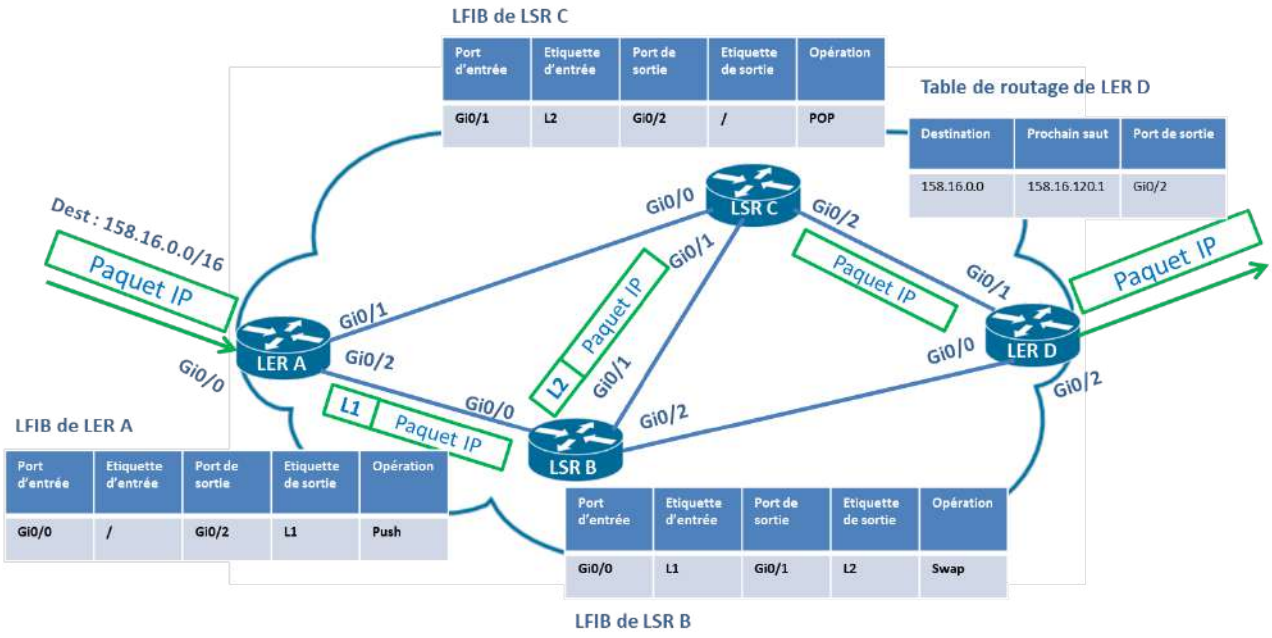


FIGURE 2.11 – Commutation d'étiquettes sous MPLS

Lorsqu'un paquet est reçu par un routeur d'entrée Ingress-LER il ne contient que des adresses IP et il sera associé à une FEC selon les informations contenues dans son en-tête. Dans l'exemple de la figure 2.11 pour acheminer le paquet destiné à une adresse appartenant au sous-réseau 158.16.0.0/16, le routeur d'entrée LER A se base sur sa table LFIB pour déterminer la classe FEC associée au sous-réseau 158.16.0.0/16,il insère le label L1 sur le paquet (opération PUSH) et le transmet au prochain LSR selon sa table par l'interface de sortie Gi0/2 Le paquet contenant un label arrive au LSR B, celui-ci consulte sa table LFIB pour acheminer le paquet puis change le label L1 par L2 (Opération SWAP) et transmet le paquet via l'interface Gi0/1 au suivant, Le routeur LSR C reçoit le paquet, consulte sa LFIB, étant le dernier il supprime l'étiquette via l'opération POP et l'envoie au routeur de sortie LER D. Enfin, pour

acheminer le paquet contenant que des adresses IP vers le prochain routeur (158.16.120.1) situé en dehors du réseau MPLS, le routeur D utilisera sa table de routage IP.

2.5.6 Distribution d'étiquettes

Plusieurs protocoles ont été définis pour assurer la distribution d'étiquettes et construire des chemins LSP. Pour notre étude nous allons nous intéresser aux protocoles standards les plus utilisé dans MPLS à savoir, LDP et RSVP-TE [32].

2.5.6.1 LDP

Ce protocole se charge de la distribution implicite des labels assignés localement par les routeurs aux autres routeurs adjacents, pour tous les préfixes de la table de routage. Il se base sur les informations transmises par la couche réseau pour construire des chemins LSP et il associe une classe d'équivalence FEC à chaque chemin LSP crée. Les labels sont spécifiés selon le chemin "Saut par saut" défini par l'IGP pour construire un LSP du LER d'entrée au LER de sortie [34].
Pour découvrir les voisins LDP, les routeurs LSR s'échangent périodiquement des messages Hello, transmis sous forme de paquets UDP, pour établir et maintenir les sessions. Quand on configure LDP sur les routeur LSR, les routeurs commencent à envoyer des messages de découverte LDP sur toutes les interfaces compatibles LDP. Lorsqu'un LSR voisin reçoit des messages de découverte LDP, il établit une connexion TCP via le port 646, puis une session LDP est créée au-dessus de la session TCP et les routeurs peuvent commencer à s'échanger des étiquettes.

Avantages de LDP :

— Prise en charge de Equal Cost Multiple Path (ECMP) : Puisque le LDP s'appuie sur IGP pour transmettre les paquets, il prend en charge le ECMP. [3]qui est une technique de routage où il existe plusieurs "meilleurs chemins" pour envoyer les données.

— Configuration simple : La configuration de LDP est simple, il suffit de configurer le protocole de routage IGP et activer le LDP.

Inconvénients de LDP :

— Trou noir : La perte de synchronisation entre IGP et LDP peut provoquer un trou noir et une perte de paquets. En effet, dans certains cas, les sessions LDP sont défectueuses, par conséquent, les paquets ne sont pas étiquetés, mais IGP les envoie quand même.

— Aucune méthode d'optimisation du trafic : LDP ne prend pas en charge les contraintes de Traffic Engineering, les chemins sont sélectionnés uniquement en fonction de la valeur du coût.

3. ECMP est un algorithme de routage où il existe deux ou plusieurs chemins de mérite égal pour envoyer les données vers le " prochain saut" à travers le réseau.

— Faible évolutivité.

2.5.6.2 CR-LDP

Constraint-Based LSP Setup using LDP (CR-LDP) est un protocole explicite où le LSP est routé par le routeur source, il étend le protocole LDP en lui introduisant la notion du Traffic Engineering, dont l'objectif est le suivant :

— Utiliser efficacement des ressources du réseau.

— Éviter les points de forte congestion en répartissant le trafic sur l'ensemble du réseau.

Ainsi, il impose au réseau des contraintes sur les flux, et choisi les chemins les plus optimaux suivies par les clients FEC avec une qualité de service prédéfinie.

Cependant, pour de larges réseaux, la mise en place de chemin avec ce protocole peut nécessiter des ressources considérables, ce qui explique son échouement.[34]

2.5.6.3 RSVP-TE

RSVP-TE est un protocole de couche de transport, utilisé pour établir des chemin MPLS, réserver des ressources à travers un réseau et pour la signalisation de la qualité de service. Le RSVP-TE est une extension du RSVP permettant de supporter le Traffic Engineering ainsi que la distribution des labels. Il permet également de détecter rapidement les pannes de lien ou de noeuds, ce qui permet d'introduire la technologie FRR qui permet de re-router très rapidement un LSP lorsqu'un noeud ou un lien tombe en panne.

Tous les noeuds du réseau partagent la base de données d'informations de liaison du traffic engineering, qui contient des informations en temps réel, via l'IGP. Ensuite, l'établissement d'un tunnel LSP se fait grâce aux messages échangées entre les nouds MPLS, et plus précisément grâce au message PATH du Ingress LER au Egress LER, envoyé grâce au protocole de routage unicast ou multicast. Ces messages contiennent des informations sur la spécification du trafic dans le but d'établir une connexion. Ainsi que du message RESV du Egress LER au Ingress LER qui est une réponse au message PATH. RESV se propage de noeud en noeud jusqu'au Ingress LER, lorsque ce dernier le reçoit, le LSP sera établi et les ressources nécessaires seront allouées dans chaque nœud qui compose le réseau MPLS. Ce processus est illustré dans la figure 2.12.

FIGURE 2.12 – Les messages PATH et RESV dans RSVP-TE

Pour N noeuds du réseau nous devons créer et configurer le nombre suivant de tunnels :

$$Nombredetunnels = \frac{N * (N-1)}{2}$$

Avantages de RSVP-TE :

— Permet le Traffic Engineering et la sélection flexible de chemin en fonction des changements d'état de la liaison sur le réseau, contrairement à LDP qui ne fournit pas cette fonction.

— Permet un FRR efficace, contrairement à LDP.

Inconvénients de RSVP-TE :

— Configuration complexe. Les tunnels RSVP-TE doivent être configurés manuellement et chaque tunnel a des exigences de liaison spécifiques.

— Protocole complexe. Outre la configuration complexe, le mécanisme du protocole RSVP-TE est également compliqué. Tous les routeurs du réseau doivent maintenir une grande base de données d'informations sur les liaisons. Par conséquent, l'échelle d'un réseau RSVP-TE ne peut pas être étendu, son déploiement ne convient pas à un réseau de grande échelle.

— ECMP non pris en charge. Selon le principe de fonctionnement RSVP-TE, il calcule les chemins en fonction des informations de liaison, configure les tunnels et distribue les étiquettes, sans dépendre de l'IGP. Ainsi, il ne peut pas permettre le routage ECMP comme IGP. Si l'équilibrage de charge est requis, un autre tunnel avec les mêmes adresses IP source et de destination que celui d'origine doit être créé ce qui est définitivement compliqué.

2.6 Applications de MPLS

Le MPLS met en oeuvre diverses applications adaptées aux fonctionnalités recherchées grâce à sa façon différente d'assigner et distribuer les labels et commuter les paquets. Les applications phares du MPLS sont détaillées dans ce qui suit.

2.6.1 VPN-MPLS

Les VPN sont une solution qui permet d'établir une connexion entre les sites distants, par exemple entre les bureaux d'une entreprise éloignées géographiquement. Ce sont des tunnels qui garantissent des échanges sécurisés au sein d'un réseau privé étendu sur un réseau public comme Internet.

Il existe plusieurs types de VPN, parmi eux, VPN IPSec et VPN MPLS. Nous nous intéressons dans ce mémoire au VPN MPLS.

2.6.1.1 Définition d'un VPN-MPLS

L'un des plus importants avantages du protocole MPLS est la possibilité de créer des VPN grâce à son mécanisme d'acheminement des paquets qui n'est pas basé sur l'adresse de destination du paquets IP, mais sur sa valeurs de label.

Nous avons vu précédemment que le protocole MPLS est situé entre la couche 2 et 3, il a donc la possibilité de créer des VPN de couche 2 et de couche 3 qu'on verra en détails par la suite. Il est à noter que dans un environnement VPN-MPLS les routeurs LER et LSR sont appelés PE et P respectivement. Les routeurs P (Provider) composent le coeur du backbone MPLS, ils n'ont aucune connaissance de la notion de VPN. Ils se contentent d'acheminer les données grâce à la commutation de labels. Quant aux PE (Provider Edge), ce sont des routeurs de frontière et ont une ou plusieurs interfaces reliées à des routeurs clients. On y trouve aussi les routeurs CE (Customer Edge) qui représentent les routeurs client et n'ont aucune connaissance des VPN ni de la notion de label.

MPLS layer 2 VPN Le VPN de couche 2 simule le comportement d'un réseau local (LAN) sur un protocole IP ou un réseau IP-MPLS permettant aux périphériques Ethernet de communiquer entre eux comme s'ils étaient connectés avec un LAN commun.Le MPLS Layer 2 VPN utilise des étiquettes MPLS pour transporter des données. La communication se fait entre les routeurs PE, car ils se trouvent à la périphérie du réseau du fournisseur, à côté du réseau du client

MPLS layer 3 VPN Un L3VPN fonctionne au niveau de la couche réseau et manipule un modèle peer-to-peer qui utilise le protocole BGP pour distribuer les informations relatives au VPN. Il est composé d'un ensemble de clients connectés sur le réseau d'un fournisseur de services qui partagent des informations de routage communes.
Dans ce type de VPN le routage se produit au niveau des routeurs PE du fournisseur de services. Ces derniers stockent et traitent les routes des clients qui doivent partager les informations sur la topologie de leur réseau et c'est le fournisseur de services qui détermine les politiques et le routage.
Des étiquettes sont ajoutées aux paquets IP des clients lorsqu'ils entrent par des routeurs (CE) vers les routeurs (PE) et seront supprimées dans le cas inverse. Il utilise des Virtual Routing and Forwarding (VRF) pour créer et gérer les données utilisateurs, le protocole MP-BGP pour distribuer les informations de routage VPN sur le réseau du fournisseur et MPLS pour transmettre le trafic VPN à travers le réseau vers les clients distants.
Ce mode de VPN est constitué des éléments suivants :

— **Une table de routage virtuelle VRF** : Elle est utilisée pour isoler le trafic des différents clients sur le même routeur. [4]

Une interface sur un routeur ne peut appartenir qu'a une seule VRF. Chaque instance VRF crée une table RIB, FIB et LFIB distincte.

— **Un Multi protocol BGP (MP-BGP) :** C'est une extension du protocole BGP qui supporte les familles d'adresses IPv4 et IPv6 et leurs variantes unicast et multicast. Il est utilisé dans un milieu L3VPN pour échanger les étiquettes VPN apprises pour les routes des sites clients sur le réseau MPLS afin de distinguer les différents sites clients lorsque le trafic des autres sites clients arrive au fournisseur.
— **RD (Route Distinguisher) :** Est une valeur 64 bits attachée à l'adresse IP du client et placée dans sa propre VRF. Elle identifie de manière unique une route VPN et produit une adresse VPNv4 de 96 bits unique. Les routes VPN sont transportées sur le réseau avec MP-BGP qui a besoin que les routes transportées soient uniques.
— **RT (Route Target) :** Est une valeur 64 bits attachée aux routes VPNv4 pour indiquer les routes importées et exportées. Les routes importées sont utilisés pour sélectionner les routes VPNv4 à insérer dans les tables VRF correspondantes. Les routes exportées sont attachées à une route lorsqu'elle est envoyée dans la table de routage VPNv4 vers l'autre extrémité du client ou sa destination. Elle sont utilisées pour identifier l'appartenance VPN des routes.

2.6.1.2 Commutation des paquets sur un réseau VPN MPLS

L'acheminement des paquets dans un réseau VPN-MPLS se base sur les principes du routage MPLS standard à quelques différences près.
La figure 2.13 illustre un exemple d'un VPN établi dans un réseau MPLS. Un VPN nommé NORD est configuré entre les clients CE1 et CE2. Ce VPN se repose sur une VRF crée sur les Ingress et Egress LER (PE1 et PE2 respectivement) et peuplée à l'aide du protocole MP-BGP, ce protocole va permettre d'envoyer un label VPN L100 de PE2 à PE1.
Lorsque PE1 reçoit le paquet via CE1, il saura qu'il fait partie de la VRF NORD, il effectue deux opérations PUSH, il encapsule l'étiquette VPN L100 ainsi que l'étiquette L1. Le paquet est commuté à travers le réseau MPLS selon le mode d'acheminement MPLS, les routeurs internes P1 et P2 sont seulement concernés par la commutation des étiquettes L1 et L2 et seul PE2 est concerné par la décapsulation du label L100.
Une fois le paquet arrivé à P2, et comme P2 est L'avant dernier routeur du réseau MPLS, une opération PHP est effectuée sur le label L2 puis envoie le paquet à PE2. PE2 va lire le label L100, et saura que ce label fait partie de la VRF NORD. Il fait un POP du label L100 et à travers la VRF NORD il va trouver que pour acheminer le paquet vers CE2, il faudra passer par l'interface eth0/1.

4. Umar Bashir Sofi, Er. Rupinder Kaur Gurm, Comparative Analysis of MPLS Layer 3 vpn and MPLS Layer 2 VPN, 2015.

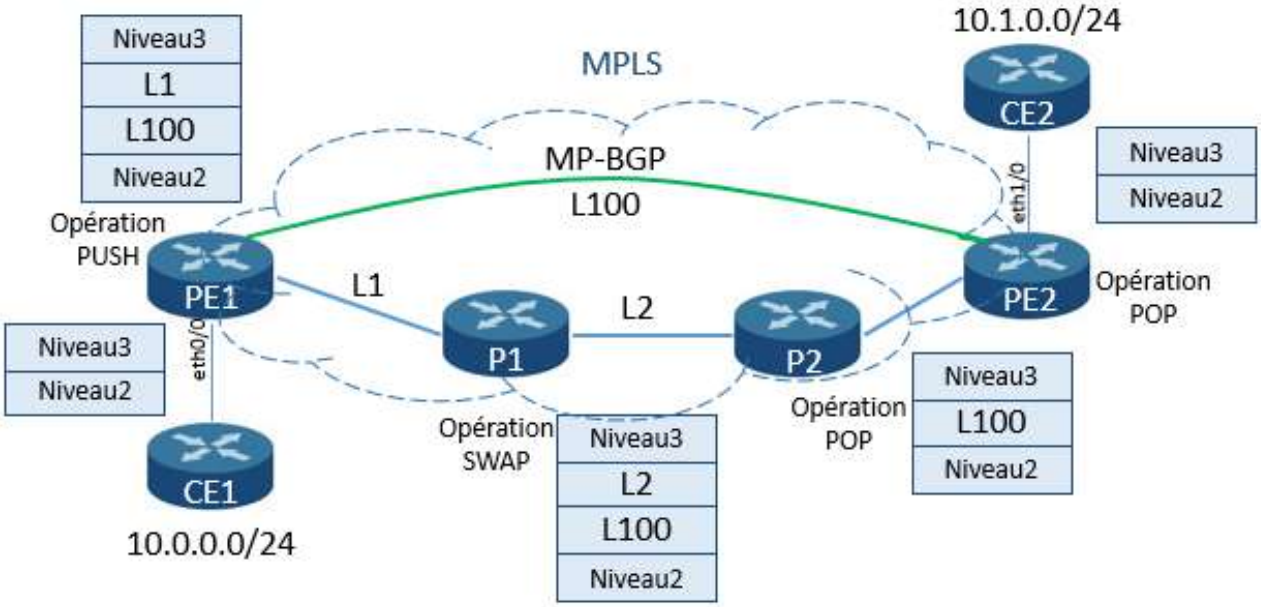


FIGURE 2.13 – Commutation des paquets sur un réseau VPN-MPLS

2.6.2 Qualité de service

La qualité de service d'un réseau désigne sa capacité à transporter dans de bonnes conditions les données [32]. Tout en réduisant la perte de paquets, la latence et la gigue (jitter) sur le réseau.

En d'autres termes, la qualité de service est la capacité d'offrir différentes priorités à différentes applications ou flux de données pour garantir que chaque type de trafic soit traité de manière spécifique par ses conditions.

Par exemple, le réseau MPLS donne la priorité au trafic des données sensibles à la latence, comme la voix et la vidéo, par rapport au reste du trafic, moins sensible. La qualité de service est un élément crucial pour un réseau d'opérateur car les opérateurs doivent assurer à leurs clients une qualité de service irréfutable, et cela ce fait en respectant des critères bien définit, nous citons :

- **Le débit** ou bandwidth en anglais, il définit la quantité maximale de données (bits) émise sur un support de transmission par une unité de temps.
- **Le délai** ou delay en anglais, appelé aussi la latence, il correspond au temps de la transmission d'un paquet entre sa source et sa destination. Les conséquences du délai sont surtout visibles pour les services qui fonctionnent en temps réel tel que le streaming.
- **La gigue** ou jitter en anglais, elle correspond aux variations de latence des paquets selon la charge du réseau. Elle a également une influence sur les services en temps réel.
- **Taux de perte** ou packet loss en anglais, il correspond au nombre de paquets qui n'arrivent pas correctement jusqu'à leurs destination. ça peut être due à des erreurs d'intégrité sur les données ou des rejets de paquets en cas de congestion.

Deux types d'architectures sont présentes par l'IETF pour définir la QoS IP : [5]

— **IntServ**

Le modèle de gestion IntServ définit pour un système hôte, une demande de service spécifique (délai, bande passante et seuil min de perte des paquets) à un réseau. Ce modèle est basé sur RSVP pour la réservation des ressources sur l'ensemble des noeuds par lesquelles doivent transiter les données. IntServ est un modèle complexe, car chaque routeur doit mémoriser un grand nombre d'information [32].

— **DiffServ**

Vu que le IntServ n'est pas adapté à Internet à cause de l'abondance de RSVP, l'IETF a adopté un second modèle, le DiffServ. DiffServ assure une distinction des paquets par classes de flux identifiés par une valeur, de cette manière les flux d'une même classe ont les mêmes garanties de service.

Par rapport à IntServ, DiffServ est beaucoup plus évolutif car il n'est pas nécessaire de mémoriser les besoins individuels de chaque flux sur le réseau, mais seulement d'offrir un traitement différencié des paquets, selon la valeur de priorité indiquée dans l'en-tête du paquet [32].

Les deux approches sont complémentaires car IntServ réalise un contrôle de bout en bout des ressources utilisées, alors que DiffServ spécifie des comportements à chaque saut [32]. Néanmoins MPLS est amené à interfonctionner avec DiffServ. La signalisation de DiffServ est beaucoup moins importante que IntServ car elle ne nécessite pas de maintien de l'état des flux par RSVP.

2.6.3 Traffic Engineering

2.6.3.1 Définition du Traffic Engineering

L'expression de Traffic Engineering ou ingénierie de trafic désigne l'ensemble des mécanismes de contrôle de l'acheminement du trafic dans le réseau afin d'optimiser l'utilisation des ressources et de limiter les risques de congestion.

Autrement dit, l'ingénierie du trafic consiste à sélectionner les meilleurs itinéraires pour le trafic de données afin de déplacer la charge de trafic des parties encombrées du réseau vers les parties non encombrées, et maximiser ainsi la quantité du trafic transitant dans le réseau tout en gardant la qualité de service.

Les mécanismes d'ingénierie du trafic décident en fonction de la surcharge des liaisons si le chemin le plus court calculé par le IGP peut être utilisé, sinon, s'il est très saturé, il cherche des itinéraires alternatifs qui n'ont pas autant de charge.

5. Le Faucheur, L.Wu, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J.heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services, RFC 3270, May 2002

2.6.3.2 Traffic Engineering avec MPLS

L'ingénierie de trafic MPLS (MPLS-TE) représente une solution pour pallier aux limitations du routage IP qui souffre de difficultés importantes quant à l'ingénierie des trafic. Le mécanise MPLS-TE permet l'établissement de LSP MPLS routés de façon explicite indépendant de la route IP en prenant en compte des contraintes de trafic ainsi que des ressources disponibles dans le réseau. Les chemins du Traffic Engineering sont appelés TE-LSP ou « tunnels MPLS-TE ».

Les étapes d'établissement d'un tunnel TE sont les suivantes :

1. Découverte des ressources et distribution des informations de l'état du réseau dans tout le domaine IGP par le protocole IS-IS ou OSPF.
2. Calcul du chemin en se basant sur les contraintes pour trouver le chemin le plus court qui répond aux besoins en ressources du flux du trafic avec l'algorithme Constrained Shortest Path First (CSPF) qui opère sur la tête de tunnel.
3. L'établissement du chemin par un protocole de signalisation CR-LDP ou RSVP-TE, pour attribuer les étiquettes et établir les tunnels.
4. Placement du trafic dans les tunnels qui assureront son transfert.

MPLS-TE fournit ainsi un meilleur contrôle du routage et permet d'optimiser l'utilisation des ressources, réduire les risques de congestion, garantir la qualité de service et le FRR après une panne de noeuds ou de lien dans le réseau avec un temps de réparation de moins de 100ms.

2.7 Conclusion

A travers ce chapitre nous avons définit les bases d'un réseau informatique ensuite nous avons vu que dans un réseau, les protocoles de communications peuvent être groupés selon leur fonctionnalités et leur niveau de fonctionnement, on utilise pour cela deux modèles représentatifs des différentes couches réseau, qui sont les modèles OSI et TCP/IP. Nous nous sommes ensuite intéressés au fonctionnement du protocole IP et du processus de routage, notamment le routage interne et externe où nous avons expliqué le fonctionnement des protocoles OSPF, IS-IS et BGP.

Ensuite nous avons évoqué les réseaux étendus où nous avons cité les inconvénients et les avantages des technologies ATM et Frame Relay qui étaient l'une des raisons de l'apparition de la technologie MPLS que nous avons introduite par la suite et nous avons vu que le MPLS qui est une technologie de commutation d'étiquettes utilisée principalement par les fournisseurs d'accès Internet pour connecter différents sites distants. Elle peut être utilisé pour transporter tout type de données et elle offre la possibilité de créer des VPN à la fois sur la couche 2 et la couche 3. En outre, le MPLS est utilisé pour assurer la qualité de service pour garantir la disponibilité de la quantité de bande passante et elle implémente l'ingénierie du trafic afin d'optimiser le flux de trafic et l'utilisation des liaisons. Cependant, les protocoles de TE existants souffrent de plusieurs limitations.

Dans le prochain chapitre nous présenterons l'innovante technologie du Segment Routing qui offre une approche simple pour surmonter les limites du MPLS.

Chapitre 3

Segment Routing

3.1 Introduction

Comme nous l'avons souligné précédemment, le MPLS utilise des protocoles de signalisation complexes et difficiles à entretenir alors que nous sommes dans une ère où les réseaux ne cessent de grossir à vitesse phénoménale avec l'apparition de nouveau services et applications, posant une variété d'exigences de réseau. Dans ces conditions, les chercheurs ont été amené à développer la technologie du Segment Routing que nous présentons dans la suite de ce chapitre.

3.2 Définition

Le SR est une récente technologie introduite pour la première fois par cisco en 2013 [6], puis son architecture a été standardisée au sein de IETF par le groupe (Source Packet Routing in Networking (SPRING). Le SR est basée sur le routage source, ce qui signifie que le chemin vers la destination est déterminé avant que le paquet ne quitte le noeud d'entrée. Une liste ordonnée de segments est insérée dans l'en-tête du paquet par le routeur d'entrée. Ces segments constituent une suite d'instructions du chemin requis, que chaque routeur exécute pour transmettre le paquet à travers le réseau, éliminant ainsi le besoin pour les autres noeuds de conserver et de maintenir les informations de chemin. La liste de segment est appelée aussi politique de SR. L'ensemble des nœuds participants constituent un domaine appelé le domaine SR. L'architecture du SR supporte un plan de contrôle distribué, centralisé ou hybride. Dans le cas distribué les segments sont distribués par le IGP et BGP et dans le cas centralisé ils sont distribués par un contrôleur centralisé. L'architecture SR peut être instanciée sur un plan de données MPLS (SR-MPLS) où les segments sont des labels ou bien sur un plan de données IPv6 (SRv6) où les segments sont des adresses IPv6 [9]. Nous allons nous concentrer dans cette étude sur le SR-MPLS.

3.3 SR-MPLS

Le SR-MPLS est un routage de segment basé sur le plan de données MPLS, il s'applique au plan de données MPLS, sans modification de son architecture, ce qui ne nécessite pas de changement matériel. Cependant, il nécessite une évolution sur le plan de contrôle, entraînant une évolution logicielle des routeurs.

3.4 Terminologie

Nous allons définir dans cette section la terminologie qui sera utilisée dans le reste de ce mémoire.

3.4.1 Segment

Le segment est l'un des principaux concepts du Segment Routing, il peut représenter un composant physique du réseau tel qu'un nœud ou un lien, ou un composant logique tel qu'un service ou une application. À l'entrée du réseau, un ensemble de segments est assigné à chaque paquet en fonction des actions demandées (routage spécial, service particulier...) permettant ainsi de programmer la transmission directement depuis l'entrée du réseau. Un segment est identifié par un identifiant de segment Segment Identifier (SID) qui est inséré dans l'en-tête du paquet. Les segments sont distribués et signalés à travers le réseau à l'aide d'un contrôleur via des protocoles Path Computation Element Communication Protocol (PCEP) ou Network Configuration (NETCONF) dans une approche centralisée ou des protocoles de routage IGP et BGP dans une approche distribuée. Pour tous ces protocoles, des extensions sont définies pour inclure des informations de Segment Routing [9].

3.4.2 Segment actif

C'est le segment qui doit être utilisé par le routeur récepteur pour traiter le paquet. Dans le plan de données MPLS, il s'agit de l'étiquette de sommet du paquet [9]. Chaque SID du paquet SR devient au moins une fois actif avant que le paquet n'atteigne sa destination. Un SID global peut rester actif et s'étend sur plusieurs nœuds, par contre, un SID local n'est actif que sur le nœud qui le publie.

3.4.3 SRGB

Un Segment Routing Global Block (SRGB) est l'ensemble des segments globaux dans le domaine SR [9]. La plage SRGB par défaut est 16000-23999. Il est fortement recommandé d'utiliser le même SRGB sur tous les nœuds. Néanmoins, il est également possible d'utiliser différents SRGB sur différents nœuds mais cela rend les opérations plus compliquées.

Chaque noeud annonce son SRGB suivi d'un index Prefix-SID unique à l'échelle du domaine, puis il calcule les labels qui identifient les SID globaux. Une fois calculés ils serrent placé dans la table LFIB de chaque noeud.

3.4.4 SRLB

Segment Routing Local Block (SRLB) est un ensemble d'étiquettes locales réservées aux segments locaux. Ces étiquettes sont localement significatives et valide uniquement pour les noeuds qui les allouent [9].

3.4.5 Segment global

C'est un segment unique dans un domaine SR, il prend une valeur incluse dans la SRGB [9]. Ajoutons qu'il est lié à une instruction prise en charge par tous les nœuds du domaine. C'est-à-dire qu'il possède une entrée qui figure dans les tables de transfert de tous les nœuds du domaine. Accordant ainsi un avantage considérable pour le SR en réduisant l'état du plan de données à chaque saut. Le SID global est calculé en additionnant l'index du préfix-SID à la limite inférieur de son SRGB.

$$\text{SID global} = \text{index Prefix-SID} + \text{base SRGB}.$$

SID global $\leq limitesuprieureduSRGB$.

3.4.6 Segment local

C'est un segment dont la valeur est en dehors du SRGB et incluse dans le SRLB. l'instruction associée est définie au niveau du nœud qui en est à l'origine [9]. Un noeud n'a pas connaissance des segments locaux des autres noeud dans un domaine. Donc, le même SID peut être réutilisé par d'autres nœuds du même domaine. Notons que le segment local est lu par tous les nœuds mais seul son propriétaire installe une entrée de transfert qui lui est associée.

3.4.7 PCE

Un Path Computation Element (PCE) ou élément de calcul de chemin est un composant système, une application ou un nœud qui est capable de déterminer et de trouver le chemin approprié en fonction des contraintes pour transporter les données entre la source et la destination. Le noeud connecté au PCE est appelé Path Computation Client (PCC) lorsqu'il a besoin d'un chemin, il fait une demande au PCE en utilisant le protocole PCEP. Le PCE a accès aux informations de topologie pour l'ensemble du réseau et les utilises dans les calculs de chemin.

3.5 Identificateurs de segments

Les identificateurs de segment SID sont utilisés dans le réseau SR pour identifier différentes parties du réseau, ils sont schématisés sur la figure 3.1.

Nous allons découvrir dans cette section les différents segments distribués par l'IGP.

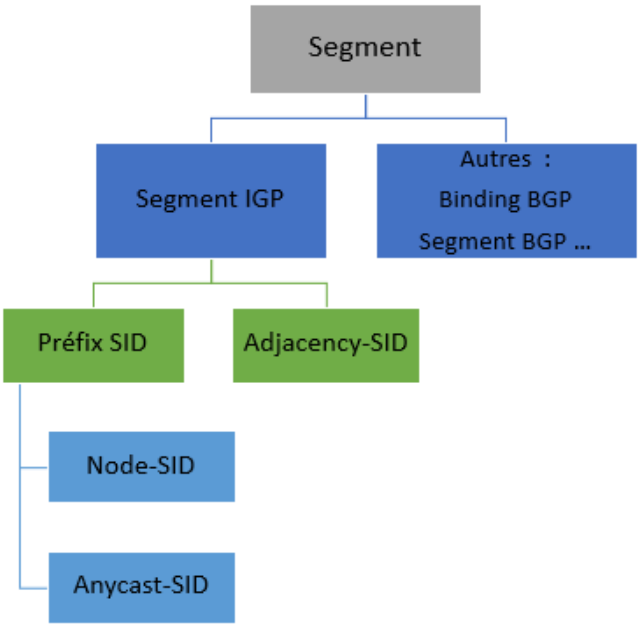


FIGURE 3.1 – Segments SR

3.5.1 Prefix SID

Un préfixe-SID est un segment globale et est associé à un préfixe IP, généralement avec une adresse de loopback. Il dirige le traffic sur le chemin le plus court calculé par IGP pour rejoindre le nœud pointé par le prefix SID [9]. Il est allouer à partir du SRGB et il est distribué par le protocole IS-IS ou OSPF.

Notons bien qu'un prefix SID doit être unique sur le réseau et connu de tous les équipements, qui sauront ainsi comment l'interpréter.

Un préfixe SID peut représenter un nœud ou un groupe de nœuds dans un domaine IGP et il est divisé en Node-SID et Anycast-SID :

3.5.1.1 Node-SID

Un Node-SID fait référence à un noeud spécifique. Il possède une signification globale et il identifie le préfixe avec l'adresse loopback du nœud [9].

Dans l'exemple illustré dans la figure 3.2 nous avons un réseau composé de cinq noeuds, chaque noeud possède son propre Node SID unique, par exemple Skikda distribue son Node SID 16006 . Si on veut envoyer le traffic vers Skikda, tous les noeuds savent qu'ils doivent utiliser

le SID 16006, ainsi, nous utiliserons le même SID dans tout le réseau, contrairement à LDP où le label change dans chaque saut.

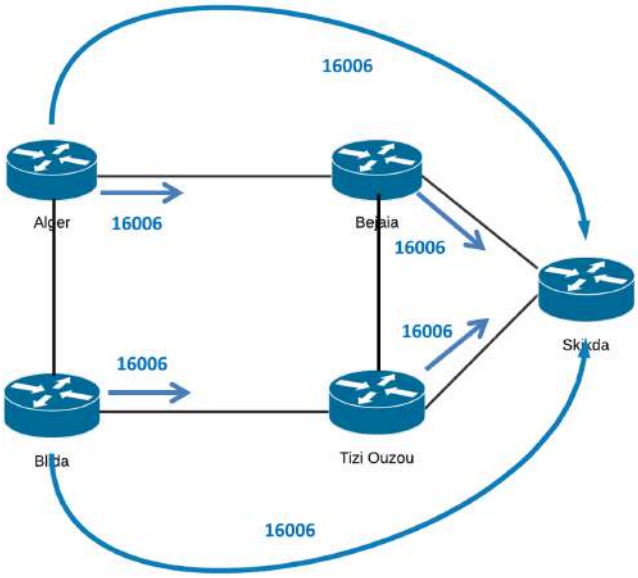


FIGURE 3.2 – Node Segment ID

3.5.1.2 Anycast-SID

Il identifie un ensemble de routeurs d'un même domaine SR qui ont le même préfixe avec la même valeur SID [9]. Il permet l'utilisation de chemins disjoints dans le réseau dans le but de séparer deux services afin qu'ils ne puissent pas passer par le même routeur. Il est utile pour des mécanismes de protection par exemple.

Les Anycast-SID sont configurés en attribuant un SID secondaire au routeur. Dans l'exemple de la figure 3.3 les routeurs Mostaganem et Alger, de plus de leur Prefix ID ils ont été configurés avec l'Anycast SID de 16200 et les routeurs Relizane et Blida avec l'Anycast SID de 16300. Les liaisons croisées seront utilisées que si l'un des chemins principaux échoue. Le premier service d'Oran à Setif utilise un tunnel SR-TE avec les segments 16200 et 16109 pour atteindre Setif. De même, de Tlemcen à Bejaia est configuré avec les segments 16300 et 16004.

3.5.2 Adjacency SID

Il identifie les liens entre les nœuds, soit une paire par lien. Il est utilisé pour le Traffic Engineering et le FRR car il oblige les paquets à passer à travers un lien spécifique, ce qui offre un transfert de chemin plus précis qu'un Prefix-SID.

Le Adj-SID possède une signification locale, c'est-à-dire qu'un routeur gère les Adj-SID uniquement pour ses voisins, donc il n'est pas nécessairement unique dans le domaine SR.

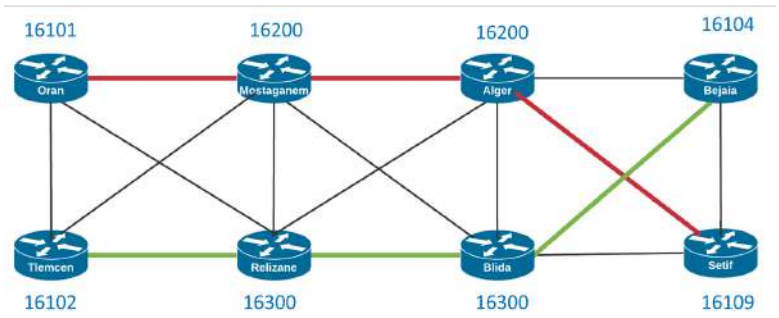


FIGURE 3.3 – Deux services disjoints

Les segment Adj-SID doivent prendre une valeur en dehors de l'intervalle SRGB, en générale ils sont allouées dynamiquement par un routeur mais ils peuvent être configurés manuellement.

Dans l'exemple de la figure 3.4 le routeur Tizi-Ouzou possède trois liens d'adjacence, il attribut donc un Adj-SID diffèrent à chacun d'eux. Une fois qu'il voit un Adj-SID dans la pile d'étiquettes entrante, il sait sur quel lien le trafic doit être transmis.

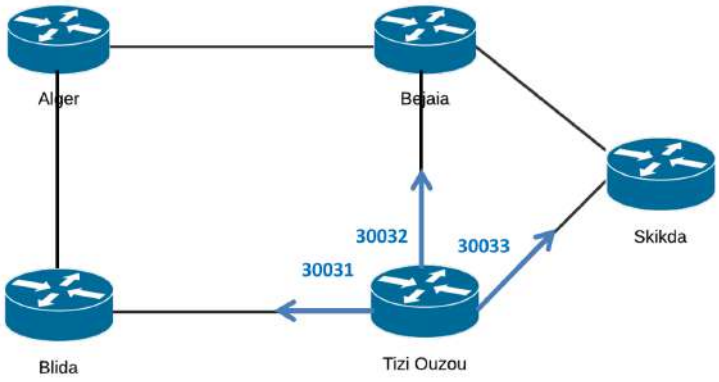


FIGURE 3.4 – Adjacency SID

3.5.3 Binding SID

Le BSID est lié à une politique et donc, à une liste de SID. Tous les paquets reçus avec un segment actif égal à BSID sont dirigés vers la politique SR liée. Un BSID peut être un SID local ou global. Son utilisation permet de diminue le nombre de segments imposés par la source aussi il permet à l'instanciation de la politique d'être stockée uniquement sur les nœuds qui sont concernés par la politique et si la politique change, seuls les nœuds concernés sont mis à jours fournissant ainsi plus d'évolutivité [9].

3.6 De l'MPLS vers le Segment Routing

Nous avons vu qu'en MPLS, les principaux protocoles de distributions d'étiquettes utilisés sont LDP et RSVP-TE. La nouveauté du SR réside dans le fait qu'il élimine le besoin des protocoles de distribution tout en étendant les protocole IGP et EGP déjà déployés. En effet, contrairement au LDP qui fonctionne comme un deuxième émetteur d'IGP pour associer à chaque adresse IP une étiquette MPLS valide localement, le SR supprime le rôle du deuxième émetteur et définit un SID unique pour identifier un noeud globalement, ainsi, les paquets peuvent être transférés vers le noeud en se basant sur son SID global, de cette façon, le ECMP peut être implémenté, chose qui n'est pas possible avec le RSVP-TE.

D'un coté, si le chemin optimal choisi par l'IGP est encombré, on a besoin d'effectuer du Traffic Engineering, chose qui n'est pas possible avec le LDP et qui est complexe avec le RSVP-TE, elle est possible avec le SR qui introduit le concept d'ID adjacent. Cet ID identifie de manière unique un lien local qui force le trafic à emprunter un chemin.

D'un autre coté, l'introduction d'un contrôleur centralisé révolutionne l'ingénierie de trafic et résout la principale cause de la complexité de RSVP-TE qui réside dans le fait que chaque noeud du réseau doit maintenir un ensemble de signalisation complexe.

Le SR résout ce problème en supprimant le mécanisme de signalisation. Il change l'architecture distribuée en une architecture centralisée qui correspond à l'architecture des réseaux SDN en ajoutant le contrôle centralisé pour permettre le Traffic Engeneering et avoir une surveillance et un contrôle complet du réseau en temps réel. Après le déploiement d'un contrôleur, toutes les informations sur la configuration du réseau sont acquises et la configuration manuelle des tunnels peut être omise.

Par ailleurs, le Segment Routing introduit le Topology Independent-Loop-Free Alternate (TI-LFA) comme solution fiable de FRR afin de réacheminer rapidement le trafic en cas de panne d'un lien ou d'un noeud et cela, en assurant une couverture totale du réseau, ce qui permet de remédier aux problèmes du LFA et Remote Loop free Alternate (RLFA).

Les différences entre le Segment Routing et le MPLS sont résumés dans le tableau 3.4

3.7 Opérations de Segment Routing

Les opération qui peuvent êtres effectuées sur les segments sont très similaires à celles effectuées sur les étiquettes MPLS. Ces opérations sont :

— **PUSH :** Action d'ajout d'un ou plusieurs segments devant l'en-tête SR du paquet.

— **CONTINUE :** Action de transfert effectuée sur la base du segment actif qui correspond

à changer une étiquette entrante par une étiquette sortante.

— **NEXT :** Action de suppression du segment actif de la pile et marquage du segment suivant comme segment actif.

3.8 Acheminement des paquets en SR

Les chemins LSP sont composés d'une liste ordonnée de différents types de SID, ils sont calculés soit via l'algorithme du plus court chemin, soit manuellement par l'administrateur, soit via un contrôleur centralisé.

Pour acheminer les paquets, chacun des noeuds présent dans le réseau traite l'en-tête et exécute les instructions encodées du segment actif dans la table de transfert pour savoir comment transmettre le paquet au saut suivant. Une fois traité, le paquet sera redirigé en se basant sur l'entrée du segment actif présente dans la table LFIB.

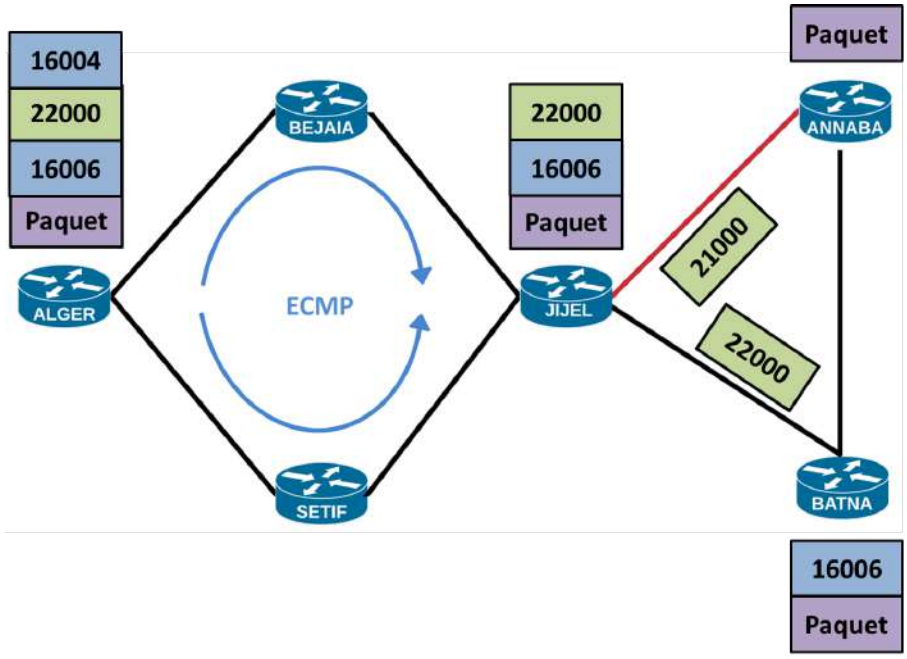


FIGURE 3.5 – Acheminement d'un paquet en SR

Selon l'exemple illustré sur la figure 3.5 un paquet est envoyé d'Alger vers Annaba, les deux chemins Alger - Bejaia - Jijel et Alger - Setif - Jijel ont la même préférence, on peut passer par les deux, puis le chemin Jijel - Annaba (le lien rouge) est le chemin le plus court choisit par l'IGP. Néanmoins ce chemin est encombré. On souhaite passer par le lien noir (Jijel - Batna - Annaba).

Pour effectuer cela, on attribue à Jijel un Node-SID de valeur 16004, à Annaba un Node-SID de valeur 16006, et pour forcer le trafic via un lien particulier pour permettre l'ingénierie du trafic, on attribue au lien rouge un ADJ-SID de valeur 21000 et au lien noir un ADJ-SID de valeur 22000.

Le routeur d'entrée, Alger, effectue l'opération PUSH, il ajoute la liste des SID qui composent le chemin que devra suivre le paquet, à savoir, le Node-SID de Jijel, le ADJ-SID du lien noir et le Node-SID de Skikda. Ensuite, il envoie le paquet à Bejaia. A la réception du paquet par Bejaia, celui-ci trouve qu'il ne lui est pas destiné, il transfert le paquet vers l'interface de sortie en direction du prochain saut Jijel. Une fois le paquet arrivé à Jijel, il s'aperçoit que le segment actif est son Node-SID, il effectue l'opération NEXT pour le supprimer puis il découvre l'étiquette d'adjacence 22000 indiquant le lien noir, il envoie donc le paquet via ce lien en direction de Batna. Batna reçoit le paquet et l'envoie à son tour vers Annaba qui découvre que son Node-SID est le segment actif et donc le paquet lui ai destiné et enfin il supprime le segment.

3.9 Extensions des protocoles IGP

L'un des plus grands avantages du SR est que la communication de labels et la diffusion d'informations sur la topologie se fait via l'IGP et le BGP. L'utilisation des protocoles LDP et RSVP-TE n'est plus nécessaire. Pour cela, les protocoles classiques sont étendus pour supporter les préfixes SR. Nous verrons dans cette sections les extensions des protocoles pour supporter le SR.

3.9.1 Extensions d'OSPF

Pour activer le SR, OSPF étend ses TLV pour transporter et diffuser les informations nécessaires. Les tableaux 3.1 et 3.2 définissent les nouvelles extensions [12].

TLV	Fonction
SR-Algorithm TLV	Annonce l'algorithme utilisé
SID/Label Range TLV	Annonce le SR SID ou la portée SRGB.
SR Local Block TLV	Annonce le SRLB.
SRMS Preference TLV	Annonce une préférence associée au nœud qui agit comme un serveur de mappage SR

Table 3.1 – Extension TLV OSPF pour SR

Sub-TLV	Fonction
SID/Label Sub-TLV	Annonce les SR SID ou les étiquettes MPLS.
Prefix SID Sub-TLV	Annonce les SR préfixe SID
Adj-SID Sub-TLV	Annonce les SR Adjacency SID sur un réseau P2P.
LAN Adj-SID Sub-TLV	Annonce les SR Adjacency SID sur un réseau local.

Table 3.2 – Extension SUB TLV OSPF pour SR

3.9.2 Extensions d'IS-IS

Pour activer le SR, IS-IS étend ses TLV pour transporter et diffuser les informations nécessaires, ces extensions sont définies dans le tableau 3.3 [17].

Sub-TLV	Fonction
Prefix-SID Sub-TLV	Annonce le prefixe SID
Adj-SID Sub-TLV	Annonce le Adjacency SIDs dans les réseaux P2P
LAN-Adj-SID Sub-TLV	annonce les SID SR Adjacency sur un réseau local
SID/Label Sub-TLV	Annonce les SR SID ou les étiquettes MPLS
SID/Label Binding TLV	Annonce un mappage entre le préfixe et le SID.
SR-Capabilities Sub-TLV	Annonce les capacités SR.
SR-Algorithm Sub-TLV	Annonce l'algorithme utilisé
SR Local Block Sub-TLV	Annonce le SRLB

TABLE 3.3 – Extensions IS-IS pour SR

3.10 Extensions du protocole BGP

3.10.1 BGP-Prefix-SID

Les Segments IGP ne sont pas suffisants pour transmettre les informations du Traffic Engineering d'un domaine à l'autre. Le protocole BGP a été étendu pour prendre en charge le Segment Routing et transmettre le trafic vers l'extérieur du domaine.
Pour prendre en charge le SR, BGP nécessite la possibilité d'annoncer un identificateur de segment (SID) pour un préfixe BGP. Des segments sont associés à un préfixe BGP et ils sont identifiés par un BGP-Prefix-SID. Un BGP-Prefix-SID est global au sein d'un domaine. Il identifie une instruction pour transmettre le paquet sur le meilleur chemin compatible ECMP calculé par BGP vers la destination specifiée. Il est configuré manuellement à partir de la plage d'étiquettes du SRGB.

3.10.2 BGP-LS

Le BGP-LS est une extension du BGP conçue pour transporter et partager les informations d'état de liaison collectées par le IGP à un PCE pour que ce dernier aie une image complète de la topologie. Afin de supporter le SR, BGP-LS définit :

— Un nouveau type de Network Layer Reachability Information (NLRI) BGP qui comporte un NLRI de noeud qui identifie le routeur, un NLRI de lien qui identifie le lien et un NLRI de préfixe qui identifie un préfixe IPv4 ou IPv6.

— Un nouvel attribut. Attribut BGP-LS qui est facultatif, il est au format TLV, il comprend les attributs nécessaires pour caractériser les objets décrits ci-dessus, c'est-à-dire

les NLRI de noeud, lien et préfixe. Par exemple, il peut s'agir de noms de nœuds, de métriques IGP, de métriques TE, de Bande passante disponible...[16].

3.11 Applications du SR

Les applications du SR sont diverses, nous allons présenter dans cette section une liste non exhaustive des applications du SR à savoir le FRR qui permet une protection et une récupération rapide en cas de pane d'un lien ou d'un noeud, le VPN où le SR simplifie son déploiement et le TE où il est remarquablement amélioré.

3.11.1 FastReroute avec SR

Le FRR ou réacheminement rapide est un mécanisme essentiel dans tout réseau de communication fiable, permettant de récupérer rapidement et localement, des défaillances du réseau, sans invoquer le plan de contrôle. Autrement dit, c'est la protection du trafic en cas de panne d'un nœud ou d'un lien.

Le SR combine entre le TI-LFA et Bidirectional Forwarding Detection (BFD) pour fournir une solution efficace au FRR. On utilise BFD pour détecter une défaillance et TI-LFA pour choisir un chemin de post-convergence sans attendre une reconvergence de l'IGP. TI-LFA couvre toute sorte de pannes et redirige le trafic ultra rapidement. Avant TI-LFA, LFA et RLFA ont été utilisées pendant des années pour le FRR.

Le TI-LFA étend le LFA et le RLFA en permettant au PLR qui est le routeur relié au lien qui est en panne d'utiliser des piles d'étiquettes plus profondes pour construire des chemins de sauvegarde. De plus, il garantit de pouvoir trouver une protection quels que soient la panne, son type, la topologie du réseau et la destination. De surcroît, le chemin de post-convergence est le meilleur chemin possible qu'un IGP aurait choisi.

Chaque noeud et chaque lien possède un chemin de sauvegarde pré-calculé et préinstallé dans le plan de données. Le temps de convergence pour un chemin est de 50 millisecondes ou moins [27]. Cela signifie que même les applications les plus sensibles à la latence ou à la perte de paquets peuvent fonctionner sans interruption en cas de défaillance d'un nœud ou d'une liaison.
TI-LFA calcule le chemin de sauvegarde en supprimant temporairement le lien ou le nœud de la base de données. Ensuite, il calcule le chemin de sauvegarde qui soit le plus court avec la meilleure métrique. Une liste d'étiquettes détermine le nouvel itinéraire vers la destination.

Le TI-LFA nécessite le Segment Routing, c'est pourquoi les opérateurs optent pour cette technologie, notament pour les divers avantages suivant :

— Répond aux exigences de base de la convergence rapide de IP FRR.
— Prend théoriquement en charge tous les scénarios de protection (liens, noeuds).
— Très simple à déployer. Pas besoin d'exécuter et de gérer un protocole supplémentaire.
— Il peut fonctionner et fournir une commutation de moins de 50 ms dans n'importe quelle topologie.
— Sélectionne un chemin de sauvegarde sur une route convergée et n'a pas d'état intermédiaire, par rapport aux autres techniques FRR.

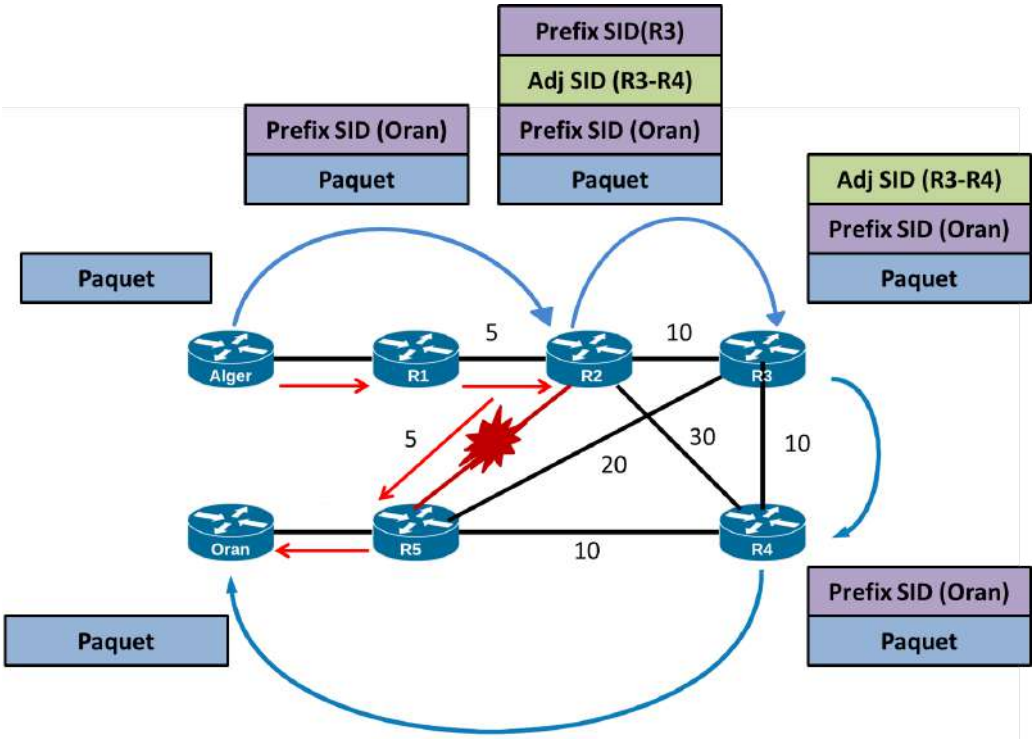


FIGURE 3.6 – TI-LFA

Dans l'exemple présenté dans la figure 3.6, le plus court chemin pour atteindre Oran à partir d'Alger est R1→R2→R5. R2 installe dans sa table de forwarding des entrées alternatives pour re-router le traffic vers R3 en cas où R5 est inaccessible via R2.

Lorsque le paquet arrive à R2, R2 détecte que le lien entre R2 et R5 est en panne à l'aide du BFD, R2 active les entrées de sauvegarde TI-LFA FRR et ajoute de nouvelles informations de chemin (les étiquettes) au paquets pour garantir la transmission des paquets le long du chemin de sauvegarde. Il calcule alors le chemin de post-convergence, R2→R3→R4→R5, qui est plus court que les deux autres chemins alternatifs, il insère le Prefix d'Adjcency entre R3 et R4 ainsi que le Prefix SID de R3 et envoie le paquet à R3. R3 supprime son Prefix SID et envoie le paquet vers R4 grâce au label d'adjacency R3-R4, R4 supprime ce label et envoie le paquet vers Oran. Tout cela se passe en moins de 50 milisecondes et sans attendre l'IGP.

3.11.2 VPN avec le Segment Routing

MPLS est essentiellement utilisé par les fournisseurs de service car il offre la possibilité de créer des VPN comme nous avons vu dans la section 2.6.1.

le SR révolutionne cette fonctionnalité en simplifiant le déploiement des VPN qui ce traduit par l'élimination des protocoles de signalisation LDP et RSVP-TE.
En réalité, le VPN-MPLS et le SR ne s'excluent pas mutuellement mais ils sont complémentaires, car le SR fournit le transport et le VPN-MPLS fournit le service. Nous allons voir à travers l'exemple illustré dans la figure 3.7 comment le VPN fonctionne dans le cas du Segment Routing.

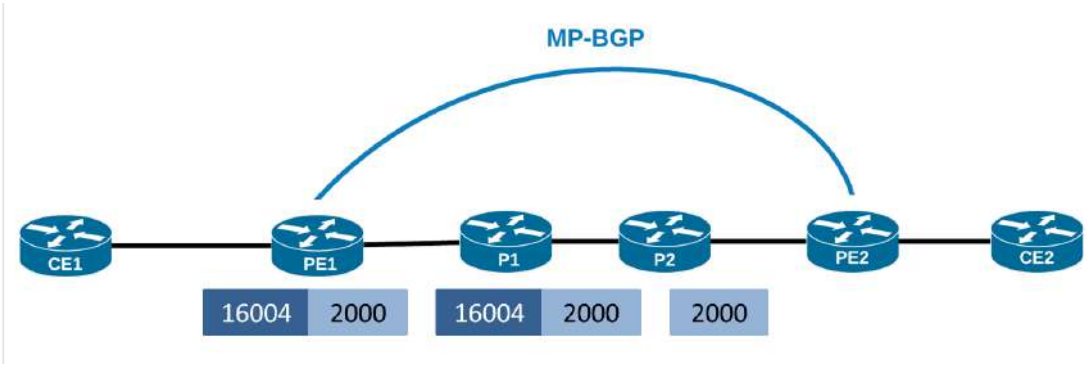


FIGURE 3.7 – Un VPN sous SR

Supposons que nous voulons créer un VPN entre CE1 et CE2, on active le SR dans les routeurs du réseau coeur. IGP est utilisé pour échanger des informations SR (Préfixes, SRGB...) ce qui élimine le besoin d'utiliser un protocole de signalisation et résout le problème de synchronisation entre LDP et IGP. L'équilibrage de charge ECMP est activé par défaut. Les services Target-LDP (T-LDP) et MP-BGP sont configurés entre PE1 et PE2 afin de distribuer les labels VPN entre les extrémités du réseau. Le déroulement du processus est comme suit :

1. CE2 annonce son adresse (son préfixe) à PE2.
2. PE2 installe le préfixe dans la VRF appropriée, il le lie au label VPN 2000 et l'annonce à PE1 en utilisant MP-BGP.
3. PE1 PUSH l'étiquette 2000 distribué par PE2 et le segment 16004 qui est le SID du routeur PE2 et qui est distribué via l'IGP (les sub-TLV d'IS-IS ou les LSA d'OSPF). Tous les autres routeurs exécutent ce même segment unique pour atteindre le noeud PE2, contrairement à LDP où l'étiquette change d'un routeur à l'autre.
4. P1 transmet le paquet à P2 sans apporter de changement à la pile d'étiquette.
5. Si P2 reçoit une étiquette spéciale de PE2 pour supprimer le segment, il exécute PHP et supprime le segment 16004 et seul l'étiquette VPN est envoyée à PE2. Quand ce dernier reçoit le paquet il supprime l'étiquette 2000 et envoie le paquet IP vers la destination

CE2.

3.11.3 TE avec le Segment Routing

Le Segment Routing - Traffic Engineering (SR-TE) surmonte les limites et les problèmes d'évolutivé identifiés dans le MPLS-TE en offrant une nouvelle technique d'ingénierie de traffic basée sur une extension IGP fournissant une évolutivité et une flexibilité améliorées tout en répondant aux nouvelles exigences du SDN.

3.11.3.1 Fonctionnement

En SR, il n'y a pas de protocoles de signalisation comme RSVP-TE. Un contrôleur centralisé appelé PCE peut être introduit dans le réseau pour prendre en charge le TE et mettre à jour la disponibilité des ressources et garantir les contraintes QoS.
Une fois que les prefix et adjacency SID sont distribués, le contrôleur acquiert une vue globale sur le réseau puis stocke les informations des noeuds et des liens dans une base de données Traffic Engineering Database (TED).
Le PCE établit une session BGP-LS avec au moins un nœud du réseau SR afin de récupérer la topologie. En plus du TED, le contrôleur gère une base de données de chemins appelée LSP-DB. Il maintient les deux bases de données à jour et synchronisées avec ce qui existe réellement sur le réseau physique (chemins instanciés et leur exigence de QoS, réservation de ressources, etc.), afin d'effectuer correctement le calcul de chemin et de mettre à jour correctement les ressources disponibles sur les liens.
Les routeurs PE agissent comme des clients de calcul de chemin PCC. Un PCC établit une session PCEP avec le PCE puis lance des demandes de calcul de chemin pour des FEC spécifiques. Une requête contient les paramètres suivants : adresses IP source et destination, exigences TE (bande passante, retard, gigue) qui seront utilisées pour calculer le chemin. Une fois le chemin calculé, le PCE envoie via le protocole PCEP au PCC la liste des SID qui compose le chemin appartenant à la FEC. Une fois signalé par le PCC, le PCE stocke dans la LSP-DB le nouveau chemin avec ses caractéristiques TE comme la quantité de bande passante utilisée. Ceci est nécessaire afin de maintenir l'état de réservation de bande passante dans le réseau et permet de nouveaux calculs de chemin qui tiennent compte des réservations précédentes. La figure 3.8 illustre ce processus.

Ce type d'architecture s'inscrit dans l'esprit de l'approche SDN, où les fonctionnalités PCE et le protocole PCEP peuvent être intégrées directement dans un contrôleur SDN. Le SDN est détaillé dans la section 3.12

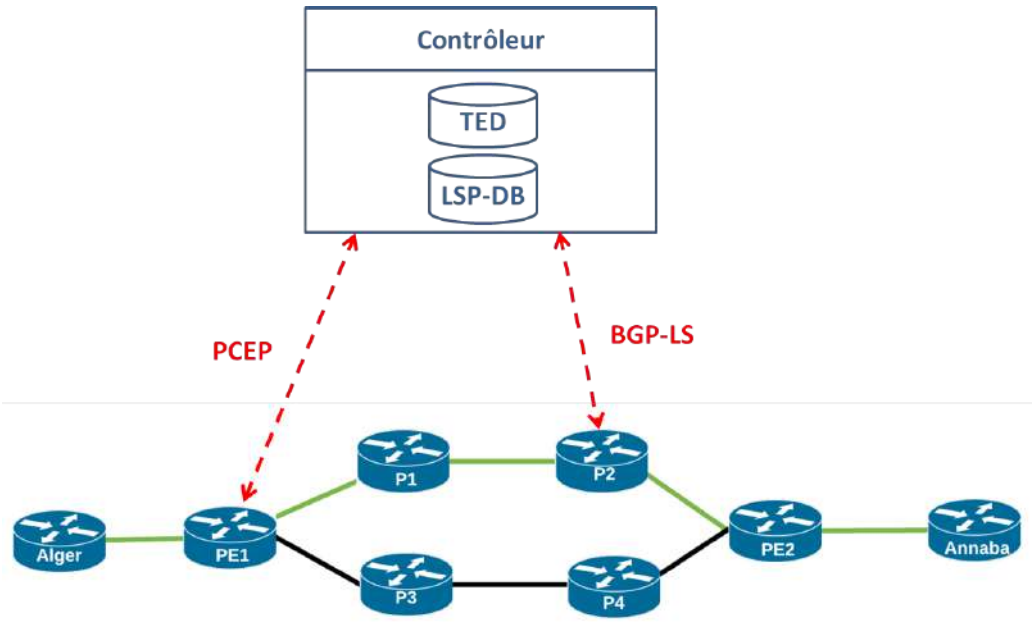


FIGURE 3.8 – TE en SR

3.11.3.2 Stratégie SR

Le Segment routing utilise une stratégie pour diriger le trafic à travers le réseau. La stratégie est identifiée par :

- Tête de réseau, où la politique est initiée
- Point final, qui est la destination de la stratégie.
- Couleur, une valeur numérique arbitraire qui montre différents types de politique, par exemple, vert pour un chemin à faible latence ; rouge pour un chemin à bande passante élevée.

La stratégie est associée à un ou plusieurs chemins candidats, un chemin candidat est exprimé sous la forme d'une liste de segments appelée liste de SID avec un poids, qui permettent de spécifier le chemin vers la destination. La sélection du chemin se fait en fonction de la valeur de la priorité la pus élevé. Le meilleur chemin sélectionné est enregistré dans table FIB, il est identifié par un Biding SID et il possède un état (valide ou invalide) et le protocole source(BGP, statique ou PCEP).

L'exemple présenté dans la figure 3.9 illustre un réseau pour transporter les paquets entre Alger et Annaba, il existe deux classes de trafic (bleu et vert), chacune possède une stratégie de routage. La première stratégie possède deux chemins candidats, la deuxième possède un seul.

Chaque stratégie SR possède un Binding SID pour diriger le trafic. Il est fondamental pour le SR-TE et apporte évolutivité et indépendance de service au segment routing. Généralement,

0. https ://tools.ietf.org/pdf/draft-ietf-spring-segment-routing-policy-07.pdf

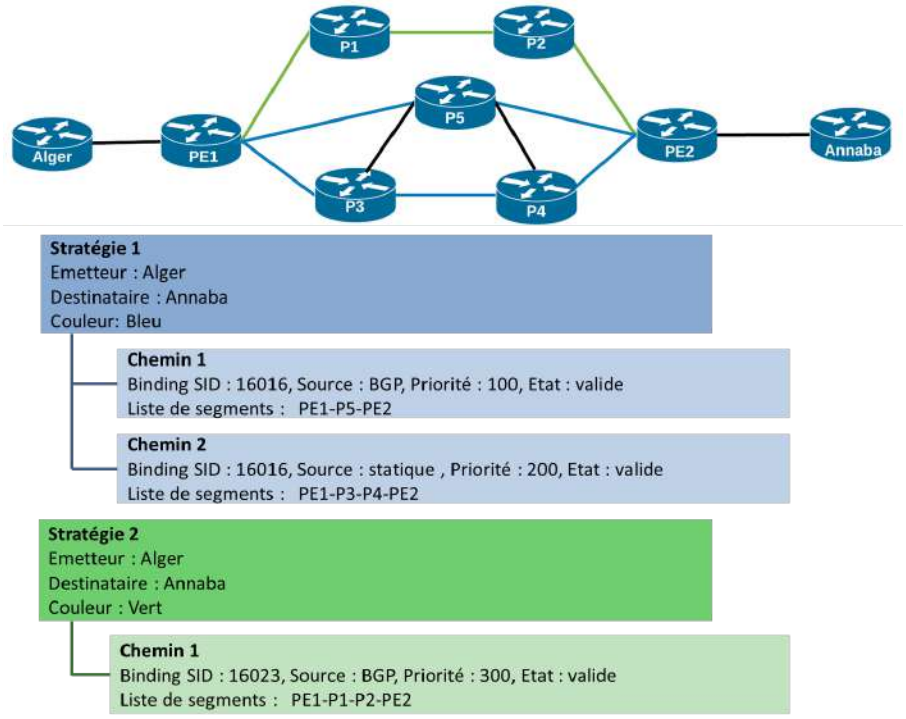


FIGURE 3.9 – Stratégie SR

tous les chemins candidats d'une stratégie SR se voient attribuer le même BSID.

3.12 Segment routing et SDN

Le Segment routing a été conçu avec un contrôleur SDN à l'esprit, bien qu'il ne le nécessite pas forcement pour fonctionner mais leur combinaison est très puissante. Dans cette section nous expliquons d'abord le concept de la technologie du SDN ensuite nous présentons son utilisation avec le Segment Routing.

3.12.1 SDN

Dans les réseaux traditionnels, le contrôle et les protocoles distribués sur les périphériques rendent ces dernières responsables de prendre des décisions de manière autonome, mais cette programmation est rigide, elle ne peut être changée que manuellement, ce qui prend évidemment du temps et ne se prête guère à des changements de contexte rapides causés principalement par le manque d'automatisation.
Pour surmonter ces limites et apporter de la souplesse au déploiement de services réseaux, un nouveau paradigme a été proposé et qui est la mise en réseau définie par logiciel SDN.

3.12.1.1 Définition

Le SDN désigne le fait de piloter une infrastructure réseau par un logiciel. L'idée est de mettre en place un ou plusieurs serveurs centralisés nommé contrôleur SDN, qui ont une vision globale du réseau, capables de piloter tout ou partie des composants réseau (physiques ou virtuels) de l'infrastructure ainsi que de s'informer en temps réel sur leurs état et activité [34].

Le principe du SDN est le suivant :

— Séparer le plan de contrôle constituant les informations de routages (la table RIB par exemple) du plan de donné qui permet d'acheminer des paquets en se basant sur des informations contenu dans des tables (FIB par exemple).
— Centraliser et mutualiser le plan de contrôle entre tous les équipements.
— Réduire les équipements à leur fonction la plus élémentaire : transmettre (ou ne pas transmettre) des données sur le réseau.
— Apporter de la souplesse en rendant le réseau programmables par le biais d'un contrôleur et d'API (interface de programmation applicative).
— La fonctionnalité de contrôle est placée sur une entité dédiée appelée contrôleur SDN.

3.12.1.2 Architecture du SDN

L'architecture du SDN comprend trois sections fonctionnelles [34]. illustrée dans la figure 3.10.

La couche infrastructure comprend des équipements de transmission réseau tel que les commutateurs et les routeurs, connectés de manière filaire ou sans fil. ils effectuent un ensemble d'opérations de transfert élémentaires. Ce sont des appareils programmables et ils se comportent selon des instructions envoyées par le contrôleur.

La communication entre le contrôleur SDN et les équipements programmables est orchestrée par les interfaces de programme d'application Southbound Application Protocols (SUD) qui utilise le plus couramment le protocole OpenFlow ou d'autres protocoles tel que (CLI, NETCONF/YANG, ...). Les SUD permettent un contrôle réseau efficace et facile et activent le contrôleur SDN pour apporter dynamiquement des changements dans le plan de transmission en temps réel.

Le contrôleur SDN est le cerveau du réseau, c'est un point de contrôle centralisé qui gère le contrôle de flux vers les périphériques réseaux et la logique des applications. Le contrôleur SDN fait une vue d'abstraction du réseau y compris les statistiques et l'état du réseau et l'envoie au niveau d'application. La notion d'abstraction signifie que le contrôleur offre des interfaces

programmables appelés Northbound Application Programming Interface (API) aux applications réseaux et se charge de piloter le plan de données en injectant des règles d'acheminement spécifiques répondant aux besoins des applications sans que les applications connaissent ces règles.

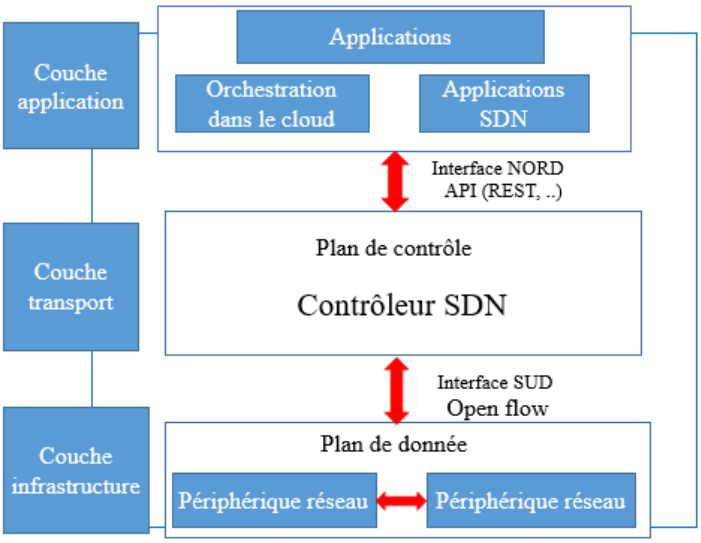


FIGURE 3.10 – Architecture SDN

3.12.1.3 Avantage du SDN

Le SDN permet plusieurs améliorations par rapport au fonctionnement classique :

— Meilleur contrôle du réseau, l'architecture centralisée simplifie l'administration d'une infrastructure de grande taille mais aussi elle offre une visibilité et un contrôle complet sur le réseau assurant un contrôle d'accès et une ingénierie du trafic appropriés.

— La programmabilité permet de répondre aux besoins d'automatisation afin d'améliorer les besoins du réseau et son orchestration.

— Réduction des dépenses opérationnelles, l'entreprise peut utiliser du matériel de différents fabriquants et exploiter les composants avec le moins de dépenses possibles.

— Garantir l'innovation car on peut introduire une nouvelle fonctionnalité très facilement, il suffit de l'implémenter sur le contrôleur.

3.12.2 SR-SDN

La combinaison du SR au SDN représente une proposition efficace pour les fournisseurs de service. Avec une vue globale du réseau fusionné à son intelligence le SDN est capable de traiter directement les exigences et mapper le trafic du chemin optimal sur les segments. Dans un environnement SR le SDN est généralement un PCE.

L'architecture Segment Routing est prête pour le SDN puisque elle permet de prendre des décisions de routage depuis une application en se basant sur des paramètres spécifiques tel que

la latence et la charge des liaisons sans pour autant informer le réseau.
Une interconnexion SR-SDN peut prendre en charge divers cas d'utilisation, les plus pertinents sont cités ci-après :

— Implémentation de SFC.
— Surveillance du réseau.
— Apport d'une grande flexibilité, un contrôle complet et des capacités TE pour le trafic réseau.

3.13 Segment Routing VS MPLS

Caractéristique	SR	MPLS
Distribution des étiquettes	Distribués par l'IGP	Distribués par RSVP-TE/LDP.
Allocation des étiquettes	Globale et locale	Locale
Plan de contrôle	Simple car le nombre de protocoles à utiliser est réduit.	Complexe.
FRR	Totale avec TI-LFA en $<$ 50ms	Partielle avec LFA et RLFA en $<$ 100ms
Synchronisation avec l'IGP pour le FRR	Non requise.	Requise.
ECMP	Supporté.	Non supporté avec RSVP-TE.
SDN	Supporté nativement.	Non supporté nativement.
Type du routage	Basé sur la source	Basé sur la destination
État du Traffic Engineering	Simple, seuls les noeuds d'extrémité sont configurés.	Complexe, tous les noeuds conservent des informations d'états et N*(N-1)/2 tunnels sont configurés entre tous les noeuds [N].
Scalabilité	Élevée	Réduite
IPv6	Native	Limité et exige des extensions

TABLE 3.4 – Différences entre SR et MPLS

D'après les études menées autour de l'MPLS et le Segment Routing, nous pouvons résumer les différences entre les deux technologies dans le tableau 3.4. Nous déduisons que nous pouvons certifier que le SR peut en effet apporter une valeur ajouté aux réseaux,compte tenu des nombreux avantages qu'il offre au détriment du MPLS.

3.14 Bénéfices apportés par Segment Routing

Après avoir étudié le Segment Routing, nous concluons qu'il offre les avantages suivants :

— **Simplicité**. Simple à utiliser, à entretenir et à dépanner.

— **Réacheminement rapide (FRR)**. garantie en 50ms. Protection dans tous les cas, liens et noeuds, pour une récupération rapide des pannes.
— **Évolutivité**. Évolutif car les noeuds du cœur du réseau ne conservent aucune information d'état permettant ainsi au réseau d'évoluer.
— **Ingénierie du trafic**. Contrôle complet de la manière dont le trafic est acheminé dans un environnement de contrôle distribué ou centralisé.
— **Meilleure évolution vers le réseau SDN**. La technique de segment routing et le SDN sont utilisés ensemble pour contrôler et ajuster de manière flexible et pratique les chemins.

3.15 Conclusion

A travers ce chapitre nous avons introduit le Segment Routing qui permet de remédier aux inconvénients des réseaux IP / MPLS existants en termes d'évolutivité, de simplicité et de facilité d'utilisation. Nous avons vu que cette technologie ne nécessite pas de protocole de distribution d'étiquettes LDP ou RSVP-TE car les étiquettes sont distribuées à l'aide du protocole IGP et du BGP. Le fait d'exécuter de moins de protocoles à l'intérieur du réseau le rend plus stable et évolutif. Les chemins de routage de segments sont protégés par la fonction FRR, qui permet de rediriger le trafic en moins de 50 millisecondes, en cas de défaillance de la liaison ou du nœud.
Nous avons également vu que cette technologie est conçue et construite pour l'ère SDN en mettant en place un contrôleur qui collecte les informations, telles que la topologie du réseau, l'utilisation de la bande passante et les informations de retard et qui calcul les chemins qui satisfont aux exigences de service.

Chapitre 4

Conception et implémentation

Dans ce chapitre nous allons mettre en pratique les concepts introduits dans les chapitres précédents. Nous réaliserons d'abord une topologie d'un réseau MPLS avec ses différentes applications similaire à celle du réseau actuel de l'organisme d'accueil, puis nous effectuerons sa migration vers le Segment Routing, ensuite nous introduirons un contrôleur SDN et enfin nous évaluerons les résultats des performances du réseau avant et après la migration.

4.1 EVE-NG

Emulated Virtual Environment Next Generation (EVE-NG) est un émulateur de réseau virtuel, qui permet la configuration des équipements et d'assurer leurs bon fonctionnement avant de les déployer réellement. Il est accessible par les navigateurs Web permetant ainsi d'offrir une excellente expérience d'apprentissage et il est multifournisseur permettant ainsi d'intégrer différents appareils dont ceux de Juniper.

4.2 Architecture du réseau IP/MPLS

L'architecture du réseau qu'on va simuler est illustrée dans la figure 4.26, elle est composée de trois AS. Le premier AS est le réseau coeur constitué de cinq routeurs implementant l'OSPF comme IGP et les deux autres AS sont deux réseaux d'agrégation implémentant le IS-IS comme IGP.

Nous allons utiliser des routeurs vMX qui sont des routeurs virtuels de Juniper pouvant être déployés sur des serveurs x86, Amazon Web Services (AWS), AWS GovCloud et Microsoft Azures... Un routeur vMX est composé de deux parties :

- **VCP** : Le plan de contrôle virtuel, alimenté par le système d'exploitation Junos hébergé sur une machine virtuelle.
- **VFP** : Le plan de transfert virtuel qui exécute le moteur de transfert de paquets, alimenté par vTrio, le microcode Trio programmable de Juniper.

Dans ce qui suit nous allons commencer par la configuration du réseau IP/MPLS puis nous enchaînons par sa migration vers un réseau Segment Routing. Dans la suite de ce travail nous prenons le routeur vMx1 comme exemple pour montrer les configurations effectuées au sein du réseau coeur et vMx6 pour le réseau d'agrégation 1.

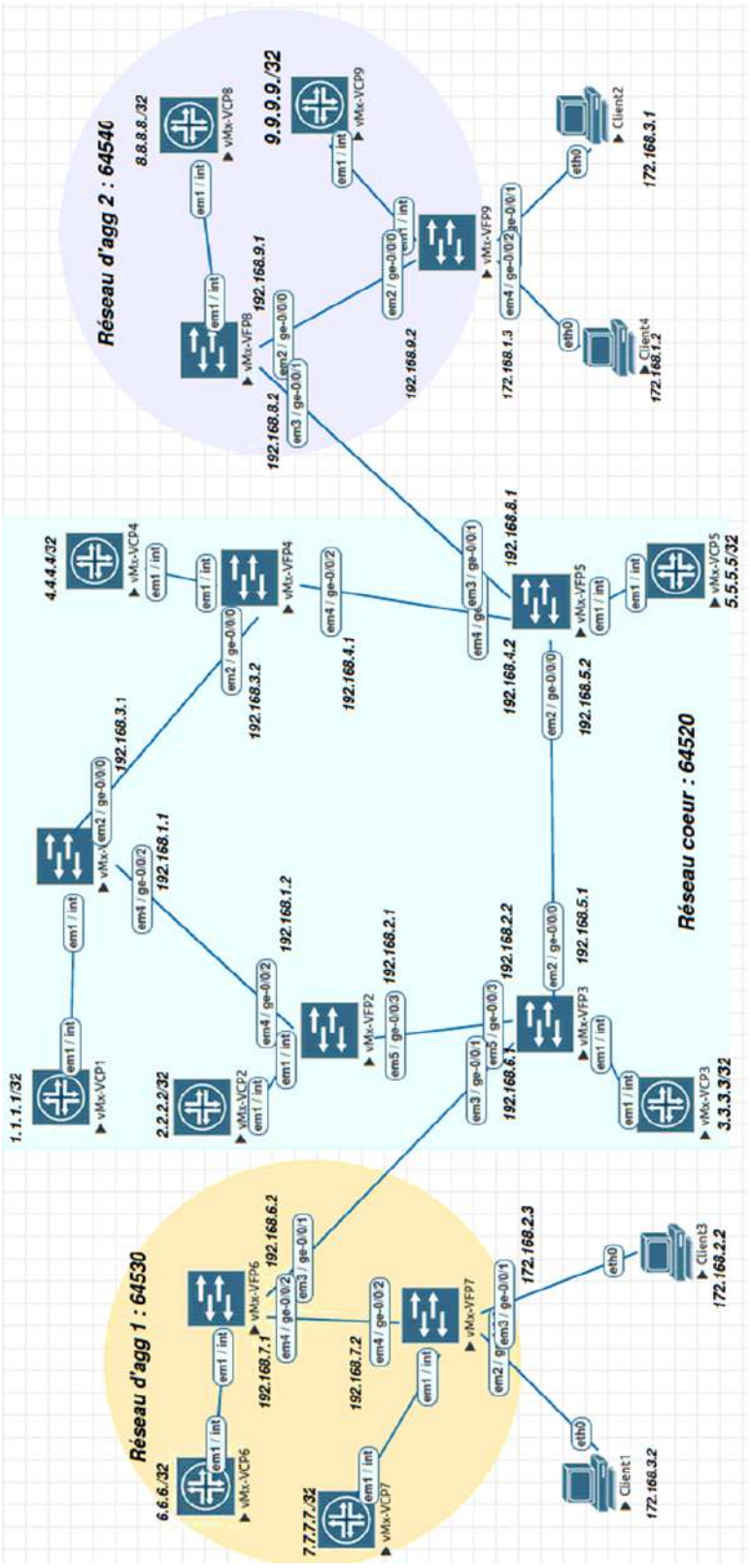


FIGURE 4.1 – Topologie du réseau simulé

4.3 Pré-configuration

4.3.1 Configuration des interfaces réseau

Nous commençons par relier les VCP et les VFP puis nous configurons les interfaces des routeurs en affectant à chacune une adresse IP via les commandes (3) et (4) ensuite nous configurons l'adresse de loopback via la commande (5). Le tableau 4.1 dans l'annexe A illustre l'adressage complet.

```
root@vMx1> configure
[edit]
root@vMx1# set interfaces ge-0/0/0 unit 0 family inet address 192.168.3.1/24
root@vMx1# set interfaces ge-0/0/2 unit 0 family inet address 192.168.1.1/24
root@vMx1# set interfaces lo0 unit 0 family inet 1.1.1.1/32
```

4.3.2 Configuration de l'IGP

Nous configurons l'IGP au sein de chaque AS. Au niveau du réseau coeur nous configurons l'OSPF sur toutes les interfaces par les commandes (2-5) et nous vérifions l'activation du protocole OSPF via la commande (8). La figure 4.2 montre la bonne configuration d'OSPF sur le routeur vMx1.

```
root@vMx1> configure
root@vMx1# edit protocols ospf
[edit protocols ospf]
root@vMx1# set area 0.0.0.0 interface ge-0/0/0
root@vMx1# set area 0.0.0.0 interface ge-0/0/2
root@vMx1# exit
[edit]
root@vMx1# run show ospf neighbor
```

```
root@vMx1# run show ospf neighbor
Address          Interface              State           ID               Pri  Dead
192.168.3.2      ge-0/0/0.0             Full            4.4.4.4          128    36
192.168.1.2      ge-0/0/2.0             Full            2.2.2.2          128    35
```

FIGURE 4.2 – Activation de OSPF sur le routeur vMx1

Nous configurons l'IS-IS sur les AS d'agrégation via les commandes (1-4) entre les routeurs vMx 6 et vMx 7 et entre vMx 8 et vMx 9. Ensuite comme IS-IS utilise l'adressage ISO nous ajoutons pour chaque interface la famille ISO via la commande (7) et nous ajoutons cette famille à l'adresse de loopback suivie de son adresse via la commande (8). Avec la commande (9) nous vérifions le bon établissement du protocole IS-IS.

```
root@vMx6# edit protocols isis
[edit protocols isis]
```

```
root@vMx6# set interface ge-0/0/2 level 2 metric 20
root@vMx6# set interface ge-0/0/2 level 1 disable
root@vMx6# exit
[edit]
root@vMx6# set interfaces ge-0/0/2 unit 0 family iso
root@vMx6# set interfaces lo0 unit 0 family iso address 49.0010.0100.1001.00
root@vMx6# run show isis adjacency
```

la figure 4.3 affiche le voisinage directe du routeur vMx6.

```
root@vMx6# run show isis adjacency
Interface             System         L State       Hold (secs) SNPA
ge-0/0/2.0            vMx7           1  Up                   22  50:0:0:f:0:4
```

FIGURE 4.3 – Activation d'IS-IS sur le routeur vMx6

Enfin, nous testons la connectivité entre les routeurs vMx1 et vMx5 pour le réseau coeur et entre vMx6 et vMx7 pour le réseau d'agrégation 1 avec la commande ***ping***. Les résultats sont affichés dans les figures 4.4 et 4.5.

```
root@vMx1# run ping 5.5.5.5 source 1.1.1.1
PING 5.5.5.5 (5.5.5.5): 56 data bytes
64 bytes from 5.5.5.5: icmp_seq=0 ttl=63 time=2331.521 ms
64 bytes from 5.5.5.5: icmp_seq=1 ttl=63 time=748.906 ms
64 bytes from 5.5.5.5: icmp_seq=2 ttl=63 time=34.193 ms
```

FIGURE 4.4 – Test ping entre vMx1 et vMx5

```
root@vMx6# run ping 7.7.7.7 source 6.6.6.6
PING 7.7.7.7 (7.7.7.7): 56 data bytes
64 bytes from 7.7.7.7: icmp_seq=0 ttl=64 time=275.037 ms
64 bytes from 7.7.7.7: icmp_seq=1 ttl=64 time=2.393 ms
64 bytes from 7.7.7.7: icmp_seq=2 ttl=64 time=2.393 ms
```

FIGURE 4.5 – Test ping entre vMx6 et vMx7

4.4 Configuration du MPLS

Pour déployer le MPLS et permettre aux interfaces d'échanger des labels, nous devons activer le MPLS sur chaque routeur et sur chaque interface puis rajouter la famille MPLS sur chaque interfaces sortante de ces routeurs.

```
root@vMx1# edit protocols mpls
[edit protocols mpls]
root@vMx1# set interface ge-0/0/0
root@vMx1# set interface ge-0/0/2
root@vMx1# exit
```

```
[edit]
root@vMx1# set interfaces ge-0/0/0  unit 0 family mpls
root@vMx1# set interfaces ge-0/0/2  unit 0 family mpls
```

4.4.1 Configuration du LDP

Une fois la configuration du MPLS faite, nous passons à l'activation du protocole de signalisation LDP sur toutes les interfaces qui sont dans le nuage MPLS. L'activation du LDP signifie qu'un LSP est automatiquement crée pour toutes les adresses de loopback pour chaque routeur de l'AS. Pour synchroniser le protocole LDP et IGP nous ajoutons la commande (5).

```
root@vMx1# edit protocols ldp
[edit protocols ldp]
 root@vMx1# set interface ge-0/0/0
 root@vMx1# set interface ge-0/0/2
 root@vMx1# set track-igp-metric
```

La consultation de la table mpls.0 qui stocke les étiquettes MPLS et l'action qu'un routeur doit effectuer lorsqu'il reçoit des paquets MPLS, illustrée dans la figure 4.6, nous permet de voir que la distribution d'étiquettes a été faite grâce au protocole LDP ainsi que les étiquettes distribuées et les opérations que les routeurs doivent effectuer sur chaque étiquette.

```
300304             *[LDP/9] 00:13:21, metric 1
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
300304(S=0)        *[LDP/9] 00:13:21, metric 1
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
300352             *[LDP/9] 00:13:03, metric 1
                    >  to 192.168.3.2 via ge-0/0/0.0, Pop
300352(S=0)        *[LDP/9] 00:13:03, metric 1
                    >  to 192.168.3.2 via ge-0/0/0.0, Pop
300368             *[LDP/9] 00:13:03, metric 1
                    >  to 192.168.3.2 via ge-0/0/0.0, Swap 300256
300384             *[LDP/9] 00:13:03, metric 1
                    >  to 192.168.1.2 via ge-0/0/2.0, Swap 300672
```

FIGURE 4.6 – Vérification de la distribution des labels

4.4.2 Configuration du RSVP-TE

Pour pouvoir créer des tunnels et mettre en oeuvre l'ingénierie de trafic dans le réseau, nous devons activer le protocole RSVP dans les interfaces des routeurs de chaque AS avec les commandes (1-4) puis nous devons permettre à l'IGP d'offrir les informations de topologie au protocole RSVP, grâce à la commande (7). La définition de plusieurs LSP permet de fournir différentes garanties de bande passante ou de performances. Ainsi le trafic prioritaire pourra se placer dans un LSP et le trafic de moyenne priorité dans un autre LSP. Pour notre réseau, nous créons deux LSP dans l'AS coeur. Le premier LSP relie les routeurs VMx1 et VMx3, le second

est crée entre les routeurs VMx1 et VMx5. Cette opération est faite à l'aide des commandes (8) et (9).

```
root@vMx1# edit protocols rsvp
[edit protocols rsvp]
root@vMx1#  set interface ge-0/0/0
root@vMx1#  set interface ge-0/0/2
root@vMx1# exit
[edit]
root@vMx1#  set protocols ospf traffic-engineering
root@vMx1#  set protocols mpls label-switched-path  vMx1-to-vMx5 to 5.5.5.5
root@vMx1#  set protocols mpls label-switched-path  vMx1-to-vMx3 to 3.3.3.3
```

Une fois les LSP crées, nous pouvons observer leur activation sur la figure 4.7.

```
root@vMx1# run show mpls lsp
Ingress LSP: 2 sessions
To              From            State Rt P     ActivePath       LSPname
3.3.3.3         1.1.1.1         Up     0 *                      vMx1-to-vMx3
5.5.5.5         1.1.1.1         Up     0 *                      vMx1-to-vMx5
Total 2 displayed, Up 2, Down 0
```

FIGURE 4.7 – Activation des chemins LSP

4.4.3 Configuration du BGP

Afin de délimiter le périmètre des zones et créer les trois AS, nous procédons par l'affectation d'un même numéro d'AS pour chaque routeur appartenant à la même zone, en utilisant la commande (2). Vu que nos trois AS appartiennent au même fournisseur nous avons choisi des numéros d'AS privés : 64520, 64530 et 64540. Ensuite nous configurons le BGP interne (i-BGP) avec les commandes (3-11). Pour cela, nous définissons des groupes BGP nommés internal-peers de type interne sur tous les routeurs des trois AS. Nous spécifions par la suite les voisins directs et indirects de chaque routeur appartenant au même AS. Enfin avec la commande (12) nous spécifions la famille labeled-unicast afin que BGP soit utilisé pour publier des étiquettes à l'intérieur et l'extérieur du réseau avec l'extension resolve VPN pour stocker les routes étiquetées dans la table de routage inet.3.

```
[edit]
root@vMx1# set routing-options autonomous-system 64520
root@vMx1# edit protocols bgp group internal-peers
[edit protocols bgp group internal-peers]
root@vMx1# set type internal
root@vMx1# set local-address 1.1.1.1
root@vMx1# set local-as 64520
root@vMx1# set neighbor 2.2.2.2
root@vMx1# set neighbor 3.3.3.3
root@vMx1# set neighbor 4.4.4.4
```

```
root@vMx1# set neighbor 5.5.5.5
root@vMx1# set family inet labeled-unicast resolve-vpn
```

Afin de configurer la connexion entre les AS, nous avons crée des groupes BGP nommés ebgp-peers via les commandes (2-7) dans les routeurs d'extrémité des AS identifiés par VMx3, VMx5, VMx6 et VMx8. Au sein de ces groupes nous spécifions le type externe, l'adresse du voisin appartenant à l'AS distant, la famille labeled-unicast ainsi que le numéro de l'AS distant.

```
[edit]
root@vMx3# edit protocols bgp group ebgp-peers
[edit protocols bgp group ebgp-peers]
root@vMx3# set type external
root@vMx3# set neighbor 192.168.6.2 peer-as 64530
root@vMx3# set family inet labeled-unicast
root@vMx3# set peer-as 64530
```

Enfin, nous spécifions les routes à exporter vers l'AS distant en créant dans chaque routeur une policy nommée export via la commande (2) puis nous lui indiquons l'adresse à exporter à partir de la commande (5) et nous spécifions l'action (accept) pour accepter la route et la partager, puis nous appliquons cette policy créée au protocole BGP afin qu'il exporte la route spécifiée via la commande (9).

```
[edit]
root@vMx3# edit policy-options policy-statement export
[edit policy-options policy-statement export]
root@vMx3# set term 1 from protocols direct
root@vMx3# set term 1 from route-filter 3.3.3.3/32 exact
root@vMx3# set term 1 then accept
root@vMx3# exit
[edit]
root@vMx3# set protocols bgp export export
```

Grâce à la figure 4.8, nous confirmons la bonne connectivité entre les réseaux d'agrégation en effectuant le ping entre les routeurs vMx7 et vMx9.

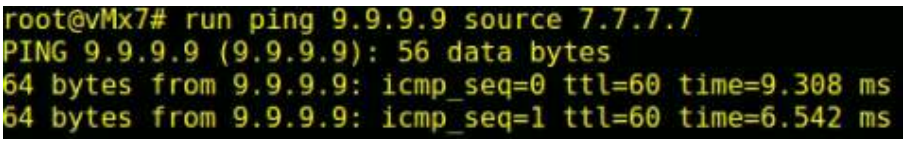


FIGURE 4.8 – Test ping entre VMx7 et VMx9

La visualisation de la table de routage inet.0 illustrée dans la figure 4.9 montre que les deux protocoles IGP et BGP coexistes dans le réseau et travaillent ensemble. le protocole préféré pour atteindre les destinations est précédé par une étoile *.

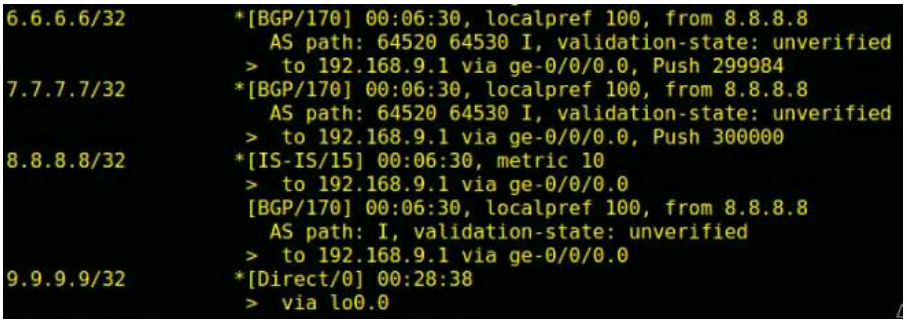


FIGURE 4.9 – Table de routage inet.0 du noeud Vmx9

4.4.4 Création des VPN

4.4.4.1 Établissement d'un Layer 2 VPN

Nous configurons un L2VPN entre les clients 1 et 2 pour permettre leur connexion, ce VPN correspond à un cable virtuel reliant les deux clients, ils doivent donc appartenir au même sous réseau. Nous procédons par la création d'un circuit de couche 2 avec la commande (2) entre les interfaces ge-0/0/0 et ge-0/0/1 de VMx7 et VMx9 respectivement, par la suite nous ajoutons à ces interfaces l'encapsulation ethernet-ccc afin qu'elles supportent ce type de VPN avec la commande (3).

```
1 [edit]
2 root@vMx7# set protocols l2circuit neighbor 9.9.9.9 interface ge-0/0/0
     encapsulation-type ethernet
3 root@vMx7# set interfaces ge-0/0/0 encapsulation ethernet-ccc
4 root@vMx7# run show l2circuit connections brief
```

La figure 4.10, obtenue grâce à la commande (4) nous confirme le bon établissement du tunnel. Nous testons le ping entre les PC des clients et le résultat est affiché dans la figure 4.11

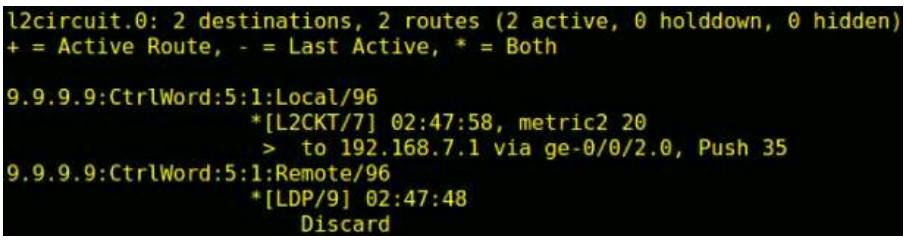


FIGURE 4.10 – Établissement du Layer 2 VPN

4.4.4.2 Établissement d'un Layer 3 VPN

Un L3VPN est crée entre les clients 3 et 4, et donc entre les interfaces ge-0/0/1 et ge-0/0/1 des routeurs VMx7 et VMx9 respectivement. Pour configurer ce type de service, nous procédons par les étapes suivantes :

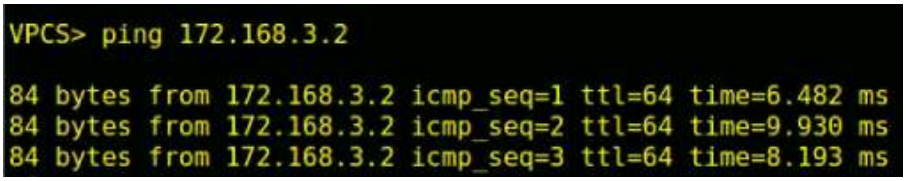


FIGURE 4.11 – Test ping entre client 1 et client 2

1. **Création des tables VRF :** Cette table est crée avec les commandes (2-6) pour chaque CE (Dans notre simulation les CE sont représenté par des terminaux) en indiquant l'interface reliant le routeur local au CE, nous prédisant ensuite un Route Distinguisher (RD) sous forme (adresses de loopback :id) puis nous activons la commande (7) qui permet d'allouer un seul label VPN pour l'ensemble de la VRF ce qui économise l'espace d'étiquette.
2. **Activation du MP-BGP :** Cette session est activée en ajoutant la famille ***inet-vpn*** aux groupes interne et externe du protocole BGP, via la commade (10)
3. **Configuration des Policy-options :** Cette étapes se traduit par la définition de deux politiques ***export*** et ***import*** via les commandes (11-16) et (19-24) respectivement, qui vont nous permettre de spécifier les routes à exporter et les routes à importer afin de les ajouter dans la table VRF avec les commandes (27) et (28).

```
1  [edit]
2  root@vMx7# edit routing-instance l3vpn
3  [edit routing-instance l3vpn]
4  root@vMx7# set instance-type vrf
5  root@vMx7# set interface ge-0/0/1.0
6  root@vMx7# set route-distinguisher 7.7.7.7:123
7  root@vMx7# set vrf-table-label
8  root@vMx7# eixit
9  [edit]
10 root@vMx7# set protocols bgp family inet-vpn unicast
11 root@vMx7# edit policy-options policy-statement l3vpn-export
12 [edit policy-options policy-statement l3vpn-export]
13 root@vMx7# set term 1 from protocol direct
14 root@vMx7# set term 1 then community l3vpn-rt memberstarget:64530:123
15 root@vMx7# set term 1 then accept
16 root@vMx7# set term deny then reject
17 root@vMx7# exit
18 [edit]
19 root@vMx7# edit policy-options policy-statement l3vpn-import
20 [edit policy-options policy-statement l3vpn-import]
21 root@vMx7# set term 1 from protocol bgp
22 root@vMx7# set term 1 then community l3vpn-rt memberstarget:64530:123
23 root@vMx7# set term 1 then accept
24 root@vMx7# set term deny then reject
```

```
root@vMx7# exit
[edit]
root@vMx7# set routing-instance l3vpn vrf-export l3vpn-export
root@vMx7# set routing-instance l3vpn vrf-import l3vpn-import
```

Les résultats de la figure 4.12 exécuté sur vMx7 nous montrent le succès de la configuration.

```
bgp.l3vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

9.9.9.9:123:172.168.1.0/24
                    >  to.70] 00:01:24, localpref 100, from 6.6.6.6
                       AS path: 64520 64540 I, validation-state: unverified
                    >  to 192.168.7.1 via ge-0/0/2.0, Push 300160
```

FIGURE 4.12 – Établissement du Layer 3 VPN

Nous testons le ping entre les PC des clients et le résultat est affiché dans la figure 4.13

```
VPCS> ping 172.168.1.2

84 bytes from 172.168.1.2 icmp_seq=1 ttl=58 time=37.454 ms
84 bytes from 172.168.1.2 icmp_seq=2 ttl=58 time=6.417 ms
84 bytes from 172.168.1.2 icmp_seq=3 ttl=58 time=8.132 ms
```

FIGURE 4.13 – Ping entre client 3 et client 4

4.5 Configuration du Segment Routing

4.5.1 Migration de l'OSPF vers ISIS

Une migration du protocole OSPF vers IS-IS dans le AS cœur s'impose car les routeurs Juniper supportent mieux le Segment Routing avec IS-IS. Nous configurons IS-IS avec les mêmes commandes utilisées dans la section 4.0.3.2 et nous choisissons le niveau 2 qui correspond au niveau 0 de OSPF et donc au réseau coeur.

Après avoir configuré IS-IS, nous vérifions via la table inet.0 illustrée dans la figure 4.14 qu'il dispose des mêmes entrées que le protocole OSPF et qu'il pointe vers la même interface de sortie.

Nous remarquons qu'OSPF est toujours le protocole préféré, c'est pourquoi nous le supprimons en utilisant la commande ***delete protocols ospf***. Cela nous permet d'obtenir la table de routage illustrée sur la figure 4.15.

4.5.2 Configuration des paramètres SR

La configuration du Segment Routing dans le réseau commence par la configuration du mode IP amélioré dans tous les routeurs du réseau afin qu'ils prennent en charge la fonctionnalité

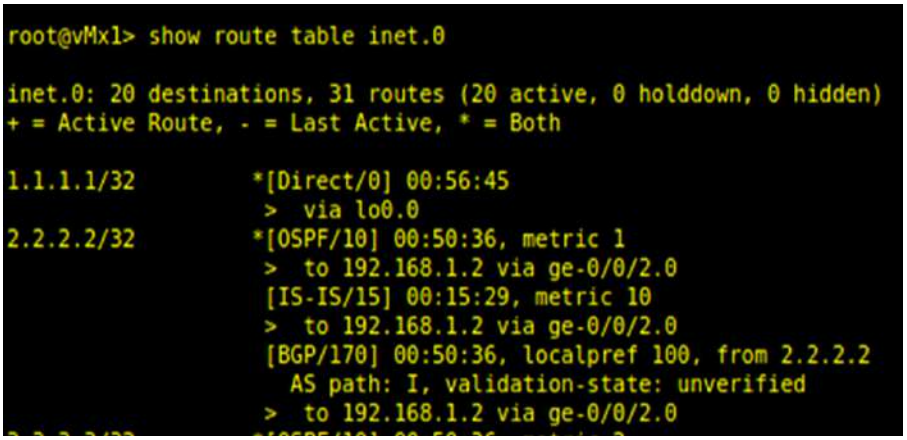


FIGURE 4.14 – Vérification des entrées et sorties de OSFP et IS-IS

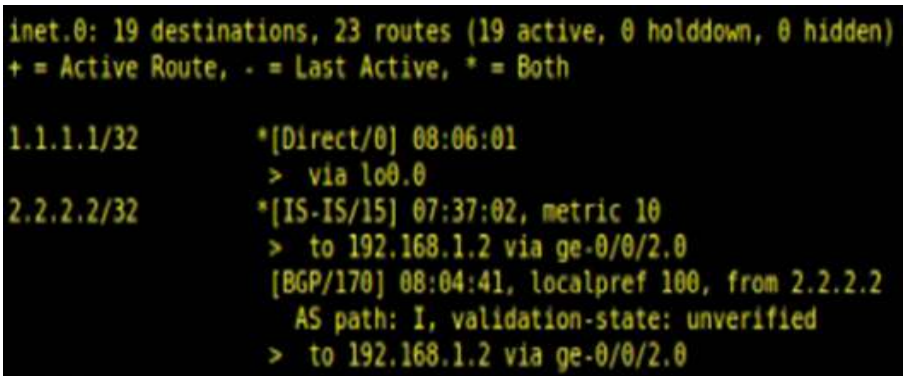


FIGURE 4.15 – table de routage après migration vers is-is

SRGB. Pour cela, on utilise la commande (2), ensuite nous passons à la configuration de la SRBG avec la plage d'adresses [16000-19999] pour tous les noeuds et en choisissant un index pour chaque noeud avec les commandes (3-6).

```
[edit]
root@vMx1# set chassis network-services enhaced-ip
root@vMx1# edit protocols isis source-packet-routing
[edit protocols isis source-packet-routing]
root@vMx1# set srgb start-label 16000 index-range 4000
root@vMx1# set node-segment ipv4-index 100
root@vMx1# exit
[edit]
root@vMx1# show isis adjacency detail
root@vMx1# deactivate protocol ldp
```

Sur la figure 4.16 nous pouvons observer les informations relatives à la bonne configuration du SR.

Les résultats de la commande (9) illustrés dans la figure 4.17 nous permettent de constater que les ADJ-SID ont été allouées dynamiquement pour chaque voisin IS-IS.

```
root@vMx1> show isis overview
Instance: master
  Router ID: 1.1.1.1
  Hostname: vMx1
  Sysid: 0004.1000.0001
  Areaid: 49
  Adjacency holddown: enabled
  Maximum Areas: 3
  LSP life time: 1200
  Attached bit evaluation: enabled
  SPF delay: 200 msec, SPF holddown: 5000 msec, SPF rapid runs: 3
  IPv4 is enabled, IPv6 is enabled, SPRING based MPLS is enabled
  Traffic engineering: enabled
  Restart: Disabled
    Helper mode: Enabled
  Layer2-map: Disabled
  Source Packet Routing (SPRING): Enabled
    SRGB Config Range :
      SRGB Start-Label : 16000, SRGB Index-Range : 4000
    SRGB Block Allocation: Success
      SRGB Start Index : 16000, SRGB Size : 4000, Label-Range: [ 16000, 19999 ]
    Node Segments: Enabled
      Ipv4 Index : 100
  Post Convergence Backup: Disabled
```

FIGURE 4.16 – Détails de la configuration du SR

```
[edit]
root@vMx1# run show isis adjacency detail
vMx4
  Interface: ge-0/0/0.0, Level: 2, State: Up, Expires in 20 secs
  Priority: 64, Up/Down transitions: 3, Last transition: 00:15:41 ago
  Circuit type: 2, Speaks: IP, IPv6, MAC address: 50:0:0:8:0:2
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  LAN id: vMx1.02, IP addresses: 192.168.3.2
  Level 2 IPv4 Adj-SID: 16

vMx2
  Interface: ge-0/0/2.0, Level: 2, State: Up, Expires in 21 secs
  Priority: 64, Up/Down transitions: 1, Last transition: 00:28:51 ago
  Circuit type: 2, Speaks: IP, IPv6, MAC address: 50:0:0:9:0:4
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  LAN id: vMx1.03, IP addresses: 192.168.1.2
  Level 2 IPv4 Adj-SID: 25
```

FIGURE 4.17 – Distribution dynamique des Adj-SID

D'après la table mpls.0 illustrée sur la figure 4.18 nous pouvons voir que les deux protocoles LDP et L-ISIS qui est une extension du protocole IS-IS pour supporter le SR, travaillent ensemble pour la distribution des labels. Pour forcer le trafic à passer par les routes SR et d'utiliser le

```
25                 *[L-ISIS/14] 00:17:03, metric 0
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
                       to 192.168.3.2 via ge-0/0/0.0, Swap 16200
25(S=0)            *[L-ISIS/14] 00:17:03, metric 0
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
                       to 192.168.3.2 via ge-0/0/0.0, Swap 16200
30                 *[LDP/9] 00:17:03, metric 1
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
30(S=0)            *[LDP/9] 00:17:03, metric 1
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
```

FIGURE 4.18 – Coexistence des protocoles IS-IS et LDP

protocole L-ISIS, nous désactivons LDP du réseau à l'aide de la commande (10).

Une nouvelle constatation de la table mpls.0 confirme les modifications apportées (figure 4.19).

```
25                 *[L-ISIS/14] 01:15:30, metric 0
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
                       to 192.168.3.2 via ge-0/0/0.0, Swap 16200
25(S=0)            *[L-ISIS/14] 01:15:30, metric 0
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
                       to 192.168.3.2 via ge-0/0/0.0, Swap 16200
16200              *[L-ISIS/14] 01:15:30, metric 20
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
                       to 192.168.3.2 via ge-0/0/0.0, Swap 16200
16200(S=0)         *[L-ISIS/14] 01:15:30, metric 20
                    >  to 192.168.1.2 via ge-0/0/2.0, Pop
                       to 192.168.3.2 via ge-0/0/0.0, Swap 16200
```

FIGURE 4.19 – Table mpls.0 après la migration

La migration d'un réseau MPLS vers SR-MPLS fut réalisée avec succès, nous la concrétisons avec un test de ping et de traceroute illustrés dans les figures 4.20 et 4.21 respectivement, où nous pouvons voir que le label utilisé est celui du SR.

```
[edit]
root@vMx1# run ping mpls segment-routing isis 5.5.5.5
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

FIGURE 4.20 – Test de connectivité

```
[edit]
root@vMx1# run traceroute mpls segment-routing isis 5.5.5.5
  Probe options: ttl 64, retries 3, wait 10, paths 16, exp 7, fanout 16

  ttl    Label  Protocol    Address          Previous Hop     Probe Status
    1    16500  ISIS        192.168.3.2      (null)           Success
  FEC-Stack-Sent: ISIS
  ttl    Label  Protocol    Address          Previous Hop     Probe Status
    2        3  ISIS        192.168.4.2      192.168.3.2      Egress
  FEC-Stack-Sent: ISIS

  Path 1 via ge-0/0/0.0 destination 127.0.0.64
```

FIGURE 4.21 – Tracé de route SR

Le Segment Routing est bien configuré, à présent, nous pouvons entamer la configuration des applications SR.

4.5.3 Configuration des applictions SR

4.5.3.1 Activation de TI-LFA

La protection du trafic contre les liens et les noeuds défaillants avec TI-LFA dans un environnement SR se fait dans chaque interface des routeurs à l'aide des commandes (2) et (3).

```
[edit]
root@vMx1# set protocols isis interface ge-0/0/0 level 2 post-convergence-
    lfa node-protection
root@vMx1# set protocols isis interface ge-0/0/2 level 2 post-convergence-
    lfa node-protection
root@vMx1# run show isis database vMX1 level 2 extensive
```

La confirmation de cette application se fait via la commande (4) et les résultats apparaissent sur la figure 4.22 où nous pouvons voir l'ajout d'un indicateur B dans le drapeau du sub-TLV qui se traduit par un drapeau de sauvegarde, c'est-à-dire qu'un ADJ-SID est utilisé pour protéger un autre nœud.

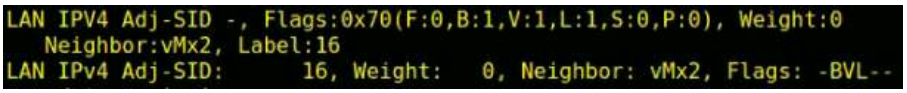


FIGURE 4.22 – Activation du TI-LFA

4.5.3.2 Activation du SBFD

Seamless Bidirectional Forwarding Detection (S-BFC) définit un mécanisme généralisé pour permettre aux nœuds du réseau d'effectuer de manière transparente des contrôles de continuité vers des entités distantes. Avec la commande (2) nous déterminons la valeur de discriminateur de chaque routeur et la durée de détection des messages S-BFD.

```
[edit]
root@vMx1# set protocols bfd sbfd local-discriminator 999  minimum-receive-
    interval 1000
root@vMx1# show bfd seamless session
```

La vérification de la bonne activation de ce mécanisme se fait via la commande (3) et est illustré sur la figure 4.23

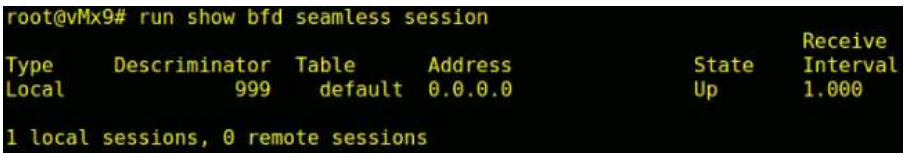


FIGURE 4.23 – Activation du BFD sur VMx9

4.5.3.3 Activation de ECMP

Le partage des charges est configuré au niveau de chaque routeur avec la commande (2). Les routeurs peuvent prendre en charge [N] chemin de sauvegarde ECMP, en cas de liaison

défectueuse. De ce fait lorsque le lien principale tombe en panne, le trafic sera équilibré sur les N autres nœuds.

```
[edit]
root@vMx1# set protocols  isis  backup-spf-options use-post-convergence-lfa
   maximum-backup-paths 2
root@vMx1# show isis overview | match backup
```

Sur la figure 4.24 nous pouvons voir les différents chemin de sauvegardes créés en utilisant la commande (3).

```
[edit]
root@vMx1# run show isis overview | match backup
  Post Convergence Backup: Enabled
    Max labels: 3, Max spf: 100, Max Ecmp Backup: 2
```

FIGURE 4.24 – Disponibilité du ECMP

4.5.3.4 Activation du VPN

La configuration du VPN dans un environnement SR est similaire à celle du MPLS, que ce soit pour le L3VPN ou le L2VPN. Toutefois, les L2VPN de Mobilis sont reliés avec d'autres clients et opérateurs qui n'implémentent pas le Segment Routing et donc nous avons besoin du LDP. Pour cela, nous activons le LDP uniquement sur les intefaces des routeurs qui utilisent le L2VPN. A noter que le SR reste le protocole préféré à coté du LDP pour les opérations de transfert d'étiquettes. La figure 4.25 démontre l'activation du L2VPN avec l'utilisation des labels SR.

```
l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

9.9.9.9:CtrlWord:5:1:Local/96
                   *[L2CKT/7] 02:47:58, metric2 20
                    >  to 192.168.7.1 via ge-0/0/2.0, Push 35
9.9.9.9:CtrlWord:5:1:Remote/96
                   *[LDP/9] 02:47:48
                       Discard
```

FIGURE 4.25 – Activation du SR-L2VPN

4.6 Configuration du contrôleur SDN

Dans cette section, nous abordons la configuration du contrôleur NorthStar dans le réseau pour permettre le Traffic Enginering d'une manière centralisée et avoir ainsi une meilleure visibilité et contrôle du réseau.

L'architecture du réseau après l'introduction du contrôleur NorthStar est illustrée sur la figure 4.26.

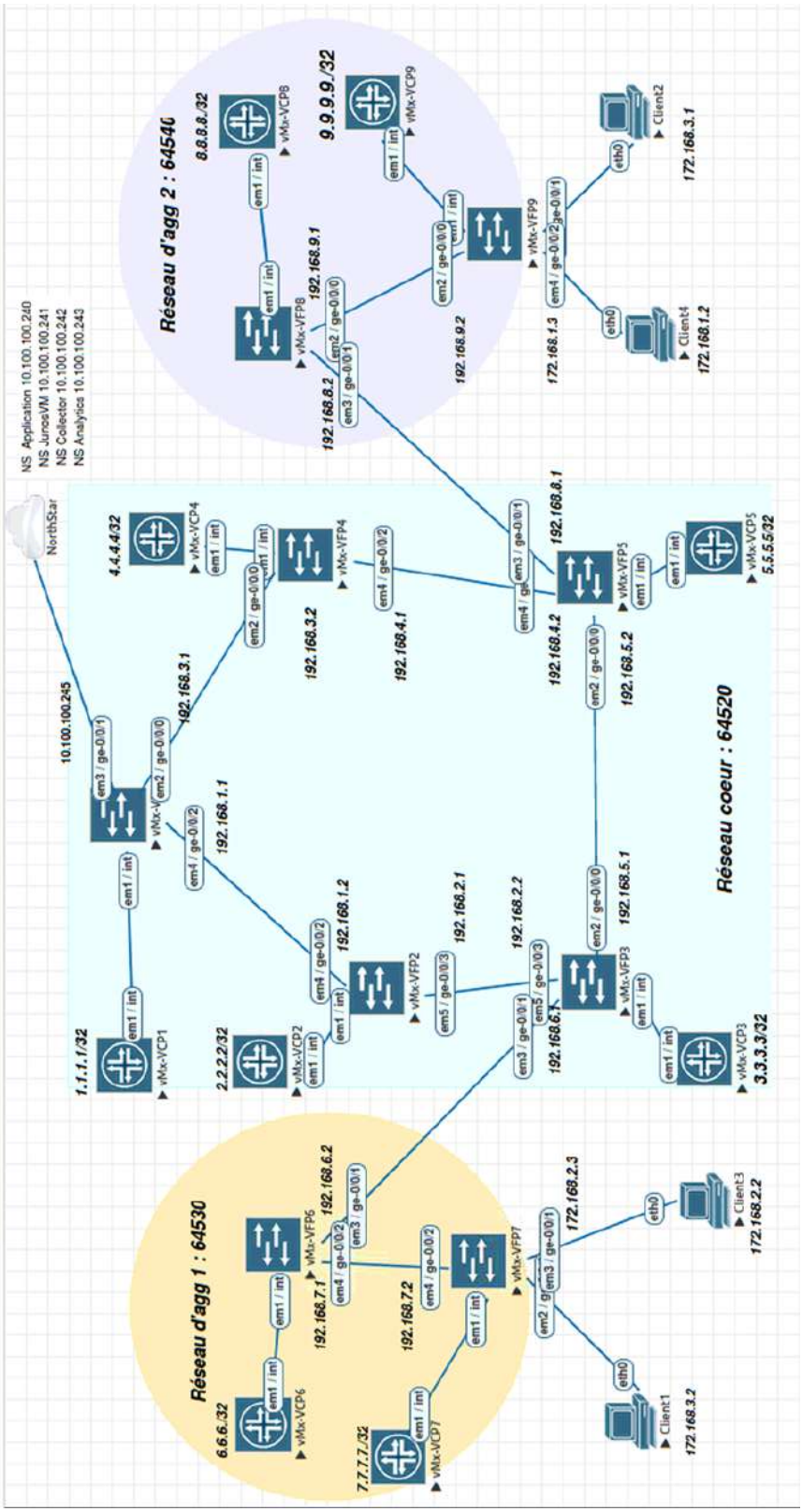


FIGURE 4.26 – Topologie du réseau après introduction du contrôleur

4.6.1 Controleur NorthStar

NorthStar est un contrôleur SDN de Juniper. Il permet d'avoir une visibilité du réseau en temps réel et une automatisation de contrôle sur les tunnels IP/MPLS des réseaux des fournisseurs de services et des larges réseaux d'entreprise.

Il fournit une puissante solution d'ingénierie de trafic avec plusieurs fonctionnalités intéressantes tel que le calcul complexe de chemins inter-domaines, la vue globale de l'état du réseau pour la surveillance, l'analyse, la gestion et la planification... [1]

Il utilise PCEP pour récupérer l'état actuel des tunnels existants puis il calcul les chemins optimaux et fournit les attributs que le PCC utilise pour signaler le chemin LSP.

Northstar est composé des éléments suivants :

— **JunosVM :** Il s'agit d'une virtualisation du système d'exploitation JunOS connecté au réseau via BGP-LS pour acquérir la topologie du réseau et ainsi faciliter les testes et la validation dans un environnement de teste.

— **Application :** Récupère la topologie acquise par JunosVM via le protocole Secure Shell (SSH), NETCONF ou bien SNMP.

— **Collector :** Collecte les informations relatives a la gestion du réseau via le protocole SNMP ou SSH.

— **Analytics :** Fourni les statistiques nécessaires pour la visibilité du réseau.

Parmi les protocoles qui permettent d'établir une communication entre le contrôleur et le réseau nous citons :

— **SNMP** : Pour permettre aux administrateurs de gérer les équipements du réseau et de diagnostiquer les problèmes à distance.

— **SSH** : Pour établir une connexion sécurisée et à distance entre le contrôleur et les routeurs du réseau.

— **NETCONF** : Pour fournir un moyen de gestion, de configuration et d'installation d'une nouvelle configuration des périphériques réseau.

4.6.2 Configuration du PCE

Pour activer la communication du PCE vers PCC, nous configurons le protocole PCEP sur le PCC identifié par vMx1 à l'aide des commandes (2-9). pour cela, on spécifie l'adresse loopback du routeur comme adresse local et l'adresse externe du contrôleur comme adresse de destination. Puis nous configurons le port de destination par lequel le routeur PCC se connecte au contrôleur PCE, ensuite nous maintenons la synchronisation de l'état des tunnels avec le type (active stateful) pour que le PCC délègue tous les LSP au PCE. Enfin nous activons le Segment Routing pour le PCE en incluant le Spring-capability. Nous passons ensuite à l'activation du

1. https ://www.juniper.net/documentation/en$_U S/northstar$4.1.0/$topics/concept/northstar-controller-overview.html$

calcul de chemin externe pour les LSP-TE d'un PCC avec la commande (12).

```
[edit]
root@vMx1# edit protocols pcep pce northstar
[edit protocols pcep pce northstar]
root@vMx1# set local-address 1.1.1.1
root@vMx1# set destination-ipv4-address 10.100.100.240
root@vMx1# set destination-port 4189
root@vMx1# set pce-type active stateful
root@vMx1# set lsp-provisioning
root@vMx1# set spring-capability
root@vMx1# exit
[edit]
root@vMx1# set protocols mpls lsp-external-controller pccd
```

4.6.3 Configuration du BGP-LS

Nous passons à la configuration du protocole BGP-LS qui va permettre au contrôleur d'acquérir la topologie du réseau. Nous procédons à cet égard par la configuration d'un groupe BGP nommée northstar via la commande (2). A l'intérieur de ce groupe nous définissons le type interne puis nous indiquons l'adresse loopback comme adresse locale pour établir des connexions avec le contrôleur, puis nous activons la fonction d'ingénierie de trafic et enfin nous spécifions l'adresse externe de JunosVm utiliser pour accepter et établir des connexions vers l'homologue distant.

Comme notre simulation de réseau se compose de trois AS, nous devons configurer les routeurs de bordure à savoir vMx3 et vMx5 afin que la liaison inter-as peut être signalée au contrôleur en luis attribuant un numéro de label indiquant l'adresse du routeur voisin. Nous procédons à cette configuration par les commandes (10-13). Nous ajoutons par la suite la configuration des commandes (15-18) afin d'importer le contenu de la TED dans la lsdist.0 qui est une table qui stocke les informations relatives à l'ingénierie du trafic et nous les insérons dans cette table via la commande (21). Enfin nous annonçons les routes au contrôleur via la commande (22).

```
[edit]
root@vMx1# edit protocols bgp group northstar
[edit protocols bgp group northstar]
root@vMx1# set type internal
root@vMx1# local-address 1.1.1.1
root@vMx1# set family traffic-engineering unicast
root@vMx1# set local-as 10000
root@vMx1# set neighbor 10.100.100.241
[edit]
root@vMx3# edit protocols bgp group epgp-peers
```

```
[edit protocols bgp group epgp-peers]
root@vMx3# set neighbor 192.168.8.2 egress-te-node-segment label 1046666
root@vMx3# set neighbor 192.168.8.2 egress-te
[edit]
root@vMx1# edit policy-options policty-statement export-bgp-ls
[edit policy-options policty-statement export-bgp-ls]
root@vMx1# set term 1 from family traffic-engineering
root@vMx1# set term 1 then accept
root@vMx1# exit
[edit]
root@vMx1# set protocols mpls traffic-engineering database import policy
    export-bgp-ls
root@vMx1# set protocols bgp group northstar export export-bgp-ls
```

Sur l'interface du contrôleur Northstar illustrée dans la figure 4.27 nous pouvons constater qu'il a acquit la topologie de notre réseau avec succès sur laquelle est affichée tous les numéros des Node-SID et Adj-SID. Toutes les informations des routeurs, des liens et des tunnels ont été importées et elles sont illustrées sur les figures 4.28, 4.29 et 4.30 respectivement où nous pouvons constater leurs activation.

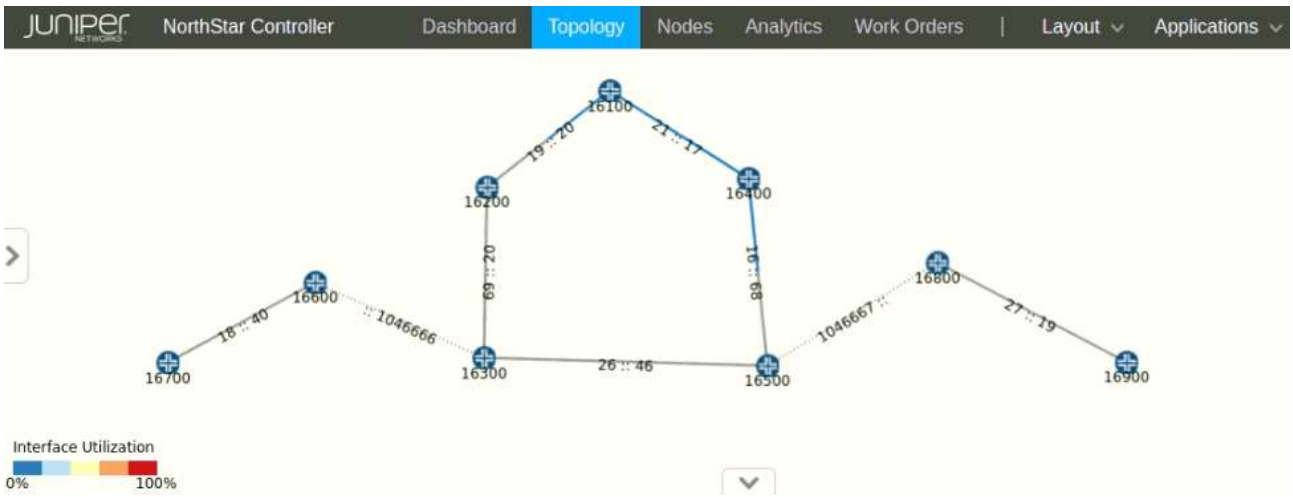


FIGURE 4.27 – Topologie importée par le contrôleur

FIGURE 4.28 – Activation des noeuds importés par le contrôleur

FIGURE 4.29 – Activation des liens importés par le contrôleur

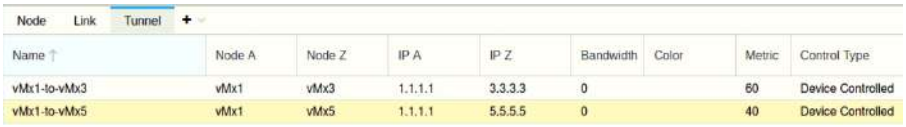


FIGURE 4.30 – Activation des tunnels TE importés par le contrôleur

4.6.4 Ingénierie du trafic avec Northstar

Nous finalisons la configuration du Segment Routing par la configuration du Traffic Engeneering avec SR uniquement et cela depuis le contrôleur. Pour cette étape nous créons deux LSP avec chacun une route primaire et une autre secondaire, similaires à ceux crées avec RSVP mais qui utilisent le SR et avec une contrainte de bande passante de 3G. Les LSP crés sont affichés sur la figure 4.31 identifiés par le type SR.

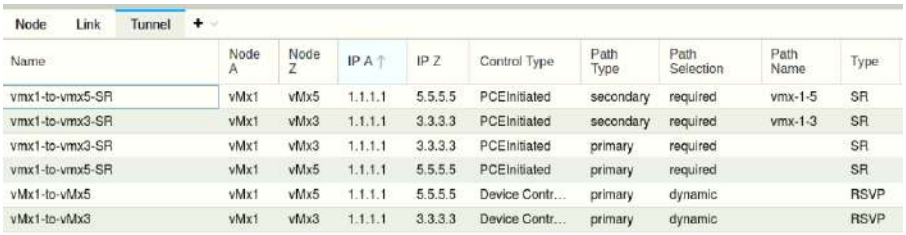


FIGURE 4.31 – Affichage des Tunnels SR

Avec la table de routage inet.3 qui stocke les routes IP de vMx1 illustrées sur la figure 4.32 nous pouvons visualiser que les LSP crées par le contrôleur figurent dans cette table seulement ils ne sont pas favorisés.

Pour les avantager nous devons supprimer les LSP-RSVP avec la commande (2) et laisser uniquement ceux crés avec le SR.

```
[edit]
root@vMx1# delete protocols mpls label-switched-path
```

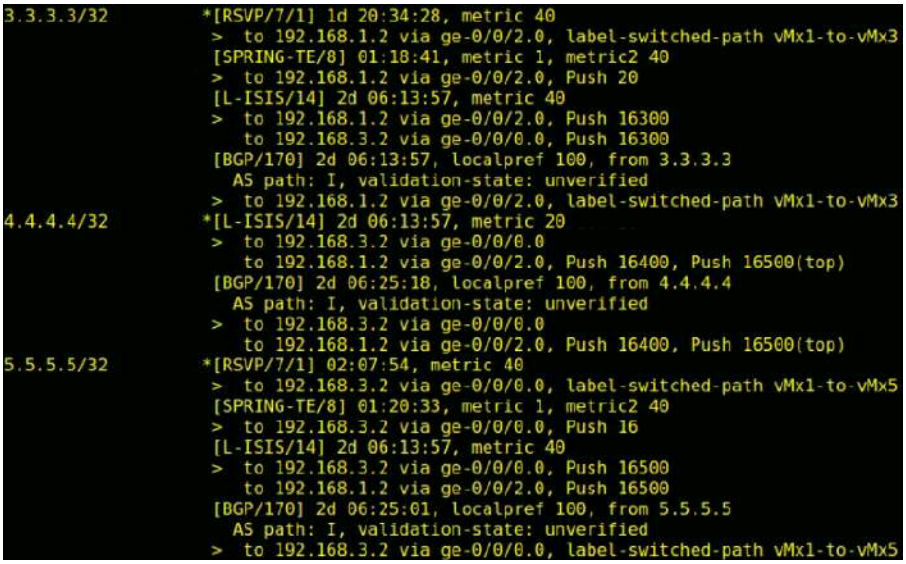


FIGURE 4.32 – Visualisation de la table inet.3 de vMx1

4.7 Comparaison des performances avant et après la migration

Afin de tester et comparer les performances entre MPLS et SR par rapport au délai de transmission, nous avons testé deux scénarios, le premier avec MPLS, le second après la combinaison du SR avec le controleur SDN. Nous avons utilisé l'outil RPM pour générer le traffic et collecter les informations et utilisé le logiciel Excel pour représenter les résultats graphiquement.

4.7.1 RPM

Junos RPM permet aux administrateurs réseau de mesurer les paramètres de performance entre deux points de terminaison du réseau. Pour collecter des statistiques réseau, RPM utilise des "probes". On configure un point de terminaison pour envoyer des probes ciblées à une adresse IP ou une URL de destination. Une fois qu'une réponse est reçue, des statistiques telles que le temps d'aller-retour (maximum, minimum et moyen), l'écart type, la gigue, le nombre de probes peuvent être vérifiées. Un autre avantage de Junos RPM est sa capacité à définir des marquages de qualité de service sur les probes de test. Junos RPM peut également être utilisé pour suivre si les voisins BGP sont actifs

4.7.2 Tests

Nous choisissons d'utiliser le Ping pour tester l'accessibilité du destinataire et pour avoir des rapports de diagnostic sur les erreurs, la perte de paquets et les temps d'aller-retour. Le Ping fonctionne sur la couche 3 et utilise un Internet Control Message Protocol (ICMP) d'interrogation et de réponse d'écho.

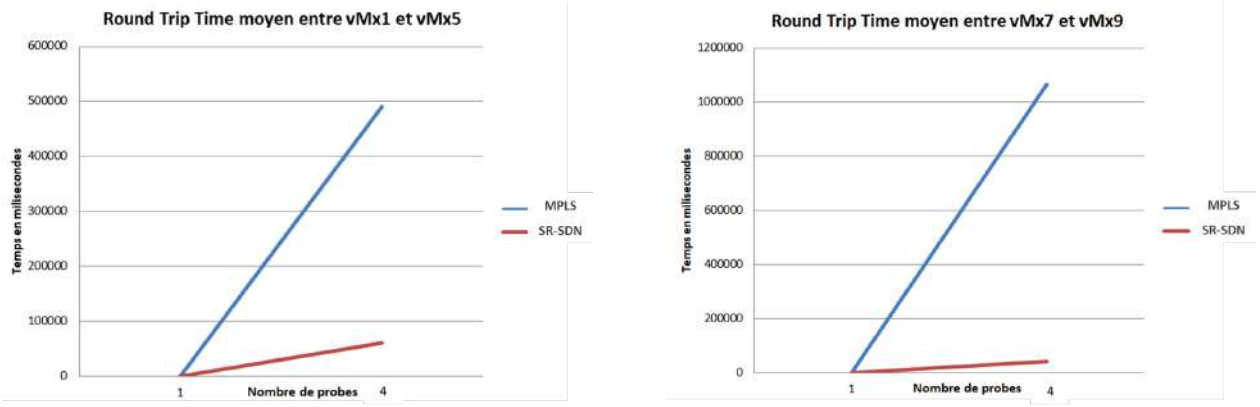
Le code du test RPM entre vMx1 et vMx5 est présenté ci-dessous.

```
root@vMx1# edit services rpm probe probe1 test t1
[edit services rpm probe probe1 test t1]
root@vMx1# set probe-type icmp-ping
root@vMx1# set target address 5.5.5.5
root@vMx1# set probe-count 4
root@vMx1# set probe-interval 5
root@vMx1# set test-interval 300
root@vMx1# set source-address 1.1.1.1
```

4.7.3 Résultats

4.7.3.1 Round Trip Time

Le Round Trip Time (RTT) est le temps du trajet aller-retour le plus court entre deux noeuds. Plus sa moyenne est petite et mieux c'est, car un temps d'aller-retour moyen élevé peut entraîner des valeurs de gigue élevées et cela peut signifier que des problèmes de performances existent au sein du réseau.



(a) RTT moyen entre vMx1 et vMx5 (b) RTT moyen entre vMx7 et vMx9

FIGURE 4.33 – Résultats du RTT moyen

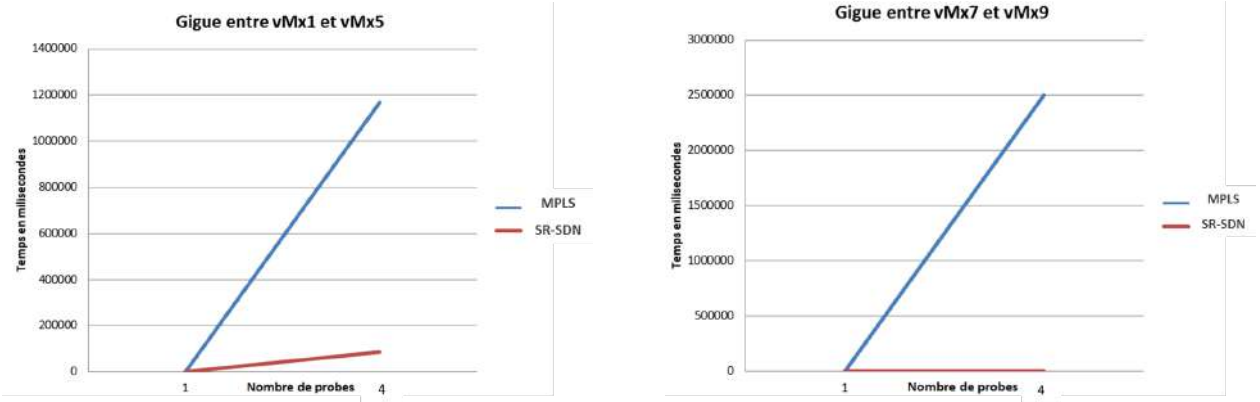
Les résultats du RTT moyen illustrés dans les graphes de la figure 4.33 affichent que entre les routeurs du réseau coeur vMx1 et vMx5 qu'en MPLS et avec le RSVP-TE le temps du RTT moyen était de 490535 usec puis après la migration vers le SR et en le combinant avec le contrôleur SDN on a obtenu 61334 usec.

Quant aux routeurs des deux réseaux d'agrégation, vMx7 et vMx9, le temps du RTT moyen était de 1066305 usec en MPLS puis après la migration vers le SR et en le combinant avec le contrôleur SDN on a obtenu 41715 usec.

A partir de ces résultats, nous déduisons que la combinaison du SR-SDN donne des résultats nettement plus intéressants en temps d'aller-retour que ceux du MPLS.

4.7.3.2 Gigue

La gigue est la différence de délai de transmission entre les paquets transmis entre les noeuds. La valeur de la gigue nous permet de connaître la cohérence des tests. Idéalement, nous cherchons à obtenir une petite valeur de gigue après l'implementation du SR, ce qui signifie que tout le trafic prend plus ou moins le même temps pour traverser le réseau et donc aucun problème n'affecte le réseau.



(a) Gigue entre vMx1 et vMx5 (b) Gigue entre vMx7 et vMx9

FIGURE 4.34 – Résultats de la gigue

Les résultats de la gigue obtenus à partir des tests sur les routeurs du réseau coeur et entre les réseaux d'agrégation illustrés sur les graphes de la figure 4.34 affichent que entre vMx1 et vMx5, en MPLS la gigue était de 1166948 usec puis après la migration vers le SR elle est passée à 86970 usec. Or, entre vMx7 et vMx9, en MPLS la gigue était de 2504194 usec, après la migration vers le SR elle a diminué jusqu'à 5204 usec.

Nous retenons que la combinaison SR-SDN offre des résultats avec une faible valeur de gigue par rapport à ceux du SR.

4.8 Conclusion

Au cours de ce chapitre nous avons vu la configuration du réseau IP-MPLS et les étapes de sa migration vers un réseau SR ou nous l'avons amélioré en lui introduisant de nouveaux mécanismes tel que TI-LFA, SBFD et ECMP. Nous avons également vu la mise en place du contrôleur qui nous a permit de mettre à exécution l'ingénierie du trafic afin d'assurer une meilleure gestion du réseau. En définitive nous avons pu constater l'amélioration des performances du réseau après l'implémentation du SR en comparant les résultats des paramètres de la gigue et le RTT moyen avant et après la migration obtenus grâce à Junos RPM.

Conclusion générale et perspectives

Selon la dernière étude du Visual Networking Index (VNI) de Cisco sur l'évolution du trafic IP, il y aura d'ici 2022 8.5 milliard d'objets connectés et la vidéo occupera 82% du trafic. Le trafic annuel mondial sera multiplié par 3 et atteindrait les 4,8 zettaoctets, c'est-à-dire 4,8 milliards de teraoctets et la région d'Afrique du Nord et le Moyen-Orient est estimé à avoir le plus grand pourcentage de croissance du trafic IP de 2017 à 2022, soit à 41%. [2]

Les évolutions technologiques et l'explosion du nombre d'applications en temps réel déployées dans les réseaux ont conduit à la recherche, l'étude et le développement de nouvelles technologies qui permettent aux réseaux d'opérateurs de relever les nouveaux défis liés à l'évolution des usages et services.

Le travail présenté dans ce mémoire porte sur l'étude et l'implémentation de la technologie du Segment Routing sur le réseau IP/MPLS de l'opérateur mobile Mobilis afin de surmonter les limites de son réseau actuel notamment, sa complexité et son manque d'évolutivité.

Nous avons vu dans un premier temps que le réseau IP basé sur le routage du plus court chemin est principalement dédié au transfert de données non gourmandes en bande passante. Cependant, les réseaux IP ont connu une diversité de trafics et d'applications ainsi que l'apparition de nouvelles exigences en matière de qualité de service. Ce qui a poussé les réseaux à évoluer vers plus d'agilité et de flexibilité d'où l'apparition de la technologie MPLS.

Nous avons dans un second temps fait le tour des concepts du MPLS où nous avons constaté que l'application des VPN que le MPLS a introduit en utilisant son mécanisme d'acheminement d'étiquettes a connu un grand succès. Néanmoins, l'ingénierie du trafic n'a pas eu le même essor, son application est complexe, pas très évolutive et ne prend pas en charge l'équilibrage de charge.

Dans un troisième temps, nous avons mené une étude théorique sur la technologie du Segment Routing, qui permet de répondre aux nouvelles contraintes et de remédier aux inconvénients de l'ingénierie de traffic en MPLS.

Le segment routing offre une nouvelle façon de router le trafic en permettant aux paquets d'utiliser l'IGP sans avoir besoin d'autres protocoles de signalisation tel que LDP et RSVP-TE.

2. https ://www.cisco.com/c/dam/m/en$_u$*s/network − intelligence/service − provider/digital − transformation/knowledge − network − webinars/pdfs/*1213 − *business − services − ckn.pdf*

Il permet au nœud d'entrée d'un réseau de spécifier le chemin que les paquets doivent suivre à l'intérieur du réseau. Ce chemin est spécifié comme une série d'étiquettes, appelées segments, ajoutées à chaque paquet.

Dans un quatrième temps, nous avons exploité le Segment Routing, en le combinant avec un contrôleur SDN, pour résoudre les problèmes d'ingénierie de trafic de Mobilis et permettre d'utiliser optimalement les ressources du réseau et améliorer ainsi les capacités du réseau pour écouler des volumes massifs de données en perpétuelle croissance et répondre aux exigences des utilisateurs, ce qui constitue donc un intérêt majeur pour l'opérateur d'une part et pour les utilisateurs finaux d'autre part.

Plus concrètement, nous avons effectué les configurations nécessaires à la migration du réseau MPLS vers le Segment Routing que nous avons enrichi avec les applications qui ont participé à son succès tel que le ECMP et le TI-LFA comme solution pour le FRR, puis nous avons configuré un contrôleur Northstar qui nous a permis d'effectuer l'ingénierie du trafic.

Dans un dernier temps, nous avons comparé les résultats des performances du réseau avant et après sa migration vers le SR. Les résultats des études comparatives ont démontré l'amélioration des performances en terme de délai de transmission et de gigue.

Ce projet a été une bonne occasion pour découvrir le monde des réseaux en profondeur et acquérir des connaissances en routage, MPLS, ingénierie de trafic, qualité de service et Segment Routing.

Perspectives

Le travail effectué dans ce projet ouvre la voie à plusieurs perspectives intéressantes. Premièrement, l'évolution des technologies nous amène à penser qu'il serait nécessaire de passer à l'IPv6. Nous envisageons d'implémenter le SR compte tenu de la possibilité de l'implémenter sur un plan de données IPv6. Mais surtout, il fournit un grand contrôle et une flexibilité qui permettront d'accélérer l'adoption et la migration d'IPv6.

Deuxièmement, les applications de Mobilis évoluent, certaines s'exécutent sur des machines virtuelles, d'autres dans des containers, certaines sont dans le cloud, d'autres dans des datacenters, et plein d'autres sont hébergées sur des serveurs physiques. La connectivité de L2 reste indispensable pour les applications d'ancienne génération mais les protocoles en couche L3 sont devenus plus populaires pour les nouvelles applications grâce à leur capacité de monter en charge simplement et efficacement.

Nous proposons de migrer vers le EVPN qui permet la virtualisation en couche L3 pour les nouvelles applications, tout en maintenant la connectivité L2 des anciennes applications.

Il fonctionne avec des protocoles L2 tels que VXLAN et il permet de créer des tunnels virtuels entre les différents réseaux. Ils établissent des ponts entre les clouds, datacenters, sites distants... et donnent l'impression que tout se passe au même endroit. La gestion des tunnels est simplifiée à l'aide d'un contrôleur SDN. Déployer le EVPN sur le Segment Routing est le plus convenable car le SR adopte déjà une architecture centralisée contrôlée par un contrôleur SDN et il offre les nombreux avantages qu'on a vu précédemment.

Troisièmement, Mobilis comme tout autre opérateur, déploie fréquemment des services dans son réseau tels que le filtrage de paquets, l'équilibrage de charge, les proxys ou d'autres services.

Le déploiement de ces services est de plus en plus réalisé via des applications virtualisées tel que le Network Function Virtualization (NFV) qui est une technique qui vise à remplacer les équipements matériels en virtualisant les fonctions réseau dans des logiciels hébergés.

Le SFC ou le chaînage des fonctions services est une technique qui dirige le trafics à travers une liste ordonnée de fonction de service réseau. Étant donné que le Segment Routing fournit déjà un cadre similaire, il est le plus approprié pour implémenter le SFC où chaque service est représenté par un segment. En se basant sur l'architecture du SDN, un contrôleur centralisé analyse les types de flux en s'appuyant sur une base de données pour connaître les services et les règles de politiques à appliquer puis le nœud d'entrée ajoute les segments appropriés.

Nous proposons d'appliquer la combinaison du SR, SFC, SDN et NFV pour permettre de mettre en œuvre, déployer et maintenir des services avec une grande flexibilité et donc de réduire les dépenses en capital et les dépenses opérationnelles.

Bibliographie

[1] Farrel A, Yasukawa S, and Komolafe O. An Analysis of Scaling Issues in MPLS-TE Core Networks. RFC 5439, Février 2009. Disponible en ligne `https://www.rfc-editor.org/rfc/pdfrfc/rfc5439.txt.pdf`.

[2] Philippe Atelin. *Réseaux informatiques, notions fondamentales*. ENI éditions, 3 edition, 2009.

[3] François Aubry. Models and algorithms for network optimization with segment routing. `https://segment-routing.org/upload/References/thesis-aubry.pdf`. [En ligne ; consulté en juin 2020].

[4] Joe Casad. *TCP/IP*. CampusPress, 2002.

[5] Bruce S Davie and Adrian Farrel. *MPLS : Next Steps*. Morgan kaufmann Publishers, 2008.

[6] Mike DiVincenzo. Segment routing : The future of mpls. `https://www.wwt.com/article/segment-routing-the-future-of-mpls`. [En ligne ; consulté en mai 2020].

[7] Jérôme Durand. Segment routing – l'art de faire plus avec moins. `https://gblogs.cisco.com/fr/reseaux/segment-routing-lart-de-faire-plus-avec-moins/`. [En ligne ; consulté en avril 2020].

[8] A. Bashandy et al. Segment Routing with the MPLS Data Plane. RFC 8660, Internet Engineering Task Force, Decembre 2019. Disponible en ligne `https://www.rfc-editor.org/rfc/rfc8660.pdf`.

[9] C. Filsfils et al. Segment Routing Architecture. RFC 8402, Internet Engineering Task Force, Juillet 2018. Disponible en ligne `https://www.rfc-editor.org/rfc/rfc8402`.

[10] C. Filsfils et al. *Segment Routing Policy Architecture*. Juillet 2020. Disponible en ligne `https://tools.ietf.org/pdf/draft-ietf-spring-segment-routing-policy-08.pdf`.

[11] E. Rosen et al. Multiprotocol Label Switching Architecture. RFC 3031, Internet Engineering Task Force, Janvier 2001. `https://tools.ietf.org/html/rfc3031`.

[12] P. Psenak et al. OSPF Extensions for Segment Routing. RFC 8665, Internet Engineering Task Force, Décembre 2019. Disponible en ligne `https://www.rfc-editor.org/rfc/rfc8665.pdf`.

[13] P. Sarkar et al. *Anycast Segments in MPLS based Segment Routing*. Internet Engineering Task Force, Avril 2020. Disponible en ligne https://www.ietf.org/archive/id/draft-ietf-spring-mpls-anycast-segments-03.pdf.

[14] P. Ventre et al. Segment routing : a comprehensive survey of research activities, standardization efforts and implementation results. .., Juin 2020. Disponible en ligne https://arxiv.org/pdf/1904.03471.pdf.

[15] S. Litkowski et al. *Topology Independent Fast Reroute using Segment Routing*. Août 2020. Disponible en ligne https://www.ietf.org/archive/id/draft-ietf-rtgwg-segment-routing-ti-lfa-04.txt.

[16] S. Previdi et al. *BGP Link-State extensions for Segment Routing*. Juin 2019. Disponible en ligne https://www.ietf.org/archive/id/draft-ietf-idr-bgp-ls-segment-routing-ext-16.txt.

[17] S. Previdi et al. IS-IS Extensions for Segment Routing. RFC 8667, Internet Engineering Task Force, Decembre 2019. Disponible en ligne https://www.rfc-editor.org/rfc/rfc8667.pdf.

[18] S. Previdi et al. Segment Routing Prefix Segment Identifier Extensions for BGP. RFC 8669, Internet Engineering Task Force, Decembre 2019. Disponible en ligne https://tools.ietf.org/pdf/rfc8669.pdf.

[19] Adrian Farrel. *The Internet and Its Protocols : A Comparative Approach*. Morgan kaufmann Publishers, 2004.

[20] Luc De Ghein. MPLS Fundamentals. Technical report, Cisco Press, 2007.

[21] W. G. Hannes Gredler. *Traffic Engineering and MPLS, the Complete IS-IS Routing Protocol*. 2005.

[22] Steve Greer, Peter Luff, and Sean Yarboroug. Frame relay testing and training. http://www.ittoday.info/AIMS/DCM/51-10-32.PDF. [En ligne ; consulté en avril 2020].

[23] Rabah Guedrez. Enabling traffic engineering over segment routing, 2018. https://tel.archives-ouvertes.fr/tel-02301017/document [En ligne ; consulté en mai 2020].

[24] Gredler Hannes and Goralski Walter. *The Complete IS-IS Routing Protocol*. Springer, 2005.

[25] Renaud Hartert. Fast and scalable optimization for segment routing, 2018. https://www.info.ucl.ac.be/~pschaus/assets/thesis/2018-hartert.pdf [En ligne ; consulté en mai 2020].

[26] Kurose James and Ross Keith. *Analyse structurée des réseaux*. Pearson Education, 2 edition, 2003.

[27] Lucek Julian and Szarkowic Krzysztof. Day one : Configuring segment routing with junos. https://www.juniper.net/documentation/en_US/day-one-books/DO_SegmentRouting.pdf. [En ligne ; consulté en juin 2020].

[28] Nupur Kanoi. Day one : Mpls up and running on junos. https://www.juniper.net/documentation/en_US/day-one-books/MPLS_UR.pdf. [En ligne ; consulté en mars 2020].

[29] Dave Kosiur. Understanding policy-based networking. https://books.google.dz/books?id=RdzNuYrHW-4C&printsec=frontcover&hl=fr#v=onepage&q&f=false. [En ligne ; consulté en mai 2020].

[30] J. Moy. OSPF Version 2. RFC 2328, Internet Engineering Task Force, Avril 1998. Disponible en ligne https://tools.ietf.org/pdf/rfc2328.pdf.

[31] John T. Moy. *OSPF Anatomy of an Internet Routing Protocol.* Addison-Wesley Professional, 1998.

[32] Jean-Louis Mélin. *Qualité de service sur IP.* Eyrolles, 2001.

[33] André Perez. *IP, Ethernet and MPLS Networks.* Wiley, 2011.

[34] Guy Pujolle. *Les réseaux.* Eyrolles, 9 edition, 2018.

[35] Clement SAAD. Instabilités du protocole bgp. http://www.lirmm.fr/acisr2i/archives/rapport_saad.pdf, 2005. [En ligne ; consulté en mars 2020].

[36] Claude Servin. *Réseaux et télécoms.* Dunod, 2 edition, 2006.

[37] Lohier Stéphane and Présent Dominique. *Réseaux et transmissions.* Dunod, 6 edition, 2006.

[38] Huawei Technologies. Segment routing technology white paper. https://e.huawei.com/mediafiles/MarketingMaterial_MCD/EBG/PUBLIC/en/2018/09/596d79d7-23d1-4364-a2ea-d96c20c19d36.pdf, 2018. [En ligne ; consulté en Mars 2020].

[39] Josselin Vallet. Optimisation dynamique de réseaux ip/mpls, 2015. https://tel.archives-ouvertes.fr/tel-01164635/document [En ligne ; consulté le 15 mars 2020].

Annexes

Annexe 1

1 Adressage

Nous présentons dans le tableau 4.1 l'adressage des différentes interfaces des routeurs de notre réseau.

Routeur	Interfaces	Addresse	Addresse Loopback
As 64520			
VMx1	ge-0/0/0	192.168.3.1/24	1.1.1.1/32
	ge-0/0/2	192.168.1.1/24	
	ge-0/0/1	10.100.100.245/25	
VMx2	ge-0/0/2	192.168.1.2/24	2.2.2.2/32
	ge-0/0/3	192.168.2.1/24	
VMx3	ge-0/0/0	192.168.5.1/24	3.3.3.3/32
	ge-0/0/1	192.168.6.1/24	
	ge-0/0/3	192.168.2.2/24	
VMx4	ge-0/0/0	192.168.3.2/24	4.4.4.4/32
	ge-0/0/2	192.168.4.1/24	
VMx5	ge-0/0/0	192.168.5.2/24	5.5.5.5/32
	ge-0/0/1	192.168.8.1/24	
	ge-0/0/2	192.168.4.2/24	
As 64530			
VMx6	ge-0/0/1	192.168.6.2/24	6.6.6.6/32
	ge-0/0/2	192.168.7.1/24	
VMx7	ge-0/0/0	/	7.7.7.7/32
	ge-0/0/1	172.168.2.3/24	
	ge-0/0/2	192.168.7.2/24	
As 64530			
VMx8	ge-0/0/0	192.168.9.1/24	8.8.8.8/32
	ge-0/0/1	192.168.8.2/24	
VMx9	ge-0/0/0	192.168.9.2/24	9.9.9.9/32
	ge-0/0/1	/	
	ge-0/0/2	172.168.1.3 /24	

TABLE 4.1 – Table d'adressage des interfaces des routeurs du réseau