REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

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

Mémoire de Master

Présenté par

RAHIL Djedjiga Sabrina

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Routage de segments sur un réseau IP-MPLS

Soutenu le ...../...../ 2022 devant le jury composé de :

Dr.Yassine	**MERIAH**	**MCA**	**UMBB**	**Président**
Dr. Yasmine	**GUERBAI**	**MCA**	**UMBB**	**Examinateur**
Dr.MAHDI	**ISMAHAN**	**MCB**	**UMBB**	**Rapporteur**

Année Universitaire : 2021/2022

Remerciements

Je remercie Dieu le tout puissant de m'avoir donné la santé et la volonté d'entamer et de terminer ce modeste travail, ainsi je tiens à exprimer ma profonde gratitude à Madame ISMAHAN MAHDI enseignante à l'Université M'Hamed Bougera de Boumerdès, sans tout autant oublier les membres du jury pour l'évaluation de ce mémoire de fin d'études.
Enfin, toutes mes pensées vont vers Mr ADDOUM Azeddine pour sa contribution et ses compétences dans le domaine professionnel.

Dédicace

Je dédie ce mémoire de fin d'études :

À mes chers parents,
À mon frère IDIR et ma sœur NASSIMA,
Pour leurs affections, leurs soutiens et encouragements pour la réussite de mes études.

الملخص:

تم اعتبار شبكة بروتوكول الإنترنت/تبديل طبقة البروتوكول المتعددة (IP/MPLS) لفترة طويلة معيارًا بلا منازع لمواجهة قيود خدمات التوجيه ولكن استخدامها محدود جدًا بسبب تعقيدها وافتقارها إلى قابلية التوسع لأن عدد أجهزة الشبكة وكمية حركة المرور تزداد بسرعة بمرور الوقت. ومع ذلك، فإن التطور السريع للسوق يمكن أن يمنح ميزة لـ SR-MPLS، فإن تنفيذه في الشبكة له مصلحة في تحسين قلب شبكة MPLS نحو اتجاه جديد أبسط وأكثر كفاءة مع تعقيد أقل دون الحاجة إلى إشارات البروتوكولات والتي تفتح طرقًا جديدة لمرونة وقابلية التوسع للشبكة.

الكلمات المفتاحية: الشبكة - IP/MPLS- SR-MPLS.

RÉSUMÉ :

Le réseau IP/MPLS (Internet Protocol/Multiprotocol Layer Switching) a été considéré pendant longtemps comme étant le standard incontesté pour répondre aux contraintes de services routage mais son usage est très limité par sa complexité et son manque de scalabilité car le nombre de périphériques réseau et la quantité de trafic augmentent rapidement au fil du temps. Cependant, le développement rapide du marché pourrait bien donner l'avantage au SR-MPLS, sa mise en place dans le réseau à l'intérêt d'améliorer le cœur de réseau MPLS vers une nouvelle tendance plus simple et plus performante avec moins de complexité sans avoir besoin de protocoles de signalisation et ce qui ouvre de nouvelles voies de flexibilité et évolutivité du réseau.

MOTS-CLEFS : Réseau -IP/MPLS- SR-MPLS.

Abstract :

IP/MPLS (Internet Protocol/Multiprotocol Layer Switching) has long been considered the undisputed standard for meeting routing service constraints but its use is severely limited by its complexity and lack of scalability as the number of network devices and the amount of traffic increases rapidly over time. However, the rapid development of the market may well give the advantage to SR-MPLS, its implementation in the network has the interest to improve the MPLS core network towards a new trend of simpler and more performing with less complexity without the need of signalling protocols and which opens new ways of flexibility and scalability of the network.

KEYWORDS: Network -IP/MPLS- SR-MPLS

Table des matières

Table des matières

Chapitre 2 :Étude théorique de la technologie routage de segment

Liste des figures

Liste des tableaux

Liste des abréviations

AS Système autonome.
BGP Border Gateway Protocol.

CE Customer Edge.

CR-LDP Constraint based Routing LDP.

E-BGP external-BGP.

EGP Exterior Gateway Protocol.

FEC Forwarding Equivalency Classes.

FIB Forwarding Information Base.

I-BGP internal-BGP.

IntServ: Integrated Services.

IETF Internet Engineering TaskForce.

IGP Interior Gateway Protocol.

ISO International Organization for Standardization.

OSPF Open Shortest Path First.

L3VPN Layer3VPN.

LDP Label Distribution Protocol.

LER Label Edge Router.

LFIB Label Forwarding Information Base.

LIB Label Information Base.

LSP Label Switch Path.

LSR Label Switch Router.

MP-BGP Multi Protocol BGP.

MPLS MultiProtocol Label Switching.

MPLS-TE MPLS - Traffic Engineering.

P Provider Router.

PE Provider Edge Router .

QOS Quality of Service.

RD Route Distinguisher.

RSVP Ressource Reservation Protocol.

RSVP-TE Resource Reservation Protocol-Traffic Engineering.

RT Route Target.

SID Segment ID.

SPRING Source Packet Rou-ting in Networking.

SR Segment Routing.

SRGB Segment Routing Global Block.

TTL Time To Live.

VRF Virtual Routing and Forwarding.

VPN Virtual Private Network.

VRF Virtual Routing and Forwarding.

Introduction Générale

Introduction générale

Depuis quelques années, nous assistons à une évolution rapide dans le monde de la communication. En effet, Internet est devenu une partie intégrante dans la vie des personnes et des entreprises, les nouvelles technologies de l'information et les nombreuses applications telles que les appels VOIP (Voice Over Internet Protocol), la télé robotique, les jeux interactifs, les transactions bancaires, ..., etc font que le nombre d'utilisateurs en croissance permanente ne cesse de s'agrandir.

Aujourd'hui, le réseau Internet s'est transformé en une architecture de communication globale offrant des services en temps-réel, qui ont des contraintes de qualité de service beaucoup plus strictes que les services traditionnels. Cette augmentation du trafic sur les réseaux a mis en évidence l'absolue nécessité d'en optimiser l'usage.

Les protocoles de routage dynamiques ne permettent que la mise en place de règles assez basiques reposant uniquement sur l'adresse de destination et n'offrent pas nativement la capacité de réaliser une ingénierie de trafic évoluée. Pour cela les opérateurs doivent déployer des réseaux à haut débit avec des technologies de transport de données numériques évoluées et plus adaptées aux exigences des services temps réels.

Le MultiProtocol Label Switching (MPLS) est parmi les technologies largement déployées dans les réseaux d'opérateurs. Cette technologie a permis la conception des réseaux multiservices capables de transporter aussi bien les flux de données que les flux temps réel (voix, vidéo). Cette dernière est capable de satisfaire les diverses exigences des différents flux qu'elle transporte jusque-là grâce à la mise en place des actions d'ingénierie de trafic (réservation de bande passante, définition des chemins et des contraintes).

Cependant, le réseau MPLS tend à arriver à ces limites vu la complexité des protocoles utilisés, d'ingénierie de trafic, d'administration et les problèmes de scalabilité. Et pour ces raisons-là, la technologie de routage de segments a vu le jour en offrant des modèles de services simples et évolués et surtout adaptés à l'ingénierie du trafic.

Dans ce cadre, nous nous sommes intéressés à étudier la technologie routage de segments sur réseau IP/MPLS afin d'offrir une meilleure optimisation et plus de flexibilité et de scalabilité au réseau.

Ce document est scindé en trois chapitres qui sont les suivants :

Dans le premier chapitre, nous avons donné un aperçu sur les notions du routage IP et sur la technologie IP-MPLS .

Dans le deuxième chapitre, nous avons présenté la technologie routage de segments sur un réseau MPLS, son fonctionnement de ses différentes caractéristiques.

Dans le troisième chapitre, la mise en fonctionnalité du routage de segment sur un réseau MPLS (SR-MPLS) et à l'interprétation des résultats obtenus lors de sa réalisation sous EVE-NG serons présentés.

Finalement nous clôturons par une conclusion générale.

Chapitre 1 : Notions sur le routage et la technologie IP-MPLS

1.1 Introduction

Dans ce chapitre, nous abordons deux principales sections : la première est consacrée pour les notions sur le routage IP, et la seconde présente la technologie IP-MPLS

1.2 Notions sur le routage IP

1.2.1 Définition de routage

Il s'agit d'un processus de sélection d'un chemin à travers un ou plusieurs réseaux pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires, par ex. réseau téléphonique, réseaux de données électroniques (Internet) et réseaux de transport.

1.2.2 Le routage sur IP

Le routage IP est le processus d'envoi de paquets d'un hôte sur un réseau à un autre hôte sur un autre réseau distant. Ce processus est généralement effectué par des routeurs(voir annexe). Les routeurs examinent l'adresse IP de destination d'un paquet, déterminent l'adresse du saut suivant et transfèrent le paquet. Les routeurs utilisent des tables de routage pour déterminer l'adresse du prochain saut vers laquelle le paquet doit être transmis **[01].**

Fig I.1 Architecture du réseau IP

1.2.3 Mécanisme de routage

La première étape du routage IP consiste à sélectionner le meilleur chemin pour le transport des données. La question qui se pose ici est de savoir comment sélectionner ce chemin. Les tables de routage sont la réponse à cette question. Les routeurs maintiennent des tables de routage qui incluent des informations sur la suite. **[02]**

• Réseaux directement connectés.

• Réseaux connectés à distance.

• Informations sur le réseau, c'est-à-dire la source d'informations, l'adresse réseau, le masque de sous-réseau, l'adresse IP du saut suivant.

Le routeur lit l'adresse IP de destination à partir de l'en-tête des paquets entrants et la vérifie pour trouver l'adresse réseau de destination. Ensuite, il examine sa table de routage et trouve une adresse IP qui est l'adresse d'un périphérique directement connecté et transmet le paquet entrant à cette route. Cet appareil directement connecté dispose des informations sur l'hôte de destination. Si l'adresse IP de destination n'est pas trouvée dans la table de routage du routeur, le paquet est acheminé vers une route par défaut. La route par défaut est une entrée de la table de routage utilisée pour transférer les paquets pour lesquels un saut suivant n'est pas explicitement répertorié dans la table de routage**.**

1.2.4 Les types de routages

1.2.4.1 Le routage statique

Le routage statique est un mécanisme de routage géré par le protocole Internet (IP) et qui dépend de tables de routage configurées manuellement. Les routeurs qui utilisent le routage statique sont appelés routeurs statiques.

Les routeurs statiques sont généralement utilisés dans les petits réseaux qui ne contiennent que quelques routeurs ou lorsque la sécurité est un problème. Chaque routeur statique doit être configuré et géré séparément car les routeurs statiques n'échangent pas d'informations de routage entre eux. **[03]**

1.2.4.2 Le routage dynamique

Le routage dynamique est le processus de sélection du meilleur chemin qu'un paquet de données doit suivre à travers un réseau pour atteindre une destination spécifique. Le routage dynamique permet aux routeurs de sélectionner des chemins en fonction des changements de configuration du réseau logique en temps réel. Dans le routage dynamique, le protocole de routage fonctionnant sur le routeur est responsable de la création, de la maintenance et de la mise à jour de la table de routage dynamique. Dans le routage statique, toutes ces tâches sont effectuées manuellement par l'administrateur système. **[04]**

1.2.5 Les protocoles de routage

Les protocoles de routage sont des mécanismes par lesquels les informations de routage sont échangées entre les routeurs afin que les décisions de routage puissent être prises. Son but est d'aider les routeurs à créer et à maintenir des tables de routage. Sur Internet, il existe trois types de protocoles de routage couramment utilisés. Ce sont : le vecteur de distance, l'état du lien et le vecteur de chemin. Les protocoles de routage connus sont Routing Information

Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP) et Border Gateway Protocol (BGP).

1.2.5.1 Protocoles de routage interne IGP

Est un protocole de mise à jour de route dynamique utilisé entre des routeurs qui s'exécutent sur des hôtes TCP/IP au sein d'un système autonome unique (voir annexe). Les routeurs utilisent ce protocole pour échanger des informations sur les routes IP **[05].**

1.2.5.2 Protocoles de routage à vecteur de Distance

Les routeurs utilisent des algorithmes (tels que Bellman-Ford) pour partager périodiquement des informations de routage avec leurs routeurs voisins immédiats de manière omnidirectionnelle. Chaque récepteur ajoute sa valeur de distance (vecteur de distance) à la table et la transmet à ses voisins immédiats. Le processus aboutit à une table cumulative utilisée par chaque routeur pour mettre à jour sa propre table de routage et pour obtenir des informations sur la distance administrative aux autres périphériques réseau **[02].**

Les protocoles utilisant cette technique de routage sont :

• Protocole d'informations de routage (RIP).

• Protocole d'informations de routage version 2 (RIPv2).

• Protocole de routage de passerelle intérieure (IGRP).

Le processus prend un certain temps en fonction du nombre d'appareils participants.

Par conséquent, en cas de défaillance de la liaison, le trafic réseau peut en pâtir. Souvent utilisée pour les grands réseaux, cette technique n'est pas recommandée pour les petits réseaux car les informations de routage transmises par les routeurs peuvent en fait avoir un volume plus élevé que le trafic utilisateur réel. Les routeurs ignorent la topologie physique du réseau dans le routage à vecteur de distance.

1.2.5.3 Protocoles de routage à état de lien

Le routage à état des liens est la deuxième famille de protocoles de routage. Alors que les routeurs à vecteur de distance utilisent un algorithme distribué pour calculer leurs tables de routage, le routage à état de liens utilise des routeurs à état de liens pour échanger des messages qui permettent à chaque routeur d'apprendre la topologie complète du réseau. Sur la base de cette topologie apprise, chaque routeur est alors capable de calculer sa table de routage en utilisant le calcul du chemin le plus court **[06].**

- Caractéristiques des protocoles de routage à état des liens :
    - **Paquet d'état de liaison** : un petit paquet qui contient des informations de routage.
    - **Base de données d'état des liens** : une collection d'informations recueillies à partir du paquet d'état des liens.
    - **Algorithme du chemin le plus court en premier (algorithme de Dijkstra) :** un calcul effectué sur la base de données aboutit au chemin le plus court.
    - **Table de routage** : une liste de chemins et d'interfaces connus.

OSPF (Open Short est Path First) et IS-IS (Inter médiate System to Inter médiate System) sont deux exemples de protocoles de routage à état de liaison.

- **Le protocole OSPF (Open Shortest Path First) :** c'est un protocole de routage à état de lien crée en 1988 par l'IETF. C'est à l'heure actuelle l'IGP (Interior Gateway Protocol) le plus répandu. OSPF est un protocole libre.
- **Le protocole IS-IS :** c'est comme OSPF un protocole interne de routage à états de liens. Cela signifie que chaque routeur transmet l'état de ses liaisons dans le but de dresser une carte de l'état du réseau puis de construire sa table de routage. Comme OSPF, IS-IS est également un protocole de routage hiérarchique permettant de définir plusieurs domaines (zones) de routage et ainsi réduire la taille des tables ainsi que le temps de convergence.

1.2.5.4 Protocoles de routage externe EGP

Est un protocole de routage utilisé pour trouver des informations sur le chemin du réseau entre différents réseaux. Il est couramment utilisé sur Internet pour échanger des informations de table de routage entre deux hôtes de passerelle voisins (chacun avec son propre routeur) **dans un réseau de systèmes autonomes**. Border Gateway Protocol (BGP) est le seul protocole de passerelle extérieure (EGP) à l'heure actuelle. **[05]**

- **BGP**

Permet d'échanger des informations de routage entre les AS. Le routage BGP gère les tables de routage entrantes et sortantes pour stocker les chemins de routage entrants et sortants. Chaque fois qu'un processus de routage est lancé, ces tables sont accessibles pour sélectionner un chemin et le système autonome qui doivent traversés pour atteindre la

destination. Le protocole BGP est utilisé par les Fournisseur d'Accès Internet (FAI) pour communiquer entre eux ou aux frontières extérieures des réseaux d'entreprise (différents AS). **[07]**

Il existe deux modes de fonctionnement de BGP :

- **IBGP** : utilisé à l'intérieur d'un Autonomous System ;
- **EBGP** : utilisé entre deux AS.

1.2.6 Les limites du réseau

Les réseaux IP ont bien fonctionné jusqu'à l'identification de plusieurs limitations clés, qui ont incité la mise en œuvre des **réseaux MPLS**. Ces limites sont :

- Les routeurs ont d'énormes tables de routage et ces tables augmentent avec chaque ajout de segments physiques au réseau
- Les services de priorité supérieure peuvent être fournis avant les services de priorité inférieure.
- Le concept de classe de service (CoS) n'est pas une fonctionnalité largement disponible dans le routage IP actuel et ne peut donc pas être utilisé.
- Le routage peut créer une congestion du réseau.

1.3 La technologie IP/MPLS

1.3.1 Présentation des réseaux MPLS

Multi Protocol Label Switching (MPLS) est un mécanisme de transport de données basé sur la commutation d'étiquettes ou « labels », qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie.

Les réseaux de transport basés sur le protocole IP ont montré leurs limites, le protocole IP fonctionne en mode non connecté ce qui signifie que les décisions de routages sont prises localement par chaque nœud. Les paquets d'un même flux peuvent prendre des chemins différents ce qui limite la tâche des opérateurs de télécommunications à transporter les paquets sans pouvoir garantir des fonctions de gestion plus avancées comme la possibilité de décider du routage en fonction de la qualité de service, du type de flux, ou du prix que le client paye, d'où l'intérêt du MPLS qui va apporter aux opérateurs réseaux la possibilité de gérer et d'optimiser le trafic tout en garantissant le respect de certaines contraintes (bande passante, délai, etc..).

L'objectif principal du groupe de travail MPLS est de normaliser une technologie de base qui intègre le paradigme de la transmission par commutation de labels avec le routage de couche réseau du modèle OSI.

Cette technologie est destinée à améliorer le ratio cout/performance du routage de couche réseau, à accroitre l'évolutivité delà couche réseau et à fournir une grande souplesse dans la remise des (nouveaux) services de routage, tout en permettant l'ajout de nouveaux services de routage sans modification du paradigme de transmission. Parmi ses avantages (MPLS) :

- Simplifier le traitement dans le cœur du réseau.
- Assurer n'importe quel transport.
- Support de la qualité de service.
- Ingénierie de trafic.
- Support des VPNs.
- Déroutage rapide (Fast reroute).

L'entête MPLS a une taille de 4 octets (32bits) et est composé par les champs suivants :

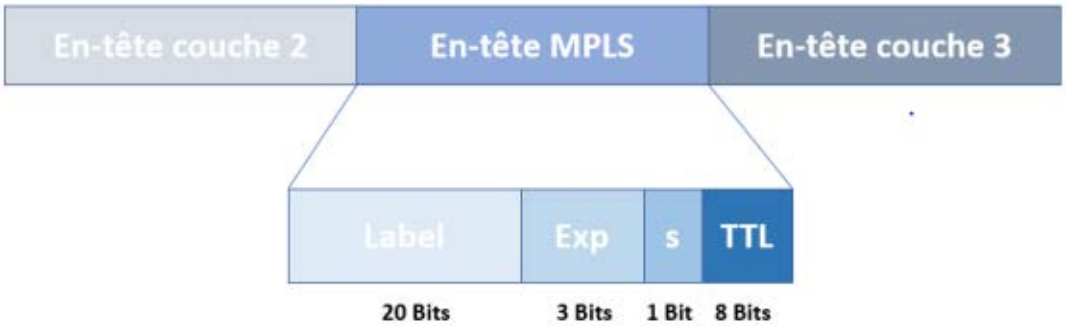


Fig I.2 Format du Label MPLS

- **Le champ (Label)** : sert à identifier la valeur numérique du label de 20 bits.
- **Le champ (Exp)** : il est composé de 3 bits. Ils sont utilisés pour la qualité de service.
- **Le champ S** : indique s'il y a empilement de labels (il est en fait commun d'avoir plus qu'un label attaché à un paquet). Cette notion sera reprise dans le paragraphe suivant. Le bit S est à 1 lorsque le label se trouve au sommet de la pile, à 0 sinon.

- **Le champ (TTL)** : codé sur 8 bits, il limite la durée de vie du paquet. Il est initialisé à une certaine valeur, puis décrémenté de un par chaque routeur qui traite le paquet. Lorsque ce champ atteint 0, le paquet est rejeté. Afin d'éviter les boucles de routage.

➢ ***Label Stack :***

Chaque paquet MPLS est susceptible de transporter plusieurs labels, formant ainsi une pile de labels, qui sont empilés et dépilés par les LSR. Cette possibilité d'empiler des labels désignés sous le terme de Label Stacking utilisé par le Traffic Engineering et MPLS/VPN. Lorsqu'un LSR commute un paquet, seul le premier label est traité.

Les applications suivantes l'exigent :

- **MPLS VPN** : MP-BGP (Multi Protocol Border Gateway Protocol) est utilisé pour propager un label secondaire en addition à celui propagé par LDP.
- **MPLS TE** : MPLS TE utilise RSVP TE (Ressource Réservation Protocol TE) pour établir un tunnel LSP (Label Switched Path). RSVP TE propage aussi un label en addition de celui propagé par LDP.

1.3.2 La structure fonctionnelle

Pour prendre en charge plusieurs protocoles, la structure fonctionnelle de la technologie MPLS est fondée sur deux plans principaux à savoir : le plan de contrôle et le plan le plan de données.

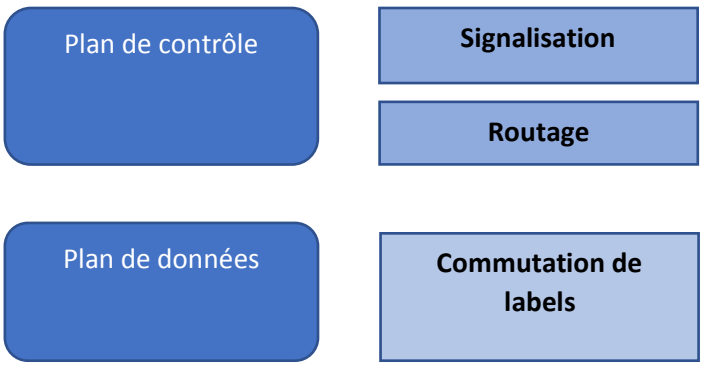


Fig I.3 Structure fonctionnelle du MPLS

1.3.2.1 Le plan de contrôle

Il est composé d'un ensemble des protocoles de routage classique et de signalisation. Il est chargé de la construction, du maintien et de la distribution des tables de routages et de commutation. Pour ce faire, le plan de contrôle utilise des protocoles de routage classique

tels qu'IS-IS ou OSPF afin de créer la topologie des nœuds du réseau MPLS et des protocoles de signalisation spécialement développés pour le réseau MPLS comme LDP, MP-BGP (utilisé par MPLS-VPN) ou RSVP (utilisé par MPLS-TE).

1.3.2.2 Plan de données

Le plan de données permet de transporter les paquets labélisés à travers le réseau MPLS en se basant sur les tables de commutations.

Le plan de données est indépendant des algorithmes de routages et d'échanges des labels et utilise une table de commutation appelée LFIB pour transférer les paquets labélisés avec les bons labels.

Cette table est remplie par les protocoles d'échange de label comme le protocole LDP. A partir des informations de labels apprises par LDP, les routeurs LSR construisent deux tables la LIB et la LFIB.

1.3.3 Le protocole de distribution de label LDP

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

1.3.3.1 Principe de connexion de LDP [07]

1) deux routeurs adjacents vont s'échanger des messages UDP de type "HELLO" pour s'informer mutuellement de leur présence.

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

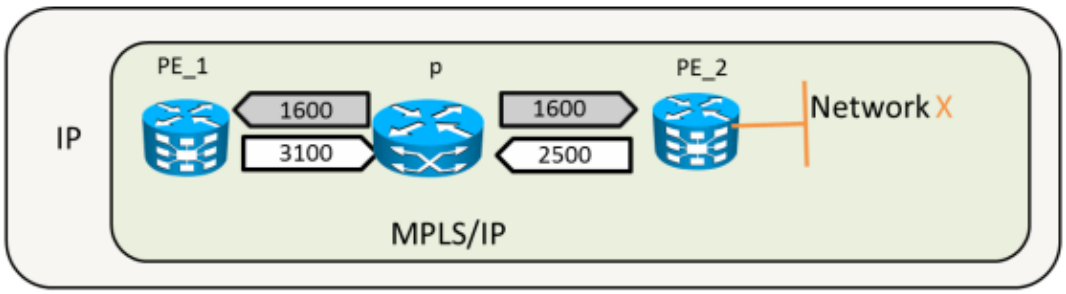
3) LDP commence la distribution des labels :

- avec le mode sollicité : un message "Label Request" est envoyé par l'Ingres LER vers l'Egress LER, ce dernier répond par un message "Label Mapping" qui contient un label.
- avec le mode non sollicité : l'Egress LER distribue directement les labels avec le message "Label Mapping", sans demande de l'Ingres LER par un message "Label Request".

1.3.4 Allocations et distribution de labels [08]

- Le protocole de routage IGP est utilisé pour construire des tables de routages dans tous les routeurs dans un réseau.

- Le protocole CEF va copier la table de routage dans une nouvelle table qui s'appelle FIB (Forwarding Information Base).
- Pour chaque routeur Le protocole LDP va allouer un label pour chaque destination dans la table LIB (Label Information Base) et distribuer ces labels aux voisins.
- Chaque routeur va enregistrer son label local ainsi les labels reçu en indiquant pour chacun le routeur annonceur dans une table (LIB).
- Chaque routeur va enregistrer le label d'entrée (In), le label de sortie (Out) et le saut suivant (Next Hop) qui conduit à la destination dans une table (LFIB)



FIB (P)

Network	Next Hop	Label
X	PE_2	2500

LIB (P)

Network	LSR	Label
X	Local	1600
X	PE_2	2500

LFIB (B)

In	Out	Next Hop
2500	1600	PE_2

Fig I.4 Allocation des labels

1.3.5 Principe de fonctionnement du MPLS

A l'entrée du réseau MPLS, les paquets IP se voient insérés un label par le routeur d'entrée INGRESS LER. Ces paquets labélisés sont ensuite commutés vers le cœur du réseau selon leur numéro de label. Ensuite, les routeurs MPLS du cœur de réseau (les LSR) commutent les paquets labélisés jusqu'au routeur de sortie (EGRSS LER) par changement de labels à chaque nœud. Un routeur LSR, recevant un paquet labélisé, se base sur la table LFIB pour transiter le paquet. A partir d'un label d'entrée (label local), il en déduit l'interface et le label de sortie (Out going interface et Outgoing tag) pour faire suivre les paquets.

Lors de l'arrivée du paquet au dernier routeur « EGRESS LER », ce dernier va retirer le label et transmettre le paquet à sa couche de niveau 3 (la couche réseau) qui va se charger du routage classique du paquet.

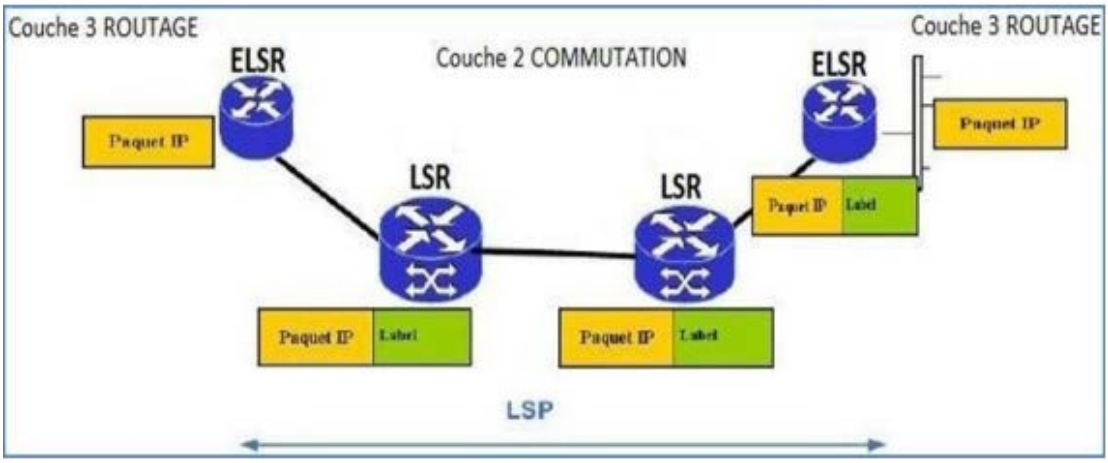


Fig I.5 Principe de fonctionnement du MPLS

1.3.6 Les applications du MPLS

1.3.6.1 Qualité de services (QoS) [08]

La QoS est la méthode qui permettra de garantir au trafic de données, quelle que soit sa nature, de prendre les meilleures conditions d'acheminement répondant à des exigences prédéfinies.QOS fixe notamment des règles de priorité entre différents flux.

MPLS permet à son tour de simplifier l'administration d'un cœur du réseau en ajoutant de nouvelles fonctionnalités particulièrement intéressantes pour la gestion de la QoS.

En MPLS la qualité de services peut être fournie par deux approches :

- ***1IntServ :*** utilise la réservation de ressources mise en place par RSVP. IntServ classifie les données par flux. En effet, chaque flux va être placé dans une file d'attente séparée. La granularité est forte, car la classification se fait flux par flux selon le protocole de réservation. En revanche, c'est un processus coûteux en ressources machine, et qui supporte difficilement la montée en charge car les routeurs de coeur doivent maintenir une liste des flux en cours afin de rechercher à chaque fois la qualité de service à appliquer. En effet, plus les flux seront nombreux, plus les traitements à effectuer au niveau des routeurs seront importants notamment au niveau de l'ordonnancement.
- ***DiffServ :*** dans cette configuration, les flux sont agrégés pour former des classes de services. De cette manière les flux d'une même classe ont les mêmes garanties de service. Par rapport à IntServ, la granularité est donc beaucoup plus faible. Cependant, DiffServ repose sur l'utilisation d'un système de marquage des paquets pour définir le comportement à adopter par les noeuds recevant le paquet. C'est ce que l'on nomme le **Per-Hop Behavior**. Le but ici n'étant pas de détailler l'ensemble

des mécanismes mis en oeuvre dans DiffServ, nous allons donc voir l'utilisation de ces approches dans MPLS**.**

1.3.6.2 MPLS VPN

1.3.6.2.1 Les Réseaux privés virtuels (VPN)

Un réseau privé virtuel (VPN) est un ensemble de sites partageant la même table de routage. Un VPN est également un réseau dans lequel la connectivité client à plusieurs sites est déployée sur une infrastructure partagée avec les mêmes politiques administratives qu'un réseau privé.

Le modèle VPN MPLS est un véritable modèle VPN pair qui applique des séparations de trafic en attribuant des tables de transfert de routage VPN (VRF) uniques au VPN de chaque client. Ainsi, les utilisateurs d'un VPN spécifique ne peuvent pas voir le trafic en dehors de leur VPN. La séparation du trafic se produit sans tunnel ni cryptage car elle est directement intégrée au réseau.

1.3.6.2.2 Les composants des VPNs MPLS

- **CE (Customer Edge)** : équipement de périphérie du réseau du client, avec une interface directement connectée au réseau du fournisseur de services. CE peut être un routeur, un commutateur ou un hôte. Dans des circonstances normales, CE n'a pas connaissance d'un VPN et n'a pas besoin de la prise en charge MPLS.
- **PE (Provider Edge):** c'est la périphérie du réseau du fournisseur de services et est directement connecté à CE. Dans le réseau MPLS, tout le traitement VPN est effectué sur PE, ce qui nécessite des performances élevées pour PE.
- **P (Provider device)** : dispositif dorsal du réseau du fournisseur de services, qui n'est pas directement connecté au CE. Les dispositifs P n'ont besoin que des capacités de transfert MPLS de base et ne conservent pas les informations VPN.

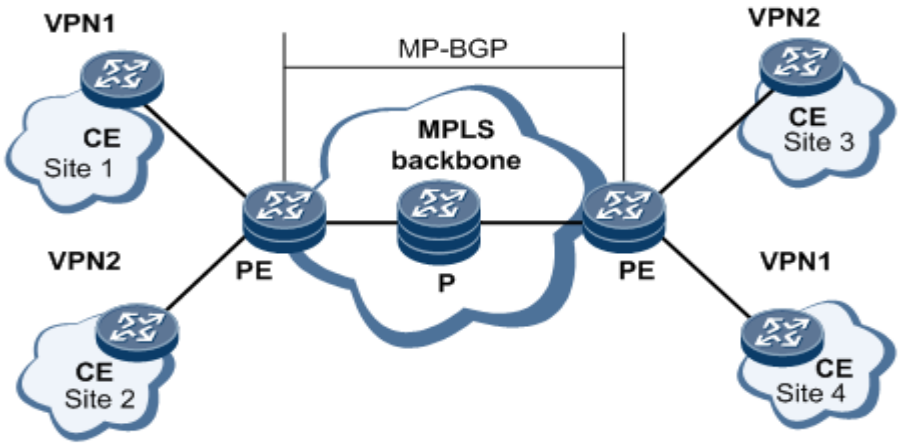


Fig I.6 VPN IP BGP/MPLS de base

1.3.6.2.3 Table de transmission VRF [09]

La table virtuelle de routage et de transfert (VRF) est un élément clé de la technologie VPN MPLS. VRF Table est une table de routage associée à un VPN qui donne les routes vers les réseaux IP faisant partie de ce VPN.

Permet de virtualiser une partie du routeur car un opérateur a plusieurs clients sur le même PE .Par exemple, un routeur qui doit traiter le trafic de plusieurs AS ayant le même adressage, afin de ne pas les mélanger, mettra chaque AS dans une VRF.

Constituée d'une table de routage, d'une FIB (Forwarding Information Base) et d'une table CEF spécifiques, indépendantes des autres VRF et de la table de routage globale

Chaque VRF est désignée par un nom sur les routeurs PE. Les noms sont affectés localement, et n'ont aucune signification vis-à-vis des autres routeurs. Chaque interface de PE reliée à un site client est rattachée à une VRF particulière

1.3.6.2.4 Propagation des informations du routage VPN

- **MP-BGP (Multi-Protocol BGP):** il s'agit d'une extension du protocole BGP qui permet à BGP de transporter des informations de routage pour plusieurs couches réseau et familles d'adresses. MP-BGP prend en charge les routes IPv4 monodiffusion/multidiffusion, IPv6 monodiffusion/multidiffusion et VPNv4.
- **Notion de RD (Route Ditinguisher) :** La fonction de RD est de rendre les routes appartenant à différents VRF uniques dans le noyau MPLS. Pour ce faire, nous devons annoncer les routes VPNv4 et nous accomplissons cette tâche en utilisant MP-BGP (Multi-Protocol BGP).
- **Notion de RT** (Route Target) : Maintenant, pour obtenir un routage correct sur un VPN MPLS, nous devons discuter des Route Targets (RT). Les RT définissent l'appartenance VPN car ils permettent au routeur de contrôler l'importation et l'exportation de routes entre différents VRF. Ainsi, disons que si le client A situé dans la succursale X souhaite avoir une connectivité avec le client A situé dans la succursale Y, les RT devront être importés et exportés entre les VRF respectifs.

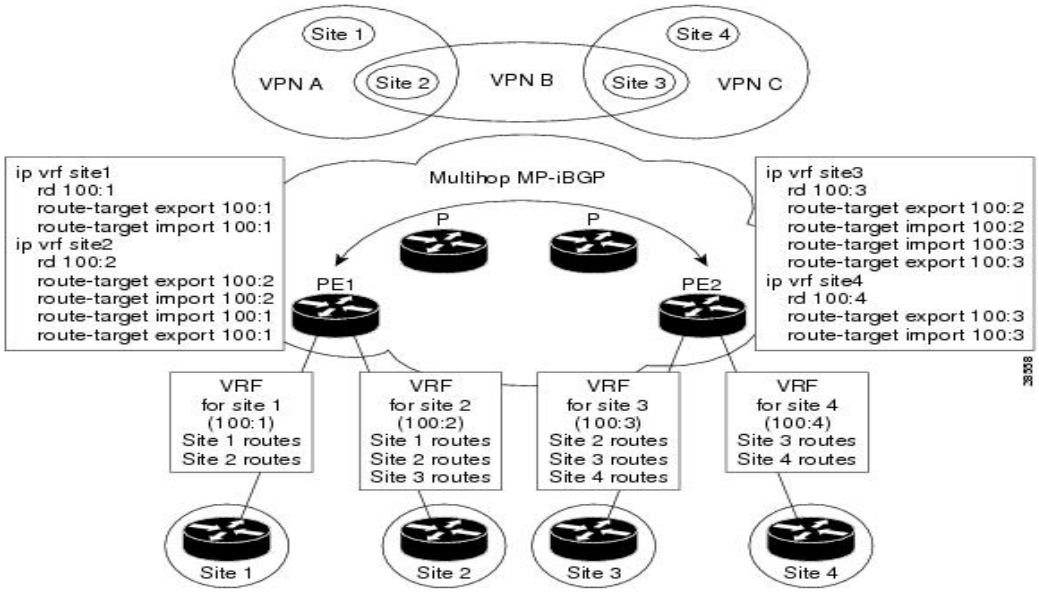


Fig I.7 VRF pour les sites dans plusieurs VPNs

1.3.6.3 MPLS et l'ingénierie de trafic [11]

Avec l'ingénierie du trafic (TE), MPLS offre de multiples possibilités de tenir compte de contraintes de de qualité de service (QoS) et la charge de bande passante dans le réseau. Au lieu d'envoyer le trafic via un chemin le moins coûteux mais encombré.

1.3.6.3.1 Concept de MPLS-TE

l'ingénierie de trafic MPLS (MPLS-TE) basé sur le concept de routage de tunnels (trafic trunk) où le tunnel est unidirectionnel et défini par deux LER (Ingress et Egress) routés de façon explicite ,le LSP n'est plus déterminé à chaque bond mais choisit par l'ingress node. En prenant compte des contraintes telle que la bande passante et les ressources disponibles et le re-routage rapide après une panne ou en cas de surcharge sur les LSP. Avec le routage explicite et la réservation de ressource est réalisée par des protocoles de signalisation ou Resource Réservation Protocol-Trafic Engineering (RSVP-TE) ou CR-LDP (Constraint Based Routing LDP).

1.3.6.3.2 RSVP-TE (Resource Reservation Protocol-Traffic Engineering)

Nous parlerons de RSVP-TE ici car c'est la seule méthode de signalisation actuellement di6sponible pour MPLS-TE, CR-LDP étant devenue obsolète. Le RSVP est un protocole de signalisation utilisait initialement un échange de messages pour réserver les ressources des flux IP à travers un réseau.

.Le protocole RSVP-TE effectue trois fonctions principales dans le but de signaler les tunnels de LSP le long du chemin préalablement défini :

- effectue un contrôle d'admission local, pour s'assurer que les contraintes sont bien respectées (bande passante, groupes administratifs). Ce contrôle d'admission local est nécessaire pour prendre en compte les cas d'erreur de calcul de route.
- Il réserve la bande passante. Cette réservation de ressources est purement logique et ne se traduit pas par une réservation physique de bande passante.
- Il distribue les labels et entraîne une mise à jour des tables MPLS en transit.

L'établissement d'un LSP-TE avec RSVP-TE se fait comme suit **:**

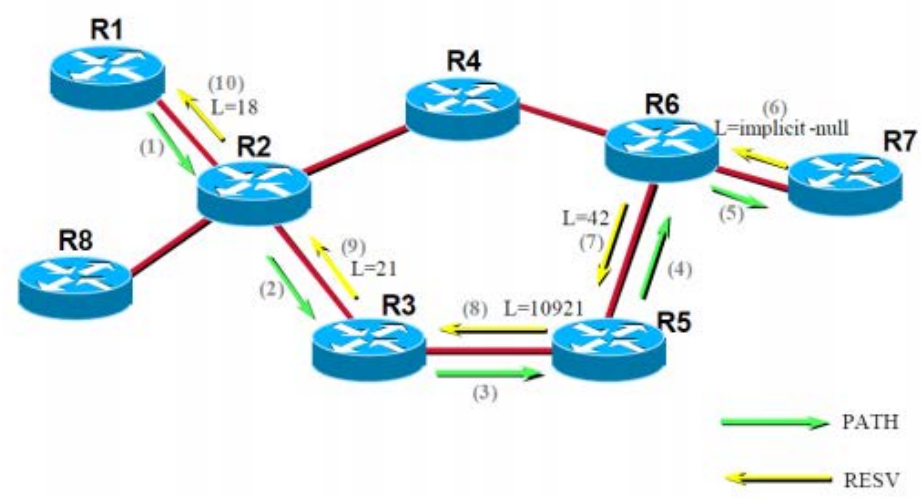


Fig I.8 Etablissement LSP-TE avec RSVP-TE

Etablissement LSP-TE avec RSVP-TE (1) R1 est tête de tunnel TE, il envoie un message Path (établit et maintient le LSP-TE dans le sens descendant) à R2 demandant une réservation de lien. Celui-ci vérifie le format du message et la disponibilité des ressources TE demandées. Si les ressources ne sont pas disponibles, R2 renvoie un message PathErr (Indique une erreur) à R1, la séquence d'établissement est alors annulée. (2) R2 envoie un message Path à R3. R3 fait les mêmes vérifications qu'en (1) (3) Ainsi de suite jusqu'à (5)
(6) R7 est la queue du tunnel TE. Il envoie un message Resv à R6. Ce message contient le label de commutation MPLS à employer pour le tunnel TE par R6. (7) R6 envoie un message Resv (établit et maintient le LSP-TE dans le sens montant) à R5 et indique un label L=42 Il en est de même pour (8), (9) et (10) sur la figure Fig I.8

1.4 Conclusion

MPLS est donc une technologie qui a su prendre une place prépondérante dans les réseaux longue distance opérateurs. Son but premier, qui était d'optimiser le temps de traitement des paquets au sein du coeur de réseau s'est peu à peu effacé pour laisser place aux extensions et applications du MPLS.

MPLS ajoute en effet la capacité d'envoyer un paquet le long de n'importe quel chemin désiré. Les principales applications sont une meilleure réaction du réseau en cas de panne, l'ingénierie de trafic en particulier pour des besoins particuliers (tactiques) et une amélioration de l'opération des réseaux. Ces avantages ont permis une standardisation rapide de SR-MPLS, son implémentation par tous les constructeurs majeurs de routeurs et des déploiements variés.

Chapitre 2 :Étude théorique de la technologie routage de segment

2.1 Introduction

Au cours des dernières années, l'évolutivité du réseau est essentielle car le nombre de périphériques réseau et la quantité de trafic augmentent rapidement au fil du temps.

Pour ces raisons, le groupe de travail "Source Packet Rou-ting in Networking (SPRING)" de l'IETF, a proposé le routage de segments (Segment Routing).

L'un des principaux objectifs de cette nouvelle architecture est de résoudre la complexité des réseaux MPLS actuellement utilisés par les fournisseurs de services pour transporter les données dans leurs réseaux centraux. Elle s'appuie sur un paradigme de réseau connu sous le nom de routage à la source qui disposent d'un plan de contrôle facile à gérer et fournir une ingénierie de trafic (TE) efficace tout en simplifiant le fonctionnement.

2.2 Définition Segment Routing

Le routage de segment SR est une architecture standardisée qui présente une approche innovante et simple. SR est essentiellement une nouvelle vue du routage source où un paquet porte dans son en-tête le chemin pour atteindre sa destination en éliminant les protocoles de signalisation lourds en ressources de MPLS, amélioré tout en minimisant la nécessité de maintenir l'état du chemin sur chaque routeur, ce qui ouvre de nouvelles voies de flexibilité et évolutivité. **[10]**

2.3 Terminologie

2.3.1 Segment :

SR définit un segment comme une instruction codée dans l'en-tête du paquet pour que les nœuds capables de SR puissent l'exécuter. **[11]**

2.3.2 ID de segment (SID) :

identifie de manière unique un segment. Un SID est mappé à une étiquette MPLS sur le plan de transfert. Chacun de ces segments est défini avec un SID différent. Ces différents SID sont donnés ci-dessous :

- **Un SID de préfixe** (également appelé étiquette de préfixe) : est une étiquette mappée à une adresse IP de destination.

- **Un SID de nœud** (également appelé étiquette de nœud) : Est une étiquette mappée à l'adresse IP d'une interface de bouclage sur un périphérique. Il peut être considéré comme un préfixe spécial SID.

- **Un SID de contiguïté** (également appelé étiquette de contiguïté) :est annoncé par un périphérique à son voisin d'interface afin de spécifier explicitement un lien pour le transfert de paquets dans la direction désignée.

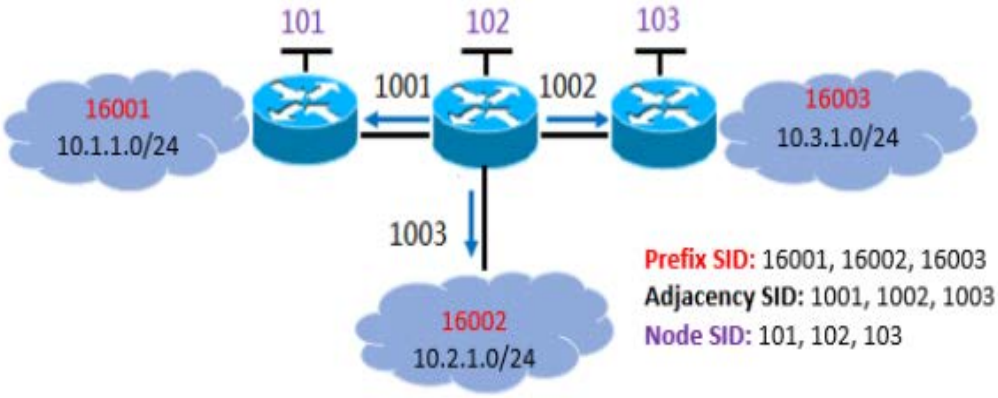


Fig II.1 Les différents types de SID

2.4 SR-MPLS

La technologie de routage de segment s'applique au plan de transfert sans modification de l'architecture ni du plan de donné .Avec SR-MPLS, chaque segment est encodé dans un label .Une liste de segments est encodée sous forme d'une pile de labels.

2.5 Allocation et propagation de SID[12]

SR-MPLS divise le chemin de transfert de paquets en différents segments, alloue des SID aux segments et insère des informations de segment dans les paquets à l'entrée du chemin pour guider le transfert de paquets vers la destination. En se concentrant sur l'allocation et la propagation des SID, ce qui suit décrit comment les LSP sont établis dans le plan de contrôle et comment les paquets de données sont transmis dans le plan de transfert.

- **Allocation et propagation de SID de nœud**

Supposons que P4 dans la figure suivante est le nœud de destination sur lequel un SID de nœud est configuré manuellement. Une fois que P4 a propagé le SID du nœud aux autres nœuds du domaine IGP via un IGP, tous ces nœuds apprennent le SID. Ils exécutent ensuite

l'algorithme du chemin le plus court en premier (SPF) pour calculer un chemin de transfert d'étiquette vers P4 et générer les entrées de transfert correspondantes.

Les chemins représentés par les nœuds SID sont des LSP BE SR-MPLS (les LSP SR optimaux calculés par l'IGP à l'aide de l'algorithme SPF).

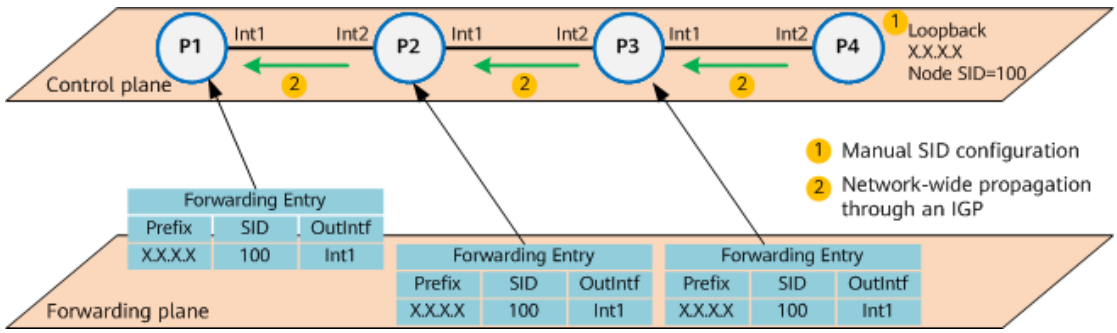


Fig II.2 Allocation et propagation de SID de nœud

- **Allocation et propagation du préfixe SID**

Supposons que P4 dans la figure suivante est le nœud de destination sur lequel un SID de préfixe est configuré manuellement. Une fois que P4 a propagé le préfixe SID aux autres nœuds via un IGP, ces nœuds analysent le SID et calculent les valeurs d'étiquette en fonction de leurs propres SRGB. Ensuite, sur la base des informations de topologie collectées par IGP, chacun de ces nœuds exécute l'algorithme SPF pour calculer un chemin de transfert d'étiquette, et fournit les informations de prochain saut et OuterLabel calculées à la table de transfert pour guider le transfert de paquets de données.

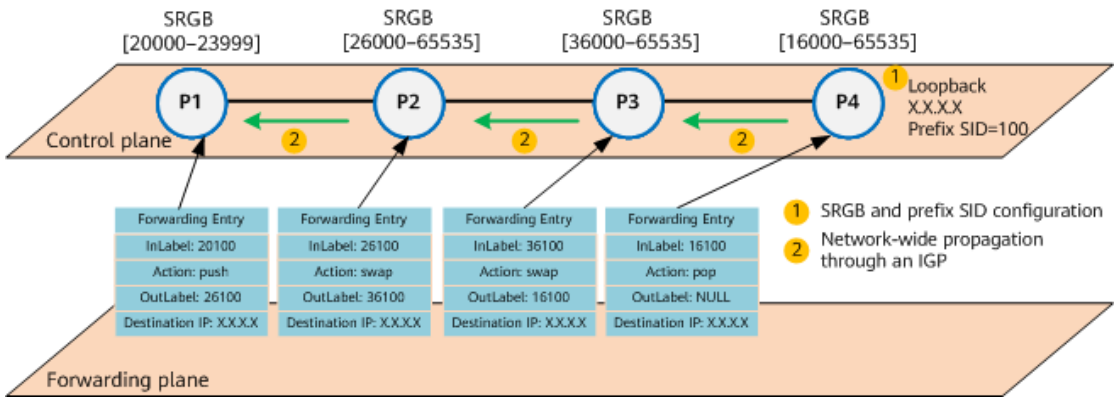


Fig II.3 Attribution et propagation du préfixe SID

Le processus d'établissement d'un LSP basé sur un préfixe SID est le suivant :

Une fois qu'un SRGB est configuré sur P4 et qu'un SID de préfixe est configuré pour l'interface de bouclage spécifiée de P4, P4 génère l'entrée de transfert correspondante et la remet. P4 encapsule ensuite le SRGB et le préfixe SID dans un paquet LSP et diffuse le paquet sur l'ensemble du réseau via un IGP.

Après avoir reçu le paquet LSP, d'autres nœuds du réseau analysent le préfixe SID annoncé par P4 et calculent également les valeurs d'étiquette en fonction de leurs propres SRGB ainsi que les valeurs OuterLabel en fonction des SRGB annoncés par les sauts suivants. À l'aide des informations de topologie collectées par IGP, ils calculent les chemins de transfert d'étiquettes et génèrent des entrées de transfert en conséquence.

1. P3 analyse le préfixe SID annoncé par P4 et calcule une valeur d'étiquette en fonction de son propre SRGB [36000–65535] à l'aide de la formule suivante : Étiquette = valeur de départ du SRGB + valeur du préfixe SID. Dans cet exemple, la valeur de départ du SRGB est 36000 et la valeur SID du préfixe est 100. Par conséquent, la valeur de l'étiquette est 36100 (36000 + 100).

   Sur la base des informations de topologie IS-IS, P3 calcule la valeur OuterLabel à l'aide de la formule suivante : OuterLabel = valeur de début du SRGB annoncé par le saut suivant + valeur SID de préfixe. Dans cet exemple, le saut suivant est P4, qui annonce le SRGB [16000–65535]. Par conséquent, la valeur OuterLabel est 16100 (16000 + 100).
2. Le processus de calcul sur P2 est similaire à celui sur P3. Dans cet exemple, la valeur de l'étiquette est 26 100 (26 000 + 100) et la valeur OuterLabel est 36 100 (36 000 + 100).
3. Le processus de calcul sur P1 est également similaire à celui sur P3. Dans cet exemple, la valeur de l'étiquette est 20100 (20000 + 100) et la valeur OuterLabel est 26100 (26000 + 100).

- **Allocation et propagation de SID de contiguïté**

Comme illustré dans la figure suivante, P2 alloue un SID de contiguïté à chaque voisin. Les SID de contiguïté sont automatiquement générés par un IGP pour les voisins par défaut, et ils peuvent également être configurés manuellement. Les SID de contiguïté sont également

propagés à d'autres nœuds via l'IGP. Cependant, les entrées de transfert sont générées uniquement sur les nœuds auxquels les SID de contiguïté sont alloués. Dans cet exemple, une entrée de renvoi est générée uniquement sur P2.

Une liste de segments contenant plusieurs SID de contiguïté peut être définie sur l'entrée3.

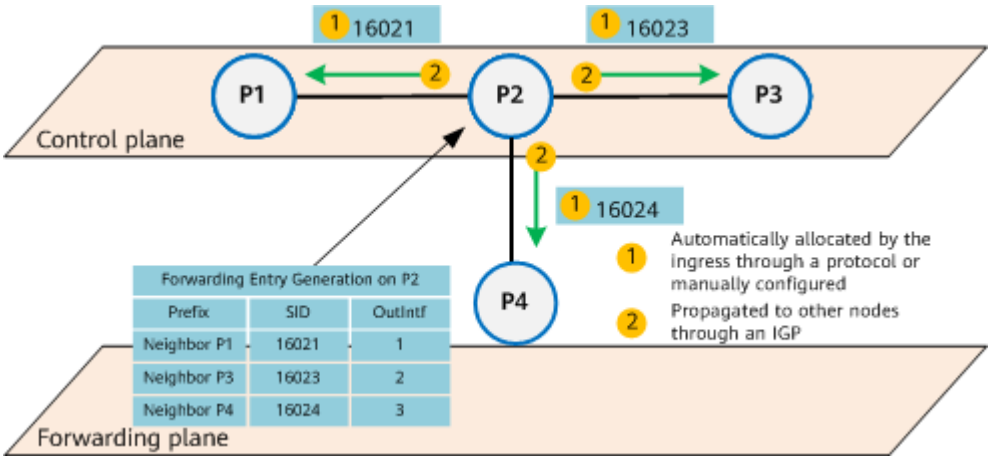


Fig II.4 Allocation et propagation de SID de contiguïté

En tant que tels**,** les chemins de transfert établis sur la base des SID de contiguïté sont appelés tunnels SR-MPLS TE**.** Ce mode d'établissement facilite la mise en œuvre du SDN. De plus**,** les chemins explicites strictement spécifiés, qui sont un type de tunnel SR-MPLS TE

2.6 Classement de Segments dans Segment Routing [15]

- **Segment global** : un segment global est une valeur d'ID qui a une signification dans l'ensemble du domaine de routage de segment, ce qui signifie que chaque nœud du domaine SR connaît cette valeur et exécute la même fonction pour le jeu d'instructions associé ou l'étiquette dans sa table de transfert (LFIB). C'est pourquoi on l'appelle Global Segment ID. La plage d'étiquettes réservées par défaut pour les nœuds Cisco utilisés à ces fins est de 16000 à 23999 et est appelée Segment Routing Global Block (SRGB).
- **Segment local** : il s'agit d'une valeur d'ID qui a une signification locale et seul le nœud source peut exécuter l'instruction associée. Étant donné que cette plage n'est pertinente que pour ce nœud particulier, ces valeurs ne se trouvent donc pas dans la plage allouée à l'aide de SRGB, mais uniquement via la plage d'étiquettes configurée localement.

2.7 Les opérations de routage de segment

Les actions à réaliser sur les segments de routage sont les suivantes [14] :

PUSH : Lorsqu'un paquet atteint le routeur d'entrée d'un réseau de routage de segments, il reçoit un segment ou une liste de segments. L'étiquette la plus haute dans la liste des segments détermine où le paquet va ensuite.

- **CONTINUE** : Lorsque le paquet atteint le prochain routeur de commutation d'étiquettes, le routeur appliquera une opération CONTINU, qui est la même que l'opération SWAP dans MPLS. Dans cette opération, la valeur de l'étiquette sortante est égale à la valeur de l'étiquette entrante.
- **NEXT** : Avant le saut final vers la destination, le routeur applique une opération next au paquet, qui supprime les étiquettes du paquet, tout comme le fait l'opération POP dans MPLS.

2.8 Fonctionnement du routage de segment - Scénario 1 [13]

2.8.1 Commutation des paquets en utilisant uniquement les SID de nœud

Le processus de transfert de paquets sur le LSP est le suivant :

1. Après avoir reçu un paquet de données, P1 ajoute l'étiquette 26100 au paquet, puis transmet le paquet.
2. Après avoir reçu le paquet étiqueté, P2 échange l'étiquette 26100 avec l'étiquette 36100, puis transmet le paquet.
3. Après avoir reçu le paquet étiqueté, P3 échange l'étiquette 36100 avec l'étiquette 16100, puis transmet le paquet.

Après avoir reçu le paquet étiqueté, P4 supprime l'étiquette 16100 et recherche dans la table de routage un autre transfert de paquet.

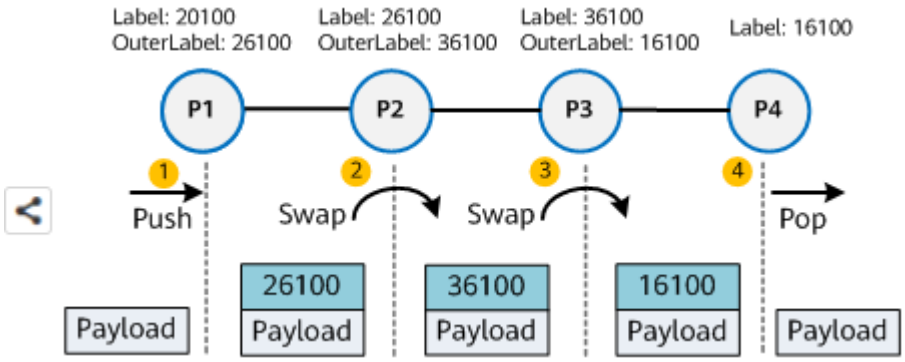


Fig II.5 Transfert de données basé sur le SID de contiguïté

2.9 Fonctionnement le routage de segment - Scénario 2 [13]

2.9.1 Commutation des paquets en basé sur le SID de contiguïté

Une fois qu'une liste de segments avec plusieurs SID de contiguïté a été définie sur l'entrée une liste de segment pour effectuer l'ingénierie du trafic

1 Après avoir reçu le paquet de données, P1 ajoute la pile d'étiquettes <1002, 2004, 4005, 5007, 7009> au paquet, recherche la contiguïté correspondant à l'étiquette supérieure 1002, constate que l'interface sortante correspondante se trouve sur la contiguï2té P1->P2, puis supprime l'étiquette 1002. Dans ce cas, le paquet transportant la pile d'étiquettes <2004, 4005, 5007, 7009> est transmis au nœud aval P2 via la contiguïté P1->P2.

2 Après avoir reçu le paquet, P2 recherche une contiguïté correspondant à l'étiquette supérieure 2004, constate que l'interface sortante correspondante se trouve sur la contiguïté P2-> P4, puis supprime l'étiquette 2004. Dans ce cas, le paquet portant la pile d'étiquettes <4005, 5007, 7009> est transmis au nœud aval P4 via la contiguïté P2->P4.

3 Après avoir reçu le paquet, P4, P5 et P7 traitent le paquet de la même manière que P2. Après avoir supprimé la dernière étiquette 7009, P7 transmet le paquet à P9.

2 Étant donné que le paquet reçu par P9 ne contient aucune étiquette, P9 recherche dans la table de routage un transfert de paquet supplémentaire.

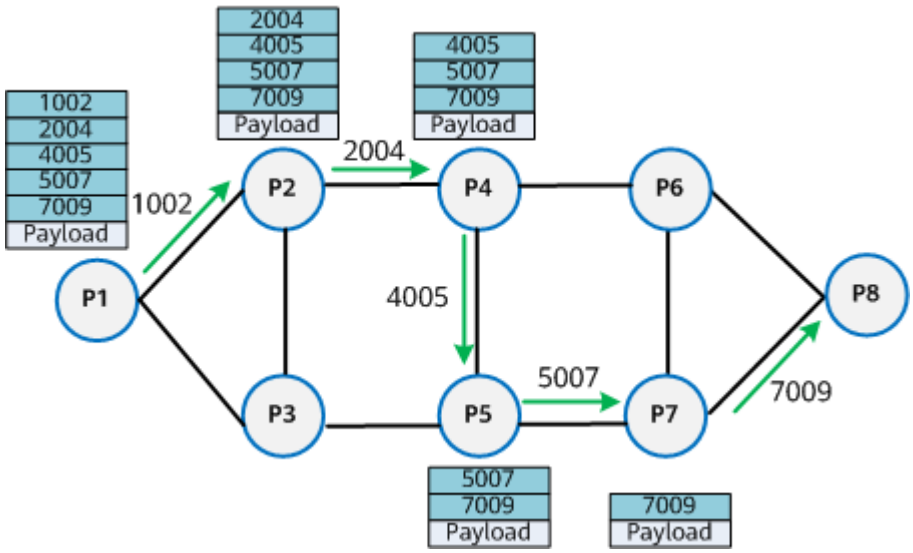


Fig II.6 Transfert de données basé sur le SID de contiguïté

2.10 Avantages du Segment Routing

L'architecture Segmeent Routing nous apporte de nombreux avantages [15] :

Simple :

Le principal avantage de SR est sa capacité à simplifier le réseau à réduire les protocoles à déployer et l'utilisation des ressources, ce qui facilite la gestion et l'exploitation du réseau.

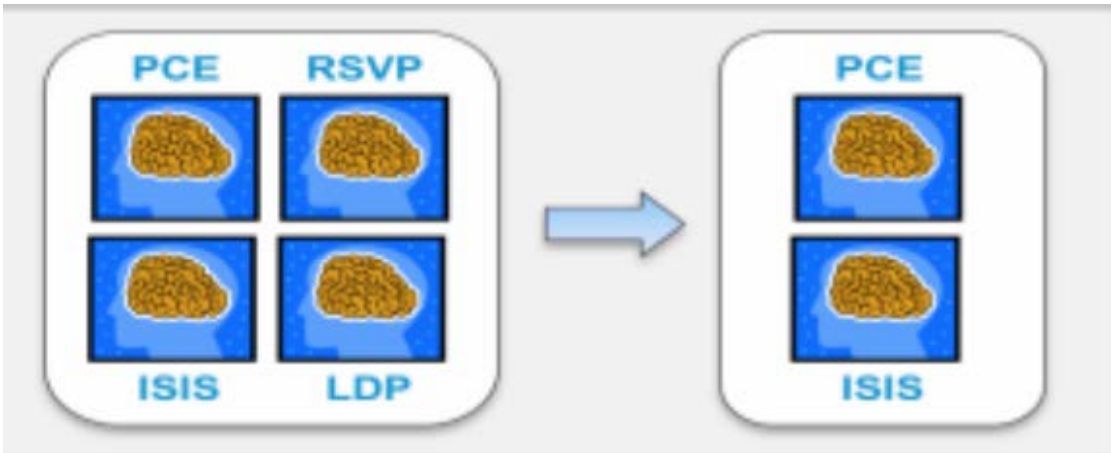


Fig II.7 Suite protocolaire simplifiée

- **Meilleure évolutivité**

SR 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.

- **Convergence rapide**

SR améliore la convergence des réseaux, car il permet d'implémenter la solution TI-LFA (Transport Independent - Loop Free Alternate). Chaque routeur peut précalculer un chemin de backup qui sera utilisé en cas de perte d'une adjacence.

- **Architecture prête pour le SDN**

SR donne une architecture SDN (Software Defined Networking) ou l'attribution des segments et le calcul des chemins sont programmés par un contrôleur SR (contrôleur SDN), qui est généralement PCE (Path Computation Engine). L'architecture SR est prête pour le SDN puisqu'elle permet de prendre des décisions de routage depuis une application. Une entité centrale, configurée avec quelques algorithmes de décision et qui a connaissance de

la charge des diverses liaisons et des latences peut simplement appliquer des changements de routage, sans pour autant créer de nouveaux états sur le réseau.

2.11 Comparaison entre IP/MPLS et Segment-Routing MPLS

Tableau II.1 Comparaison entre IP/MPLS et SR MPLS

	IP-MPLS	**SR –MPLS**
Plan de control	.LDP, R SVP, OSPF, ISIS, BGP.	OSPF, ISIS, BGP, SDN.
La distributions de labels	-la distribution labels et la réservation des ressources sont effectuées par des protocoles de signalisation LDP et RSVP-TE. Labels sont alloués aux liens adjacents et aux nœuds SR. Le routeur n'occupe pas un grand nombre d'étiquettes, ce qui réduit l'utilisation de ces ressources.	-l'ensemble de "segments" annoncés par le protocole de routage IGP. Le nombre d'étiquettes augmente avec le nombre de tunnels, ce qui augmente l'utilisation des ressources du routeur.
L'ingénierie de trafic	l'état des tunnels est maintenu. dans chaque nœud que le trafic traverse.	l'état est maintenu au niveau du nœud de tête seulement.
scalabilité de réseaux	scalabilité limitée.	Meilleure scalabilitée.
Architecture de réseau	Prend en charge le réseau traditionnel et n'est pas conforme au concept SDN	Prend en charge à la fois le réseau traditionnel et SDN.

2.12 Conclusion

Dans ce chapitre, j'ai abordé la technologie routage de segment d'un point de vue théorique dans lequel offre un ajout important aux réseaux des fournisseurs de services.

Il existe de nombreuses améliorations par rapport à RSVP-TE et MPLS LDP.

SR-MPLS est devenu une technologie phare de demain ; alliant souplesse, évolutivité et protection immédiate contre toutes les pannes de liens et pour mettre en évidence la technologie SR, nous avons implémenté un réseau avec une configuration SR-MPLS qui sera l'objet du dernier chapitre.

Chapitre 3 : Simulation routage de segments sur un réseau IP-MPLS

3.1 Introduction

Cette partie nous permettra de concrétiser l'objectif de notre étude, c'est dans le chapitre précédent que nous avons mis en évidence le principe de la technologie SR-MPLS, ainsi que ses différentes caractéristiques. Dans ce chapitre nous allons implémenter cette technologie tout en introduisant les services L3VPN recourant à un tunnel OSPF SR-MPLS pour permettre aux utilisateurs d'un même VPN d'accéder les uns aux autres en toute sécurité.

Ce chapitre consiste à la réalisation de notre projet en exposant les différentes configurations nécessaires à implémenter sur l'architecture que nous avons proposée, on se basant sur l'émulateur EVE-NG.

Pour présenter les configurations réalisées, nous nous sommes servis des captures d'écran qui illustrent les étapes de la configuration et les tests nécessaires que effectués.

3.2 Réalisation du réseau

3.2.1 Présentation du réseau

Ce réseau contient six routeurs dont :

- P1 et P2 représentent le cœur SR-MPLS.
- PE1 et PE2 représentent l'edge SR- MPLS.
- Les routeurs client(1) et client(2) désignent les sites d'un client VPN (routeurs CE).

Les routeurs PE et P sont des routeurs NE40 à base de VRP Huawei.

Les routeurs CE sont des routeurs 3700 à base d'IOS Cisco.

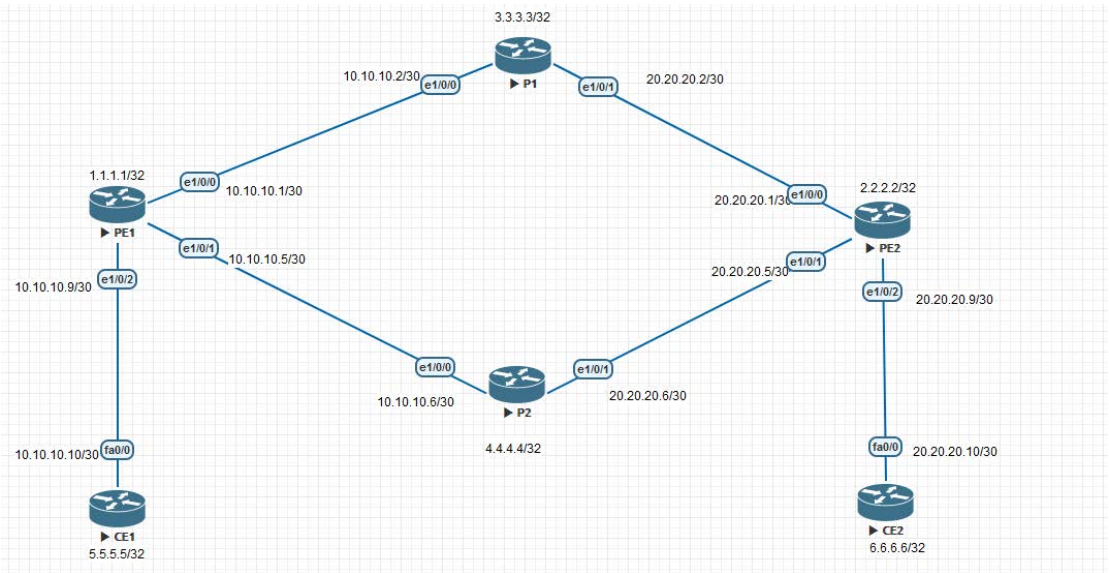


Fig III. 1 Architecture du réseau

3.2.2 Plan d'adressage

Le tableau suivant résume les adresses des différents routeurs ainsi que leurs interfaces préconfigurées dans le réseau :

Tableau III.2 : tableau d'adressage

	Adresse loop-back	**Les interfaces**	**Les adresses des interfaces**
PE1	1.1.1.1/32	Ethernet 1/0/0 Ethernet 1/0/1 Ethernet 1/0/2	10.10.10.1/30 10.10.10.5/30 10.10.10.9/30
PE2	2.2.2.2/32	Ethernet 1/0/0 Ethernet 1/0/1 Ethernet 1/0/2	20.20.20.1/30 20.20.20.5/30 20.20.20.9/30
P1	3.3.3.3/32	Ethernet 1/0/0 Ethernet 1/0/1	10.10.10.2/30 20.20.20.2/30
P2	4.4.4.4/32	Ethernet 1/0/0 Ethernet 1/0/1	10.10.10.6/30 20.20.20.6/30
Client 1	5.5.5.5/32	Fast Ethernet 0/0	10.10.10.10/30
Client 2	6.6.6.6/32	Fast Ethernet 0/0	20.20.20.10/30

3.2.3 La feuille de route de la configuration

-Activation de L'OSPF sur le réseau fédérateur pour garantir l'interfonctionnement des PE entre eux.

-Configuration de MPLS et le routage par segment sur le réseau fédérateur afin établir des LSP SR .Et activation de TI-LFA FRR (cas de panne). .

-Configuration d'instances VPN de la famille d'adresses IPv4 sur les PE et liaison de chaque interface qui connecte un PE à un CE à une instance VPN.

-Activation des extensions multi-protocoles pour le protocole de passerelle frontalière intérieure (MP-IBGP) sur les PE pour échanger des informations de routage VPN.

-Configuration du protocole EBGP (External Border Gateway Protocol) sur les CE et les PE pour échanger des informations de routage VPN.

3.3 Simulation et résultats

3.3.1 Configuration des adresses IP pour les interfaces

On sélectionne chaque interface par la commande « interface Ethernet X/Y /Z». On attribue à chaque interface une adresse IP, en utilisant la commande « ip adresse » suivie de l'adresse IP, ensuite, à la fin on valide La configuration avec la commande « commit » et sortir du mode configuration avec la commande « quit ».

#PE1 :

```
<HUAWEI>
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]
[~HUAWEI]sysname PE1
[*HUAWEI]
[*HUAWEI]interface LoopBack1
[*HUAWEI-LoopBack1] ip address 1.1.1.1 255.255.255.255
[*HUAWEI-LoopBack1]quit
[*HUAWEI]interface Ethernet1/0/0
[*HUAWEI-Ethernet1/0/0]ip address 10.10.10.1 255.255.255.252
[*HUAWEI-Ethernet1/0/0]  quit
[*HUAWEI]interface Ethernet1/0/1
[*HUAWEI-Ethernet1/0/1] ip address 10.10.10.5 255.255.255.252
[*HUAWEI-Ethernet1/0/1]  quit
[*HUAWEI]interface Ethernet1/0/2
[*HUAWEI-Ethernet1/0/2]ip address 10.10.10.9 255.255.255.252
[*HUAWEI-Ethernet1/0/2]  quit
[*HUAWEI]commit
```

A

#P1 :

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]
[~HUAWEI]sysname P1
[*HUAWEI]
[*HUAWEI]interface LoopBack1
[*HUAWEI-LoopBack1] ip address 3.3.3.3 255.255.255.255
[*HUAWEI-LoopBack1] quit
[*HUAWEI]interface Ethernet1/0/0
[*HUAWEI-Ethernet1/0/0] ip address 10.10.10.2 255.255.255.252
[*HUAWEI-Ethernet1/0/0] quit
[*HUAWEI]interface Ethernet1/0/1
[*HUAWEI-Ethernet1/0/1]  ip address 20.20.20.2 255.255.255.252
[*HUAWEI-Ethernet1/0/1]quit
[*HUAWEI]commit
```

B

#PE2 :

```
[~HUAWEI]sysname PE2
[*HUAWEI]
[*HUAWEI]interface LoopBack1
[*HUAWEI-LoopBack1] ip address 2.2.2.1 255.255.255.255
[*HUAWEI-LoopBack1]quit
[*HUAWEI]interface Ethernet1/0/0
[*HUAWEI-Ethernet1/0/0]ip address 20.20.20.1 255.255.255.252
[*HUAWEI-Ethernet1/0/0]  quit
[*HUAWEI]interface Ethernet 1/0/1
[*HUAWEI-Ethernet1/0/1] ip address 20.20.20.5 255.255.255.252
[*HUAWEI-Ethernet1/0/1]  quit
[*HUAWEI]interface Ethernet 1/0/2
[*HUAWEI-Ethernet1/0/2]ip address 20.20.20.9 255.255.255.252
[*HUAWEI-Ethernet1/0/2]  quit
[*HUAWEI]commit
```

C

P2 :

```
[~HUAWEI]sysname P2
[*HUAWEI]
[*HUAWEI]interface LoopBack1
[*HUAWEI-LoopBack1] ip address 4.4.4.4 255.255.255.255
[*HUAWEI-LoopBack1] quit
[*HUAWEI]interface Ethernet1/0/0
[*HUAWEI-Ethernet1/0/0] ip address 10.10.10.6 255.255.255.252
[*HUAWEI-Ethernet1/0/0] quit
[*HUAWEI]interface Ethernet1/0/1
[*HUAWEI-Ethernet1/0/1]  ip address 20.20.20.6 255.255.255.252
[*HUAWEI-Ethernet1/0/1]quit
[*HUAWEI]commit
[~P2]
```

D

Fig III.2 Configuration des interfaces de PE1 ,PE2 ,P1,P2

3.3.2 Configuration du protocole IGP sur le réseau fédérateur

Pour l'activation du routage classique et mise en œuvre de la connectivité au niveau du backbone, c'est-à-dire entre les PE- Routeurs et les P-Routeurs.

OSPF est utilisé comme protocole IGP représenté par :

- « ospf 100» : pour l'activation du processus ospf, le 100 représente l'identifiant du routeur.
- «area 0» : pour déclarer et spécifier le réseau participant au processus ospf, le 0 représente l'identifiant du réseau.
- « quit » : pour sortir du mode configuration.

PE1

```
[~PE1]ospf 100
[*PE1-ospf-100]opaque-capability enable
[*PE1-ospf-100] area 0
[*PE1-ospf-100-area-0.0.0.0] quit
[*PE1-ospf-100]interface loopback 1
[*PE1-LoopBack1] ospf enable 100 area 0
[*PE1-LoopBack1] quit
[*PE1]interface Ethernet 1/0/0
[*PE1-Ethernet1/0/0] ospf enable 100 area 0
[*PE1-Ethernet1/0/0]quit
[*PE1] interface Ethernet 1/0/1
[*PE1-Ethernet1/0/1]ospf enable 100 area 0
[*PE1-Ethernet1/0/1] quit
[*PE1]commit
[~PE1]
```

A

P1 :

```
[~P1]ospf 100
[~P1-ospf-100] opaque-capability enable
[~P1-ospf-100]area 0
[~P1-ospf-100-area-0.0.0.0] quit
[~P1-ospf-100]quit
[~P1] commit
[~P1]interface loopback 1
[~P1-LoopBack1] ospf enable 100 area 0
[~P1-LoopBack1]quit
[~P1]interface Ethernet1/0/0
[~P1-Ethernet1/0/0]ospf enable 100 area 0
[~P1-Ethernet1/0/0]quit
[~P1]interface Ethernet1/0/1
[~P1-Ethernet1/0/1]ospf enable 100 area 0
[~P1-Ethernet1/0/1] quit
```

B

PE2 :

```
[~PE2]ospf 100
[*PE2-ospf-100]opaque-capability enable
[*PE2-ospf-100] area 0
[*PE2-ospf-100-area-0.0.0.0] quit
[*PE2-ospf-100]interface loopback 1
[*PE2-LoopBack1] ospf enable 100 area 0
[*PE2-LoopBack1] quit
[*PE2]interface Ethernet 1/0/0
[*PE2-Ethernet1/0/0] ospf enable 100 area 0
[*PE2-Ethernet1/0/0]quit
[*PE2] interface Ethernet 1/0/1
[*PE2-Ethernet1/0/1]ospf enable 100 area 0
[*PE2-Ethernet1/0/1] quit
[*PE2]commit
[~PE2]
```

C

P2 :

```
[~P2]ospf 100
[*P2-ospf-100] opaque-capability enable
[*P2-ospf-100]area 0
[*P2-ospf-100-area-0.0.0.0] quit
[*P2-ospf-100]quit
[*P2] commit
[~P2]interface loopback 1
[~P2-LoopBack1] ospf enable 100 area 0
[*P2-LoopBack1]quit
[*P2]interface Ethernet1/0/0
[*P2-Ethernet1/0/0]ospf enable 100 area 0
[*P2-Ethernet1/0/0]quit
[*P2]interface Ethernet1/0/1
[*P2-Ethernet1/0/1]ospf enable 100 area 0
[*P2-Ethernet1/0/1] quit
[*P2]commit
[~P2]
```

D

Fig III.3 Activation d'OSPF

3.3.3 Configuration de la fonction MPLS de base sur le réseau fédérateur

Pour L'activation de MPLS sur chaque nœud d'un domaine SR MPLS , les ID LSR doivent être définis avant l'exécution de la commande « mpls».

L'utilisation de l'adresse IP d'une interface de bouclage comme ID LSR est recommandée pour un LSR.

#PE1 :

```
[~PE1] mpls lsr-id 1.1.1.1
[*PE1] mpls
Info: Mpls starting, please wait... OK!
[*PE1-mpls]commit
[~PE1-mpls]quit
[~PE1]
```

A

#PE2 :

```
[~PE2]
[~PE2]mpls lsr-id 2.2.2.2
[*PE2] mpls
Info: Mpls starting, please wait... OK!
[*PE2-mpls]commit
[~PE2-mpls]quit
[~PE2]
```

B

#P2 :

```
[~P2] mpls lsr-id 4.4.4.4
[*P2]mpls
Info: Mpls starting, please wait... OK!
[*P2-mpls]commit
[~P2-mpls] quit
[~P2]
```

C

```
[~P1]mpls lsr-id 3.3.3.3
[~P1]mpls
[~P1-mpls]commit
[~P1-mpls] quit
[~P1]
```

D

Fig III.4 Configuration MPLS des PE et P

3.3.4 Configuration du routage par segment sur le réseau fédérateur et activation du FRR TI-LFA

La configuration de la fonction SR-MPLS implique :

-L'activation de la fonction globale de routage par segment SRGB) par la commande «segment-routing global-block ».

-Définir un SID de préfixe SR avec la commande «ospf prefix-sid index ».

PE1 :

```
[~PE1]segment-routing
[*PE1-segment-routing] quit
[*PE1] commit
[~PE1] ospf 100
[~PE1-ospf-100]segment-routing mpls
[*PE1-ospf-100]segment-routing global-block 16000 23999
[*PE1-ospf-100]
[*PE1-ospf-100]frr
[*PE1-ospf-100-frr]loop-free-alternate
[*PE1-ospf-100-frr]ti-lfa enable
[*PE1-ospf-100-frr] quit
[*PE1-ospf-100] quit
[*PE1]interface loopback 1
[*PE1-LoopBack1]ospf prefix-sid index 10
[*PE1-LoopBack1]quit
[*PE1]commit
[~PE1]
```

A

PE2 :

```
[~PE2]segment-routing
[*PE2-segment-routing] quit
[*PE2] commit
[~PE2] ospf 100
[~PE2-ospf-100]segment-routing mpls
[*PE2-ospf-100]segment-routing global-block 16000 23999
[*PE2-ospf-100]
[*PE2-ospf-100]frr
[*PE2-ospf-100-frr]loop-free-alternate
[*PE2-ospf-100-frr]ti-lfa enable
[*PE2-ospf-100-frr] quit
[*PE2-ospf-100] quit
[*PE2]interface loopback 1
[*PE2-LoopBack1]ospf prefix-sid index 20
[*PE2-LoopBack1]quit
[*PE2]commit
[~PE2]
```

B

#P1 :

```
[~P1]segment-routing
[*P1-segment-routing] quit
[*P1]commit
[~P1]
[~P1]ospf 100
[~P1-ospf-100] segment-routing mpls
[*P1-ospf-100]segment-routing global-block 16000 23999
[*P1-ospf-100]
[*P1-ospf-100] frr
[*P1-ospf-100-frr] loop-free-alternate
[*P1-ospf-100-frr] ti-lfa enable
[*P1-ospf-100-frr]quit
[*P1-ospf-100]interface loopback 1
[*P1-LoopBack1]ospf prefix-sid index 30
[*P1-LoopBack1]quit
[*P1]commit
[~P1]quit
```

C

P2 :

```
[~P2]ospf 100
[~P2-ospf-100] segment-routing mpls
[*P2-ospf-100]segment-routing global-block 16000 23999
[*P2-ospf-100]
[*P2-ospf-100] frr
[*P2-ospf-100-frr] loop-free-alternate
[*P2-ospf-100-frr] ti-lfa enable
[*P2-ospf-100-frr]quit
[*P2-ospf-100]interface loopback 1
[*P2-LoopBack1]ospf prefix-sid index 40
[*P2-LoopBack1]quit
[*P2]commit
[~P2]
```

D

Fig III.5 Configuration SR-MPLS avec activation FRR TI-LFA

- Après avoir terminé la configuration, on exécute la commande display tunnel-info all sur les PE, et vous pouvez voir que les SR LSP sont configurés entre les PE.

Dans ce qui suit, la sortie de la commande sur PE2 est utilisée.

```
[~PE2] display tunnel-info all
Tunnel ID           Type               Destination                              Status
--------------------------------------------------------------------------------------
0x000000002900000003 srbe-lsp          1.1.1.1                                  UP
0x000000002900000004 srbe-lsp          3.3.3.3                                  UP
0x000000002900000006 srbe-lsp          4.4.4.4                                  UP
[~PE2]
```

Fig III.6 Résultat du Voisinage SR-LSP

```
<PE1>ping lsp segment-routing ip 2.2.2.2 32 version draft2
  LSP PING FEC: SEGMENT ROUTING IPV4 PREFIX 2.2.2.2/32 : 100  data bytes, press CTRL_C to break
    Reply from 2.2.2.2: bytes=100 Sequence=1 time=24 ms
    Reply from 2.2.2.2: bytes=100 Sequence=2 time=9 ms
    Reply from 2.2.2.2: bytes=100 Sequence=3 time=5 ms
    Reply from 2.2.2.2: bytes=100 Sequence=4 time=4 ms
    Reply from 2.2.2.2: bytes=100 Sequence=5 time=8 ms

  --- FEC: SEGMENT ROUTING IPV4 PREFIX 2.2.2.2/32 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/10/24 ms
```

Fig III.7 Résultat du ping sur PE1

3.3.5 Configurer MP-IBGP sur les PEs

Afin que CE1 etCE2 puissent communiquer en utilisant le réseau SR-MPRS, la configuration d'une MP-IBGP est nécessaire entre PE1 et PE2 afin qu'ils puissent s'échanger les routes recueillies via EBGP avec les clients. La configuration du concept MPLS-VPN, s'effectue toujours sous l'autorité du protocole BGP.

PE1 :

```
[*PE1]bgp 100
[*PE1-bgp]peer 2.2.2.2  as-number 100
[*PE1-bgp] peer 2.2.2.2 connect-interface loopback 1
[*PE1-bgp] ipv4-family vpnv4
[*PE1-bgp-af-vpnv4] peer 2.2.2.2 enable
[*PE1-bgp-af-vpnv4] commit
[~PE1-bgp-af-vpnv4]quit
[~PE1-bgp]quit
```

A

PE2 :

```
[*PE2]bgp 100
[*PE2-bgp]peer 1.1.1.1  as-number 100
[*PE2-bgp] peer 1.1.1.1 connect-interface loopback 1
[*PE2-bgp] ipv4-family vpnv4
[*PE2-bgp-af-vpnv4] peer 1.1.1.1 enable
[*PE2-bgp-af-vpnv4] commit
[~PE2-bgp-af-vpnv4]quit
[~PE2-bgp]quit
[~PE2]
```

B

Fig III.8 Configuration de MP-IBGP sur les PEs

- Après avoir terminé la configuration, on exécute la commande « display bgp peer » et « display bgp vpnv4 all peer » sur les PE, afin de voir qu'une relation BGP entre pairs est configurée entre les PE et que la relation BGP entre pairs est à l'état établi.

```
[~PE1]display bgp peer

BGP local router ID : 1.1.1.1
Local AS number : 100
Total number of peers : 1                 Peers in established state : 0

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State  PrefRcv
  2.2.2.2         4         100        0        0     0 04:44:29      Active        0
[~PE1]
```

Fig III.9 Affichage BGP peer

```
[~PE1]display bgp vpnv4 all peer

BGP local router ID : 1.1.1.1
Local AS number : 100
Total number of peers : 2                 Peers in established state : 1

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State  PrefRcv
  2.2.2.2         4         100        0        0     0 04:45:00      Active        0

  Peer of IPv4-family for vpn instance :

  VPN-Instance vpna, Router ID 1.1.1.1:
  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State  PrefRcv
  10.10.10.10     4       65100       87       98     0 01:24:33 Established        0
```

Fig III.10 Table de routage BGP VPNv4

3.3.6 Configuration d'instances VPN dans la famille d'adresses IPv4 sur chaque PE et connecté à un CE.

PE1 :

```
[*PE1]ip vpn-instance vpna
[*PE1-vpn-instance-vpna] ipv4-family
[*PE1-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[*PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
Info: VPN-Target is already configured: 111:1
 IVT Assignment result:
Info: VPN-Target assignment is failed.
Info: VPN-Target is already configured: 111:1
 EVT Assignment result:
Info: VPN-Target assignment is failed.
[*PE1-vpn-instance-vpna-af-ipv4]quit
[*PE1-vpn-instance-vpna]quit
[*PE1] interface Ethernet 1/0/2
[*PE1-Ethernet1/0/2] ip binding vpn-instance vpna
Info: All IPv4 and IPv6 related configurations on this interface are removed.
[*PE1-Ethernet1/0/2]ip address 10.10.10.9 255.255.255.252
[*PE1-Ethernet1/0/2] quit
[*PE1]commit
[~PE1]
```

A

PE2 :

```
[~PE2]
[~PE2]ip vpn-instance vpna
[*PE2-vpn-instance-vpna] ipv4-family
[*PE2-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[*PE2-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
 IVT Assignment result:
Info: VPN-Target assignment is successful.
 EVT Assignment result:
Info: VPN-Target assignment is successful.
[*PE2-vpn-instance-vpna-af-ipv4]quit
[*PE2-vpn-instance-vpna]quit
[*PE2] interface Ethernet 1/0/2
[*PE2-Ethernet1/0/2] ip binding vpn-instance vpna
Info: All IPv4 and IPv6 related configurations on this interface are removed.
[*PE2-Ethernet1/0/2]ip address 20.20.20.9 255.255.255.252
[*PE2-Ethernet1/0/2] quit
[*PE2]commit
```

B

Fig III.11 Configuration des VRF sur PE1, PE2

3.3.7 Configuration d'une politique de tunnel sur chaque PE pour sélectionner préférentiellement un SR LSP

La politique de tunnel est mise en œuvre par la configuration du sélecteur de tunnel. Cette politique permet à la fois aux services VPN et aux routes publiques non étiquetées de récourir aux tunnels SR-MPLS.

Ces figures décrit comment configurer les routes et les services pour qu'ils puissent recourir vers les tunnels SR-MPLS par le biais de politiques de tunnel.

- L'activation de la politique de tunnel par la commande « tunnel-policy policy-name».

-En sélectionne les tunnels et nombre de tunnels avec la commande « tunnel select-seq **s**r-lsp load-balance-number ».

#PE1 :

```
[~PE1]tunnel-policy p1
Info: New tunnel-policy is configured.
[*PE1-tunnel-policy-p1]tunnel select-seq sr-lsp load-balance-number 2
[*PE1-tunnel-policy-p1]quit
[*PE1]commit
[~PE1] ip vpn-instance vpna
[~PE1-vpn-instance-vpna] ipv4-family
[~PE1-vpn-instance-vpna-af-ipv4] tnl-policy p1
[*PE1-vpn-instance-vpna-af-ipv4] quit
[*PE1-vpn-instance-vpna]quit
[*PE1] commit
[~PE1]
```

A

PE2 :

```
[~PE2]tunnel-policy p1
Info: New tunnel-policy is configured.
[*PE2-tunnel-policy-p1]tunnel select-seq sr-lsp load-balance-number 2
[*PE2-tunnel-policy-p1]quit
[*PE2]commit
[~PE2] ip vpn-instance vpna
[~PE2-vpn-instance-vpna] ipv4-family
[~PE2-vpn-instance-vpna-af-ipv4] tnl-policy p1
[*PE2-vpn-instance-vpna-af-ipv4] quit
[*PE2-vpn-instance-vpna]quit
```

B

Fig III.12 : Configuration de la politique de tunnel sur chaque PE.

3.3.8 Configuration EBGP entre les PE et CE

CE1 :

```
CE1>en
CE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CE1(config)#interface loopback 1
CE1(config-if)#ip address 5.5.5.5 255.255.255.255
CE1(config-if)#no shutdown
CE1(config-if)#
CE1(config-if)#
CE1(config-if)#interface FastEthernet0/0
CE1(config-if)#ip address 10.10.10.10 255.255.255.252
CE1(config-if)#no shutdown
CE1(config-if)#
*Mar  1 01:15:45.003: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 01:15:46.003: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
CE1(config-if)#exit
CE1(config)#  router bgp 65100
CE1(config-router)#neighbor 10.10.10.9 remote-as 100
CE1(config-router)#
```

A

PE1 :

```
[~PE1]
[~PE1]bgp 100
[~PE1-bgp]ipv4-family vpn-instance vpna
[*PE1-bgp-vpna] peer 10.10.10.10 as-number 65100
[*PE1-bgp-vpna] peer 10.10.10.10 connect-interface Ethernet1/0/2
[*PE1-bgp-vpna] commit
[~PE1-bgp-vpna]
[~PE1-bgp-vpna]quit
```

B

CE2 :

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CE2
CE2(config)# interface loopback 1
CE2(config-if)#ip address 6.6.6.6 255.255.255.255
CE2(config-if)# no shutdown
CE2(config-if)#interface FastEthernet0/0
CE2(config-if)# ip address 20.20.20.10 255.255.255.252
CE2(config-if)# no shutdown
CE2(config-if)#
*Mar  1 00:04:51.427: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
 changed state to up
*Mar  1 00:04:52.863: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:04:53.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

```
CE2(config)#
CE2(config)#router  bgp 65200
CE2(config-router)#neighbor 20.20.20.9 remote-as 100
CE2(config-router)#
```

C

PE2 :

```
[~PE2]bgp 100
[~PE2-bgp]ipv4-family vpn-instance vpna
[*PE2-bgp-vpna]peer 20.20.20.10 as-number 65200
[*PE2-bgp-vpna]peer 20.20.20.10 connect-interface Ethernet1/0/2
[*PE2-bgp-vpna]commit
Committing....done.
[~PE2-bgp-vpna]quit
[~PE2-bgp]quit
```

D

Fig III.13 : Configuration EBGP sur PE,CE.

- Après la configuration, exécutez la commande display bgp vpnv4 vpn-instance peer sur les PE, à fin de voir que les relations BGP entre PE et CE ont été établies et sont dans l'état Established.

Dans l'exemple suivant, la relation d'égal à égal entre PE1 et CE1 est utilisée.

```
<PE1>display bgp vpnv4 vpn-instance vpna peer

 BGP local router ID : 1.1.1.1
 Local AS number : 100

 VPN-Instance vpna, Router ID 1.1.1.1:
 Total number of peers : 1                 Peers in established state : 1

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State  PrefRcv
  10.10.10.10     4       65100       94      108     0 01:30:14 Established        1
```

Fig III.14 Affichage bgp vpnv4 vpn-instance peer

3.3.9 vérification de la configuration

On Exécute la commande «display ip routing-table vpn-instance » sur chaque PE, afin de visualiser les routes vers les interfaces de bouclage des CE.

```
<PE1>
<PE1>display ip routing-table vpn-instance vpna
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : vpna
         Destinations : 7        Routes : 7

Destination/Mask    Proto   Pre  Cost        Flags NextHop         Interface

        5.5.5.5/32  EBGP    255  0             RD  10.10.10.10     Ethernet1/0/2
        6.6.6.6/32  IBGP    255  0             RD  2.2.2.2         Ethernet1/0/0
                    IBGP    255  0             RD  2.2.2.2         Ethernet1/0/1
     10.10.10.8/30  Direct  0    0             D   10.10.10.9      Ethernet1/0/2
     10.10.10.9/32  Direct  0    0             D   127.0.0.1       Ethernet1/0/2
    10.10.10.11/32  Direct  0    0             D   127.0.0.1       Ethernet1/0/2
      127.0.0.0/8   Direct  0    0             D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0             D   127.0.0.1       InLoopBack0
```

Fig III.15 Tables de routage VPN-BGP pour PE1

Les CE au sein d'un même VPN peuvent s'envoyer des pings entre eux.

-Ping1

```
CE1#ping 6.6.6.6 source 5.5.5.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/23/36 ms
CE1#
```

Fig III.16 Résultat du Ping

CE1 réussit à envoyer un Ping à CE2 sur 6.6.6.6.

-Ping 2 :

```
CE2#ping 5.5.5.5 source 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 6.6.6.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/18/24 ms
CE2#
CE2#
```

Fig III.17 Résultat du Ping

CE2 réussit à envoyer un ping à CE1 sur 5.5.5.5.

3.3.10 Conclusion

Dans ce chapitre nous avons présenté la simulation et la configuration du protocole SR-MPLS, au sein du réseau Backbone, tout en mettant l'accent sur les concepts relatifs à ce protocole en fonction des protocoles de routage interne et externe tel que BGP et OSPF. Nous avons également effectué des vérifications tout au long de ce travail et des tests de pings entre les clients.

Conclusion Générale

Conclusion Générale

Cette étude met en évidence une forte concurrence entre les différentes solutions actuellement utilisées par les fournisseurs de services pour transporter les données dans leurs réseaux centraux Il s'agit notamment de Segment Routing MPLS. Cependant, le développement rapide du marché pourrait bien donner l'avantage au SR-MPLS, sa mise en place dans le réseau à l'intérêt d'améliorer le cœur de réseau MPLS classique qu'était très complexe et qu'il manquait de l'évolutivité.

En effet, les réseau SR-MPLS permettent de passer des réseaux d'opérateurs classique vers une nouvelle tendance plus simple et plus performante destinée à être utilisée dans les futurs réseaux. La solution « SR-MPLS » présente un apport immense pour les réseaux grâce à son coût et la facilité d'installation justifiée par l'adaptation avec la configuration réseau MPLS existante (réseau opérationnel).

Pour cela, nous avons tenté de mettre en place la solution qui permettrait à l'entreprise de rendre leur réseau plus simple et à la fois évolutif. Ce travail a nécessité une étude des deux technologies MPLS et Segment Routing où nous somme basées sur l'architecture réseau existante, à partir de laquelle, nous avons configuré dans un premier temps le réseau MPLS et en second implémenter le protocole SR toute en introduisant les services L3VPN a permis la création de réseaux privés virtuels (VPN) qui a la capacité d'isoler les trafics. Cette technique permet la sécurisation des transferts de données tout en utilisant les réseaux publics pour réseau de transmission avec moins de complexité sans avoir besoin de protocoles de signalisation et ce qui ouvre de nouvelles voies de flexibilité et évolutivité.

D'autres étapes de recherche et de développement se poursuivront avec l'intégration du contrôleur de nœud SDN au sein du réseau SR.

Références bibliographiques

[01] https://study-ccna.com/what-is-ip-routing/ consulté le 15 mai 2022 a 14.30 h

[02] Azhar Ali Mian Sardar et Usman Khalid, 2010:Multi-Protocol Label Switching Traffic Engi-neering with QoS.

[03] https://networkencyclopedia.com/ consulté le 10 mai 2022 a 15 :24 h

[04] https://definir-tech.com/routage-dynamique consulté le 02 juin 2022 a 09 :00 h

[05] https://www.ibm.com/docs/en/zos/2.1.0?topic=terminology-interior-gateway-protocols consulté le 02 juin 2022 a 10 :00 h

[06] https://fr.acervolima.com/routage-de-monodiffusion-routage-d-etat-de-lien consulté le 03 juin 2022 a 12 :00h

[07] Randa BERKANI : Etude et simulation d'un réseau IP-MPLS sous GNS3, Université Mouloud Mammeri de Tizi-Ouzou.

[08] http://igm.univ-mlv.fr/~dr/XPOSE2007/ykarkab_MPLS/mpls.html consulté le 10 mai 2022 a 19 :24 h

[09] RAHANTANIRINA Odile Samoella ,2016 : PERFORMANCE VPN – MPLS, RAHAN, Licence UNIVERSITE D'ANTANANARIVO .

[10] R.MOTA. Segment Routing, Technical report, ACG, 2018. consulté le 28 mai 2022 a 10 :30h

[11] Duo Wu, **Lin Cui (2002).** A Comprehensive Survey on Segment Routing Traffic Engineering, digital communications and networks, vilume 8, issue 4.

[12] https://info.support.huawei.com/info-finder/encyclopedia/en/SR-MPLS.html consulté le 10 juin 2022 a 16 :15 h

[13] https://www.networkurge.com/2020/04/introduction-to-segment-routing.html consulté le 15 juin 2022 a 14 :25 h

[14] SAMU VARKAMA, 2017 : MPLS Segment Routing Technology Study, kaakkois-Suomen ammattikeakoulu.

[15] J.DURAND. Segment Routing, Technical report, Cisco Systems, 2017.

Annexe

Un routeur : est un équipement matériel informatique dont la fonction principale consiste à orienter les données à travers un réseau. Il permet, entre autres, de faire circuler des données entre deux interfaces réseau. Il peut également être présenté comme une passerelle entre plusieurs serveurs et facilite alors l'accès aux ressources disponibles sur le réseau pour les utilisateurs.

Un système autonome : Un système autonome (AS) est un groupe de réseaux et de routeurs contrôlés par un seul gestionnaire autorité.