الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Projet de fin d'études pour l'obtention du diplôme de Master

Filière : Télécommunication
Spécialité : Systèmes des télécommunications

Présenté par

Souilamas Hiba

Boukabous Meriem

Modèles d'inter connexion AS option C pourle service L3 VPN MPLS

Proposé par : Mr Yacine Kabir & Mr Tadjine Rabeh

Année Universitaire 2021-2022

Remerciements

Tout d'abord On remercie dieu qui nous a donné la force, le courage, la capacité et la volonté pour pouvoir terminer nos études avec succès et finir ce modeste projet qui reflète notre fierté et notre personnalité.

Nos remercîment s'adressent à tous ceux qui d'une manière ou d'une autre ont coopéré à l'élaboration de ce travail et particulièrement :

Notre promoteur Mr. KABIR Yacine et notre encadreur Mr. TADJINE Rabah qui nous ont guidé à concrétiser ce projet

A tous nos enseignants de l'université et Aussi ; à tous ceux qui ont de loin ou de prés enseignés à élaborer notre humble travail.

Les mots nous manquent pour exprimer notre profonde reconnaissance à notre tendre famille pour l'amour, la patience et le sacrifice qu'ils nous ont donné durant tous nos études.

Enfin, on adresse nos remerciements à tous nos proches, amis, qui nous ont toujours soutenus et encouragés.

Dédicace

JE Dédie ce modeste travail particulièrement à mes chers parents, qui ont consacré leur existence à bâtir la mienne, pour leur soutiens, patience, soucis tendresse et d'affections pour tout ce qu'ils ont fait pour que je puisse arriver à ce jour.

A **ma Mère** ; qui m'a encouragé durant toutes mes études et qui sans elle ma réussiten'auras pas eu lieux.

A **mon Père** ; qui est toujours disponible pour nous et prêt pour nous aider je lui confirme mon attachement et mon profond respect.

A mes chère frères **Hakim** et **EL Hadi**.

A ma tante **Amel** et ma petite sœur **Férial** qui me sont très chère.

A toute ma famille, qui m'a toujours soutenu, source d'espoir et motivation.

A mes meilleurs amis : **Hayat**, **Redha, Sarah, Nelma** et tous mes amis de ma promotion

A **Mr. TADJINE Rabah** qui m'a vraiment aider.

En fin je remercie **Meriem**, chère amie avant d'être mon binôme qui a contribué à la de ce modeste travail.

HIBA

Dédicace

A JE DÉDIE CE MÉMOIRE À:

La femme la plus merveilleuse de ma vie, qui s'est sacrifiée pour ma réussite et mon bonheur ; ma chère maman

A l'homme de ma vie pour tous ses sacrifices, son amour, sa tendresse et son soutien ; mon cher papa

Mes deux chers frères **LAMINE** et **ISLEM**

Mes chères cousines que j'aime beaucoup

Toute ma famille qui est ma source de joie et de bonheur

Mes meilleurs amis ; **CHAKIB**, **TEDJ EDDINE**, et mes amis de promotion

Monsieur **TADJINE RABAH** pour son aide, sa disponibilité et ses conseilsToutes

les personnes qui m'ont soutenue à la réalisation de ce travail.

Chère amie et mon binôme **HIBA**, pour son soutien, et sa compréhension tout aulong de ce projet

MERIEM

ملخص:

يفي الحل المنشور حاليا من قبل اتصالات الجزائر ا بالقيود المفروضة علىA VPN L3 inter AS option من حيث قابلية التوسع، وعزل VRFs بواسطة شبكات VPN على مستوىASBR، ووقت الاسترداد في حالة حدوث عطل وجودة الخدمة. في مواجهة هذا الموقف لجأنا إلى حل أكثر فاعلية يسمى AS inter MPLS / L3 VPN الخيار C والذي يسمح بتوصيل نظامين مستقلين مختلفين عن طريق تعيين Hop-Multi EBGP-MP المسؤول عن إعادة توزيع مسارات VPN خلال النهاية -يتم ضمان الاستمرارية بين MPLS ASBRs عن طريق تسمية بروتوكولات التبادل. سيكون لهذا الحل آثار كبيرة على تلبية توقعات الشركة ولكن أي من خلال ضمان جودة أفضل للخدمة) QoS) دون الحاجة إلى تغيير المعدات .

كلمات المفاتيح:.MPLS ،BGP-LU،MP-EBGP، L3 VPN

Résumé :

La solution déployée, actuellement, par Algérie Télécom répond partiellement aux contraintes du VPN L3 inter AS option A en termes de l'évolutivité, l'isolation des VRF par VPN au niveau de l'ASBR temps de rétablissement en cas de panne et QoS. Face à cette situation, nous avons eu recours à une solution plus efficace appelée VPN L3/MPLS inter AS option C qui permet de connecter deux autonome système différent par Une cession MP-EBGP Multi-Hop qui est chargée de redistribuer des routes VPN tandis que la continuité MPLS de bout en bout est effectuée entre les ASBR par des protocoles d'échange de labels. Cette solution aura comme principaux impacts de répondre aux attentes de l'entreprise mais aussi des clients en assurant une meilleure qualité de service (QoS) sans nécessité de changement d'équipements.

Mots clés : L3 VPN, MP-EBGP, BGP-LU, MPLS.

Abstract :

The solution currently published by Algeria Telecom partly meets the limitations of the L3 inter AS Option A VPN in terms of scalability, isolation of VRFs by ASBR level VPNs, recovery time in the event of a crash and quality of service. Faced with this situation, we have resorted to a more efficient solution called VPN L3/MPLS inter AS Option C, which allows to connect two different independent systems by assigning a MP-EBGP Multi-Hop which is responsible for redistributing the VPN paths during the End-to-continuity being ensured between MPLS ASBRs by naming exchange protocols. This solution will have major implications for meeting the expectations of the company but also of customers by ensuring better Quality of Service (QoS) without the need to change equipment.

Keywords : L3 VPN, MP-EBGP, BGP-LU, MPLS.

Table des matières :

Chapitre 3 : Simulation et résultats

Liste des acronymes et abréviations :

A

AT: Algérie Télécom.

AS: Autonome System.

ATM: Asynchronoustransfer modus.

ABR: Area Border Router

ASBR: Autonomous System Boundary Routers

AFI: Address-family Identifier

B

BGP: Border Gateway Protocol.

BGP –Lu: Border Gateway Protocol label unicast loop back

C

CE: Customer Edge.

E

ELSR: Edge Label Switching Router.

EVPN: Ethernet virtual private area network.

EBGP: Exterior Border Gateway Protocol

EBGP–Lu: Exterior Border Gateway Protocol label unicast loop back

F

FIB: Forwarding Information Base

I

IP : Internet Protocol.

IPv4 : Internet Protocol version 4

IPV6 : Internet Protocol version 6

IGP: Interior Gateway Protocol

IS-IS: Intermediate System to Intermediate System

IMET: inclusive multicast Ethernet Target

L

LDP: Label Distribution Protocol.

LIB: Label Information Base

LFIB: Label Forwarding Information Base

LSR: Label Switching Router.

LSP: Label Switched Path.

M

MPLS: Multiprotocol Label Switching

MP-BGP: Multiprotocol-Border Gateway Protocol

MP-EBGP: Multiprotocol-Exterior Border Gateway Protocol

MP-IBGP: Multiprotocol-interior Border Gateway Protocol

O

OSI: Open System Interconnection.

OSPF: Open Shortest Path First.

P

PBB: Provider Backbone Bridging.

P: Provider.

PE: Provider Edge.

Q

QoS: Quality of Service.

R

RSVP : Resource Réservation Protocol.

RD : Route distinguisher.

RMS : Réseau Multiservices.

RT: Route Target.

S

SAFI: Subsequent Address-family Identifier

SI : Système intermédiaire

V

VPN : Virtual Private Network.

VPN L2: Virtual Private Network Layer 2

VPN L3: Virtual Private Network Layer3

VRF: Virtual Routing and Forwarding.

VPLS: Virtual Private LAN Service

Liste des figures :

Liste des tableaux

Introduction générale

La croissance remarquable du nombre d'utilisateurs et la forte demande de servicesmultimédia étaient parmi les causes principales des dégradations du routage classique entermes de vitesse de traitement de données ainsi que pour le déploiement des nouveaux services. Les limites de ce routage ont donné naissance à l'idée de converger vers des réseaux plus performants afin de répondre aux besoins des clients en matière de débit, demobilité, et de disponibilité du réseau. MPLS (Multi Protocol Label Switching) s'est imposée comme alternative aux réseaux traditionnels.

L'évolution du réseau IP Core (IP MPLS Backbone) d'Algérie télécom et la croissance des sites assez considérable via ce réseau, a rendu plus difficile la gestion de la QOS client.

La solution utilisée actuellement par Algérie Télécom pour répondre aux besoins de leurs clients est les L3 VPN MPLS, basés sur des technologies bien connues comme MPLS et IP, sont actuellement les offres VPN les plus répandues commercialement qui est de manières d'interconnecter deux sites VPN alors qu'ils se trouvent géographiquement dans des **Systèmes Autonomes** (As) distincts.

pour effectuer de l'inter AS VPN, c'est-à-dire pour interconnecter des VPN de AS distincts faut opté a ces modèles, appelés options, sont au nombre de 3 option A, B, C. le VPN L3 MPLS inter AS option A est la solution déployée actuellement par Algérie Télécom qui sert à des connexions directes entre des VRF déclarés sur les routeurs de bordure de chaque As (VRF sur chaque routeur frontière).appelé VRF a VRF

Cette technologie, malgré ces nombreux avantages, présentent certaines contraintestelle que la transparence d la qualité de service, le temps de rétablissement en cas de panne, mais la véritable limitation de l'option A est l'évolutivité, 'isolation des VRF par VPN au niveau de l'ASBR … ont étaient observées par l'équipe d'exploitation de l'opérateur.

Cette problématique est constitué l'une des préoccupations majeures des ingénieursd'Algérie télécom. C'est pour cette optique qui nous a été proposé une solution qui permetde prendre en charge les limitations relevées par l'organisme d'accueil et qui sera capabled'ajouter de nouvelles fonctionnalités spécifiques à la gestion et permet une convergencerapide des réseaux.

Parmi les solutions existantes et disponibles qui permettra à Algérie Télécom de résoudre ces

contraintes, on retrouve le L3 VPN/MPLS inter AS option C, est une fonction qui permet de connecter deux autonome système différent par Une cession MP-EBGP Multi-Hop qui est chargée de redistribuer des routes VPN tandis que la continuité MPLS de bout en bout est effectuée entre les ASBR par des protocoles d'échange de labels. Elle peut être utilisé aussi dans la conception à grande échelle si l'entreprise dispose de plusieurs systèmes autonomes cela est fournis pour une bonne évolutivité.

Pour l'aboutissement à la solution décrite par notre thématique, nous avons segmenté le travail en trois chapitres :

Dans le premier chapitre, nous allons donner un aperçu global sur la technologie MPLS en expliquant dans un premier lieu son principe de fonctionnement et ses protocoles utilisées.

Ensuite, le deuxième chapitre Présentera l'étude théorique de la solution L3VPN/MPLS inter AS option C, sont fonctionnement, ses concepts, et ses avantages.

Enfin, le troisième chapitre présentera l'approche pratique de notre sujet L3VPN/MPLS option C en utilisant l'EVE et la présentation des résultats

Chapitre 1 Généralité et Concept

1.1 Introduction :

Le besoin en communication des entreprises a beaucoup évolué, aussi bien qualitativement que quantitativement. Il a donc été nécessaire de développer de nouveaux moyens d'échange, à base de réseaux informatiques. Pour une interconnexion sécurisée entre les sites distants d'une même entreprise partageant les mêmes ressources, l'une des solutions développe est la technologie VPN (Virtual Privat Network).

Virtual Privat Network L3, est une technologie de VPN niveau 3 éprouvée et largement déployée, chez Algérie Telecom on trouve le L3 VPN inter AS option A. cette dernière présente un certain nombre de limitations en ce qui concerne l'évolutivité, la redondance et la qualité de service QOS. Ces limitations sont des considérations importantes pour le développement d'une nouvelle solution, cette solution étant VPN L3 inter AS option C

Au cours de ce chapitre nous allons donner un aperçu de différentes technologies participant à la mise en place du VPN L3/MPLS inter AS option C. Nous allons passer par l'étude de l'existant d'Algérie Telecom, puis par quelques informations de base sur la technologie MPLS, ainsi que les protocoles BGP, RSVP et IS-IS.

1.2 Multi Protocol Label Switching :

Dans les réseaux informatiques et les télécommunications, la commutation multi protocole par étiquette MPLS (Multi protocol Label Switching) est un mécanisme de transfert de données basé sur la commutation d'étiquettes, qui sont insérées à l'entrée d'un réseau MPLS et supprimées à la sortie. [1]

Initialement, cette insertion se faisait entre la couche liaison de données (couche 2) et la couche réseau (couche 3) afin de transporter des protocoles comme IP. C'est pourquoi MPLS est appelé protocole de couche "2.5" ou "2/3". [1]

Le protocole a été développé pour fournir aux clients un service de transfert de données unifié utilisant la technologie de commutation de paquets. MPLS peut être utilisé pour transporter presque tous les types de trafic, tels que la voix ou les paquets IPv4, IPv6 et même les trames Ethernet ou ATM. Par conséquent, MPLS peut acheminer différents types de trafic sur une même infrastructure tout en les isolant. [1]

L'utilisation d'étiquettes dites de transport permet au routeur initiateur, pour chaque paquet, de déterminer à la source le routeur de sortie du réseau, sans que les routeurs intermédiaires aient besoin de consulter des tables de routage étendues lors de la transmission des paquets. MPLS fournit une technologie de commutation dont le rôle principal est de combiner les mécanismes des liaisons de données de couche 2 (vitesse) avec les concepts de réseau de couche 3 (flexibilité). [1]

1.2.1 Architecture MPLS (Multi protocol Label Switching):

En règle générale, on parle d'architecture MPLS. En fait, MPLS décrit une méthode d'encapsulation de différents protocoles de niveau 2 et de niveau 3 pour améliorer leur fonctionnement. Ensuite, nous disons qu'un protocole de niveau 2.5 fait référence à sa place entre la couche de liaison et la couche de routage

L'architecture MPLS (Multiprotocol Label Switching) est basée sur deux composants de base :

Plan de contrôle : Il permet de créer et de distribuer des routes et des étiquettes. Il utilise des protocoles tels que (OSPF, IS-IS ou BGP) pour contrôler les informations de routage de niveau 3, et des protocoles tels que (LDP, RSVP) pour contrôler l'échange d'informations et l'attribution d'étiquettes entre périphériques voisins.

Plan de données : Également appelé plan de transmission, il permet de contrôler la transmission des données. Il est responsable du routage des paquets marqués via le LSP et est principalement basé sur les tables MPLS suivantes :

- **LIB (Label Information Base) :** contient pour chaque sous-réseau IP la liste de l'étiquette affectée par lui et par les LSR voisins.

- **LFIB (Label Forwarding Information Base) :** est utilisé pour la commutation proprement dite du paquet labellisé. Il ne contient que les étiquettes du meilleur prochain saut.

- **FIB (Forwarding Information Base) :** est utilisé pour acheminer les paquets ne portant pas encore des étiquettes. [2]

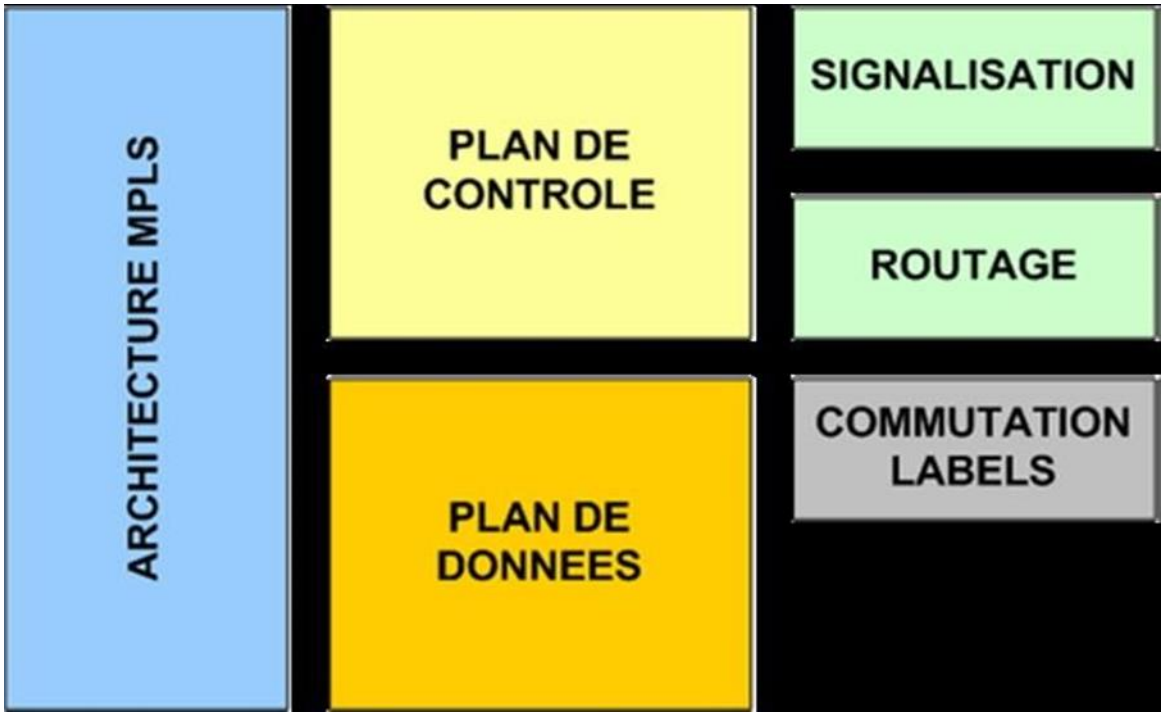

Figure 1.1 : Architecture de MPLS

1.2.2 Avantage MPLS (Multi protocol Label Switching):

MPLS fonctionne avec les protocoles réseau IP (Internet Protocol), ATM (Asynchronous Transfer Mode) et Frame Relay. Une erreur courante est de penser que c'est uniquement pour les réseaux privés.

Cependant, il a trouvé son emplacement choisi dans tous les réseaux du fournisseur deservices. Il permet une interconnexion optimisée et sans contrainte. Il offre également aux entreprises la possibilité d'externaliser plus facilement leur routage. Comme pour tous nos services aux professionnels, la mise en place d'un réseau d'entreprise utilisant la technologieMPLS s'accompagne d'un contrat (contrat SLA) garantissant niveaux et qualité de service.

Comme mentionné ci-dessus, en plus de cela, la qualité de service (QoS) est prise en charge, offrant plusieurs niveaux de service. Cette QoS est définie par votre opérateur et fait l'objet de services complémentaires à souscrire.[3]

1.2.3 Principe de réseau MPLS (Multi protocol Label Switching) :

Un domaine MPLS se compose de deux types de routeurs, LSR (Label Switching Router) et ELSR (Edge Label Switching Router). Les LSR sont des routeurs centraux capables de prendre en charge MPLS, tandis que les ELSR sont des routeurs utilisés pour établir un pont entre les domaines MPLS et d'autres réseaux tels que les clients IP.[18]

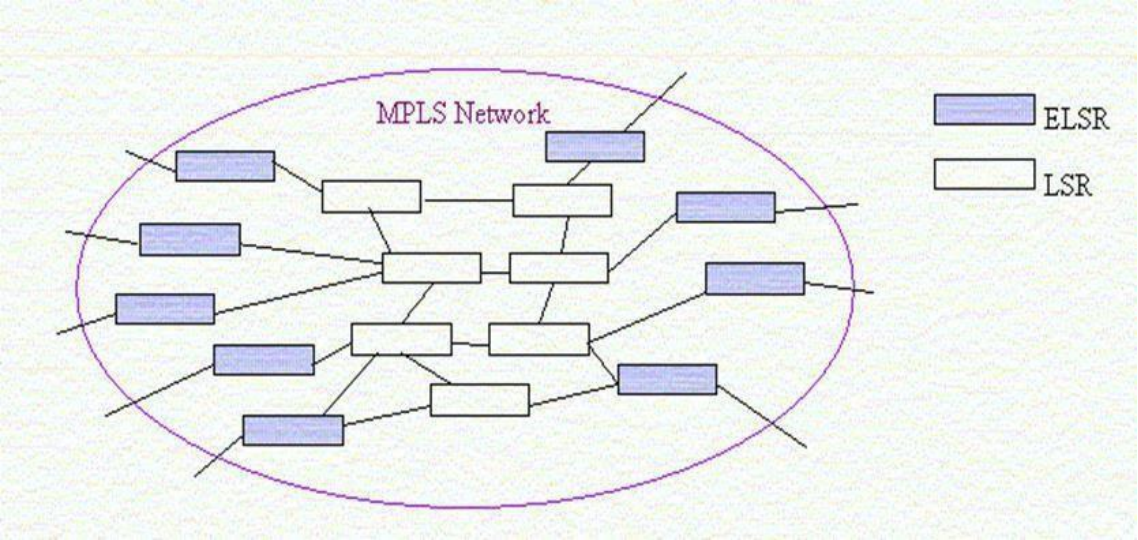

Figure 1.2 : MPLS Network

- **LSR** (Label Switching Router) : C'est le routeur central du réseau MPLS et il commute ces étiquettes vers la destination à travers le réseau sans consulter les en- têtes IP et les tables de routage.

- **LER** (Label Edge Router) : C'est le routeur d'interface entre le domaine MPLS et le monde extérieur. Il existe deux types de **LER** :

  - **Ingress LER** : Il s'agit d'un routeur qui gère le trafic entrant dans le réseau MPLS.
  - **Egress LER** : C'est le routeur qui gère le trafic sortant du réseau MPLS.[18]

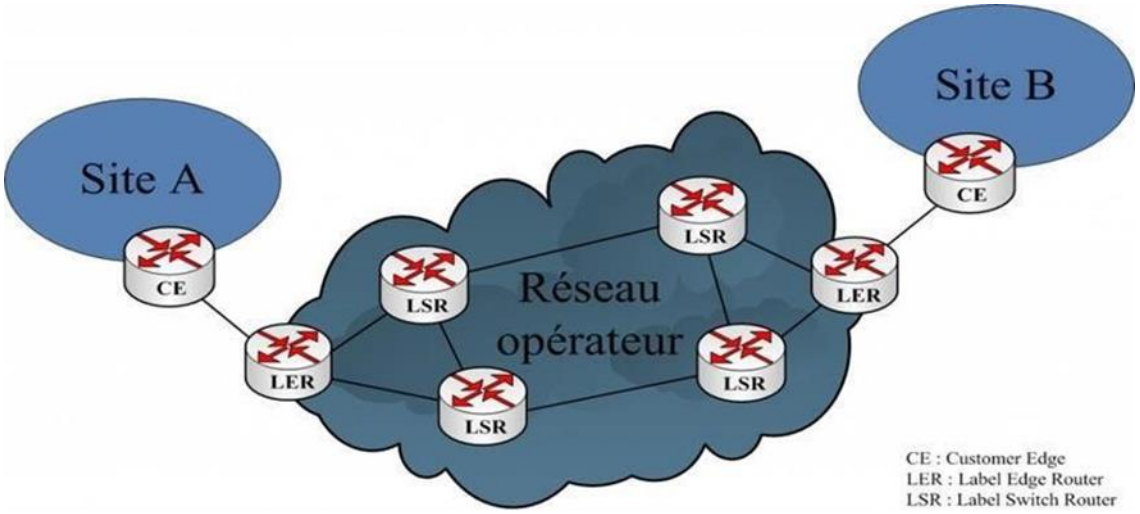

Figure1.3 : LSR-LER Architecture

1.3 Commutation de labels :

1.3.1 Labels :

Un en-tête MPLS est composé d'un ou plusieurs éléments de 4 octets chacun, les labels. Ce ou ces labels forment un empilement ou « pile » de labels, le Label Stack. Le nombre de labels dans le Stack dépendra des services MPLS utilisés.
Cet en-tête MPLS est inséré dans un paquet juste après l'en-tête de couche 2 (par exemple Ethernet, dont le champ Ethertype indiquera alors un contenu de type MPLS), et donc avant le protocole de couche 3 (au sens du modèle OSI) comme par exemple IP.[58]

1.3.2 Format :

Un label comporte 32 bits (4 octets), divisés en :

- Valeur du label (20 bits)
- Traffic Class (classe de trafic) pour la gestion de la QoS (qualité de service) (3 bits)
- 1 bit S «Bottom of Stack», indiquant s'il s'agit du dernier label dans le paquet (sinon, ce label est lui-même suivi d'un autre label)
- TTL (Time to Live), valeur positionnée selon le champ TTL du paquet IP ou à une valeur par défaut par le routeur d'entrée du nuage MPLS, et décrémentée à chaque saut, permettant ainsi lorsque le TTL arrive à 0 de détruire les paquets qui seraient victimes d'une boucle de routage (8 bits). [58]

Figure1.4 :L'entête de label

1.3.3 Valeurs :

Les labels de 0 à 15 sont réservés à des usages spécifiques (RFC 3032 et RFC 7274). On trouvera notamment :

0 : IPv4 Explicit Null Label : utilisé notamment dans le cadre de l'« Ultimate HopPopping » (UHP)

- ✓ 2 : IPv6 Explicit Null Label : utilisé notamment dans le cadre de l'« Ultimate HopPopping » (UHP)
- ✓ 3 : Implicit Null Label : utilisé dans le cadre de la signalisation du « Penultimate Hop Popping » (PHP) ce label correspond enréalité à une absence de label. [58]

1.4 Principe de fonctionnement de MPLS (Multi protocol Label Switching):

MPLS utilise divers protocoles pour transporter les paquets sur le réseau. Le fournisseur de services équipe les paquets d'étiquettes ou de balises afin que le chemin à utiliser puisse être déterminé.

Les différents chemins sont appelés LSP ou Label Switche Paths. Ce processus permet aux fournisseurs de services de décider à l'avance quel chemin est le meilleur pour différents types de trafic dans les réseaux privés ou publics. L'étiquette détermine le chemin à utiliser.

Le premier routeur MPLS (ou routeur d'entrée) insère une ou plusieurs étiquettes avantl'en-tête IP, puis transmet le paquet.

Les commutateurs de routage suivants ignorent l'en-tête IP et transmettent les paquetsen fonction des informations d'étiquette.

Le dernier routeur (appelé Egress) supprime alors l'étiquette et achemine le paquetIP vers sa destination finale. [19]

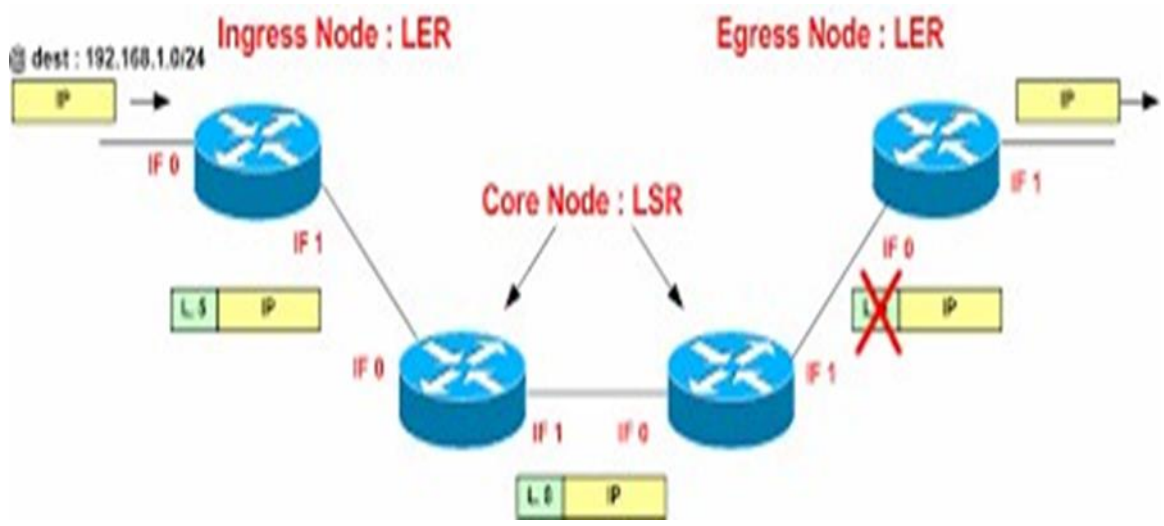

Figure 1.5 : Principe de fonctionnement de MPLS

1.5 Label Switch path LSP :

Un chemin à commutation d'étiquettes (LSP) est un chemin unidirectionnel à travers le réseau MPLS. Vous pouvez configurer un LSP à l'aide de l'un des protocoles de signalisation tels que LDP, RSVP ou BGP.

Le chemin commence au niveau d'un commutateur de périphérie du fournisseur d'entrée (PE), qui prend une décision sur l'étiquette à préfixer à un paquet en fonction de la classe d'équivalence de transfert (FEC) appropriée.

Les FEC sont un ensemble de paquets qui ont des caractéristiques identiques (ils utilisent le même saut suivant, la même interface) et doivent être transmis de manière similaire.[4]

Le commutateur PE transfère ensuite le paquet au commutateur suivant sur le chemin (le commutateur du fournisseur), qui permute l'étiquette externe du paquet ou fait apparaîtreune autre étiquette et la transmet au commutateur suivant.

L'action effectuée par le commutateur du fournisseur (éjection ou permutation) est déterminée par la position du commutateur dans le LSP.

L'avant-dernier commutateur du fournisseur ou le dernier commutateur du chemin (le commutateur de périphérie du fournisseur de sortie) supprime (saute) l'étiquette du paquet et transmet le paquet en fonction de son en-tête de niveau suivant (par exemple, IPv4).

Étant donné que le transfert de paquets via les LSP est opaque pour les couches réseausupérieures, les LSP sont parfois appelés tunnels MPLS. [4]

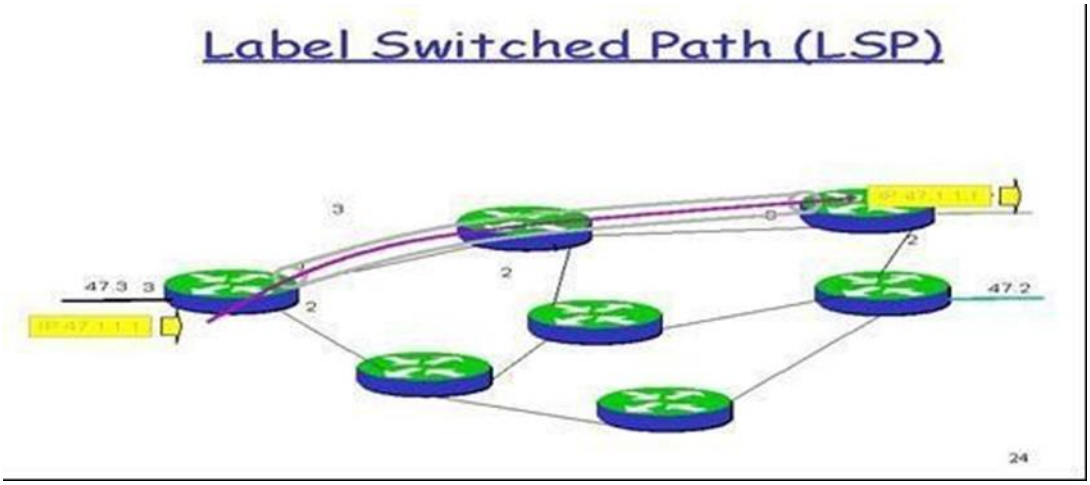

Figure1.6 : LSP Principe de fonctionnement

1.6 Les Protocoles LDP et RSVP :

1.6.1 Le Protocole LDP :

LDP (Label Distribution Protocol) est un protocole de distribution pas à pas défini parle groupe de travail MPLS de l'IETF (Internet Engineering Task Force). Il est totalement indépendant des protocoles préexistants.

D'autre part, il est le résultat d'un consensus durement acquis au sein d'un groupe de travail, et intègre généralement de nombreuses options opérationnelles qui sont autant de concessions à ce consensus. Nous n'en verrons ici qu'une partie pour ne pas surcharger le texte. LDP fonctionne sur le modèle de protocole de routage IP.

Il utilise ces tables de routage générées pour créer une table de commutation MPLS. Ilétablit automatiquement un chemin (LSP) entre le routeur d'entrée et le routeur de sortie du réseau (le chemin que les paquets IP appartenant à cette classe d'équivalence sortent du nuage MPLS) pour chaque "classe d'équivalence".

Il offre différents modes d'attribution et d'enregistrement d'étiquettes, ce qui le rend adaptable à différentes utilisations.

LDP à un principe très simple, chaque LSR attribue une étiquette à chaque LSR adjacent pour chaque classe d'équivalence qu'il reconnaît. Le voisin peut alors utiliser cette étiquette pour tous les paquets correspondant à cette classe d'équivalence qu'il lui adresse.[8]

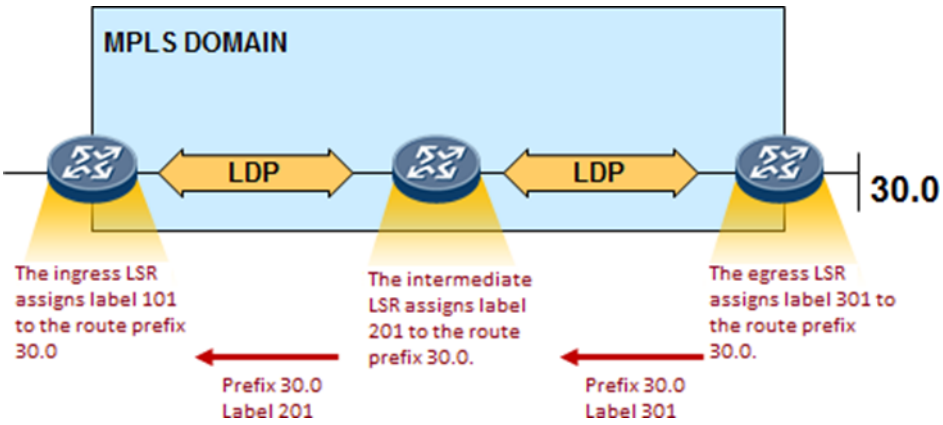

Figure 1.7 : L'architecture de LDP

1.6.2 Le Protocole RSVP :

Le protocole de réservation de ressources RSVP est un protocole de couche de transport qui réserve des ressources réseau et permet d'exécuter des applications Internet pour implémenter des données de qualité de service (QoS).

Cependant, à l'ère actuelle des systèmes en réseau, le temps est souvent plus important que la fiabilité. En revanche, RSVP est soutenu par un réseau QoS, fournissant à la fois la QoS et des données garanties.

RSVP est utilisé pour le flux de données et fournit la QoS à tous ses proxys/périphériques réseau. En utilisant RSVP, les clients peuvent demander la QoS du réseau pour les flux de données.

Les périphériques réseau tels que les routeurs utilisent RSVP pour fournir des informations à tous les nœuds du réseau.

Étant donné que RSVP n'est pas un protocole de routage, il obtient le chemin de données et les informations de routage des routeurs voisins

Les applications sur un réseau envoient des demandes de QoS. Les routeurs du réseau fournissent ensuite les informations demandées.

RSVP conserve tous les enregistrements des informations échangées.

RSVP est également utilisé pour maintenir et transporter les problèmes de trafic et de contrôle des politiques. [17]

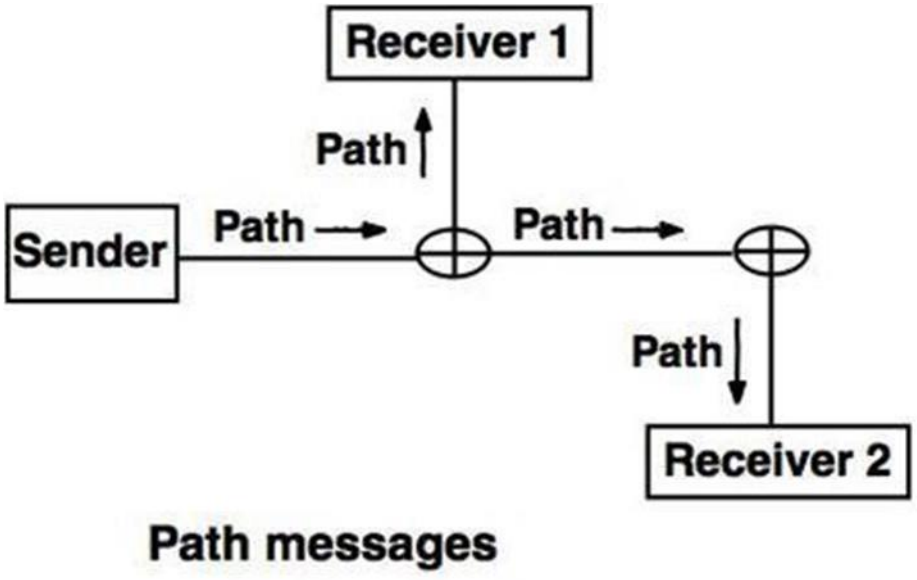

Figure 1.8 : Le protocole RSVP

1.7 Les divers Protocoles :

1.7.1 Le protocole OSPF :

Le protocole OSPF est un protocole de routage à état de liens normalisé par l'Internet Engineering Task Force (IETF). C'est actuellement l'IGP le plus utilisé.

Les messages d'état des liens permettent aux routeurs d'avoir une vue globale du réseauet de sa topologie, et ne déclenchent la publication de mises à jour que si la topologie change.

Pour générer la table de routage, le protocole OSPF utilise une autre arborescence Path (SPF Tree Short Path First Tree) et Short est Path Algorithm (SPF Algorithm) correspondant à l'algorithme de Dijkstra, qui détermine le meilleur chemin en fonction du coût.

Le coût d'un chemin dépend d'une métrique définie par l'opérateur sur chaque interface réseau, qui est un coût sans dimension.

Lorsque plusieurs routes ont le même coût, un équilibrage de charge équitable (Load-Balancing) peut être utilisé entre ces routes. Le nombre de routes pouvant être équilibrées est généralement limité (à quatre sur certains routeurs)[20]

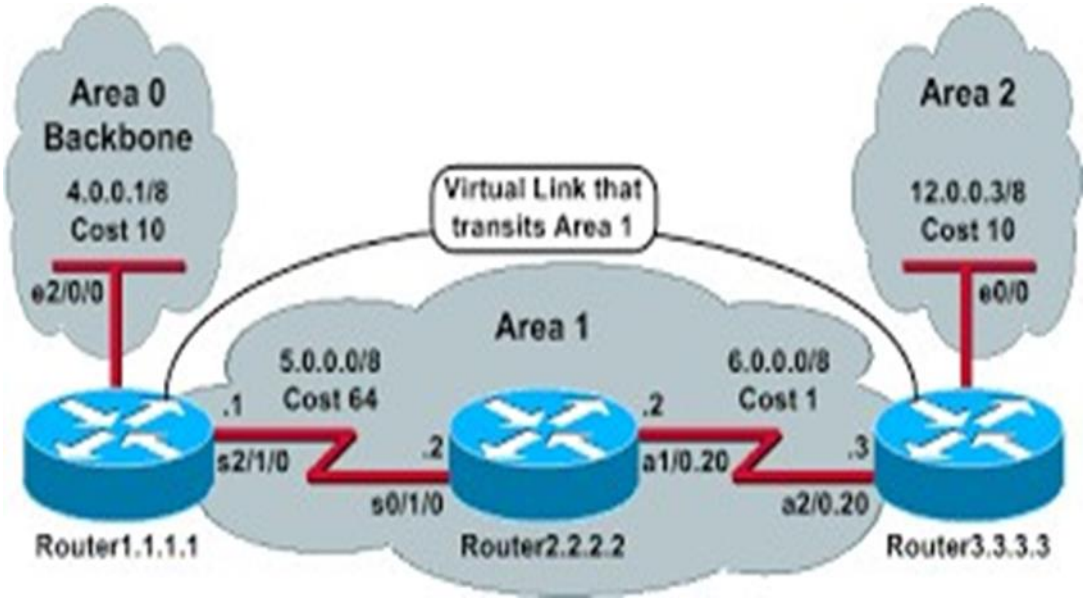

Figure 1.9: Liaison OSPF virtuelle

1.7.1.1 Les types d'areas de l'OSPF :

Les différents types d'areas de l'OSPF sont :

- **Backbone Area (Area 0) :** Le Backbone area est une area standard mais elle est le point central d'un réseau OSPF. Il n'y en a qu'une seule par architecture et toutes les autres areasdoivent être connectées à la Backbone Area

- **Standard Area :** L'area standard est une area normale. Elle doit être connectée à l'area 0.Elle peut faire transiter les paquets LSA de type 1, 2, 3, 4,5.
- **Stub Area :** L'area Stub est utilisé pour réduire le nombre de LSA. L'area Stub accepte les LSA de types 1,2 et 3 mais ne propage pas les routes externes LSA type 5 mais une route par défaut à la place. Pour qu'une area puisse être configurée en stub, il faut que tous les routeurs de l'area soient configurés en mode "stub".

- **Totally Stub Area :** L'area Totally Stub, tout comme la stub area ne propage pas les routes externes LSA type 5 mais elle ne propage pas non plus les routes inter-area

LSAtype 3, tout cela est remplacé simplement pour une route par défaut.

- **Not So Stubby Area (NSSA) :** L'area NSSA a les mêmes caractéristiques que l'area stub mais pas totalement. Contrairement à l'area stub elle accepte les routes externes générées par un ASBR. Ces routes externes sont de type LSA type 7. Ces routes sont converties en LSA type 5 avant d'être redistribuées dans les autres areas.

- **Totally NSSA :** L'area Totally NSSA ressemble à l'area NSSA à la différence qu'elle ne propage pas cette fois-ci les paquets LSA type 3 mais les remplace par une route par défaut.[5]

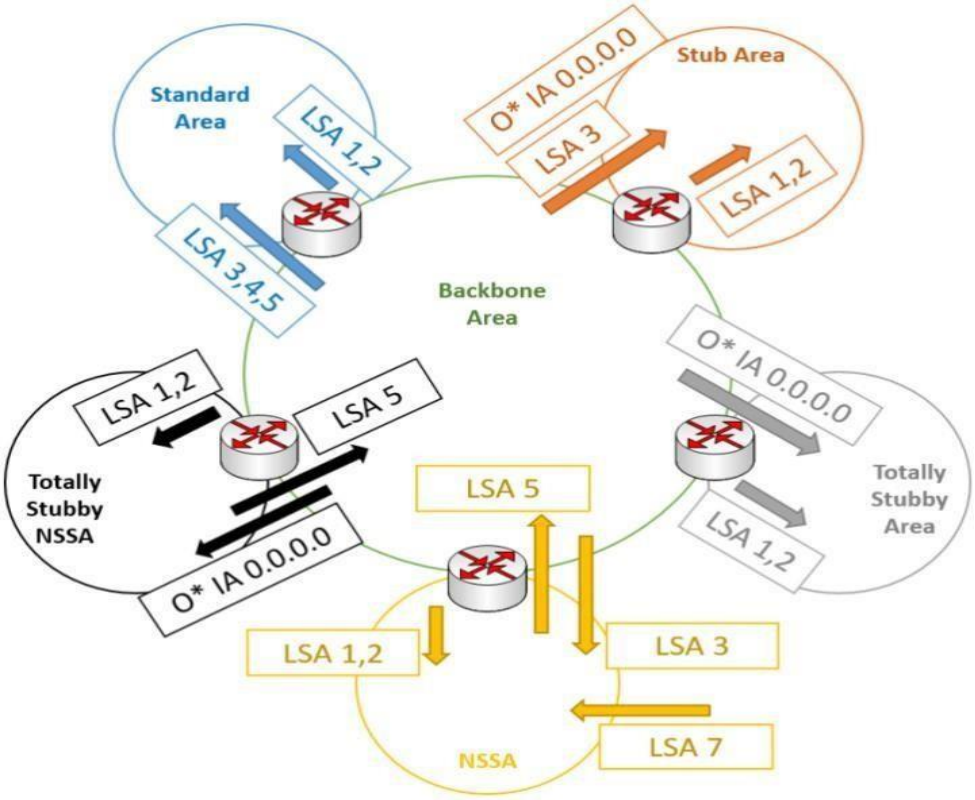

Figure1.10 : Les Area de l'OSPF

1.7.1.2 Les types des routeurs :

Dans les areas on trouve plusieurs types de routeurs en fonction de leur positionnementdans l'area.

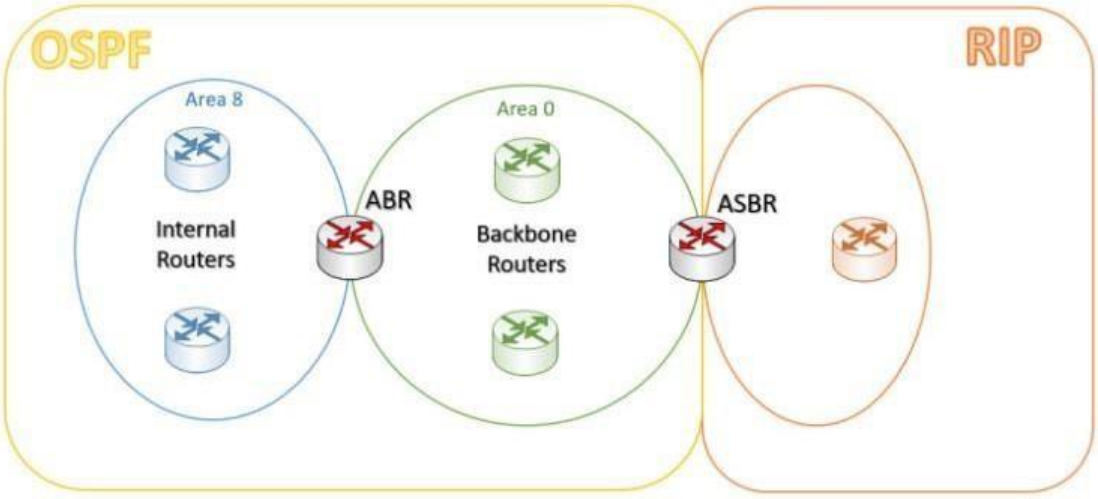

Figure 1.11 : les routeurs de l'OSPF

Les différents types de routeurs sont :

- **Internal Router :** Représente un routeur interne à une Area
- **Backbone Router :** Représente un routeur à l'intérieur de la Backbone Area
- **Area Border Router (ABR) :** Représente un routeur qui a une interface dans minimum 2 areas différentes.
- **Autonome Système Boundary Router (ASBR) :** Représente un routeur qui a une interface dans une area OSPF et une autre interface dans un autre protocole de routage.[6]

1.7.1.3 Les types de paquets LSA :

Les différents types de paquets LSA de l'OSPF sont :

- **Type 1** – Le LSA type 1 est généré par le routeur pour informer des liens qui sont directement connecté à lui
- **Type 2** – Le LSA type 2 est généré par le DR et décrit tous les routeurs de l'area

- **Type 3** – Le LSA type 3 est généré par un ABR pour transmettre un résumé des routes d'une area à une autre
- **Type 4** – Le LSA type 4 est généré par un ASBR et permet de faire connaître aux autres area le routeur ASBR
- **Type 5** – Le LSA type 5 est généré par un ABR pour redistribuer dans une area une route apprise par un autre protocole de routage
- **Type 7** – Le LSA type 7 est généré par un ASBR pour redistribuer une route externe dans une NSSA [7]

1.7.2 Le Protocole IS-IS :

IS-IS (Intermediate System to Intermediate System) est un protocole de routage conçupour déplacer des informations en déterminant le meilleur itinéraire pour les datagrammes via un réseau à commutation de paquets. [10]

IS-IS est un protocole d'état de liaison utilisé à l'intérieur des systèmes autonomes.
Les routeurs IS-IS conservent une vue topologique commune.

La base de données de topologie est construite séparément puis partagée entre tous lesrouteurs. Les paquets voyagent par le chemin le plus court

1.7.2.1 Principe de fonctionnement d'IS-IS :

Le Fonctionnement du protocole IS-IS est une hiérarchie à deux niveaux est utilisée pour prendre en charge les grands domaines de routage. Un grand domaine peut être divisé en plusieurs régions.

Les routes à l'intérieur d'une zone sont appelées routes de premier niveau et les routesentre zones sont appelées routes de second niveau. Le système intermédiaire peut être au premier niveau, au second niveau ou aux deux. [11]

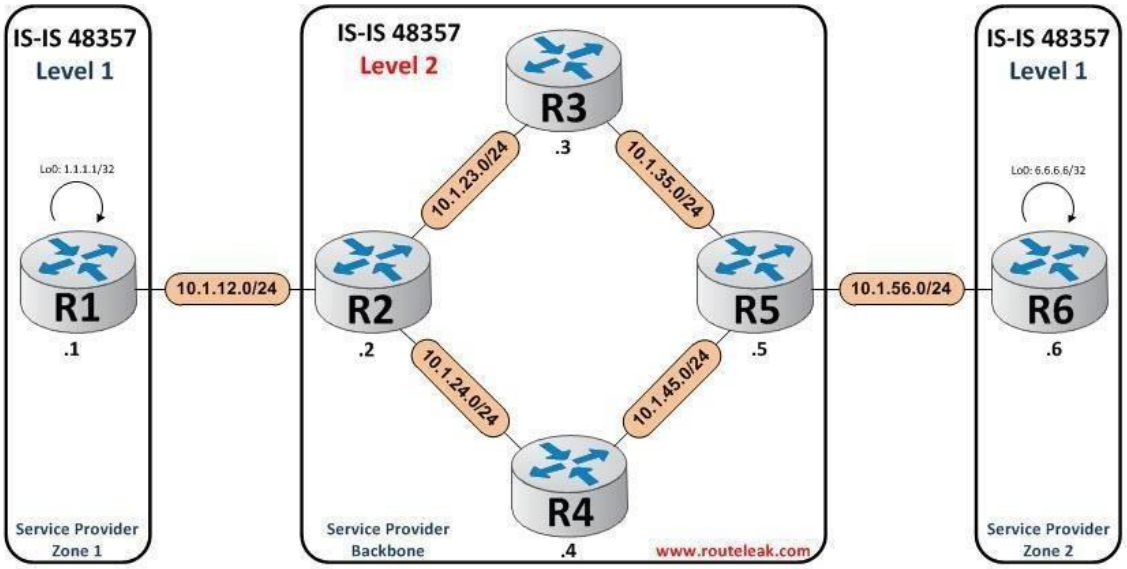

Figure 1.12 : IS-IS architecture

1.7.2.2 Les Types de zone IS-IS:

Dans OSPF, toutes les interfaces de routeur peuvent être affectées à une zone spécifique, mais le concept de zone dans IS-IS est différent. Ici en général, chaque routeur appartient à une zone.

L'idée vient du fait qu'IS-IS a été conçu à l'origine pour router CLNP (Connectionles Network Protocol), où les adresses appartiennent à des périphériques (routeurs), alors qu'enIP (Internet Protocol) les adresses appartiennent à des interfaces spécifiques.

Le protocole IS-IS a deux niveaux ou structures hiérarchiques, le niveau 1 et 2 :

Le niveau 1 correspond aux routes OSPF dans la zone, le niveau 2 correspond aux routes OSPF dans la zone dorsale 0, et les zones de niveau 2 sont toutes ajoutées à la zone de la zone dorsale.

Par défaut, chaque routeur est fourni en tant que routeur de couche 1-2 (L1/L2) pour faciliter la configuration et le déploiement.

Les routeurs de niveau 1 peuvent être adjacents aux routeurs de niveau 1 et de niveau1 à 2 (L1/L2). Les routeurs de niveau 2 peuvent être adjacents aux routeurs de niveau 2 ou de niveau 1 à 2 (L1/L2). Il n'y a pas de contiguïté entre les routeurs L1 uniquement et les routeurs L2 uniquement. [14]

1.7.2.3 Les Types de routeur IS-IS :

- ✓ **ROUTEUR DE NIVEAU 1 IS-IS (L1) :**

Un routeur IS-IS de niveau 1 possède les informations d'état de liaison de sa proprezone pour toute la topologie intra-zone.

Pour acheminer les paquets vers d'autres zones, il utilise le routeur de niveau 2 le plusproche (L1/L2).

La zone de niveau 1 se comporte à peu près comme la zone de Stubby OSPF. Lerouteur L1 uniquement envoie les paquets Hello L1.

- ✓ **ROUTEUR IS-IS DE NIVEAU 1-2 (L1/L2) :**

Un routeur L1/L2 IS-IS gère deux informations de base de données d'état de liens.
L'un concerne le niveau 1 et l'autre le niveau 2.

Par conséquent, deux calculs SPF (ShortestPath First) distincts sont exécutés, l'un surla base de données d'état de liaison de niveau 1 et l'autre sur la base de données d'état de liaison de niveau 2.

Le routeur IS-IS de niveau 1-2 se comporte très près du routeur ABR (Area Border Router) OSPF. Le routeur L1/L2 envoie des HELLO L1 et L2.

En tant que comportement par défaut, le routeur L1/L2 autorise uniquement le passaged'un chemin des préfixes de la zone L1 à la zone L2, mais pas en sens inverse.

Cependant, s'il est nécessaire de déplacer les préfixes de la zone L2 vers la zone L1, lacommande redistribute sous la configuration IS-IS est requise.

- ✓ **ROUTEUR DE NIVEAU 2 (L2) IS-IS :**

Un routeur IS-IS de niveau 2 possède les informations d'état de liaison pour le routageIntra-zone et Inter-zone.

Le routeur de couche 2 envoie uniquement des HELLO de couche 2.

La zone IS-IS de niveau 2 peut être comparée à la zone de Backbone 0 OSPF. [15]

1.8 Structure de réseaux multi service :

Algérie Télécom à deux domaines dans son réseau, et chaque domaine est indépendantde l'autre, comme s'il s'agissait de deux réseaux différents en termes de protocoles utilisés et de configuration particulière des services.

Le premier est Backbone IP/MPLS qui désigne le cœur d'un réseau informatique. Il s'agit, dans le monde d'Internet et des réseaux à haut débit, du centre névralgique du réseau.Il supporte à lui seul la plus grosse partie du trafic Internet. Pour réussir cette mission, le Backbone a deux grandes particularités : il met à profit les technologies les plus rapides (comme la fibre optique), et il dispose d'une bande passante très importante. (Figure 1.13)

Le second est Métro/Ethernet est une partie critique dans l'architecture réseau d'Algérie Telecom. Elle est constituée de plusieurs boucles régionales, pour couvrir tout le territoire national. Cette boucle permet d'assurer la distribution de services : voix, data, LTE(Long Terme Evolution), Wimax, wifi, liens spécialisés. L'une des solutions qu'Algérie Télécom fournit à ses clients est le VPN L3, qui permet à différents clients de connecter ses agences entre elles. . (Figure 1.14)

Après le développement dans le réseau Algérie Télécom, notamment dans le réseau Ethernet métropolitain, un problème est apparu dans le service VPNL3, qui n'était initialement utilisée que dans la zone Backbone IP/MPLS. Il a également dû être utilisé dans le réseau Ethernet du métro, ce qui entraîne beaucoup de problèmes de mauvaise évolutivité, une difficulté de prendre en charge la transparence de la qualité de service de l'entreprise et une répétition dans la configuration de chaque client plutôt qu'une seule fois, Et c'est la solution qui est maintenant appliqué dans le réseau Algérie Télécom, qui est connue sous le nom de BGP option A.

Afin de résoudre ce problème nous avons swap vers une autre solution connue sous le nom de BGP option C à travers le quelle la configuration sera deux fois seulement dans deux routeurs PE via un protocole connue sous le nom de BGP-LU.

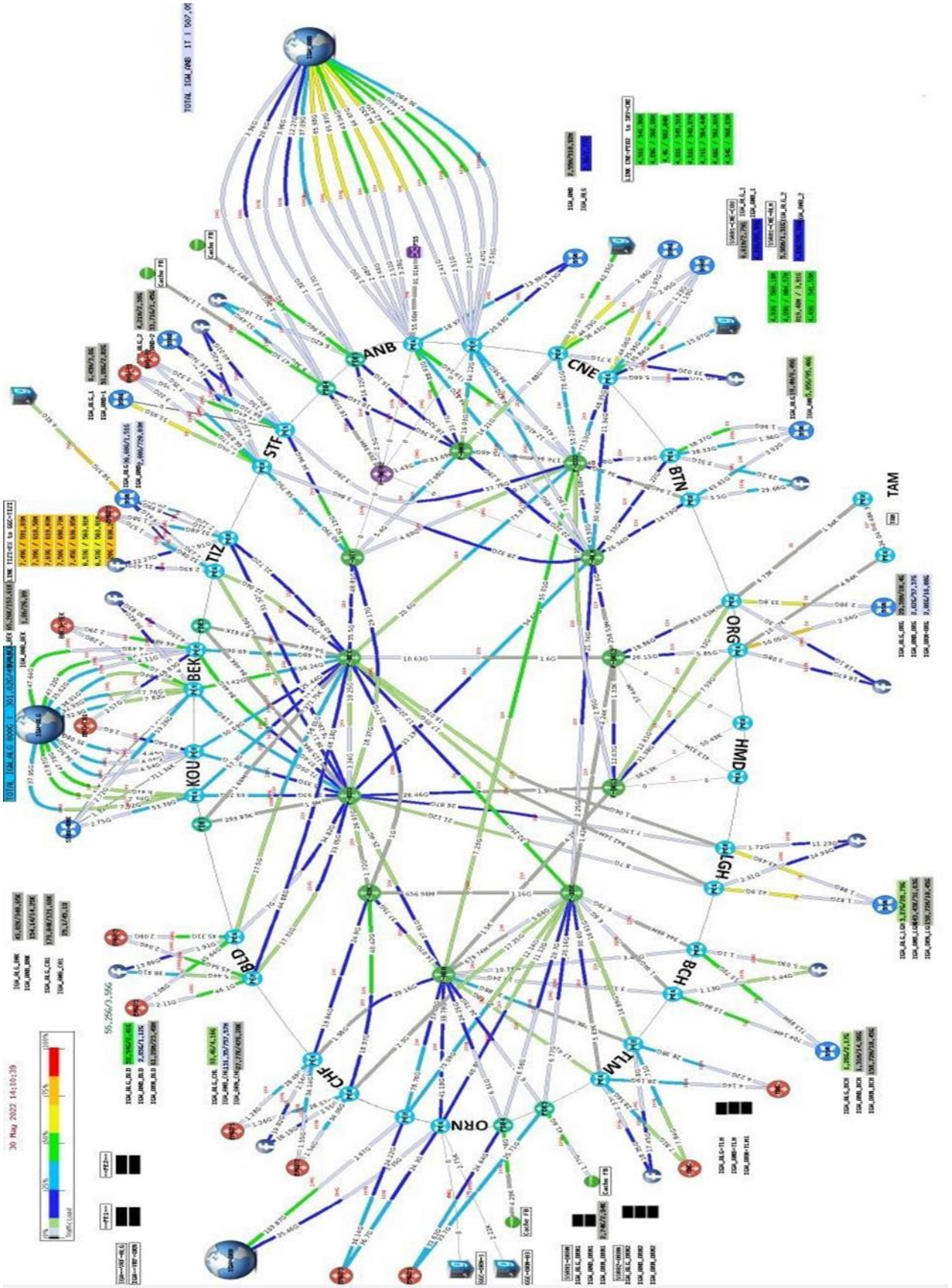
ANB
CNE
STF
BTN
TIZ
BEK
KOU
ORG
HMD
GLG
BLB
BCH
TLM
CHF
ORN
TAM
30 May 2022 14:10:29

Figure 1.13 : Architecture du Backbone AT.

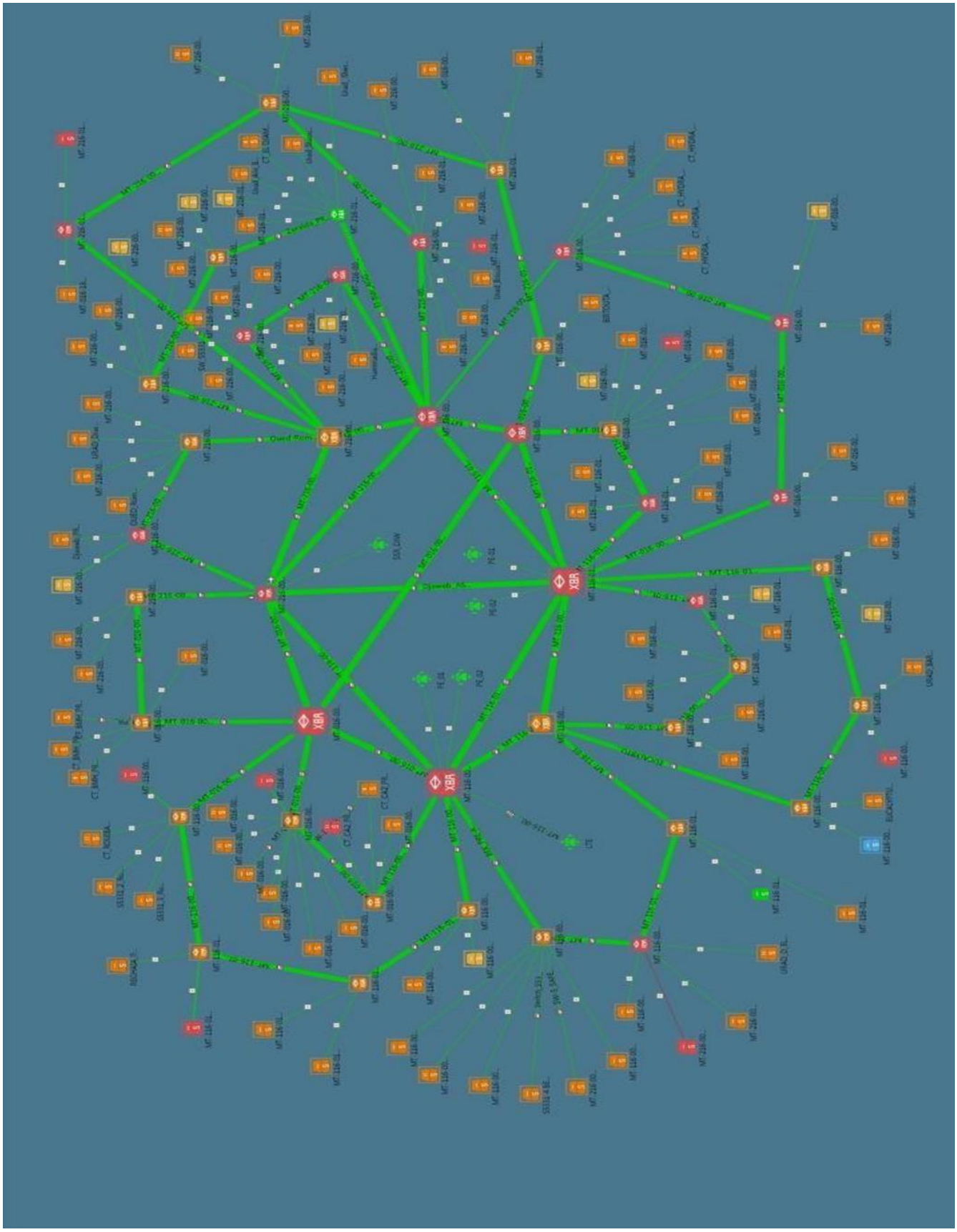

Figure 1.14 : Topologie du Backbone Métropolitaine

1.9 Conclusion :

Dans ce chapitre, nous avons présenté d'une part des généralités sur les différentes technologies, et d'autre part une étude sur le Backbone de l'opérateur AT.

Chapitre 2 Interconnexion AS option C pour le service L3 VPN /MPLS

2.1 Introduction :

La technologie mise en place actuellement au niveau d'Algérie Telecom (VPN L3inter AS option A) Inter AS VPN répond à un besoin simple qui survient lorsque deux sites clients VPN sont géographiquement situés dans des systèmes autonomes différents.

Le mécanisme d'interconnexion est alors utilisé, et ces modèles sont appelés : Options A, B et C. Le choix entre toutes ces technologies dépend de nombreux critères, comme la sécurité, la qualité de service, l'évolutivité, la convergence, ou encore la complexité de la mise en œuvre. Cela a poussé AT à proposer la nouvelle technologie VPN L3 inter AS option C qui ajoute de nouvelles fonctionnalités spécifiques et permet une convergence rapide des réseaux.

Dans ce chapitre, nous allons voir comment une solution basée sur BGP MPLS appelée Ethernet VPN (EVPN) peut répondre aux limitations précédentes

2.2 Les Protocoles de routage :

2.2.1 Le Protocol BGP :

BGP est un protocole de passerelle extérieure (EGP) basé sur des normes et il est considéré comme un protocole de routage "Path Vector".

BGP n'est pas conçu pour le routage au sein d'un système autonome (AS), mais pour le routage entre AS. Au lieu des métriques IGP (Interior Gateway Protocol) comme la distance ou le coût.

BGP maintient une table de routage séparée basée sur le chemin AS le plus court etdiverses autres propriétés. Au lieu d'utiliser des métriques traditionnelles, BGP prend desdécisions de routage basées sur les chemins traversés, les attributs de préfixe et un ensemble de règles de sélection définies par l'administrateur AS. C'est ce qu'on appelle le protocole de vecteur de chemin (pathvector protocol).

BGP prend en charge le routage sans classe et utilise l'agrégation de routes pour limiter la taille des tables de routage. La version 4 du protocole est utilisée sur Internet depuis 1994 et

le protocole précédent est considéré comme obsolète. Sa spécification estdécrite dans RFC 4271 A Border Gateway Protocol (BGP-4). [13]

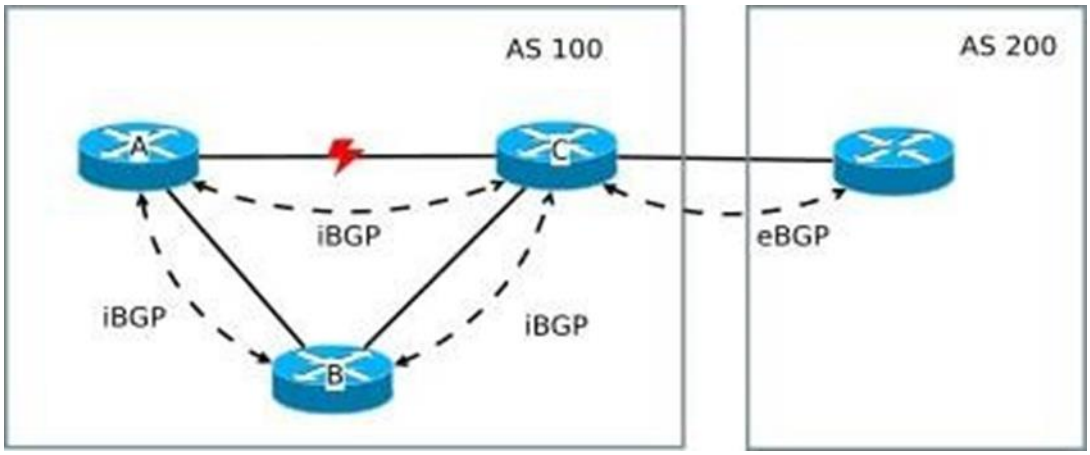

Figure 2.1 : Border Gateway Protocol

Pour que BGP fonctionne, les routeurs BGP doivent former des relations devoisinage. Il existe deux types de relations de voisinage BGP :

- **IBGP Peers- Voisins BGP** au sein du même système autonome.
- **EBGP Peers - Voisins BGP** se connectant séparément systèmes. [13]

2.2.2 Le Protocol MP-BGP :

La version normale de BGP (Border Gateway Protocol) ne prend en charge que lespréfixes de monodiffusion IPv4.

Maintenant nous utilisons MP-BGP (Multi-Protocol BGP) qui supporte différentesadresses :

- Monodiffusion IPv4
- Multidiffusion IPv4
- Monodiffusion IPv6
- Multidiffusion IPv6

Pour prendre en charge ces nouvelles adresses, MBGP dispose de nouvellesfonctionnalités que l'ancien BGP n'avait pas :

- **Identifiant de famille d'adresses (AFI):** spécifie la famille d'adresses.
- **Identifiant de famille d'adresses ultérieures (SAFI) :** Contient des informations supplémentaires pour certaines familles d'adresses.

- **Informations d'accessibilité de la couche réseau inaccessible multi protocole (MP_UNREACH_NLRI) :** il s'agit d'un attribut utilisé pour transporter des réseaux inaccessibles.
- **Annonce de fonctionnalité BGP :** utilisée par un routeur BGP pour annoncer les fonctionnalités qu'il prend en charge à un autre routeur BGP. MP-BGP et BGP-4 sont compatibles.[12]

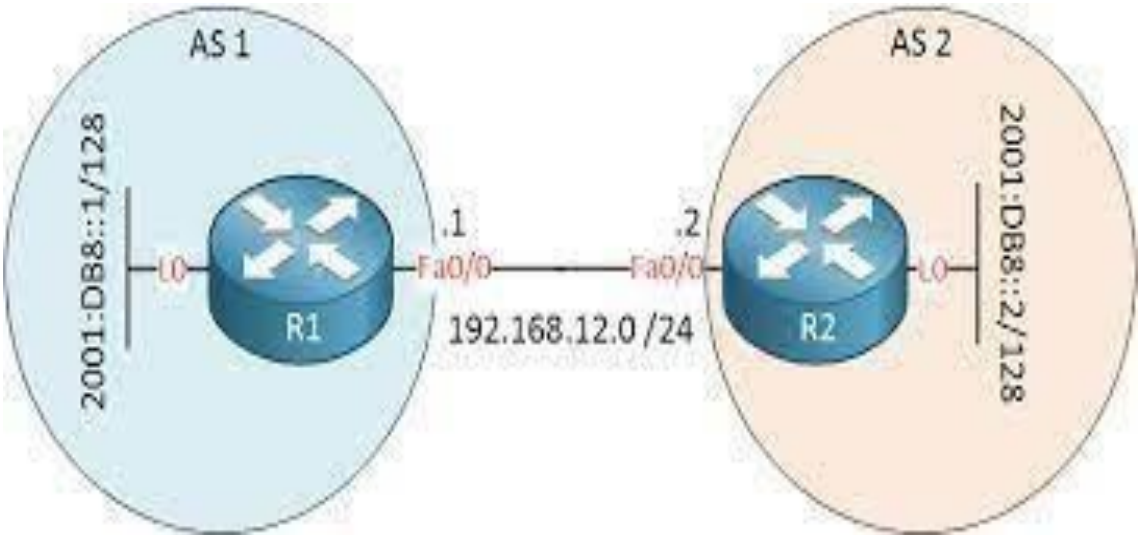

Figure 2.2: Multi-protocol Border Gateway Protocol configuration

2.2.3 Le protocole BGP-LU :

BGP- Lu permet à BGP d'annoncer une étiquette MPLS pour les préfixes IPv4 et IPv6 Unicast, si un préfixe IP est appris via des protocoles de routage IGP tels qu'OSPFet IS-IS, alors LDP, RSVP et Segment Routing peuvent attribuer une étiquette MPLS.

Mais si le préfixe est appris via BGP, seul BGP peut attribuer une étiquette MPLS.

L'attribution d'une étiquette par BGP pour le préfixe IPv4 ou IPv6 Unicast est appelée BGP Labeled Unicast.[16]

2.2.3.1 BGP-Lu dans le VPN MPLS Inter-AS :

Il est utilisé dans Inter-AS MPLS VPN Option C, entre les ASBR (Autonomous System Boundary Routers).

Dans l'Inter-AS Option C, les préfixes d'infrastructure des AS sont échangés etpour ces préfixes, l'étiquette MPLS est attribuée par BGP.

Inter-AS MPLS VPN Option C est utilisé lorsque l'évolutivité est requise, donc engénéral, il est utilisé lorsque l'évolutivité est l'exigence de conception de réseau fonctionnel (doit avoir une exigence). [16]

2.3 Virtuel Private Network VPN :

Un réseau privé virtuel *(*Virtual Private Network*)* est un tunnel sécurisé à l'intérieur d'un réseau (Internet notamment). Il permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP différente de celle de votre ordinateur. [9]

Un VPN inter-fournisseurs assure la connectivité entre différents AS. Cette fonctionnalité peut être utilisée par les clients VPN se connectant à plusieurs fournisseursde services différents ou au même fournisseur de services dans différentes régions géographiques (chacun avec un AS). La figure 11 illustre les types de topologies de réseauutilisées par les VPN fournisseurs. [55]

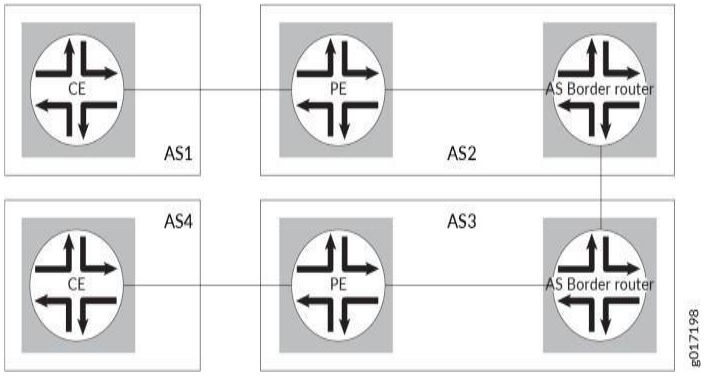

Figure 2.3 : Topologie de réseau VPN inter-fournisseur

2.3.1 Les types de VPN :

Un réseau privé virtuel (VPN) se compose de deux zones topologiques : le réseau du fournisseur et le réseau du client. Le réseau du client est généralement situé sur plusieurs sites physiques et est également privé (hors Internet). Un site client se composegénéralement d'un groupe de routeurs ou d'autres équipements de réseau situés à un seul emplacement physique. Le réseau du fournisseur, qui s'étend sur l'infrastructure Internet publique, se compose de routeurs qui fournissent des services VPN au réseau d'un clientainsi que de routeurs qui fournissent d'autres services. Le réseau du fournisseur relie les différents sites du client dans ce qui apparaît au client et au fournisseur comme un réseauprivé.

Pour garantir que les VPN restent privés et isolés des autres VPN et de l'Internet public, le réseau du fournisseur maintien des politiques qui séparent les informations de routage des différents VPN. Un fournisseur peut desservir plusieurs VPN tant que ses politiques séparent les routes des différents VPN. De même, un site client peut appartenirà plusieurs VPN tant qu'il sépare les routes des différents VPN. [56]

Chacun des VPN suivants a des capacités différentes et nécessite différents types de configuration :

2.3.1.1 VPN layer 2 :

Sur un VPN de layer 2, le routage s'effectue sur les routeurs du client, généralementsur le routeur CE. Le routeur CE connecté à un fournisseur de services sur un VPN de layer 2 doit sélectionner le circuit approprié sur lequel envoyer le trafic.

Le routeur PE recevant le trafic l'envoie via le réseau du fournisseur de services aurouteur PE connecté au site de réception. Les routeurs PE n'ont pas besoin de stocker ou de traiter les routes du client ; il suffit de les configurer pour envoyer des données au tunnel approprié.

Pour un VPN de layer 2, les clients doivent configurer leurs propres routeurs pour transporter tout le trafic de layer 3. Le fournisseur de services doit uniquement connaîtrela quantité de trafic que le VPN de layer 2 doit transporter. Les routeurs du fournisseur de services acheminent le trafic entre les sites du client à l'aide d'interfaces VPN de layer 2.
La topologie VPN est déterminée par les politiques configurées sur les routeurs PE. [57]

L'un des types de VPN layer2 le plus utilisé est l'EVPN et le VPLS

2.3.1.2 VPLS :

Le service de réseau local privé virtuel (VPLS) vous permet de connecter des sitesclients dispersés géographiquement comme s'ils étaient connectés au même réseau local. À bien des égards, cela fonctionne comme un VPN de couche 2. Les VPN VPLS et Layer 2 utilisent la même topologie de réseau et fonctionnent de manière similaire. Unpaquet provenant du réseau d'un client est d'abord envoyé à un dispositif CE. Il est ensuiteenvoyé à un routeur PE au sein du réseau du

fournisseur de services. Le paquet traverse le réseau du fournisseur de services via un MPLS LSP. Il arrive au routeur PE de sortie, qui transmet ensuite le trafic au périphérique CE sur le site client de destination.

La principale différence dans VPLS est que les paquets peuvent traverser le réseaudu fournisseur de services de manière point à multipoint, ce qui signifie qu'un paquet provenant d'un appareil CE peut être diffusé vers des routeurs PE dans le VPLS. En revanche, un VPN de couche 2 transfère les paquets uniquement de manière point à point. La destination d'un paquet reçu d'un périphérique CE par un routeur PE doit être connue pour que le VPN de couche 2 fonctionne correctement.

2.3.1.3 VPN Layer 3 :

Dans un VPN de layer 3, le routage s'effectue sur les routeurs du fournisseur de services. Par conséquent, les VPN de couche 3 nécessitent davantage de configuration dela part du fournisseur de services, car les routeurs PE du fournisseur de services doivent stocker et traiter les routes du client. [56]

L'un des types de VPN L3 le plus utilisé chez Algérie télécom est le VRF

2.4 VRF (Virtual Routing and Forwarding Table) :

La VRF est une table de routage associée à un VPN qui donne les routes vers les réseaux IP faisant partie de ce VPN. Chaque interface de PE, reliée à un site client, est rattachée à une VRF particulière. La table VRF permet de créer une isolation du trafic entre les différents sites clients n'appartenant pas au même VPN.

Cette technologie incluse dans les routeurs de réseau IP (Internet Protocol) qui permet à plusieurs instances d'une table de routage de coexister dans un routeur et de travailler simultanément. La fonctionnalité réseau est alors améliorée, car les chemins réseau peuvent être segmentés sans faire appel à plusieurs routeurs. Dans la mesure où letrafic est automatiquement isolé, le VRF permet aussi d'accroître la sécurité du réseau et d'éviter le chiffrement et l'authentification. Les fournisseurs d'accès Internet (FAI) s'appuient souvent sur le concept VRF pour créer des réseaux privés virtuels (VPN) distincts pour chaque client. C'est pourquoi on fait également référence à cette technologie sous l'appellation Routage et transfert VPN.

Le VRF se comporte comme un routeur logique, mais contrairement à ce dernier qui inclut plusieurs tables de routage, une instance VRF n'en utilise qu'une. En outre, le VRF requiert une table de réacheminement qui désigne le saut suivant - le trajet entre deux points de commutation étant appelé « bond » ou « saut » (hop) - pour chaque paquet de données, une liste des périphériques susceptibles de participer au transfert du paquet et un ensemble de règles et de protocoles de routage régissant le mode de transmission dupaquet. .[66]

Le BGP VRF offre un contrôle supplémentaire des routes de trafic, ainsi qu'une prise en charge des annonces conditionnelles compatibles BGP VRF vers ces familles deprotocoles d'adresse IP :

- ✓ Monodiffusion IPv4
- ✓ VRF monodiffusion IPv4 (vpn-ipv4)
- ✓ Monodiffusion IPv6
- ✓ VRF monodiffusion IPv6

L'affectation d'un ID de routeur BGP permet à la communication BGP VRF à VRF de seproduire sur le même routeur. Il peut être configuré manuellement pour chaque VRF différent ou attribué automatiquement via le mode de configuration de la famille d'adresses. [77]

2.4.1 Route Distinguisher (RD) :

Les routes échangées entre PE doivent être rendues uniques. Pour cela, un identifiant appelé RD (Route Distinguisher) codé sur 64 bits est ajouté à l'adresse IPv4 d'une VRF donnée pour créer une route unique, ce qu'on appelle VPN-IPv4. Les VPNv4sont supportées par MP-BGP.

Une distinction de route (RD) *distingue* un ensemble de routes (un VRF) d'un autre. Il s'agit d'un numéro unique ajouté au début de chaque route dans un VRF pour l'identifier comme appartenant à ce VRF ou client particulier. Un RD est transporté avecune route via MP-BGP lors de l'échange de routes VPN avec d'autres routeurs PE.

Un RD a une longueur de 64 bits et comprend trois champs : type (deux octets), administrateur et valeur. Il existe actuellement trois formats définis pouvant être utilisés par un fournisseur :

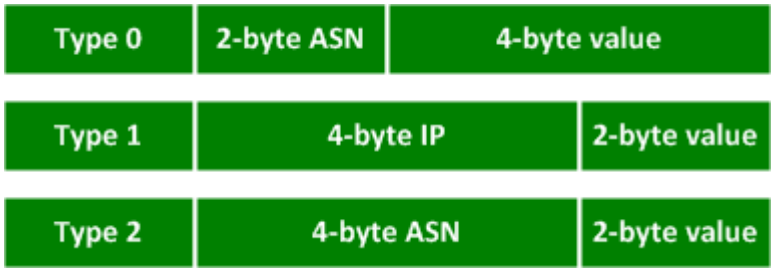

Figure 2.4 : Type de format RD

Le choix du format est en grande partie cosmétique : cela ne fait aucune différencepour BGP car le RD n'est en fait qu'un numéro plat ajouté au début d'une route. Le choixdes formats existe uniquement pour permettre une gestion flexible de l'espace des numéros.

Voici un exemple de configuration IOS montrant les RD affectés aux VRF en utilisant le format AS à deux octets. Le type est impliqué par le format dans lequel nous avons attribué le RD.

```
ip vrf Site_A
 rd 65000:10
!
ip vrf Site_B
 rd 65000:20
!
ip vrf Site_C
 rd 65000:30
```

Figure2.5 : Configuration IOS

Lorsque les routes VPN sont annoncées parmi les routeurs PE via MP-BGP, le RDest inclus dans la route avec le préfixe IP. Par exemple, une route pour 192.0.2.0/24 dans VRF Site_B est effectivement annoncée comme 65000:20:192.0.2.0/24 (en ignorant certaines complexités concernant la longueur réelle du préfixe). [21]

2.4.2 Route Target (RT) :

Un autre identifiant dit RT (Route Target) est utilisé pour définir la manière dont les routes VPN-IPv4 vont être insérées dans les VRFs des routeurs PE.

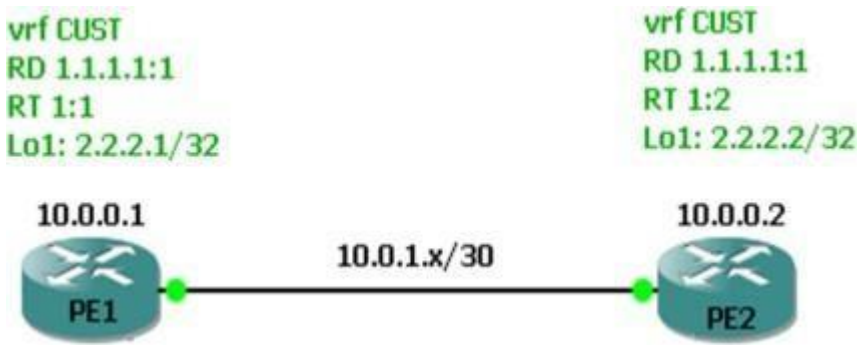

Figure2.6 : Le route Target entre deux routeurs

Alors que les rd sont utilisés pour maintenir l'unicité entre des routes identiques dans différents VRF, les RT peuvent être utilisées pour partager des routes entre elles. Nous pouvons appliquer des RT à un VRF pour contrôler l'importation et l'exportation de routes entre lui et d'autres VRF.

Une route Target prend la forme d'une communauté BGP étendue avec une structure similaire à celle d'un rd (ce qui explique probablement pourquoi les deux sont si facilement confondus). Une ou plusieurs routes Target peuvent être apposées aux routes dans un VRF à l'aide de la commande de configuration VRF **route-Target- export** :

```
ip vrf Customer_A
 rd 65000:100
 route-target export 65000:100
```

Figure2.7 : Commande de Configuration de VRF RT export

Les routes contenues dans ce VRF seront exportées avec un RT de 65000:100. Nous pouvons utiliser Wireshark pour examiner précisément comment ces informations sont transportées dans une mise à jour MP-BGP [21]

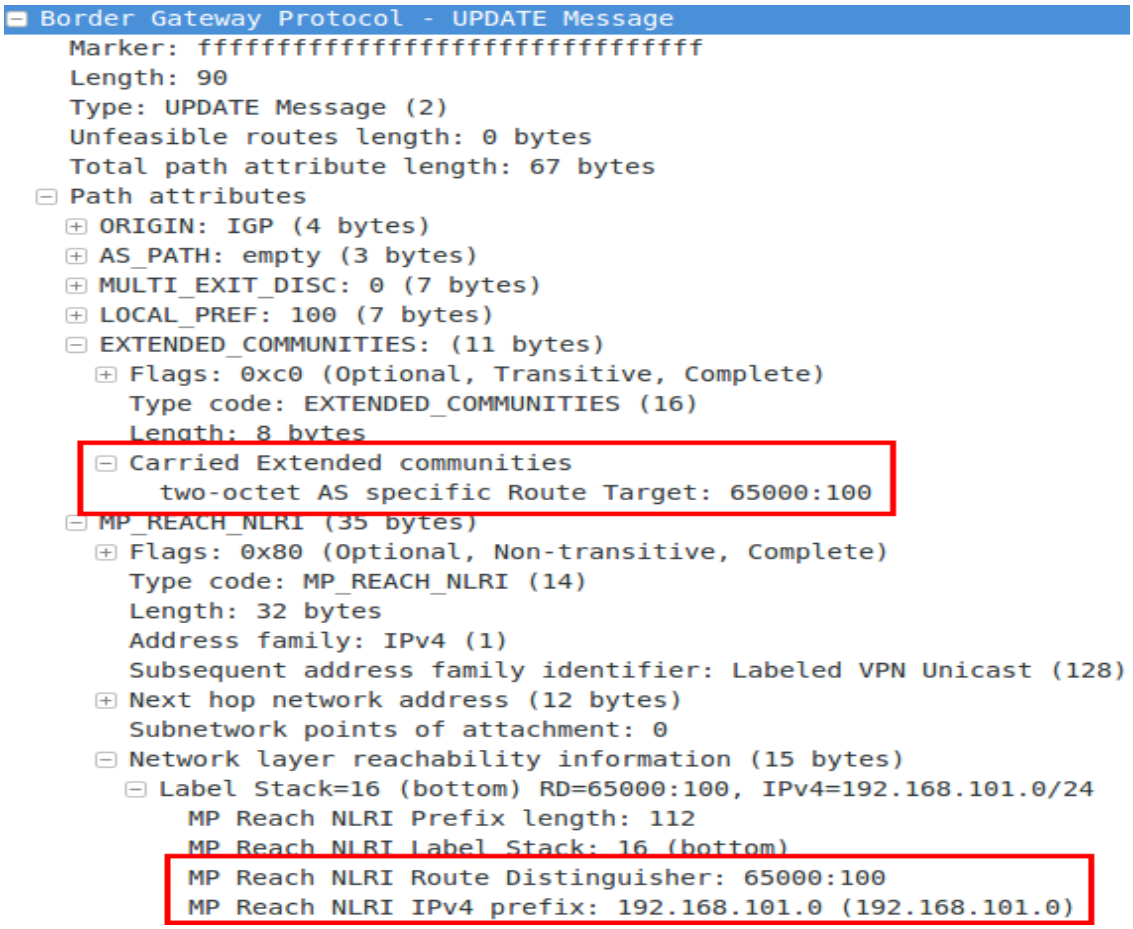

Figure 2.8 : Commande de Configuration de VRF RT import

En pratique, nous souhaitons généralement que toutes les instances d'un VRF sur le réseausoient informées de toutes les autres routes au sein de ce VRF sur les routeurs voisins. Nous ajoutons donc une deuxième déclaration pour permettre également l'importation :

```
ip vrf Customer_A
 rd 65000:100
 route-target export 65000:100 route-target import 65000:100
```

On peut utiliser la commande **route-Target-both** de raccourci en tant que macro pour ajouter les deux commandes simultanément. Les deux commandes s'afficheront séparément dans la configuration.[21]

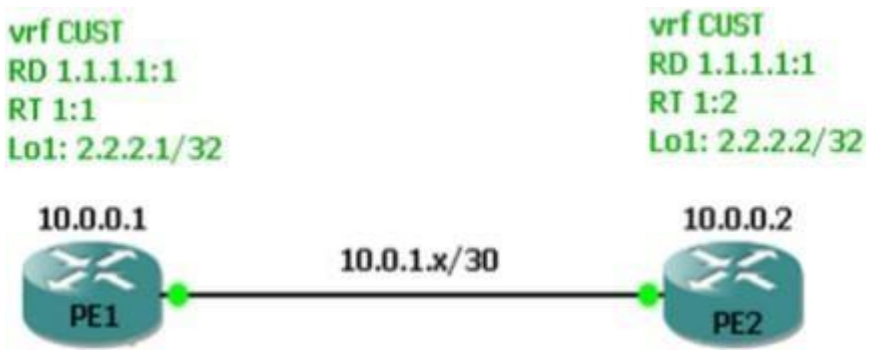

Figure 2.9 : les notions de VRF

2.4.3 Liaison des tables VRF entre système autonomes :

Vous pouvez connecter deux points d'accès distincts en reliant simplement la tablede routage et de routage VPN (VRF) du routeur de bordure AS (ASBR) d'une AS à la table VRF de l'ASBR dans l'autre AS. Chaque ASBR doit inclure une instance de routageVRF pour chaque VPN configuré dans les deux réseaux de fournisseurs de services. Vousconfigurez ensuite une session IP entre les deux ASBR. En effet, les ASBR se traitent lesuns les autres comme des routeurs de périphérie du CE client.

En raison de la complexité de la configuration, notamment en matière d'évaluation, cette méthode n'est pas recommandée. Les détails de cette configuration ne sont pas fournis avec la documentation. [65]

2.4.4 Avantages VRF :

Les VPN MPLS de couche 3 utilisent un modèle pair à pair qui utilise le protocoleBGP (Border Gateway Protocol) pour distribuer les informations relatives au VPN. Ce modèle Peer-to-Peer hautement évolutif permet aux abonnés d'entreprise d'externaliser les informations de routage vers des fournisseurs de services, ce qui se traduit par des économies de coûts importantes et une réduction de la complexité opérationnelle pour lesentreprises. Les fournisseurs de services peuvent alors offrir des services à valeur ajoutéetels que la qualité de service (QOS) et l'ingénierie du trafic, permettant une convergence du réseau qui englobe la voix, la vidéo et les données.

Les VPN basés sur IP utilisent l'instance Virtual Routing/Forwarding (VRF)-Lite de nouvelle génération, appelée Easy Virtual Network (EVN). Cela simplifie la virtualisation du réseau de couche 3 et permet aux clients de fournir facilement une séparation du trafic et une isolation des chemins sur une infrastructure réseau partagée, éliminant ainsi le besoin de déployer MPLS dans le réseau de

l'entreprise. EVN estentièrement intégré au MPLS-VPN traditionnel ou MPLS VPNomGRE.

2.5 Les Types d'interconnexion AS VPN L3 :

Pour les L3 VPN de couche 3 de nouvelle génération, les routeurs PE de l'AS utilisent le BGP externe multi protocole (MP-EBGP) pour distribuer les routes VPN- Internet Protocol version 4 (IPv4) à l'ASBR ou au réflecteur de route client ASBR. Les ASBR utilisent le BGP externe multi protocole (MP-EBGP) pour distribuer les routes VPN-IPv4 à leurs homologues ASBR dans l'AS. L'ASBR homologue utilise ensuite MP-IBGP pour distribuer les routes VPN-IPv4 étiquetées aux routeurs PE ou aux réflecteurs de route avec des routeurs PE en tant que clients. [59]

Cette partie décrit les différents modèles pour effectuer de l'inter AS VPN, c'est-à-dire pour interconnecter des VPN d'AS distincts. Ces modèles, appelés options, sont au nombre de 3 :

2.5.1 Inter AS Option A :

L'option A est la plus simple des options d'interconnexion. L'ASBR de chaque ASdéfinit une interface ou une sous-interface par VRF. Une fois défini, l'ASBR instancie leVRF en attribuant la sous-interface au VPN. Cela doit être fait par VPN nécessitant un service Inter-AS.

Les sous-interfaces faisant face à l'autre AS ne transportent pas de trafic étiqueté, uniquement du trafic IP normal. Afin d'échanger des informations de routage avec l'ASBR distant, n'importe quel protocole de routage peut être utilisé. [70]

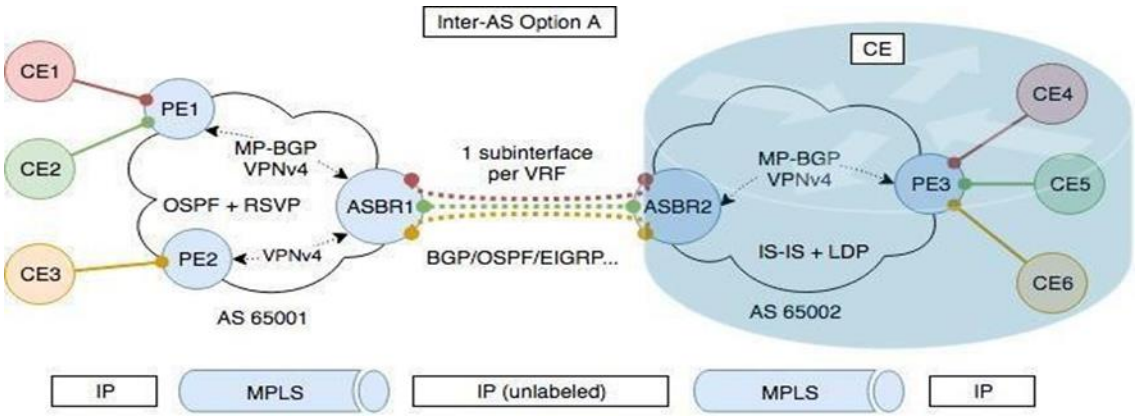

Figure 2.10 : Topologie inter-AS Option a

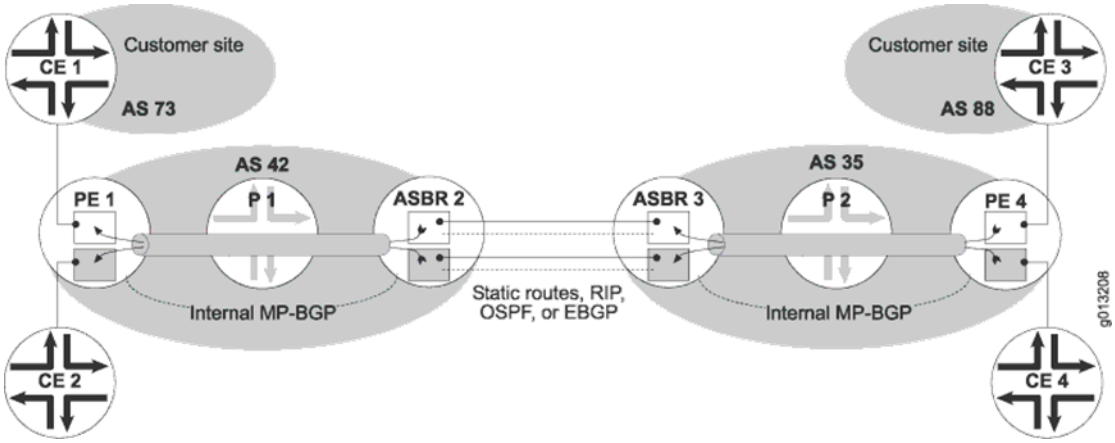

Figure 2.11 : VRF sur chaque routeur frontière AS

Au sein de chaque AS, les routes sont annoncées par MP-BGP interne et les paquetsde données sont transmis via un tunnel MPLS. Vous créez une connexion logique telle qu'un VC ATM entre chaque paire de VRF (sur des routeurs de frontière AS distincts) ces connexions logiques peuvent partager la même connexion physique.

Les tunnels MPLS sont unidirectionnels, La figure 2.11 montre uniquement les tunnels établis pour acheminer le trafic de l'ASBR 2 vers le PE 1 et du PE 4 vers l'ASBR 3. Notez que l'ASBR 2 et l'ASBR 3 sont également des routeurs PE. En ce sens, l'ASBR 2 traite l'ASBR 3 comme un routeur CE et l'ASBR 3 traite l'ASBR2 comme un routeur CE.

Inter AS Option A est la technologie VPN MPLS inter-système autonome la plussimple, la plus flexible et la plus sécurisée.

2.5.1.1 Les Avantages de l'option A :

- Facile à comprendre, déployer et dépanner
- Points de démarcation clairement définis entre les fournisseurs (démarcation SLA)
- Maintien de l'ordre, filtrage et comptabilité par VPN sur un seul point (sous-interface VRF)
- Flexibilité dans la sélection de protocole par AS et entre ASBR
- Définit des points de démarcation clairs entre les fournisseurs de services VPNMPLS L3
- Facile de déploiement [70]

2.5.1.2 Les Inconvénients de l'option A :

- Mauvaise évolutivité
- Difficile de prendre en charge la transparence de la qualité de service del'entreprise

Mais la véritable limitation de l'option A est l'évolutivité de la solution L'isolation des VRF par VPN au niveau de l'ASBR est réalisée en définissant :

- Une sous-interface par VRF
- Un VRF par VPN (le VRF doit être instancié sur l'ASBR)
- Une session de routage EBGP (si BGP est utilisé) par VRF

Et cela a un impact ÉNORME sur l'évolutivité à mesure que le nombre de VPN à étendre augmente. [70]

2.5.2 Inter AS Option B :

La deuxième méthode est appelée option inter-AS B ou 2547 bis option B.

Cette méthode utilise BGP pour envoyer des étiquettes VPN entre les routeurs de bordure AS.

Les tunnels MPLS de base sont locaux à chaque AS. Les tunnels empilés s'exécutent de bout en bout entre les routeurs PE sur différents AS. Cette approche offre une plus grande évolutivité car seul le RIB BGP stocke toutes les routes VPN inter- domaines.

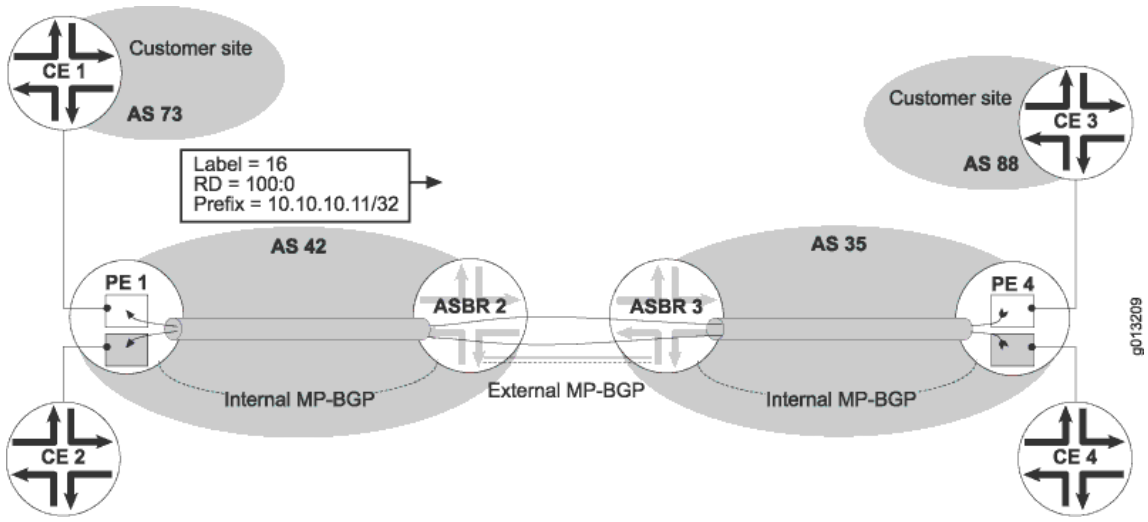

Figure 2.12 : ***Topologie inter-AS option b avec tunnels MPLS***

Le PE 1 attribue des étiquettes pour les routes aux sites clients et distribue à la foisles attributions d'étiquettes et les routes VPN-IPv4 dans l'AS 42 dans des messages de mise à jour BGP étendus au moyen de MP-BGP interne. L'ASBR 2 distribue ensuite les routes à l'ASBR 3 avec MP-BGP externe ; L'ASBR 2 se définit comme l'adresse du saut suivant et attribue une nouvelle étiquette à la route afin que l'ASBR 3 puisse diriger correctement le trafic. L'ASBR 3 propage les routes par MP-BGP interne dans l'AS 35, ycompris vers le PE 4. [71]

2.5.3 Inter AS Option C :

L'option C'est La troisième méthode de configuration des services inter-AS et desVPN inter-AS C'est l'option la plus évolutive des trois à ce jour Cette option présente de nombreuses similitudes avec l'architecture et les concepts de l'opérateur, comme les routes externes et internes, les protocoles utilisés pour échanger ces informations de routage et la configuration des chemins commutés étiquetés des PE d'entrée aux PE de sorti. [69]

L'option inter-AS C nécessite un chemin à commutation d'étiquettes entre le routeurPE d'entrée du paquet et son routeur PE de sortie. L'option C introduit la redistribution EBGP multi-sauts des routes VPN-IPv4 étiquetées entre les systèmes autonomes source et de destination. Les routes IPv4 balisées sont redistribuées par EBGP entre les systèmesautonomes adjacents.

Chaque ASBR maintient des routes IPv4/32 étiquetées vers ses routeurs intra-AS PE. ASBR distribue ces routes à d'autres systèmes autonomes utilisant EBGP. Si la topologie contient des systèmes autonomes de transit, leurs ASBR doivent également distribuer les routes /32 étiquetées EBGP. Cette configuration crée un chemin à commutation d'étiquettes du routeur PE d'entrée au routeur PE de sortie. Cette configuration permet aux routeurs PE de différents systèmes autonomes d'établir des connexions EBGP multi-sauts entre eux et d'échanger des routes VPN-IPv4 sur ces connexions.

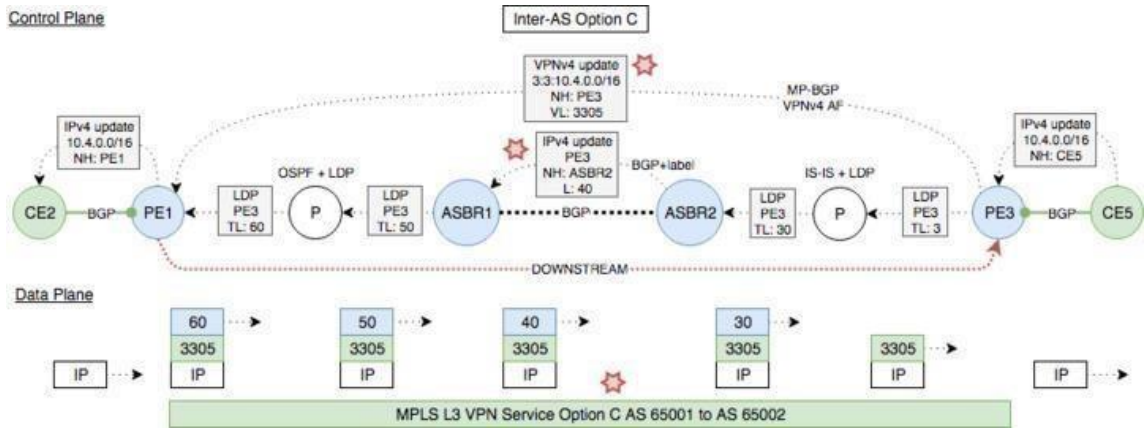

Figure2.13 : Topologie inter-AS Option c

L'Inter-AS Option C utilise BGP comme protocole de distribution d'étiquettes. Lesroutes IPv4 balisées sont redistribuées entre les systèmes autonomes adjacents par eBGP. Une nouvelle famille d'adresses étiquetées inet a été ajoutée pour maintenir le routage unicast étiqueté. Ce tableau aide à résoudre les routes L3VPN qui utilisent l'encapsulationMPLS. La figure 22 illustre la connectivité et les rôles des différents composants de cettearchitecture.

2.5.3.1 Les Avantages de l'Inter-AS Option C :

- Bonne évolutivité
- Les ASBR ne stockent pas d'informations de routage externe
- Préservation des ressources car les informations externes ne sont pas dupliquéessur les ASBR. Les RR stockent déjà les routes.
- Intégration MPLS simplifiée
- Conservation des ressources
- Il peut toujours être utilisé dans la conception à grande échelle si l'entreprisedispose de plusieurs systèmes autonomes. (Pas entre les fournisseurs de services). [68]

2.6 conclusion :

Dans ce chapitre nous avons présentées la solution la plus adaptés VPN L3 inter ASoption C qui répond aux problèmes rencontrés par AT, en se basant sur ses notions et sesprincipes.

Dans le prochain chapitre, on définit les étapes de notre application et la simulationde VPN L3/MPLS option C

Chapitre 3 La mise en place de la solution L3 VPN MPLS inter AS Option C

3.1 Introduction :

Algérie Télécom utilise pour ses clients la technologie VPN L3 inter AS option A comme technologie de VPN niveau 3. Cette la technologie malgré ses nombreux avantages, présentent certaines contraintes telles que la mauvaise évolutivité, le temps de rétablissement en cas de panne, et la qualité de service QOS et la sécurité qui ont étaient observées par l'équipe d'exploitation de l'opérateur. C'est pour ces raisons que ces derniers ont envisagé d'implémenter une nouvelle solution, qui répond à l'attente des clients (besoin).
Après avoir effectué une étude de l'existant, au niveau d'Algérie Télécom, et présenté certaines solutions pouvant répondre aux besoins de l'opérateur telle que la solution VPN L3 inter AS option C que nous avons présentée, lors des chapitres précédents, nous passons maintenant la partie pratique qui présente la mise en œuvre de la simulation de notre réseau basé sur cette technologies.
En premier lieu nous fournissons un aperçu des outils choisis pour réaliser la simulation.
Ensuite nous présenterons les configurations mises en place pour établir la solution VPN L3 MPLS inter AS option C

3.2 Description de l'application :

Dans la technologie VPN L3 MPLS déployée actuellement chez Algérie Télécom, on trouve le VPN L3 inter AS option A, Ce dernier, même si il a plusieurs avantages, Il présente des inconvénients et des limites tel que le problème de, l'évolutivité, QOS sécurité et convergence qui ont étaient observées par l'équipe d'exploitation. Afin de surmonter ces limites, et arriver à atteindre les performances recherchées en terme de bonne évolutivité et de rétablissement rapide en cas de panne, nous suggérons le déploiement de le VPN L3 MPLS inter AS option C.

3.3 Outils utilisé :

- **Junos :**

Le système d'exploitation Junos (Junos OS) utilisé dans les périphériques réseau Juniper Networks crée un environnement permettant d'accélérer le déploiement de services et d'applications sur un

réseau unique.

- **Eve EVE-NG :**

Est un outil similaire à GNS3 qui fournit aux administrateurs réseau des moyens de simuler des routeurs, des commutateurs, des pare-feu et de nombreux autres équipements virtuels. Vous pouvez créer un laboratoire réseau avec des appareils Cisco, Jupier et bien plus encore.

- **Routeur vmx Le vMX (Virtual MX) :**

Estun routeur UniverselEdge 3D MX séries doté de nombreuses fonctionnalités. Le vMX offre des services de routage avancés qui permettent la prise en charge d'applications de périphérie fournisseur virtuelle (vPE), de réflecteur de route virtuelle (vRR) ou encore d'équipement virtuel côté client (vCE). Il est adapté à la modification flexible de services pour les fournisseurs de services et les opérateurs cloud.

3.4 Application :

Nous présenterons dans cette partie :

La topologie simulée, les configurations réalisées et enfin les résultats des configurations.

3.4.1 Topologie :

Nous avons utilisé dans notre solution 12 routeurs Juniper VMX

Deux Router ASBR, deux clients CE1 et CE2, quatre routeur P et deux routeurs PE. La solution L3 VPN MPLS sera implémentée sur les routeurs PE.

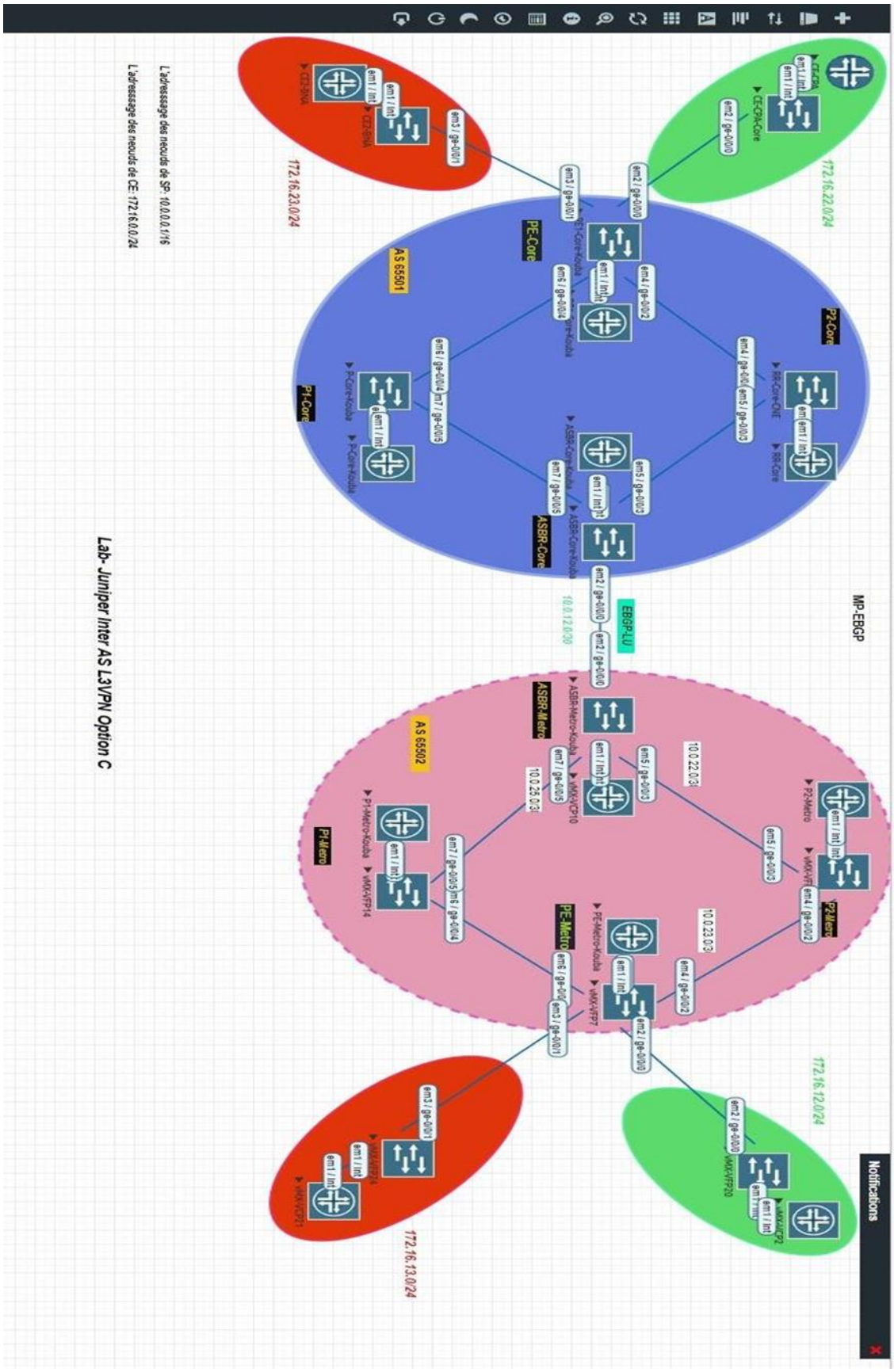

Figure.3.1 : Topologie du LAB.

3.4.2 Table d'adressage :

Pour la réalisation de cette application, nous utiliserons la tabled'adressage du tableau suivant :

Tableau d'adressage de l'AS 65501 (AS- Core) :

Routeur	Interface	Adresse
P1	**Ge.0/0/4** vers **PE.Core**	**10.0.14.2/30**
	Ge.0/0/5 vers **ASBR.Core**	**10.0.15.2/30**
	lo0	**10.10.20.4/32**
P2	**Ge.0/0/2** vers **PE.Core**	**10.0.11.2/30**
	Ge.0/0/3 vers **ASBR.Core**	**10.0.13.2/30**
	lo0	**10.10.20.1/32**
PE	**Ge.0/0/0** vers **CE.CPA**	**172.16.22.1/30**
	Ge.0/0/1 vers **CE.BNA**	**172.16.23.1/30**
	Ge.0/0/2 vers **P1**	**10.0.11.1/30**
	Ge.0/0/4 vers **P2**	**10.0.14.1/30**
	lo0	**10.10.20.2/32**
ASBR	**Ge.0/0/0** vers **ASBR Métro**	**10.2.12.1/30**
	Ge.0/0/3 vers **P2**	**10.0.13.1/30**
	Ge.0/0/5 vers **P1**	**10.0.15.1/30**
	lo0	**10.10.20.3/32**

Tableau d'adressage de l'AS 65502 (AS- Métro) :

Routeur	Interface	Adresse
P1	**Ge.0/0/4** vers **PE.Core**	**10.0.24.2/30**
	Ge.0/0/5 vers **ASBR.Core**	**10.0.25.2/30**
	lo0	**10.10.30.4/32**
P2	**Ge.0/0/2** vers **PE.Core**	**10.0.23.2/30**
	Ge.0/0/3 vers **ASBR.Core**	**10.0.22.2/30**
	lo0	**10.10.30.1/32**
PE	**Ge.0/0/2** vers **P2**	**10.0.23.1/30**
	Ge.0/0/4 vers **P1**	**10.0.24.1/30**
	Ge.0/0/0 vers **CE.CPA**	**172.16.12.1/30**
	Ge.0/0/1 vers **CE.BNA**	**172.16.13.1/30**
	lo0	**10.10.30.2/32**
ASBR	**Ge.0/0/0** vers **ASBR.Core**	**10.0.12.2/30**
	Ge.0/0/3 vers **P2**	**10.0.22.1/30**
	Ge.0/0/5 vers **P1**	**10.0.25.1/30**
	lo0	**10.10.30.3/32**

3.5 Configuration :

Les configurations suivantes sont réalisées sur tous les routeurs P, PE, ASBR.

○ Configuration de l'AS 65501 (AS- Core) :

- **Configuration des interfaces** :

On effectue la configuration suivante sur les interfaces des routeurs P1, P2, PE etASBR du Backbone Core.

```
root@PE1-KOUBA-Core# show interfaces ge-0/0/1.15 |display set
set interfaces ge-0/0/1 unit 15 description to-CE-BNA
set interfaces ge-0/0/1 unit 15 vlan-id 15
set interfaces ge-0/0/1 unit 15 family inet address 172.16.23.1/30
```

Figure 3.2 : Configuration des interfaces du Backbone Core.

On effectue la configuration suivante sur les interfaces des routeurs PE, sortant vers les routeurs clients (CE) :

```
[edit]
root@PE1-KOUBA-Core# show interfaces ge-0/0/0
unit 0 {
    description to-CE-CPA;
    family inet {
        address 172.16.22.1/30;
    }
}
```

Figure 3.3 : Configuration des interfaces PE clients (CE)

```
[edit]
root@CE-CPA-Core# show interfaces ge-0/0/0 |display set
set interfaces ge-0/0/0 unit 0 description to-PE
set interfaces ge-0/0/0 unit 0 family inet address 172.16.22.2/30
```

Figure 3.4: Configuration des interfaces CE vers PE

- **Configuration de l'IGP :**

Sur tous les routeurs (PE) et (P), on configure le protocole OSPF du réseau Backbone Core .

```
root@PE1-KOUBA-Core# show protocols ospf|display set
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-0/0/2.0
set protocols ospf area 0.0.0.0 interface ge-0/0/4.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
```

Figure 3.5 : Configuration du protocole OSPF

- **Configuration du protocole MPLS et LSP :**

Sur tous les routeurs faisant partie du Backbone Core, on configure le protocole MPLS et entre le routeur ASBR et PE on configure le protocole LSP.

```
[edit]
root@PE1-KOUBA-Core# show protocols mpls |display set
set protocols mpls label-switched-path PE1_to_ASBR from 10.10.20.2
set protocols mpls label-switched-path PE1_to_ASBR to 10.10.20.3
set protocols mpls interface ge-0/0/2.0
set protocols mpls interface ge-0/0/4.0
set protocols mpls interface lo0.0
```

Figure 3.6 : Configuration du protocole MPLS et LSP

- **Configuration du protocole RSVP :**

Sur tous les routeurs appartenant au Backbone Core (PE Pet ASBR), on configure leprotocole RSVP.

```
[edit]
root@PE1-KOUBA-Core# show protocols rsvp |display set
set protocols rsvp interface ge-0/0/2.0
set protocols rsvp interface ge-0/0/4.0
set protocols rsvp interface lo0.0
```

Figure 3.7 : Configuration du protocole RSVP

- **Configuration du protocole IBGP-LU :**

Sur les routeurs (PE) et (ASBR), on configure le protocole IBGP-LU sur les routeurs (PE) et(ASBR) du réseau Backbone Core.

```
set protocols bgp group ASBR-Core type internal
set protocols bgp group ASBR-Core family inet labeled-unicast resolve-vpn
set protocols bgp group ASBR-Core family inet-vpn unicast
set protocols bgp group ASBR-Core neighbor 10.10.20.3
```

Figure 3.8 : Configuration du protocole IBGP-LU

○ Configuration de l'AS 65502 (AS- Métro) :

- **Configuration des interfaces :**

On effectue la configuration suivante sur les interfaces des routeurs P1, P2, PE etASBR de Backbone Métro.

```
root@PE1-Metro# show interfaces ge-0/0/2|display set
set interfaces ge-0/0/2 description to-P2
set interfaces ge-0/0/2 unit 0 family inet address 10.0.23.1/30
```

Figure 3.9 : Configuration des interfaces du Backbone Métro

On effectue la configuration suivante sur les interfaces des routeurs CE :

```
[edit]
root@CE2-BNA-Metro# show interfaces ge-0/0/1 |display set
set interfaces ge-0/0/1 unit 0 description to-PE-Metro
set interfaces ge-0/0/1 unit 0 family inet address 172.16.13.2/30
```

Figure 3.10: Configuration des interfaces CE (BNA) Métro

- **Configuration de l'IGP :**

Sur les routeurs (PE) et (P) du réseau Backbone Métropolitaine, on configure le protocole IS-IS.

```
root@PE1-Metro# show protocols isis |display set
set protocols isis reference-bandwidth 1000g
set protocols isis level 1 disable
set protocols isis level 2 wide-metrics-only
set protocols isis interface ge-0/0/2.0
        set protocols isis interface ge-0/0/4.0
set protocols isis interface lo0.0 passive
```

Figure 3.11 : Configuration du protocole l'IS-IS

- **Configuration du protocole MPLS, LSP :**

On configure le protocole MPLS sur les routeurs (PE, P, ASBBR) du Backbone Métro, etentre le routeur ASBR et PE on configure le LSP.

```
[edit]
root@PE1-Metro# show protocols mpls |display set
set protocols mpls label-switched-path PE1_to_ASBR from 10.10.30.2
set protocols mpls label-switched-path PE1_to_ASBR to 10.10.30.3
set protocols mpls interface ge-0/0/2.0
set protocols mpls interface ge-0/0/4.0
set protocols mpls interface lo0.0
```

Figure 3.12 : Configuration du protocole MPLS.

```
[edit]
root@PE1-Metro# show protocols mpls |display set
set protocols mpls label-switched-path PE1_to_ASBR from 10.10.30.2
set protocols mpls label-switched-path PE1_to_ASBR to 10.10.30.3
```

Figure 3.13 : Configuration du protocole LSP.

- **Configuration de protocole RSVP :**

Sur les routeurs appartenant au Backbone Métro (PE Pet ASBR), on configure le protocole RSVP.

```
[edit]
root@PE1-Metro# show protocols rsvp |display set
set protocols rsvp interface ge-0/0/2.0
set protocols rsvp interface ge-0/0/4.0
set protocols rsvp interface lo0.0
```

Figure 3.14 : Configuration du protocole RSVP

- **Configuration du protocole IBGP-LU :**

On configure l'IBGP-LU sur les routeurs (PE) et (ASBR),du réseau Backbone Métro

```
set protocols bgp group ASBR-Metro type internal
set protocols bgp group ASBR-Metro local-address 10.10.30.2
set protocols bgp group ASBR-Metro family inet labeled-unicast resolve-vpn
set protocols bgp group ASBR-Metro family inet-vpn unicast
set protocols bgp group ASBR-Metro neighbor 10.10.30.3
```

Figure 3.15: Configuration du protocole IBGP-LU.

Les configurations suivantes seront réalisées sur les routeurs afin d'implémenter la solution

- **Configuration du protocole EBGP-LU :**

Sur les routeurs (ASBR) du Backbone Core et du Backbone Métro on configure leprotocole EBGP-LU.

```
set protocols bgp group to-ASBR-Metro type external
set protocols bgp group to-ASBR-Metro local-address 10.0.12.1
set protocols bgp group to-ASBR-Metro family inet labeled-unicast
set protocols bgp group to-ASBR-Metro export to-ASBR-Metro
set protocols bgp group to-ASBR-Metro peer-as 65502
set protocols bgp group to-ASBR-Metro neighbor 10.0.12.2
```

Figure 3.16 : Configuration du protocole EBGP-LU dans le routeur ASBR duBackbone Core.

```
set protocols bgp group to-ASBR-Core type external
set protocols bgp group to-ASBR-Core local-address 10.0.12.2
set protocols bgp group to-ASBR-Core family inet labeled-unicast
set protocols bgp group to-ASBR-Core export to-ASBR-Core
set protocols bgp group to-ASBR-Core peer-as 65501
set protocols bgp group to-ASBR-Core neighbor 10.0.12.1
```

Figure 3.17 : Configuration du protocole EBGP-LU dans le routeur ASBR du Backbone Métro

- **Configuration du protocole MP-EBGP :**

Sur le routeur (PE) du Backbone Core et le routeur (PE) du Backbone Métro onconfigure le MP-EBGP.

```
set protocols bgp group AS-optionC type external
set protocols bgp group AS-optionC traceoptions file bgp-optionC
set protocols bgp group AS-optionC traceoptions file size 10k
set protocols bgp group AS-optionC traceoptions flag all
set protocols bgp group AS-optionC multihop ttl 2
set protocols bgp group AS-optionC local-address 10.10.20.2
set protocols bgp group AS-optionC family inet-vpn unicast
set protocols bgp group AS-optionC export VPN-CPA-export
set protocols bgp group AS-optionC export VPN-CPA-import
set protocols bgp group AS-optionC export VPN-BNA-import
set protocols bgp group AS-optionC export VPN-BNA-export
set protocols bgp group AS-optionC peer-as 65502
set protocols bgp group AS-optionC neighbor 10.10.30.2
```

Figure 3.18 : Configuration du protocole MP-EBGP

- **Configuration du VPN L3 (VRF) :**

Sur les routeurs PE des deux Backbones, on configure l'instance VRF avec le même route Target.

```
[edit]
root@PE1-KOUBA-Core# show routing-instances VPN-CPA |display set
set routing-instances VPN-CPA instance-type vrf
set routing-instances VPN-CPA interface ge-0/0/0.0
set routing-instances VPN-CPA interface lo0.1
set routing-instances VPN-CPA route-distinguisher 65501:11684
set routing-instances VPN-CPA vrf-import VPN-CPA-import
set routing-instances VPN-CPA vrf-export VPN-CPA-export
set routing-instances VPN-CPA vrf-table-label
```

Figure 3.19 : Configuration du VRF au niveau du Backbone Core.

```
[edit]
root@PE1-Metro# show routing-instances VPN-CPA |display set
set routing-instances VPN-CPA instance-type vrf
set routing-instances VPN-CPA interface ge-0/0/0.0
set routing-instances VPN-CPA interface lo0.1
set routing-instances VPN-CPA route-distinguisher 65502:11684
set routing-instances VPN-CPA vrf-import VPN-CPA-import
set routing-instances VPN-CPA vrf-export VPN-CPA-export
set routing-instances VPN-CPA vrf-table-label
```

Figure 3.20 : Configuration du VRF au niveau du Backbone Métro.

3.6 Affichage des résultats de configuration :

- **Résultats de configuration des interfaces :**

Cette description permet de constater que les interfaces sont **UP** (activé).

```
[edit]
root@PE1-KOUBA-Core# run show interfaces descriptions
Interface        Admin Link Description
ge-0/0/0.0       up    up   to-CE-CPA
ge-0/0/1.15      up    up   to-CE-BNA
ge-0/0/2         up    up   to-RR
ge-0/0/4         up    up   to-P-Core
lo0.0            up    up   loopback Interface
lo0.1            up    up   Loopback for VPN-CPA
lo0.45           up    up   Loopback for VPN-BNA
```

Figure 3.21 : Le résultat de la configuration des interfaces

- **Le Résultats de la configuration de l'OSPF / IS-IS :**

Les figures suivantes démontre que le protocole ISIS et l'OSPF sont **UP**, ainsiqueles routeurs adjacents dans la base de données.

```
root@PE1-Metro# run show isis adjacency
Interface             System         L State       Hold (secs) SNPA
ge-0/0/4.0            P-Metro        2  Up                   5  50:0:0:e:0:6
```

Figure 3.22 : Le Résultat de configuration du protocole IS-IS

```
[edit]
root@ASBR-Kouba-Core# run show ospf neighbor
Address          Interface              State     ID               Pri  Dead
10.0.13.2        ge-0/0/3.0             Full      2.2.2.2          128    35
10.0.15.2        ge-0/0/5.0             Full      10.10.20.4       128    29
```

Figure 3.23 : Le Résultat de configuration du protocole OSPF

- **Résultats de configuration des protocoles MPLS-LSP :**

La figure 3.23 montre que le protocole MPLS est **UP** sur tous les routeurs, onpeut voir ainsi que le Labels Switche Path est en état **UP** entre les PEs et les ASBRs .

```
root@PE1-KOUBA-Core# run show mpls lsp
Ingress LSP: 1 sessions
To              From            State Rt P     ActivePath       LSPname
10.10.20.3      10.10.20.2      Up     0 *                      PE1_to_ASBR
Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.10.20.2      10.10.20.3      Up       0  1 FF       3        - PE1_to_ASBR
Total 1 displayed, Up 1, Down 0

Transit LSP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

Figure 3.24 : Résultat de configuration de MPLS-LSP

- **Résultats de la configuration de RSVP :**

La figure 3.26 montre que le protocole RSVP est **établi** entre les PEs et les ASBRs.

```
[edit]
root@PE1-KOUBA-Core# run show rsvp session
Ingress RSVP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.10.20.3      10.10.20.2      Up       0  1 FF       -   299776 PE1_to_ASBR
Total 1 displayed, Up 1, Down 0

Egress RSVP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.10.20.2      10.10.20.3      Up       0  1 FF       3        - PE1_to_ASBR
Total 1 displayed, Up 1, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

Figure 3.25 : Le Résultat de configuration de RSVP

- **Résultats de configuration du protocole IBGP-Lu :**

La figure 3.27 montre que le protocole IBGP-Lu est **établi** entre les PEs et les ASBRs.

Chaque PE des deux Backbone reçoit les adresses Loop-Back de l'autre via le protocole IBGP-LU avec le même label.

```
[edit]
root@PE1-Metro# run show route table inet.3

inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.20.2/32      *[BGP/170] 00:00:02, MED 2, localpref 100, from 10.10.30.3
                      AS path: 65501 I, validation-state: unverified
                    > to 10.0.23.2 via ge-0/0/2.0, Push 456032
```

Figure 3.26 : Résultat du protocole IBGP-Lude PE métro.

PE Métro reçoisles adresses Loop-Back de PE Core via le protocole IBGP-LU.

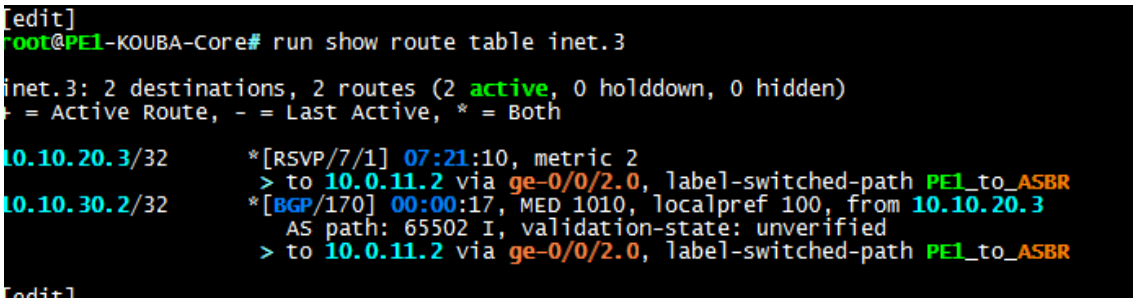

Figure 3.27 : Résultat du protocole IBGP-Lu de PE Core.

PE Core reçois les adresses Loop-Back de PE Metro via IBGP-LU.

- **Résultats de configuration du protocole EBGP –lu :**

La figure 3.29 montre que le protocole EBGP-Lu est **établi** entre les ASBRs

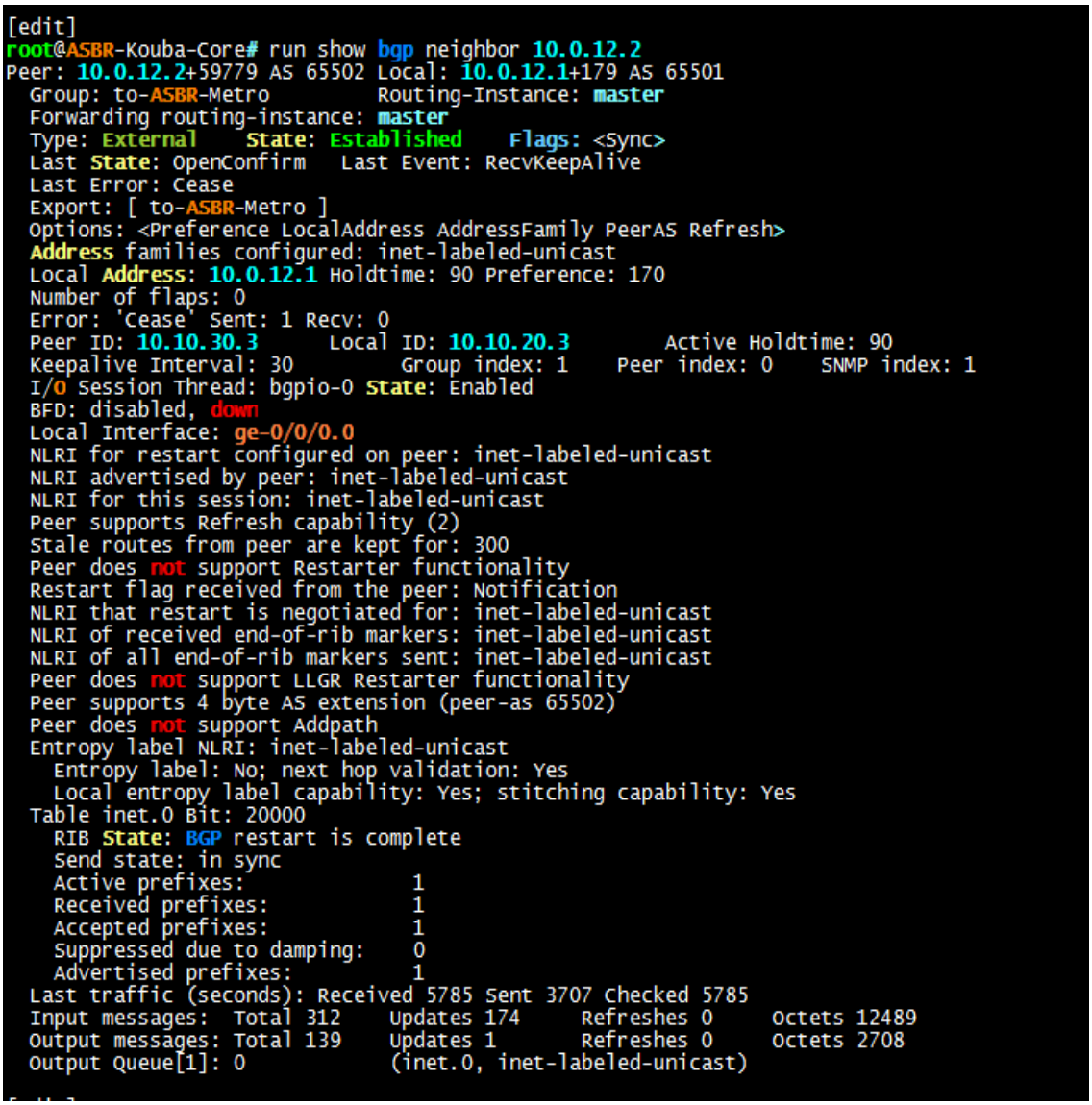

Figure 3.28 : Le Résultat de la configuration d'EBGP-Lu dans ASBR.

On voie que l'EBGP- LU est **UP** entre ASBR CORE ET ASBR Métro.

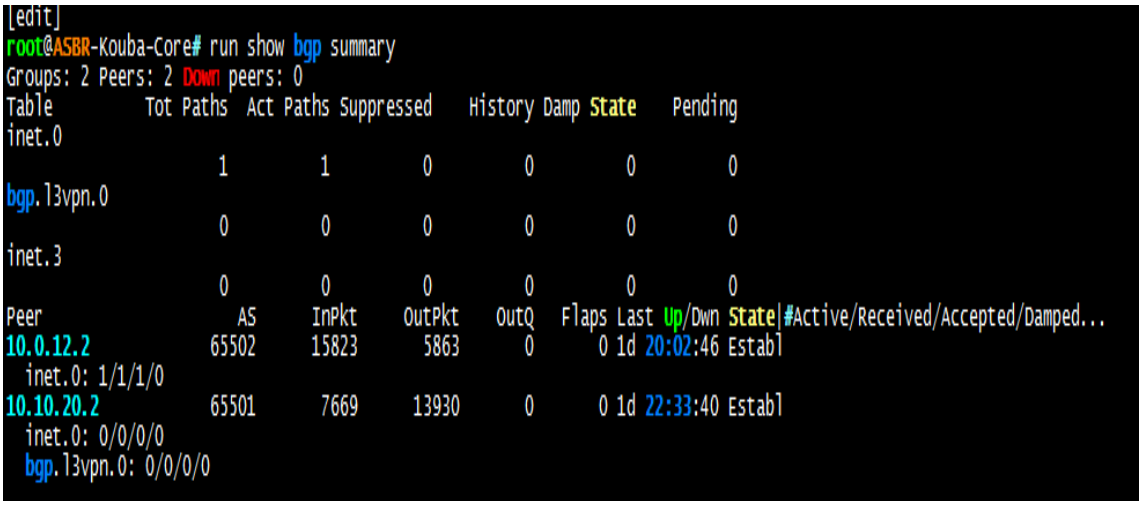

Figure 3.29 : Résultat du protocole EBGP-LU Core.

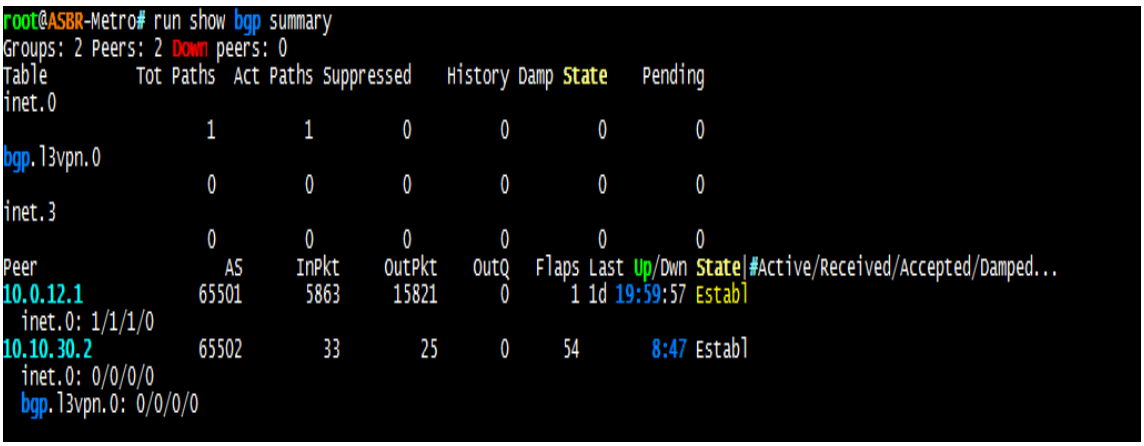

Figure 3.30 : Résultat du protocole EBGP-LU Métro.

Chaque ASBR des deux Backbone reçois les adresses Loop-Back de chaque PEdes deux Backbone via le protocole EBGP-LU.

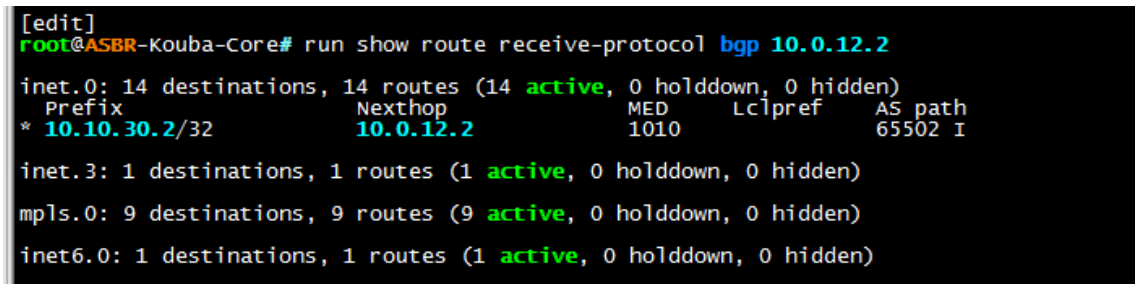

Figure 3.31 : Résultat du protocole EBGP-LU Core

L'ASBR du Backbone Core reçois les adresses Loop- de PE Métro .

```
[edit]
root@ASBR-Metro# run show route receive-protocol bgp 10.0.12.1

inet.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.10.20.2/32           10.0.12.1            2                  65501 I
```

Figure 3.32 : Résultat du protocole EBGP-LU Métro

L'ASBR du Backbone Métro reçois les adresses Loop- Back de PE Core .

- **Résultats de la configuration MP-EBGP :**

La figure 3.34 montre que le protocole MP-EBGP est **UP**

```
root@PE1-KOUBA-Core# run show bgp neighbor 10.10.30.2
Peer: 10.10.30.2+53262 AS 65502 Local: 10.10.20.2+179 AS 65501
  Group: AS-optionC              Routing-Instance: master
  Forwarding routing-instance: master
  Type: External    State: Established    Flags: <Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ VPN-CPA-export VPN-CPA-import VPN-BNA-import VPN-BNA-export ]
  Options: <Multihop Preference LocalAddress Ttl AddressFamily PeerAS Rib-group Refresh>
  Address families configured: inet-vpn-unicast
  Local Address: 10.10.20.2 Holdtime: 90 Preference: 170
  Number of flaps: 0
  Peer ID: 10.10.30.2      Local ID: 10.10.20.2        Active Holdtime: 90
  Keepalive Interval: 30         Group index: 1    Peer index: 0    SNMP index: 1
  I/O Session Thread: bgpio-0 State: Enabled
  BFD: disabled, down
  NLRI for restart configured on peer: inet-vpn-unicast
  NLRI advertised by peer: inet-vpn-unicast
  NLRI for this session: inet-vpn-unicast
  Peer supports Refresh capability (2)
  Stale routes from peer are kept for: 300
  Peer does not support Restarter functionality
  Restart flag received from the peer: Notification
  NLRI that restart is negotiated for: inet-vpn-unicast
  NLRI of all end-of-rib markers sent: inet-vpn-unicast
  Peer does not support LLGR Restarter functionality
  Peer supports 4 byte AS extension (peer-as 65502)
  Peer does not support Addpath
  Table bgp.l3vpn.0 Bit: 30001
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete
    Send state: in sync
    Active prefixes:              5
    Received prefixes:            5
    Accepted prefixes:            5
    Suppressed due to damping:    0
    Advertised prefixes:          5
  Table VPN-BNA.inet.0
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete
    Send state: not advertising
    Active prefixes:              2
    Received prefixes:            2
    Accepted prefixes:            2
    Suppressed due to damping:    0
  Table VPN-CPA.inet.0
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete
    Send state: not advertising
    Active prefixes:              3
    Received prefixes:            3
    Accepted prefixes:            3
    Suppressed due to damping:    0
```

Figure 3.33 : Le Résultat de la configuration MP-EBGP

- **Résultas advirtising métro – reciving core :**

```
[edit]
root@PE1-Metro# run show route advertising-protocol bgp 10.10.20.2

VPN-BNA.inet.0: 5 destinations, 5 routes (3 active, 0 holddown, 2 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 40.40.40.40/32          Self                                    I
* 172.16.13.0/30          Self                                    I

VPN-CPA.inet.0: 7 destinations, 7 routes (4 active, 0 holddown, 3 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 60.60.60.60/32          Self                                    I
* 172.16.12.0/24          Self                                    I
* 192.168.102.1/32        Self                                    I

bgp.l3vpn.0: 12 destinations, 12 routes (7 active, 0 holddown, 5 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  65502:11684:60.60.60.60/32
*                         Self                                    I
  65502:11684:172.16.12.0/24
*                         Self                                    I
  65502:11684:192.168.102.1/32
*                         Self                                    I
  65502:11685:40.40.40.40/32
*                         Self                                    I
  65502:11685:172.16.13.0/30
*                         Self                                    I
```

Figure 3.34 : Résultat advertising route Métro

PE Core a reçu les adresses loop-back de PE métro par le Protocol EBGP-LU

```
[edit]
root@PE1-KOUBA-Core# run show route receive-protocol bgp 10.10.30.2

inet.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

VPN-BNA.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 40.40.40.40/32          10.10.30.2                              65502 I
* 172.16.13.0/30          10.10.30.2                              65502 I

VPN-CPA.inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 60.60.60.60/32          10.10.30.2                              65502 I
* 172.16.12.0/24          10.10.30.2                              65502 I
* 192.168.102.1/32        10.10.30.2                              65502 I

mpls.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)

bgp.l3vpn.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  65502:11684:60.60.60.60/32
*                         10.10.30.2                              65502 I
  65502:11684:172.16.12.0/24
*                         10.10.30.2                              65502 I
  65502:11684:192.168.102.1/32
*                         10.10.30.2                              65502 I
  65502:11685:40.40.40.40/32
*                         10.10.30.2                              65502 I
  65502:11685:172.16.13.0/30
*                         10.10.30.2                              65502 I

inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

VPN-BNA.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

VPN-CPA.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

Figure 3.35 : Résultat receiving route Core.

- **Advertising Core – receiving Métro:**

```
[edit]
root@PE1-KOUBA-Core# run show route advertising-protocol bgp 10.10.30.2

VPN-BNA.inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 30.30.30.30/32          Self                                    I
* 172.16.23.0/30          Self                                    I

VPN-CPA.inet.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 50.50.50.50/32          Self                                    I
* 172.16.22.0/24          Self                                    I
* 192.168.101.1/32        Self                                    I

bgp.l3vpn.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  65501:11684:50.50.50.50/32
*                         Self                                    I
  65501:11684:172.16.22.0/24
*                         Self                                    I
  65501:11684:192.168.101.1/32
*                         Self                                    I
  65501:11685:30.30.30.30/32
*                         Self                                    I
  65501:11685:172.16.23.0/30
*                         Self                                    I
```

Figure 3.36 : Résultat advertising route Core.

```
[edit]
root@PE1-Metro# run show route receive-protocol bgp 10.10.20.2

inet.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)

inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

VPN-BNA.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 30.30.30.30/32          10.10.20.2                              65501 I
* 172.16.23.0/30          10.10.20.2                              65501 I

VPN-CPA.inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 50.50.50.50/32          10.10.20.2                              65501 I
* 172.16.22.0/24          10.10.20.2                              65501 I
* 192.168.101.1/32        10.10.20.2                              65501 I

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

mpls.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)

bgp.l3vpn.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  65501:11684:50.50.50.50/32
*                         10.10.20.2                              65501 I
  65501:11684:172.16.22.0/24
*                         10.10.20.2                              65501 I
  65501:11684:192.168.101.1/32
*                         10.10.20.2                              65501 I
  65501:11685:30.30.30.30/32
*                         10.10.20.2                              65501 I
  65501:11685:172.16.23.0/30
*                         10.10.20.2                              65501 I

inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

VPN-BNA.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

VPN-CPA.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

Figure 3.37 : Résultat receiving route Métro

PE Métro a reçu les adresses Loop-Back de PE Core par le protocole MP-EBGP

- **Résultats de configuration de L3 VPN (VRF) :**

La figure ci-dessous permet de voir les tables de routage VRF des deux routeursPEs.

```
[edit]
root@PE1-Metro# run show route table VPN-CPA.inet

VPN-CPA.inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

50.50.50.50/32     *[BGP/170] 00:00:06, localpref 100, from 10.10.20.2
                      AS path: 65501 I, validation-state: unverified
                    > to 10.0.23.2 via ge-0/0/2.0, Push 17, Push 310560(top)
60.60.60.60/32     *[Static/5] 06:02:47
                    > to 172.16.12.2 via ge-0/0/0.0
172.16.12.0/24     *[Direct/0] 06:02:47
                    > via ge-0/0/0.0
172.16.12.1/32     *[Local/0] 06:02:47
                      Local via ge-0/0/0.0
172.16.22.0/24     *[BGP/170] 00:00:06, localpref 100, from 10.10.20.2
                      AS path: 65501 I, validation-state: unverified
                    > to 10.0.23.2 via ge-0/0/2.0, Push 17, Push 310560(top)
192.168.101.1/32   *[BGP/170] 00:00:06, localpref 100, from 10.10.20.2
                      AS path: 65501 I, validation-state: unverified
                    > to 10.0.23.2 via ge-0/0/2.0, Push 17, Push 310560(top)
192.168.102.1/32   *[Direct/0] 06:11:47
                    > via lo0.1

VPN-CPA.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

ff02::2/128        *[INET6/0] 06:12:00
                      MultiRecv
```

Figure 3.38 : la table de routage de VRF CPA-au niveau de PE Métro la configuration de VRF

On peut voir les adresses de CE-CPA Core via le protocole MP-EBGP.

Objectif entre les PE c'est l'échange des routes des VRF

- **Résultats de PING :**

```
[edit]
root@PE1-KOUBA-Core# run ping 10.10.30.2 source 10.10.20.2
PING 10.10.30.2 (10.10.30.2): 56 data bytes
64 bytes from 10.10.30.2: icmp_seq=2 ttl=60 time=10757.662 ms
64 bytes from 10.10.30.2: icmp_seq=3 ttl=60 time=9755.042 ms
64 bytes from 10.10.30.2: icmp_seq=4 ttl=60 time=8809.833 ms
64 bytes from 10.10.30.2: icmp_seq=5 ttl=60 time=7835.445 ms
64 bytes from 10.10.30.2: icmp_seq=6 ttl=60 time=6854.651 ms
64 bytes from 10.10.30.2: icmp_seq=7 ttl=60 time=5862.108 ms
64 bytes from 10.10.30.2: icmp_seq=8 ttl=60 time=4871.678 ms
64 bytes from 10.10.30.2: icmp_seq=9 ttl=60 time=4183.995 ms
64 bytes from 10.10.30.2: icmp_seq=10 ttl=60 time=3182.622 ms
64 bytes from 10.10.30.2: icmp_seq=11 ttl=60 time=2182.912 ms
64 bytes from 10.10.30.2: icmp_seq=12 ttl=60 time=1183.044 ms
```

Figure 3.39 : Résultat PING PE Core to PE Métro.

```
[edit]
root@PE1-KOUBA-Core# run ping routing-instance VPN-BNA 172.16.23.2
PING 172.16.23.2 (172.16.23.2): 56 data bytes
64 bytes from 172.16.23.2: icmp_seq=5 ttl=64 time=14420.796 ms
64 bytes from 172.16.23.2: icmp_seq=15 ttl=64 time=4426.010 ms
64 bytes from 172.16.23.2: icmp_seq=16 ttl=64 time=3425.872 ms
64 bytes from 172.16.23.2: icmp_seq=17 ttl=64 time=2422.015 ms
64 bytes from 172.16.23.2: icmp_seq=18 ttl=64 time=1420.739 ms
64 bytes from 172.16.23.2: icmp_seq=19 ttl=64 time=412.755 ms
64 bytes from 172.16.23.2: icmp_seq=20 ttl=64 time=4991.303 ms
64 bytes from 172.16.23.2: icmp_seq=21 ttl=64 time=3986.123 ms
64 bytes from 172.16.23.2: icmp_seq=22 ttl=64 time=2986.123 ms
64 bytes from 172.16.23.2: icmp_seq=23 ttl=64 time=1987.608 ms
64 bytes from 172.16.23.2: icmp_seq=24 ttl=64 time=987.254 ms
64 bytes from 172.16.23.2: icmp_seq=25 ttl=64 time=365.435 ms
64 bytes from 172.16.23.2: icmp_seq=9 ttl=64 time=20871.163 ms
64 bytes from 172.16.23.2: icmp_seq=26 ttl=64 time=3854.518 ms
64 bytes from 172.16.23.2: icmp_seq=27 ttl=64 time=2853.788 ms
64 bytes from 172.16.23.2: icmp_seq=28 ttl=64 time=1850.942 ms
64 bytes from 172.16.23.2: icmp_seq=29 ttl=64 time=852.513 ms
64 bytes from 172.16.23.2: icmp_seq=30 ttl=64 time=5580.881 ms
64 bytes from 172.16.23.2: icmp_seq=31 ttl=64 time=5392.749 ms
64 bytes from 172.16.23.2: icmp_seq=32 ttl=64 time=4390.969 ms
64 bytes from 172.16.23.2: icmp_seq=33 ttl=64 time=3385.599 ms
```

Figure 3.40 : Résultat PING PE Core to CE BNA Core.

3.7 Valeur ajoutée de la solution :

La solution présentée sur ce chapitre, le VPN L3 MPLS inter AS option C par une session MP-EBGP Multi-hop consiste de redistribuer des routes VPN tandis que la continuité MPLS de bout en bout est effectuée entre les ASBR par des protocoles d'échange de labels. Cela est fait pour augmenter la fiabilité ou les performances, afin de pouvoir bénéficier totalement de ce privilège le Protocol VPN L3 inter AS option A doit être migré vers l'inter AS option C car ce dernier présente des limitations qui freinentla mise en place de cette solution, pour cela, l'inter AS option C, est la solution idéale pource travail.

VPN L3 MPLS option C, permettra à Algérie Télécom de résoudre les problèmes de convergence, l'évolutivité, la qualité de service QOS et de temps de rétablissement en cas de panne posés par la solution utilisée actuellement qui est le VPN L3 MPLS inter AS option A.

3.8 Conclusion

La simulation, réalisée avec le simulateur de la solution VPN L3/MPLS option C adonné un résultat positif et satisfaisant. Les différents tests ont donné entière satisfactionet les résultats ont été jugés par l'opérateur concluant. De ce fait, nous pouvons conclureque nous avons atteint notre objectif**.**

Conclusion Générale

Actuellement, les opérateurs de télécommunication tels qu'ALGERIE TELECOM mettent beaucoup d'investissements sur les réseaux de télécommunication modernes, vu leurs utilités, leurs facilités d'utilisation et l'intégration de nouvelles gammes de serviceset leur exploitation à faible coût.

Au cours de notre projet, nous avons commencé par présenté la technologie MPLS son fonctionnement et les et protocoles utilisés, Après nous avons opté pour la solution VPN L3 /MPLS option C en détaillons ses concepts, son fonctionnement ses avantages, Ensuite nous avons simulées la solution VPN L3 /MPLS option C en utilisant le simulateur EVE.

Au terme de ce projet, nous avons abouti à la mise en œuvre d'une solution de inter AS option C qui consiste à connecter deux autonome système (AS) différent par une session MP-EBGP Multi-Hop qui est chargée de redistribuer des routes VPN tandis que la continuité MPLS de bout en bout est effectuée entre les ASBR par des protocoles d'échange de labels. Cela peut être fait pour augmenter la fiabilité, la convergence ou les performances, afin de pouvoir bénéficier totalement de ce privilège le Protocol VPN L3-MPLS inter AS option A doit être migré car ce dernier présente des limitations qui freinent la mise en place de cette solution, pour cela, Le VPN L3 –MPLS inter AS option C'est la solution idéale pour ce travail.

L3 VPN MPLS inter AS option C permettra à Algérie Télécom de remédier aux contraintes du l'inter AS l'option A, La Sécurité, La Qualité De Service, La Convergence, La Disponibilité Ou Bien Le Passage A L'échelle t ainsi de répondre aux attentes des clients.

Arrivées au terme de ce projet, il nous a été possible de pouvoir répondre à certaines des contraintes et limitations relevées par AT en proposant une solution dont les résultats sont jugés satisfaisants et encourageants. Néanmoins, comme tout travail, celui-ci mérite d'être enrichi et poursuivi. C'est dans ce contexte précis que nous proposons à titre de perspective le **RSV6** qui remplace la technologie MPLS et ajoute des nouveaux avantagesdans le déploiement des infrastructures réseaux.

Bibliographie

[10] Wikipedia [2022.05.16].is-is .récupérésur https://fr.wikipedia.org/wiki/isis. 10/05/2022

[11] VMWARE. (2016, 07 19). Configurer le protocole IS-IS. Récupéré sur https://docs.vmware.com/fr/VMware-NSX-Data-Center-forvSphere/6.2/com.vmware.nsx.admin.doc/GUID-E62990A1-7AE5-4BA1-A861-278840FDA0FC.html 10/05/2022

[12] networklessons. (s.d.). Multi Protocol BGP (MP-BGP) Configuration. Récupéré sur https://networklessons.com/bgp/multiprotocol-bgp-mp-bgp-configuration 10/05/2022

[13] routeralley. (2022, 05 10). BGP. Récupéré sur http://www.routeralley.com/guides/bgp.pdf visioné 10/05/2022

[1] [2022.05.16]. PYXYA. (s.d.). Réseau MPLS : comment fonctionne cette solution ? . Récupéré surhttps://www.pyxya.fr/en-savoir-plus/reseau-mpls-comment-fonctionne-cette-solution/

[2] http://www-igm.univ-mlv.fr/~dr/XPOSE2006/marot/architecture.html 10/05/2022

[3] PYXYA. (s.d.). Réseau MPLS : comment fonctionne cette solution ? . Récupéré sur https://www.pyxya.fr/en-savoir-plus/reseau-mpls-comment-fonctionne-cette-solution/ 10/05/2022

[4] https://stringfixer.com/fr/IP/MPLS

[2022.05.16].

[8] bonnin,j.- M.(2003,11 10). LDP et CR- LDP. Récupéré sur https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/reseau-internet-protocoles-multicast-routage-mpls-et-mobilite-42289210/ldp-et-cr-ldp-te7540/ldp-label- distribution-protocol-te7540niv10001.html
[2022.05.16].

[9] https://www.futura-sciences.com/tech/definitions/connection-vpn-1819/ [2022.05.16].

[5] https://networkcorp.fr/protocole-de-routage-ospf/#Types_d8217areas [2022.05.18].

[6] https://networkcorp.fr/protocole-de-routage-ospf/#Types_de_routeurs [2022.05.18].

[7]https://networkcorp.fr/protocole-de -routage-ospf/#Types_de_paquets_LSA[2022.05.18].

[14] https://www.cisco.com/c/fr_ca/support/docs/ip/integrated-intermediate-system-to- intermediate-system-is-is/200293-IS-IS-Adjacency-and-Area-Types.html#anc6 [2022.05.20].

[15] https://orhanergun.net/bgp-lu-labeled-unicast-rfc-3107/ [2022.05.30].

[55] https://www.juniper.net/documentation/us/en/software/junos/vpn- l2/topics/concept/vpn-types.html#id-types-of-vpns id-10058355 [2022.06.06].

[56] https://fr.wikipedia.org/wiki/Multiprotocol_Label_Switching [2022.06.06].

[57] https://www.juniper.net/documentation/fr/fr/software/junos/vpn- l3/topics/topic-map/l3-vpns-interprovider.html

[2022.06.06].

[68] https://www.juniper.net/documentation/en_US/junose15.1/topics/concept/mbgp- inter-as-option-b-overview.html

[2022.05.19].

[55] https://www.juniper.net/documentation/fr/fr/software/junos/vpn-l3/topics/topic- map/l3-vpns-interprovider.html

[2022.05.18].

[56] https://www.juniper.net/documentation/us/en/software/junos/vpn- l2/topics/concept/vpn-types.html#id-types-of-vpns id-10022623

[2022.05.18].

[16] https://definir-tech.com/protocole-de-reservation-de-ressources-rsvp/ [2022.06.03].

[17] https://wapiti.telecom-lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2002ttnfa03/Bordessoule s-Bret/Site/MPLS.htm[2022.06.03].

[18] https://www.pyxya.fr/en-savoir-plus/reseau-mpls-comment-fonctionne-cette-solution/ [2022.06.02].

[19] https://cisco.goffinet.org/ccna/ospf/introduction-au-protocole-routage-dynamique- ospf/ [2022.06.02].

[20] https://packetlife.net/blog/2013/jun/10/route-distinguishers-and-route-targets/ [2022.06.04].

[77] https://www.techtarget.com/searchnetworking/definition/virtual-routing-and-forwarding-VRF

[2022.06.1].

[66] https://www.lemagit.fr/definition/Routage-et-transfert-virtuels-virtual-routing-and-forwarding-VRF

[2022.06.1].

[61] https://www.juniper.net/documentation/fr/fr/software/junos/evpn-vxlan/topics/concept/vxlan-evpn-integration-overview.html

[2022.06.1].

[65] https://www.juniper.net/documentation/fr/fr/software/junos/vpn-l3/topics/topic-map/l3-vpns-interprovider.html

[2022.06.1].

[68] https://learningnetwork.cisco.com/s/question/0D

[2022.05.11].

[69] 53i00000Ksqy9CAB/interas-option-c

[2022.05.11].

[70] https://www.juniper.net/documentation/en_US/junose15.1/topics/concept/mbgp- inter-as-option-c-overview.html

[2022.05.18].

[71] [2022.05.17]. https://learningnetwork.cisco.com/s/question/0D53i00000KsrNrCAJ/interas-option-a