الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي

Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة

Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا

Faculté de Technologie

قسم الإلكترونيك

Département d'Électronique

Mémoire de Master

Filière télécommunication

Spécialité système de télécommunication

Présenté par :

Houas Dihia

Bedja Yasmine

Thème

Etude, conception et implémentation du segment routing sur un réseau IP/MPLS

Encadreur : Abed lahcen

Poromoteur : Rochdi Benlaksira

Jury : Dahmani Samir et Bendoumia Rédha

Année Universitaire 2020-2021

Remercîment

Au premier lieu Nous tenons à remercier le bon dieu, qui nous a donné la force et le courage pour terminer ce modeste travail

Nous voulons exprimer notre plus profondre gratitude à tous ceux qui, de prés ou de loin on contribué a l'élaboration de ce travail

En achevant ce modeste travail , nous remercions infiniment le responsable de service IP de l'entreprise Mobilis HAMADI Rafik et notre promoteur Mr BENKASIRA.R et notre encadreur Mr ABED

Nous remercions ainsi tous les enseignants de département d'électronique spécialement la filiére télécommunication , qui ont contribué à notre formation durant notre cursus universitaire surtout :

Mr.Dahmani Samir Mr.AIT SAADI Hocine Mr.MAMOUNE Mountassar

Nous adressons notre vifs remerciements également à tous les ingénieur et le personnel de la direction pour tous l'attention et l'aide qu'ils nous ont accordées , que tous les intervenant qui ont contribué à notre stage pratique trouvent ici l'expression de notre profond respect

Un grand merci à nos famille respective et nos amis

En fin nos remerciment s'adressent aux membres de jury qui nous feront l'honneur de juger notre mémoire de master

Dédicace

Je dédie ce modeste travail à :

Ma vie, ma confidente amie, mon adorable maman Nadia qui a toujours été prés de moi dans les meilleur moment comme les pire , Je t'aime maman

A mon papa chéri qui m'a gâté m'a toujours fait confiance et ne cesse de ne pousser a avancé vers nouvels horizons je t'aime papou

A mes sœur Sarah tu es mon idole Asma ma douce tu m'aide m'aides à y voir plus clair je vous aime beaucoup

A mon très cher petit frére Mohamed Abderrahim

A mon petit neveu Adam Eliane qui est le plus beau cadeau q'une sœur puisse vous faire

Tu as apporté beaucoup de bonheur à notre famille je t'aiime

A mes très cher grand parent

A mes tante et oncle

A cousines plus particulièrement Meriem, Hend, Narimane, Maroua, Sonia, Hiba, Imen, Nesrine, Selma, Lydia et spécialement mon meilleur cousin Ramzi je les souhaite tous bonne continuation

A ma cher Binôme Houas Dihia qui m'as toujours motivé avec qui j'ai passé les meilleurs moment à faire des bêtise

Merci

Dédicace:

Tiens tout d'abord à remercier le bon dieu de m'avoir aidé à réaliser ce mémoire.

Que je dédie à :

A la prunelle de mes yeux, celle qui m'a soutenu surtout avec son douaa jour et nuit pour qu'elle me voie au sonnet et comme une étoile, à la source de la douceur.

A toi ma très chère mère.

A la personne qui a sacrifié sa vie pour moi, et qui a pris le défi pour mes études et ma éclairé le chemin de ma réussite.

A toi mon très cher père.

A toi ma très chère sœur, t'avoir dans ma vie est une chance inouïe, je t'aime d'un amour infini et merci de si bien accomplir ton rôle, et aussi son mari et leur enfants ishak et mohamed idris.

A la mémoire de ma grand-mère ayyi ellah yerhamha.

A Mes chers grands parents

A Mes chère oncles et tantes en particulier Sidali, Hamza et Zina pour leur soutien et toutes les valeurs qu'ils ont su m'inculquer. Que dieu leur apporte le bonheur, les aide à réaliser tous leurs vœux et leur offre un avenir plein de succès.

A toi ma meilleur amie et mon âme sœur Yasmine, tu es tout ce que j'ai de plus cher au monde tu représentes tellement pour moi que ces quelques mots ne suffiront pas à te dire à quel point tu comptes pour moi, je t'aime. Je t'aimerai toujours. Et aussi Ikram.

A mon très cher ami M.Abderrazak qui a toujours été présent à mes coté pour me soutenir et m'encourager à donner le meilleur pour moi et tu fais partie des personnes les plus importants de ma vie.

A tous mes cousines et mes cousins.

A tous mes ami(e).

HOUAS Dihia

Resumé :

Les évaluations technologiques ont entrainé une explosion de donnes et une grande variabilité des trafics. A cet égard, les opérateurs sont amenés 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 nœud, 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 appelés segments dans l'en-tête des paquets, éliminant ainsi le besoin de créer et maintenir des états sur les autres nœuds du réseau.

Dans le cadre de ce travail, il a été question d'étudier, réaliser et démonter 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 a l'ère du déluge de données.

Mots clés : Segment Routing, MPLS, Ingénierie de trafic, SDN, VPN, Fast ReRoute.

Tables des matières

Introduction général :

Chapitre I

1.1 introduction

1.2 Généralités sur les réseaux

1.2.1 Définition d’un réseau

1.2.2 Architecture du réseau

1.2.2.1 L’architecture OSI (Open System Interconnections) :

1.2.2.2 L’architecture TCP/IP :

1.2.2.3 Les différentes couches du modèle OSI et TCP/IP :

1.3 Protocole IP et routage

1.3.1 Protocole IP :

1.3.2 Routage :

1.3.3 Système Autonome

1.3.4 Type de routage :

1.3.5 Routage statique :

1.3.6 Routage dynamique :

1.3.7 Les protocoles de routage internes (IGP) :

1.3.7.1 Routing Information Protocol (RIP) :

1.3.7.2 Open Shortest Path First (OSPF) :

1.3.7.3 Protocole IS-IS :

1.3.8 Les protocoles de routage externes (EGP) :

1.3.8.1 Border Gateway Protocol (BGP) :

1.4 MPLS :

1.4.1Introduction :

1.4.2 Définition

1.4.3 Architecture :

1.4.3.1 Le plan de contrôle :

1.4.3.2 Le plan de données :

1.4.4 Fonctionnement de MPLS :

1.4.5 Opérations sur les labels

1.4.6 Distribution de Label :

1.4.6.1 LDP (Label Distribution Protocole) :

1.4.6.2 RSVP-TE

1.4.7 Application de MPLS

1.4.7.1 L'ingénierie du trafic(TE) :

1.4.7.2 Qualité de service (QOS) :

1.4.7.2.1 Modele IntServ :

1.4.7.2.2 Modele DiffServ :

1.4.7.3 Les réseaux privés virtuel (VPN) :

1.5 Conclusion :

Chapitre II

SEGMENT ROUTING

2.1 Introduction

2.2 Définition

2.3 Source Routing

2.3.1 Source Routing with IPV4

2.3.2 Source Routing with IPV6

2.3.3 Source Routing with MPLS

2.4 Principe du Segment Routing

2.5 SR-MPLS

2.6 Terminologie

2.6.1 Segment

2.6.2 Segment actif

2.6.3 Segment global

2.6.4 Segment local

2.6.5 SRGB

2.6.6 SRLB

2.6.7 PCE

2.7 Identificateurs de segment

2.7.1 Préfix SID

2.7.1.1 Node - SID

2.7.1.2 Anycast – SID

2.7.2 Adjacency SID

2.7.3 Binding SID

2.8 De l’MPLS vers le SR

2.9 Opération de SR

2.10 Acheminement des paquets en SR

2.11 Extensions des protocoles IGP

2.11.1 Extensions d’OSPF

2.11.2 Extensions d’ISIS

2.12 Extensions des protocoles BGP

2.12.1 BGP-préfix-SID

2.12.2 BGP-LS

2.13 Application du SR

2.13.1 Fast ReRoute avec SR

2.13.2 VPN avec SR

2.13.3 TE avec le SR

2.13.3.1 Fonctionnement

2.13.3.2 La gestion du trafic aves des contrôleurs de segment Routing

2.13.3.3 Stratégie SR

2.14 Segment Routing et SDN

2.14.1 SDN

2.14.1.1 Définition

2.14.1.2 Architecture de SDN

2.14.1.3 avantage du SDN

2.14.1.4 La comparaison entre réseau traditionnel et SDN

2.14.2 SR-SDN

2.15 SR vs MPLS

2.16 Bénéfices apportés par le SR

2.17 Conclusion

Chapitre III

Implémentation du segment Routing

3.1 EVE-NG

3.2 Architecture du réseau IP/MPLS

3.3 Pré-configuration

3.3.1 Configuration des interfaces réseau

3.3.2 Configuration de l'IGP

3.4 Configuration du MPLS

3.4.1 Configuration du LDP

3.4.2 Configuration du RSVP-TE

3.4.3 Configuration du BGP

3.4.4 Création des VPN

3.4.4.1 Établissement d'un Layer 2 VPN

3.4.4.2 Établissement d'un Layer 3 VPN

3.5 Configuration du Segment Routing

3.5.1 Migration de l'OSPF vers ISIS

3.5.2 Configuration des paramètres SR

3.5.3 Configuration des applications SR

3.5.3.1 Activation de TI-LFA

3.5.3.2 Activation du SBFD

3.5.3.3 Activation d'ECMP

3.5.3.4 Activation du VPN

3.6 Configuration du contrôleur SDN

3.6.1 Contrôleur NorthStar

3.6.2 Connexion du contrôleur au réseau

3.6.3 Configuration du PCE

3.6.4 Configuration du BGP-LS

3.6.5 Ingénierie du trafic avec NorthStar

3.7 Comparaison des performances avant et après la migration

3.7.1 RPM

3.7.2 Tests

3.7.3 Résultats

3.7.3.1 Round Trip Time

3.7.3.2 Gigue

3.8 Conclusion

Conclusion générale

Annexe

Référence bibliographique

Liste des figures

Figure	page
Figure 1.1 : modèle OSI et TCP/IP	
Figure 1.2 : topologie IS-IS	
Figure 1.3 : L'architecture de l'MPLS	
Figure 1.4 : Fonctionnement de l'MPLS	
Figure 1.5: Les messages entre PATH ET RESV dans RSVP-TE	
Figure 1.6 : les applications de l'PMLS	
Figure 1.7 : réseau privé virtuel	
Figure 2.1 : Chemin A est un chemin strict où tous les nœuds intermédiaires sont transportés Dans l'en-tête du paquet. Le chemin B est un chemin lâche car seul un sous-ensemble de L'intermédiaire de nodes est porté dans l'en-tête du paquet	
Figure 2.2 : Segments SR	
Figure 2.3 : segment mixe composé de prefix SID et d'adjacency SID	
Figure 2.4 : Adjacency Segment ID	
Figure 2.5 – Acheminement d'un paquet en SR	
Figure 2.6 : Protection locale de la liaison entre P2-P3 avec acheminement de segment	
Figure 2.7 : Segment Routing and MPLS VPN	
Figure 2.8 : Stratégie SR	
Figure 2.9 : fonctionnement d'une structure d'équipement réseau utilisant la technologie SDN	
Figure 3.1-topologie du réseau simulé	
Figure 3.2-configuration des interfaces	
Figure 3.3- configuation IGP au sein du coeur	
Figure 3.4 : Activation de OSPF sur le routeur vMx1	
Figure 3.5-configuration IGP au sein des AS d'agrégation	
Figure 3.6-activation d'IS-IS sur le routeur vMx6	

Figure 3.7 : test Ping entre vMx1 et vMx5	
Figure 3.8 : test Ping entre vMx6 et vMx7	
Figure 3.9- configuration de l'mpls	
Figure 3.10- configuration du LDP	
Figure 3.11- vérification de la distribution des labels	
Figure 3.12- configuration du RSVP-TE	
Figure 3.13-Activation des chemins LSP	
Figure 3.14- Configuration du BGP	
Figure 3.15-Configuration de la connexion entre Les AS	
Figure 3.16- Création des policy	
Figure 3.17-Test ping entre VMx7 et VMx9	
Figure 3.19-configuration du VPNL2	
Figure 3.20 Établissement de L2vpn	
Figure3.21-test ping entre client 1 et client 2	
Figure 3.21-Activation d'un L3vpn	
Figure 3.22-Activation d'un L3vpn	
Figure 3.23-Activation d'un L3vpn	
Figure 3.24-Etablisement de L3vpn	
Figure 3.25 ping entre client 3 et 4	
Figure 3.26- Vérification des entrées et sorties d'OSPF et IS-IS	
Figure 3.27-Table de routage après la migration vers IS-IS	
Figure 3.28-configuration des paramètre SR	
Figure 3.29-Detail de la configuration du SR	
Figure 3.30-Distribution dynamique Adj-SID	
Figure 3.31-Coexistance des protocoles IS-IS et LDP	
Figure 3.32-Table mpls.0 après la migration	
Figure 3.33-Test de connectivité	
Figure 3.34-Trace de route SR	
Figure 3.35- Configuration de TI-LFA	
Figure 3.36- Activation de TI-LFA	
Figure 3.37-configuration du SBFD	
Figure 3.38- Activation BFD sur VMx9	
Figure 3.39-configuration d'ECMP	

Figure 3.40-Disponibilité d'ECMP	
Figure 3.41-Activation de SR-L2VPN	
Figure 3.42-Topologie du réseau après introduction de contrôleur	
Figure 3.43- Configuration de la connexion du réseau au contrôleur	
Figure 3.44-Configuration du SNMP, SSH et NETCONF	
Figure 3.45-Activation des protocole sur le contrôleur	
Figure 3.46-Configuration du PCE	
Figure 3.47-Configuration du BGP-LS	
Figure 3.48- Suite de la configuration du BGP-LS	
Figure 3.49-Topologie importé par le contrôleur	
Figure 3.50-Activation des nœud importé par le contrôleur	
Figure 3.51-Activation des liens importé par le contrôleur	
Figure 3.52-Activation des tunnels TE importée par le contrôleur	
Figure 3.53-Affichage des tunnels SR	
Figure 3.54-Visualisation de la tabale inet.3 VMx1	
Figure 3.55- Le code du test RPM entre VMX1 et VMx 5	
Figure 03.56- Résultats de RTT moyen	
Figure 03.57-Résultats de la gigue	

Listes des tableaux

Tableau	page
Tableau 2.1 : Extension TLV OSPF pour SR	
Tableau 2.2 : Extension SUB TLV OSPF pour SR	
Tableau 2.3 : extensions IS-IS pour SR	
Tableau 2.5 : déférence entre segment Routing et MPLS	
Tableau 2.4 : tableau comparatif entre le SDN et les réseaux traditionnels	

.

Acronymes

ABR Area Border Router .

API Application Programming Interface .

ARPA Advanced Research Projects Agency .

AS Autonomous System .

ASBR Autonomous System Boundary Router .

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 général

Introduction général :

Les réseaux ne cessent d'évoluer, notamment dans cette dernière décennie, Avec la montée en puissance d'une génération férue de technologies tels que le Cloud, 5G , le streaming vidéo les opérateurs algériens devant de réelles difficultés .le nombre de consommateurs a connu une croissance remarquable, plus connecter que jamais . Cette hausse engendre une augmentation de la quantité de trafic transporter par le réseau ces dernier exigent un meilleur service incitant 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 IP/MPLS utilisée actuellement au niveau du réseau de MOBILS. Est devenue la technologie la plus répandue pour les réseaux WAN d'entreprise. Grâce à sa capacité à prendre en charge les exigences de qualité de service et à attribuer différentes classes de service selon les besoins des applications. 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 réalité, LDP empêche l'ingénierie de trafic, par conséquent lorsqu'un un lien est surchargé, il reste malgré tout choisi pour le transport des 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 nœuds après un redémarrage. Par conséquent le réseau ne peut être étendu étant donné que la capacité de mémoire d'un nœud est limitée. D'autant plus que ce protocole ne permet l'équilibrage de charge.

Dans le cadre d'optimiser les offres de l'opérateur Mobilis notamment par rapport à la problématique de l'ingénierie de trafic sur les réseaux IP/MPLS, nous avons effectué une étude approfondie dans laquelle nous avons constaté que la méthode utilisé actuellement est très limitant, cette dernière freine le développement des offres de l'opérateur pour ses clients. Suite à cela nous voudrions vous suggérer une solution qui repousse ces limites et répondre plus facilement à moindre coût à la demande, vous avez besoin d'une solution de transport de réseau qui vous permettra de mieux contrôler, d'être plus agile, de mieux connaître les

applications et de simplifier la gestion du trafic sur vos réseaux. Toutes ces caractéristiques sont disponibles dans la solution de routage de segments qui 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.

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.

Le document présent est le fruit de nos recherches, afin de vous donner davantage de détails nous l'avons reparti en quatre chapitres :

Chapitre 1 : Ce 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.

Chapitre 2 : Ce chapitre est dédié 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.

Chapitre 3 : Le dernier chapitre sera réservé à la partie pratique, ou 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.

Nous terminons ce mémoire par une conclusion générale, une bibliographie et des annexes.

Chapitre I

Etat de l’art

1.1 introduction

Au cours de ces dernières années, Internet a évolué et a inspiré le développement de nouvelles variétés d'applications . 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.

1.2 Généralités sur les réseaux

1.2.1 Définition d'un réseau

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo est généralisée dans les réseaux informatiques, même si cela ne va pas sans difficulté.

1.2.2 Architecture du réseau

Le transport des données d'une extrémité à une autre d'un réseau nécessite un support physique ou hertzien de communication. Pour que les données arrivent correctement au destinataire, avec la qualité de service exigé il faut en outre une architecture logicielle chargée du contrôle des paquets dans le réseau. Les deux grandes architecture suivantes se disputent actuellement le marché mondial des réseaux :

1.2.2.1 L'architecture OSI (Open System Interconnections) :

L'ISO (International Standardisation Organisation) a normalisé sa propre architecture sous le nom d'OSI. L'architecture ISO est la première à avoir été définie, et ce de façon relativement parallèle à celle d'Internet. La distinction entre les deux est que l'architecture ISO définit formellement les différentes couches, tandis que l'architecture Internet s'applique à réaliser un environnement pragmatique.

1.2.2.2 L'architecture TCP/IP :

Dans les années 1970, le département de la Défense américain, ou DOD (Département Of Défense), décide, devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture. Cette architecture, dite TCP/IP, est à la source du réseau Internet. Elle est aussi adoptée par de nombreux réseaux privés, appelés intranet. Les deux principaux protocoles définis dans cette architecture sont les suivants :

• IP (Internet Protocol), de niveau réseau, qui assure un service sans connexion.

• TCP (Transmission Control Protocol), de niveau transport, qui fournit un service fiable avec connexion. [1]

1.2.2.3 Les différentes couches du modèle OSI et TCP/IP :

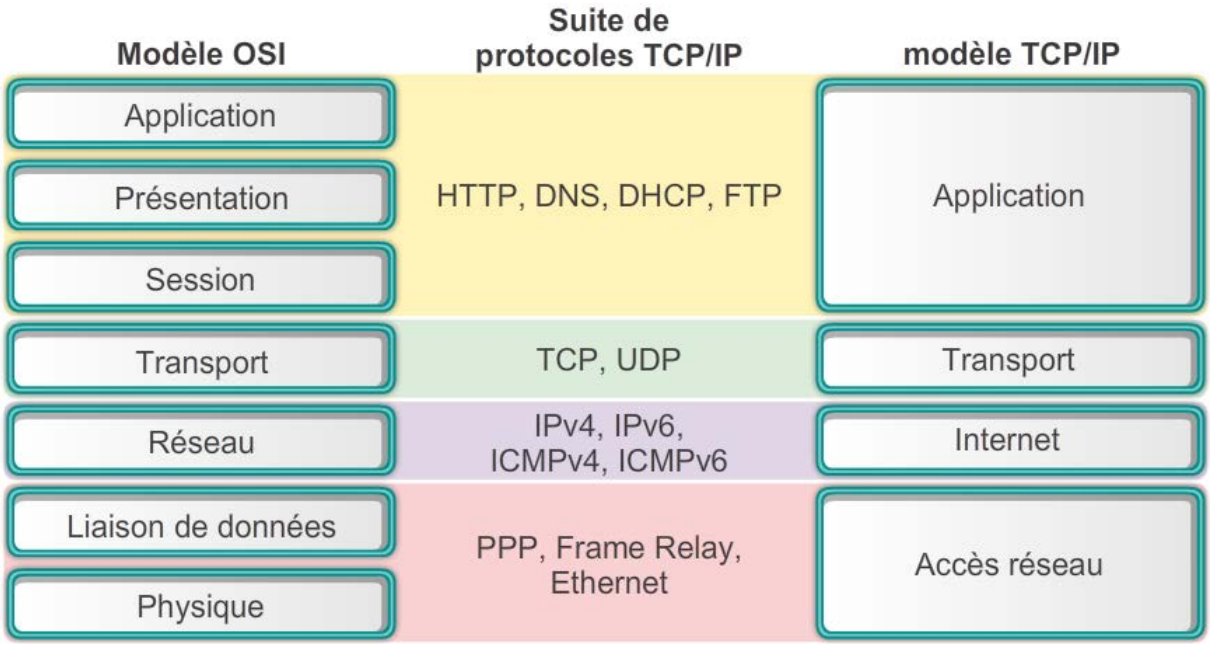


Figure 1.1 : modèle OSI et TCP/IP

1.3 Protocole IP et routage

1.3.1 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 la structure des informations qui concernent la source et la destination des données à envoyer. 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 puis le rassembler à son arrivée. Mais le flux de données ne suit pas forcément le même ordre que celui dans lequel il a été envoyé, c'est donc un protocole non orienté connexion [2]

1.3.2 Routage :

Le routage est le mécanisme permettant d'établir des chemins entre une ou des sources vers une ou plusieurs destination cette fonction est remplie par le routeur sur chaque interface du routeur un sous réseau y est connecté, cette interface représente aussi une passerelle pour les terminaux du même sous réseau, afin qu'ils puissent atteindre les destinations qui se trouvent sur d'autre sous réseaux [3]

1.3.3 Système Autonome

On appelle un système autonome ou AS (Autonomes System), un ensemble de réseaux interconnectés partageant la même stratégie de routage, tous les routeurs d'un AS respectant le même protocole de routage, et régissent par une autorisation administrative [4]

1.3.4 Type de routage :

Un routeur peut apprendre des réseaux distants de deux manières distinctes :

1.3.5 Routage statique :

Un administrateur réseau peut configurer manuellement une route statique pour accéder à un réseau spécifique pour ce faire, l'administrateur réseau doit avoir une parfaite connaissance de la topologie de son réseau.

1.3.6 Routage dynamique :

Dans ce type de routage, c'est au routeur que revient la décision de déterminer la route par laquelle le paquet va transiter, afin d'arriver à destination. Pour cela une communication entre les équipements de couche 3 s'impose, cette communication consiste à l'échange et la mise à jour des tables de routage entre les différents noeuds du réseau, pour déterminer le chemin le plus adéquat pour l'acheminement des données, ce qui exclut toute intervention d'opérateur humain.

1.3.7 Les protocoles de routage internes (IGP) :

Ce sont des protocoles de routage interne utilisés dans systèmes autonomes (AS) pour permettre aux routeurs de communiquer entre eux, on distingue :

1.3.7.1 Routing Information Protocol (RIP) :

De type vecteur distance, RIP est le premier protocole interne. Utilisé dans la communauté Internet, il est aujourd'hui remplacé par OSPF. Malgré une convergence lente et un trafic de gestion important, RIP reste le protocole de routage le plus employé. Il existe en

Deux version RIPv1 et RIPv2. Les messages RIP sont portés par des datagrammes UDP. [5]

1.3.7.2 Open Shortest Path First (OSPF) :

C'est un protocole à état de lien qui est exécuté en interne dans un système autonome, le OSPF maintient dans sa base de données une vue complète de la topologie du système. De cette base de données, une table de routage est construite en calculant l'arborescence des chemins du système. En outre, l'OSPF est sensible à la détection d'un quelconque changement topologique et cela en utilisant un minimum de trafic de protocole de routage, ce qui en fait un candidat idéal pour les réseaux évolutifs.

1.3.7.3 Protocole IS-IS :

IS-IS est un protocole de passerelle intérieure (IGP) qui utilise Des informations sur l'état des liaisons pour prendre des décisions de routage. Il utilise l'algorithme SPF (Short-Path-First) pour déterminer les routes.

IS-IS évalue les changements de topologie et détermine s'il est possible d'effectuer un calcul complet du SPF ou un calcul de route partiel (PRC). Ce protocole a initialement été développé pour le routage des paquets CLNP (protocole Connectionless Network Protocol) et ISO.

Tout comme le routage OSPF, dans IS-IS, les paquets Hello permettent la convergence rapide du réseau en cas de détection des modifications. À l'aide du OSPF, IS-IS évalue les modifications de topologie réseau et détermine si un calcul de route complet ou partiel est nécessaire [6]

La figure 1.2 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'intérieur 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 n'aura pas besoin de routeur L1-L2 .

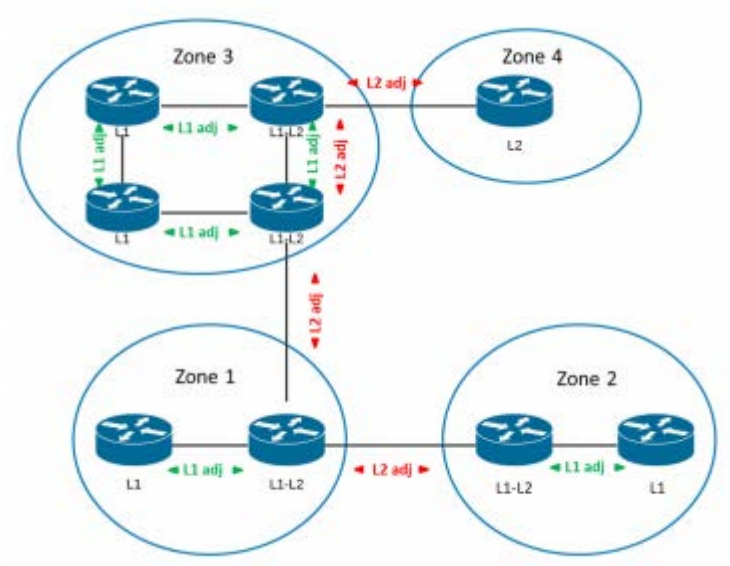


Figure 1.2 : topologie IS-IS

1.3.8 Les protocoles de routage externes (EGP) :

EGP est le premier algorithme de routage à avoir été mis au point, au début des années 1980, pour router un paquet d'un système autonome vers un autre. Ses faiblesses sont apparues avec le développement exponentiel d'Internet et le besoin d'éviter certaines zones politiquement sensibles. Il a été remplacé par le protocole BGP [5]

1.3.8.1 Border Gateway Protocol (BGP) :

Le BGP est un protocole inter-AS, il est construit sur l’expérience acquise des EGP voisins, son principale objectif est d’échanger des informations de routage et d’accessibilité du réseau entre AS. La version quatre du protocole (BGP-4) est très utilisée sur internet et permet l’agrégation des routes, afin de limiter les tables de routage pour un meilleur acheminement des données.

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, l’i-BGP est chargé des communications entre les routeurs internes, et entre les routeurs externes des différents AS l’e-BGP est chargé de gérer la communication entre eux.

1.4 MPLS :

1.4.1Introduction :

A la fin de l'année 2001, MPLS (Multi Protocol Label Switching) est le sujet d'un grand nombre d'articles et de conférences, mais il est aussi l'objet d'un nombre croissant d'annonces de la part des constructeurs de matériel réseau. À l'heure où les premiers services commerciaux s'appuyant sur un coeur de réseau MPLS/IP apparaissent, l'intérêt de la technologie semble démontré par leur bon fonctionnement. Il reste nécessaire de bien comprendre MPLS pour être capable de faire la part des choses. C'est pourquoi, au-delà des effets de mode, les motivations ayant présidé à la définition de MPLS et les réels apports de MPLS et des technologies associées dans les cœurs de réseaux modernes doivent être compris.

Le but de ce chapitre est de présenter les principaux éléments de l'architecture Multi Protocol Label Switching, (MPLS) et les mécanismes de fonctionnent que l'on peut traduire par « commutation d'étiquettes multi protocolaire ».

1.4.2 Définition

MPLS (Multi-Protocol Label Switching) est un technique réseau en cours de normalisation à l'IETF dont le rôle principal est de combiner les concepts du routage IP de niveau 3, et les mécanismes de la commutation de niveau 2 telles que implémentée dans ATM ou Frame Relay. Le protocole MPLS doit permettre d'améliorer le rapport performance/prix des équipements de routage, d'améliorer l'efficacité du routage (en particulier pour les grands réseaux) et d'enrichir les services de routage (les nouveaux services étant transparents pour les mécanismes de commutation de label, ils peuvent être déployés sans modification sur le coeur du réseau). [7]

1.4.3 Architecture :

On distingue deux parties logiques bien distinctes.

1.4.3.1 Le plan de contrôle :

Qui va être chargé de gérer et maintenir les labels contenus dans chaque routeur du réseau MPLS. Ce plan de contrôle utilise des protocoles de routages classiques, tels qu'OSPF ou RIP afin de créer la topologie des noeuds du réseau MPLS, ainsi que des protocoles spécialement développés pour le MPLS comme Label Distribution Protocol que nous étudierons par la suite.

1.4.3.2 Le plan de données :

Celui-ci contient le mécanisme de transmission des données et est complètement indépendant de la partie signalisation. Ce découpage est par exemple à la base des migrations ATM vers MPLS, car elle permet de conserver le matériel ATM utilisé en coeur de réseau. Grâce au simple changement logiciel du plan de contrôle, le commutateur ATM pourra être transformé en routeur MPLS. [8]

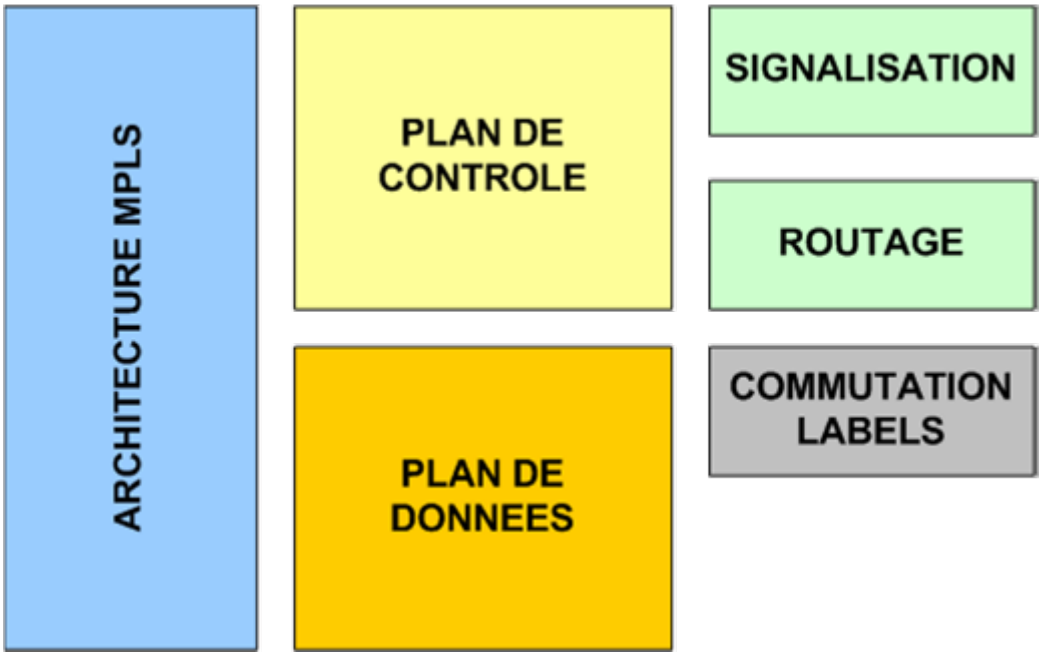


Figure 1.3 : L'architecture de l'MPLS

1.4.4 Fonctionnement de MPLS :

Le principe de fonctionnement du MPLS est basé sur la permutation d'étiquettes, un mécanisme de transfert simple qui offre des possibilités de nouveaux paradigmes de contrôle et de nouvelles applications. Lorsqu'un paquet arrive à un LER d'entrée (Ingress LER), ce dernier lui affecte un label en fonction de son FEC auquel il appartient, Puis ce paquet est commuté par les LSR ou chaque LSR change le label d'entrée par un autre de sortie, jusqu'au LER de sortie (Egress LER) qui supprime le label, le routage IP prend alors le relais, et remet les paquets à leurs destination finale.

Le chemin emprunté par le paquet dans le réseau MPLS est appelé un LSP, il est déterminé par des protocoles de routage tels que l'OSPF, qui permettent de créer des tables de routage dans chaque routeur.

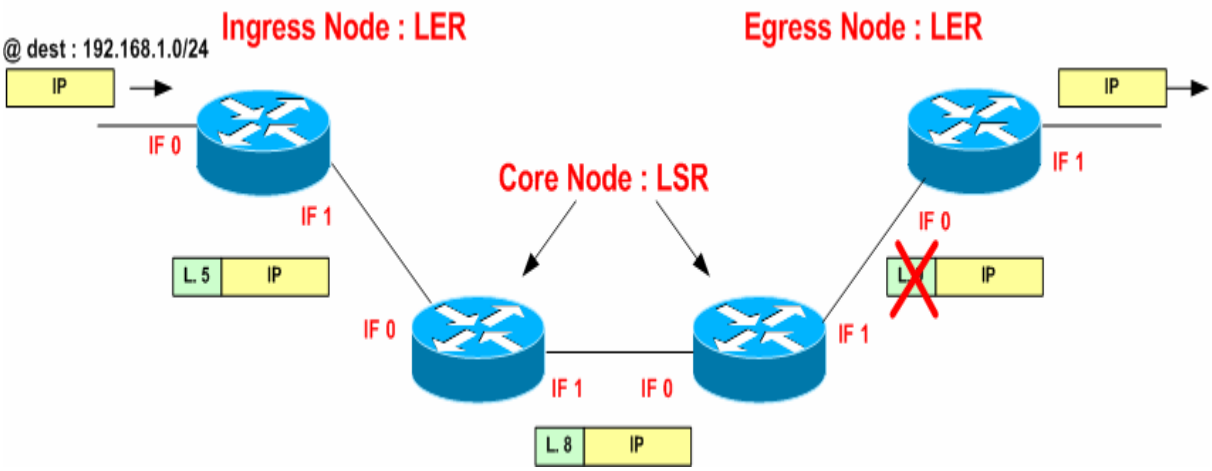


Figure 1.4 : Fonctionnement de l'MPLS

1.4.5 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 pur 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.[6]

1.4.6 Distribution de Label :

La distribution de labels fait partie du plan de contrôle et plus particulièrement de la signalisation, deux protocoles ont étés spécialement développés pour MPLS, il s'agit de Label Distribution Protocol et Contraint Routing

1.4.6.1 LDP (Label Distribution Protocole) :

Un label est attribué à chaque FEC, cette distribution peut être manuelle ce qui n'est réaliste que pour un nombre très limité de classes d'équivalence FEC, ou bien automatique en Utilisant le nouveau protocole de distribution des labels LDP (Label Distribution Protocol) qui est l'exemple de cette approche.

LDP définit une suite de procédures et de messages utilisés par les LSR pour s'informer mutuellement du map ping entre les labels et le flux. Une connexion LDP peut être établie entre deux LSR directement ou indirectement connectés. [9]

1.4.6.2 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. LeRSVP-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 nœud, ce qui permet d'introduire la technologie FRR qui permet de re-router très rapidement un LSP lorsqu'un nœud ou un lien tombe en panne. Tous les nœud 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 Ingres 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 de l'Egress LER à l'Ingres LER qui est une réponse au message PATH. RESV se propage de nœud en nœud jusqu'au Ingres 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 1.5 [10]

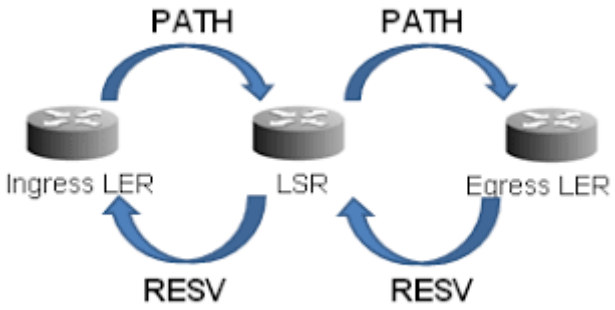


Figure 1.5: Les messages entre PATH ET RESV dans RSVP-TE

1.4.7 Application de MPLS

En plus de la rapidité, MPLS apporte plusieurs services, Nous avons proposé une taxonomie des applications MPLS illustrée dans la figure1.6.

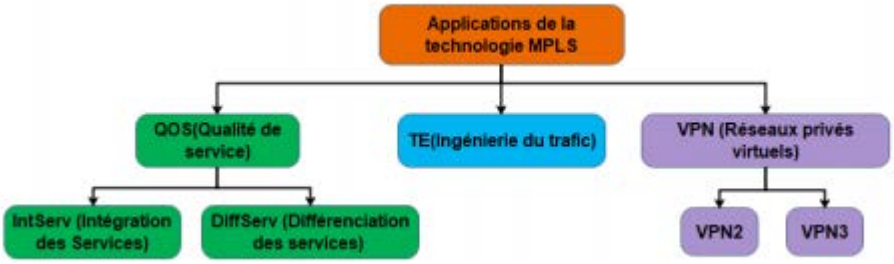


Figure 1.6 : les applications de l'PMLS

1.4.7.1 L'ingénierie du trafic(TE) :

Les application de La convergence des réseaux multiservices, qui transportent le trafic Internet, VoIP (Voice/Video over IP), IP TV, vidéo à la demande et le trafic VPN, nécessite une optimisation de l'utilisation des ressources pour limiter les coûts d'investissement, une garantie stricte de la qualité de service (QoS) et une disponibilité élevée. A tous ces besoins s'ajoute le besoin de limiter les coûts d'exploitation. Par conséquent, des mécanismes de trafic s'avèrent nécessaires pour répondre à tous ces besoins. On appelle ingénierie de trafic l'ensemble des fonctions permettant de contrôler l'acheminement du trafic dans le réseau afin d'optimiser l'utilisation des ressources et de réduire les risques de congestion tout en garantissant la QoS. [9]

1.4.7.2 Qualité de service (QOS) :

QoS (Quality of Service) est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau et de garantir de bonnes performances aux applications critiques pour l'organisation.

C'est la capacité de véhiculer dans de bonnes conditions un type de trafic donné, Il permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par application (ou activité) suivant les protocoles mis en œuvre au niveau de la structure. La qualité de service peut être fournie par deux approches relativement différentes :[9]

1.4.7.2.1 Modele IntServ :

Utilise la réservation de ressources mise en place par RSVP. IntServ classifie les données par flux. En effet, chaque flux va être placé dans une file d'attente séparée. La granularité est forte, car la classification se fait flux par flux selon le protocole de réservation. En revanche, c'est un processus coûteux en ressources machine, et qui supporte difficilement la montée en charge car les routeurs de coeur doivent maintenir une liste des flux en cours afin de rechercher à chaque fois la qualité de service à appliquer. En effet, plus les flux seront nombreux, plus les traitements à effectuer au niveau des routeurs seront importants notamment au niveau de l'ordonnancement.[7]

1.4.7.2.2 Modele DiffServ :

L'autre approche servant de support à la qualité de service est DiffServ. Dans cette configuration, les flux sont agrégés pour former des classes de services. De cette manière les flux d'une même classe ont les mêmes garanties de service. Par rapport à IntServ, la granularité est donc beaucoup plus faible. Cependant, DiffServ repose sur l'utilisation d'un système de marquage des paquets pour définir le comportement à adopter par le nœud recevant le paquet. C'est ce que l'on nomme le **Per-Hop Behavior**. Le but ici n'étant pas de détailler l'ensemble des mécanismes mis en œuvre dans DiffServ, nous allons donc voir l'utilisation de ces approches dans MPLS.[7]

1.4.7.3 Les réseaux privés virtuel (VPN) :

Il est courant qu'une entreprise constituée de plusieurs sites géographiquement éloignés et dont elle souhaite les interconnecter à travers un réseau étendu. La solution la plus connue et la plus utilisée consiste à relier les sites au moyen des liaisons spécialisées dédiées à

l'entreprise. Toutefois, le coût prohibitif et la difficulté technique, amènent à rechercher des solutions plus abordables.

Les fournisseurs d'accès internet disposent des réseaux MPLS étendus, couvrant la plupart du temps une large portion de territoire. Il est donc plus simple pour une entreprise de relier ses sites à travers le réseau de l'opérateur et mettre en place une solution MPLS-VPN (Virtual Private Network).

Un réseau privé virtuel fournit une méthode de raccordement de sites distants appartenant à un ou plusieurs VPN. [9]

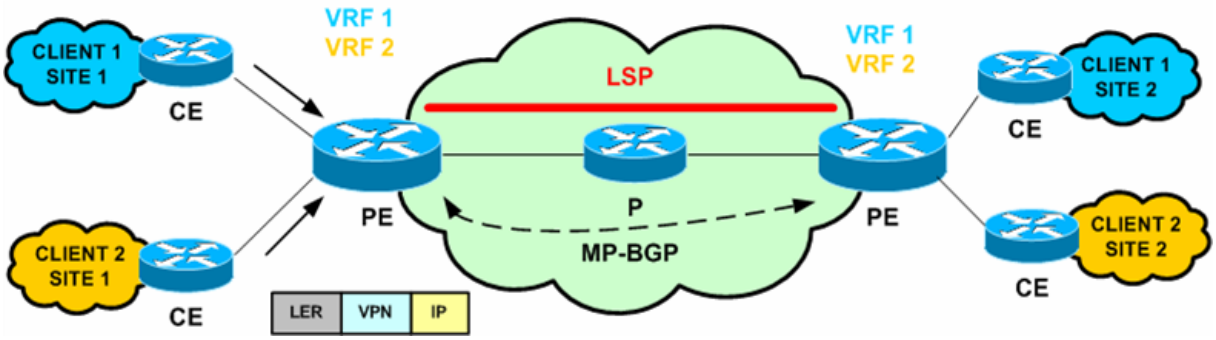


Figure 1.7 : réseau privé virtuel

1.5 Conclusion :

A travers ce chapitre nous avons défini 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 ensuit 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 II

SEGMENT ROUTING

2.1 Introduction

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

2.2 Définition

Le routage de segments (SR) est une technique de routage basée sur la source qui simplifie l'ingénierie et la gestion du trafic sur tous les domaines du réseau. Il élimine les informations sur l'état du réseau des routeurs et des nœuds de transit et place les informations sur l'état du chemin dans les en-têtes des paquets reçus à un nœud d'entrée. Le routage de segments est hautement réactif aux modifications de réseau, car l'information est déplacée des nœuds de transit au paquet. De ce fait, il est plus agile et flexible que les autres solutions gérant les aspects techniques du trafic. La gestion des aspects techniques du trafic du SR lui permet de fournir une qualité de service (QoS) pour les applications, et de mapper des services réseau au trafic des utilisateurs finaux et des applications qui traverse le réseau.

2.3 Source Routing

Le paradigme de routage source a d'abord été introduit dans les premières versions du protocole Internet IPv4. Depuis lors, diverses architectures et protocoles réseau ont adopté, tels que MPLS, IPv6 et les protocoles de Réseaux sans fil : dynamique DSR Source Routing et Source Demand Routing Protocol (SDRP). En outre, le routage des sources est une composante principale de l'architecture SR. Comprendre le routage des sources est essentiel pour une meilleure compréhension de la RS.

À cette fin, nous détaillons dans ce le fonctionnement du routage des sources et sa mise en œuvre dans différents protocoles. Le routage source permet au nœud source (entrée) de spécifier explicitement le chemin que les paquets doivent suivre pour atteindre leur destination. Le Source-Routed Path (SRP) se compose d'une séquence de nœuds et relie les paquets. Les composants du SRP (nœuds, liens) sont portés dans chaque en-tête de paquet. Le SRP peut exprimer tous les chemins topologiques. Par conséquent, il permet l'acheminement

du trafic sur chemins qui ne sont pas les chemins IGP les plus courts. Une telle caractéristique est intéressante pour cas d'utilisation multiple tels que l'ingénierie de la circulation, la surveillance des chemins et le dépannage. Nous distinguons deux types d'acheminement des sources :

- Strict Source Routing : Dans le routage source strict, tous les sauts intermédiaires (nœuds, liens, etc.) entre la source et la destination sont listés dans le paquet header. Dans ce cas, le paquet doit passer exclusivement par les sauts listés. Deux sauts successifs dans l'en-tête du paquet sont adjacents. Les nœuds intermédiaires font ne pas avoir à déterminer le prochain saut parce que la décision de transfert est uniquement basée sur les informations contenues dans l'en-tête du paquet. Fig. 2.1, fournisseur de services connecte deux routeurs Customer Edge (CE) CE1 et CE2, et décide que le trafic envoyé de CE1 à CE2 suit le chemin A : P E1 P2 P3 P E4.

Par conséquent, P E1 reçoit les paquets de CE1 puis les encode dans chaque en-tête de paquet la liste de tous les identifiants de sauts intermédiaires. Lorsque le paquet atteint un nœud, ce nœud recherche la référence du saut suivant dans la liste afin de déterminer à quel saut il doit acheminer le paquet. Enfin, P E4 supprime le hop list avant de transférer le paquet vers CE2.

-Loose Source Routing : Dans le Routing source non défini, le paquet ne porte qu'un sous-ensemble des identificateurs hop qui constituent le chemin complet. Le paquet passe par tous les sauts indiqués dans l'en-tête, mais pas seulement, c'est-à-dire que les paquets peuvent passer par les sauts qui ne sont pas présents dans leur tête. Cela se produit lorsque deux sauts successifs dans l'en-tête du paquet est physiquement séparés par un ou plusieurs nœuds intermédiaires.

Pour revenir à l'exemple de la fig. 2.1, CE1 envoie son trafic à CE2 chemin suivant B : P E1 P3 P E4, seul P3 est spécifié comme intermédiaire nœud. Dans ce cas, P E1 détermine que P6 est le saut suivant pour atteindre P3 par vers le haut de sa table de renvoi. Ceci est considéré comme un chemin lâche parce que P E1 et P3 ne sont pas des voisins directs, par conséquent les paquets doivent passer par P6, qui n'est pas présent dans la liste hop du chemin source.[11]

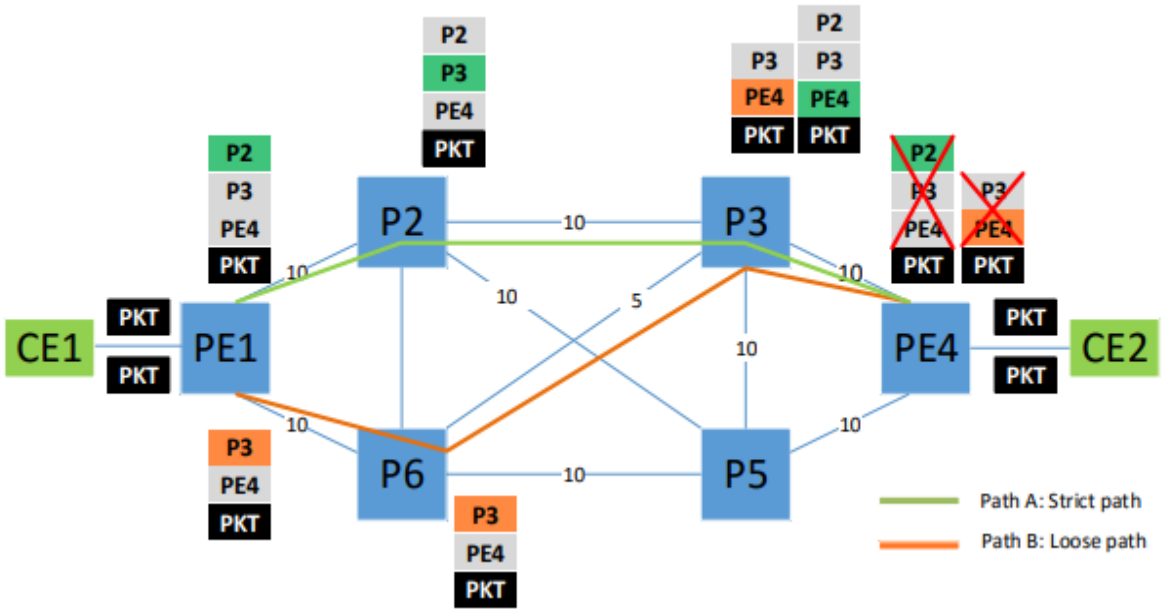


Figure 2.1 : Chemin A est un chemin strict où tous les nœuds intermédiaires sont transportés Dans l'en-tête du paquet. Le chemin B est un chemin lâche car seul un sous-ensemble de L'intermédiaire de nodes est porté dans l'en-tête du paquet

2.3.1 Source Routing with IPV4

Comme mentionné ci-dessus, le routage source a été introduit dans les premières versions de l'IPv4 standards, il a été implémenté en option dans l'en-tête IPv4, pour lequel deux Types ont été définis : type 131 pour Loose Source and Record Route (LSRR) et type 137 pour Strict Source and Record Route (SSRR).

La norme IPv4 limite la longueur du SRP à un maximum de 9 adresses IPv4 Car il est transporté en option dans l'en-tête du paquet IPv4, qui a une taille maximale de 40 octets. Chaque nœud traversé par le paquet est enregistré, ce qui permet la destination de construire son propre itinéraire lâche ou strict afin de répondre par le même chemin.

Le routage source IPv4 était à l'origine utilisé par les administrateurs réseau pour effectuer Tâches telles que la découverte du réseau, les mesures et le débogage. En raison de la découverte Vulnérabilités et son exploitation à des fins malveillantes, telles que la conduite d'attaques par déni de service, d'usurpation d'identité, de contournement de pare-feu et d'autres attaques. Ainsi, la majorité des administrateurs réseau ont désactivé la prise en charge de ces options dans leurs réseaux. En conséquence, l'IETF conseille maintenant que les paquets avec LSRR et SSRR les options devraient être abandonnées. [12].

2.3.2 Source Routing with IPV6

Le comportement de routage source d'IPv4 a été reproduit dans l'en-tête d'extension IPv6 Type 0 En-tête de routage (RH0), copiant presque les mêmes concepts que dans IPv4. Au contraire vers IPv4, le RH0 est un en-tête d'extension et sa taille est limitée uniquement par le maximum unité de transmission. Pour cette raison, un RH0 peut transporter des chemins plus longs par rapport à IPv4. Par exemple, avec une unité de transmission maximale de 1500 octets, un SRP peut être composé de 90 adresses IPv6, avec la possibilité d'inclure la même adresse plusieurs fois. Cependant, les gros SRP ont aggravé les choses à partir d'un point de sécurité de vue. Par exemple, une attaque par déni de service peut être effectuée par amplification sur un chemin spécifique entre deux nœuds, cette attaque est plus puissante avec RH0 qu'avec le routage source IPv4, en raison du fait que le nombre d'adresses IP porté dans le RH0 est beaucoup plus grand que l'option de routage source IPv4 : le RH0 peut porter jusqu'à 90 adresses par rapport à seulement 9 pour IPv4, ce qui donne à l'attaquant le possibilité d'osciller jusqu'à 44 fois entre deux nœuds, ce qui créer une congestion sur cette voie. En conséquence, l'IETF a déprécié le soutien de RH0 La dépréciation de RH0 visait à mettre fin à son exploitation à des fins malveillantes, mais pas à empêcher totalement l'utilisation du routage des sources dans les réseaux IPv6. En effet, de nouveaux en-têtes de routage sécurisés ont été définis pour fournir le routage source pour différents types de réseaux. Par exemple, un en-tête de routage IPv6 pour les routes sources avec Protocole de routage pour les réseaux à faible consommation et à perte et le routage de segment en-tête d'extension. [13]

2.3.3 Source Routing with MPLS

Les réseaux MPLS ont également profité du routage des sources. Utilisation de l'opération PUSH
plusieurs étiquettes sont ajoutées à l'en-tête du paquet, ce qui est connu sous le nom d'empilage d'étiquettes.
Chaque étiquette de la pile identifie un LSP unique. Ces LSP sont préétablis
soit par RSVP-TE ou par LDP ou BGP. Chaque nœud intermédiaire installe un état dans sa table d'acheminement pour chaque LSP qui la traverse.
Contrairement à l'implémentation IPv4/IPv6 du routage source où une adresse IP identifie un nœud unique. Dans MPLS, un label est local au nœud et détermine le chemin vers

un saut (direct ou au-dessus d'un LSP). De plus, la mise en œuvre de MPLS ne souffre des mêmes problèmes de sécurité que dans IPv4/IPv6, car un fournisseur de services le trafic provenait de sources non fiables.

Dans la section suivante, nous expliquons plus en détail comment l'architecture de la RS tire parti du paradigme de routage source et spécificités d'implémentation pour chaque plan de données : MPLS et IPv6. [11]

2.4 Principe du Segment Routing

Le Segment Routing est un routage par la source qui identifie une route par un ensemble de segments connus par leurs identifiants, SID (Segment Identifier (SID)). La route est calculée par un contrôleur de route qui la transmet aux éléments du réseau. Le nœud d'entrée rajoute aux informations à transmettre un entête constitué d'un ensemble d'identifiants de segments par lesquels l'information va circuler. Un identifiant de segment entraine une action de type relayage ou de type service. Avec ce routage, il n'y a plus besoin d'utiliser de protocoles d'établissement de chemin distribué, les chemins et leurs labels sont prédéfinis.

2.5 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.

2.6 Terminologie

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

2.6.1 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 Elément 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. [14]

2.6.2 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. 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. [10]

2.6.3 Segment global

L'instruction associée est supportée par tous les SR-nœuds capables dans le domaine. Dans l'architecture MPLS, Le segment a un indice unique au monde. L'étiquette locale associée à un nœud donné N est trouvé en ajoutant l'index global-unique à la SRGB du nœud N. Dans l'architecture IPv6, un segment global est une adresse IPv6 unique.

SID global = index Préfix-SID + base SRGB.

SID global ≤ limite supérieure du SRGB.

2.6.4 Segment local

L'instruction associée est supportée uniquement par le nœud Dans l'architecture MPLS, il s'agit d'une étiquette locale en dehors de la SRGB Dans l'architecture IPv6, cela peut être n'importe quel IPv6 adresse dont l'accessibilité n'est annoncée dans aucun protocole de routage. (Par conséquent, le segment n'est connu que par le nœud local).

2.6.5 SRGB

Segment Routing Global Block (SRGB) est l'ensemble des segments globaux dans le domaine SR. 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 nœud 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 nœud.[23]

2.6.6 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 nœuds qui les allouent. [15]

2.6.7 PCE

Un Path Computation Elément (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 nœud 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 utilise dans les calculs de chemin.[10]

2.7 Identificateurs de segment

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. [10]

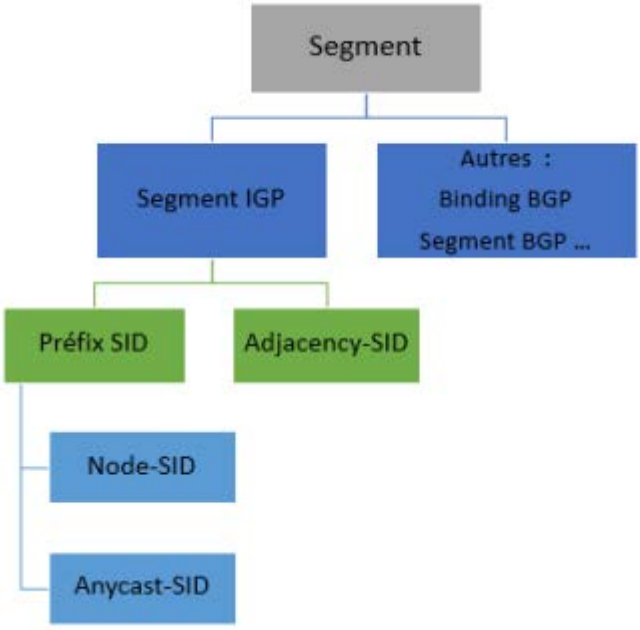


Figure 2.2 : Segments SR

2.7.1 Préfix SID

Il correspond à un segment qui permet d'atteindre une adresse IP configurée sur le réseau et annoncée dans l'IGP4. En ajoutant dans un paquet le préfix SID configuré sur un routeur, on est certain que le paquet transitera par celui-ci. C'est l'IGP qui déterminera le chemin à emprunter sur le réseau pour rejoindre le nœud pointé par le préfix SID. Il est aussi possible de positionner un préfix SID qui serait configuré sur plusieurs routeurs afin de faire passer le paquet par une zone donnée sans toutefois spécifier un équipement particulier. Par exemple, si l'on souhaite faire transiter un paquet par un point de présence de Marseille composé de plusieurs routeurs, on configurera simplement le même préfix SID sur tous les équipements marseillais et on l'ajoutera dans le paquet. Notons bien qu'un préfix SID doit être unique sur le réseau et connu de tous les équipements, qui savent ainsi comment l'interpréter.−Adjacency SID : il représente une interface précise d'un équipement, ou plus précisément une adjacence vers un voisin. Il n'est compris que de l'équipement qui dispose de cette interface et n'a donc à être unique que sur ce dernier. Un paquet pourra donc contenir un ou plusieurs SID. Seul le premier SID est interprété par un routeur. Une fois un segment réalisé, le SID correspondant est retiré et c'est le suivant qui est considéré.

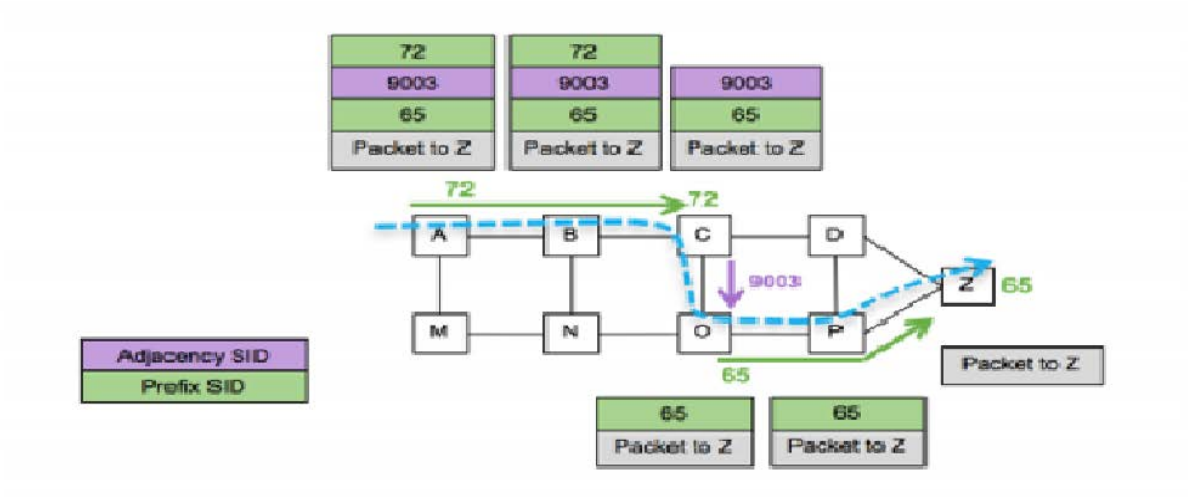


Figure 2.3 : segment mixe composé de prefix SID et d'adjacency SID

L'exemple ci-dessus montre un segment composé de deux préfix SID en vert et d'un Adjacency SID en violet. Le premier préfix SID 72 va permettre d'acheminer le paquet jusqu'à C. Le SID 72 est retiré et C voit un paquet avec un Adjacency SID de valeur 9003, correspondant à son interface vers O. Il envoie ce paquet sur cette interface et le SID est également retiré. Finalement, O envoie le paquet vers Z qui est configuré avec le préfix SID 65. On notera qu'il a fallu tout d'abord envoyer le paquet vers le routeur C en utilisant son préfix SID, car c'est uniquement ce nœud qui était en mesure de gérer l'Adjacency SID 9003 (lien entre C et O).

2.7.1.1 Node - SID

Segment IGP-Node, Node-SID est un sous type spécial de préfixe du segment. Ce dernier signifie un chemin vers un nœud (par exemple loopback) dans un domaine IGP, il est identifié par la valeur du nœud SID .qui est unique dans le domaine SR. [16]

2.7.1.2 Anycast – SID

Un segment IGP-Anycast est un segment préfixé IGP qui n'identifie pas un routeur spécifique, mais un ensemble de routeurs. Un "Anycast Segment" ou "Anycast SID" applique le chemin le plus court de l'ECMP vers le nœud le plus proche de l'ensemble anycast.

2.7.2 Adjacency SID

Un identifiant de segment de proximité (Adj-SID) est utilisé par un nœud de routage de segment pour annoncer ses liens aux routeurs adjacents [30]. Les ADJ-SIDs doivent prendre une valeur en dehors de l'intervalle SRGB, et ils ne sont pas uniques dans le domaine SR par défaut. Par conséquent, plusieurs liens peuvent avoir le même Adj-SID. 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 Préfix-SID. Dans l'exemple de la figure ci-dessous, le routeur Constantine possède trois liens d'adjacence, il attribué donc un Adj-SID diffère 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.

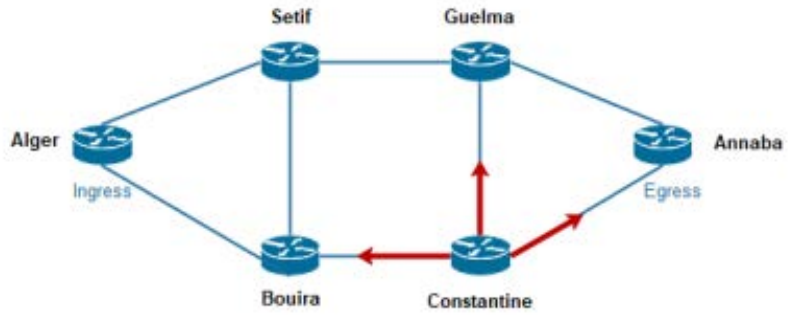


Figure 2.4 : Adjacency Segment ID

2.7.3 Binding SID

Est une étiquette qui peut être utilisée pour imbriquer et assembler les domaines. Cette fonctionnalité est utile s'il y a des domaines non-SR sur le chemin du trafic. Par exemple, si deux domaines SR sont séparés par un domaine RSVP-TE, le binding-SID peut être utilisé pour atteindre le début du tunnel RSVP-TE. En utilisant un binding-SID entre deux domaines sur une passerelle permet l'utilisation d'une pile d'étiquettes plus courtes [28]. Le segment Binding est utilisé pour associer une politique SR à une SID. Un paquet reçu avec Le BSID sera orienté sur la politique SR associée, ce qui signifie que le paquet sera transmis en utilisant la liste de segments. En utilisant le segment de liaison, il est possible de séparer les processus de classification des paquets par une politique SR spécifique. La politique SR peut être modifiée à temps sans avoir à modifier le processus de classification. Cela améliore

l'évolutivité, résilience et l'indépendance de service des solutions basées sur Acheminement des segments. [15]

2.8 De l'MPLS vers le SR

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 protocoles 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 nœud globalement. Ainsi, les paquets peuvent être transférés vers le nœud en se basant sur son SID global. De cette façon, l'ECMP 3 peut être implémenté, chose qui n'est pas possible avec le RSVP-TE. D'un côté, 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 côté, 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 nœud 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 Engineering 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. Ce concept est détaillé dans la section de TE avec segment Routing.

2.9 Opération de SR

SR-MPLS utilise le plan de transfert MPLS. Par conséquent, les paquets SR sont manipulés en utilisant les opérations de plan de données MPLS PUSH, POP (NEXT) et SWAP (CONTINUE) :

- PUSH : L'opération push est effectuée par les nœuds d'entrée (LER), qui encode dans l'en-tête du paquet la liste des labels qui composent le chemin SR. Il est également utilisé

par les nœuds intermédiaires pour ajouter une ou plusieurs étiquettes supplémentaires à des fins de réacheminement et de protection.

- SWAP (CONTINUE) : L'opération de swap est effectuée pour remplacer le label actif avec un autre qui est nouveau. Il est appelé CONTINUE parce que l'ancienne et la nouvelle étiquette pointent vers le même segment, ils appartiennent simplement à deux SRGB différentes.
- POP (NEXT) : Lorsque l'opération pop est effectuée, l'étiquette active est supprimée de la pile d'étiquettes. Dans l'implémentation de SR, l'opération POP est appelée NEXT parce que "sauter l'étiquette de niveau supérieur" signifie que la prochaine étiquette pointera vers le prochain segment du chemin SR.

2.10 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.

Selon l'exemple illustré dans la figure 2.5, un paquet est envoyé d'Alger vers Guelma, les deux chemins Alger -Sétif- Constantine, Alger - Bouira- Constantine ont la même préférence, on peut passer par les deux, puis le chemin Jijel - Guelma(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 (Constantine - Annaba -Guelma). Pour effectuer cela, nous forçons 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 32000. 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 Constantine et l'ADJ-SID du lien noir. Ensuite, il envoie le paquet à Sétif. A la réception du paquet par Sétif, celui-ci trouve qu'il ne lui est pas destiné, il transfère le paquet vers l'interface de sortie en direction du prochain saut Constantine. Une fois le paquet arrivé à Constantine, 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 32000 indiquant le lien noir, il envoie donc le paquet via ce lien en direction d'Annaba. Annaba reçoit le paquet et l'envoie à son tour vers Guelma qui découvre que son Node-SID est le segment actif et donc le paquet lui ai destiné et enfin il supprime le segment.

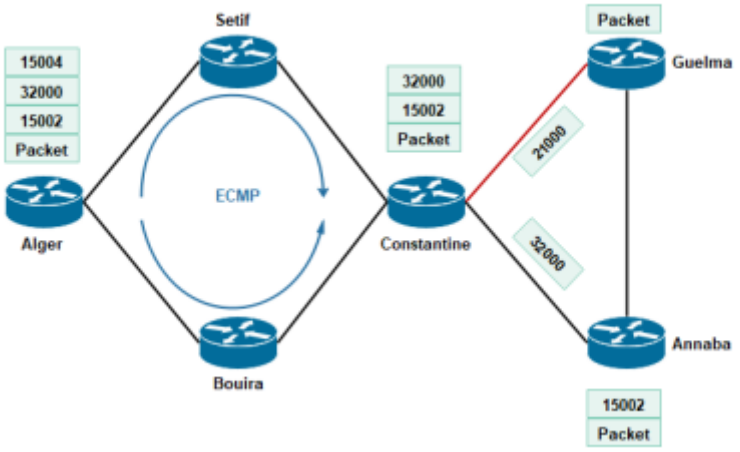


Figure 2.5 – Acheminement d'un paquet en SR

2.11 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. Dans l'IGP protocoles, les informations SR (par exemple SRGB, SIDs, etc...) sont encodées dans un format Type Length Value (TLV) et transportées dans l'opaque Link State Advertisement (LSA). Nous verrons dans cette section les extensions des protocoles pour supporter le SR.

2.11.1 Extensions d'OSPF

Pour activer le SR, OSPF étend ses TLV pour transporter et diffuser les informations nécessaires. Les tableaux 1 et 2 définissent les nouvelles extensions.

TLV	Fonction
SR-Algorithme 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

Tableau 2.1 : 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

Tableau 2.2 : Extension SUB TLV OSPF pour SR

2.11.2 Extensions d'ISIS

Pour activer le SR, IS-IS étend ses TLV pour transporter et diffuser les informations nécessaires, ces extensions sont définies dans le tableau 1.

Sub-TLV	Fonction
Prefix-SID Sub-TLV	Annonce le préfixe SID
Adj-SID Sub-TLV	Annonce l'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-algorithme Sub-TLV	Annonce l'algorithme utilisé
SR Local Block Sub-TLV	Annonce le SRLB

Tableau 2.3 : extensions IS-IS pour SR

2.12 Extensions des protocoles BGP

2.12.1 BGP-préfix-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 spécifiée. Il est configuré manuellement à partir de la plage d'étiquettes du SRGB.

2.12.2 BGP-LS

Le BGP-LS est une extension du BGP conçue pour transporter et partager les informations d'état de liaison collectées par l'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 nœud 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 nœud, lien et préfixe. Par exemple, il peut s'agir de noms de nœuds, de métriques IGP, de métriques TE, de Bande passante disponible...

2.13 Application du SR

Dans cette section, nous concentrons sur les premiers cas d'utilisation qui ont été spécifiés comme premiers scénarios pour mettre en évidence les avantages de l'acheminement des segments. Le tout premier qui a reçu beaucoup d'attention et de soutien, surtout du service fournisseurs, est la protection de lien et de nœud, qui permet une récupération rapide efficace en cas d'échecs. Le deuxième scénario est le VPN, où SR simplifie le déploiement du VPN. Le dernier est l'ingénierie du trafic (TE), c.-à-d. comment le SR est utilisé pour contraindre les chemins. [10]

2.13.1 Fast ReRoute avec SR

SR fournit une protection automatique du trafic sans aucune restriction topologique. Le réseau peut protéger le trafic contre les défaillances de liaison et de nœud sans nécessiter la signalisation dans le réseau. La technologie IP Fast Reroute (FRR) existante, en combinaison avec les capacités de routage explicites dans SR, En outre, SR FRR mécanisme connu comme Topology Independent Loop Free Alternate (TI-LFA) améliore le classique Des solutions IP-FRR offrant une couverture de protection à 100 % par rapport aux SFT variétés : SFT, SFT éloignés (RLFA) et SFT dirigée (DLFA).

En fait, un nœud SPRING précommande automatiquement la récupération post-convergence chemins pour chaque segment (par exemple, Node-SID, Adj-SID) affecté par la liaison ou la défaillance du nœud cela se fait avec un impact opérationnel minimal. Il n'est pas nécessaire d'avoir un plan de contrôle des protocoles pour établir et maintenir les voies de protection (p. ex., séances dirigées du PAP ou tunnels RSVP-TE). Dans SR-MPLS, le chemin de protection prend la forme d'une pile d'étiquettes. Selon le type de lien de défaillance ou de nœud, un nœud SPRING calcule la voie de protection post-convergence pour contourner la défaillance. Tout type de protection peut être informatique : protection des maillons, protection des noeuds, protection SRLG. Les opérations utilisées pour activer la protection en fonction de la DSRI active (étiquette du haut) dans le chemin SR initial :

pousser la pile d'étiquettes de protection, permuter l'étiquette active avec son équivalent au saut suivant du chemin de protection, ou pop l'étiquette active et poussez le chemin de récupération.

Dans l'exemple illustré à la fig. 2.15, en s'appuyant sur SR-MPLS, P E1 pousse une étiquette 1004 sur le paquet de CE1 pour atteindre CE2 en utilisant le chemin le plus court IGP P E1 P2 P3 P E4. Le nœud P2 installe dans sa table de transmission des entrées alternatives à réacheminer le trafic via P5 en cas de défaillance de la liaison P2 P3. Si P2 détecte que P3 est inaccessible (par exemple, détecté par la détection de transfert bidirectionnel (BFD) protocole). Ensuite, pour rediriger le trafic, P2 pousse l'étiquette 15035 (l'Adj-SID attaché à la contiguïté P5 P3) dans les en-têtes des paquets, et l'envoie à P5. P5 fait apparaître l'étiquette 15035, puis transmet les paquets à P3. Du P3 au P4 les paquets utilisent le Node-SID de P4 : 1004 pour atteindre P4 via le chemin IGP le plus court.

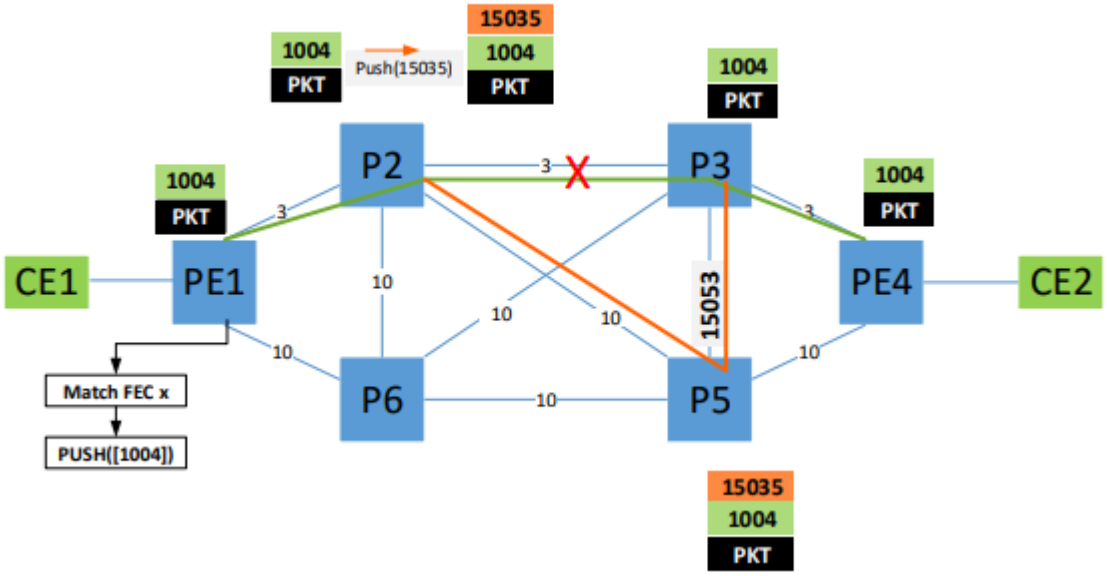


Figure 2.6 : Protection locale de la liaison entre P2-P3 avec acheminement de segment

Si P2 est configuré pour la protection des nœuds, pour rediriger le trafic il échange le NODESID de PE4 avec sa valeur équivalente à P5 et le transmet à P5 pour forcer le SR chemin de contournement P3 en suivant le P5 P E4. Dans les deux cas, SR 50 millisecondes de réacheminement rapide sans avoir besoin d'un réacheminement préétabli (signalé) chemins.

De plus, dans notre exemple, la défaillance est contournée avant que P E1 n'obtienne l'information ; P2 détecte et réagit rapidement à la défaillance (réagit au lien P2 P3 échec) en redirigeant le trafic sur le chemin de secours P2 P5 P3. Ensuite, L'IGP de P2 converge et propage les informations de défaillance à ses nœuds adjacents, P E1 obtient l'information sur l'échec et décide de recalculer un nouveau post chemin SR de convergence avec la même destination PE4. Une fois le nouveau chemin SR (i.e., P E1 P2 P5 P E4) est en place, P E1 envoie les paquets client avec le nouveau pile d'étiquettes. [11]

2.13.2 VPN avec SR

Le Segment Routing fournit le transport, MPLS VPN fournit le service. Elles ne s'excluent pas mutuellement, mais elles sont complémentaires. Afin de créer un service VPN MPLS de bout en bout, le routage de segment et le VPN MPLS doivent être fournis ensemble dans le réseau. Ainsi, le routage de segment est sous-jacent, le VPN MPLS est superposé.

Le VPN MPLS peut être configuré sans routage de segment. Au lieu de Segment Routing comme un mécanisme de transport, LDP, RSVP, BGP ou plane IP peut être un transport pour

Les VPN.
Permettez-moi d'expliquer tout ce qui précède avec l'exemple ci-dessous.

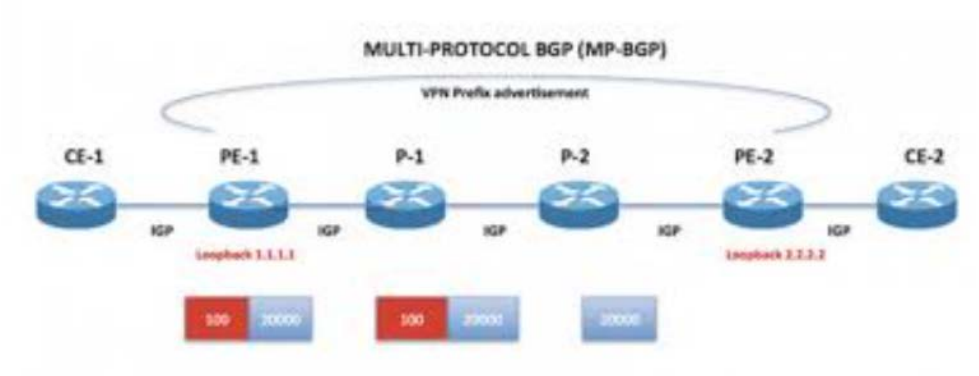


Figure 2.7 : Segment Routing and MPLS VPN

L'architecture de routage des segments est traitée dans la RFC 8402.

Si vous ne connaissez pas du tout le routage de segment, je vous suggère de lire mon article sur les points clés du routage de segment maintenant. Si les notions de base vous conviennent,

Veuillez continuer à lire.
L'étiquette 100 pour le loopback PE2 (Egress PE) est annoncée avec le protocole IGP (pas via LDP ou RSVP), et tous les routeurs utilisent un label identique. (L'étiquette Node/Prefix est Unique sur tout le réseau).

Contrairement au LDP, l'étiquette 100 ne change pas hop par hop avec Segment Routing. Grâce à MP-BGP, PE1 reçoit toujours une étiquette VPN pour les préfixes CE2 de PE2. BGP next hop est le loopback PE2 sur PE1.

La boucle PE2 se voit attribuer l'étiquette 100 et est annoncée dans les publicités IS-IS sub-TLV ou OSPF Opaque LSA.

Dans l'image ci-dessus, Label 2000 est l'étiquette VPN qui est annoncée par PE2 à PE1 pour le préfixe CE2.

Si vous êtes familier avec les VPN MPLS, n'oubliez pas que les routeurs P (P-1 et P-2 dans la topologie) ne sont pas au courant de l'étiquette VPN.

P1 ne change pas l'étiquette core/transport (Label 100), il envoie juste le paquet au P2. Si P2 reçoit un label nul implicite de PE2, P2 fait PHP (Penultimate Hop Popping). En somme, seul le label VPN est envoyé au PE2.

Sans utiliser LDP mais juste en utilisant IGP, le service VPN MPLS est fourni. L'acheminement des segments ne nécessite pas de LDP pour le tunnel de transport car il utilise IGP pour la publicité sur l'étiquette.

Veuillez noter que l'acheminement des segments élimine l'utilisation du LDP uniquement pour l'opération de l'étiquette de transport.

Si vous configurez le service VPN de la couche 2 de MPLS et que vous utilisez le LDP pour la signalisation PW, l'acheminement des segments et le LDP ciblé sont utilisés comme deux protocoles de plan de contrôle pour configurer le VPN L2 de MPLS. MPLS est très puissant avec ses applications.

Les VPN de la couche 2 de MPLS (VPWS, VPLS et VPMS), les VPN de la couche 3 de MPLS et l'ingénierie du trafic de MPLS sont les applications les plus courantes des réseaux IP/MPLS.
MPLS Traffic Engineering est utilisé dans les grands réseaux d'entreprise, en particulier dans les fournisseurs de services et Web OTT. [17]

2.13.3 TE avec le SR

L'acheminement des segments pour l'ingénierie du trafic (SR-TE) se fait par un tunnel entre la source et la destination paire. Le routage de segment pour l'ingénierie du trafic utilise le concept de routage de source, où la source calcule le chemin et l'encode dans l'en-tête du paquet en tant que segment. Chaque segment est un chemin de bout en bout à partir de la source à la destination, et instruit les routeurs dans le réseau central du fournisseur de suivre le chemin spécifié à la place du chemin le plus court calculé par l'IGP. La destination n'est pas au courant de la présence du tunnel. Besoin Avec le routage sectoriel pour l'ingénierie du trafic (SR-TE), le réseau n'a plus besoin de maintenir une application par application et à l'état par flux. Au lieu de cela, il obéit simplement aux instructions de transfert fournies dans le paquet. SR-TE utilise la bande passante du réseau plus efficacement que les réseaux MPLS-TE traditionnels en utilisant ECMP à chaque niveau de segment. Il utilise une seule source intelligente et soulage routerssremaining de la tâche de calcul le chemin requis à travers le réseau. [18]

2.13.3.1 Fonctionnement

- Lorsqu'un paquet arrive au nœud d'entrée SR, il est soumis à une stratégie. Si le paquet satisfait les conditions pour emprunter un chemin SR, le nœud d'entrée SR l'encapsule dans un tunnel SR, et il parcourt le chemin SR, segment par segment.

- Chaque segment d'un chemin SR dispose d'un nœud de terminaison. Lorsqu'un paquet arrive à l'un de ces points de terminaison, son étiquette ou son en-tête externe est examiné et il est envoyé vers le segment correspondant. Avant d'être transféré vers le point de terminaison du segment suivant, l'étiquette ou l'en-tête externe est retiré. Ce processus se poursuit jusqu'à ce que le paquet arrive au point de terminaison du segment final, souvent le nœud de sortie SR.

- Lorsqu'un paquet arrive au nœud de sortie SR, le nœud détermine si le paquet est à la fin de son chemin ou non. Si c'est le cas, le nœud retire les informations de l'en-tête SR et transfère le paquet en fonction de son adresse IP de destination.

- Les routeurs de transit transfèrent simplement les paquets en se basant sur l'identifiant de segment SR (SID), c'est pourquoi le SR peut servir à mapper des paquets associés à un utilisateur final ou à une application vers des services de fonction réseau spécifiques. Il le fait en mappant un chemin vers l'emplacement où le service sera appliqué, accompagné d'instructions sur le service, puis en fournissant le chemin supplémentaire de la passerelle de service au routeur sortant du domaine SR. [19]

2.13.3.2 La gestion du trafic aves des contrôleurs de segment Routing

Les contrôleurs SR sont un type de contrôleur SDN qui gèrent les aspects techniques du trafic, fournissent un calcul de chemin centralisé, une visibilité granulaire, et un contrôle du flux de trafic pour les plans de transfert SR dans les réseaux de fournisseurs de services et d'entreprise. Le contrôleur SR permet d'optimiser les réseaux d'opérateurs à travers une surveillance et une planification en amont, et une répartition dynamique des grandes charges de trafic en fonction de contraintes spécifiées.

L'un des principaux avantages de ces contrôleurs est leur capacité à réserver de la bande passante de façon bien plus efficace que le routage de segments lui-même. En déplaçant les informations sur l'état du chemin des routeurs de transit au paquet, le routage de segments élimine le besoin de

protocoles tels que le LDP (Label Distribution Protocol) et le RSVP-TE (Resource Reservation Protocol-Traffic Ingénierie), qui distribuent les informations sur le chemin à travers le réseau. Le protocole RSVP-TE dispose d'un mécanisme permettant de réserver la bande passante. C'est pourquoi il peut être difficile de s'en passer dans les réseaux pour qui nécessite une telle réservation.

Les contrôleurs SR, qui surveillent en temps réel les moindres recoins du réseau ainsi que les flux de trafic, répondent à ce problème. Ils utilisent ces données pour déterminer les chemins explicites que les paquets doivent emprunter à travers le réseau. Ils peuvent également allouer de la bande passante à ces chemins. Une fois que les chemins sont calculés et que la bande passante est allouée, le contrôleur ajoute ces informations à sa base de données. Le contrôleur prend en compte les besoins existants en bande passante lorsqu'il calcule de nouveaux chemins, ou lorsque certaines conditions dynamiques, un encombrement par exemple, le forcent à rediriger le trafic.

Le contrôleur réalise trois opérations de base.

- Analyse
- Optimisation
- Automatisation

En collectant soigneusement les données de télémétrie granulaire du réseau, le contrôleur analyse les données et les optimise pour qu'elles contribuent à la prise de mesures intelligentes telles que la tunnelisation du trafic à travers le chemin de réseau le plus efficace, le respect des exigences de SLA ou la résolution en amont des problèmes d'encombrement.

NorthStar Controller, le contrôleur SDN (Software-Defined Networking) WAN de Juniper pour l'optimisation du trafic, fournit ces capacités et vous permet d'avoir une visibilité et de surveiller plusieurs domaines réseau. Grâce au contrôleur NorthStar, vous bénéficiez d'une visibilité de bout en bout sur le réseau, d'une optimisation des aspects techniques inter-domaines du trafic, et du découpage de réseau de bout en bout.

Le contrôleur NorthStar vous aide également à migrer vers le SR en centralisant le contrôle du routage et en vous donnant la possibilité d'exécuter plusieurs plans de contrôle sur la même infrastructure pendant votre migration. L'interface graphique du contrôleur NorthStar fournit une

visibilité en temps réel très précise sur le réseau, qui est particulièrement utile pour sa conception et son exploitation. [20]

2.13.3.3 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 plus élevé. Le meilleur chemin sélectionné est enregistré dans table FIB, il est identifié par un Binding SID et il possède un état (valide ou invalide) et le protocole source (BGP, statique ou PCEP).

L'exemple présenté dans la figure 1 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, tous les chemins candidats d'une stratégie SR se voient attribuer le même BSID.

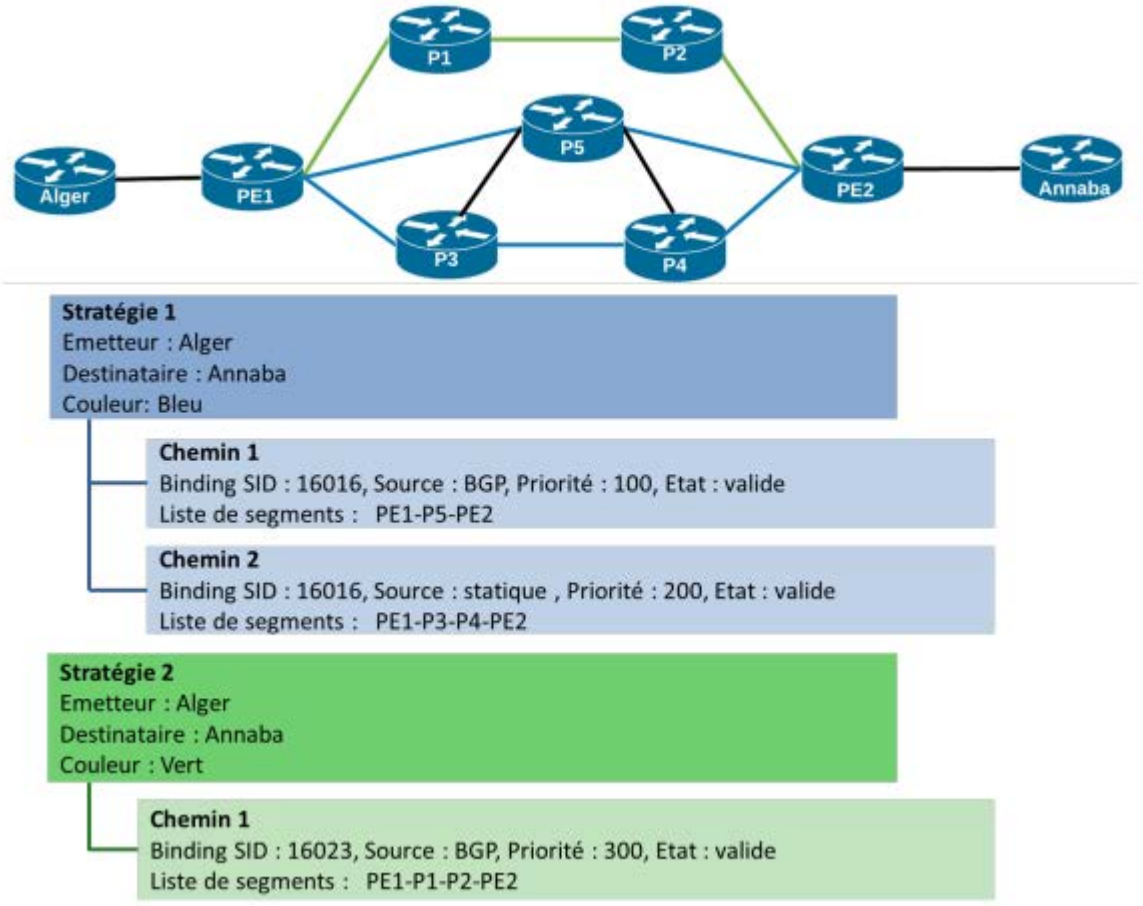


Figure 2.8 : Stratégie SR

2.14 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.

2.14.1 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. [19]

2.14.1.1 Définition

SDN est une technologie qui rend le réseau programmable c'est-à-dire réseau défini par logiciel. Ce dernier présente une architecture réseau où le plan de contrôle est totalement découplé du plan de Données.

Le plan de contrôle gère la gestion des périphériques réseau, tandis que le plan de données est la Couche matérielle responsable du transfert des paquets réseau selon les politiques définies dans Le plan de contrôle. Ce découplage transforme les commutateurs/routeurs réseau en simples dispositifs de transfert, tandis que la commande logique est implémentée dans le contrôleur qui fonctionne comme un système d'exploitation réseau centralisé. Ainsi, le SDN est composée de deux entités : le contrôleur et les Dispositifs de transfert (switch ou routeur).

Le SDN comme ensemble de solutions/architectures permettant de supprimer les frontières

Existantes entre les mondes des applications et du réseau. Ce qui le rend donc plus globalement reconnu Aujourd 'hui comme une architecture permettant d'ouvrir le réseau aux applications. Cela intègre les deux volets suivants :

- permettre aux applications de programmer le réseau afin d'en accélérer le déploiement.

- permettre au réseau de mieux identifier les applications transportées pour mieux les gérer (qualité de service, sécurité, ingénierie de trafic...). [21]

2.14.1.2 Architecture de SDN

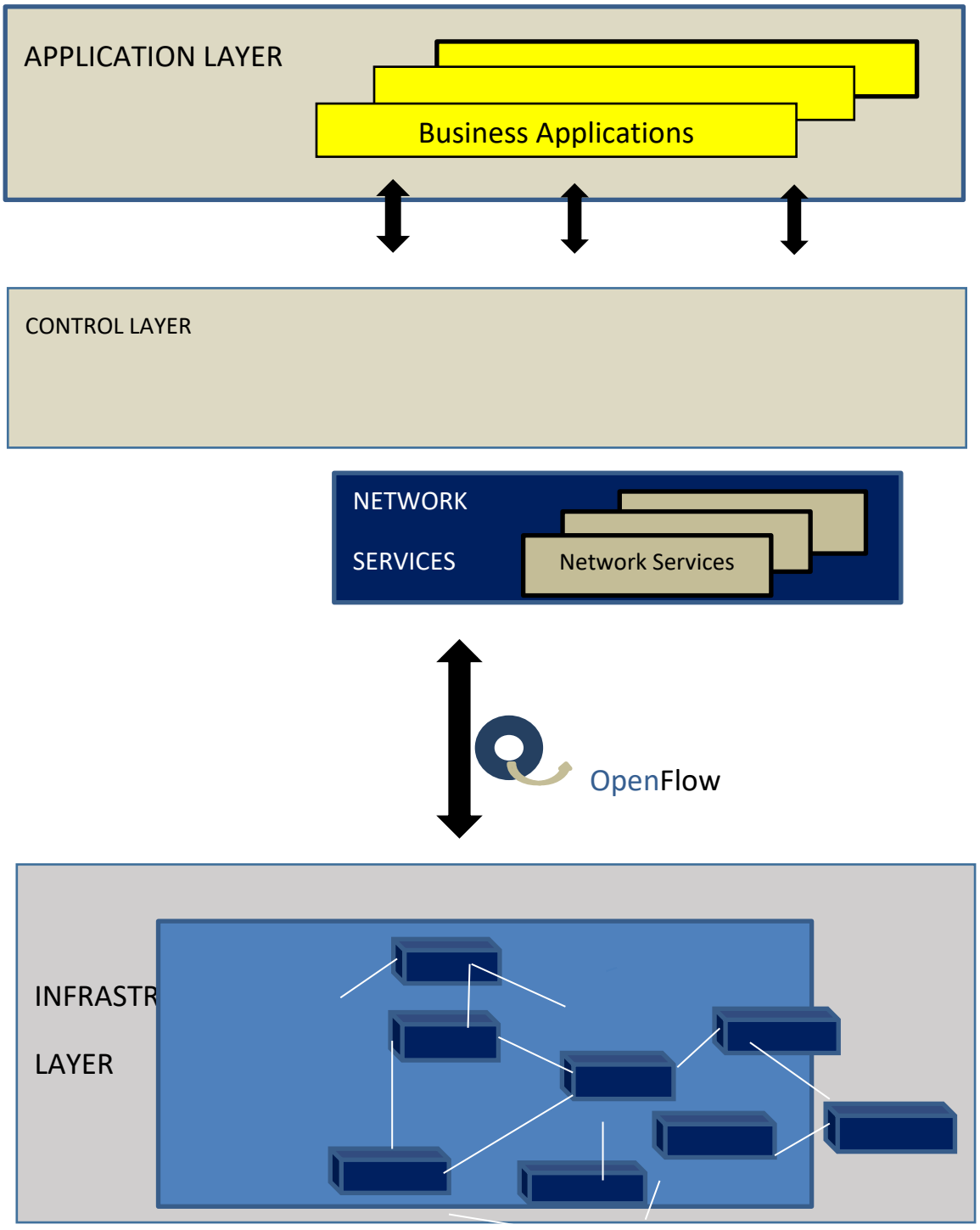


Figure 2.9 : fonctionnement d'une structure d'équipement réseau utilisant la technologie SDN

SDN se compose de 3 couches :

1- la couche infrastructure (la couche de transmission) : c'est la couche la plus basse, elle contient les équipements de transmission (FEs : forwarding éléments) tels que les switch physiques et virtuels. Son rôle principal est l'acheminement du trafic et qui supportent le protocole open flow qu'ils partagent avec le contrôleur.

2- la couche de contrôle : ces contrôleurs utilisent des interfaces southbound pour contrôler le comportement des FEs et communiquent via des APIs northbound avec la couche supérieure pour superviser et gérer le réseau. C.-à-d. offre une visibilité globale du réseau et des équipements d'infrastructure.

3- la couche applicative : héberge les applications qui peuvent introduire de nouvelles fonctionnalités réseau, comme la sécurité, la configuration dynamique et gestion et apporte l'automatisation à travers du réseau, et à l'aide des interfaces programmables alternative. [12]

2.14.1.3 avantage du SDN

- Réseaux programmables

Avec SDN, il est plus simple de modifier les stratégies réseau car il suffit de changer une politique

De haut niveau et non de multiples règles dans divers équipements de réseau. De plus, la facilité de la conception et du contrôle du réseau, et surtout l'existence d'une structure de contrôle centralisée du trafic dans le réseau avec des connaissances globales et une puissance de calcul élevée, simplifient le développement de fonctions plus sophistiquées (centralisation et programmabilité).

- Flexibilité

SDN apporte également une grande flexibilité dans la gestion du réseau. II devient facile de

Rediriger Ie trafic, d'inspecter des flux particuliers, de tester de nouvelles stratégies ou de découvrir des flux inattendus. Donc il permet d'augmenter le taux d'innovation au niveau de l'infrastructure réseau, et cela conduit à l'apparition de nouvelles idées. Par exemple, les développeurs peuvent tester des applications au sein du réseau sans affecter les performances du réseau ou des services. Ce qui nous permet d'obtenir des performances plus élevées par rapport à celles qui existent actuellement.

- Politique unifiée

Avec son contrôleur, SDN garantit également un politique réseau unifiée et à Jour, puisque le

Contrôleur est responsable de l'ajout de règles dans les commutateurs, il n'y a aucun risque qu'un Administrateur de réseau ait oublié un commutateur ou installé des règles incohérentes entre les Dispositifs.

Optimisation/Evolutivité

Technologie à faible coût à comparer avec les équipements réseaux actuels que nous achetons Fermés qu' 'il est impossible de développer ou de fusionner avec d'autres produits ou d'ajouter de Nouveaux périphériques, (on devient indépendant du foumisseur), ainsi que de réduire le nombre D'ingénieurs, et gagner le temps de travail de plus de 50% c'est-à-dire réduire le temps de travail d'un mois a moins de 15 Jours. [3]

2.14.1.4 La comparaison entre réseau traditionnel et SDN

	Réseau SDN	Réseau traditionnel
Fonctionnalité	- Découple le plan de contrôle de celui du plan de données. - Offre un meilleur contrôle du réseau et la possibilité de le programmer.	- Le contrôle du réseau est Complexe.
Configuration	- Configuration automatique à travers une centralisation du contrôle du réseau. -Optimisation de la configuration.	-Une configuration manuelle et la possibilité de faire des erreurs qui vont entrainer un comportement erroné du réseau.
Performances	- Contrôle global de l'information.	- le problème de configuration statique.
innovation	-Implémentation facile de logiciels et des mises à jour dans le réseau. -Environnements de tests Suffisants.	- Difficultés d'implémentation de logiciels et des mises à jour dans le réseau. -Environnements de tests Limites.

Tableau 2.4 : tableau comparatif entre le SDN et les réseaux traditionnels.

2.14.2 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 puisqu'elle permet de prendre des décisions de routage depuis une application en se basant sur des paramètres spécifiques tels 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. 5

- Surveillance du réseau.

- Apport d'une grande flexibilité, un contrôle complet et des capacités TE pour le trafic réseau.

2.15 SR vs MPLS

IP/MPLS	SEGMENT ROUTING
♣ En MPLS la signalisation des labels et la réservation des ressources sont effectuées par l'implémentation des protocoles de signalisation LDP et RSVP-TE. ♣ MPLS n'utilise pas des labels globaux ce qui signifie que les routeurs adjacents utilisent des labels différents pour atteindre la destination. ♣ En MPLS l'état des tunnels est maintenu dans chaque nœud que le trafic traverse. ♣ Dans les réseaux MPLS les chemins sont déterminés strictement hop by hop ce qui signifie que ECMP n'est pas pris en charge.	Dans le réseau SR il suffit d'avoir un IGP et une fois Segment-Routing est configuré l'IGP prendra les labels et les distribue dans le domaine IGP. ♣ Segment-Routing réduit l'échange des labels dans le réseau en utilisant des segments globaux. ♣ Dans Segment-Routing l'état est présent seulement au niveau du routeur de tête. ♣ Dans Segment-Routing l'équilibrage de charge entre deux chemins de coût égaux entre la source et la destination est intégré, cette propriété stabilise le réseau.

Tableau 2.5 : déférence entre segment Routing et MPLS

2.16 Bénéfices apportés par le SR

Le principal avantage de SR est sa capacité à simplifier le réseau et à réduire l'utilisation des ressources, facilitant ainsi la gestion et l'exploitation de votre réseau. D'autres avantages rendent la RS souhaitable dans un réseau.

- Le SR réduit le nombre de nœuds qui doivent être touchés pour l'approvisionnement et les changements de chemin. Cette action permet à SR d'être plus réactif aux changements de réseau, ce qui le rend plus agile et flexible que les autres solutions d'ingénierie du trafic. SR Trafic Engineering fournit la QoS des applications et cartographie les services réseau pour les utilisateurs finaux et les applications qui traversent le réseau.

- La technologie SR offre une résilience grâce à la restauration de la tête de ligne et à la technologie alternative sans boucle (TI-LFA) indépendante de la topologie, ce qui contribue à la fiabilité du trajet lors des pannes de réseau.

Lorsqu'il est utilisé avec un contrôleur PCE WAN, SR offre des avantages supplémentaires.
- Il fournit une réservation de bande passante avec une ingénierie du trafic simplifiée, car le contrôleur à la capacité d'assigner des attributs de lien et des contraintes de chemin et d'effectuer des calculs de chemin le plus court contraint en premier (CSPF).

-Il réduit le risque de transition que vous déployiez SRv6, SR-MPLS ou SRm6 sur votre réseau. Il le fait en fournissant un support hétérogène pour plusieurs plans de redirection, y compris MPLS et IPv6.

_Il facilite l'automatisation en boucle fermée en évaluant continuellement les conditions du réseau en temps réel, telles que les flux de paquets vers les services réseau, le comportement et les performances du réseau, et faire des changements une fois qui peut être distribué automatiquement sur le réseau sans avoir à pousser les changements à plusieurs routeurs via CLI.
-Il améliore la qualité de l'expérience de l'utilisateur final en définissant des chemins réseau spécifiques selon les exigences définies (également utilisés pour le découpage du réseau).

-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. [22]

2.17 Conclusion

Dans ce chapitre nous avons introduit le segment Routing qui permet de diminuer les inconvénients des réseaux IP / MPLS existants en termes d'évolutivité, de simplicité et de facilité d'utilisation. Nous avons constaté que cette technologie n'éxige 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 minimiser les protocoles à l'intérieur du réseau et primordial afin d'assurer davantage de stabilité et d'évolution. 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 III

Implémentation du segment Routing

Chapitre III

Implémentation du segment Routing

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.

3.1 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.

3.2 Architecture du réseau IP/MPLS

L'architecture du réseau qu'on va simuler est illustrée dans la figure 4.1, elle est composée de trois AS. Le premier AS est le réseau cœur constitué de cinq routeurs implémentant l'OSPF comme IGP et les deux autres AS sont deux réseaux d'agrégation implémentant l'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 cœur et vMx6 pour le réseau d'agrégation 1.

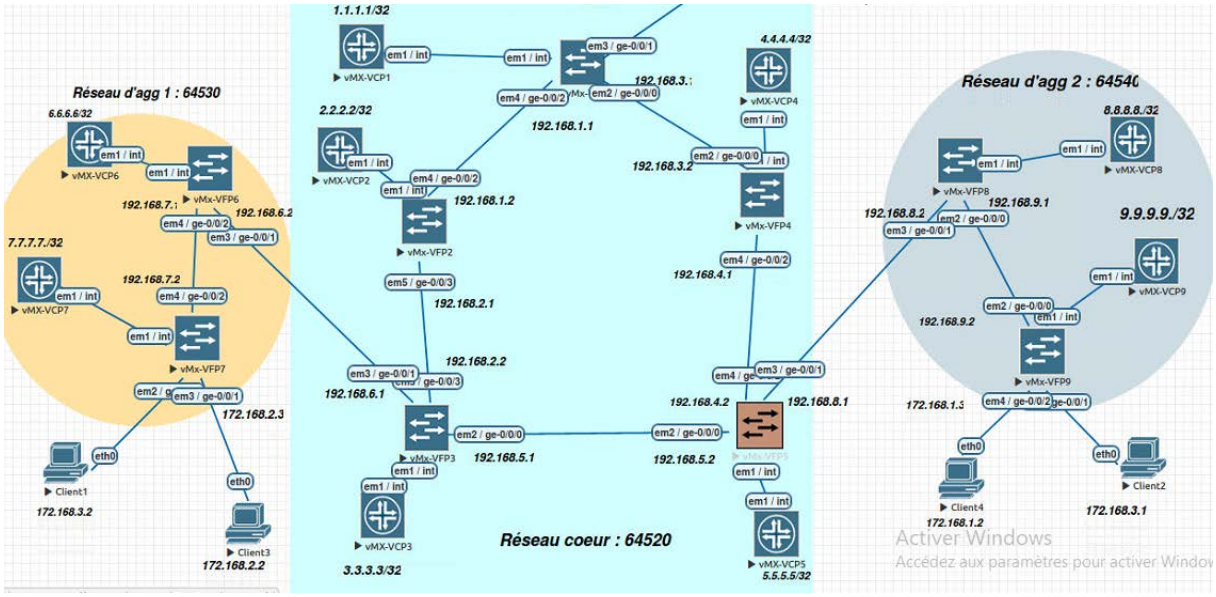


Figure 3.1-topologie du réseau simulé

3.3 Pré-configuration

3.3.1 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 (1) et (2) ensuite nous configurons l'adresse de loopback via la commande (3). Le tableau 4.1 dans l'annexe A illustre l'adressage complet.

```
[edit]
test@vMx1# set interfaces ge-0/0/2 unit 0 family inet address 192.168.1.1/2...

[edit]
test@vMx1# set interfaces ge-0/0/0 unit 0 family inet address 192.168.3.1/2...

[edit]
test@vMx1# set interfaces lo0 unit 0 family inet address 1.1.1.1/32
```

Figure 3.2-configuration des interfaces

3.3.2 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 (2-4)

```
[edit]
test@vMx1# set routing-options router-id 1.1.1.1

[edit]
test@vMx1# edit protocols ospf

[edit protocols ospf]
test@vMx1# set area 0.0.0.0 interface ge-0/0/0

[edit protocols ospf]
test@vMx1# set area 0.0.0.0 interface ge-0/0/2
```

Figure 3.3- configuation IGP au sein du cœur

et nous vérifions l'activation du protocole OSPF via la commande (1) sur La figure 3.4 qui montre la bonne configuration d'OSPF sur le routeur vMx1.

```
[edit]
root@R1# 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    39
192.168.1.2      ge-0/0/2.0             Full            2.2.2.2          128    35
```

Figure 3.4 : 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 (6) et nous ajoutons cette famille à l'adresse de loopback suivie de son adresse via la commande (7).

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

[edit protocols isis]
test@vMx6# set interface lo0

[edit protocols isis]
test@vMx6# set interface ge-0/0/2 level 1 disable

[edit protocols isis]
test@vMx6# set interface ge-0/0/2 level 2 metric 20

[edit protocols isis]
test@vMx6# exit

[edit]
test@vMx6# set interfaces ge-0/0/2 unit 0 family iso

[edit]
test@vMx6# ...terfaces lo0 unit 0 family iso address 49.0060.0600.6006.00
```

Figure 3.5-configuration IGP au sein des AS d'agrégation

Avec la commande (1) sur la figure 3.6 nous vérifions le bon établissement du protocole IS-IS.

```
[edit]
root@R6# run show isis adjacency
Interface             System         L State       Hold (secs) SNPA
ge-0/0/2.0            R7             2  Up                   20
```

Figure 3.6-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 3.7 et 3.8

```
root@R1# run ping 3.3.3.3 source 1.1.1.1
PING 3.3.3.3 (3.3.3.3): 56 data bytes
64 bytes from 3.3.3.3: icmp_seq=0 ttl=63 time=6.401 ms
64 bytes from 3.3.3.3: icmp_seq=1 ttl=63 time=3.784 ms
64 bytes from 3.3.3.3: icmp_seq=2 ttl=63 time=4.698 ms
64 bytes from 3.3.3.3: icmp_seq=3 ttl=63 time=3.571 ms
64 bytes from 3.3.3.3: icmp_seq=4 ttl=63 time=7.966 ms
64 bytes from 3.3.3.3: icmp_seq=5 ttl=63 time=6.060 ms
64 bytes from 3.3.3.3: icmp_seq=6 ttl=63 time=3.540 ms
```

Figure 3.7 : test Ping entre vMx1 et vMx5

```
root@R6# 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=4.191 ms
64 bytes from 7.7.7.7: icmp_seq=1 ttl=64 time=2.705 ms
64 bytes from 7.7.7.7: icmp_seq=2 ttl=64 time=2.362 ms
64 bytes from 7.7.7.7: icmp_seq=3 ttl=64 time=2.894 ms
64 bytes from 7.7.7.7: icmp_seq=4 ttl=64 time=2.397 ms
64 bytes from 7.7.7.7: icmp_seq=5 ttl=64 time=3.068 ms
64 bytes from 7.7.7.7: icmp_seq=6 ttl=64 time=7.303 ms
```

Figure 3.8 : test Ping entre vMx6 et vMx7

3.4 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 interface sortante de ces routeurs.

```
[edit]
test@vMx1# edit protocols mpls

[edit protocols mpls]
test@vMx1# set interface lo0

[edit protocols mpls]
test@vMx1# set interface ge-0/0/0

[edit protocols mpls]
test@vMx1# set interface ge-0/0/2

[edit protocols mpls]
test@vMx1# exit

[edit]
test@vMx1# set interfaces ge-0/0/0 unit 0 family mpls

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

Figure 3.9- configuration de l'mpls

3.4.1 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).

```
[edit]
test@vMx1# edit protocols ldp

[edit protocols ldp]
test@vMx1# set interface lo0

[edit protocols ldp]
test@vMx1# set interface ge-0/0/0

[edit protocols ldp]
test@vMx1# set interface ge-0/0/2

[edit protocols ldp]
test@vMx1# set track-igp-metric
```

Figure 3.10- configuration du LDP

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.

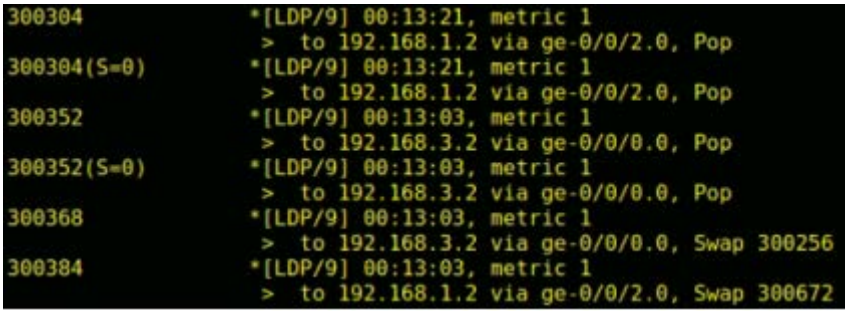


Figure 3.11- vérification de la distribution des labels

3.4.2 Configuration du RSVP-TE

Pour pouvoir créer des tunnels et mettre en œuvre l'ingénierie de trafic dans le réseau, nous devons activer le protocole RSVP dans les interfaces des routeurs de chaque AS avec les commandes (1-3) puis nous devons permettre à l'IGP d'offrir les informations de topologie au protocole RSVP, grâce à la commande (5). 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 créé entre les routeurs VMx1 et VMx5. Cette opération est faite à l'aide des commandes (6) et (7).

```
[edit]
root@R1# edit protocols rsvp

[edit protocols rsvp]
root@R1# set interface ge-0/0/0

[edit protocols rsvp]
root@R1# set interface ge-0/0/2

[edit protocols rsvp]
root@R1# exit

[edit]
root@R1# set protocols ospf traffic-engineering

[edit]
root@R1# set protocols mpls label-switched-path R1-to-R3 to 3.3.3.3

[edit]
root@R1# set protocols mpls label-switched-path R1-to-R5 to 5.5.5.5
```

Figure 3.12- configuration du RSVP-TE

Une fois les LSP crées, nous pouvons observer leur activation sur la figure 3.13 .

```
root@R1# 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 *                      R1-to-R3
5.5.5.5         1.1.1.1         Dn     0       -                R1-to-R5
Total 2 displayed, Up 1, Down 1
```

Figure 3.13-Activation des chemins LSP

3.4.3 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 (1). 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 (2-9). Pour cela, nous définissons des groupes BGP nommés internalpeers 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 (10) 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 résolve VPN pour stocker les routes étiquetées dans la table de routage inet.3.

```
[edit]
test@vMx1# set routing-options autonomous-system 64520

[edit]
test@vMx1# edit protocols bgp group internal-peers

[edit protocols bgp group internal-peers]
test@vMx1# set type internal

[edit protocols bgp group internal-peers]
test@vMx1# set local-address 1.1.1.1

[edit protocols bgp group internal-peers]
test@vMx1# set local-as 64520

[edit protocols bgp group internal-peers]
test@vMx1# set neighbor 2.2.2.2

[edit protocols bgp group internal-peers]
test@vMx1# set neighbor 3.3.3.3

[edit protocols bgp group internal-peers]
test@vMx1# set neighbor 4.4.4.4

[edit protocols bgp group internal-peers]
test@vMx1# set neighbor 5.5.5.5

[edit protocols bgp group internal-peers]
test@vMx1# set family inet labeled-unicast resolve-vpn
```

Figure 3.14- Configuration du BGP

Afin de configurer la connexion entre les AS, nous avons créé des groupes BGP nommés ebgp-peers via les commandes (1-5) 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]
test@vMx6# edit protocols bgp group ebgp-peers

[edit protocols bgp group ebgp-peers]
test@vMx6# set type external

[edit protocols bgp group ebgp-peers]
test@vMx6# set neighbor 192.168.6.1 peer-as 64520

[edit protocols bgp group ebgp-peers]
test@vMx6# set family inet labeled-unicast

[edit protocols bgp group ebgp-peers]
test@vMx6# set peer-as 64520
```

Figure 3.15-Configuration de la connexion entre Les AS

Enfin, nous spécifions les routes à exporter vers l'AS distant en créant dans chaque routeur une policy nommée export via la commande (1) puis nous lui indiquons l'adresse à exporter à partir de la commande (3) 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 (6).

```
[edit]
test@vMx1# edit policy-options policy-statement export

[edit policy-options policy-statement export]
test@vMx1# set term 1 from protocol direct

[edit policy-options policy-statement export]
test@vMx1# set term 1 from route-filter 1.1.1.1/32 exact

[edit policy-options policy-statement export]
test@vMx1# set term 1 then accept

[edit policy-options policy-statement export]
test@vMx1# exit

[edit]
test@vMx1# set protocols bgp export export
```

Figure 3.16- Création des policy

Grâce à la figure 3.17, nous confirmons la bonne connectivité entre les réseaux d'agrégation en effectuant le ping entre les routeurs vMx7 et vMx9.

```
[edit]
test@vMx7# run ping 9.9.9.9 source 7.7.7.7
PING 9.9.9.9 (9.9.9.9): 56 data bytes
64 bytes from 9.9.9.9: icmp_seq=0 ttl=60 time=53.521 ms
64 bytes from 9.9.9.9: icmp_seq=1 ttl=60 time=7.191 ms
64 bytes from 9.9.9.9: icmp_seq=2 ttl=60 time=7.496 ms
64 bytes from 9.9.9.9: icmp_seq=3 ttl=60 time=282.075 ms
64 bytes from 9.9.9.9: icmp_seq=4 ttl=60 time=6.382 ms
```

Figure 3.17-Test ping entre VMx7 et VMx9

La visualisation de la table de routage inet.0 illustrée dans la figure 3.18 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 *.

```
6.6.6.6/32          *[BGP/170] 00:06:30, localpref 100, from 8.8.8.8
                      AS path: 64520 64530 I, validation-state: unverified
                    >  to 192.168.9.1 via ge-0/0/0.0, Push 299984
7.7.7.7/32          *[BGP/170] 00:06:30, localpref 100, from 8.8.8.8
                      AS path: 64520 64530 I, validation-state: unverified
                    >  to 192.168.9.1 via ge-0/0/0.0, Push 300000
8.8.8.8/32          *[IS-IS/15] 00:06:30, metric 10
                    >  to 192.168.9.1 via ge-0/0/0.0
                     [BGP/170] 00:06:30, localpref 100, from 8.8.8.8
                      AS path: I, validation-state: unverified
                    >  to 192.168.9.1 via ge-0/0/0.0
9.9.9.9/32          *[Direct/0] 00:28:38
                    >  via lo0.0
```

Figure 3.18-Table de routage inet.0 du nœud Vmx9

3.4.4 Création des VPN

3.4.4.1 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 câble 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 (1) 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 (2).

```
[edit]
test@vMx7# set protocols l2circuit neighbor 9.9.9.9 interface ge-0/0/0 enca...

[edit]
test@vMx7# set interfaces ge-0/0/0 encapsulation ethernet-ccc
```

Figure 3.19-configuration du VPNL2

La figure 3.20, obtenue grâce à la commande (1) nous confirme le bon établissement du tunnel. Nous testons le ping entre les PC des clients et le résultat est affiché dans la figure 3.21

```
root@vMX-VCP7> show l2circuit connections brief
Layer-2 Circuit Connections:

Legend for connection status (St)
EI -- encapsulation invalid      NP -- interface h/w not present
MM -- mtu mismatch               Dn -- down
EM -- encapsulation mismatch     VC-Dn -- Virtual circuit Down
CM -- control-word mismatch      Up -- operational
VM -- vlan id mismatch           CF -- Call admission control failure
OL -- no outgoing label          IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC    TM -- TDM misconfiguration
BK -- Backup Connection          ST -- Standby Connection
CB -- rcvd cell-bundle size bad  SP -- Static Pseudowire
LD -- local site signaled down   RS -- remote site standby
RD -- remote site signaled down  HS -- Hot-standby Connection
XX -- unknown

Legend for interface status
Up -- operational
Dn -- down
Neighbor: 9.9.9.9
    Interface                 Type  St     Time last up          # Up trans
    ge-0/0/0.0(vc 1)          rmt   Up     Oct 28 09:19:27 2021           1
```

Figure 3.20 Établissement de L2vpn

```
VPCS> ping 172.168.3.2

84 bytes from 172.168.3.2 icmp_seq=1 ttl=64 time=6.313 ms
84 bytes from 172.168.3.2 icmp_seq=2 ttl=64 time=5.892 ms
84 bytes from 172.168.3.2 icmp_seq=3 ttl=64 time=6.066 ms
^C
```

Figure3.21-test ping entre client 1 et client 2

3.4.4.2 Établissement d'un Layer 3 VPN

Un L3VPN est créé 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 :

1. Création des tables VRF : Cette table est créé avec les commandes (1-4) 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 (5) 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 (7)

3. Configuration des Policy-options : Cette étape se traduit par la définition de deux politiques exports et import via les commandes (1-5) et (1-5) 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).

```
[edit]
test@vMx7# edit routing-instances l3vpn

[edit routing-instances l3vpn]
test@vMx7# set instance-type vrf

[edit routing-instances l3vpn]
test@vMx7# set interface ge-0/0/1

[edit routing-instances l3vpn]
test@vMx7# set route-distinguisher 7.7.7.7:123

[edit routing-instances l3vpn]
test@vMx7# set vrf-table-label

[edit routing-instances l3vpn]
test@vMx7# exit

[edit]
test@vMx7# set protocols bgp family inet-vpn unicast
```

Figure 3.21-Activation d'un L3vpn

```
[edit]
test@vMx7# edit policy-options policy-statement l3vpn-export

[edit policy-options policy-statement l3vpn-export]
test@vMx7# set term 1 from protocol direct

[edit policy-options policy-statement l3vpn-export]
test@vMx7# set term 1 from community l3vpn-rt

[edit policy-options policy-statement l3vpn-export]
test@vMx7# set term 1 then accept

[edit policy-options policy-statement l3vpn-export]
test@vMx7# set term deny then reject

[edit policy-options policy-statement l3vpn-export]
test@vMx7# exit
```

Figure 3.22-Activation d'un L3vpn

```
[edit]
test@vMx7# edit policy-options policy-statement l3vpn-import

[edit policy-options policy-statement l3vpn-import]
test@vMx7# set term 1 from protocol bgp

[edit policy-options policy-statement l3vpn-import]
test@vMx7# set term 1 from community l3vpn-rt

[edit policy-options policy-statement l3vpn-import]
test@vMx7# set term 1 then accept

[edit policy-options policy-statement l3vpn-import]
test@vMx7# set term deny then reject

[edit policy-options policy-statement l3vpn-import]
test@vMx7# exit

[edit]
test@vMx7# set routing-instances l3vpn vrf-import l3vpn-export

[edit]
test@vMx7# set routing-instances l3vpn vrf-import l3vpn-import
```

Figure 3.23-Activation d'un L3vpn

Les résultats de la figure 3.24 exécuté sur vMx7 nous montrent le succès de la configuration.

```
test@vMx7> show route table bgp.l3vpn.0

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
                   *[BGP/170] 22:19:47, 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 26
```

Figure 3.24-Etablisement de L3vpn

Nous testons le ping entre les PC des clients et le résultat est affiché dans la figure 3.25

```
VPCS> ping 172.168.2.2

84 bytes from 172.168.2.2 icmp_seq=1 ttl=58 time=23.616 ms
84 bytes from 172.168.2.2 icmp_seq=2 ttl=58 time=6.522 ms
84 bytes from 172.168.2.2 icmp_seq=3 ttl=58 time=8.696 ms
84 bytes from 172.168.2.2 icmp_seq=4 ttl=58 time=6.579 ms
84 bytes from 172.168.2.2 icmp_seq=5 ttl=58 time=7.102 ms
```

Figure 3.25 ping entre client 3 et 4

3.5 Configuration du Segment Routing

3.5.1 Migration de l'OSPF vers ISIS

Une migration du protocole OSPF vers IS-IS dans l'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 3.0.5.2 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 3.26 qu'il dispose des mêmes entrées que le protocole OSPF et qu'il pointe vers la même interface de sortie.

```
3.3.3.3/32          *[Direct/0] 6w5d 10:07:03
                     > via lo0.0
4.4.4.4/32          *[OSPF/10] 6w5d 01:21:17, metric 1
                     > to 10.0.0.18 via ge-0/0/2.0
                     [IS-IS/18] 01:01:00, metric 40
                     > to 10.0.0.18 via ge-0/0/2.0
                     [BGP/170] 6w1d 01:52:01, localpref 100, from 4.4.4.4
                       AS path: I, validation-state: unverified
                     > to 10.0.0.18 via ge-0/0/2.0
5.5.5.5/32          *[OSPF/10] 6w5d 01:20:35, metric 2
                     > to 10.0.0.18 via ge-0/0/2.0
                     [IS-IS/18] 01:01:00, metric 60
                     > to 10.0.0.18 via ge-0/0/2.0
```

Figure 3.26- Vérification des entrées et sorties d'OSPF et IS-IS

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 3.27.

3.5.2 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 SRGB. Pour cela, on utilise la commande (1), 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 nœud avec les commandes (2-4).

```
test@vMx1> show route table inet.0

inet.0: 18 destinations, 22 routes (18 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1.1.1.1/32          *[Direct/0] 23:14:42
                     >  via lo0.0
2.2.2.2/32          *[IS-IS/18] 23:04:04, metric 20
                     >  to 192.168.1.2 via ge-0/0/2.0
                     [BGP/170] 23:03:58, localpref 100, from 2.2.2.2
                       AS path: I, validation-state: unverified
                     >  to 192.168.1.2 via ge-0/0/2.0
                        to 192.168.3.2 via ge-0/0/0.0, Push 16200, Push 16300(top)
3.3.3.3/32          *[IS-IS/18] 23:03:37, metric 40
                     >  to 192.168.1.2 via ge-0/0/2.0
                     [BGP/170] 23:03:26, localpref 100, from 3.3.3.3
                       AS path: I, validation-state: unverified
                     >  to 192.168.1.2 via ge-0/0/2.0, Push 16300
                        to 192.168.3.2 via ge-0/0/0.0, Push 16300
4.4.4.4/32          *[IS-IS/18] 23:03:36, metric 20
                     >  to 192.168.3.2 via ge-0/0/0.0
                     [BGP/170] 23:03:32, localpref 100, from 4.4.4.4
                       AS path: I, validation-state: unverified
```

Figure 3.27-Table de routage après la migration vers IS-IS

```
[edit]
test@vMx1# set chassis network-services enhanced-ip

[edit]
test@vMx1# edit protocols isis source-packet-routing

[edit protocols isis source-packet-routing]
test@vMx1# set srgb start-label 16000 index-range 4000

[edit protocols isis source-packet-routing]
test@vMx1# set node-segment ipv4-index 100
```

Figure 3.28-configuration des paramètre SR

Sur la figure 3.29 nous pouvons observer les informations relatives à la bonne configuration du SR.

```
test@vMx1> show isis overview
Instance: master
  Router ID: 1.1.1.1
  Hostname: vMx1
  Sysid: 0010.0100.1001
  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: Enabled
    Max labels: 3, Max spf: 100, Max Ecmp Backup: 2
```

Figure 3.29-Detail de la configuration du SR

Avec commande (1) illustrés dans la figure 3.30 nous permettent de constater que les ADJ-SID ont été allouées dynamiquement pour chaque voisin IS-IS.

D'après la table mpls.0 illustrée sur la figure 3.31 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

```
test@vMx1> show isis adjacency detail
vMx4
  Interface: ge-0/0/0.0, Level: 2, State: Up, Expires in 24 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 23:18:21 ago
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 192.168.3.2
  Level 2 IPv4 Adj-SID: 17

vMx2
  Interface: ge-0/0/2.0, Level: 2, State: Up, Expires in 23 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 23:18:49 ago
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 192.168.1.2
  Level 2 IPv4 Adj-SID: 16
```

Figure 3.30-Distribution dynamique Adj-SID

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 3.31-Coexistance des protocoles IS-IS et LDP

Protocole L-ISIS, nous désactivons LDP du réseau à l'aide de la commande **dasactivate protocol ldp** . Une nouvelle constatation de la table mpls.0 confirme les modifications apportées (figure 3.32).

```
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 3.32-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 trace route illustrés dans les figures 3.33 et 3.34 respectivement, où nous pouvons voir que le label utilisé est celui du SR.

```
test@vMx1> ping mpls segment-routing isis 5.5.5.5
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

Figure 3.33-Test de connectivité

```
test@vMx1> 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 3.34-Trace de route SR

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

3.5.3 Configuration des applications SR

3.5.3.1 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 (1) et (2).

```
[edit]
test@vMx1# ...ocols isis interface ge-0/0/0 level 2 post-convergence-lfa

[edit]
test@vMx1# set protocols isis interface ge-0/0/2 level 2 post-convergence-l...

[edit]
test@vMx1# run show isis database vMx1 level 2 extensive
```

Figure 3.35- Configuration de TI-LFA

La confirmation de cette application se fait via la commande (3) et les résultats apparaissent sur la figure 3.36 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.

```
LAN IPV4 Adj-SID -, Flags:0x70(F:0,B:1,V:1,L:1,S:0,P:0), Weight:0
   Neighbor:vMx2, Label:16
LAN IPv4 Adj-SID:      16, Weight:   0, Neighbor: vMx2, Flags: -BVL--
```

Figure 3.36- Activation de TI-LFA

3.5.3.2 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 (1) nous déterminons la valeur de discriminateur de chaque routeur et la durée de détection des messages S-BFD.

```
[edit]
test@vMx1# set protocols bfd sbfd local-discriminator 999 minimum-receive-i...

[edit]
test@vMx1# run show bfd seamless session
```

Figure 3.37-configuration du SBFD

La vérification de la bonne activation de ce mécanisme se fait via la commande (1) et est illustré sur la figure 3.38 .

```
root@vMx9# run show bfd seamless session
                                                          Receive
Type     Descriminator  Table      Address          State    Interval
Local              999    default  0.0.0.0          Up       1.000

1 local sessions, 0 remote sessions
```

Figure 3.38- Activation BFD sur VMx9

3.5.3.3 Activation d'ECMP

Le partage des charges est configuré au niveau de chaque routeur avec la commande (1). Les routeurs peuvent prendre en charge [N] chemin de sauvegarde ECMP, en cas de liaison défectueuse. De ce fait lorsque le lien principal tombe en panne, le trafic sera équilibré sur les N autres nœuds.

```
[edit]
test@vMx1# set protocols isis backup-spf-options use-post-convergence-lfa m...

[edit]
test@vMx1# run show isis overview | match backup
```

Figure 3.39-configuration d'ECMP

Sur la figure 3.40 nous pouvons voir les différents chemins de sauvegardes créés en utilisant la commande (1).

3.5.3.4 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

```
test@vMx1> show isis overview | match backup
  Post Convergence Backup: Enabled
    Max labels: 3, Max spf: 100, Max Ecmp Backup: 2
```

Figure 3.40-Disponibilité d'ECMP

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 interfaces des routeurs qui utilisent le L2VPN. A noter que le SR reste le protocole préféré à côté du LDP pour les opérations de transfert d'étiquettes. La figure 3.41 démontre l'activation du L2VPN avec l'utilisation des labels SR.

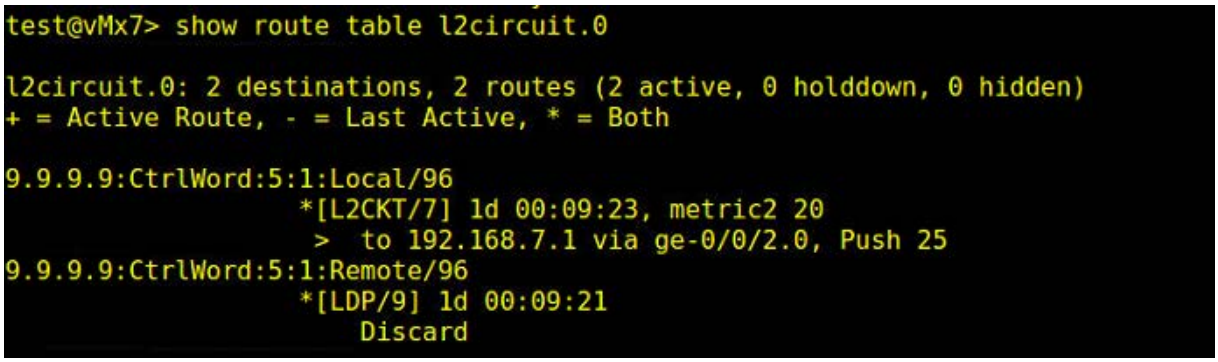


Figure 3.41-Activation de SR-L2VPN

3.6 Configuration du contrôleur SDN

Dans cette section, nous abordons la configuration du contrôleur NorthStar dans le réseau pour permettre le Traffic Engineering 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.

3.6.1 Contrôleur 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.

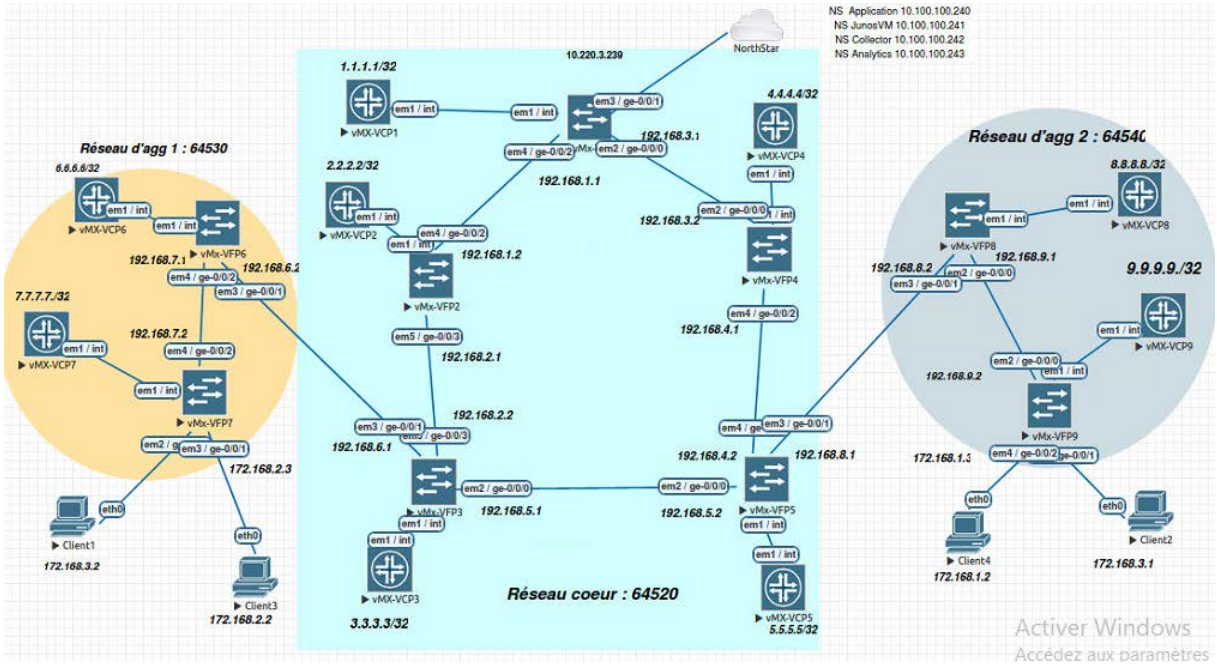


Figure 3.42-Topologie du réseau après introduction de contrôleur

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 tests 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 à la gestion du réseau via le protocole SNMP ou SSH. — Analytics : Fourni les statistiques nécessaires pour la visibilité du réseau.

3.6.2 Connexion du contrôleur au réseau

Pour connecter le réseau au contrôleur, nous configurons au niveau du routeur vMx1 des routes statiques pour chaque module cité en destination du contrôleur via les commandes (1-5).

```
[edit]
test@vMx1# edit routing-options static

[edit routing-options static]
test@vMx1# set route 10.100.100.240/32 next-hop 192.168.200.1

[edit routing-options static]
test@vMx1# set route 10.100.100.241/32 next-hop 192.168.200.1

[edit routing-options static]
test@vMx1# set route 10.100.100.242/32 next-hop 192.168.200.1

[edit routing-options static]
test@vMx1# set route 10.100.100.243/32 next-hop 192.168.200.1
```

Figure 3.43- Configuration de la connexion du réseau au contrôleur

Une fois les routes statiques établies, nous configurons 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. Nous utilisons la commande (1) pour le déploiement de ce protocole.

— SSH : Pour établir une connexion sécurisée et à distance entre le contrôleur et les routeurs du réseau. La configuration de cette session ce fait par le biais de la commande (2).

— NETCONF : Pour fournir un moyen de gestion, de configuration et d'installation d'une nouvelle configuration des périphériques réseau. Nous le mettons en place via la commande (3).

```
[edit]
test@vMx1# set snmp community northstar authorization read-only

[edit]
test@vMx1# set system services ssh

[edit]
test@vMx1# set system services netconf ssh

[edit]
test@vMx1# set system services netconf ssh
```

Figure 3.44-Configuration du SNMP, SSH et NETCONF

La disponibilité de ces protocoles est vérifiée sur la figure 3.45

Device	IP Address	Management IP	Type	Ping	SSH	SNMP	NETCONF
vMx5	5.5.5.5	5.5.5.5	JUNIPER	✓	✓	✓	✓
vMx1	1.1.1.1	1.1.1.1	JUNIPER	✓	✓	✓	✓
vMx2	2.2.2.2	2.2.2.2	JUNIPER	✓	✓	✓	✓
vMx3	3.3.3.3	3.3.3.3	JUNIPER	✓	✓	✓	✓
vMx4	4.4.4.4	4.4.4.4	JUNIPER	✓	✓	✓	✓
vMx6	6.6.6.6	6.6.6.6	JUNIPER	✓	✓	✓	✓
vMx7	7.7.7.7	7.7.7.7	JUNIPER	✓	✓	✓	✓

Figure 3.45-Activation des protocole sur le contrôleur

3.6.3 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 (1-5). 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 déléguer 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 calcul de chemin externe pour les LSP-TE d'un PCC avec la commande (7).

```
[edit protocols pcep pce northstar]
test@vMx1# set local-address 1.1.1.1

[edit protocols pcep pce northstar]
test@vMx1# set destination-ipv4-address 10.100.100.240

[edit protocols pcep pce northstar]
test@vMx1# set destination-port 4189

[edit protocols pcep pce northstar]
test@vMx1# set pce-type active stateful

[edit protocols pcep pce northstar]
test@vMx1# set spring-capability

[edit protocols pcep pce northstar]
test@vMx1# exit

[edit]
test@vMx1# set protocols mpls lsp-external-controller pccd
```

Figure 3.46-Configuration du PCE

3.6.4 Configuration du BGP-LS

Après avoir établi avec succès une connexion entre le contrôleur et le réseau nous pouvons passer 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 (1). 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 utilisé 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 (8-10). Nous ajoutons par la suite la configuration des commandes (11-13) 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 (15). Enfin nous annonçons les routes au contrôleur via la commande (16).

```
[edit]
test@vMx1# edit protocols bgp group northstar

[edit protocols bgp group northstar]
test@vMx1# set type internal

[edit protocols bgp group northstar]
test@vMx1# set local-address 1.1.1.1

[edit protocols bgp group northstar]
test@vMx1# set family traffic-engineering unicast

[edit protocols bgp group northstar]
test@vMx1# set local-as 10000

[edit protocols bgp group northstar]
test@vMx1# set neighbor 10.100.100.241

[edit protocols bgp group northstar]
test@vMx1# exit

[edit]
test@vMx1# edit protocols bgp group ebgp-peers

[edit protocols bgp group ebgp-peers]
test@vMx1# set neighbor 192.168.8.2 egress-te-node-segment label 1046666

[edit protocols bgp group ebgp-peers]
test@vMx1# set neighbor 192.168.8.2 egress-te
```

Figure 3.47-Configuration du BGP-LS

```
[edit]
test@vMx1# edit policy-options policy-statement export-bgp-ls

[edit policy-options policy-statement export-bgp-ls]
test@vMx1# set term 1 from family traffic-engineering

[edit policy-options policy-statement export-bgp-ls]
test@vMx1# set term 1 then accept

[edit policy-options policy-statement export-bgp-ls]
test@vMx1# exit

[edit]
test@vMx1# ...fic-engineering database import policy export-bgp-ls

[edit]
test@vMx1# set protocols bgp group northstar export export-bgp-ls
```

Figure 3.48- Suite de la configuration du BGP-LS

Sur l'interface du contrôleur NorthStar illustrée dans la figure 3.49 nous pouvons constater qu'il a acquis la topologie de notre réseau avec succès sur laquelle sont affichés 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 3.50, 3.51 et 3.52 respectivement où nous pouvons constater leurs activations.

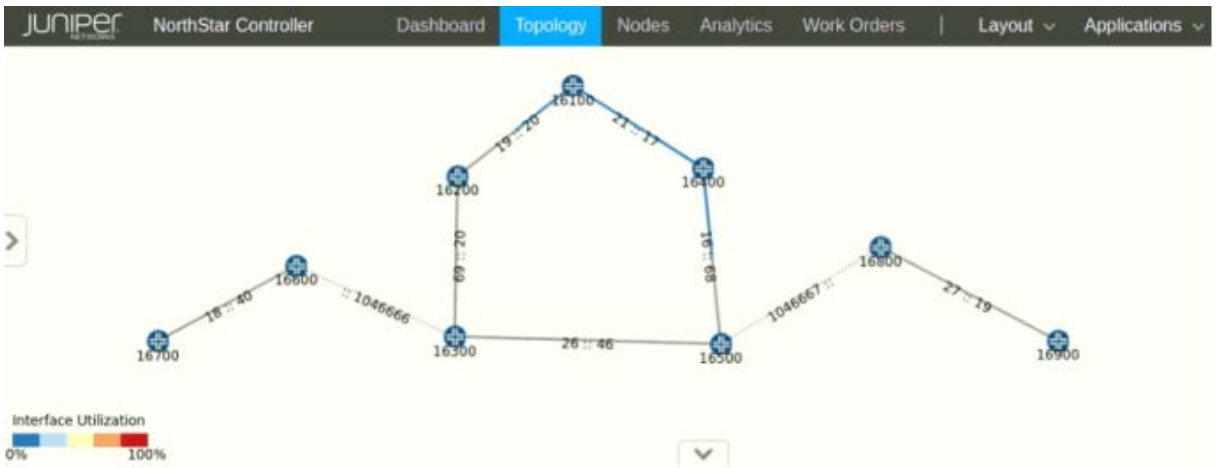


Figure 3.49-Topologie importé par le contrôleur

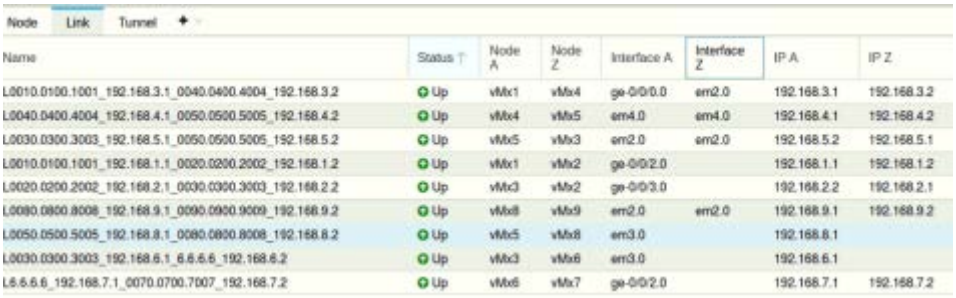
Node | Link | Tunnel

Hostname	IP Address	Type	NETCONF Status	PCEP Status	PRPD Status	AS	ISIS Area	Management IP	Layer
vMx1	1.1.1.1	JUNIPER	Up	Up		64520	49	1.1.1.1	IP
vMx2	2.2.2.2	JUNIPER	Up			64520	49	2.2.2.2	IP
vMx3	3.3.3.3	JUNIPER	Up			64520	49	3.3.3.3	IP
vMx4	4.4.4.4	JUNIPER	Up			64520	49	4.4.4.4	IP
vMx5	5.5.5.5	JUNIPER	Up			64520	49	5.5.5.5	IP
vMx6	6.6.6.6	JUNIPER	Up			64530	49	6.6.6.6	IP
vMx7	7.7.7.7	JUNIPER	Up			64530	49	7.7.7.7	IP
vMx8	8.8.8.8	JUNIPER	Up			64540	49	8.8.8.8	IP
vMx9	9.9.9.9	JUNIPER	Up			64540	49	9.9.9.9	IP

Figure 3.50-Activation des nœud importé par le contrôleur

3.6.5 Ingénierie du trafic avec NorthStar

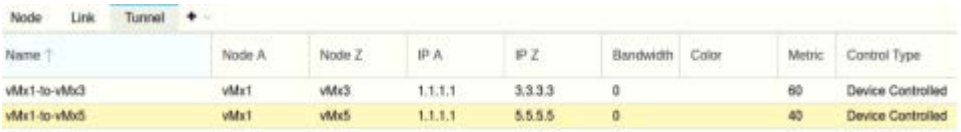
Nous finalisons la configuration du Segment Routing par la configuration du Traffic Engineering avec SR uniquement et cela depuis le contrôleur. Pour cette étape nous créons deux



Node | Link | Tunnel

Name	Status	Node A	Node Z	Interface A	Interface Z	IP A	IP Z
L0010.0100.1001_192.168.3.1_0040.0400.4004_192.168.3.2	Up	vMx1	vMx4	ge-0/0/0.0	em2.0	192.168.3.1	192.168.3.2
L0040.0400.4004_192.168.4.1_0050.0500.5005_192.168.4.2	Up	vMx4	vMx5	em4.0	em4.0	192.168.4.1	192.168.4.2
L0030.0300.3003_192.168.5.1_0050.0500.5005_192.168.5.2	Up	vMx5	vMx3	em2.0	em2.0	192.168.5.2	192.168.5.1
L0010.0100.1001_192.168.1.1_0020.0200.2002_192.168.1.2	Up	vMx1	vMx2	ge-0/0/2.0		192.168.1.1	192.168.1.2
L0020.0200.2002_192.168.2.1_0030.0300.3003_192.168.2.2	Up	vMx3	vMx2	ge-0/0/3.0		192.168.2.2	192.168.2.1
L0080.0800.8008_192.168.9.1_0090.0900.9009_192.168.9.2	Up	vMx8	vMx9	em2.0	em2.0	192.168.9.1	192.168.9.2
L0050.0500.5005_192.168.8.1_0080.0800.8008_192.168.8.2	Up	vMx5	vMx8	em3.0		192.168.8.1	
L0030.0300.3003_192.168.6.1_6.6.6.6_192.168.6.2	Up	vMx3	vMx6	em3.0		192.168.6.1	
L6.6.6.6_192.168.7.1_0070.0700.7007_192.168.7.2	Up	vMx6	vMx7	ge-0/0/2.0		192.168.7.1	192.168.7.2

Figure 3.51-Activation des liens importé par le contrôleur



Node | Link | Tunnel

Name	Node A	Node Z	IP A	IP Z	Bandwidth	Color	Metric	Control Type
vMx1-to-vMx3	vMx1	vMx3	1.1.1.1	3.3.3.3	0		60	Device Controlled
vMx1-to-vMx5	vMx1	vMx5	1.1.1.1	5.5.5.5	0		40	Device Controlled

Figure 3.52-Activation des tunnels TE importée par le contrôleur

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 créés sont affichés sur la figure 3.53 identifiés par le type SR.

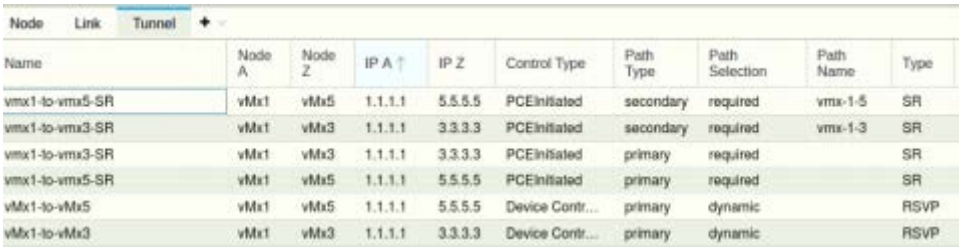


Figure 3.53-Affichage des tunnels SR

Avec la table de routage inet.3 qui stocke les routes IP de vMx1 illustrées sur la figure 4.33 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 **delete protocol mpls label-switched-path** et laisser uniquement ceux créés avec le SR.

3.7 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

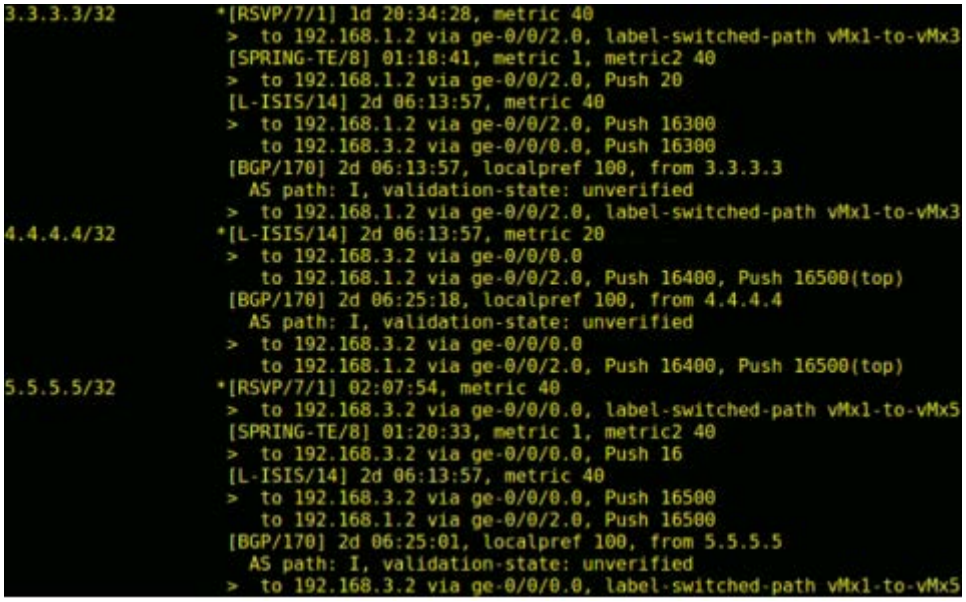


Figure 3.54-Visualisation de la tabale inet.3 VMx1

Du SR avec le contrôleur 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.

3.7.1 RPM

Junos RPM permet aux administrateurs réseau de mesurer les paramètres de performance entre deux points de terminaison du réseau. Pour collecter des statistiques réseaux, 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.

3.7.2 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.

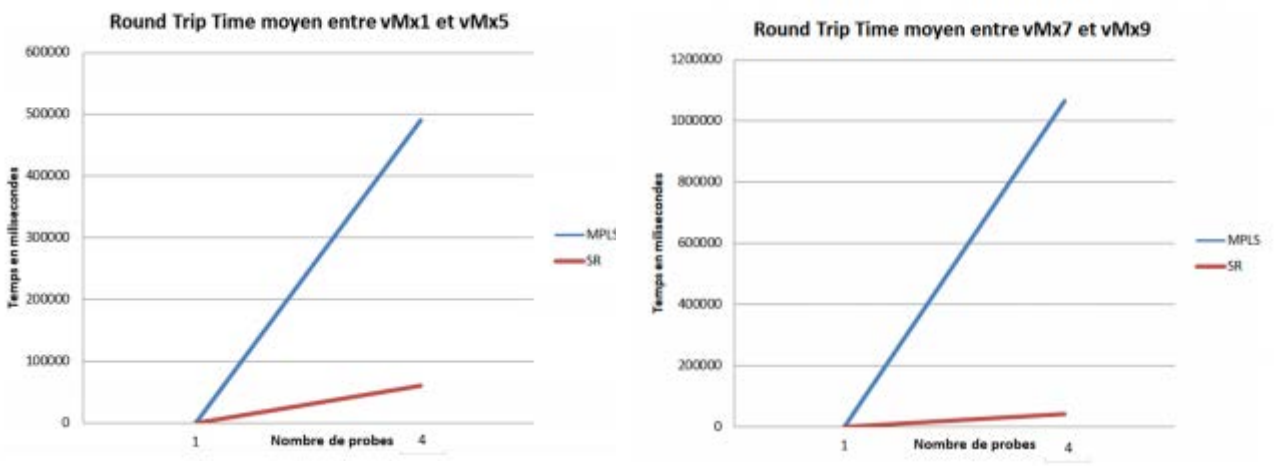
```
[edit]
test@vMx1# edit services rpm probe p1 test t1

[edit services rpm probe p1 test t1]
test@vMx1# set probe-type icmp-ping

[edit services rpm probe p1 test t1]
test@vMx1# set target address 5.5.5.5

[edit services rpm probe p1 test t1]
test@vMx1# set probe-count 4

[edit services rpm probe p1 test t1]
test@vMx1# set probe-interval 5

[edit services rpm probe p1 test t1]
test@vMx1# set test-interval 300

[edit services rpm probe p1 test t1]
test@vMx1# set source-address 1.1.1.1
```

Figure 3.55- Le code du test RPM entre VMX1 et VMx 5

3.7.3 Résultats

3.7.3.1 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 03-56 : Résultats de RTT moyen

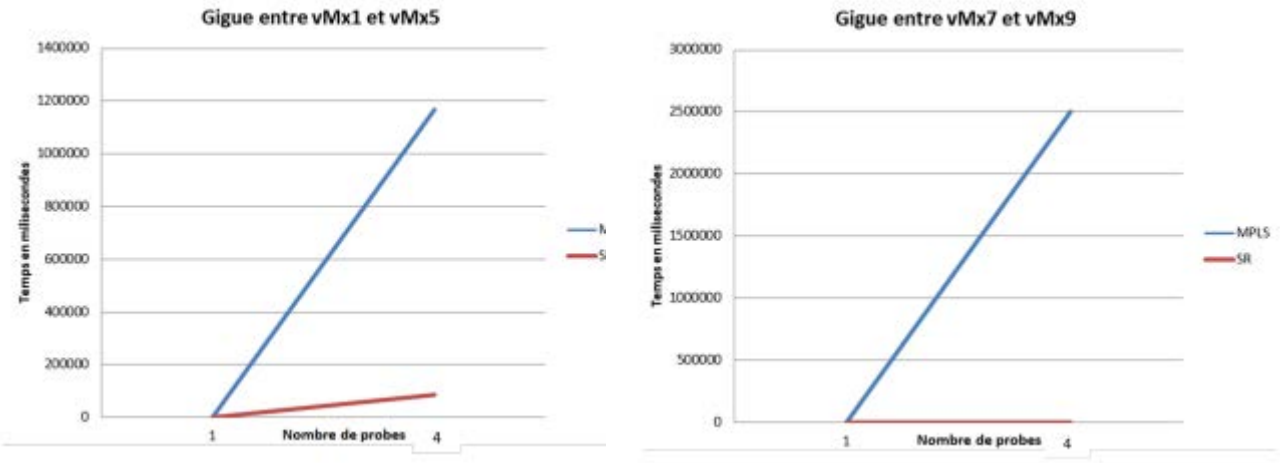
Les résultats du RTT moyen illustrés dans les graphes de la figure 4.34 affichent que entre les routeurs du réseau coeur vMx1 et vMx5 qu'en MPLS et avec le RSVP-TE le temps du RTT moyen était de 490535 usec puis après la migration vers le SR et en le combinant avec le contrôleur SDN on a obtenu 61334 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.

3.7.3.2 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'implémentation 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 03-57 : 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 4.35 affichent qu'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.

3.8 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 tels que TI-LFA, SBFD et ECMP. Nous avons également vu la mise en place du contrôleur qui nous a permis 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

Conclusion générale et perspectives

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 Seg-ment Routing, qui permet de répondre aux nouvelles contraintes et de remédier aux inconvé-nients 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. 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.

Référence bibliographique

Référence chapitre 1 :

[1] : Pujolle, G. « les reseaux » , 6eme Edition, Edition Eyrolles, 2008.

[2] : Luc De Ghein. “MPLS Fundamentals”. In : CCIE No.1897.CISCO (2013).

[3] : [M.Taklit], implementation du sdn dans une structure ip/mpls, université de tiziouzou 2018

[4] : D. Seret D. Dromard. “Architecture des réseaux.Apprendre, toujours”. In : Pearson (2013).

[5] : http://www.abdelhamid-djeffal.net/web_documents/diaposroutage.pdf

[6] M. Kadoch et Université du Québec. École de technologie supérieure. “Pro-tocoles et réseaux locaux : l’accès Internet”. In : PUQ (2012)

[7]: https://www.frameip.com/mpls/

[8] http://igm.univ-mlv.fr/~dr/XPOSE2006/marot/architecture.html

[9] [R.Berkani], Etude et simulation d’un reseau Ip/MPLS sous GNS3,université de Tiziouzou

[10] [A.Grine], « Etude, conception et implementation du Segment Routing sur un réseau IP/MPLS ». Université de boumerdes 2019

[10] : [Amine GRINE et Radia BOURAIB, étude, conception et implémentation du SR sur un réseau IP/MPLS, université de M’HAMED NOUGARA DE BOUMERDES en 2019/2020]

[11] Rabah guedrez, enabling traffic engineering over segment Routing, l’école Nationale supérieure Mines-Telecom atlantique, France le 12/12/2018.

[12] : Livre blanc de l’ONF, « SDN architecture », 2014.

[13] David Culler, Jonathan Hui, JP Vasseur, and Vishwas Manral. An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL). RFC 6554, October 2015.

[14] : [I-D.ietf-pce-segment-Routing]

[15] : C. Filsfils et al. “Segment Routing Architecture”. In : RFC 8402, Internet Engineering Task Force (2018).

[16] : ACG_Segment_Routing_201808.pdf

[17] : [https://orhanergun.net/segment-routing-and-mpls-vpn/]

[18] : [www.cisco.com]

[19] : Guy Pujolle. Les réseaux. Eyrolles, 9 edition, 2018.

[20] : https://www.juniper.net/fr/fr/research-topics/what-is-segment-routing.html

[21] : Livre blanc de ONF, « Software-Defined networking : The New Norm for Networks », 2012

[22] : [www.juniper.net]

[23] : [Reference https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/reseau-internet-protocoles-multicast-routage-mpls-et-mobilite-42289210/segment-routing-te7594/segment-routing-mpls-sr-mpls-te7594niv10002.html]

ANNEXES

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