REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Département Ingénierie des Systèmes Électriques

Mémoire de Master

Présenté par

ASKLOU Yamina

BOUGUERRA Hadjer

Filière : Télécommunication

Spécialité : Réseaux et Télécommunication

Implémentation d'une solution Segment Routing sur un environnement basé MPLS/SDN

Soutenu le 13/07/2022 devant le jury composé de :

HAROUNE	Radia	MAA	UMBB	Président
SEDJELMACI	Ibtecem	MCB	UMBB	Examinateur
MECHID	Samira	MAA	UMBB	Promotrice

Année Universitaire : 2022/2023

Remérciment

Louange à Dieu le tout puissant de nous avoir permis d’achever ce modeste travail.

Nous souhaitons adresser nos remerciements les plus sincères à **Mme.Samira mechid,** pour avoir accepter de nous encadrer. Nous la remercions pour son soutien et la confiance dont elle a fait preuve à notre égard, pour la qualité de son encadrement tant sur le plan scientifique qu’humain.

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

Il nous est impossible d'oublier **Mr. Belaid Kamel** Chacun a son temps qui nous est imparti et ses conseils et son soutien constant f Ses importantes contributions ont fait de ce travail ce qu'il est aujourd'hui.

Pour finir, nous remercions toute l’équipe IP/MPLS et toute personne ayant contribué de prés ou de loin à la réalisation de ce travail.

Dédicace

Avec un grand plaisir que je dédie ce modeste travail

À ma mère, pour son amour, ses encouragements et ces sacrifices, à mon père pour son soutien, son affection et la confiance qu'il m'a accordé, à mes chères frères et soeurs qui sont la source de mon bonheur je leur dédie tout mon amour.

À ma chère grand mère parti trop tôt avant de me voir réussir que dieu l'aceuille dans son vaste paradis.

À tout mes amis qui m'ont soutenu durant tous mon parcours et excptionnellement Sabrina,Sérine, Omar et Yamina

Pour finir je voudrais remercier ma binome Hadjer pour son travail je lui souhaite un avenir Glorieux.

Yamina

Dédicace

À ma mère,

Que je fasse ou que je dise, je ne saurai jamais assez te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

À mon père,

Tu as toujours été à mes côtés pour me soutenir et m'encourager. Que ce travail traduise mon affection envers toi.

À mon frère,

Je suis très heureuse d'être ta sœur. Tu es le meilleur, ma petite sœur Safa et ma grand-mère.

À mes amies Rayal, Fella, Ikrame, ma binôme Yamina et toutes les personnes dans ma vie, que mon idée soit sans oublier mon camarade Omar, je vous remercie sincèrement.

Que Dieu vous donne santé, bonheur et le paradis.

Hadjer

Table des matières

Liste des abréviations

AS	Autonomous System
API	Application Programming Interface
BGP	Border Gateway Protocol
CE	Customer edge
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EFVI	European Telecommunications Standards Institute
FEC	Forwarding Equivalence Class
IETF	Internet Engineering Task Force
IEC	International Electrotechnical Commission
IGRP	Interior Gateway Routing Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISG	Industry Specification Group
ISIS	Intermediate System to Intermediate System
ISO	International Organization for Standardization
LDP	Label Distribution Protocol
LER	Label Edge Router
LSA	Link-State Advertisement
LSP	Link-State Path
LSR	Link-State Router
MPLS	Multiprotocol Label Switching

NBI	Northbound Interface
NFV	Network Function Virtualisation
NFVI	Network Function Virtualisation Infrastructure
OF	OpenFlow
ONF	Open Networking Foundation
OSI	Open Systems Interconnection Model
OSPF	Open Shortest Path First
OVSBD	Open vSwitch DataBase
PCC	Path Computation Client
PCE	Path Computation Element
PCEP	Path Computation Element Protocol
PE	Provider Edge
QOS	Quality Of Service
RSVP	Resource Reservation Protocol
RIP	Routing Information Protocol
SDN	Software Defined Network
SID	Segment Identifier
SPF	Shortest Path First
SR	Segment Routing
SRGP	Segment Routing Global Block
SRLP	Segment Routing Local Block
TCP	Transmission Control Protocol
TE	Traffic Engineering
TED	Traffic Engineering Database

TLS	Transport Layer Security
VNF	Virtualised Network Function
VPN	Virtual Private Network

Liste des figures

Liste des tableaux

Résumé

Les fournisseurs IT prévoient d'offrir une variété croissante de services en informatiques pour ses clients avec l'évolution rapide de télécommunication. Les technologies qui supportent actuellement les réseaux IP/MPLS n'ont cependant pas les propriétés de flexibilité et d'évolutivité nécessaires pour réaliser une telle évolution. En revanche, une nouvelle approche s'est introduite pour optimiser la gestion de ces réseaux, qui le SDN en séparant le contrôle du trafic d'acheminement, mais ceci n'a pas pu poursuivre le développement massif de la technologie en termes d'acheminement de trafic.

Dans ce document, nous présentons le routage par segment , une nouvelle architecture de réseau qui vise à répondre à cette lacune où il met en œuvre les concepts de routage et de tunneling à la source, en permettant aux nœuds de diriger les paquets sur des chemins en utilisant une séquence d'instructions (segments) placée dans l'en-tête du paquet sans entrée par flux au niveau des routeurs intermédiaires.

Ce travail présente la mise en œuvre de la solution routage par segment sous le réseau MPLS/SDN dans un environnement virtualisé.

Mots clés : Routage par segment, MPLS, SDN, OpenDayLight.

Abstract

IT providers intend to offer an increasing variety of IT services for these customers with the rapid evolution of telecommunications. The technologies that currently support IP/MPLS networks, however, do not have the flexibility and scalability properties necessary to realize such an evolution. On the other hand, a new approach has been introduced to optimize the management of these networks, namely SDN which separates the control from the routing traffic, but this has not been able to pursue the massive development of the technology in terms of traffic routing.

In this document, we present Segment-based routing, a new network architecture that aims to address this lack where it implements the concepts of routing and tunneling at the source, allowing nodes to direct packets along paths using a sequence of instructions (segments) placed in the packet header without entering the flow at the intermediate routers.

This work presents the implementation of the segment-based routing solution under MPLS/SDN in a virtualized environment.
Key words : Segment routing, MPLS, SDN, OpenDayLight

Introduction Générale

Pendant les trois dernières décennies, les méthodes de communication et d'échange d'informations dans les réseaux informatiques ont connu une évolution considérable, grâce aux avancées rapides des solutions informatiques, notamment l'émergence de la technologie Internet Protocol (IP). Cependant, cette croissance a également suscité des préoccupations quant à la gestion efficace et aux performances de l'acheminement du trafic dans les réseaux informatiques.

Bien que les réseaux IP répondent généralement aux besoins des applications et des utilisateurs actuels, certains éléments posent fréquemment des problèmes pour un ensemble d'applications de plus en plus vaste.

L'architecture de base des réseaux informatiques n'a pas subi de changements majeurs. Cependant, avec les exigences croissantes en matière d'évolutivité et de flexibilité des réseaux modernes, les approches traditionnelles de mise en réseau, où les appareils prennent des décisions de routage indépendantes en exécutant plusieurs protocoles distribués, sont devenues un obstacle à l'innovation et à la croissance de l'industrie. Ces approches limitent la capacité d'adaptation et entravent le progrès dans le secteur.

Les professionnels de l'ingénierie, de la recherche et des fournisseurs de technologies de l'information travaillent sur le développement de nouvelles techniques, architectures et protocoles pour répondre aux besoins croissants de routage. Parmi ces avancées, la technologie de commutation multiprotocole par étiquette (MPLS) est utilisée. Elle combine à la fois de nouvelles techniques et les techniques de routage IP existantes afin d'améliorer les performances d'acheminement du trafic.

Le protocole MPLS est utilisé pour acheminer le trafic via des chemins commutés par étiquettes (LSP), ce qui permet d'améliorer et de résoudre les problèmes existants. Cependant, en raison de la complexité croissante du réseau, une gestion plus efficace et plus robuste est nécessaire.

Parmi les nouvelles approches, le Réseau Défini par Logiciel (SDN) est apparu, permettant de séparer le contrôle de l'acheminement du trafic. Cela optimise le réseau,

le rend plus flexible et renforce la sécurité. Bien que les performances aient été améliorées, les exigences en termes d'acheminement n'ont pas été entièrement satisfaites.

Une solution plus récente, actuellement en cours d'étude, vise à optimiser, simplifier et améliorer l'évolutivité des réseaux MPLS/SDN, et elle est appelée "routage par segment".

Il s'agit d'un nouveau paradigme qui repose sur un modèle de routage basé sur la source. Dans ce modèle, un nœud du réseau guide un paquet en fonction d'une liste d'instructions contenues dans l'en-tête du paquet, appelées "segments". Chaque liste de segment est identifiée par un ID unique appelé Segment ID (SID), tandis que le contrôle reste au niveau du SDN.

Parmi les nombreux fournisseurs, Ericsson Algérie, l'un des principaux fournisseurs de technologies de l'information et de la communication (TIC) pour les fournisseurs de services, a choisi cette solution. Ils nous ont proposé cette solution pour notre projet de fin d'études.

Notre projet est donc structuré en trois chapitres principaux: Dans le premier, nous décrirons les protocoles de routages et le protocole MPLS du point de vue théorique et nous parlerons sur le concept fondamental de la solution routage par segment. Le deuxième chapitre présente la nouvelle approche NFV et SDN. Le troisième chapitre sera consacré à l’implémentation de la solution proposée sous GNS3 et les simulations associées qui les valident.

Chapitre 1

1.1 Introduction

Le routage est un processus crucial dans le fonctionnement efficace de l'Internet. Il consiste à acheminer les paquets de données du centre de données vers les périphériques finaux à travers un réseau complexe. Cependant, les protocoles de routage traditionnels présentent certains problèmes, tels qu'un en-tête IP volumineux, une vitesse de routage plus lente que la commutation et une conception axée sur le chemin le plus court sans prendre en compte d'autres métriques.

C'est là qu'intervient MPLS (Multi-Protocol Label Switching), un protocole qui permet de résoudre ces problèmes. Avec MPLS, les paquets sont acheminés en utilisant des étiquettes plutôt que de nécessiter des recherches complexes dans une table de routage à chaque saut. Il gère également les flux de trafic à différentes granularités et prend en charge différents protocoles.

Dans ce contexte, il est important de comprendre les protocoles de routage existants et comment MPLS résout les problématiques mentionnées précédemment. Le chapitre abordera donc les notions de routage, les différents protocoles de routage, ensuite sur le protocole MPLS et MPLS-TE et puis nous verrons la nouvelle technique de routage qui est le routage par segment.

1.2 Le routeur

Un routeur est un élément intermédiaire essentiel dans un réseau informatique. Sa principale fonction est de faire transiter les paquets de données d'une interface réseau vers une autre en se basant sur une table de routage. Il opère à la couche 3 des modèles OSI et TCP/IP, connue sous le nom de couche réseau. Les routeurs assurent l'acheminement des paquets en utilisant des adresses IP, permettant ainsi la connectivité entre les différents réseaux, qu'ils soient locaux ou étendus [26].

1.3 Les modèles d'interconnexion d'un réseau

OSI et TCP/IP sont des modèles de références. Il s'agit de modèles architecturaux standard qui sont souvent utilisés pour décrire une pile de protocoles de réseau.

Modèle OSI

Le modèle OSI, abréviation de "Open Systems Interconnection Model", est un cadre

conceptuel utilisé pour décrire les différentes fonctions d'un système de mise en réseau. Ce modèle propose une architecture hiérarchique qui organise de manière logique les différentes tâches nécessaires à la communication entre systèmes. Il est composé de sept couches distinctes, chacune ayant des responsabilités et des fonctionnalités spécifiques [31].

Modèle TCP/IP

Le modèle TCP/IP est une version simplifiée du modèle OSI, se composant de seulement quatre couches : liaison, Internet, transport et application. La principale différence réside dans la fusion de certaines couches. Par exemple, dans TCP/IP, la couche liaison regroupe les couches physiques et liaison du modèle OSI. De même, la couche application de TCP/IP combine les couches session, application et présentation du modèle OSI [32].

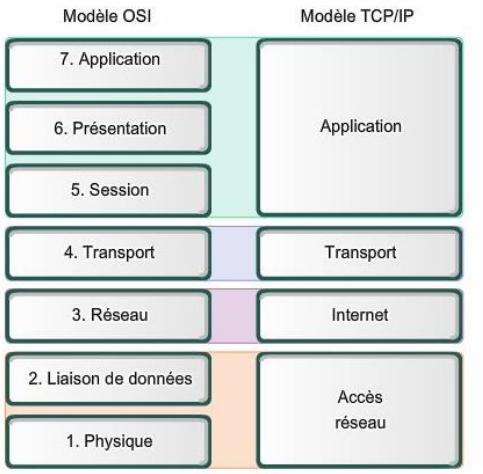


Figure 1.1 : Le modèle OSI et TCP/IP [32].

1.4 Le routage

Le routage est le mécanisme effectué par les routeurs pour acheminer les données d'un réseau jusqu'à un ou plusieurs destinataires en choisissant le meilleur chemin comme le montre la figure 1.2, par un algorithme selon une norme qui est la métrique qui lui sera présentée dans une table appelée table de routage [1].

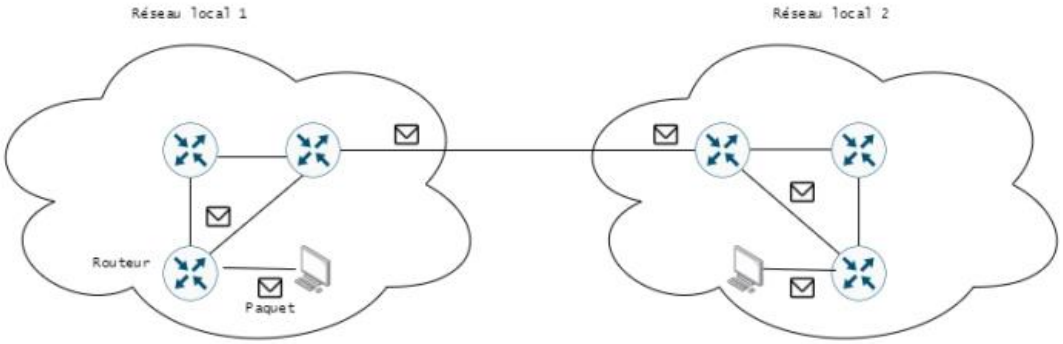


Figure 1.2 : Routage [1].

La métrique

Lorsqu'il s'agit de déterminer le meilleur itinéraire pour acheminer le trafic réseau, les algorithmes de routage utilisent des métriques pour effectuer ce calcul. Les métriques sont assignées à chaque itinéraire disponible dans la table de routage et sont calculées à l'aide de diverses techniques et méthodes basées sur les algorithmes de routage utilisés. Plusieurs paramètres sont pris en compte lors du calcul d'une métrique de routage, tels que le nombre de sauts, la fiabilité du chemin et la bande passante disponible [23].

Table de routage

Une table de routage est un ensemble de règles, représentées sous forme de tableau, qui permet de déterminer où seront acheminé les paquets de données circulant sur un réseau IP [2] qui diffère d'un protocole à l'autre en fonction de l'algorithme utilisé, où chaque ligne ou entrée de la table indique la meilleure route vers le réseau de destination souhaité, soit via une interface, soit avec une adresse du prochain saut avec la métrique (voir le tableau 1.1), puis chaque route dépend de l'algorithme utilisé, elles sont divisées en trois types : statique, dynamique et par défaut [1].

Réseau de destination	Masque réseau	Adresse passerelle	Interface	Métrique (le saut suivant/ le cout)
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.10.0	255.255.255.0	192.168.10.2	192.168.10.6	1

Tableau 1.1 : Table de routage.

Routage statique

Le routage statique est une approche simple qui ne nécessite aucune modification des tables de routage à moins qu'un administrateur réseau ne le modifie manuellement. Les paquets suivent le chemin spécifié. Si il y a changement dans le réseau la route ne sera pas modifiée, sauf si quelqu'un la corrige manuellement ce qui est le seul moyen de détourner le trafic. Cette approche est facile à mettre en œuvre et ne nécessite pas de protocoles de routage complexes [3].

Routage dynamique

Le routage dynamique est une technique de routage avancée qui vérifie les mises à jour du routage entrant et modifie les informations de routage en fonction de l'évolution des conditions du réseau telles que les ruptures de liens pannes, les changements de trafic et les changements de coût. Lorsqu'un changement se produit dans le réseau, il est envoyé aux routeurs pour indiquer ce changement, et la route est ensuite recalculée et envoyée en tant que nouvelle mise à jour de routage pour construire une connaissance commune du réseau. Le routage dynamique est meilleur que le routage statique car le routeur se met à jour avec tout changement dans le réseau, il offre donc une certaine robustesse contre les pannes [3].

Routage par défaut

Une route par défaut ou une passerelle de dernier recours peut être considérée comme un type spécial de route statique. La différence entre eux est que la route par défaut utilise le routeur s'il n'y a pas d'autres routes connues dans la table de routage jusqu'à réseau de destination. Leur destination étant inconnue, le routage par défaut permet de les envoyer à une seule adresse de saut suivant. La route par défaut dans IPv4 est désignée 0.0.0.0/0 ou simplement 0/0. En outre, dans IPv6, la route par défaut est spécifiée comme : :/0[1][4].

1.4.1 Protocoles de routage

Les routeurs utilisent des protocoles de routage pour gérer dynamiquement les informations reçues depuis leurs propres interfaces et depuis d'autres routeurs. Les protocoles de routage peuvent être également configurés pour gérer les routes entrées manuellement. Un protocole de routage dynamique prend connaissance de toutes les

routes disponibles. Il insère les meilleures routes dans la table de routage et supprime celles qui ne sont plus valides ce qui rend l'acheminement des paquets plus facile et plus rapide. Le procédé qu'utilise un protocole de routage pour déterminer la meilleure route vers un réseau de destination s'appelle un algorithme de routage [5].

Les protocoles de routage sont divisés en deux familles, Protocole de Passerelle Intérieure (IGP) et Protocole de Passerelle Extérieure (EGP) (figure 1.3).

1.4.1.1 IGP

Le protocole IGP est utilisé pour acheminer le trafic au sein de chaque réseau séparé d'un système autonome AS. Il est également connu sous le nom de "routage intra-AS". Les entreprises, les organisations et même les fournisseurs de services utilisent le protocole IGP sur leurs réseaux internes. Chaque AS possède un seul IGP. Différents systèmes autonomes peuvent utiliser différents IGP. Il existe deux types d'IGP : le routage à vecteur de distance tel que le Protocole d'Information de Routage (RIP), le Protocole de Routage de Passerelle Intérieure (IGRP) et Protocole de Routage de Passerelle Intérieure Améliorée (EIGRP) et le routage à état de liaison tel que le protocole Ouvrir le Chemin le Plus court en Premier (OSPF) et Système Intermédiaire à Système Intermédiaire (IS-IS) [1][6].

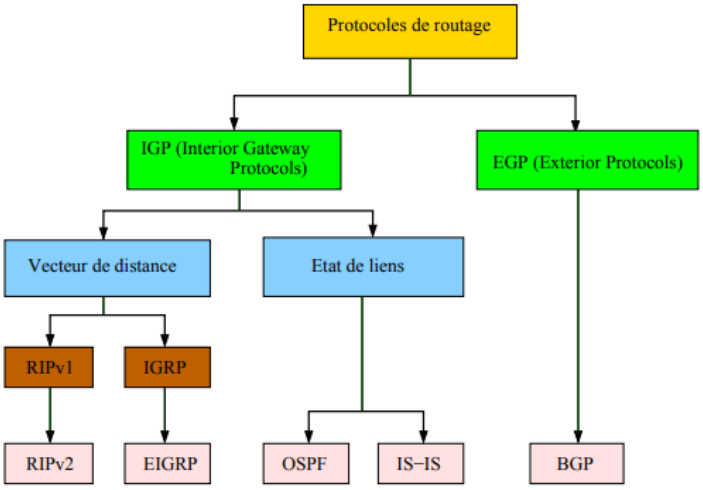


Figure 1.3 : Classification des protocoles de routage [8].

Les systèmes autonomes

Dans l'architecture hiérarchique d'Internet, les routeurs sont organisés de manière hiérarchique. Les domaines présents dans Internet sont formés par des ensembles de systèmes autonomes (AS), également connus sous le nom de "Autonomous System". Un système autonome est un réseau ou un groupe de réseaux placé sous une seule autorité administrative de routage. Au sein de leur domaine, les systèmes autonomes utilisent des protocoles de routage internes de type IGP tels que OSPF (Open Shortest Path First) ou IS-IS (Intermediate System to Intermediate System) [14].

Le protocole de routage à vecteur de distance, également connu sous le nom de Bellman-Ford, implique que chaque routeur échange des informations avec ses voisins concernant la topologie de son réseau, y compris les liens et les interfaces, ainsi que la métrique pour atteindre un nœud en passant par ces voisins. Ces échanges d'informations se font via la table de routage. L'objectif est de choisir la métrique la plus faible entre deux routeurs et de l'ajouter à leur table de routage. Cette approche permet un échange rapide d'informations et une mise à jour efficace des tables de routage, avec une complexité de calcul et une charge de messages minimales par rapport à une autre méthode.

- **RIP**

Le RIP (Routing Information Protocol) est un protocole de routage IP de type vecteur distance basé sur l'algorithme de routage décentralisé Bellman-Ford. Défini par l'Internet Engineering Task Force (IETF), il existe une première version dans le RFC 1058 et une seconde version dans le RFC 245. Son objectif est de permettre à chaque routeur de partager la métrique, c'est-à-dire la distance en termes de sauts, qui les sépare des réseaux IP. Lorsqu'un routeur reçoit un message RIP, il incrémente la distance de 1 et transmet ce message aux routeurs directement accessibles. Cette approche permet aux routeurs de maintenir la route optimale en stockant l'adresse du prochain routeur dans leur table de routage, afin de minimiser le nombre de sauts nécessaires pour at teindre un réseau donné [7].

Le RIP est généralement utilisé dans les petits réseaux homogènes car il est facile à configurer. Il perm et aux routeurs de conserver la route optimale en échangeant des

informations sur les distances vers les réseaux, facilitant ainsi la détermination des chemins optimaux pour le routage des messages [7].

- **IGRP**

L'IGRP (Interior Gateway Routing Protocol) est un protocole à vecteur de distance développé par Cisco, conçu pour fonctionner exclusivement sur leurs équipements. Il est utilisé par les routeurs pour échanger les informations de leurs tables de routage au sein d'un système autonome (AS) [8].

- **EIGRP**

L'EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage à vecteur de distance amélioré et propriétaire développé par Cisco. Il a été créé pour répondre au besoin d'un protocole offrant une convergence plus rapide, une sélection de routes optimisée et des capacités avancées de calcul de routes. De plus, il permet également de collecter des informations provenant des périphériques voisins [1].

Dans le cas du protocole de routage à l'état de liens, les routeurs échangent des informations avec leurs voisins afin de déterminer le meilleur chemin. Les protocoles

à l'état de liens prennent en compte des caractéristiques telles que la vitesse, le coût et la congestion actuelle de chaque route pour déterminer le chemin optimal. Dans cette méthode, chaque nœud reçoit une vue de la connectivité du réseau, puis calcule de manière autonome le meilleur saut suivant pour chaque destination possible dans le réseau. La collection de ces meilleurs sauts suivants forme la table de routage du nœud. Les informations sur l'état des liens sont transmises uniquement lorsqu'il y a des changements dans le réseau. Ainsi, les mises à jour de la table de routage sont effectuées de manière sélective et ne nécessitent pas une transmission continue d'informations sur l'état des liens.

- **OSPF**

L'OSPF (Open Shortest Path First) est un protocole de routage à état de lien non propriétaire développé par l'IETF. Contrairement à RIP, il n'utilise pas le concept de "nombre de sauts" pour établir la métrique, mais plutôt celui de "coût des routes". La première version de l'OSPF a été spécifiée dans le RFC 1131, suivie de la seconde

version dans le RFC 2328. Dans les réseaux OSPF, les routeurs échangent des annonces d'état de liens (LSA) pour partager des informations sur le réseau local au sein du système autonome. Ces routeurs prennent ensuite des décisions de routage en se basant sur l'algorithme link-state, également connu sous le nom d'algorithme du Chemin le Plus court en Premier (SPF), qui calcule le chemin le plus court entre les nœuds en utilisa nt un arbre répertoriant les chemins les plus courts de la source à la destination [5][9].

Comparé au protocole RIP, l'OSPF présente de nombreux avantages significatifs. Il offre une convergence plus rapide et s'adapte mieux aux réseaux de plus grande taille. Ces caractéristiques en font un choix privilégié pour les environnements réseau nécessitant une meilleure performance et une évolutivité accrue [5][9].

Les LSAs (Link-State Advertisements) transmis contiennent des informations sur les interfaces connectées et les métriques de routage d'un routeur. Chaque routeur utilise ces informations pour calculer le chemin le moins coûteux vers chaque réseau et construire une table de routage pour le protocole, en se basant uniquement sur l'adresse IP de destination présente dans l'en-tête du paquet IP. Les paquets IP sont acheminés sans être encapsulés dans d'autres en-têtes de protocole lorsqu'ils traversent le système autonome (AS). L'OSPF se distingue par sa capacité à détecter rapidement les changements topologiques au sein du système autonome, tels que les pannes d'interfaces de routeur. Il calcule de nouvelles routes sans boucle après une période de convergence courte et implique un trafic de routage minimal [27].

- **IS-IS**

Le protocole IS-IS (Intermediate System to Intermediate System) est un protocole à état de liens qui fonctionne de manière similaire à OSPF. Il est défini dans la norme internationale ISO/IEC 10589:2002 de l'Open Systems Interconnection (OSI). Les routeurs IS-IS maintiennent une vue topologique commune et construisent individuellement une base de données topologique, qui est ensuite partagée entre tous les routeurs. Les paquets sont acheminés en suivant le chemin le plus court. L'algorithme SPF (Shortest Path First) est utilisé pour calculer les routes [10].

1.4.1.2 EGP

Les EGPs sont des protocoles utilisés pour le routage entre des systèmes autonomes, également appelé "routage inter-SA". Parmi ces protocoles, le Border Gateway Protocol (BGP) est actuellement le seul protocole EGP largement utilisé et reconnu. Il est considéré comme le protocole de routage officiel d'Internet et a été défini par l'IETF dans le RFC 1105 [11].

Le protocole BGP (Border Gateway Protocol) est utilisé pour le routage entre systèmes autonomes dans le réseau Internet. Il permet l'échange d'informations de routage sous la forme de séquences de numéros d'AS, indiquant les AS à traverser pour atteindre une destination. BGP est un protocole robuste et scalable, avec des tables de routage BGP du réseau Internet comprenant plus de 90 000 routes. Sa scalabilité est rendue possible grâce à l'utilisation d'attributs associés aux routes, permettant de définir des politiques de routage entre les systèmes autonomes [14].

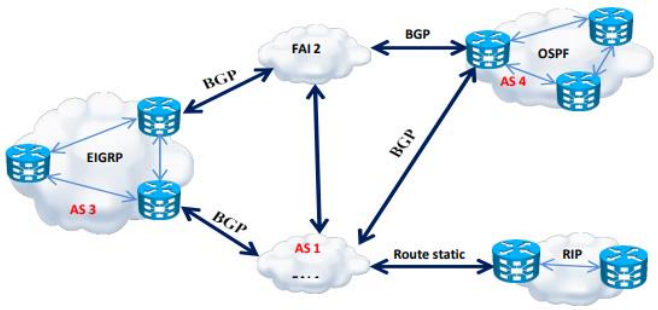


Figure 1.4 : Protocoles de routage IGP et EGP [19].

Au niveau des réseaux étendus, d'autres protocoles sont apparus afin d'acheminer les paquets avec les meilleures performances, dont, le plus répandu le MPLS où nous allons le présenter dans ce qui suit.

1.4 MPLS

MPLS (Multiprotocol Label Switching) est une technique réseau qui combine les concepts du routage IP de niveau 3 avec les mécanismes de commutation de niveau 2. Elle est définie par l'IETF dans le RFC 3031 et se caractérise par sa simplicité, sa modularité et son efficacité. Bien que les efforts de l'IETF se concentrent

principalement sur IPv4, la technique MPLS peut être étendue à différents protocoles tels que IPv6. L'objectif de MPLS est d'améliorer le rapport performance/prix des équipements de routage, d'optimiser l'efficacité du routage, en particulier dans les grands réseaux, et d'enrichir les services de routage. Grâce à la commutation de labels, de nouveaux services peuvent être déployés sans nécessiter de modifications au niveau du cœur du réseau. MPLS n'est pas limité à une couche 2 spécifique et peut être utilisé sur différents types de supports permettant l'acheminement de paquets de niveau 3 [12].

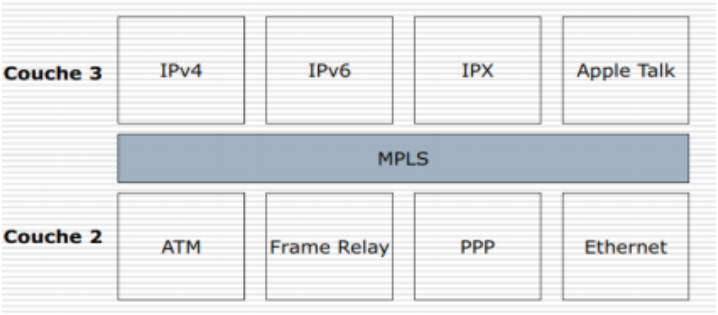


Figure 1.5 : Emplacement du MPLS entre les couches 2 et 3 [19].

1.5.1 Principe de MPLS

MPLS est un mécanisme de transport de données qui repose sur la commutation d'étiquettes. Ces étiquettes sont ajoutées à l'entrée du réseau MPLS et retirées à la sortie IP. Cette technologie permet de diriger et de transporter efficacement des données entre les différents nœuds du réseau, indépendamment de leur emplacement et de leur distance. Contrairement aux réseaux traditionnels, les en-têtes des paquets sont modifiés uniquement par les routeurs aux extrémités du réseau, plutôt qu'à chaque saut, ce qui accélère la transmission des données. De plus, MPLS offre un niveau de sécurité supplémentaire lors de la transmission des paquets [43].

Actuellement, MPLS offre bien plus que des avantages de commutation rapide. Il permet également de fournir une gamme de services tels que les réseaux privés virtuels (VPN) et l'ingénierie du trafic (TE), qui ne sont pas réalisables sur les infrastructures IP traditionnelles [13].

Lable

Dans le cadre de MPLS, un label, également appelé étiquette, est représenté par un nombre entier de 20 bits. Il est inséré entre les en-têtes de la couche 2 et de la couche 3 (IP) du modèle OSI [44].

Position dans l'en-tête

L'en-tête MPLS est positionné entre les entités des couches 2 et 3 du modèle OSI. L'en-tête de la couche 2 représente le protocole de liaison utilisé, tandis que l'en-tête de la couche 3 est l'en-tête IP. L'en-tête MPLS lui-même est composé de quatre champs distincts [19], comme illustré dans la figure ci-dessous :

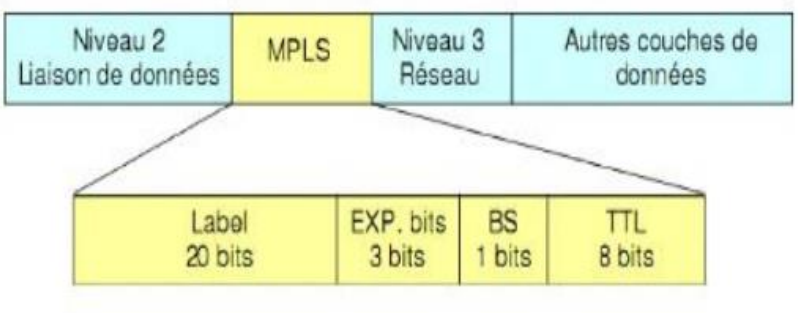


Figure 1.6 : En-tête MPLS [19].

La signification des différents champs est comme suit [19] :

- **Le champ (Label) :** sert à identifier le numéro du label, il est sur 20bits
- **Le champ (EXP) :** Champ expérimental utilisé pour porter la précédence IP, ou bien définir une classe de service (Qualité de Service), il est codé sur 3bits.
- **Le champ (BS) :** c'est un champ qui est codé sur 1bit, il indique l'empilement des labels et il est à 1 lorsque le label se trouve au sommet de la pile juste avant l'entête IP, sinon il est à 0.
- **Le champ (TTL) :**il représente la durée de vie des paquets TTL (Time to Live), et il est codé sur 8 bits.

Où les opérations effectuées sur Label sont [18] :

• Push : Il s'agit de l'ajout d'étiquettes. Cette opération est réalisée par les nœuds d'entrée et de transit d'un réseau MPLS. Lorsqu'un paquet IP atteint l'entrée d'un

réseau MPLS, une étiquette est ajoutée entre l'en-tête de la couche 2 et l'en-tête de la couche 3 du paquet avant de le transmettre. Selon les besoins, un nœud de transit à l'intérieur du réseau MPLS peut également ajouter une étiquette supplémentaire en haut de la pile d'étiquettes.

• Swap : Il s'agit du remplacement d'étiquette. Cette opération est effectuée par un nœud de transit pour remplacer l'étiquette supérieure de la pile d'étiquettes d'un paquet MPLS par une autre étiquette. Cette nouvelle étiquette est attribuée par le saut suivant dans le chemin de transmission.

• Pop : Il s'agit du retrait d'étiquette. Cette opération est réalisée par le nœud de sortie pour enlever l'étiquette du paquet MPLS. Dans certains cas, l'avant-dernier LSR peut également exécuter cette opération afin de réduire le nombre d'étiquettes dans la pile d'étiquettes.

Forwarding equivalence class (FEC) est un groupe ou un flux de paquets qui sont transmis le long du même chemin et sont traités de la même manière en ce qui concerne le traitement de transmission. Tous les paquets appartenant à la même FEC ont la même étiquette [16].

Dans certaines situations, comme l'équilibrage de charge, un Flux d'Équivalence de Transfert (FEC) peut être associé à plusieurs étiquettes d'entrée. Cependant, chaque étiquette ne représente qu'un seul FEC sur un appareil. Dans certaines applications telles que le VPN MPLS, il peut y avoir une pile d'étiquettes MPLS organisées selon la règle du dernier entré, premier sorti. Les étiquettes sont traitées à partir du haut de la pile. Dans la Figure 1.6, l'étiquette adjacente à l'en-tête de la couche 2 est en haut de la pile d'étiquettes (étiquette MPLS externe), tandis que l'étiquette adjacente à l'en-tête de la couche 3 est en bas de la pile d'étiquettes (étiquette MPLS interne). Une pile d'étiquettes MPLS peut contenir un nombre illimité d'étiquettes [42].

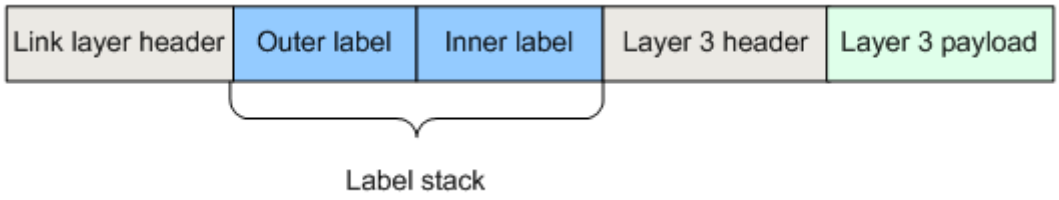


Figure 1.7 : Pile d'étiquettes [42].

- **LSR (Label Switch Router)**

Le routeur LSR, également connu sous le nom d'équipement de cœur MPLS, joue un rôle essentiel dans le réseau MPLS en effectuant la commutation des labels et en participant à l'établissement du chemin emprunté par les paquets. Lorsqu'un routeur LSR reçoit un paquet étiqueté, il procède à l'échange du label d'entrée avec un autre label de sortie approprié, puis il transmet le paquet ainsi étiqueté vers l'interface de sortie correspondante [13].

Le routeur LSR, peut jouer plusieurs rôles à savoir :

- l'échange d'informations de routage.
- l'échange des labels.
- l'acheminement des paquets.

- **Un routeur de bord d'étiquette (LER)**

Un routeur de bord d'étiquette, connu sous le nom de Provider Edge Router (LER), est un type de LSR situé à la périphérie d'un réseau MPLS et connecté à d'autres réseaux en tant que point d'accès au réseau MPLS. Les LER peuvent être équipés de plusieurs ports permettant de se connecter à différents réseaux distincts, chacun pouvant utiliser sa propre méthode de commutation. Les LER jouent un rôle essentiel dans la mise en place et la gestion des étiquettes dans le contexte du réseau MPLS. Il existe généralement deux types de LER [28] :

Ingress-LER (Ingress Label Edge Router)

Le routeur de bord d'étiquette (LER) est positionné à l'entrée du réseau MPLS et joue le rôle de point d'entrée pour les flux provenant du réseau du client. Dans ce routeur, des étiquettes sont assignées aux flux provenant du réseau du client [28].

Egress-LER (Egress Label Edge Router)

Il réalise le contraire de l'Ingress-LER et ce, en supprimant les étiquettes des paquets venant du cœur du réseau MPLS [28].

- **LSP (Label Switching Path)**

Un Label Switched Path (LSP) est un chemin unidirectionnel et point à point à travers le réseau MPLS. Pour établir un LSP, on peut utiliser différents protocoles de signalisation tels que LDP, RSVP ou BGP. Le chemin d'un LSP débute au niveau d'un routeur de fournisseur d'entrée (PE), qui prend une décision sur l'étiquette à ajouter à un paquet en fonction de la classe d'équivalence de transfert (FEC) appropriée [17].

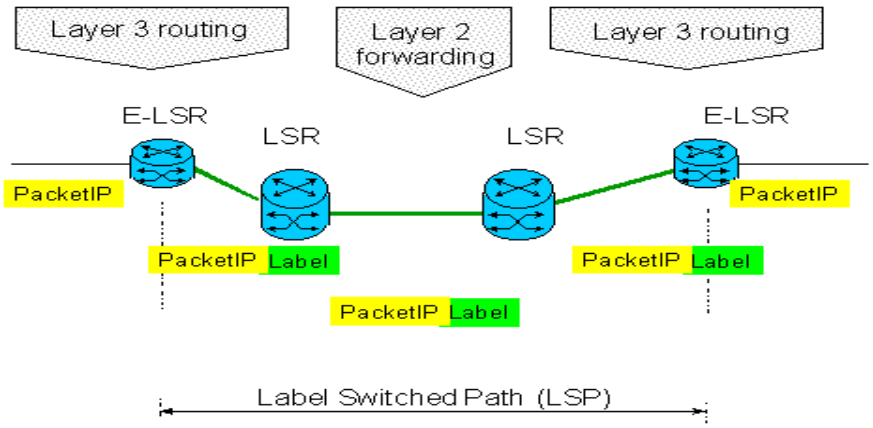


Figure 1.8 : Principe de MPLS [46].

1.5.2 Protocoles de signalisations

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 LDP et RSVP.

1.5.2.1 LDP

Chaque classe d'équivalence de transfert (FEC) se voit attribuer un label, et cette attribution peut être effectuée de manière manuelle, mais cela n'est réaliste que pour un nombre très restreint de FEC. Une approche plus pratique consiste à utiliser le protocole de distribution de labels LDP (Label Distribution Protocol).

LDP définit un ensemble de procédures et de messages utilisés par les LSR pour échanger des informations sur la correspondance entre les labels et les flux. Ce protocole a été initialement publié dans la RFC 3036 de l'IETF. Une connexion LDP

peut être établie directement entre deux LSR ou indirectement via des LSR intermédiaires. [19].

1.5.2.2 RSVP

Le protocole RSVP était utilisé pour réserver les ressources des flux IP à travers un réseau en échangeant des messages. Cependant, une version étendue de ce protocole a été développée pour prendre en charge les tunnels de chemin à commutation d'étiquettes (LSP), ce qui permet à RSVP d'être utilisé pour la distribution des étiquettes MPLS [21].

RSVP est un protocole indépendant de la couche IP et utilise des datagrammes IP (ou UDP aux limites du réseau) pour la communication entre les routeurs LSR. Contrairement aux connexions TCP, RSVP ne nécessite pas de maintenir une connexion continue, mais doit pouvoir gérer la perte de messages de contrôle. Le protocole RSVP a été étendu dans le contexte de MPLS, créant RSVP-TE, comme spécifié dans la RFC 3209 de l'IETF [21].

1.5.3 Les applications de la technologie MPLS

En plus de la rapidité, MPLS apporte plusieurs services, on peut citer l'ingénierie du trafic (TE), les réseaux privés virtuels (VPN), la qualité de service (QoS).

Ingénierie du trafic (TE)

L'ingénierie de trafic est l'une des principales utilisations de MPLS, permettant de répartir la charge sur l'ensemble du réseau en établissant des chemins explicitement définis et en contrôlant la distribution du trafic sur différentes liaisons. Cela permet d'éviter la sous-utilisation de certaines parties du réseau [15].

Dans le routage IP traditionnel utilisé par MPLS, les données sont acheminées en suivant le chemin le plus court déterminé par des protocoles de routage tels que l'OSPF. Cependant, cela peut entraîner une congestion du réseau et une perte de paquets, car toutes les données avec la même destination empruntent le même chemin.

La solution à ce problème consiste à ajouter une nouvelle fonctionnalité au réseau MPLS, appelée ingénierie de trafic (TE), ce qui donne le MPLS-TE.

• Il permet en outre d'associer des caractéristiques de qualité de service aux chemins et de subordonner l'établissement des LSP à la disponibilité de ressources dans les équipements intermédiaires.

• MPLS/TE autorise la mise en place des fonctions évoluées de partage de charge et de routage différencié. Il suffit pour cela de créer un ou plusieurs chemins concurrents pour une FEC donnée et de décider de la route à empruntée [15].

VPN

Un réseau privé virtuel (VPN) est une connexion sécurisée, à distance et permanente entre deux sites d'une organisation, permettant l'échange sécurisé de données. Il permet d'établir une communication entre deux sites distants via un réseau partagé ou public, en simulant une liaison dédiée point à point [29].

Le VPN permet d'isoler le trafic entre les sites qui ne font pas partie du même VPN, offrant ainsi une confidentialité et une sécurité accrues. Il fonctionne de manière transparente pour les sites connectés, leur donnant l'impression d'être directement connectés à leur réseau d'entreprise. Le concept de tunnel est utilisé, où les informations de l'entreprise circulent de manière sécurisée d'un bout à l'autre du tunnel, sans qu'il soit nécessaire de spécifier explicitement un routeur intermédiaire.

Les protocoles de tunneling tels que PPTP, L2TP, IPSec, etc., sont utilisés pour chiffrer les paquets de données qui doivent être transmis via le tunnel. À la réception, le protocole de tunnelisation déchiffre les paquets, permettant ainsi l'accès aux messages d'origine, à la source et à d'autres informations. Cela garantit que les données échangées sont sécurisées et confidentielles lorsqu'elles traversent des réseaux publics ou partagés. [29].

Il existe trois principaux types de VPN MPLS : les VPN de couche 2, les circuits de couche 2 et les VPN de couche 3. Tous les types de VPN MPLS partagent certains composants [29] :

• Les routeurs de bord de fournisseur, également appelés routeurs PE (Provider Edge), se trouvent à la frontière du réseau MPLS Backbone et sont équipés d'une ou plusieurs interfaces connectées aux routeurs clients, appelés routeurs CE (Customer Edge). Les routeurs PE assurent les fonctionnalités de VPN et d'étiquetage MPLS. Au sein d'un même VPN, les paires de routeurs PE sont connectées via un tunnel virtuel, généralement un chemin de commutation d'étiquettes (LSP).

•Les routeurs du fournisseur, également appelés routeurs P (Provider), constituent le cœur du réseau MPLS Backbone et n'ont pas connaissance des concepts de VPN. Leur rôle principal est d'acheminer les données en utilisant la commutation d'étiquettes.

•Les routeurs d'extrémité de client, ou routeurs CE, appartiennent aux clients et ne sont pas conscients des VPN ou même du concept d'étiquetage. Tout routeur peut être un routeur CE.

La figure ci-dessus présente un exemple de configuration d'un VPN MPLS.

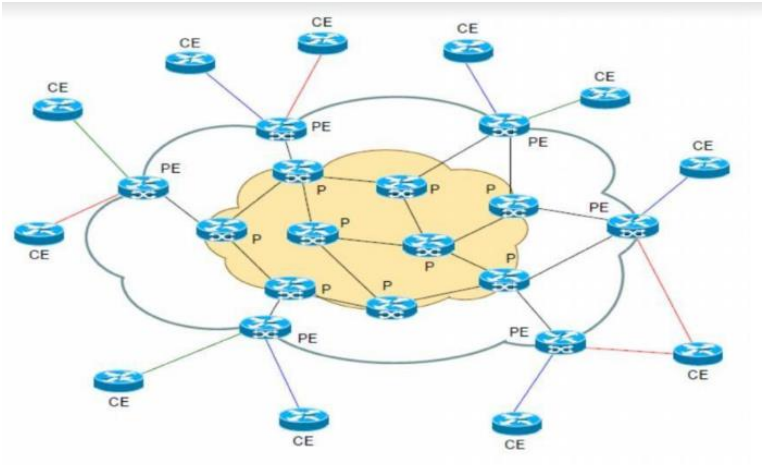


Figure 1.9 :Positionnement des routeurs P, PE et CE dans un réseau MPLS [29].

Qualité de service

La réussite d'un opérateur de réseau repose en grande partie sur un élément crucial : garantir le transport des flux de ses clients tout en assurant un débit minimal et une qualité maximale. Les paramètres essentiels pour atteindre cet objectif sont les suivants [30] :

- Le délai : il mesure le temps écoulé entre l'émission d'un paquet par la source et sa réception par la destination.

- La gigue : elle représente les variations des délais des paquets envoyés de la source vers la destination.

- Le débit : il indique la vitesse de transfert des données entre deux points d'extrémité.

- Le taux de perte de paquets : il quantifie le nombre de paquets perdus par unité de temps.

1.5.4 Avantages et inconvénients MPLS

MPLS a de nombreux avantages mais aussi des inconvénients dont nous citons [20] :

Avantages

- Amélioration des performances du routage des paquets dans le réseau.
- L'évolutivité est une option rendue facilement disponible dans MPLS.
- MPLS offre des connexions de bien meilleure qualité sans perte de paquets.
- Il existe une variété de fonctionnalités qui rendent MPLS fiable.
- Réduction des Congestions du trafics.

Inconvénients

- Il est rendu exclusif pour la connectivité point à point.
- Les routeurs doivent comprendre MPLS.
- Cela coûte cher lors de l'optimisation de la livraison dans les réseaux étendus.
- La sécurité des solutions MPLS est totalement entre les mains de l'utilisateur. Il n'y a pas de fonctionnalités de sécurité inhérentes offertes par le fournisseur MPLS.

1.6 Ingénierie de traffic (MPLS-TE)

Le mécanisme MPLS-TE permet d'établir des chemins, appelés LSP-TE (Label Switched Paths - Traffic Engineered), de la source vers la destination en prenant en compte les contraintes spécifiques du trafic telles que la bande passante, la qualité de service (QoS), le débit, etc., ainsi que les ressources disponibles sur le réseau, notamment les liens et les routeurs [30].

MPLS-TE propose une fonctionnalité appelée "reroutage rapide" (MPLS-TE Fast Re-route) en cas de défaillance dans le réseau, telle qu'une panne de liaison ou de nœud. Cette fonctionnalité permet un temps de réparation très court, généralement inférieur à 100 ms [30].

La principale différence entre MPLS et MPLS-TE réside dans l'utilisation de protocoles de routage et d'algorithmes spécifiques par MPLS-TE. Ces protocoles et algorithmes prennent en compte les contraintes de l'ingénierie de trafic (TE) ainsi que les ressources disponibles sur le réseau [30].

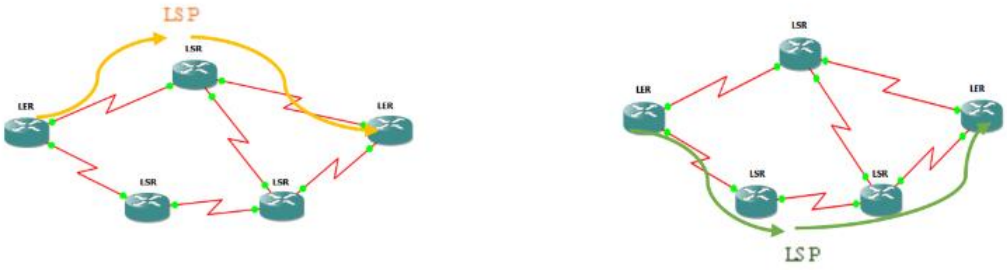


Figure 1.10 : Comparaison ente le routage statique et la TE selon MPLS [30].

Les tunnels MPLS-TE dynamiques sont configurés à l'aide de la signalisation RSVP-TE (RSVP-TE est une extension du protocole RSVP (Ressource Réservation Protocol), utilisé pour la création des routes).

1.6.1 RSVP-TE

Le protocole RSVP-TE est utilisé pour la signalisation dans le but de réserver les ressources nécessaires aux flux de données, tout en facilitant la distribution des labels. Son objectif principal est d'introduire la qualité de service (QoS) dans un réseau [30].

RSVP-TE est utilisé pour réserver les ressources requises pour les LSP dans les LSR et LER lors de l'établissement du chemin. Il permet également la détection des pannes de liens ou de routeurs, ainsi que la possibilité de rerouter rapidement les LSR.

Pour garantir un bon fonctionnement, les états de RSVP-TE sont régulièrement actualisés afin de compenser toute perte éventuelle de messages. RSVP-TE utilise principalement deux types de messages pour la réservation des ressources [30] :

-Path : demande d'établir et maintenir un LSP dans le sens descendant.
-Resv : réponse à la demande d'établissement d'un LSP dans le sens montant.

Etablissement d'un chemin :

Sachant que le travail de RSVP-TE est de signaler et maintenir la réservation de ressources à travers un réseau, il a trois fonctions de base :

- Etablir et maintenir des chemins.
- La suppression des chemins.
- La signalisation des erreurs.

1.7 Routage par segment

Le routage de segments (SR) est une technique de routage nouvelle méthode pour faire transiter les paquets sans les protocoles de signalisation (LDP et RSVP), 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 développée par la collaboration des deux groupes de travail, Source Packet Routing in Networking (SPRING avec IPv6 de l'IETF dont son architecture a été définie sous la RFC 8402. L'architecture SR peut être instanciée sur différents plans de données, deux instanciations de plan de données de SR important : SR sur MPLS (SR-MPLS) et SR sur IPv6 (SRv6), Ce qui permet de contrôler les messages pris par le trafic simplifie l'architecture et la gestion du trafic sur le réseau et permet un réseau plus évolutif [47][22].

1.7.1 Composants fondamentaux du SR

Pour comprendre le routage de segment, vous devez d'abord comprendre ses composants fondamentaux.

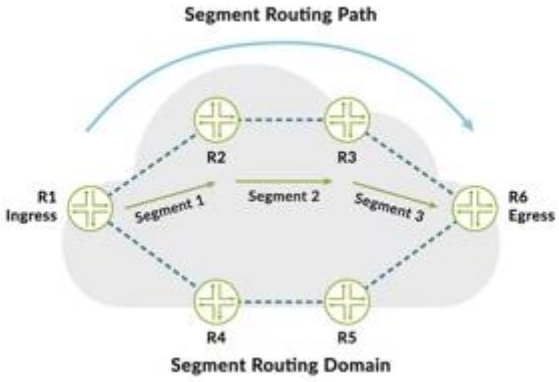


Figure 1.11 : Composants fondamentaux du SR [33].

- **Domain SR**

Un groupe de nœuds impliqués dans les protocoles SR constitue un domaine SR. À l'intérieur d'un domaine SR, chaque nœud peut remplir les rôles d'entrée, de transit ou de sortie. La division d'un domaine SR en sous-domaines SR distincts, comprenant chacun une ou plusieurs instances de protocole, permet une gestion plus flexible du

réseau et permet de répondre aux besoins spécifiques des différentes applications et types de trafic [33].

- **Chemin SR**

Il s'agit d'une séquence ordonnée de segments reliant un nœud d'entrée SR à un nœud de sortie SR. Habituellement, le chemin emprunté est celui qui présente le coût le plus bas de l'entrée à la sortie [33].

- **Segment SR**

Une directive de transfert qui guide le parcours d'un paquet à travers une partie de la topologie du réseau. SR propose divers types de segments SR, identifiés par un SID (Segment Identifier) spécifique. Ce SID d'adjacence est attribué par les protocoles ISIS ou OSPF. Le segment d'adjacence est spécifique à un routeur donné, ce qui signifie que le SID d'adjacence est localement unique pour ce routeur en particulier.

Segments d'adjacence

Un segment d'adjacence est un tunnel à saut unique qui garantit que les paquets traversent une liaison spécifique entre deux nœuds, indépendamment du coût de cette liaison. Ce tunnel est établi en utilisant le protocole de passerelle intérieure (IGP) pour connecter directement les nœuds et assurer un cheminement strict des paquets [33].

Segments de préfixe

Un segment de préfixe est un tunnel multi-sauts qui utilise des liaisons à coût égal sur le chemin le plus court pour atteindre un préfixe spécifique. Il est identifié par un ID de segment de préfixe qui peut être configuré manuellement et distribué via les protocoles ISIS ou OSPF. Ce segment est considéré comme global, ce qui signifie qu'il est unique, visible et a une portée globale dans le domaine SR. [33].

• SR Global Block (SRGB)

C'est l'ensemble des segments globaux dans le domaine SR. Si un nœud participe à plusieurs domaines SR, il y a un SRGB pour chaque domaine SR [22].

• SR Local Block (SRLB)

C'est une propriété locale d'un nœud SR. Si un nœud participe à plusieurs domaines SR, il y a un SRLB pour chaque SR domaine [22].

• Politique SR

Une liste ordonnée de segments. La tête de réseau d'une politique SR dirige les paquets vers la politique SR. Une politique SR peut être configurée par l'opérateur, provisionnée via NETCONF [RFC6241] ou provisionnée via PCEP [RFC5440]. Une politique SR peut être utilisée pour Ingénierie du trafic (TE), exploitation, administration et maintenance (OAM) ou Fast Reroute (FRR) [22].

1.7.2 Principe de fonctionnement du SR

Lorsqu'un paquet arrive au nœud d'entrée SR, il est soumis à une politique. Si le paquet répond aux critères de correspondance pour un chemin SR, le nœud d'entrée SR encapsule le paquet dans un tunnel SR qui traverse le chemin SR, segment par segment.

Chaque segment d'un chemin SR se termine à un nœud d'extrémité de segment. Lorsqu'un paquet atteint un point d'extrémité de segment, le point d'extrémité examine l'étiquette ou l'en-tête externe du paquet pour déterminer le segment correspondant. Il retire ensuite cette étiquette ou en-tête et transmet le paquet au point d'extrémité du segment suivant. Ce processus se répète jusqu'à ce que le paquet atteigne le point d'extrémité du dernier segment, qui peut être le nœud de sortie SR [33].

Lorsqu'un paquet arrive au nœud de sortie SR, ce dernier détermine si le paquet est à la fin de son chemin. Si c'est le cas, le nœud supprime les informations d'en-tête SR et transmet le paquet en fonction de son adresse IP de destination [33].

Étant donné que les routeurs de transit transfèrent simplement les paquets en fonction de l'identifiant de segment SR (SID), SR peut être utilisé pour associer des paquets liés à un utilisateur final ou à une application à des services spécifiques de fonction réseau. Pour ce faire, SR mappe un chemin vers l'emplacement où le service sera appliqué et fournit des instructions sur le service ainsi que des informations de chemin supplémentaires de la passerelle de service au routeur de sortie du domaine SR [33]

.

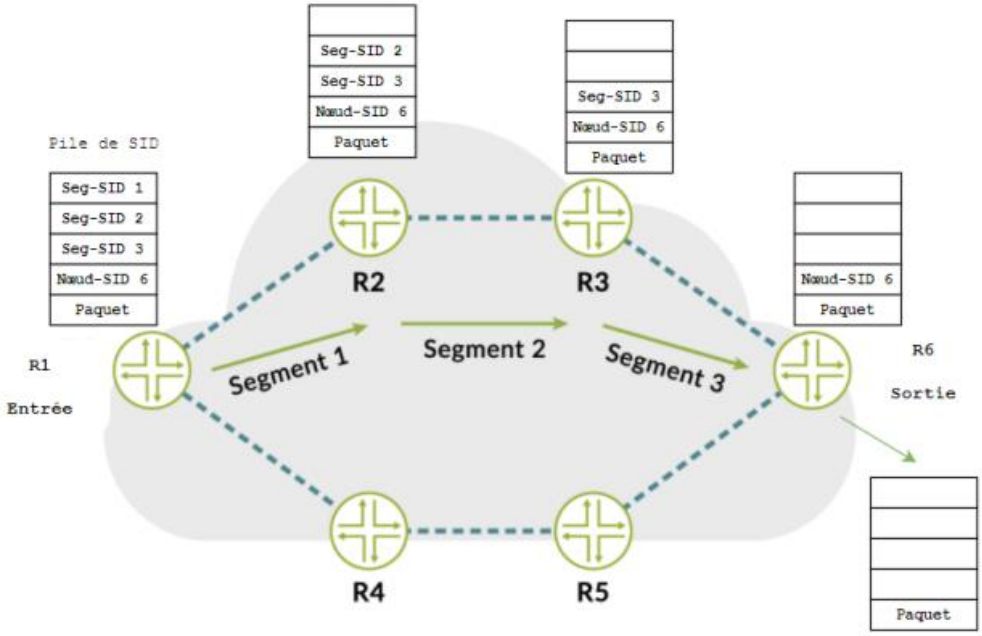


Figure 1.12 : Principe du SR [33].

1.7.3 Les avantages du routage de segment

• L'adoption de cette technologie ne nécessite pas forcément de nouveaux équipements, il suffit souvent de mieux exploiter le potentiel de l'infrastructure existante. Routage de segment peut être utilisé pour diriger le trafic de n'importe quel chemin arbitraire dans le réseau.

• Routage de segment ne nécessite aucune signalisation de chemin. Par conséquent, l'état par flux ne doit être maintenu qu'au niveau du nœud d'entrée du domaine SR, ce qui augmente la flexibilité du réseau tout en réduisant les coûts.

• Routage de segment fournit un contrôle complet sur les chemins en combinant des instructions (segments). Il ne nécessite aucun protocole tel que LDP et RSVP-TE.

• En l'adoptant, les opérateurs télécoms peuvent créer un réseau agile et efficace, mais aussi développer leurs activités en élaborant des produits novateurs et séduisants et en les introduisant rapidement sur le marché [24].

• Plan de contrôle simplifié du réseau MPLS.

• Évolution plus fluide vers les réseaux SDN.

• Capacités d'extension de capacité réseau supérieure [25].

1.8 Conclusion

MPLS est une technologie qui jouera un rôle essentiel dans les réseaux backbone IP des fournisseurs de services et opérateurs. Elle apporte de nombreux avantages tels que l'évolutivité, la performance, une meilleure utilisation de la bande passante, la réduction de la congestion du réseau et une meilleure expérience pour les utilisateurs finaux.

Cependant, MPLS présente également quelques désavantages majeurs. Premièrement, il est optimisé pour une connectivité point à point plutôt que point à cloud, ce qui signifie qu'il n'y a pas de moyen d'accéder directement à chaque cloud avec MPLS. Deuxièmement, il nécessite une optimisation du réseau étendu (WAN) pour simplifier la diffusion, ce qui ajoute des coûts supplémentaires à une solution qui peut déjà être coûteuse.

Cela ne signifie pas que MPLS sera complètement abandonné, mais plutôt que de nouvelles technologies sont nécessaires pour résoudre ces problèmes. C'est là que le routage par segment entre en jeu. Il offre une plus grande flexibilité, permettant aux utilisateurs d'avoir un contrôle accru et une gestion plus facile des ressources virtuelles dans tout le plan de contrôle. Il facilite également l'ingénierie du trafic dans les nouveaux réseaux.

Chapitre 2

2.1 Introduction

La configuration et l'implémentation d'un réseau informatique en utilisant l'infrastructure traditionnelle présentent un défi majeur pour les ingénieurs en informatique. Avec les technologies basées sur le matériel, les besoins actuels des fournisseurs et des utilisateurs finaux ne sont pas compatibles avec l'approche classique. C'est pourquoi de nouvelles approches basées sur la virtualisation ont émergé, notamment la virtualisation des fonctions réseau (NFV) et le SDN (Software-Defined Networking).

Ces nouvelles approches de virtualisation ont rendu les réseaux plus agiles. L'apparition du routage par segment a permis de résoudre les problèmes importants présents dans les réseaux IP/MPLS. L'objectif est d'avoir un réseau plus flexible, fiable et optimisé en termes de temps, de coûts et de ressources.

Dans ce qui suit, nous présenterons en détail l'architecture, le principe et les avantages de la technologie NFV et SDN.

2.2 NFV

Le NFV a été standardisé par l'Industry Specification Group (ISG) de l'ETSI (European Telecommunications Standards Institute). Il est né de la volonté d'accélérer le déploiement de nouveaux services réseau.

Le NFV vise à transformer la manière dont les opérateurs de réseau conçoivent les réseaux en développant la technologie de virtualisation informatique standard pour consolider de nombreux types d'équipements de réseau sur des serveurs, commutateurs et stockage à grand volume standard de l'industrie, qui pourraient être situés dans les Datacentres, Nœuds de réseau et dans les locaux de l'utilisateur final. Il s'agit de la mise en œuvre de fonctions de réseau dans des logiciels qui peuvent fonctionner sur une gamme de matériel de serveur standard de l'industrie et qui peuvent être déplacés ou instanciés à divers endroits du réseau, au besoin, sans qu'il soit nécessaire d'installer de nouveaux équipements [36].

2.2.1 Architecture du NFV

L'architecture NFV définie par l'ETSI est représentée sur la figure 2.1 :

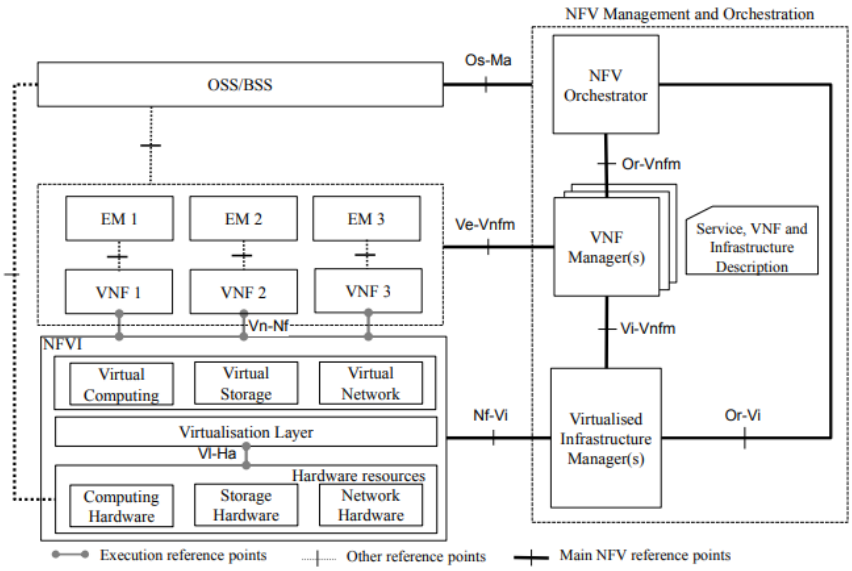


Figure 2.1 : Architecture NFV définit par ETSI [46].

L'architecture NFV est constituée de [34] :

Network Function Virtualisation Infrastructure (NFVI)

Fournit les ressources matérielles et le logiciel de virtualisation. Le NFV Infrastructure se compose de :

- Une interface matérielle (stockage, réseau, calcul).
- Une couche de virtualisation entre le matériel et le logiciel.
- Une interface virtuelle (stockage, réseau, calcul).

Virtualised Network Function (VNF)

Correspond aux fonctions réseaux virtualisées. Il s'agit de machines virtuelles fonctionnant sur l'infrastructure NFV (NFVI).

NFV Management and Orchestration

Permettant de gérer les services réseaux de bout en bout est composé de trois blocs :
• L'orchestrateur (NFV Orchestrator) : assure l'orchestration des ressources de l'IVNF sur plusieurs VIM et la gestion du cycle de vie des services de réseau.

• un gestionnaire (VNFM) en charge du cycle de vie des VNFs (la création, l'exploitation et la terminaison).

• un gestionnaire (VIM) a une relation avec NFVI pour la virtualisation ses

ressources, la création et la suppression des ressources virtuelles et le suivi de leur bon fonctionnement.

Les services OSS/BSS

Elles doivent pouvoir transmettre au bloc NFV management and orchestration des informations sur le profil des utilisateurs, la facturation, les politiques de qualités, …

2.2.2 Avantages et inconvénients du NFV

Avantages

• Réduction des coûts de l'équipement et réduction de la consommation d'énergie grâce à la consolidation de l'équipement.

• Allongement du cycle de vie des équipements matériels du réseau.

• Le NFV permet aux opérateurs d'ajouter, de supprimer, de configurer et de mettre à niveau des services et fonctionnalités réseau en temps réel et en fonction des besoins des clients, plutôt que d'exiger la commande d'Appliance réseau et leur livraison aux succursales et sites distants ou d'imposer des services identiques à tous les clients ert la vitesse de service est améliorée.

• les ressources de réseau sont accessible à tout moment (Disponibilité).

Inconvénients

• Les environnements NFV sont plus dynamiques que les environnements traditionnels, ce qui peut nécessiter une mise à l'échelle avec des fonctionnalités supplémentaires pour faire face.

• NFV exige également un réalignement des processus afin que les infrastructures traditionnelles et virtuelles puissent être gérées simultanément.

• Le NFV s'avère complexe et difficile pour de nombreux opérateurs à déployer à grande échelle. L'étendue de l'architecture et le nombre de composants distincts rendent difficile la conception, la construction et le support [34].

2.3 SDN

SDN a été normalisé grâce à une collaboration entre deux organisations, l'Open Networking Foundation (ONF) et l'Union internationale des télécommunications (UIT), plus précisément l'UIT-T. L'ONF a présenté l'architecture et les principes du SDN. Par la suite, d'autres organisations ont adopté ces normes, notamment l'IETF avec sa RFC 7426 et l'International Electrotechnical Commission (IEC) avec sa norme IEC 61850.

Le SDN est un ensemble de techniques visant à faciliter l'architecture, la livraison et l'opération de services réseaux de manière déterministe, dynamique et pouvant être déployé à grande échelle [35].

Le SDN est définit comme étant une architecture qui sépare le plan de contrôle du plan de données, et unifie les plans de contrôle de plusieurs périphériques dans un seul software de contrôle externe appelé « Contrôleur », qui voit le réseau dans sa totalité pour gérer l'infrastructure via des interfaces de communications appelées APIs. Le contrôleur en question fait abstraction de la couche physique pour les applications qui communiquent en langage développeur, permettant la programmation du réseau [37].
Globalement un réseau est dit SDN en considération des 5 caractéristiques suivantes :

- Séparation du plan de données et du plan de contrôle.
- Périphériques simplifiés.
- Contrôle centralisé.
- Automatisation du réseau et virtualisation.

2.3.1 Architecture du SDN

L'ONF a décrit une architecture de haut niveau du SDN (voir la figure2.2), qui se divise fonctionnellement en quatre couches distinctes sont : infrastructure, contrôle, application et management.

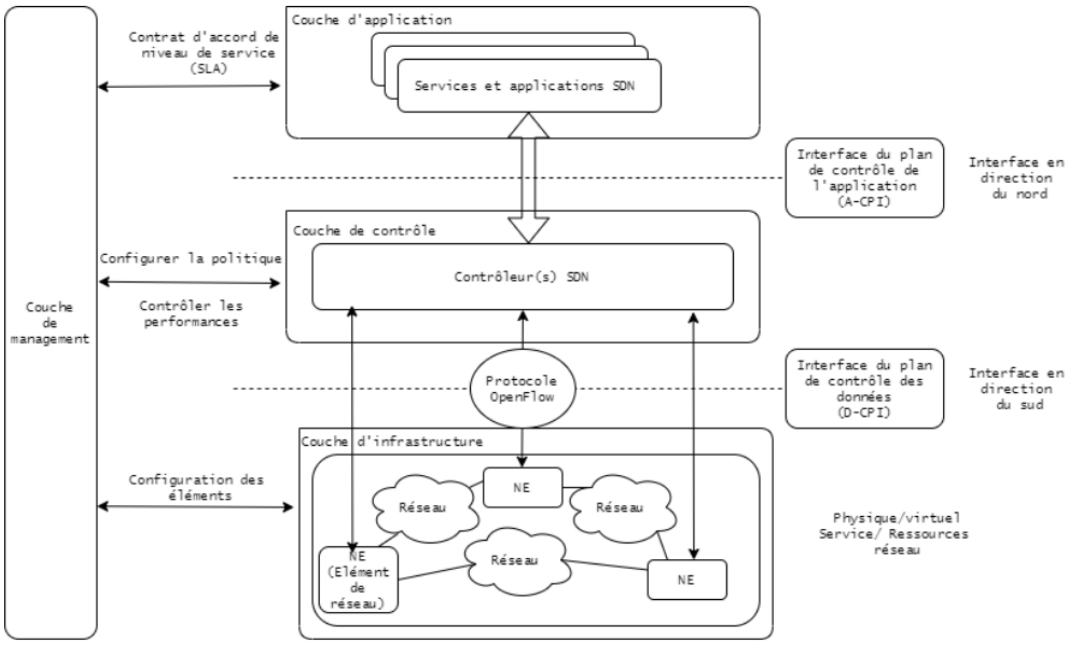


Figure 2.2 : Architecture de haut niveau du SDN [1].

Couche d'infrastructure

Elle représente la couche inférieure ou couche physique du SDN, qui est composée de dispositifs physiques ou virtuels appelés "Dispositifs SDN", dont le rôle est d'acheminer et de traiter le trafic en fonction des règles fournies par un contrôleur.

Couche de contrôle

La couche de contrôle est le point central du réseau où la logique intelligente des contrôleurs SDN réside pour contrôler l'infrastructure avec des règles fournies à partir des statistiques du réseau.

La communication entre ses entités traverse une interface appelée l'interface " est-ouest ", est généralement mise en œuvre par le biais des protocoles de passerelle tels que BGP, l'élément de calcul du chemin (PCE) ou le protocole de communication (PCEP).

Elle est également la couche intermédiaire qui relie la couche application et la couche infrastructure via les deux types d'interfaces de programmation d'applications (API) : vers le nord et vers le sud, qui seront détaillés ultérieurement. Cette couche traite les instructions et les exigences envoyées par la couche application (via l'interface sud) et

les transmet sous forme d'applications en messages aux composants du réseau (via l'interface nord).

Elle communique également les informations nécessaires extraites des dispositifs de mise en réseau tel que les statistiques de trafic, la topologie du réseau, avec les mêmes interfaces du sud vers le nord, à l'application pour qu'elle fonctionne de manière optimale.

Couche d'application

Elle s'agit d'un domaine ouvert qui permet de fournir ou même de développer, des applications et des services à la couche de contrôle tout en exploitant le comportement souhaité et les exigences du réseau recueillies par la couche d'infrastructure.

Couche de management

Selon l'ONF, la couche de management est la couche sensible de l'architecture SDN, qui doit être isolée et cachée du reste du réseau, car elle est responsable des tâches délicates à traiter selon l'état du réseau, à savoir, la gestion des pannes et de la surveillance, ainsi, la gestion de la configuration du réseau, où elles sont mieux gérées en dehors des trois couches, dans le but est d'assurer un fonctionnement optimal et une meilleure protection de l'ensemble du réseau [38].

Interface de programmation d'application

Une interface de programmation d'application ou l'API, est un intermédiaire logiciel qui permet à deux applications de communiquer entre elles à l'aide des protocoles. Or, dans les réseaux SDNs, les APIs se divisent en deux types, vers le nord et vers le sud.

• APIs vers le nord (NBI) : Elles constituent le lien entre la couche d'application et la couche de contrôle. Les NBIs ont de nombreuses fonctions notamment, les équilibreurs de charge, les pare-feu ou d'autres services de sécurité définie par logiciel, les applications d'orchestrations ou d'automatisation sur les ressources du réseau, etc.

• APIs vers le sud (SBI) : Elles constituent le lien entre la couche de contrôle et la couche d'infrastructure. Où ce type d'interface permet de fournir des protocoles de virtualisation de réseau, d'interagir avec la ma- trice de commutation ou d'intégrer

l'informatique distribuée. Les SBI les plus répandus sont le OpenFlow, Opflex, Open virtual switch database (OVSDB), etc [38].

2.3.2 OpenFlow

OpenFlow est un protocole de lien entre le plan de contrôle et le plan de données. L'échange de messages se fait au cours d'une session TCP établie via le port 6633 du serveur contrôleur. Openflow est donc une composante du SDN, son développement a commencé en 2007 dans le cadre d'une collaboration entre les mondes de l'université et des affaires. Etablie à l'origine par l'université de Stanford et l'université de Californie à Berkeley, Un switch OpenFlow est déterminé par une ou plusieurs tables de flux (flow table). Chaque table s'assimile à un ensemble de flux. Lorsqu'un paquet parvient au switch, les valeurs contenues dans ses en-têtes sont comparées aux différentes règles enregistrées dans la table de flux du switch [45].

Le rôle de cette technologie sera plus compréhensif tout en présentant ces trois principaux éléments qui sont : Commutateur OpenFlow, canal OpenFlow et contrôleur OpenFlow comme il est illustré dans la figure 2.3 et figure 2.4, où :

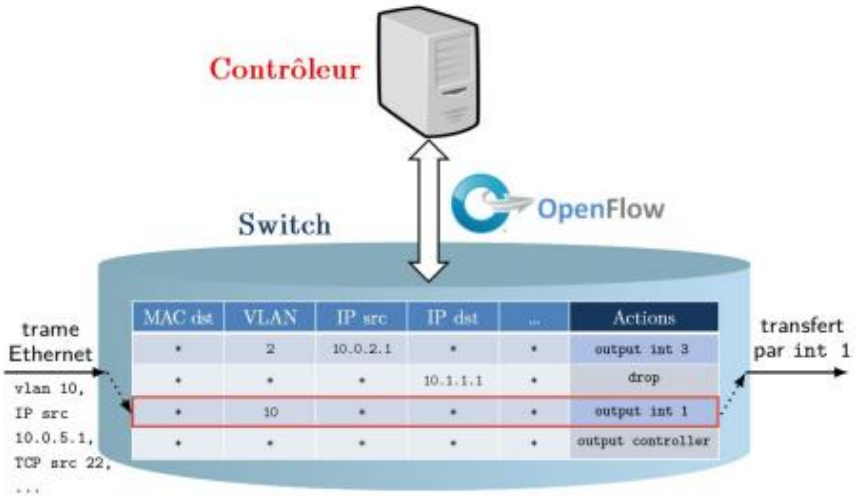


Figure 2.3 : Architecture de la technologie OpenFlow [45].

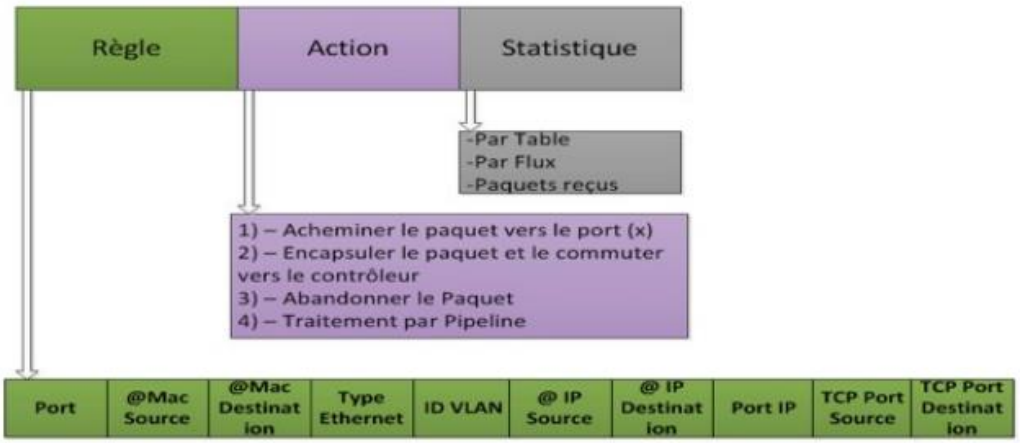


Figure 2.4 : Structure de la table de flux [45].

• Les commutateurs OpenFlow (OF) sont des dispositifs physiques ou logiques spécifiques à l'environnement OpenFlow. Ils permettent de transférer les paquets dans un environnement SDN en utilisant des tables appelées "tables de flux". Un commutateur OF peut contenir une ou plusieurs de ces tables. Chaque table de flux est composée d'une liste d'entrées de flux. Chaque entrée comprend des champs d'en-tête, des compteurs et des actions. Les champs d'en-tête sont utilisés pour comparer les paquets et contiennent des informations telles que l'ID VLAN, les ports source et destination, les adresses IP, etc. Les compteurs sont utilisés pour enregistrer des statistiques sur les paquets, comme le nombre de paquets, le nombre d'octets, etc. Les actions spécifient comment traiter et acheminer les paquets dans un flux, par exemple en les transférant vers un port spécifique, en les envoyant vers un contrôleur ou en les supprimant (voir la figure 2.4). Ces commutateurs sont gérés par des contrôleurs OpenFlow qui résident dans la couche de contrôle du réseau. La communication entre les commutateurs et les contrôleurs s'effectue via le canal OpenFlow, qui est sécurisé par le protocole TLS (Transport Layer Security). Cette communication est établie via un protocole propriétaire spécifique à OpenFlow, qui permet uniquement la connexion entre le contrôleur et le commutateur.

• Le contrôleur OpenFlow (OF) est l'élément central d'un environnement SDN. Il joue le rôle essentiel de maintenir, distribuer et mettre à jour les politiques et les instructions pour les périphériques du réseau. Le contrôleur OF est chargé de gérer et de configurer le trafic des flux en ajoutant ou supprimant des entrées de flux dans les tables de flux des commutateurs. Un commutateur OF peut être connecté à un ou plusieurs contrôleurs OF. Une meilleure fiabilité du réseau est obtenue en utilisant plusieurs contrôleurs. Lorsque la technologie OF est mise en œuvre, le commutateur doit se connecter

simultanément à tous les contrôleurs qui lui sont configurés. Cependant, seuls les messages pertinents sont envoyés au commutateur correspondant.

• Le canal OpenFlow (OF) est l'interface qui permet la communication entre le contrôleur OF et les commutateurs OF. Il permet l'échange de messages en utilisant le protocole OpenFlow. Dans ce contexte, nous pouvons distinguer trois types de messages : les messages du contrôleur au commutateur, les messages asynchrones et les messages symétriques.

Messages OpenFlow

Les messages contrôleur à commutateur sont envoyés par les contrôleurs pour gérer et inspecter correctement l'état du commutateur, notamment [45] :

• **Caractéristiques** dont le commutateur les envoie au contrôleur après une demande de la part de ce dernier.

• **Configuration** permet au contrôleur de définir et consulter les paramètres de configuration du commutateur.

• **Modifier** l'état sont envoyés par le contrôleur pour gérer l'état des commutateurs. Ils sont utilisés pour ajouter/supprimer ou modifier les entrées de la table de flux ou pour définir les priorités des ports des commutateurs.

• **Envoi du paquet** sont responsables de l'envoi et de la transmission des paquets de la part du commutateur à l'aide de table de flux.

Les messages asynchrones sont envoyés sans que le contrôleur ne les sollicite auprès du com- mutateur. Ils sont envoyés par le commutateur pour mettre à jour le contrôleur sur les événements du réseau et les changements d'état du commutateur, nous citons [45] :

• **Paquet d'entrée** transfert le contrôle du paquet au contrôleur dans le cas où les paquets qui n'ont pas d'entrée de flux correspondant ou si un paquet correspond à une entrée avec une action d'envoi au contrôleur, un message 'entrée de paquet est envoyé au contrôleur.

• **Elimination du flux** informe le contrôleur de la suppression d'une entrée de flux d'une table de flux. Le message de modification de flux précise également si le

commutateur doit envoyer un message de suppression de flux au contrôleur lorsque le flux expire.

• **Etat du port** informe le contrôleur de l'état du port du commutateur, tel que le changement d'état du port (le cas de spanning tree IEEE 802.1D). Le commutateur doit envoyer l'état du port au contrôleur via les messages port-update.

• **Erreur** aide le commutateur d'informer le contrôleur qu'il existe des problèmes.

Les messages symétriques peuvent être initiés par le commutateur ou le contrôleur et envoyés sans sollicitation. Les trois types de messages symétriques sont les suivants [45] :

• **Hello** présentent les messages d'accueil sont échangés entre le commutateur et le contrô- leur lors de l'établissement de la connexion.

• **Echo** sont utilisé pour indiquer la latence, la bande passante et/ou la disponibilité d'une connexion contrôleur-commutateur.

• **Vendeur** offrent une fonctionnalité supplémentaire dans l'espace du type de message OpenFlow pour les futures révisions d'OpenFlow.

2.3.3 Avantages du SDN

- Meilleur contrôle du réseau - SDN favorise un point de contrôle central pour
- distribuer les politiques et la configuration du fournisseur de manière cohérente le réseau. Les contrôleurs SDN offrent une visibilité et un contrôle complets sur le réseau assurant un contrôle d'accès et une ingénierie du trafic appropriés.
- Orchestration d'environnements multifournisseurs – le contrôleur SDN peut configurer et gérer tout appareil compatible SDN. Un protocole unique est utilisé pour la communication entre un contrôleur et des appareils de n'importe quel fournisseur.
- Induit l'innovation - SDN offre des possibilités aux fournisseurs, aux opérateurs ou à un tiers pour développer des applications, des services et des modèles commerciaux et déclencher les flux de revenus et plus de valeur du réseau.

- Réduit les dépenses opérationnelles - le matériel réseau est simplifié par suppression de la fonction de contrôle. Les coûts d'exploitation globaux sont réduits de contrôle plus facile du réseau et une meilleure utilisation du réseau.
- Améliore l'efficacité du réseau - contrôle et gestion centralisés augmenter l'automatisation et l'orchestration du réseau. Pas besoin de configurer dispositifs réseau individuels dans le plan de transfert pour répondre à la politique commerciale en changeant. Le réseau est directement programmable par un logiciel propriétaire ou un outil d'automatisation open source [39].

2.3.4 SDN versus réseau traditionnel

La structure de l'Internet et les réseaux informatiques se composent généralement de différents dispositifs de réseau tels que routeur, commutateur et différents types de middlebox qui sont intégrés verticalement et conçus par des puces et ASIC (circuits intégrés spécifiques à l'application) avec un débit élevé et une fonction spécifique [40].

Pour la gestion et la configuration de ces périphériques réseau, un ensemble de commandes de ligne spécifiques et prédéfinies basées sur un système d'exploitation intégré est utilisé. Par conséquent, on peut faire valoir que la gestion d'un grand nombre de périphériques réseau est un grand défi qui est sujet à de nombreuses erreurs. Ainsi, les réseaux traditionnels souffrent d'importantes lacunes en matière de recherche et d'innovation, la fiabilité, l'extensibilité, la flexibilité et gestion. Depuis la naissance de l'internet, les réseaux se développent et de nouvelles technologies telles que le cloud, les réseaux sociaux et la virtualisation ont vues le jour, le besoin de réseaux avec une bande passante plus large, une plus grande accessibilité et une gestion dynamique plus élevée est devenu un problème critique [48].

Pour résoudre les problèmes et les limites des réseaux traditionnels, une structure a été proposée, connue sous le nom de SDN, où le contrôle du réseau est séparé du mécanisme de transmission et peut être programmé et contrôlé directement [40].

La différence architecturale entre l'Internet traditionnelle et le SDN est illustrée dans la Figure 1. Il représente clairement comment le contrôle est géré (logiquement) de manière centralisée, et le data plane est simplifié en simples éléments de transfert. Les commutateurs programmables du plan de données peuvent être implémentés dans le

matériel ou le logiciel à condition qu'ils supportent le protocole OpenFlow pour la communication et la configuration avec le contrôleur [49].

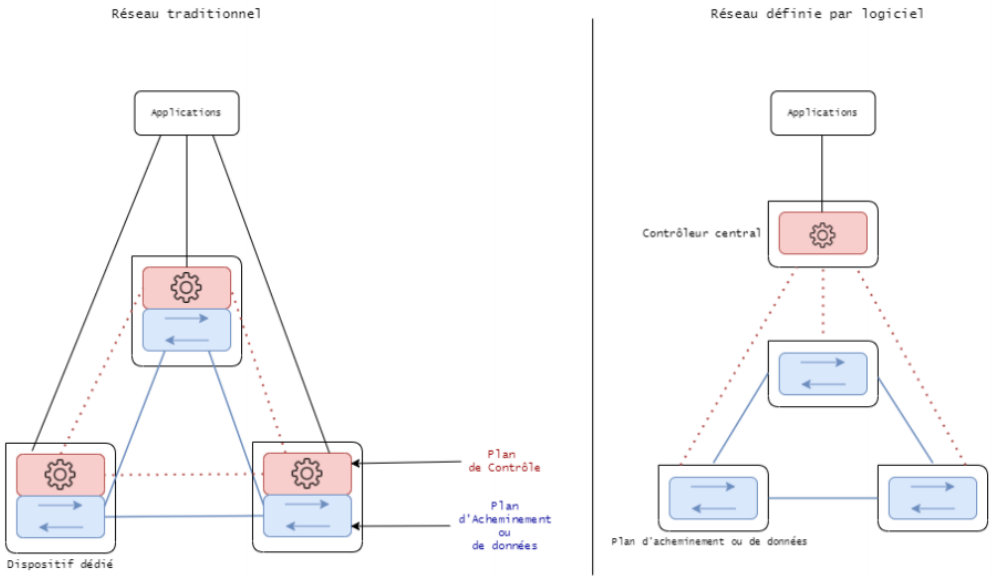


Figure 2.5 : SDN versus le réseau traditionnel (architecture) [1].

2.4 Le protocole PCEP

Le protocole PCEP est un protocole TCP défini par l'IETF dans RFC 5440 qui définit un ensemble de messages et d'objets utilisés pour gérer les sessions PCEP et demander et envoyer des chemins pour les LSP techniques de trafic engineering.

Le protocole PCEP fournit le mécanisme de communication entre les PCE et les PCC. Les PCC envoient des demandes de calcul de chemin aux PCE en utilisant le protocole PCEP, et les PCE utilisent ces demandes pour calculer les chemins optimaux et les renvoyer aux PCC via le protocole PCEP. Cette séparation des fonctions de calcul de chemin et de commutation de trafic permet une gestion plus efficace des ressources réseau et une optimisation des performances globales du réseau.

- Un élément de calcul de chemin (PCE) est une entité (composant, application ou nœud réseau) capable de calculer un chemin ou un routage réseau en fonction d'un graphique du réseau et d'appliquer des contraintes de calcul.
- Un client de calcul de chemin (PCP) est une application cliente demandant un calcul de chemin à effectuer par un PCE.

- Traffic Engineering Database (TED) est une base de données qui contient tout les informations sur les ressources d'une topologie d'un réseau [41].

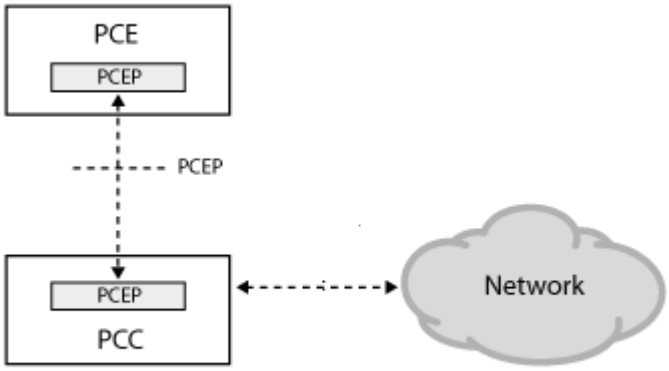


Figure 2.6 : Architecture du protocole PCEP [41].

2.5 Conclusion

Grâce aux avantages offerts par le SDN et le routage par segment, la mise en place d'une architecture et l'ingénierie du trafic sont devenues plus faciles à gérer, à configurer et à sécuriser pour les professionnels de l'informatique. Après avoir présenté les concepts liés à notre travail, le prochain chapitre se concentrera sur la simulation détaillée de la solution proposée dans un environnement virtuel.

Chapitre 3

3.1 Introduction

La technologie du segment routing a suscité un vif intérêt parmi les ingénieurs et chercheurs du domaine, qui l'ont étudiée et mise en œuvre à la fois sur le plan logiciel et matériel. Cependant, notre approche a été de suivre la méthode proposée et supervisée par les fournisseurs d'Ericsson.

Nous avons présenté cette idée et l'avons étudiée en simulant les environnements de travail GNS3 et OpenDaylight.

Ce chapitre se concentrera sur la présentation de l'environnement de travail utilisé, ainsi que sur les étapes de simulation de la solution proposée. Par la suite, nous procéderons à l'analyse des résultats obtenus.

3.2 Environnement de travail

Nous allons présenter l'environnement logiciel et matériel que nous avons utilisé dans la simulation du réseau.

Environnement materiel

L'environnement matériel utilisé est un ordinateur portable avec les caractiristiques svuivantes :

• **Processeur :** Intel(R) Core(TM) i5-1035G1

• **Mémoire :** 16G

• **Disquedur :** 250G

• **Systèmed'exploitation :** Ubuntu 18.04

Environnement logiciel

GNS3

GNS3 (Graphical Network Simulator) est un logiciel open source qui permet de simuler et émuler des réseaux complexes tout en étant aussi proche que possible du fonctionnement des réseaux réels. GNS3 est constitué de deux composants logiciels :

- **Logiciel GNS3-all-in-one (GUI) :** Il s'agit de la partie client du GNS3 et de l'interface utilisateur graphique (GUI) (voir figure 3.1).

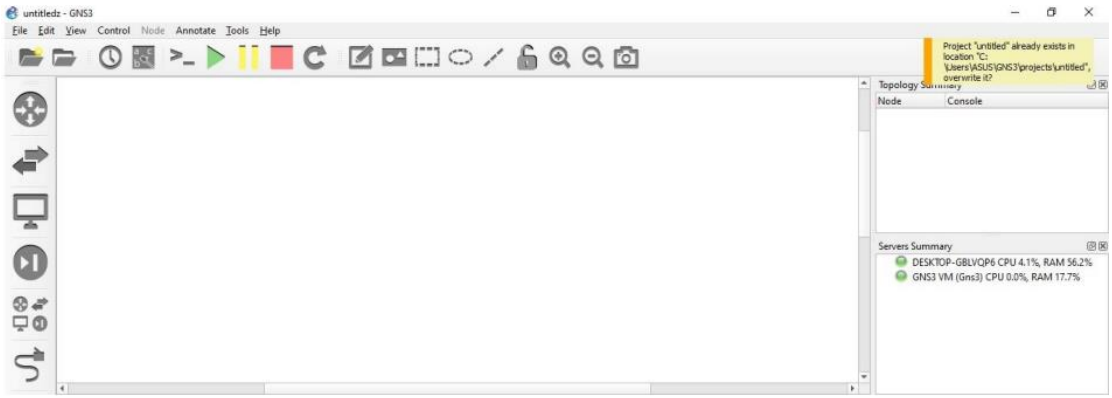


Figure 3.1 : GNS3 GUI.

- **Serveur GNS3 :** Il est nécessaire d'héberger et d'exécuter les périphériques créés via un processus serveur. Le serveur peut être installé localement en tant que serveur autonome, une machine virtuelle locale ou une machine virtuelle distante.

  Dans notre situation, nous utilisons des images Qemu et, conformément à la documentation officielle de GNS3, il est recommandé d'utiliser une machine virtuelle dans ce cas.

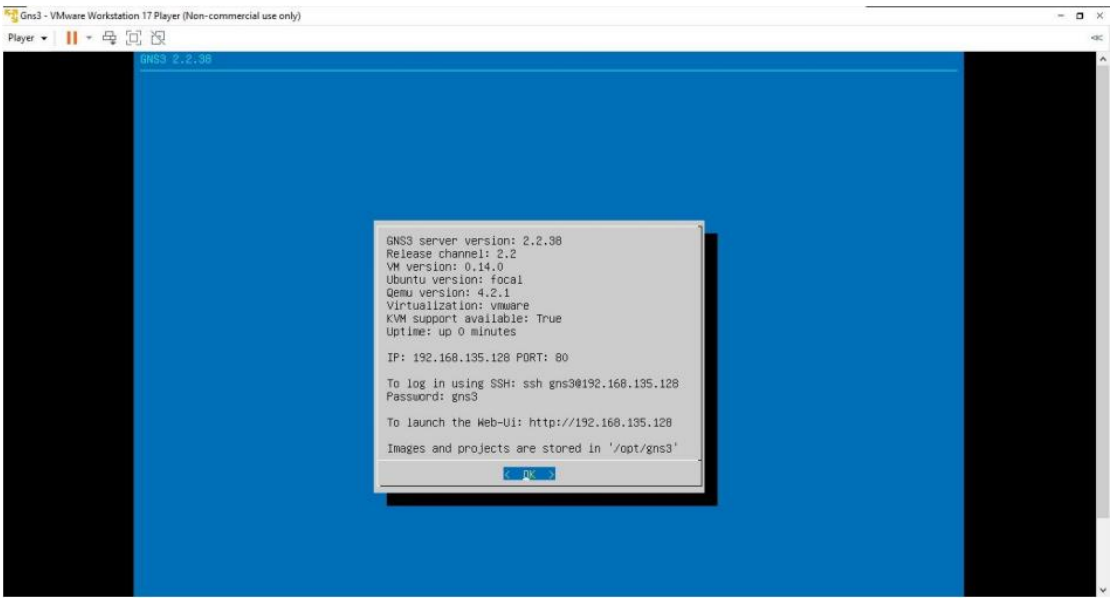


Figure 3.2 : GNS3 serveur VM (vmware).

VMware

VMware Player est un logiciel de virtualisation de bureau qui peut exécuter plusieurs invités systèmes d'exploitation en même temps sur un seul PC. L'interface utilisateur est assez facile à utiliser et toutes les fonctionnalités sont faciles à trouver. VMware player supports des centaines de systèmes d'exploitation invités, des anciens systèmes d'exploitation aux derniers ceux.

VMware prend également en charge la portabilité du système d'exploitation invité. Où on peut prendre facilement prendre le système d'exploitation invité déjà installé et faire clone de cette machine virtuelle, qui plus tard peut être prise à un autre endroit. Cette élimine le besoin de mettre en place une nouvelle machine virtuelle à partir de zéro.

OpenDayLight

OpenDayLight ou ODL est un contrôleur et un framework SDN open source hébergé par la fondation Linux. ODL est basé sur la programmation Java langage et supporte OpenFlow standard.Certaines des entreprises qui contribuer au développement d'ODL sont Cisco, Juniper Networks, VMware, Microsoft, Ericsson, etc.la figure 3.3.

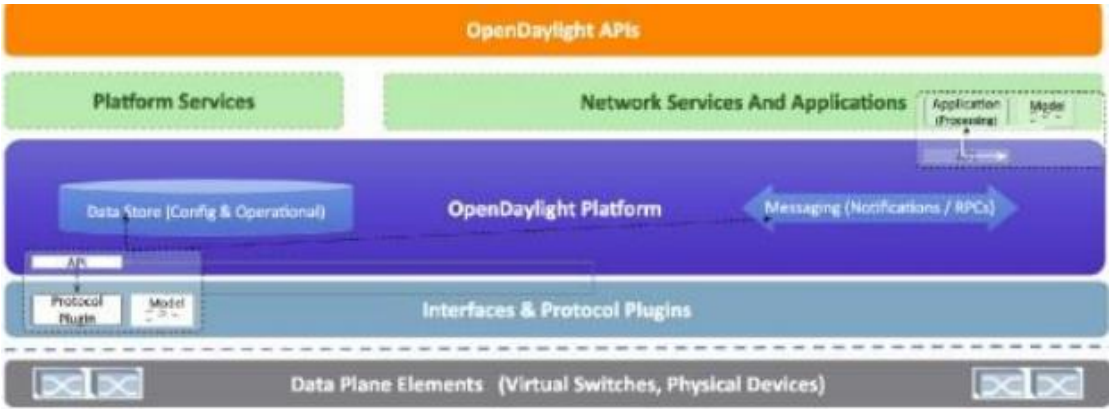


Figure 3.3 : Architecture d'ODL.

Où :

• ODL API est une API northbound qui est utilisée pour communiquer avec la couche supérieur principalement basée sur REST. La couche d'abstraction de service orientée modèle rend les API REST conformément à la spécification RESTCONF basée sur les modèles YANG définis par les applications via des protocoles tels que

HTTP.Comme chaque outil, ODL à aussi une partie d'authentification dont nous allons présenter dans la suite.

• AAA ou Authentification, l'Autorisation et la Comptabilité (Acounting) permet d'identifier les périphériques et contrôleur du réseau, où nous avons gardé l'identification par défaut, "admin" pour le nom d'utilisateur et le mot de passe, mais, nous pouvons rendre la sécurité plus robuste en modifiant cette configuration.

• Plateforme de contrôleur présente la partie cœur d'ODL, dont nous trouvons :

• NetVirt ou Network Virtualization est une plateforme de virtualisation de réseau qui permet de créer et de gérer les réseaux VPN.

• MD-SAL ou la couche d'adaptation de service pilotée par modèle est un composant middleware extensible qui fournit des fonctionnalités de messagerie et de stockage de données basées sur des modèles de données et d'interface définis par les développeurs d'applications.

• Pluggins ou enfichables permettent d'effectuer différentes tâches sur le réseau telles que, la collecte de statistiques sur le réseau.

• Les protocoles OpenFlow et OVBSD (Open vSwitch Database Management Protocol) sont présentés dans le chapitre précédent. La configuration des API d'ODL se fait dans la GUI de cette plateforme, mais il existe des applications qui ont facilité cette tâche dont celui que nous avons choisi : l'application Postman.

Application Postman

Postman est un outil dédié au développement d'API (Interface de programmation d'applications) qui simplifie la création, le test et la modification des API. Il permet d'envoyer différents types de requêtes HTTP tels que GET, POST, PATCH, PUT et DELETE, en utilisant les formats de données JSON et XML. Ces requêtes sont transmises via une URL spécifiant l'adresse de notre contrôleur OpenDaylight et le port TCP approprié, généralement en utilisant le protocole HTTP (port 80) ou HTTPS (port 8181).

Tel que :

• **GET** pour récupérer des données d'un API.

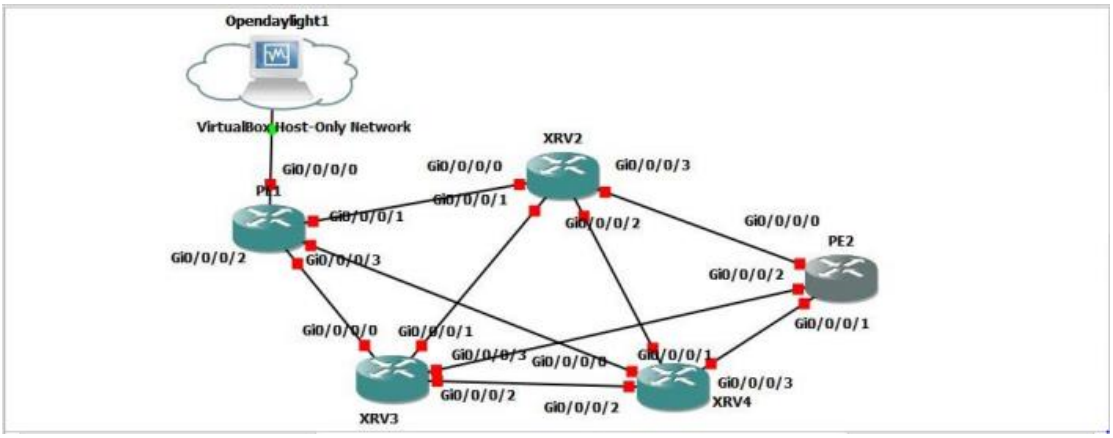
• **POST** pour envoyer les nouvelles données d'un API.

• **PATCH** et **PUT** pour actualiser les données existantes.

• **DELETE** pour supprimer les données existantes.

. 3.3 Construction de la topologie

Dans cette section, nous allons aborder l'architecture réseau de notre projet afin de vous la présenter.



.. Figure 3.4 : Topologie.

Pour la topologie abordée, nous avons opté pour le routeur virtuel du fournisseur Cisco, le Cisco XRv Cette machine virtuelle contient un seul processeur de routage (RP) avec une fonctionnalité de plan de contrôle et des interfaces réseau de carte de ligne (LC : line control) avec leurs fonctionnalités associées.

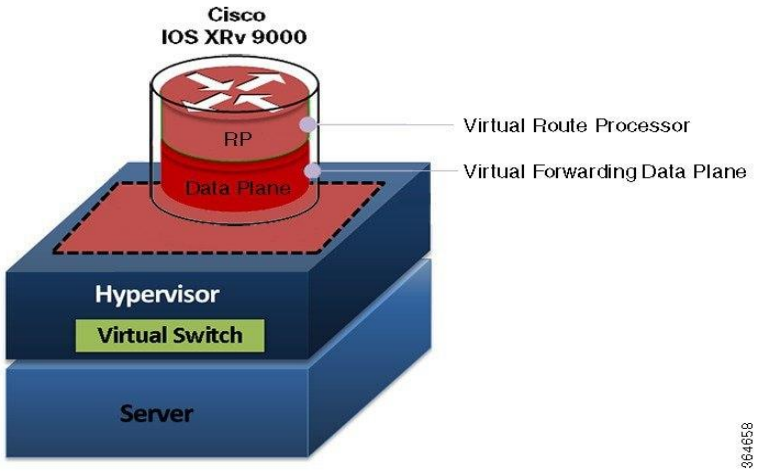


Figure 3.5 : Architecture du XRV

Le routeur Cisco XRV nécessite des ressources importantes minimum 4Gb de RAM pour chaque routeur, et au vu des contraintes matérielles nous n'allons utiliser que 5 routeurs. Dans le cas d'un petit réseau ceci ne pose pas de problème car nous n'allons pas acheminer les paquets aux clients finaux. Dans notre architecture nous avons utilisé un NAT Cloud connectant notre machine virtuelle (virtualbox) dans notre cas Ubuntu, dans laquelle est installé Opendaylight où nous communiqueront avec celle-ci avec Postman.

3.4 Configuration de connectivité

Chaque routeur dispose de quatre interfaces ethernet pour lier les routeurs entre eux, à l'exception du routeur d'extrémité PE2.

Nous avons commencé par l'attribution des adresses ipv4 au contrôleur et aux interfaces des routeurs, permettant ainsi d'assurer l'acheminement du trafic entre les routeurs. Plan d'adressage Nous avons attribué les adresses ip en suivant le plan d adressage illustre dans la figure 3.3

3.4.1 Plan d'adressage

Nous avons attribué les adresses ip en suivant le plan d'adressage illustré dans le Tableau 3.1

Nœud	Adresse de bouclage	Adresse de l'interface Ethernet de Gigabyte
Hote Odl	Pas DE CONFIGURATION	E0 :192.168.56.106
		E0 : DHCP
PE1	1.1.1.1	E0 :192.168.56.200
		E1192.168.12.1
		E2 :192.168.13.1
		E3 :192.168.14.1
XRV2	2.2.2.2	E0 :192.168.12.2
		E1 :192.168.23.1
		E2 :192.168.24.1
		E3 :192.16825.1
XRV3	3.3.3.3	E0 :192.168.13.2

		E1 :192.168.23.2
		E2 :192.168.34.1
		E3 :192.168.35.1
XRV4	4.4.4.4	E0 :192.168.14.2
		E1 :192.168.24.2
		E2 :192.16834.2
		E3 :192.168.45.1
PE2	5.5.5.5	E0 :192.168.25.2
		E1 :192.168.35.2
		E2 :192.168.45.2

Tableau 3.1 : Plan d'adressage.

```
RP/0/0/CPU0:ios#show ip int br
Mon Jun  5 13:19:31.023 UTC

Interface                  IP-Address      Status          Protocol Vrf-Name
Loopback0                  1.1.1.1         Up              Up       default
tunnel-te1                 unassigned      Down            Down     default
tunnel-te2                 unassigned      Down            Down     default
tunnel-te3                 unassigned      Down            Down     default
tunnel-te4                 unassigned      Down            Down     default
MgmtEth0/0/CPU0/0          unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/0     192.168.56.200  Up              Up       default
GigabitEthernet0/0/0/1     192.168.12.1    Up              Up       default
GigabitEthernet0/0/0/2     192.168.13.1    Up              Up       default
GigabitEthernet0/0/0/3     192.168.14.1    Up              Up       default
GigabitEthernet0/0/0/4     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/5     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/6     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/7     unassigned      Shutdown        Down     default
```

Figure 3.6 : PE1.

```
Mon Jun  5 13:25:09.141 UTC

Interface                  IP-Address      Status          Protocol Vrf-Name
Loopback0                  3.3.3.3         Up              Up       default
MgmtEth0/0/CPU0/0          unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/0     192.168.13.2    Up              Up       default
GigabitEthernet0/0/0/1     192.168.23.2    Up              Up       default
GigabitEthernet0/0/0/2     192.168.34.1    Up              Up       default
GigabitEthernet0/0/0/3     192.168.35.1    Up              Up       default
GigabitEthernet0/0/0/4     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/5     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/6     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/7     unassigned      Shutdown        Down     default
RP/0/0/CPU0:ios#
```

Figure 3.7 : XRV3.

```
RP/0/0/CPU0:ios#show ip int br
Mon Jun  5 21:06:17.966 UTC

Interface                  IP-Address      Status          Protocol Vrf-Name
Loopback0                  4.4.4.4         Up              Up       default
MgmtEth0/0/CPU0/0          unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/0     192.168.14.2    Up              Up       default
GigabitEthernet0/0/0/1     192.168.24.2    Up              Up       default
GigabitEthernet0/0/0/2     192.168.34.2    Up              Up       default
GigabitEthernet0/0/0/3     192.168.45.1    Up              Up       default
GigabitEthernet0/0/0/4     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/5     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/6     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/7     unassigned      Shutdown        Down     default
RP/0/0/CPU0:ios#
```

Figure 3.8 : XRV4.

```
Interface                  IP-Address      Status          Protocol Vrf-Name
Loopback0                  5.5.5.5         Up              Up       default
MgmtEth0/0/CPU0/0          unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/0     192.168.25.2    Up              Up       default
GigabitEthernet0/0/0/1     192.168.45.2    Up              Up       default
GigabitEthernet0/0/0/2     192.168.35.2    Up              Up       default
GigabitEthernet0/0/0/3     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/4     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/5     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/6     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/7     unassigned      Shutdown        Down     default
RP/0/0/CPU0:ios#
```

Figure 3.9 : PE2.

3.4.2 Configuration de protocole ISIS

Nous allons mettre en place un réseau MPLS/TE qui utilise le protocole ISIS pour le calcul du chemin le plus court. Chaque nœud du reseau sera en mesure de construire une carte de connectivite sous forme de graphe, ce qui facilitera la gestion du réseau. Pour ce faire,nous allons configurer le protocole ISIS sur les 5 routeurs et activer sur toutes les interfaces,à léxceptin de l'interface de gestion qui ne nécessite par de routage ,ainsi que les interfaces de bouclage.

```
router isis 1
 is-type level-2-only
 net 49.0000.0000.0001.00
 distribute bgp-ls
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  redistribute connected
  redistribute static
  segment-routing mpls
 !
 interface Loopback0
  circuit-type level-2-only
  address-family ipv4 unicast
   prefix-sid absolute 17001
  !
 !
 interface GigabitEthernet0/0/0/1
  point-to-point
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/2
  point-to-point
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/3
  point-to-point
```

Figure 3.10: Configuration ISIS.

La vérification de cette configuration sera faite via un ping entre ces routeurs figure3.11

```
RP/0/0/CPU0:ios#ping 3.3.3.3
Mon Jun  5 21:19:22.824 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/9 ms
RP/0/0/CPU0:ios#ping 4.4.4.4
Mon Jun  5 21:19:29.294 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
RP/0/0/CPU0:ios#ping 5.5.5.5
Mon Jun  5 21:19:33.924 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms
RP/0/0/CPU0:ios#
```

Figure 3.11 : Vérification de la connectivité entre les routeurs.

La vérification de cette configuration sera faite via un ping entre ces routeurs

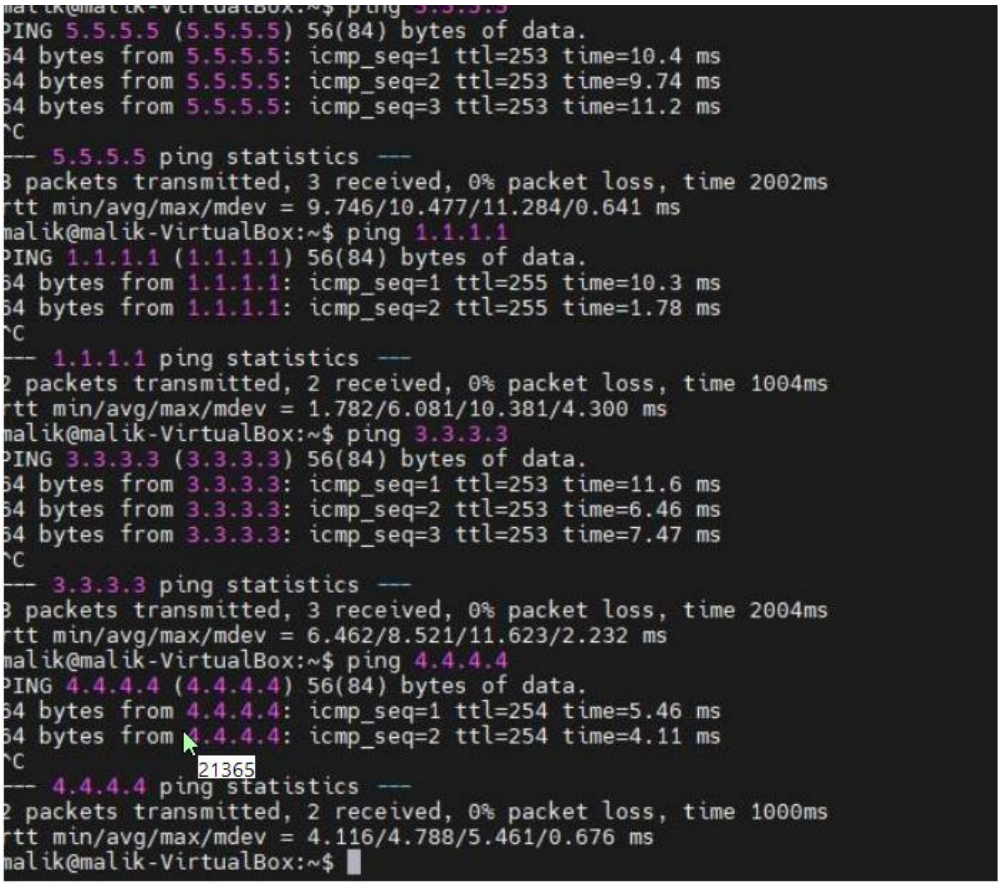


Figure 3.12: Opendaylight connectivite entre les routeurs.

Sons oublier de verifier la connectivité entre l'hôte est les routeurs est réussie aussi.

3.5 Configuration d'un réseau MPLS/SDN

Le réseau MPLS/SDN se compose d'un routeur Provider Edge (PE) et de routeurs P. Les routeurs PE servent d'interface entre le cœur du réseau et les nœuds externes pour acheminer le trafic rapidement et bénéficier d'un contrôle robuste en utilisant des étiquettes LSP (Label Switched Paths). L'introduction du réseau SDN améliore le contrôle d'un réseau MPLS, où le nœud externe joue ce rôle. Ainsi, le réseau MPLS/SDN est formé grâce à cette collaboration.

Les informations échangées entre le cœur du réseau et le nœud externe sont gérées au niveau des routeurs PE1 et PE2. Pour transporter les informations de routage du réseau et les étiquettes MPLS entre ces deux nœuds, il est nécessaire de configurer un protocole BGP interne. De plus, une communication doit être établie entre les routeurs

PE et le contrôleur SDN. Dans notre cas, le protocole PCEP est utilisé, où le PCE représente le contrôleur SDN et le PCC représente les routeurs PE. Les routeurs PE1/PE2 sont désignés comme nos routeurs PE, tandis que les routeurs XRV2, XRV3 et XRV4 sont nos routeurs P.

Dans les sections suivantes, nous présenterons étape par étape la configuration établie pour le réseau MPLS/SDN. Nous avons commencé par la configuration de l'EBGP au niveau du routeur, comme illustré dans la figure. 3.13, où :

Figure 3.13 : BGP-LS configuration PE1 et PE2.

L'adresse IP du contrôleur OpenDaylight, 192.168.56.105, mentionnée comme voisin (neighbor), permettra aux routeurs PE1 et PE2 de transmettre les informations de notre réseau à OpenDaylight. En résumé, les informations sur l'état des liens collectées par le protocole IGP (ISIS dans ce projet) dans le domaine seront transmises via le protocole BGP-LS au pair BGP d'OpenDaylight. Cela permettra de maintenir les autres routeurs à jour en cas de connexion ou de déconnexion d'un routeur voisin.

À l'intérieur de l'address-family ipv4 unicast, nous avons d'abord configuré le style de métrique "wide", ce qui signifie que seuls les TLV (Type-Length-Value) de nouveau style peuvent être reçus par l'IS (Intermediate System). Pour permettre à un routeur de propager des informations sur les liens MPLS (Multiprotocol Label Switching) via IS-IS dans le niveau configuré, il doit être configuré à l'intérieur de l'instance IS-IS (voir figure

Dans notre cas, nous avons configuré la distribution des liens MPLS uniquement dans le niveau 2 et avons spécifié l'adresse 192.168.56.200 pour PE1, ainsi que Loopback0 en tant qu'identifiant du routeur PE2.

Enfin, nous avons configuré les interfaces annoncées par IS-IS. Nous avons également spécifié le Node-SID (Segment IDentifier) qui sera associé à l'adresse Loopback du

routeur. Les deux autres interfaces ont été configurées en tant que liens GigabitEthernet en mode point-à-point et avec une famille d'adresses unicast.

3.5.1 Configuration MPLS, PCEP et Segment routing

Cependant, lorsque nous utilisons le contrôleur SDN ODL (OpenDayLight), il est important de configurer l'adresse IP source de manière appropriée. Si cette configuration n'est pas correcte, nous pourrons établir la connexion PCEP (Path Computation Element Protocol), mais nous ne pourrons pas ajouter de LSP (Label Switched Path). Pour assurer une connexion réussie, l'adresse IP de loopback du routeur utilisée pour BGP-LS doit correspondre à l'adresse IP PCEP (dans ce cas, l'adresse IP PCEP serait 192.168.56.105). C'est ainsi que les deux topologies sont liées. Par conséquent, lors de l'utilisation d'ODL, la configuration du PCE sur le routeur doit être réalisée de la manière suivante.

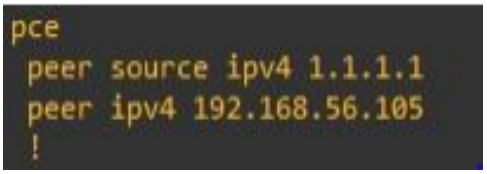


Figure 3.14 : Peer ODL.

Veuillez noter que pour établir une connexion PCE-P, votre instance ODL doit être en mesure de router vers les adresses loopback de votre réseau XRv. Par exemple, si ces adresses se trouvent dans le réseau 10.10.0.0/16, vous pouvez exécuter la commande suivante sur l'hôte ODL : sudo route add -net 192.168.56.200/30 gw 192.168.56.200. Si vous souhaitez que cette configuration persiste après un redémarrage, vous pouvez modifier le fichier /etc/network/interfaces (si vous utilisez Ubuntu) et ajouter la ligne suivante : up route add -net 192.168.56.200/16 gw 192.168.56.200.

La configuration du PCE est nécessaire sur nos routeurs PE afin d'activer la création de chemin. De plus, dans OpenDaylight, dans le module PCE, nous allons configurer l'adresse de connexion. Il est important de préciser que nous souhaitons effectuer des calculs de chemin en mode SR (Segment Routing). En tant que client stateful, le routeur ajoutera un TLV (Type-Length-Value) de capacités stateful lors de l'ouverture d'une nouvelle session. De plus, nous pouvons configurer la délégation de tous les tunnels

actifs au PCE. Cette commande permet au contrôleur SDN de modifier les LSP existants tout en calculant de nouveaux chemins. Cela s'avère utile si le PCE souhaite réoptimiser les tunnels d'ingénierie de trafic. L'identifiant du speaker correspond à l'ID de l'interface de bouclage du routeur. Pour configurer la plage d'IDs de tunnel à utiliser pour les demandes d'instanciation du PCE stateful, nous utilisons la commande "auto-tunnel-pcc" en spécifiant l'ID de tunnel minimum et maximum. La réoptimisation est configurée pour un nombre de secondes spécifié, ce qui signifie que l'installation de nouveaux LSP avec de nouveaux labels après la réoptimisation du tunnel se produira dans le délai spécifié en secondes.

```
mpls traffic-eng
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 pce
  peer source ipv4 1.1.1.1
  peer ipv4 192.168.56.105
  !
  segment-routing
  logging events peer-status
  stateful-client
   instantiation
   cisco-extension
  !
 !
 logging events all
 auto-tunnel pcc
  tunnel-id min 1 max 99
 !
 reoptimize timers delay installation 0
!
segment-routing
!
end
```

Figure 3.15 : segment-routing/stateful-client configuration.

Tous les routeurs s’ont été vu attribués un segment-ID (NODE-SID) au niveau de leurs adresses de loopback respectives.

```
interface Loopback0
 circuit-type level-2-only
 address-family ipv4 unicast
  prefix-sid absolute 17001
```

Figure 3.16 : node SID 17001 PE1.

- Voilà les segment-ID pour chaque routeur :

17002 pour XRV2 / 17003 pour XRV3/ 17004 pour XRV4 /17005 pour PE2

Dans ce réseau, nous avons désigné PE1 comme speaker BGP chargé de redistribuer toutes les informations IGP vers OpenDaylight.

Les routeurs XRV2, XRV3 et XRV4 ont une configuration simple des interfaces ainsi que d'ISIS. Il est nécessaire d'activer MPLS-TE sur ces routeurs principaux. La configuration BGP est présentée dans la figure ci-dessous. Tout comme pour IS-IS, il est d'abord nécessaire d'ouvrir une instance BGP. Nous avons également spécifié l'adresse IP de la boucle du routeur en tant qu'identifiant du routeur. Le voisin BGP correspond au contrôleur SDN, qui appartient à un AS distant.

3.6 Configuration d'Opendaylight

Dans ODL, le module BGP qui est placé '/etc/opendaylight/karaf' dans le fichier 41-bgpexample.xml doit être reconfiguré. Dans la ligne 81, nous avons spécifié L'interface de gestion du speaker BGP (PE1)

```
78          <module>
79              <type xmlns:prefix="urn:opendaylight:params:xml:ns:yang:controller:bgp:rib:impl">prefix:bgp-peer</type>
80              <name>example-bgp-peer</name>
81              <host>192.168.56.200</host>
82              <holdtimer>180</holdtimer>
83              <retrytimer>10</retrytimer>
84              <peer-role>ibgp</peer-role>
85              <rib>
```

Figure 3.17 : BGP speaker pe1 address.

3.7 MPLS-TE et SR-TE Tunnel Setup avec OpenDayLight

Pour établir un nouveau tunnel MPLS, il est nécessaire d'envoyer une commande REST au module PCEP situé à l'intérieur d'ODL (OpenDaylight) et de demander l'ajout d'un LSP (Label Switched Path). À l'aide de l'application Postman, il est nécessaire de configurer les paramètres pour établir la connexion avec ODL et d'envoyer le modèle de données approprié au format XML ou JSON. Un exemple de création de tunnel PCEP est présenté ci-dessous :

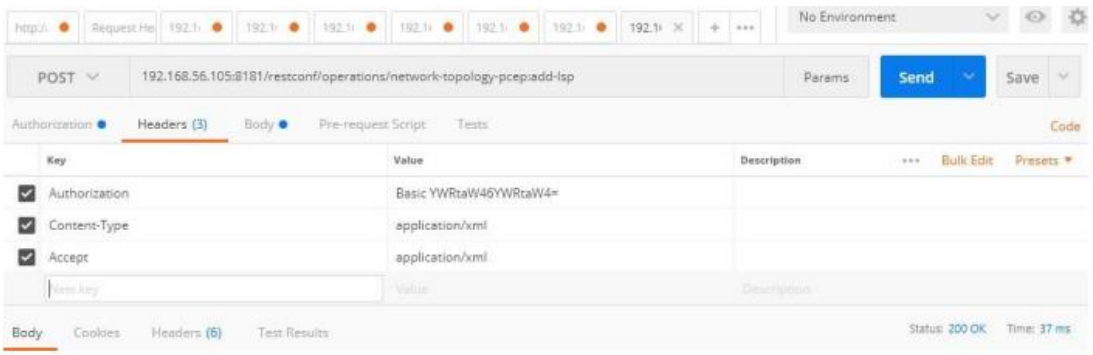


Figure 3.18 : Application postman.

Tout d'abord on selectionne cette commande

*192.168.56.105:8181/restconf/operations/network-topology-pcep:add-lsp * A laction post et le envoye en module ODL.

Les paramètres de connexion doivent être définis comme suit :

• **Autorisation** : nom d'utilisateur et mot de passe de l'ODL qui est admin/admin par défaut.

• **header> content-type** : application/xml.

• **header > accept** : application/xml.

Pour remplir le corps de notre message, nous devons définir l'entrée et la sortie du tunnel, ainsi que l'ERO (Explicit Route Object) indiquant les nœuds à traverser pour ce LSP (Label Switched Path). L'exemple suivant illustre l'ajout d'un tunnel LSP du nœud PE1 au nœud PE2, en passant par un chemin explicite comprenant les routeurs

PE1 >XRV3 > XRV4 > PE2

1. **Les modification dans le fichier xml :**

✓ La ligne 2 définit l'adresse IP du nœud PCEP auquel ODL appliquera la configuration

✓ La ligne 6 délègue le contrôle de ce LSP au PCE qui est ODL, donc que ce tunnel ne peut pas être supprimé ou modifié par CLI sur le routeur.

```
<input xmlns="urn:opendaylight:params:xml:ns:yang:topology:pcep">
<node> pcc://1.1.1.1</node>
<name>test15</name>
<arguments>
<lsp xmlns="urn:opendaylight:params:xml:ns:yang:pcep:ietf:stateful">
<delegate>true</delegate>
<administrative>true</administrative>
</lsp>
<endpoints-obj>
<ipv4>
<source-ipv4-address>1.1.1.1</source-ipv4-address>
<destination-ipv4-address>5.5.5.5</destination-ipv4-address>
</ipv4>
</endpoints-obj>
<ero>
<subobject>
<loose>false</loose>
<ip-prefix>192.168.13.1/30</ip-prefix>
</subobject>
<subobject>
<loose>false</loose>
<ip-prefix>192.168.34.1/30</ip-prefix>
</subobject>
<subobject>
<loose>false</loose>
```

```
subobject>
loose>false</loose>
ip-prefix>192.168.42.1/30</ip-prefix>
/subobject>
/ero>
/arguments>
network-topology-ref xmlns:topo="urn:TBD:params:xml:ns:yang:network-topology">/topo:network-topology/topo:topology[topo:topology-id="pcep-topology"]</network
  -topology-ref>
/input>
```

Figure 3.19 : Label switching path de PE1 a PE2.

2. Vérification :

Pour vérifier le tunnel à créer correctement, il faut le tester en insérant la commande "show mpls traffic-engineering tunnels ", comme sur la figure ci-dessous :

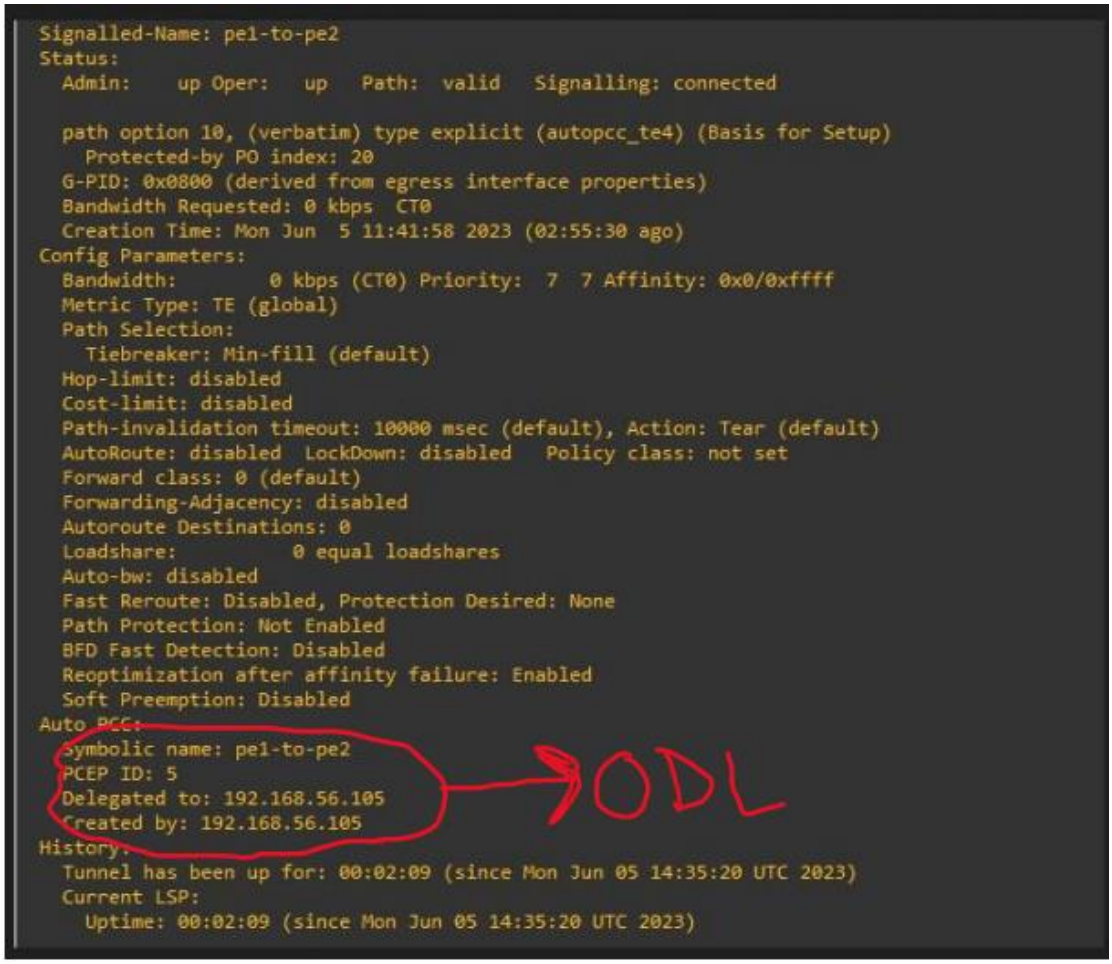


Figure 3.20 : Tunnel PE1-PE2.

Comme on remarque le controleur ODL a réalisé ce tunnel PE1-PE2

3.8 Segment Routing

Pour ajouter un nouveau tunnel de routage par segment, le processus est similaire à la création d'un tunnel MPLS. Nous utilisons l'application Postman avec les mêmes paramètres de connexion et envoyons la configuration au module PCEP d'ODL. Cependant, la différence réside dans le fait que, pour ajouter des tunnels SR, nous devons spécifier la destination et l'itinéraire du tunnel en utilisant des numéros SID (Segment Identifier). Dans l'exemple suivant, j'ai ajouté un chemin SR depuis PE1 en tant que source jusqu'à PE2 en tant que destination, en spécifiant explicitement le passage par XRV3. Au sein de la partie centrale du réseau, dans ce scénario, lorsqu'un routeur de cette partie reçoit un paquet, et qu'il ne prend pas en charge le routage de segment, il achemine le paquet en se basant sur l'algorithme du chemin le plus court

vers l'adresse IP correspondant au prochain saut défini pour le tunnel. Vous pouvez envoyer cette configuration à OpenDaylight de la manière suivante :

```
<subobject>
  <loose>false</loose>
  <sid-type xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">ipv4-node-id</sid-type>
  <m-flag xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">true</m-flag>
  <sid xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">17001</sid>
  <ip-address xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">192.168.13.1</ip-address>
</subobject>
<subobject>
  <loose>false</loose>
  <sid-type xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">ipv4-node-id</sid-type>
  <m-flag xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">true</m-flag>
  <sid xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">17003</sid>
  <ip-address xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">192.168.34.1</ip-address>
</subobject>
<subobject>
  <loose>false</loose>
  <sid-type xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">ipv4-node-id</sid-type>
  <m-flag xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">true</m-flag>
  <sid xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">17004</sid>
  <ip-address xmlns="urn:opendaylight:params:xml:ns:yang:pcep:segment:routing">192.168.45.1</ip-address>
</subobject>
</ero>
```

Figure 3.21 : Création tunnel basé sur les SID.

Nous avons spécifié explicitement qu'il doit passé par les routeurs ayant comme préfixe 17001-17003- 17004

3.9 Conclusion

Ce travail a été réalisé dans le but d'étudier le paradigme de routage source appelé Segment Routing et de le comparer à l'ingénierie du trafic MPLS. Dans un premier temps, nous avons examiné le Segment Routing de manière générale et souligné ses avantages dans le contexte des réseaux définis par logiciel (SDN). L'implémentation a consisté à créer un réseau dans GNS3, configurer le contrôleur SDN et établir sa

connexion au réseau, ainsi que créer des tunnels MPLS-TE et des tunnels de routage par segment à l'intérieur du réseau en utilisant le contrôleur SDN**.**

L'un des principaux objectifs de ce travail était d'utiliser l'émulateur de réseau GNS3 en tant que plateforme gratuite présentant peu d'inconvénients par rapport aux autres méthodes précédemment utilisées par d'autres chercheurs.

Dans cette étude, j'ai présenté deux méthodes différentes pour obtenir des numéros SID (Segment Identifier) : la première consiste à obtenir les numéros SID directement à partir des routeurs, tandis que la deuxième consiste à extraire les numéros SID à partir de la base de routage BGP (Border Gateway Protocol) dans OpenDayLight. Ces numéros SID peuvent être utilisés comme paramètre clé pour toute application liée au routage par segment. Pour les travaux futurs, il serait possible d'utiliser ces numéros SID pour développer une application graphique faisant partie de l'orchestrateur de réseau, permettant ainsi l'exploitation et la maintenance des tunnels de routage par segment. En utilisant GNS3 comme plateforme gratuite et bénéficiant de sa fonctionnalité permettant de l'exécuter sur différents ordinateurs en laboratoire, tout en ayant la possibilité de les connecter via un commutateur matériel, il devient possible de créer un réseau étendu afin d'évaluer différents scénarios aussi vastes que les réseaux réels disponibles à travers le monde.

Conclusion Générale

L'infrastructure du réseau MPLS/SDN devient de plus en plus complexe en raison de l'augmentation du trafic, ce qui entraîne une consommation élevée de stockage et des coûts de déploiement élevés. Pour résoudre ces problèmes, une solution récente appelée routage par segment a été introduite par l'IETF (Internet Engineering Task Force). Cette solution combine le concept du routage par segment, les protocoles de routage IP/MPLS et les fonctionnalités SDN pour offrir un réseau optimisé, flexible, facile à mettre en œuvre et sécurisé.

Le principe du routage par segment est d'acheminer le trafic entre les routeurs du réseau Internet en utilisant des identifiants de segment (SIDs) encapsulés dans l'en-tête des paquets, en se basant sur la commutation des paquets du réseau et le contrôle MPLS/SDN. De nombreux fournisseurs informatiques, dont Ericsson, mettent actuellement en œuvre le routage par segment pour améliorer les réseaux MPLS.

Notre objectif était d'étudier le routage par segment, de comprendre son principe d'acheminement du trafic en utilisant des SIDs, et de tester ses capacités d'ingénierie du trafic dans les réseaux MPLS. Nous avons construit un environnement de test virtualisé à l'aide de l'outil GNS3, ce qui nous a permis d'atteindre nos objectifs. Cependant, le routage par segment et les réseaux MPLS/SDN sont des technologies nouvelles, vastes et complexes, ce qui rendait difficile la compréhension de certaines notions avec la documentation existante au début de notre étude. Grâce au soutien de nos encadreurs, nous avons pu acquérir et renforcer nos connaissances théoriques et pratiques sur l'acheminement du trafic dans les réseaux MPLS/SDN avec la solution du routage par segment. Nous avons également appris à simuler et à programmer le routage dans un réseau en utilisant différents types de routage sous GNS3. De plus, nous avons découvert et utilisé deux nouveaux outils, Opendaylight et Postman, qui ont contribué à optimiser la gestion de notre réseau simulé.

Dans une perspective future, nous envisageons d'améliorer notre travail en utilisant des ressources plus performantes afin de nous rapprocher davantage d'un réseau réel. Nous aimerions également tester notre simulation avec de vrais routeurs pour vérifier l'efficacité de cette solution dans un environnement réel.

Références

[1] : HAMIDOUCHE Yamina, Implémentation d'une solution Segment Routing sur un environnement basé MPLS/SDN, mémoire Université des Sciences et de la Technologie Houari Boumediene, 22/09/2021, 59 p.

[2] : La Rédaction TechTarge, Table de routage, juin 2016 <https://www.lemagit.fr/-definition/Table-de-routage>.

[3] : *M_Amine*, Différence entre le Routage Statique et Dynamique, *2022-2-6 18:51:16*, < https://forum.huawei.com/enterprise/fr/index.html>.

[4] : Exelib.net, Configuration des routes statiques et par défaut IPv4, 17/12/15 <https://www.exelib.net/routage/configuration-des-routes-statiques-et-par-defaut-ipv4.html >.

[5] : <https://www.mcours.net/cours/pdf/leilclic1/leilclic366.pdf >.

[6] : <http://cisco.ofppt.info/ccna2/course/module7/7.1.4.2/7.1.4.2.html>.

[7] : N.Salmon, Routage RIP, article, 19 juillet 2011, 16 p.

[8] : Nina Pelagie BEKONO, Impact du changement du protocole de routage dans un réseau, mémoire UNIVERSITÉ CLERMONT-AUVERGNE, décembre 2018, 188 p.

[9] : nsi4noobs. (n.d.), c3_tnsi_routage.pdf, nsi4noobs.

[10] : Techno-Science.net, < https://www.techno-science.net/glosaire-definitio>.

[11] : EL MEHDI SKIA, Protocoles de routage dynamique, Dec 06, 2019, 7 p.

[12] : MEGRI Hmanou, Etude, Conception et Evaluation d'une Architecture MPLS/VPN Désignée pour une Infrastructure Operateur, 2014/2015, 87 p.

[13] : RAMAHAROBANDRO Rahasina Fenomanjato Mariah, ETUDE DES PERFORMANCES DES MECANISMES DE QUALITE DE SERVICE DANS UN RESEAU MPLS AVEC TRAFFIC ENGINEERING, 2012 / 2013, 109 p.

[14]: J. Doyle, "Routing TCP/IP – Volume I", Cisco Press, 2001.

[15] : Tangup, F-R. ''Conception et déploiement de la technologie MPLS dans un réseau Métropolitain'', Mémoire d'Ingénieur, <https://www.memoireon-line.com/-09/13/74-05/Conception-et-deploiement-de-la-technologie- MPLS-dans-un-reseau-metropo-litain.html>, Consulté le : 10 Juin 2018.

[16] :O'Reilly. MPLS Fundamentals : Label Distribution Protocol (LDP). O'Reilly, <https://www.oreilly.com/library/view/mpls-fundamentals/1587051974/158705197-4_-ch02lev1sec5.html >.

[17] : Erdem, What is a label-switched path, 02-05-2016 12:13, <https://community.juniper.net/browse/blogs/blogviewer?blogkey=948b0114-04aa-4cee-a92c-b34c874635ff>.

[18]: Huawei Technologies, what Is MPLS, 2019-12-18, <https://support.huawei.com/enterprise/fr/doc/EDOC1100118961#EN-US_TOPIC_0211261034>.

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

[20]: Mishal Roomi, advantages and disadvantages of MPLS, august 10,2021, <https://www.hitechwhizz.com/2021/08/5-advantages-and-disadvantages-limitations-benefits-of-mpls.html>.

[21]: "RFC 2208 : RSVP Version 1 Applicability Statement, Some Guidelines on Deployment".

[22] : Filsfils Clarence, Segment Routing Architecture, 2018-07, <https://datatracker.ietf.o-rg/doc/rfc8402/>.

[23] : <https://fr.theastrologypage.com/routing-metric>.

[24] : OULD LAMARA SAMI, IMPLEMENTATION DU SDN DANS UNE STRUCTURE IP/MPLS, 12/07/2018, UNIVERSITE DE MOULOUD MAMMERI DE TIZI-OUZOU, 120p.

[25]: Huawei, Overview of Segment Routing MPLS - New IP Technologies – Huawei, 2020/10/10, <https://support.huawei.com/enterprise/en/doc/EDOC10-00173015/4e8b-f78b/overview-of-segment-routing-mpls>.

[26] : Techno-science, Routeur - Définition et Explications, https://www.techno-science.net/glossaire-definition/Routeur.html>.

[27]: J. Moy, OSPF Version 2, April 1998, <https://www.ietf.org/r-fc/rfc2328.txt>.

[28] : G. Pujolle, Les Réseaux, 6EME ÉDITIONS EYROLLES, 2008.

[29] : Mokhtari Abdelghani Issam Eddine, Implémentation de la VoIP sur une architecture MPLS/VPN, Université –Ain Temouchent- Belhadj Bouchaib, 2020/2021, 82p.

[30] : MAHMOUDI azeddine, Extension du réseau MPLS via la technologie VSAT, Université Mouloud Mammeri de Tizi-Ouzou, 2017/2018,110p.

[31] : < https://www.perimeter81.com/fr/glossary/modele-osi#h-quelle-est-la-d-finition-et-la-signification-du-mod-le-osi>.

[32] : <https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/Les_mod-%C3%A8les_OSI_et_TCP#Mod%C3%A8le_TCP/IP>.

[33] : Juniper Networks. qu'est-ce que SR. 2019. Consulté le Mai 2021.

[34]: ETSI, "Network Functions Virtualisation (NFV), Architectural Framework", GS NFV 002 (v. 1.1.1), 2013.

[35]: Azodomolky, S. (2013). Software Defined Networking with Openflow. Packt Publishing. Premiére édition. Birmingham, Royaume uni.

[36] : M.Chiosi et all. "Network Functions Virtualisation - An Introduction, Benefits, Enablers, Challenges and Call for Action", SDN and OpenFlow World Congress, Darmstadt-Allemagne, vol. 48, pp.5, October 22-24, 2012.

[37]: Open Networking Foundation. (2013). Software-Defined Networking (SDN) Definition. Consulté sur : <https://www.opennetworking.org/sdn-resources/sdn-definition>.

[38]: Haleplidis Evangelos, Software-Defined Networking (SDN): Layers and Architecture Terminology, January 2015, <https://datatracker.ietf.org/doc/rfc7426>.

[39]: Ana Kos, SEGMENT ROUTING PRINCIPLES AND APPLICATIONS FOR SDN, POLITECNICO DI MILANO, 2013-2015,110p.

[40]: R. Masoudi et A. Ghaffari, « Software defined networks : A survey », J. Netw. Comput. Appl.,vol. 67, p. 1025, mai 2016.

[41]: PCEP Configuration | Juniper Networks, <https://www.juniper.net/documentation/fr/fr/software/junos/mpls/topics/topic-map/pcep-configuration.html>.

[42] : HuaweiTechnicalGuide. Qu'est-cequempls. <https://support.huawei.com/enterprise/ en/doc/EDOC1100118961, 2019. Consulté le Mai 2021>.

[43] : Claude Servin «" Réseaux et Télécoms" Préface de Jean-Pierre Arnaud » Livre -2003- Edition Dunod.

[44] : MPLS Concepts, <https://www.10gea.org/images/CISCO-MPLS-Concept >- Consulté le : 05 Juin 2018.

[45] : Enric Caceres, « Le Protocole OpenFlow dans l'Architecture SDN », EFORT 2016.

[46] : FRAMEIP.COM, Protocole MPLS, 2022-04-11, https://www.frameip.com/mpls/ .

[47] : Houas Dihia, etude conception et implémentation du segment routing sur un réseau IP/MPLS ,2020/2021,88p.

[48]: « The Road to SDN - ACM Queue ». [En ligne]. Disponible sur <https://queue.acm.org/detail.cfm?id=2560327>. [Consulté le: 27-août-2019].

[49]: N. McKeown et al.,« OpenFlow: Enabling innovation in campus networks» Comput.Commun. Rev., vol. 38, p. 69074, avr. 2008