REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN – TIARET

MEMOIRE

Présenté à :

FACULTÉ DES MATHEMATIQUES ET DE L'INFORMATIQUE

DÉPARTEMENT DE L'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : **Réseaux et Télécommunication**

Par :

AIT AMAR MEZIANE Arezki Amir

BENTHABET Mohamed

Sur le thème

Etude de la gestion du plan de contrôle pour le GMPLS (Generalized Multi-Protocol Label Switching).

Soutenu publiquement le 21/06/2023 à Tiaret devant le jury composé de :

Mr KOUADRIA Abderrahmane	MCB	Université Ibn Khaldoun Tiaret	Président
Mr KHERICI Cheikh	MCB	Université Ibn Khaldoun Tiaret	Encadreur
Mr NASSANE Samir	MAA	Université Ibn Khaldoun Tiaret	Examinateur

2022-2023

Remerciements

À l’issue de cette étude, nous souhaitons exprimer notre profonde gratitude envers toutes les personnes qui nous ont aidés à mener à bien ce travail dans des conditions optimales. En particulier, nous tenons à adresser nos sincères remerciements à :

Monsieur le Dr. **KHERICI Cheikh**, notre encadreur, pour son soutien, ses encouragements et sa bienveillance tout au long de cette étude. Grâce à ses conseils précieux, nous avons pu mener nos travaux à terme dans des conditions relativement favorables.

Nos enseignants, dont le dévouement et les efforts ont été inestimables tout au long de notre parcours universitaire.

L’ensemble du personnel du département informatique, pour leur précieuse assistance et leur disponibilité lors de nos recherches.

Nos camarades de promotion, avec qui nous avons partagé des moments joyeux et parfois plus difficiles tout au long de ces cinq années passées à l'université de Tiaret.

Enfin, nous tenons à exprimer notre profonde gratitude et reconnaissance envers nos chers parents, nos frères, nos sœurs et tous les membres de nos familles honorables, qui nous ont soutenus et encouragés tout au long de notre parcours scolaire. Leur soutien indéfectible a été une source d’inspiration et de motivation tout au long de cette étude. Nous leur en sommes infiniment reconnaissants.

Dédicaces

Je dédie ce travail

A l'être le plus cher de ma vie, ma mère.

A celui qui m'a fait de moi un homme, mon père.

Qu'ils trouvent ici le témoignage de ma profonde reconnaissance.

A vous mes deux grands-pères, que dieu vous guérisses, ceci est ma profonde gratitude pour votre éternels amours, que ce rapport soit le meilleur cadeau que je puisse vous offrir.

A mes chères sœurs, chères tantes et oncles et toute ma famille, elle qui m'a doté d'une éducation digne, son amour a fait de moi ce que je suis aujourd'hui.

A tous mes amis et tous ceux qui m'aiment.

Amir

Dédicaces

Je tiens à dédier ce projet de fin d'études à la mémoire de mon défunt père, qui a toujours été ma source d'inspiration et de soutien. À ma famille, qui a été mon pilier tout au long de ce parcours académique. À mon fils Abderezak, qui est ma plus grande motivation et mon plus grand bonheur.

Je souhaite également adresser mes remerciements à tous mes amis, qui ont été présents dans les moments de joie et de difficulté, sans citer de nom en particulier, car chacun a contribué à sa manière à ma réussite.

Enfin, un sincère merci à tous mes professeurs, du primaire à l'université, qui ont partagé leurs connaissances, leur expertise et leur passion pour l'apprentissage. Leurs enseignements ont façonné mon parcours et m'ont permis d'atteindre ce stade de ma vie académique.

Cette dédicace est un témoignage de ma gratitude envers tous ceux qui ont contribué à ma formation et à ma croissance personnelle.

Mohamed

Abréviations

AS : Autonomous System.

ATM : Asynchronous Transfer Mode

BGP : Border Gateway Protocol

CE : Customer edge

DMZ : Demilitarized zone

DOCSIS : Data Over Cable Service Interface Specification.

DSL : Digital Subscriber Line.

DSLAM : Digital Subscriber Access Multiplexer.

DWDM : Dense Wavelength Division Multiplexing.

eBGP : external Border Gateway Protocol.

EoMPLS : Ethernet over MPLS.

FEC : Forwarding Equivalence Class.

FSC : Fiber Switching Capable.

GMPLS : Generalized Multi-Protocol Label Switching.

HDLC : High-level Data Link Control.

iBGP : interior Border Gateway Protocol.

IETF : Internet Engineering Task Force.

IGP : Interior Gateway Protocol

ISDN : Integrated Services Digital Network

IS-IS : Intermediate System to Intermediate System)

IS-IS-TE : Intermediate System to Intermediate System-Traffic Engineering)

L2S : Level 2 Switching.

L2SC : Level 2 Switching Capable.

LAN : Local Area Network.

LAP : Link Access Protocol.

LAP-D : Link Access Procedure for the D-channel.

LDP : Label Distribution Protocol.

LER : Label Edge Router.

LMP : Link Management Protocol.

LSC : Lambda Switching Capable.

LSP : Label Switched Path.

LSR : Label Switching Router.

MAN : Metropolitan Area Network.

MPLS : Multi-Protocol Label Switching.

OIF : Optical Internetworking Forum.

OSPF : Open Shortest Path First

OSPF-TE : Open Shortest Path First – Traffic Engineering.

OVPN : Optical Virtual Private Network.

PAN : Personal Area Network.

P : Provider

PE : Provider edge

POP : Point Of Presence.

PPP : Point-to-Point Protocol

PSC : Packet Switching Capable.

RNIS : Réseau Numérique à Intégration de Services

RSVP-TE : Resource ReSerVation Protocol – Traffic Engineering.

SDLC : Synchronous Data Link Control.

TDMC : Time Division Multiplexing Capable.

TDP : Tag Distribution Protocol.

VPN : Virtual Private Network.

VRF : Virtual Routing and Forwarding.

WAN : Wide Area Network.

Table des matières

Liste des figures

Liste des tableaux

Introduction Générale

Aujourd'hui, les réseaux étendus jouent un rôle crucial dans le domaine des communications, permettant la connectivité et l'échange de données à grande échelle. Avec l'évolution constante des besoins en matière de transmission de données, il devient essentiel de développer des protocoles et des mécanismes de gestion efficaces pour garantir des performances optimales et une utilisation efficace des ressources réseau. C'est dans ce contexte que le GMPLS (*Generalized Multi-Protocol Label Switching*) se distingue en tant que protocole de commutation polyvalent et puissant, offrant des fonctionnalités avancées pour la gestion des réseaux étendus.

Le présent mémoire, se concentre sur l'analyse de la gestion du plan de contrôle dans le contexte du GMPLS pour les réseaux étendus, en mettant l'accent sur le GMPLS et ses implications détaillées pour une gestion efficace du réseau en tenant compte la gestion de l'état des liens grâce aux protocoles de routage tels que l'OSPF (*Open Shortest Path First*) et IS-IS (Intermediate System to Intermediate System), contrôle et gestion des routes à l'aide du protocole RSVP (*Resource ReSerVation Protocol*) ainsi que la protection des liens. Ce plan est appliqué sur trois villes algériennes à savoir, Alger, Oran et Constantine dont une comparaison détaillée entre deux architectures proposées sera étudiée tout en gardant une meilleure qualité de service QoS.

Ce mémoire est structuré comme suit :

- Dans le premier chapitre nous allons présenter les différents types de réseaux informatiques. En basant particulièrement sur les réseaux étendus (WAN), ces différentes topologies ainsi que les équipements utilisés dans ce contexte. Aussi, nous allons citer les différents protocoles exploités dans ces réseaux.
- Le deuxième chapitre, se concentre sur le MPLS et le GMPLS. Nous avons examiné les principes de base du MPLS, ses avantages en termes de flexibilité et d'évolutivité, ainsi que son rôle dans l'amélioration des performances et de l'efficacité des réseaux. Ensuite, nous avons plongé dans le GMPLS, une extension du MPLS qui permet la gestion de divers types de ressources de réseau. Nous avons étudié les fonctionnalités étendues offertes par le GMPLS, ainsi que ses applications et ses avantages pour la gestion des réseaux étendus.
- Le troisième chapitre, présente en détail le plan de contrôle GMPLS, en analysant les différents protocoles et mécanismes utilisés pour sa gestion efficace. Nous examinerons les composants clés du plan de contrôle, tels que la signalisation, le routage et la gestion des liens, en soulignant les défis et les solutions associés.

- Dans le quatrième et dernier chapitre nous présenterons la conception et l'implémentation de la simulation, ainsi que l'outil qui nous a servi pour la réalisation de notre simulation, et enfin nous discuterons les différents scenarios de trafic testés et de topologie de réseau afin d'optimiser les performances. Dans ce contexte, nous allons appliquer ce plan de contrôle sur trois villes algériennes à savoir, Alger, Oran et Constantine.

Chapitre I :
Notions sur les réseaux étendus WAN

1 Introduction

Les réseaux sont omniprésents dans notre vie quotidienne. Les ordinateurs, les télévisions, les téléphones portables, les tablettes et les objets connectés sont tous des dispositifs qui dépendent des réseaux pour fonctionner. Les réseaux sont des ensembles de dispositifs connectés entre eux pour permettre la communication et l'échange de données, permettent de connecter des personnes, des organisations et des dispositifs situés à des endroits différents. Au cours des dernières décennies, les réseaux étendus WAN (*Wide Area Network*) ont connu une évolution rapide et une adoption accrue grâce aux technologies avancées et à la demande croissante pour des communications interconnectées.

Dans ce chapitre, nous allons explorer les différents types de réseaux informatiques, les différentes topologies ainsi que les équipements utilisés dans ce contexte en focalisant particulièrement sur les réseaux étendus (WAN). Aussi, nous allons citer les différents protocoles exploités dans ces réseaux.

2 Réseaux informatiques

Un réseau est constitué d'un ensemble d'objets interconnectés et reliés les uns aux autres, organisés de manière à pouvoir communiquer. Lorsqu'il s'agit d'ordinateurs, on parle de réseau informatique. Les réseaux informatiques ont émergé de la nécessité de connecter des terminaux distants à un site central, puis de relier des ordinateurs entre eux, et enfin de connecter des machines terminales telles que des stations de travail ou des serveurs. Les réseaux informatiques, qui ont initialement permis de connecter des terminaux passifs à de grands ordinateurs centraux, permettent désormais l'interconnexion de toutes sortes d'ordinateurs, qu'il s'agit de grands serveurs, de stations de travail, d'ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie intégrante de la vie quotidienne des entreprises et des administrations (banques, gestion, commerce, bases de données, recherche, etc.) ainsi que des particuliers (messagerie, loisirs, services d'informations, Internet, etc.) **[web1].**

Il est important de souligner ici l'adage informatique selon lequel "*le réseau, c'est l'ordinateur*", ce qui signifie que sans réseau, l'ordinateur est sous-exploité. C'est pourquoi les individus ont rapidement compris l'intérêt de connecter ces ordinateurs entre eux afin de réaliser et faciliter la communication.

Voici, quelques intérêts de la réseautique :

- La mise en place d'un réseau informatique permet de faciliter et de sécuriser le stockage de l'information.
- Un réseau permet de partager des fichiers, des applications et des ressources.

- Facilite les opérations de gestion et de maintenance des applications et des équipements informatiques.
- Assure la communication entre personnes (grâce au courrier électronique, messagerie, appel vidéo…), la communication entre processus (entre des machines industrielles).
- La mise en réseau permet de réduire considérablement les coûts d'infrastructure. Grâce au réseau, les ressources matérielles et logicielles sont partagées entre plusieurs utilisateurs.
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).

3 Différents types de réseaux informatiques

Les réseaux informatiques sont des ensembles de dispositifs connectés entre eux pour permettre la communication et l'échange de données. Il existe plusieurs types de réseaux, chacun ayant ses propres caractéristiques et utilisations spécifiques (Figure 1).

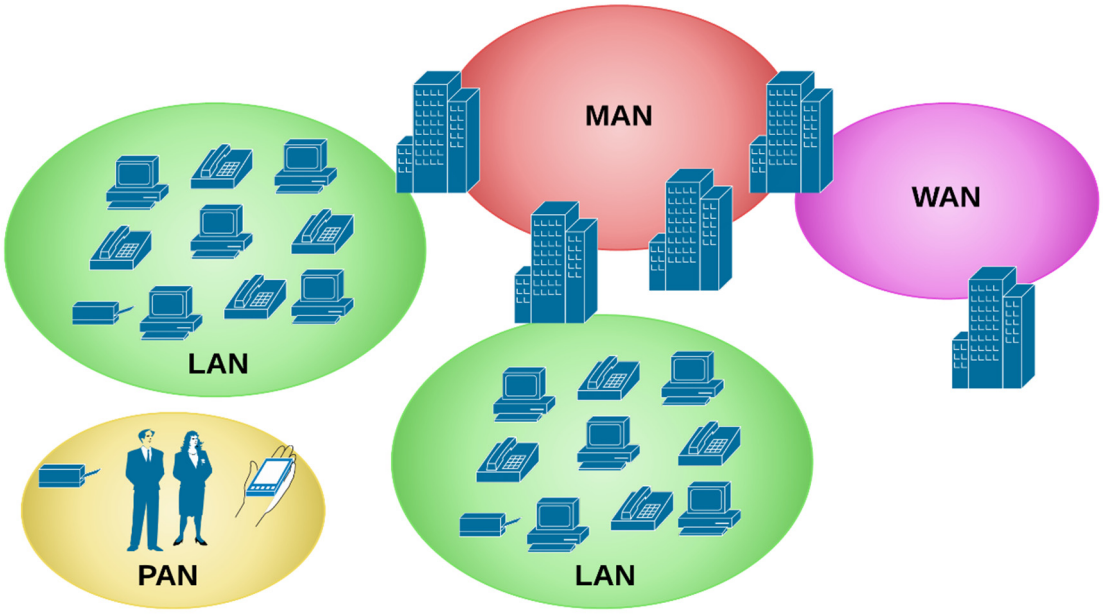

Figure 1 : Différents types des réseaux **[web2].**

- Un réseau personnel PAN (*Personal Area Network*) est un réseau organisé autour d'une personne et utilisé à des fins personnelles. Il couvre généralement une distance de quelques centimètres à environ 10 mètres. Les PAN sont utilisés pour connecter des appareils personnels tels que des ordinateurs, des imprimantes, des smartphones ou des tablettes.
- Un réseau local LAN (*Local Area Network*) est utilisé pour interconnecter des équipements informatiques situés dans une zone géographique restreinte, comme une entreprise ou un bâtiment. Les LAN utilisent des technologies de communication à haute vitesse telles que

l'Ethernet, le Wi-Fi ou la fibre optique. Ils permettent le partage de ressources informatiques et facilitent la communication entre les employés d'une entreprise.

- Un réseau métropolitain MAN (*Metropolitan Area Network*) couvre une zone géographique plus vaste qu'un LAN, généralement une ville ou une région métropolitaine. Les réseaux métropolitains fournissent des connexions haut débit pour relier différents réseaux locaux situés dans la ville ou la région. Ils sont utilisés pour permettre la communication entre les réseaux locaux d'une entreprise et utilisent des technologies telles que le WiMAX, la fibre optique et les liaisons sans fil.
- Un réseau étendu WAN (*Wide Area Network*) couvre une zone géographique étendue, souvent à l'échelle nationale ou internationale. Les réseaux WAN permettent de connecter des réseaux locaux situés dans différentes parties du monde, des filiales d'entreprise, des centres de données distants et des utilisateurs à distance. Les technologies utilisées dans les réseaux étendus comprennent les réseaux de téléphonie fixe et mobile, la fibre optique, les liaisons par satellite et les réseaux sans fil.

La figure 2, montre l'architecture d'un réseau WAN **[1]** :

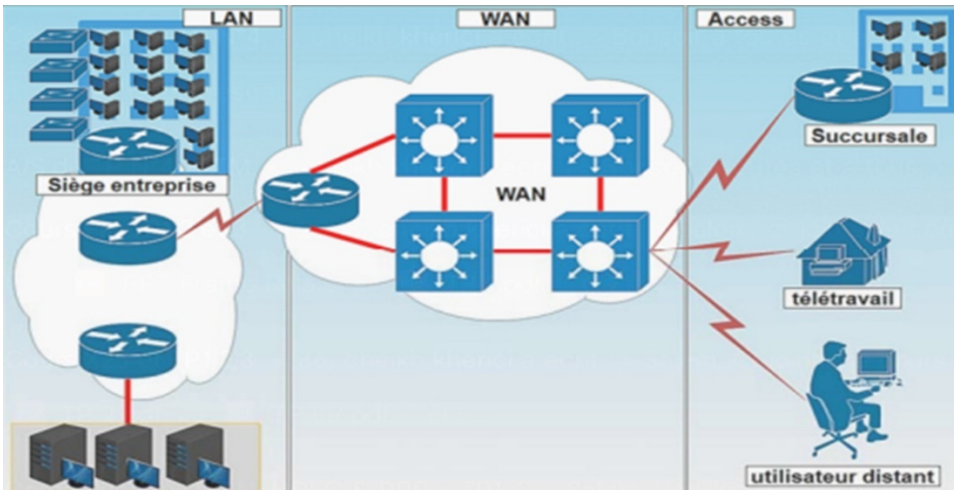

Figure 2 : Architecture réseaux WAN

Un VPN est un réseau de communication virtuel qui utilise l'infrastructure d'un réseau physique pour relier les systèmes informatiques. Il utilise principalement Internet comme moyen de transmission et permet de connecter les réseaux locaux sur Internet ou d'accéder à distance à un réseau ou à un ordinateur spécifique via une connexion publique. Les données sont sécurisées grâce au cryptage pour assurer la confidentialité des informations **[web3]**.

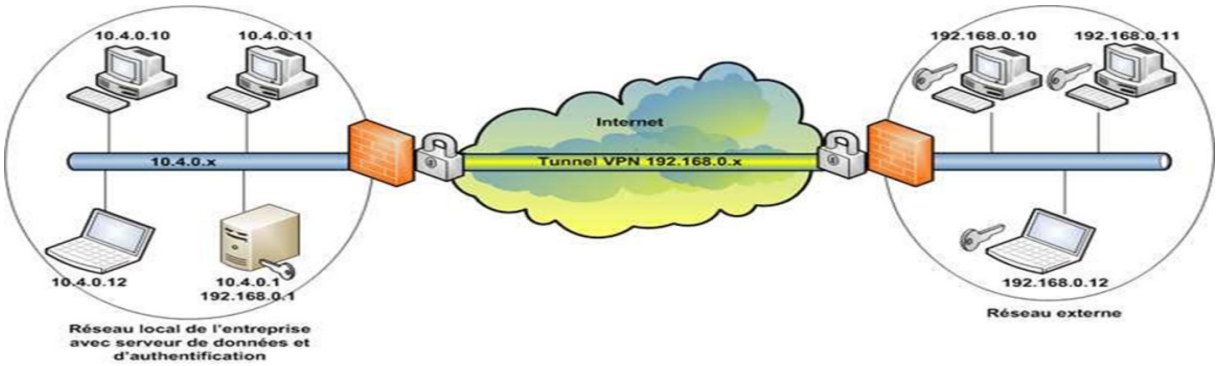

Figure 3 : Réseau privé virtuel

4 Réseaux étendus

4.1 Histoire du réseau étendu

Le réseau étendu (WAN : Wide Area Network) est un réseau de communication dont la portée s'étend à plusieurs sites géographiques. Ces réseaux peuvent être privés pour associer les différents appareils d'une entreprise ou ils peuvent être progressivement publics pour interfacer des réseaux plus petits. Internet n'est rien d'autre que le plus grand réseau étendu du monde **[2]**.

Le réseau étendu est apparu pour la première fois dans les années 1960, lorsque les grandes entreprises ont commencé à avoir besoin de communiquer entre différents sites géographiques. À l'époque, les communications se faisaient principalement par l'intermédiaire de lignes téléphoniques dédiées ou de liaisons louées, qui étaient coûteuses et souvent peu fiables.

Dans les années 1980, les réseaux étendus (WAN) sont devenus de plus en plus importants pour les entreprises et les organisations. Les nouvelles technologies telles que la transmission de données par fibre optique, l'émergence des réseaux de communication par satellite et les progrès dans la compression des données ont permis aux entreprises de se connecter à des réseaux à travers le monde entier. Le développement de l'Internet a également contribué à l'expansion des réseaux étendus, en permettant aux entreprises d'accéder à des réseaux publics et privés pour la transmission de données. Dans les années 1990, les entreprises avaient principalement recours à des réseaux privés pour connecter leurs différents sites et leurs bureaux, mais l'utilisation de réseaux publics a augmentée avec l'arrivée de l'Internet. L'expansion des réseaux étendus a également entraînée une augmentation de la demande des services de connectivité gérés. Les fournisseurs de services de télécommunications ont commencé à proposer des services de réseaux privés virtuels (VPN) pour permettre aux entreprises de connecter leurs différents sites via Internet de manière sécurisée **[web4]**.

Arrivant au années 2000, l'arrivée de la 2G et de la 3G a également permis le développement des réseaux étendus mobiles, offrant une connectivité sans fil à haute vitesse à travers le monde.

Les réseaux étendus ont également continué à se développer pour répondre aux besoins croissants de connectivité à l'échelle mondiale. Les entreprises ont commencé à étendre leurs réseaux à l'international pour répondre aux besoins de leurs filiales et de leurs employés travaillant à distance.

4.2 Pourquoi les réseaux étendus ?

Les réseaux étendus permettent de connecter le réseau central d'une entreprise à ses branches distantes. Cela offre à l'entreprise l'avantage de fournir une connectivité sécurisée entre le réseau central de l'entreprise et Internet en utilisant des services tels que les Zones démilitarisées DMZ (*Demilitarized zone*), les connexions VPN et d'autres services connexes. Il existe de nombreuses options de transport WAN et Internet disponibles, et de nouvelles émergent constamment. Cependant, lors du choix des technologies de transport WAN, il est important de prendre en compte des facteurs tels que le coût, la bande passante, la fiabilité et la facilité de gestion, ainsi que les capacités matérielles et logicielles de l'équipement **[3]**.

Il y a trois objectifs clés pour une conception efficace d'un réseau WAN **[3]** :

- Le WAN doit prendre en charge les objectifs et les politiques de l'organisation.
- Les technologies WAN sélectionnées doivent répondre aux exigences actuelles des applications et prévoir croissance de l'organisation dans le futur.
- La conception proposée doit intégrer la sécurité partout et garantir une haute disponibilité applicable tout en respectant le budget défini.

4.3 Equipements et dispositifs des réseaux WAN

Les équipements et dispositifs des réseaux WAN sont utilisés pour connecter des réseaux locaux situés dans des zones géographiques distinctes, à travers de grandes distances.

Voici une description des principaux équipements et dispositifs utilisés dans les réseaux WAN:

4.3.1 Modems : Les modems sont utilisés pour convertir les signaux numériques en signaux analogiques pour la transmission sur les lignes téléphoniques. Ils peuvent également être utilisés pour convertir les signaux analogiques en signaux numériques à la réception.

Figure 4 : Modem

4.3.2 Routeurs : Les routeurs sont des dispositifs qui permettent de faire transiter les paquets de données entre différents réseaux. Ils utilisent des protocoles de routage pour déterminer le meilleur chemin pour acheminer les paquets de données.

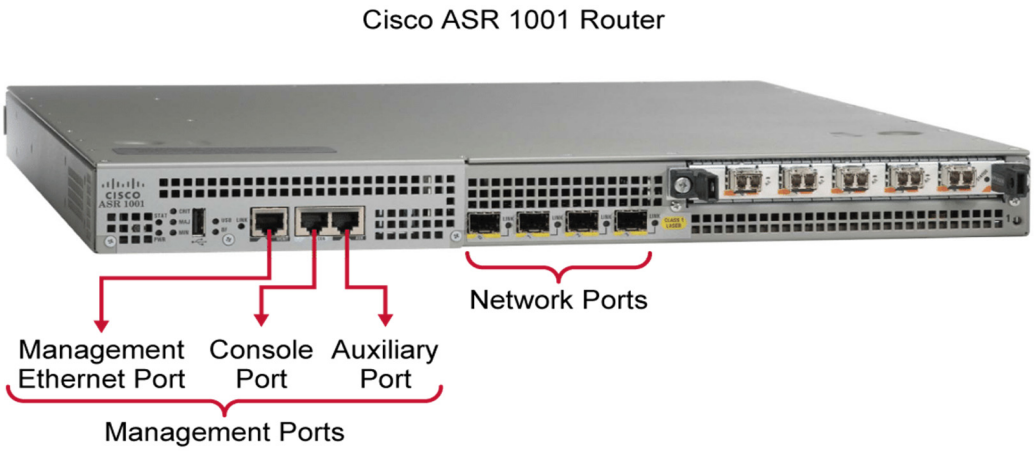

Figure 5 : Routeur

4.3.3 Commutateurs WAN : Les commutateurs WAN sont des dispositifs qui permettent de connecter plusieurs liens WAN ensemble pour former un réseau étendu plus grand. Ils sont des unités multiports qui assurent les commutations du trafic WAN. Sont utilisés pour augmenter la bande passante et améliorer la fiabilité du réseau.

Figure 6 : Commutateur WAN

4.3.4 Accélérateurs WAN : Les accélérateurs WAN sont des dispositifs qui permettent d'améliorer les performances du réseau en compressant les données et en optimisant la transmission des paquets de données.

Figure 7 : Accélérateur WAN

4.3.5 Concentrateurs : Les concentrateurs sont des dispositifs qui permettent de connecter plusieurs périphériques sur un réseau WAN. Ils agissent comme des points de connexion centralisés pour les périphériques.

Figure 8 : Concentrateur

4.3.6 Pare-feu : Le pare-feu est un dispositif de sécurité qui permet de contrôler l'accès au réseau WAN en bloquant les connexions non autorisées et en surveillant le trafic réseau.

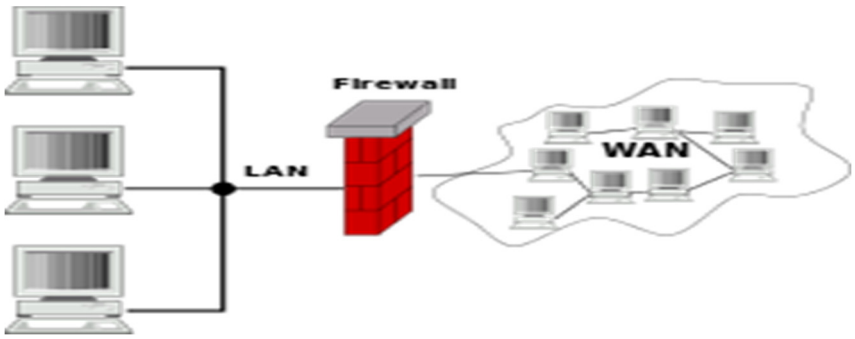

Figure 9 : Illustration d'un pare-feu

4.3.7 Passerelles : Les passerelles sont des dispositifs qui permettent de connecter des réseaux différents en traduisant les protocoles de communication utilisés par ces réseaux. Par exemple, une passerelle peut être utilisée pour connecter un réseau LAN à un réseau WAN.

Figure 10 : Passerelle

4.4 Types de circuits

4.4.1 Circuit point-à-point

Est un circuit physique dédié aux extrémités (exemple : Circuit RNIS en anglais ISDN (Integrated Services Digital Network)).

➢ Caractéristiques :

- Coûte cher.
- Meilleure qualité de service (2Mb/s) p/r aux anciens Modems 56kb/s.

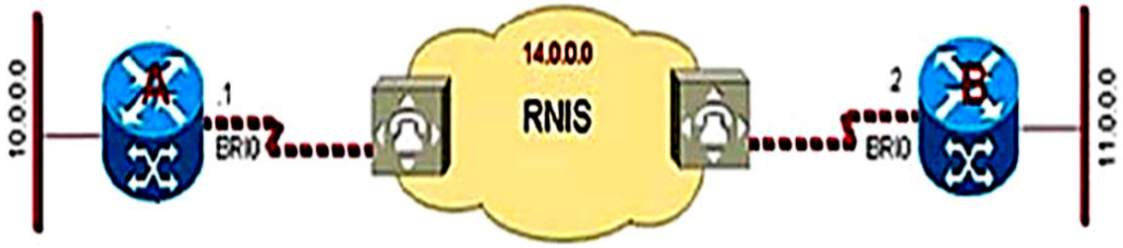

Figure 11 : Circuit point-à-point (P2P)

La connexion point à point comme illustrée dans la figure 11, est utilisée pour connecter un réseau LAN au réseau WAN du fournisseur de services, et pour connecter des segments de LAN dans un réseau d'entreprise. La connexion point à point du LAN au WAN est aussi appelée connexion série ou ligne louée. C'est dû au fait que les lignes sont louées à un opérateur (généralement la compagnie de la téléphonie) et sont dédiées à cet usage par la société qui les loue. Les entreprises paient pour bénéficier d'une connexion continue entre deux sites distants, et la ligne est active et disponible en permanence. Les lignes louées sont fréquemment utilisées pour accéder à un réseau étendu. Leur prix se base généralement sur la bande passante requise et la distance entre les deux points connectés **[4]**.

4.4.2 Circuit virtuel

Est un circuit logique passant au travers d'un nuage (exemple : ATM, Frame Relay, X25).

➢ Caractéristiques :

- Séquencement des paquets garanti (avantage).
- Court en-tête, acheminement plus rapide (avantage).
- Chaque connexion ouverte consomme des ressources (inconvénients).
- Perte de tous les circuits en cas de défaillance d'un routeur (inconvénients).

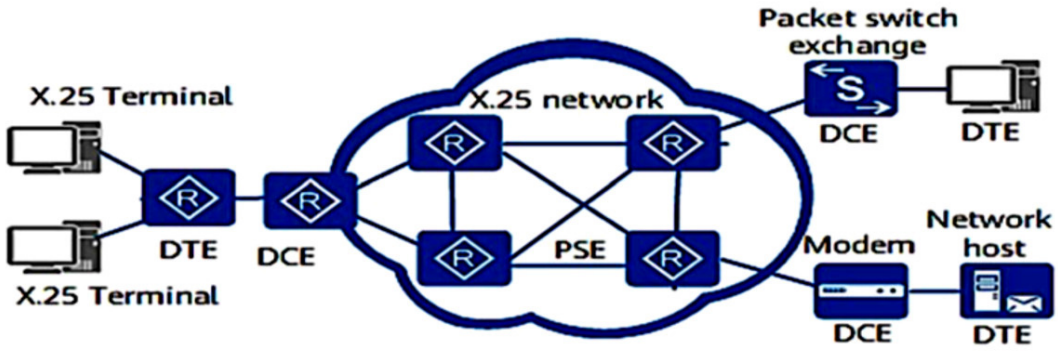

Figure 12 : Circuit virtuel (VC)

4.5 Topologies des réseaux étendus

Parmi les principales topologies utilisées dans le réseau WAN, à savoir la topologie en étoile (Hub and Spoke), en maillage global (Full Mesh) et en double réseau (Dual-Homed).

4.5.1 Topologie en étoile (Hub and Spoke)

La topologie en étoile (Hub and Spoke) est une topologie utilisée pour connecter plusieurs sites. Dans ce type de topologie, il existe deux rôles comme son nom l'indique. Hub et Spoke. Hub (Site A dans la figure ci-dessous) est l'appareil central d'un site connecté à tous les autres appareils. Spoke est le nom de chacun des autres sites et appareils. Les Spokes sont uniquement connectés au Hub. Il n'y a pas de connexion directe entre les Spokes (Site B, C et D dans la figure ci-dessous). La topologie Hub and Spoke est moins coûteuse si on compare cette conception avec une liaison point-à-point, parce qu'il n'est pas nécessaire de connecter chaque site *un par un* à d'autres sites. La seule connexion nécessaire est vers le site Hub **[5]**.

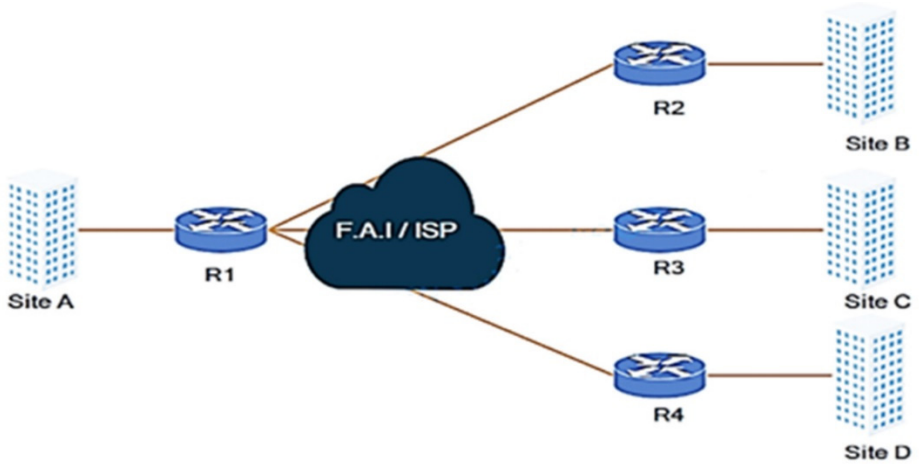

Figure 13 : Topologie Hub and Spoke

4.5.2 Topologie Full Mesh (Maillage global)

La topologie à maillage global est donc la topologie selon laquelle chaque site est connecté aux autres sites un par un. Cette topologie nécessite plus de ressources et coûte cher. De plus,

il faut un effort supplémentaire en raison du nombre de connexions. Il s'agit de la topologie la plus tolérante aux pannes. Par exemple, si le site B perd la connectivité avec le site A, il peut donc envoyer les données via le site C ou le site D **[5]**.

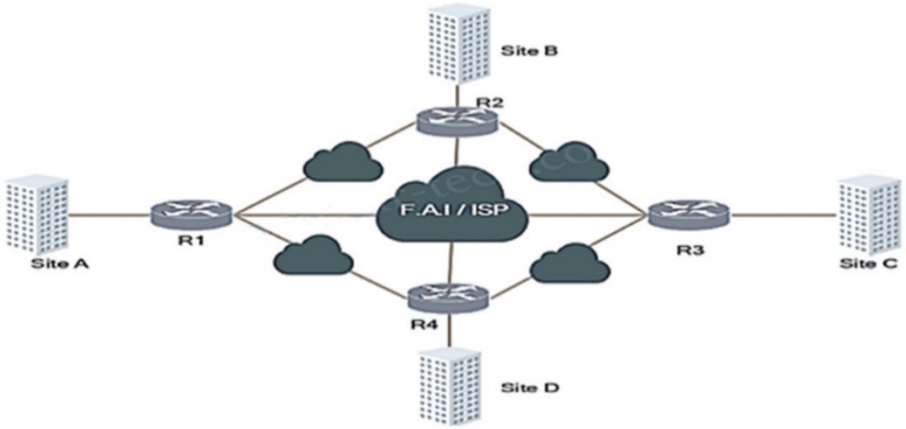

Figure 14 : Topologie Full Mesh

4.5.3 Topologie en double réseau (Dual-Homed)

La topologie en double réseau (Dual-Homed) est une très bonne solution pour de meilleures performances, de répartitions des charges et de redondances, mais cela a un inconvénient sur le coût, c'est une solution très coûteuse.

Dans la topologie Dual-Homed (à double réseau), un site est connecté à deux autres sites centraux (Site A et B par exemple). Même si l'un de ces sites est en panne, la connexion se poursuit. Dans des situations normales, répartition des charges est également fourni entre deux liaisons **[5]**.

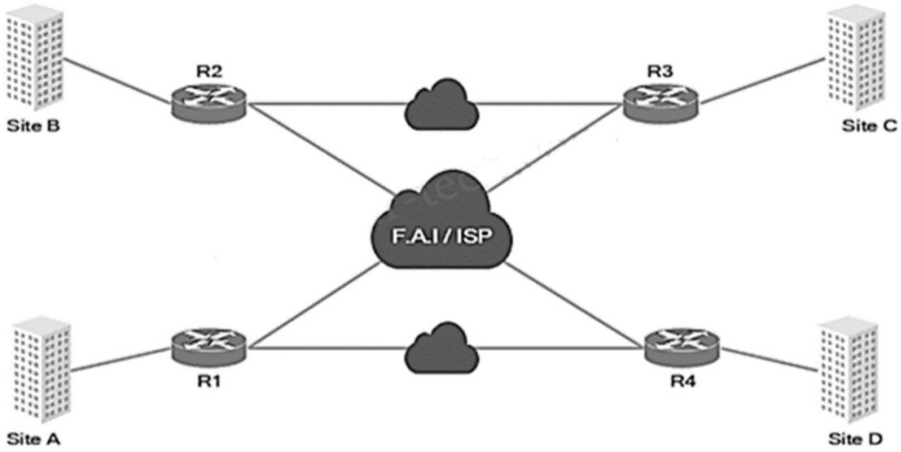

Figure 15 : Topologie Dual-Homed

4.6 Techniques de connectivité et protocoles

Il existe trois techniques de connectivité pour les réseaux étendus :

1. La ligne louée.
2. Commutation de circuit.
3. Commutation de paquet.

4.6.1 Ligne louée

Une ligne louée est une connexion directe au réseau que l'on peut louer auprès d'un fournisseur de réseau majeur, comme le Fournisseur d'Accès Internet (FAI/ISP : Internet Service Provider). Elle permet de relier deux points d'extrémité du réseau local. Il est important de noter que les lignes louées ne sont pas nécessairement des connexions physiques, mais peuvent également être des connexions virtuelles mises en place par les fournisseurs de services sur d'autres infrastructures réseau existantes **[web5]**.

4.6.2 Commutation de circuit

La commutation de circuit est un mode d'établissement d'une liaison de télécommunication pour laquelle : un chemin physique ou logique est établi entre deux équipements et est bloqué pour toute la durée de la communication. L'établissement de circuit est aujourd'hui exécuté de manière électronique. Dans la commutation par circuit, il y a un risque de sous-utilisation du support en cas de "silence" pendant la communication alors qu'avec de type de commutation, le temps passé est facturé. Un exemple de technologie à commutation de circuit est le réseau numérique à intégration de service "RNIS" **[web6]**.

Le RNIS en anglais ISDN (*Integrated Services Digital Network*) est un réseau à haut débit développé via un réseau téléphonique numérisé. Il autorise une connectivité de bout en bout et permet de transmettre des données (voix, images, texte…) à une vitesse tellement supérieure.
Pour ces deux types de connectivités précédentes, généralement on utilise les protocoles HDLC et PPP.

- **HDLC** (*High-level Data Link Control*) : est un protocole dit point-à-point de niveau 2 (couche liaison de données du modèle OSI), dérivé de SDLC (*Synchronous Data Link Control*). Son but est de définir un mécanisme pour délimiter des trames de différents types, en ajoutant un contrôle d'erreur " FCS " (*Frame check sequence*).

  En 1976, l'ISO a introduit une norme appelée HDLC qui permettait la communication entre deux ordinateurs. C'était le premier protocole standardisé au niveau de liaison. Avant cela, des protocoles moins avancés étaient utilisés, où l'envoi d'une trame était suivi d'une attente de confirmation de réception. HDLC a introduit un mécanisme anticipatif où l'attente de

confirmation n'empêchait pas l'envoi des trames suivantes. Pour les besoins des réseaux des opérateurs, l'UIT-T a adopté une partie de la norme HDLC, appelée LAP (Link Access Protocol), avec des options spécifiques. Après des mises à jour en 1980 et 1984, la procédure a été renommée LAP-B (Link Access Protocol-Balanced), adaptée au niveau 2 du RNIS (Réseau Numérique à Intégration de Services) pour les canaux de type B en mode circuit. Il existe également le protocole LAP-D (Link Access Procedure for the D-channel) associé au canal D du RNIS. En outre, il est possible de travailler en mode multi-liaison en multiplexant plusieurs protocoles LAP-B équilibrés sur une seule liaison **[6].**

- **PPP :** le protocole PPP (*Point-to-Point Protocol*) est couramment utilisé pour les connexions d'accès à Internet et les liaisons entre deux routeurs. Il est spécifié dans la norme RFC 1661 et opère au niveau de la couche de liaison de données (couche 2 du modèle OSI). Son principal objectif est d'encapsuler les paquets IP afin de les transporter vers le nœud suivant. Bien qu'il soit largement basé sur le protocole HDLC, il ajoute la fonctionnalité de spécifier le type d'informations transportées dans le champ de données de la trame. Étant donné que l'Internet est un réseau multi-protocole, il est essentiel de détecter l'application transportée à l'aide d'un champ spécifique au niveau de la trame, ce qui permet de l'acheminer vers la destination appropriée **[6].**

4.6.3 Commutation de paquet

La commutation de paquets, est une technique utilisée pour le transfert de données informatiques dans des réseaux spécialisés. Elle existe en deux grandes variantes : **les datagrammes** (données transmises sans connexions connues dans le réseau), et **les circuits virtuels** (données transmises avec connexions connues dans le réseau).

La commutation par paquets est une méthode de transmission de données sur un réseau numérique, où les données sont regroupées en paquets comprenant un en-tête et une charge utile. L'en-tête contient des informations utilisées par le matériel de mise en réseau pour acheminer le paquet vers sa destination, où la charge utile est extraite et utilisée par le logiciel d'application. La commutation par paquets constitue le fondement des communications de données dans les réseaux informatiques du monde entier. Elle diffère de la commutation de circuits, où les terminaux sont physiquement connectés pendant toute la durée de la communication. La commutation par paquets découpe les données afin d'utiliser efficacement le réseau, contrairement à la commutation de circuits où les ressources sont réservées en permanence. Chaque paquet contient un en-tête qui indique son contenu et sa destination,

permettant aux commutateurs de diriger les paquets vers leur point final. La décision de commutation est basée sur une étiquette présente dans l'unité de données de protocole (PDU), qui est extraite par le commutateur pour trouver la bonne interface de sortie dans sa table de commutation. Cela permet au commutateur de déterminer la nouvelle interface de transmission du paquet, ainsi que, éventuellement, une nouvelle valeur d'étiquette **[web7]** :

En mode datagramme un nœud du réseau est désigné comme un routeur. L'étiquette dont il est question correspond à l'adresse de destination présente dans l'en-tête IP, qui normalement ne change pas en cours de route (à l'exception de certaines situations depuis l'introduction de la fonction NAT dans Internet). De même, dans un commutateur Ethernet, l'étiquette correspond à l'adresse MAC de destination. Grâce à la consultation répétée d'une table de routage pour chaque paquet, ce qui représente un traitement non trivial, il est assuré qu'une panne de routeur ne provoque pas la rupture des connexions qui le traversent (à condition que la mise à jour des tables de routage en amont soit suffisamment rapide).

En mode circuit virtuel, un nœud du réseau est appelé un commutateur (service X.25, FR, ATM, MPLS). Ce mode de fonctionnement est basé sur une connexion établie. L'étiquette utilisée identifie la connexion en cours parmi celles qui traversent le commutateur. À l'arrivée d'un paquet, l'étiquette entrante permet à chaque commutateur de déterminer directement la prochaine liaison à emprunter, ainsi que l'étiquette de sortie à y associer. Cette correspondance est établie et enregistrée lors de l'établissement de la connexion. L'avantage de ne pas avoir à consulter une table de routage pour chaque paquet se traduit par un temps de traitement plus rapide. Cependant, en cas de panne du commutateur, la connexion devra être rétablie par son initiateur **[7].**

Pour ce type de connectivite plusieurs protocoles étaient utilisés tel que le **X25**, **Frame Relay (FR)**, **ATM** et **MPLS**.

- **Protocole X25 :** C’est l'un des premiers protocoles utilisés pour assurer le transfert de données à haut débit sur les réseaux étendus (WAN). Il repose sur l'utilisation de commutateurs de paquets (PSE) pour acheminer les données à travers les câbles de connexion vers une destination donnée. Le protocole X.25 utilise des paquets de taille standard, envoyés de manière séquentielle, et intègre également un mécanisme de correction d'erreurs. Les liaisons physiques utilisées peuvent inclure des lignes louées, des services téléphoniques à commutation ou des connexions du réseau numérique à intégration de services (RNIS) **[7]**.

- **Frame Relay (FR)** : Le relais de trames a été introduit après le protocole X.25. Il divise les données en plusieurs trames de tailles variées et délègue aux utilisateurs finaux la correction des erreurs et la retransmission des paquets manquants. Ces caractéristiques améliorent le débit global des données. De plus, ce protocole repose moins sur des connexions dédiées, ce qui permet la création de réseaux maillés. Cela réduit le nombre de circuits physiques nécessaires et permet aux entreprises de réaliser des économies.
- **Mode de transfert asynchrone ou ATM** : L'ATM (*Asynchronous Transfer Mode*) présente des similitudes avec le relais de trames, mais avec une différence majeure : les données sont réparties en paquets de taille standard appelés cellules. Ces cellules facilitent la fusion de différentes couches de trafic sur un même circuit physique et garantissent la qualité de service. Cependant, l'inconvénient de l'ATM réside dans le fait que, en utilisant des cellules relativement petites, une part importante de la capacité de transmission est consommée par les en-têtes. Par conséquent, l'utilisation de sa bande passante globale est moins efficace que celle du relais de trames.
- **MPLS** : De nos jours, le MPLS (Multi-Protocol Label Switching) est largement utilisé pour le transport des données d'entreprise sur les liaisons WAN. Dans ce type de réseau, les routeurs MPLS sont capables de prendre rapidement des décisions sur la destination des paquets et de les traiter en fonction de la classe de service indiquée par les étiquettes. Cette approche permet l'exécution de différents protocoles au sein des paquets MPLS, tout en donnant la priorité appropriée aux différentes applications lorsque le trafic se déplace entre les sites. Le protocole Internet (IP), qui est devenu omniprésent dans les années 1990, est couramment utilisé dans le contexte du MPLS **[7].**
- Le trafic entre les stations WAN peut être protégé par des **réseaux privés virtuels (VPN**). En effet, ce système couvre la sécurité du réseau physique sous-jacent, notamment l'authentification, le cryptage, la confidentialité et la non-répudiation.

D'autre techniques de connectivités sont utilisées au niveau d'internet pour les réseaux étendus à savoir :

- **DSL** : Le DSL (Digital Subscriber Line) est devenu une option très populaire pour accéder à Internet à haut débit en utilisant les câbles téléphoniques analogiques déjà présents dans la plupart des maisons et immeubles. La vitesse de connexion dépend de la distance entre l'immeuble et la compagnie de téléphone, ainsi que du support utilisé. Chez le client, un répartiteur est connecté à la ligne téléphonique fournie par l'opérateur de téléphonie. Un câble RJ11 est connecté d'un côté au téléphone analogique et de l'autre à un modem DSL.

Ce modem DSL est généralement équipé d'une connexion Ethernet vers un routeur. De nos jours, le modem DSL est souvent intégré au routeur lui-même. L'opérateur téléphonique utilise un dispositif appelé DSLAM (*Digital Subscriber Access Multiplexer*) pour séparer le trafic de données du trafic vocal. Le trafic de données est acheminé vers un routeur, tandis que le trafic vocal est dirigé vers un commutateur vocal **[8].**

- **Câble** : L'Internet par câble est similaire au DSL, il est également devenu populaire depuis que la plupart des maisons et des bâtiments disposent d'une connexion par câble. L'internet par câble utilise la norme DOCSIS (*Data Over Cable Service Interface Specification*) pour transporter les données sur un câble coaxial ou même par une fibre optique.
- **Ethernet** : L'Ethernet s'est également étendu jusqu'au WAN. Par exemple, la norme 1000BASE-ZX prend en charge une distance d'environ 40 miles sur des connexions en fibre monomode. Du point de vue du client, cela ressemble à une ligne louée. Chaque site client est équipé d'un routeur qui est connecté au fournisseur d'accès WAN Ethernet via une connexion en fibre optique. La connexion du côté du fournisseur de services est appelée POP (*Point of Presence*). De nombreux fournisseurs utilisent le terme "ligne privée Ethernet" pour désigner cette configuration. Il est également possible d'avoir plus de deux sites, créant ainsi un réseau multi-accès. L'Ethernet est également utilisé en combinaison avec différentes technologies WAN sous-jacentes telles que EoMPLS (Ethernet over MPLS) **[8].** Encore d'autres technologies comme le **sans fils** et le **satellite** sont aussi utilisés pour la connectivité WAN.

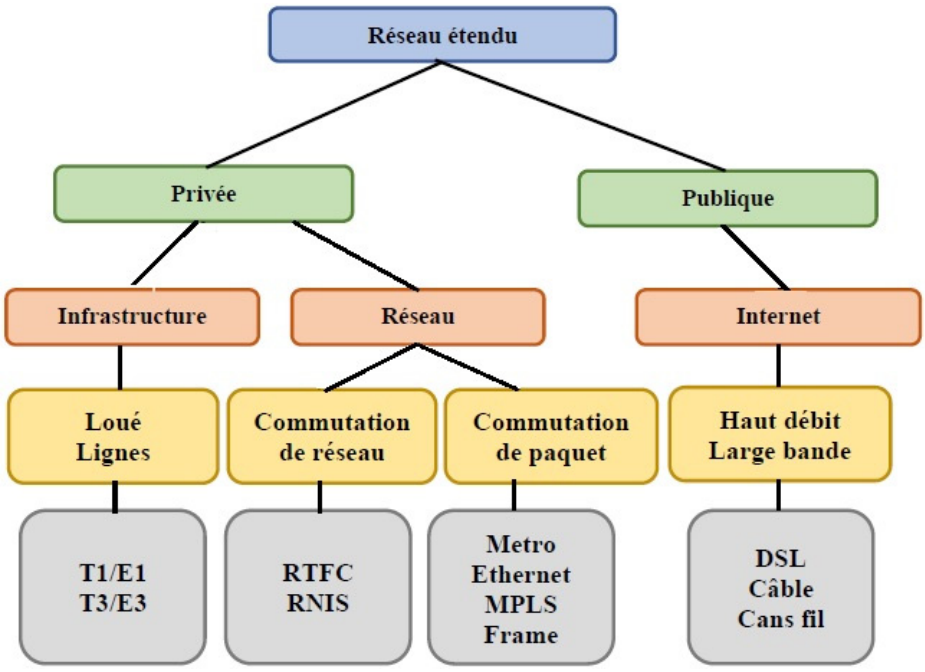

Figure 16 : Options de connexions de réseaux étendus WAN

5. Conclusion

Dans ce chapitre, nous avons élaboré les différents types de réseaux à savoir le PAN, le LAN, le MAN et le WAN et ses domaines d'applications, après nous avons cité les différentes topologies utilisées dans le réseau étendu WAN, et nous avons détaillé les équipements utilisés dans ce dernier avec une large discussion sur les différents protocoles exploités dans les réseaux étendus.

Nous avons également souligné l'importance du réseau WAN pour les entreprises, les opérateurs et les utilisateurs, en soulignant leurs avantages en termes d'efficacité, de partage de ressources, d'accès distant et de communication entre les sites distants.

Le chapitre suivant, décrive les deux protocoles importants utilisés dans le réseau étendus WAN à savoir le protocole MPLS et son successeur GMPLS (Generalized Multi-Protocol Label Switching). Une comparaison détaillée en termes de performances, de flexibilités, et d'applications sera abordée.

Chapitre II :
Fondements théoriques de GMPLS

1 Introduction

Le MPLS a été créé dans les années 1990 pour améliorer les performances de réseaux informatiques, en utilisant une technique d'étiquetage de paquets de données, proposé par l'ingénieur de Cisco Systems, Yakov Rekhter.

La première spécification du MPLS a été publiée en 1997 par l'IETF (Internet Engineering Task Force), et il a été initialement utilisé pour les réseaux privés des entreprises et les fournisseurs de services Internet. Le MPLS a évolué pour inclure de nombreuses fonctionnalités et est largement utilisé dans de nombreux domaines, offrant une connectivité hautement fiable et efficace.

Dans ce chapitre nous allons décrire le principe du protocole MPLS avec ses fonctionnalités, ses architectures et son acheminement du trafic dont le but est de comparer celui avec son successeur GMPLS (Generalized Multi-Protocol Label Switching).

2 MPLS (Multi-Protocol Label Switching)

MPLS est une technologie de réseau permettant un routage efficace du trafic en utilisant des labels plutôt que des adresses IP.

L'utilisation des labels nous offre une rapidité et une efficacité meilleure de la commutation de paquets, ce qui nous permettra une amélioration des performances et de la qualité de service dans les grands réseaux. MPLS est souvent utilisé par des fournisseurs de services Internet dans les réseaux WAN, comme il peut être utilisé dans les réseaux d'entreprise pour connecter des sites distants.

2.1 Fonctionnement de MPLS

La transmission des données s'effectue sur des chemins appelés LSP. Un LSP est une suite de références partant de la source et allant jusqu'à la destination.

Les LSP sont établis avant la transmission des données ou après la détection d'un flux voulant traverser le réseau **[9].**

Les références contenues dans les trames sont réparties selon le protocole de signalisation. Le plus important de ces protocoles est le LDP, mais le RSVP est également utilisé, éventuellement en conjonction avec un protocole de routage tel que l'OSPF. Les trames transportant des paquets IP, elles aussi transportent les références d'un nœud à un autre **[6].**

2.2 Architecture du MPLS

Les nœuds participant au MPLS sont classés en tant que Label Edge Router (LER, Routeur d'extrémité supportant les labels) et Label Switching Router (LSR, routeur de commutation des labels). Le LSR est un routeur de réseau central qui vous permet de configurer le circuit virtuel à travers lequel les trames sont acheminées. Le LER est le nœud d'accès au réseau MPLS. Le

LER peut avoir plusieurs ports donnant accès à différents réseaux, chacun avec sa propre technologie de commutation. Dans la mise en place des références les routeurs LER ont un rôle important à jouer **[web8]**.

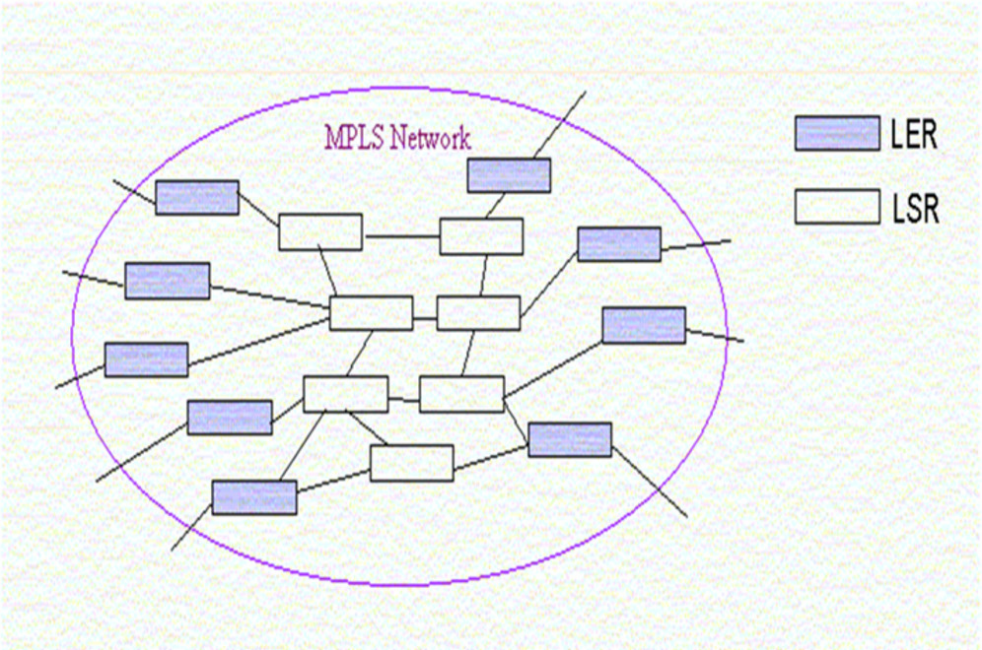

Figure 17 : Architecture d'un réseau MPLS

2.3 En tête MPLS (Shim Header)

L'entête MPLS se place entre les deux entêtes des couches protocole de liaison et la couche réseau. Elle est composée de quatre champs (32 bits) **[web9]** :

- Le champ Label (20 bits), pour représenter le label, fournissant des informations sur le protocole de la couche réseau et des informations pour transférer les données.
- Le champ Exp (CoS) (3 bits) c'est la classe de service.
- Un bit Stack (BS) qui va servir pour l'empilement des labels.
- Le champ TTL (Time To Live) pour limitation de la durée de vie de paquet (8 bits).

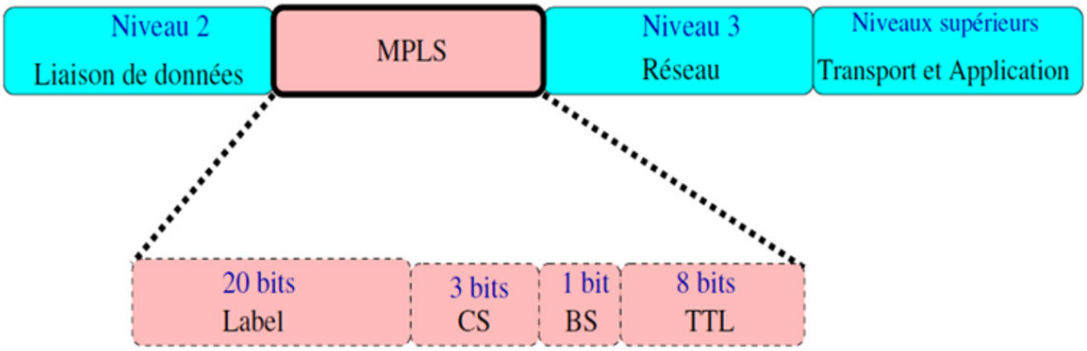

Figure 18 : Entête MPLS

2.4 Label (étiquette)

Le label MPLS est un identifiant de 20 bits attribué à chaque paquet IP par le premier LSR pour permettre le routage efficace des paquets dans les réseaux MPLS. Ce label est utilisé par les LSR suivants pour acheminer le paquet vers sa destination en suivant le chemin prédéfini dans la table de routage MPLS **[web10].**

2.5 Empilement de labels (Label Stack)

Une pile de labels c'est l'ajout de plusieurs labels en vue de l'association de plus qu'un contrat de service à un flux de données en ajoutant plusieurs labels à l'en-tête du paquet dans un réseau MPLS. Cela permet une gestion plus précise de la QoS et de la bande passante pour les applications sensibles aux délais et à la performance **[web10].**

Les labels sont organisés en une pile c.à.d. le dernier entré, premier sorti.

L'empilement de labels exige **[web11] :**

- MPLS VPN : ou on utilise MP-BGP (Multi-Protocol Border Gateway Protocol) pour distribuer le deuxième label, il est d'ajouter celui qui a été distribué par le TDP ou le LDP.
- MPLS-TE (MPLS-Traffic Engineering) : dans ce cas RSVP-TE sera utilisé pour l'établissement du tunnel LSP, et l'ajout du deuxième label au label distribué par le TDP ou le LDP.

2.6 FEC (Forwarding Equivalence Class)

Tous les paquets IP entrant sur le réseau MPLS sont associés à une FEC, ces paquets seront classifier dans se FEC dans un groupe pour unifier leur traitement en ce qui concerne **[web12] :**

- La manière d'expédition.
- Le chemin à empreindre.
- Le traitement d'expédition.

Le protocole de distribution de label utilisé : LDP ou RSVP-TE va entrer dans les paramètres de classification d'un paquet dans une FEC en respectant les paramètres de QoS.

2.7 LSP (Label Switched Path)

Les LSP sont des chemins définis par des références déterminées par la signalisation. Dans le cas le plus classique, les LSP sont déterminés dans le domaine avant l'arrivée des données. Deux options sont utilisées pour cela **[6]** :

- **Routage saut par saut (hop-by-hop) :** pour cela Le LSR utilise pour cela un protocole de routage (OSPF, IS-IS), pour que les LSR sélectionnent les prochains sauts indépendamment les uns des autres.

- **Routage explicite :** dans un domaine MPLS, la liste des nœuds par lesquels la signalisation sera routée est définie par le LER d'entrée, le choix de cette route pouvant avoir été contraint par des demandes de qualité de service.

Le chemin parcouru par les trames dans un sens de la communication peut être différent dans le sens inverse.

2.8 Acheminement du trafic dans un réseau MPLS

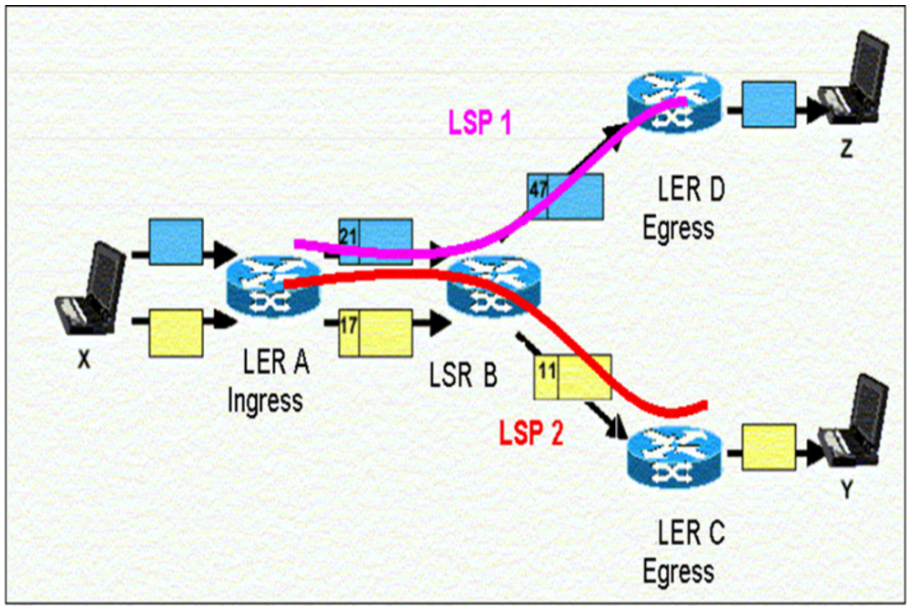

Figure 19 : Différentes étapes dans l'acheminement

Etape 1

Dans un domaine MPLS le 1er LER A va recevoir un trafic IP entrant, il analysera l'adresse IP de ces paquets et le FEC pour regrouper tous les paquets qui se ressemble. Quand le bon LSP a emprunté est déterminé, chaque paquet aura un label pour être envoyés sur la bonne interface. Comme on peut le voir sur la figure 19, le LER A assigne le label 21 au paquet bleu et le label 17 au paquet jaune **[web13].**

Etape 2 à étape (n-1)

Les LSR situés dans le cœur du réseau MPLS vont examiner le label affecté à chaque paquet et consulter leur table de commutation appelée " Forwarding Table " pour faire un échange de label sur les paquets comme illustré dans la figure 19.

La table de commutation " Forwarding Table " du LSR B comme exemple, va remplacer les labels 21 et 17 par les labels 47 et 11, Le paquet est affecté de nouveau label et sera envoyé sur la bonne interface de sortie.

Comme la correspondance entre les différents labels au niveau des LSR est fixée, le chemin (LSP) est déterminé par la valeur du 1er label affecté par le premier LSR.

Etape n

Arrivé aux LER de sortie (LER C et LER D) ces derniers retireront les labels aux paquets pour continuer leur trajet hors MPLS.

2.9 Agrégation de flots

Pour éviter l'augmentation du nombre de références utilisable et l'allégement des tables de commutation, les flots provenant de différentes interfaces peuvent être fusionner et dirigé vers une interface de sortie commune **[6].**

2.10 Signalisation

La signalisation dans le MPLS est le processus par lequel les routeurs MPLS échangent des informations sur les étiquettes (labels) à utiliser pour acheminer les paquets de données à travers le réseau. La signalisation est essentielle pour l'établissement des LSP dans MPLS, qui permettent un acheminement plus rapide et plus efficace des paquets de données.

Il existe deux protocoles de signalisation couramment utilisés dans MPLS :

- **LDP (Label Distribution Protocol) :** LDP est un protocole de signalisation simple qui permet aux routeurs MPLS de s'échanger des informations sur les étiquettes à utiliser pour acheminer les paquets de données. Lorsqu'un routeur MPLS reçoit un paquet de données, il examine l'adresse IP de destination et utilise LDP pour déterminer l'étiquette MPLS appropriée à utiliser pour acheminer le paquet vers le prochain routeur du LSP. **[web14].**
- **RSVP-TE (Resource ReSerVation Protocol - Traffic Engineering) :** RSVP-TE est un protocole de signalisation plus avancé qui permet une QoS (Quality of Service) plus granulaire et une gestion plus fine de la bande passante. Avec RSVP-TE, les routeurs MPLS peuvent échanger des informations sur la bande passante disponible sur les liens du réseau et réserver des ressources pour des LSP spécifiques. Cela permet de garantir une QoS élevée pour des applications telles que la voix et la vidéo **[web15].**

Dans les deux cas, la signalisation permet aux routeurs MPLS de communiquer et de se coordonner pour acheminer efficacement les paquets de données à travers le réseau.

2.11 VPN niveau 2 et 3

Les VPN exploitent une infrastructure de télécommunications publique, comme l'Internet, afin de permettre aux utilisateurs individuels ou aux bureaux distants de bénéficier d'un accès sécurisé au réseau de leur organisation. Les VPN sont conçus pour offrir des performances et une sécurité similaire à celles des réseaux privés propriétaires ou loués, mais sans les frais associés **[web16].**

2.11.1 VPN niveau 2

Les premiers VPN d'entreprise étaient de niveau 2 et transportaient des trames d'un port d'entrée à un port de sortie via des circuits virtuels permanents de niveau trame. Les points d'accès de l'entreprise assuraient les fonctions de filtrage, tandis que l'opérateur ne fournissait que les circuits virtuels pour acheminer les paquets IP encapsulés dans les trames LAP-D d'un relais de trames ou les cellules d'un réseau ATM. D'autres types de tunnels tels que PPTP, L2F, L2TP ont été proposés pour réaliser ces VPN, mais ils sont en décroissance aujourd'hui. Les VPN Ethernet ont été développés pour réaliser des VPN peu coûteux et offrant une grande souplesse d'utilisation. Les VPN de niveau 2 sont maintenant délaissés **[6].**

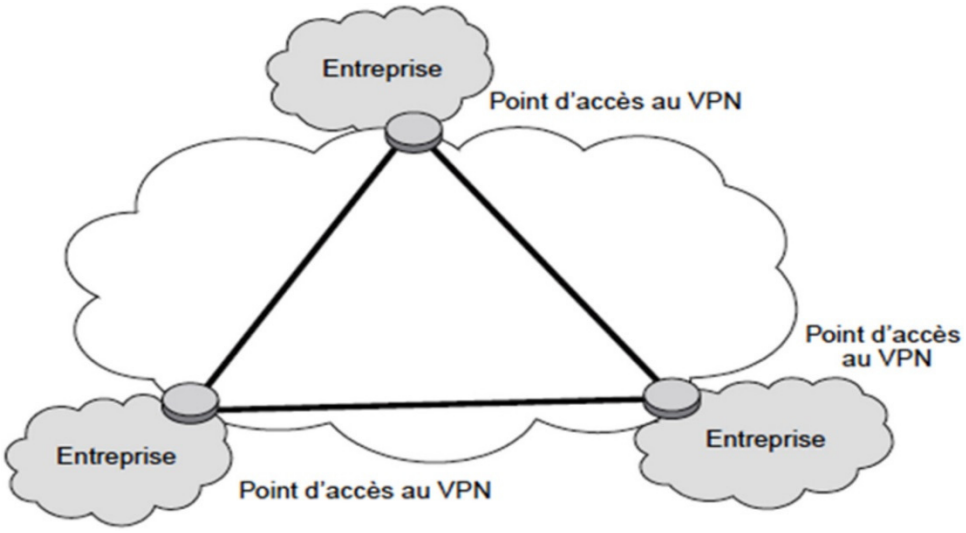

Figure 20 : Exemple de VPN niveau 2

2.11.2 VPN niveau 3

Les VPN de niveau 3 sont appelés VPN IP car ils utilisent la couche IP. Cette technologie de VPN est développée pour permettre aux entreprises distribuées de bénéficier de toutes les fonctionnalités d'un réseau intranet ou extranet. Les terminaux fixes et mobiles peuvent être intégrés grâce à la solution IP. Les routeurs IP sont utilisés comme points d'accès pour permettre aux paquets IP d'entrer et de sortir des entreprises A, B et C, qui ont des VPN IP. Les clients d'un même VPN utilisent le réseau IP pour se déplacer entre les points d'accès appartenant au VPN. Les utilisateurs prennent en charge la qualité de service et la sécurité, qui est un élément essentiel de ces réseaux. Pour assurer la sécurité, la première génération de VPN IP a utilisé le protocole IPsec pour créer des tunnels chiffrés, avec la possibilité pour l'utilisateur de choisir ses algorithmes de chiffrement et d'authentification. Les points d'accès des VPN communiquent entre eux via ces tunnels chiffrés. L'opérateur doit maintenant configurer les nœuds dynamiquement pour répondre aux exigences de tous les SLA (Service Level Agreement), ce

qui pose de nouveaux défis. Une solution qui se développe repose sur la configuration par politique, mais nous allons d'abord examiner les autres types de VPN **[6].**

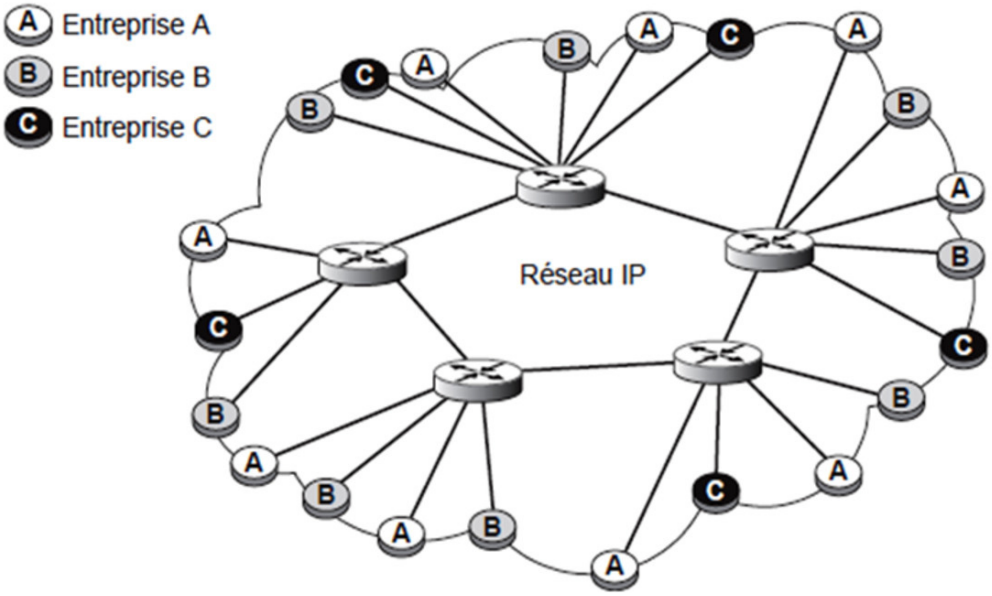

Figure 21 : Exemple de VPN niveau 3

2.12 MPLS et VPN

Dans le cadre de MPLS/VPN, des tunnels sont établis entre les routeurs MPLS périphériques de l'opérateur, dédiés à des groupes restreints d'utilisateurs spécifiques, formant ainsi des VPN. Selon cette approche, un VPN est un ensemble de sites qui sont placés sous la même autorité administrative ou qui sont regroupés en fonction d'un intérêt commun **[web17].**

En ce qui concerne les VPN, si tous les sites appartiennent à la même entreprise, on parle d'un "intranet" d'entreprise. Si les sites appartiennent à différentes entreprises, on parle d'un "extranet"**.**

Dans un environnement MPLS/VPN, une terminologie spécifique est utilisée pour désigner les différents types de routeurs selon leur rôle. On distingue ainsi les routeurs P (Provider), PE (Provider Edge), et les routeurs CE (Customer Edge). Les routeurs PE se trouvent à la frontière entre le réseau du client et le backbone MPLS. Ils sont responsables de l'attribution des labels aux paquets en fonction des VPN associés. Les routeurs P appartiennent au cœur du backbone MPLS, ils n'ont pas connaissance des VPN et ne sont donc pas en mesure de déchiffrer les labels VPN mais ils sont chargés de l'acheminement des paquets en se basant sur les labels. Enfin les routeurs CE sont la propriété du client et sont des équipements situés à la frontière du réseau privé du client et du réseau MPLS, leur rôle c'est de connecter les équipements du client au réseau MPLS **[web17].**

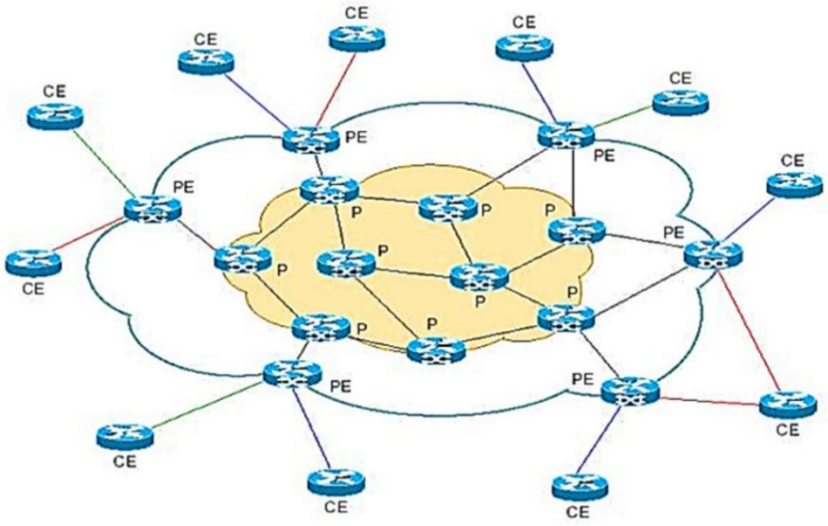

Figure 22 : Emplacement des différents routeurs dans une architecture MPLS

3 GMPLS (Generalized Multi-Protocol Label Switching)

GMPLS est une extension de MPLS permettant la gestion et de contrôler des réseaux optiques, les réseaux sans fil et les réseaux de satellites.

GMPLS permet également de gérer la commutation de circuits et de longueurs d'onde dans les réseaux optiques. Cette fonctionnalité est particulièrement utile dans les réseaux de transport de données à haute capacité, où les circuits optiques sont utilisés pour acheminer des volumes de données massifs à des vitesses très élevées.

3.1 Principe général

Comparé à MPLS, le GMPLS dispose de fonctionnalités avancées telles que la découverte des voisins, la distribution des informations de liaison, la gestion de la topologie, des chemins, la protection des liens et la garantie de la reprise. De plus, le GMPLS permet de faire circuler les paquets à la vitesse de la lumière à travers le réseau, tout en prenant en compte le contrôle centralisé. Cela comprend des fonctionnalités telles que le provisioning automatique, l'équilibrage de charge, les services de bande passante provisionnée, les services de bande passante garantis et les réseaux privés virtuels optiques (OVPN : Optical Virtual Private Network).

La figure présentée ci-dessous illustre l'évolution de l'encapsulation des données dans les réseaux IP jusqu'à la couche optique DWDM (Dense Wavelength Division Multiplexing) **[web18].**

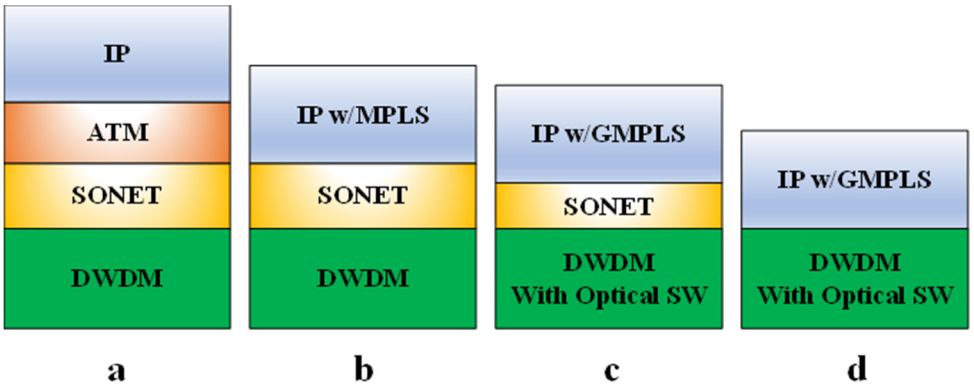

Figure 23 : Evolution de l'encapsulation des données dans les réseaux IP jusqu'à la couche optique DWDM

- Dans la figure a, les données à la sortie des routeurs sont acheminées vers les commutateurs ATM. Ces derniers sont à leur tour connectés aux multiplexeurs SONET/SDH, qui sont reliés au réseau DWDM.
- Dans la figure b, la couche ATM est enlevée parce que dans beaucoup de réseaux de cœur actuels, on transporte directement l'IP sur la couche SDH/SONET. Pour garantir la remise fiable des paquets au même titre que l'ATM, la fonctionnalité MPLS a été ajoutée à l'IP.
- Dans la figure c, la couche SONET/SDH a été réduite grâce à l'introduction de GMPLS.
- Enfin, dans la figure d, grâce à GMPLS, on achemine le trafic IP directement sur la couche DWDM tout en gardant une remise fiable et avec un plan de contrôle centralisé.

3.2 Extensions de MPLS

MPLS est une technologie de commutation de niveau 2 (L2S : Level 2 Switching) qui permet de router des paquets sur des réseaux de données. Cependant, grâce à des extensions, il est possible d'introduire des références sur d'autres supports tels que le temps partagé ou la longueur d'onde d'une fibre optique. Les extensions principales de MPLS comprennent **[6]** :

- PSC (Packet Switching Capable) pour les paquets qui peuvent recevoir une référence. Habituellement, la trame PPP sert de support pour les paquets IPv6 avec le flow-label comme référence. Par conséquent, il est nécessaire d'encapsuler le paquet dans une trame pour assurer sa transmission.
- L2SC (Level 2 Switching Capable) qui correspond à la commutation de labels utilisée dans la norme MPLS.
- TDMC (Time Division Multiplexing Capable) permettant l'introduire d'une référence dans un multiplexage temporel sous forme de slot. Cette extension est adaptée aux techniques de commutation avec une structure sous forme de trame comportant des slots, notamment pour les techniques hertziennes avec division temporelle, qui sont intégrées dans le GMPLS.

- LSC (Lambda Switching Capable) utilisant le numéro de la longueur d'onde comme référence de commutation à l'intérieur de la fibre optique. Cette technique était la première extension de MPLS sous le nom de MPLS.
- FSC (Fiber Switching Capable) utilisant le numéro d'une fibre optique comme référence de commutation. Les fibres d'un faisceau sont numérotées de 1 à n, n correspondant au nombre de fibres optiques.

3.3 Contrôle et gestion dans le GMPLS

Dans le but d'améliorer le contrôle et la gestion, il est essentiel de bien séparer les plans : utilisateur, de gestion et de contrôle, surtout dans les réseaux complexes, y compris ceux utilisant des fibres optiques. Comme dans le cas de l'ATM, GMPLS distingue trois plans **[6]** :

- Le plan utilisateur, chargé de transporter les données utilisateur d'une extrémité à l'autre.
- Le plan de contrôle, destiné à établir des circuits virtuels, à les détruire à la fin de la transmission ou à les maintenir si nécessaire.
- Le plan de gestion, qui transporte les messages nécessaires à la gestion du réseau.

Les groupes de travail de GMPLS ont élaboré une telle architecture pour permettre le contrôle de l'ensemble des composants du réseau par un plan spécifique. Pour s'adapter au protocole GMPLS, les protocoles de signalisation ont également été développés.

3.4 Label GMPLS

Les labels GMPLS sont similaires aux labels MPLS en ce sens qu'ils sont utilisés pour acheminer le trafic sur des circuits virtuels prédéfinis, mais ils prennent également en compte les caractéristiques spécifiques des réseaux optiques et des réseaux de transport. Les labels GMPLS peuvent être utilisés pour identifier les chemins optiques, les longueurs d'onde, les fréquences et les ports d'interface, entre autres. Ils sont utilisés pour activer les connexions sur demande, réservées ou partagées dans les réseaux optiques et de transport. Les labels GMPLS peuvent être attribués par le nœud d'entrée de l'information ou par le nœud de sortie, selon le mode de signalisation utilisé **[web19].**

GMPLS se base sur la notion "label généralisé". Ainsi, un label généralisé peut représenter :

- Un brin unique de fibre optique dans un faisceau,
- Une bande unique de longueurs d'ondes dans une fibre optique,
- Une unique longueur d'onde dans une bande (ou une fibre),
- Ou un ensemble de Time-slots dans une longueur d'onde (ou une fibre).
- Un label généralisé peut également porter un label qui représente un label MPLS générique, un label Frame Relay ou un label ATM.

3.5 Types LSP GMPLS

On distingue quatre types de LSP GMPLS : **[web19]**

- **Commutation de fibre (FSC) :** pour équipements utilisant des fibres optiques (OXC opérant au niveau des fibres individuelles).
- **Commutation Lambda (LSC) :** pour équipements DWDM (OXC opérant au niveau des longueurs d'onde individuelles).
- **Commutation TDM (TDM) :** pour équipements TDM, (MMA SONET).
- **Commutation de paquets (PSC) :** pour équipements utilisant des paquets (routeurs, commutateurs ATM).

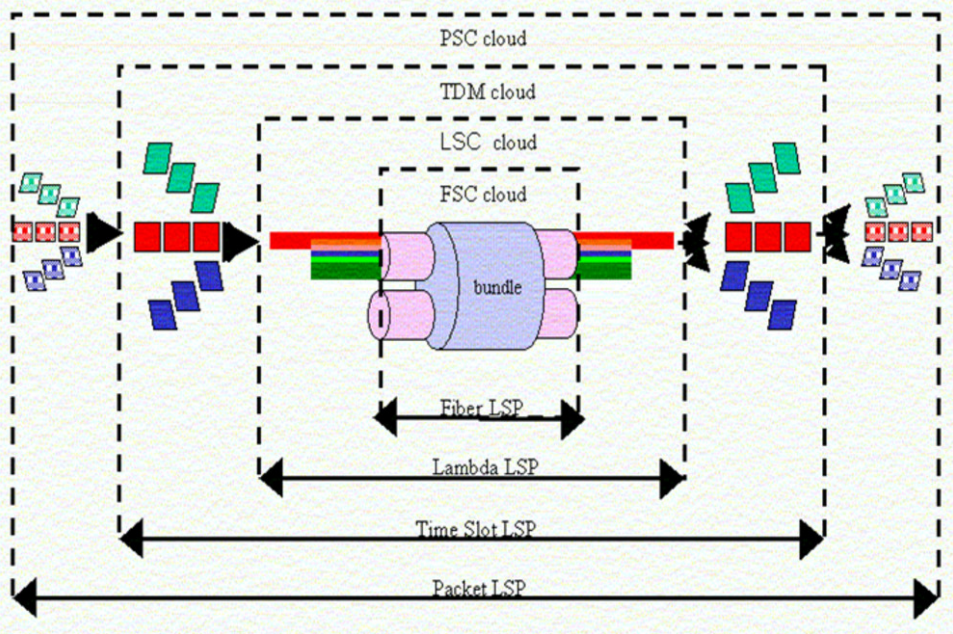

Figure 24 : Types LSP GMPLS

3.6 Etablissement LSP

Dans le GMPLS pour établir des LSP, on utilise les mécanismes suivants **[web19]** :

- Un canal de contrôle hors bande et un canal de données : les messages RSVP pour la configuration des LSP sont envoyés sur un réseau de contrôle hors bande. Quand la configuration des LSP est terminée et que le chemin est provisionné, le canal de données est activé et pour le transporte du trafic.
- Le protocole de gestion de lien (LMP) est utilisé pour la définition et la gestion des canaux de données entre deux nœuds.
- RSVP-TE est déjà conçu pour la signalisation de la configuration des LSP de paquets. Cela a été étendu pour GMPLS afin de pouvoir demander la configuration de chemins pour différents types de LSP (non paquets) et faire une demande des étiquettes (longueurs d'onde, créneaux horaires et fibres en tant qu'objets d'étiquette).

- LSP bidirectionnels ou les données circulerons dans les deux sens entre dispositifs GMPLS sur le même chemin.

3.7 LSP hiérarchiques

Grâce au GMPLS, il est maintenant possible la création et la configuration d'un chemin traversant différents réseaux de bout en bout. En effet, plusieurs LSP de type "Packet" peuvent être encapsulés dans un LSP de type "TDM" pour être transportés au sein d'un réseau SDH. De même, ce LSP de type "TDM" peut être encapsulé dans un LSP de type "Lambda" pour le transport, et plusieurs LSP de type "Lambda" peuvent être encapsulés dans un LSP de type "FSC" pour permettre la commutation de fibres. Cette fonctionnalité est appelée LSP hiérarchiques.

Un nouveau LSP peut être créé à l'intérieur d'un LSP existant de niveau supérieur, de sorte que cette dernière serve de support pour le nouveau LSP. L'ordre d'encapsulation de ces LSP est déterminé par les capacités de multiplexage des différents nœuds. Le nœud de la frontière de deux régions peut créer des LSP de niveaux supérieurs et regrouper des LSP de niveaux inférieurs en fonction de ses capacités de multiplexage. Ainsi, la demande de création d'un LSP de niveau inférieur pourra entraîner la création d'un LPS de niveau supérieur **[web20].**

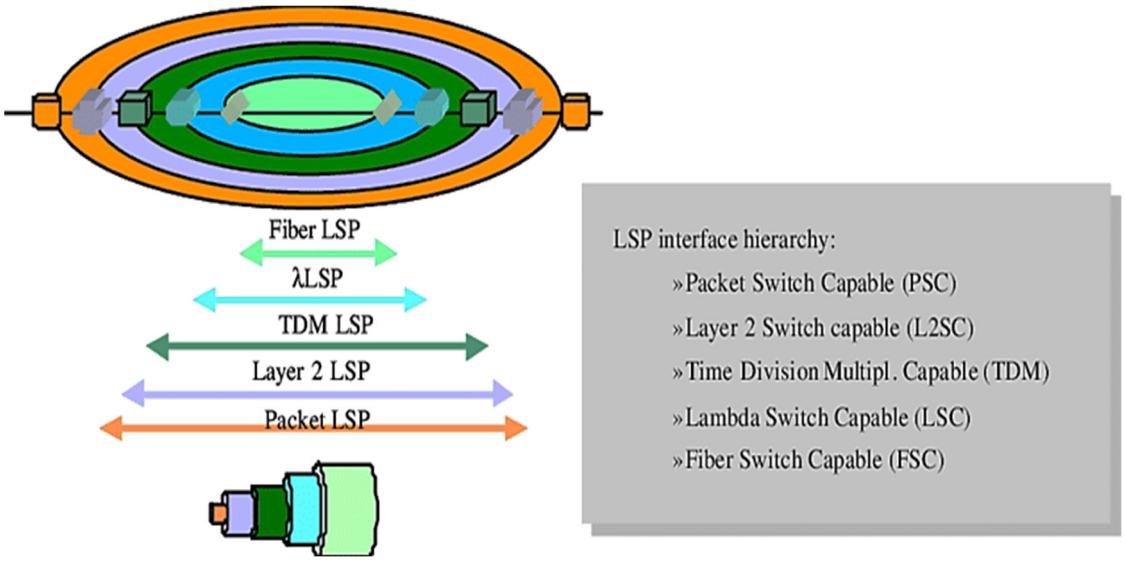

Figure 25 : Concept de LSP hiérarchiques **[web21]**

3.8 Protocoles utilisés

GMPLS est composé de trois principaux protocoles **[10]** :

- Un protocole de signalisation : Ressource ReSerVation Protocol with Traffic Engineering extensions (RSVP-TE)
- Un protocole de routage: Open Shortest Path First with Traffic Engineering extensions (OSPF-TE)
- Un protocole de gestion des liens : Link Management Protocol (LMP).

3.8.1 Extensions de RSVP-TE

D'abord un mot sur RSVP et RSVP-TE. RSVP est utilisé dans MPLS comme protocole de signalisation pour établir, maintenir et supprimer une connexion. RSVP-TE est l'extension d'ingénierie de trafic de RSVP qui permet l'établissement de LSP en tenant compte de contraintes supplémentaires telles que la bande passante disponible et les sauts/routes optimaux. RSVP-TE utilise le message PATH du routeur d'entrée au routeur en aval pour demander la réservation de chemin/bande passante. Ce message atteint saut par saut et le routeur de sortie répond par le message RESERVE. Le message RESERVE atteint le routeur d'entrée en réservant les ressources saut par saut sur le chemin. Les étiquettes sont toujours suggérées par le routeur en aval au routeur en amont **[web22]**.

Il y a quelques extensions faites à RSVP-TE dans le GMPLS **[web23]** :

1. Utilisation de la configuration LSP hiérarchique. RSVP-TE permet désormais d'établir des LSP hiérarchiques à différentes couches, par exemple Packet LSP, OTN LSP, Lambda LSP.
2. Configuration LSP bidirectionnelle. Alors que les LSP traditionnels dans MPLS étaient unidirectionnels. GMPLS permet la configuration de LSP bidirectionnels (LSP dans lesquels le trafic en amont et en aval suit la même route). Ceci est plus adapté au transport traditionnel comme la communication qui repose sur des chemins opposés bidirectionnels.
3. Suggestion d'étiquette en amont - GMPLS permet au nœud en amont de suggérer une étiquette au nœud en aval. Ceci est très approprié pour le monde du transport, par exemple, il n'est pas toujours possible de changer une longueur d'onde si une suggestion provient d'un nœud en aval.
4. Message de notification - Un nœud passant des connexions de transit doit avoir la capacité de NOTIFIER le nœud responsable de la restauration du trafic pour restaurer.

3.8.2 Extensions d'OSPF-TE

OSPF-TE a ajouté la possibilité de publier des informations sur la bande passante (disponibles et utilisées) dans la publicité standard utilisée par OSPF. D'autres ajouts dans les publicités ont été faits pour GMPLS. Ces ajouts sont destinés à rendre le protocole de routage plus adapté au monde du transport. Celles-ci incluent la capacité de commutation de liaison (par exemple, différentes capacités de commutation du nœud avec la bande passante prise en charge), la capacité de protection de nœud (par exemple, plusieurs routes de protection vers un nœud) et SRLG (groupe de liaison à risque partagé). Le groupe de liaison à risque partagé

contient des informations sur les routes logiques partageant les mêmes routes physiques qui peuvent constituer un point de défaillance unique **[web23].**

3.8.3 LMP (Link Management Protocole)

LMP, ou le protocole de gestion de liens, est un ensemble de procédures locales permettant de fournir certains services, notamment **[web20]** :

- **Gestion des canaux de contrôle (Control Channel Management) :** utilisée pour établir et maintenir les canaux de contrôle entre les nœuds, cette fonctionnalité utilise le protocole "Hello" pour détecter les problèmes et assurer la connectivité entre les nœuds adjacents. Cette procédure se compose de deux phases : une phase de négociation et une phase "keepalive".
- **Vérification de la connectivité des liens (Link Connectivity Verification) :** utilisée pour la vérification de la connectivité physique des liens de données, et aussi pour l'échange des identifiants de "Component Links".
- **Corrélation des propriétés des liens (Link Property Correlation) :** cette fonctionnalité permet d'échanger les propriétés d'un lien, de regrouper plusieurs "Component Links" en un seul "Bundled Link" ou d'ajouter un "Component Link" à un "Bundled Link". Elle permet également de modifier dynamiquement certaines caractéristiques du lien, telles que les mécanismes de protection ou les identifiants de ports.
- **Gestion d'incidents (Fault Management) :** cette fonctionnalité est essentielle d'un point de vue opérationnel et comprend la détection, la localisation et la notification des incidents. Lorsqu'un incident est détecté, l'opérateur doit être informé de sa localisation exacte pour prendre les mesures nécessaires.

3.8.4 LMP pour la protection et la restauration

La proposition d'utiliser LMP pour propager des informations de défaillance a été soumise au groupe de travail CCAMP. Deux nouveaux messages LMP, FaultNotify et FaultNotifyAck, ont été définis pour transporter des identifiants de liaisons défaillantes ou des ensembles d'identifiants SRLG (Shared Risk Link Group) ainsi que l'ID du nœud émetteur. Lorsqu'un nœud détecte une défaillance, il envoie un message FaultNotify à chaque voisin avec lequel il partage une adjacence LMP. Si le nœud récepteur possède déjà les informations sur les éléments défaillants, il ne transmet pas le message, sinon il transmet une copie du message FaultNotify à chacun de ses voisins et envoie un message FaultNotifyAck à l'expéditeur. Si un nœud reçoit un message FaultNotify et détermine qu'il est sur le chemin de récupération, il reconfigure sa matrice de commutation pour prendre en charge le chemin de récupération. Cependant, cela peut causer des problèmes potentiels tels que la redirection de trafic supplémentaire vers des

destinations non prévues. Le groupe de travail CCAMP discute de ces questions, ainsi que de la performance de cette approche par rapport au mécanisme de signalisation de défaillance canonique pour le GMPLS **[web24].**

3.9 Modèles GMPLS

3.9.1 Modèle Pair à Pair

Le modèle Pair à Pair est utilisé dans un système autonome unique avec une seule instance du protocole de routage IGP (Interior Gateway Protocol) pour distribuer et maintenir les informations d'état de liens. Les bases d'état de liens sont identiques pour les routeurs et les brasseurs, et le calcul du chemin pour l'établissement d'un circuit GMPLS en tenant compte toute la topologie du système. Le processus d'établissement de circuit commence avec une demande d'établissement de chemin, suivi de l'initiation d'un circuit GMPLS interconnectant les routeurs de bord locaux et distants en utilisant des circuits optiques secondaires comme liens virtuels **[web18].**

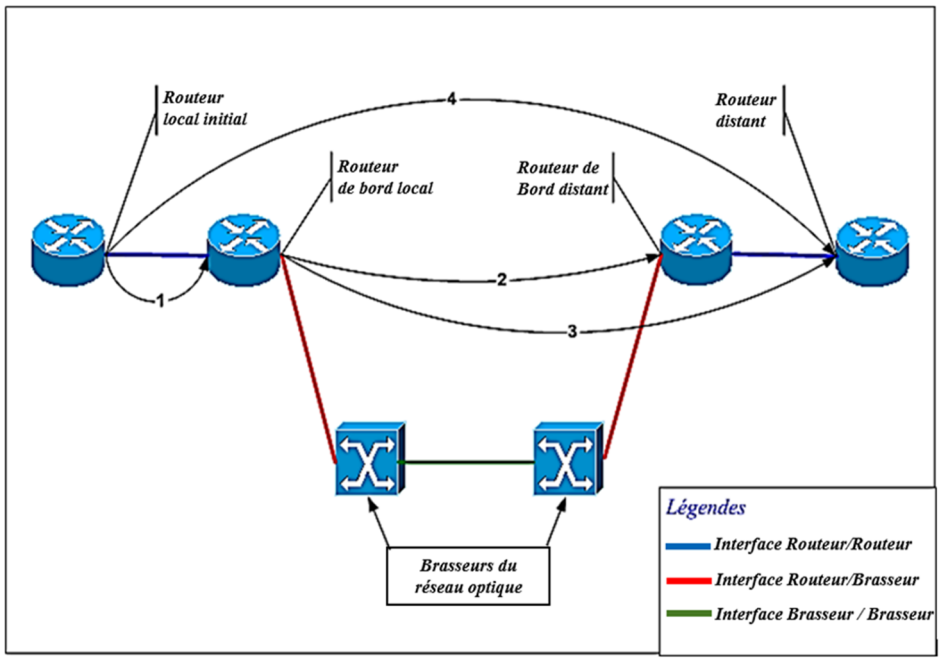

Figure 26 : Modèle Pair à Pair

3.9.2 Modèle Superposé

Le modèle Superposé GMPLS est une architecture de réseau qui permet à plusieurs réseaux de transport de travailler ensemble pour fournir des services aux utilisateurs. Chaque réseau conserve sa propre gestion de ressources et de routage, mais les informations de contrôle sont échangées entre les différents réseaux via des interfaces normalisées. Ce modèle est couramment utilisé dans les réseaux de télécommunications pour fournir des services à haut débit. Les avantages incluent une utilisation efficace des ressources, une évolutivité élevée et la capacité de fournir une qualité de service garantie pour différents types de trafic **[web18]**.

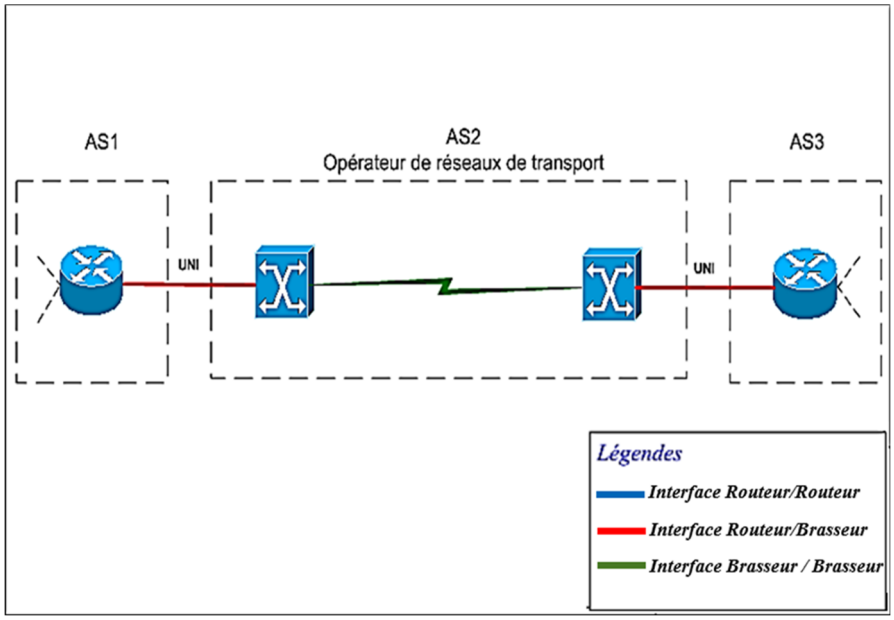

Figure 27 : Modèle Superposé

3.9.3 Modèle Amélioré

Modèle Amélioré GMPLS est un modèle d'interconnexion de réseaux de communication qui permet l'opération intégrée des réseaux IP et des réseaux de transport optiques. Il utilise le protocole de routage inter-domaine BGP pour transmettre les informations d'accessibilité entre les différents réseaux et le processus de signalisation GMPLS pour établir des circuits optiques. Ce modèle est particulièrement adapté pour les services d'interconnexion de bout en bout impliquant un premier fournisseur de services Internet, un opérateur de réseau optique longue distance et un second ISP distant. Modèle Amélioré GMPLS permet également à un même circuit optique de porter plusieurs chemins GMPLS de niveau paquet **[web18].**

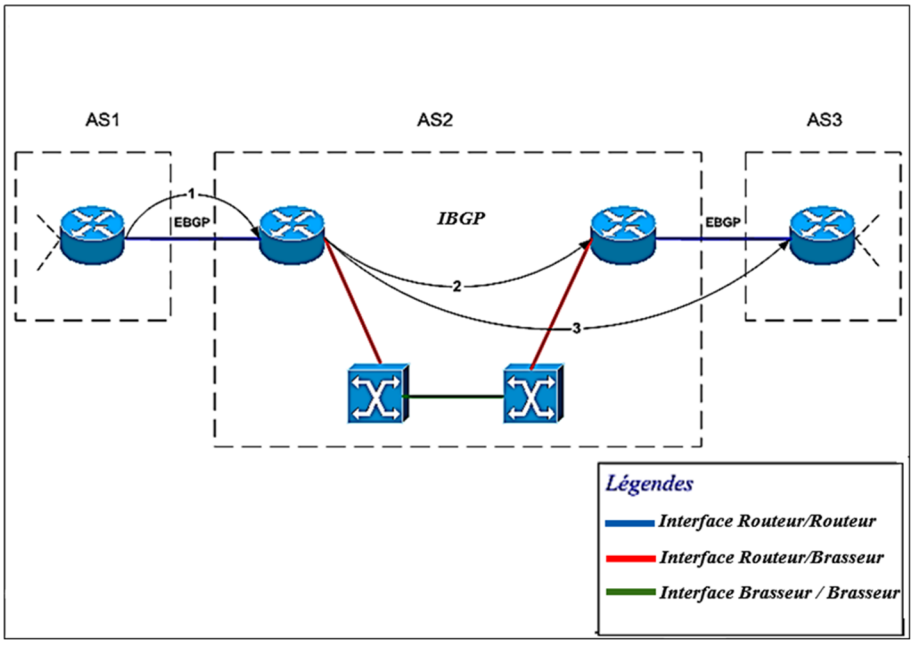

Figure 28 : Modèle Amélioré

4 MPLS vs GMPLS

Voici un tableau récapitulatif qui présente une comparaison entre MPLS et GMPLS pour différents critères.

Désignation de critères	MPLS	GMPLS
Protocoles exploités	- LDP (Label Distribution Protocol). - RSVP-TE (Resource ReSerVation Protocol -TE). - BGP (Border Gateway Protocol).	- RSVP-TE (pour la réservation de bande passante). - OSPF-TE (pour la distribution des étiquettes de commutation de lien). - LMP (Link Management Protocol pour la gestion des liens).
Bande passante	- RSVP-TE est utilisé pour réserver une quantité spécifique de bande passante.	- RSVP-TE et OSPF-TE sont utilisés pour réserver une quantité spécifique de bande passante. - Étend MPLS pour prendre en charge différents types de réseaux de communication.
État des liens	- Déterminé par OSPF ou IS-IS.	- Déterminé par OSPF-TE ou IS-IS-TE.
Signalisation	- Utilise les protocoles LDP et RSVP-TE.	- Utilise le protocole RSVP-TE.
Échange de données	- Les données sont encapsulées dans des paquets et acheminées via des chemins LSP établis à l'aide de protocoles de signalisation tels que LDP et RSVP-TE.	- Dans GMPLS, des adaptations spécifiques peuvent être nécessaires pour assurer une connectivité efficace entre différents types de réseaux de communication.
Types LSP	- Utilise : - LSP de base - LSP explicite - LSP de secours - LSP de point à multipoint - LSP de couche de liaison	- Utilise : - LSP de base - LSP explicite - LSP de secours - LSP de point à multipoint - LSP de couche de liaison
Domaine d'application	- Utilisé pour améliorer la performance et l'efficacité des réseaux IP.	- Extension de MPLS qui est conçue pour gérer les réseaux de transport optique.
Coût	- Le coût est lié à la mise en place de l'infrastructure de commutation et de routage. - Coûts d'entretien des équipements. - Les coûts de bande passante. - Les coûts de gestion de la QoS.	- Le coût est lié à la mise en place de l'infrastructure de transport optique. - Coûts d'entretien des équipements. - Les coûts de bande passante. - Les coûts de gestion de la QoS.
Bande passante	- RSVP-TE est utilisé pour réserver une quantité	- RSVP-TE et OSPF-TE sont utilisés pour réserver une quantité spécifique de bande passante.

	spécifique de bande passante.	- Étend MPLS pour prendre en charge différents types de réseaux de communication.
État des liens	- Déterminé par OSPF ou IS-IS.	- Déterminé par OSPF-TE ou IS-IS-TE.
Signalisation	- Utilise les protocoles LDP et RSVP-TE.	- Utilise le protocole RSVP-TE.
Échange de données	- Les données sont encapsulées dans des paquets et acheminées via des chemins LSP établis à l'aide de protocoles de signalisation tels que LDP et RSVP-TE.	- Dans GMPLS, des adaptations spécifiques peuvent être nécessaires pour assurer une connectivité efficace entre différents types de réseaux de communication.
Types LSP	Utilise : - LSP de base - LSP explicite - LSP de secours - LSP de point à multipoint - LSP de couche de liaison	Utilise : - LSP de base - LSP explicite - LSP de secours - LSP de point à multipoint - LSP de couche de liaison
Domaine d'application	- Utilisé pour améliorer la performance et l'efficacité des réseaux IP.	- Extension de MPLS qui est conçue pour gérer les réseaux de transport optique.
Coût	- Le coût est lié à la mise en place de l'infrastructure de commutation et de routage. - Coûts d'entretien des équipements. - Les coûts de bande passante. - Les coûts de gestion de la QoS.	- Le coût est lié à la mise en place de l'infrastructure de transport optique. - Coûts d'entretien des équipements. - Les coûts de bande passante. - Les coûts de gestion de la QoS.

Tableau 1 : Comparaison entre MPLS et GMPLS

Conclusion

Dans ce chapitre nous avons abordé les différentes fonctionnalités concernant les deux protocoles MPLS et GMPLS en tenant compte de leurs caractéristiques notamment les protocoles utilisés pour la gestion des liens, la réservation de la bande passante, l'ingénierie de trafic (TE), la signalisation, …etc. Ainsi que les différents mécanismes de la gestion du plan de contrôle. A la fin de ce chapitre nous avons présenté les différentes architectures pour le GMPLS dont la partie de simulation sera consacrée à ses modèles et nous avons terminé par une comparaison entre les deux protocoles.

Le chapitre suivant sera consacré à la gestion du plan de contrôle afin d'augmenter les performances du réseau et de diminuer les défaillances et les erreurs.

Chapitre III :
Plan de contrôle GMPLS

1 Introduction

Le développement des technologies de communication optique a permis une augmentation exponentielle de la capacité de transmission de données à travers les réseaux. Cependant, la gestion de ces réseaux de communication optique pose de nombreux défis, notamment la nécessité de fournir des services de qualité de service (QoS) et de gérer efficacement la bande passante disponible.

Le plan de contrôle GMPLS (Generalized Multi-Protocol Label Switching) est un protocole qui a été développé pour répondre à ces défis. Le GMPLS permet une gestion avancée de la bande passante et une fourniture de QoS améliorée en utilisant des étiquettes pour identifier les connexions et les services de communication. Le GMPLS est utilisé pour contrôler les réseaux de communication optique en fournissant des fonctions telles que la gestion de la topologie, la découverte de voisins, la création et la libération de connexions.

Dans ce chapitre, nous allons discuter des principaux concepts et des fonctionnalités du plan de contrôle GMPLS. Nous allons également explorer les différents types de messages et les protocoles utilisés pour contrôler les réseaux optiques.

2 Plan de contrôle GMPLS

Le plan de contrôle GMPLS joue un rôle important dans la gestion des ressources de réseau et l'établissement des connexions GMPLS. Il est essentiel pour la communication des informations de contrôle et pour la négociation des paramètres de connexion nécessaires pour établir une connexion GMPLS réussie.

L'IETF (The Internet Engineering Task Force) a chargé plusieurs groupes de travail de développer un plan de contrôle GMPLS ainsi que les protocoles nécessaires à son fonctionnement. Le travail de ces groupes a construit sur le travail précédent de l'IETF sur le MPLS (Multi-Protocol Label Switching), qui a été développé pour permettre aux routeurs de paquets de fonctionner plus efficacement.

Dans cette partie, nous décrivons alors ce plan de contrôle GMPLS qui est composé de trois fonctions principales : **la signalisation, le routage et la gestion des liens** GMPLS.

2.1 Signalisation GMPLS

L'architecture MPLS ne précise pas explicitement comment les étiquettes doivent être demandées et distribuées. Le mécanisme pour ce faire est laissé à l'opérateur de réseau, bien que l'IETF ait créé une architecture de signalisation pour le GMPLS **[11].**

L'ancêtre de MPLS développé par Cisco utilisait le protocole RSVP pour demander et distribuer des étiquettes. Il était donc naturel que RSVP soit proposé comme protocole standard pour la signalisation de la mise en place et du démontage des LSP dans le GMPLS. Des efforts

sont actuellement en cours pour standardiser le protocole qui étend le RSVP-TE, qui est un protocole de signalisation de MPLS qui a été étendu pour répondre aux besoins de GMPLS.

2.1.1 RSVP-TE (Resource ReSerVation Protocol-Traffic Engineering)

Est un protocole de signalisation de la couche transport utilisé pour établir des connexions de circuits dans les réseaux MPLS (Multi Protocol Label Switching). Dans le contexte de GMPLS, RSVP-TE a été étendu pour prendre en charge les exigences spécifiques des réseaux de transport optiques et de transport de paquets. La signalisation RSVP-TE permet à un nœud de réserver des ressources pour un chemin de commutation d'étiquettes prédéfini appelé LSP (Label Switched Path). Pour établir un LSP, la signalisation RSVP-TE envoie des messages de signalisation entre les nœuds de réseaux, pour négocier la bande passante requise et réserver les ressources nécessaires pour le LSP. Ces messages de signalisation comprennent des informations telles que l'adresse de destination, la bande passante requise, la priorité de la connexion, ...etc.

2.1.2 Fonctionnement de RSVP et RSVP-TE

Dans sa forme classique, RSVP supporte des réservations initiées par le récepteur pour les sessions multicast. Les applications avec des données à transmettre, appelées les émetteurs, annoncent leur état en envoyant des messages Path en aval vers un ou plusieurs récepteurs.

Au fur et à mesure que les messages Path traversent le réseau, ils établissent des informations d'état dans les routeurs compatibles RSVP qu'ils traversent. Ces informations comprennent généralement une spécification de trafic qui inclut les informations nécessaires pour prendre en charge les fonctions de qualité de service (par exemple, le débit de données maximal, la taille maximale de rafale, etc.). Ils contiennent également des informations permettant d'identifier l'émetteur qui a créé le message Path et le routeur immédiatement en amont (c'est-à-dire, vers l'émetteur) du routeur qui a reçu le message. Une fois qu'un message Path atteint sa destination, ce nœud peut commencer à envoyer des messages de réservation (Resv) en amont vers le nœud source d'origine. À mesure que le message Resv se propage vers l'émetteur, il incite les routeurs compatibles RSVP le long du trajet à réserver des ressources pour prendre en charge les caractéristiques de trafic qui sont annoncées dans le message Resv. Lorsque l'émetteur de la session reçoit un message Resv, il peut commencer à envoyer des données au récepteur **[12]**.

Lorsque le protocole MPLS (Multi Protocol Label Switching) était en cours de développement par le groupe de travail MPLS, RSVP a été étendu pour permettre la prise en charge de l'ingénierie de trafic (TE) en demandant et en distribuant des liaisons de libellé **[13]**.

Ces dernières sont utilisées pour prendre en charge la création de tunnels LSP, c'est-à-dire des LSP qui sont utilisés pour se faufiler en dessous d'un routage basé sur IP standard.

Après que l'TE est utilisée pour acheminer de tunnels LSP, le nœud sur le chemin après que le LSP ait été établi émet périodiquement le message Path ou le message RESV. Ce message Path ou RESV est également appelé "Message de rafraîchissement". L'état du LSP de chaque nœud est vérifié par ce message de rafraîchissement, et le LSP est maintenu. Si un certain nœud ne reçoit pas le message de rafraîchissement pour une raison quelconque, le nœud concerné considère qu'une erreur s'est produite et supprime l'état du LSP dans le nœud lui-même. En même temps, il émet un message d'erreur de chemin (Path ERROR) et un message de déconnexion de chemin (Path TEAR) vers les côtés amont et aval. Un nœud qui reçoit le message Path supprime l'état du LSP. Lorsque le nœud d'origine reçoit le message d'erreur, il émet le message Path TEAR vers le côté aval pour déconnecter le LSP.

RSVP-TE gère l'état du LSP selon le message de rafraîchissement à chaque nœud et déconnecte le LSP en fonction de l'état du réseau. Une telle méthode de gestion du LSP est appelée « management by soft state » **[14]**.

2.1.3 Signalisation de chemin bidirectionnelle

Dans un réseau MPLS, un LSP est un chemin à sens unique. Cependant, lorsque la communication est étendue dans un réseau GMPLS, la voie de longueur d'onde et la voie de fibre sont considérées comme des voies bidirectionnelles en principe, ce qui implique que la signalisation doit être étendue pour accueillir une voie bidirectionnelle. Pour étendre la signalisation unidirectionnelle à la signalisation bidirectionnelle, la solution la plus évidente serait simplement d'appliquer une signalisation unidirectionnelle différente dans chaque direction. Cependant, cette approche n'a pas été adoptée pour diverses raisons pratiques, notamment la durée de la mise en place, le doublement de la quantité de messages de signalisation, etc. Dans un réseau GMPLS, un chemin bidirectionnel est établi en faisant circuler la signalisation entre le nœud d'origine et le nœud de destination à l'aide des messages Path et RESV, tout comme dans la signalisation unidirectionnelle, en utilisant une étiquette en amont. La figure 29 exprime l'établissement d'une signalisation de chemin bidirectionnelle comme exemple. Dans la signalisation de chemin bidirectionnelle, le nœud qui émet le message Path est appelé un "initiateur", et le nœud qui émet le message RESV est appelé un "terminateur". Le LSP qui transfère des données du nœud d'origine au nœud de destination est appelé un "chemin aval", et inversement, le LSP qui transfère des données du nœud de destination au nœud d'origine est appelé un "chemin amont". Lors de la mise en place du chemin unidirectionnel, l'état du LSP est établi avec un message Path et la configuration de l'étiquette

est exécutée lorsqu'un message RESV est transmis. La configuration de l'étiquette pour le chemin aval dans un chemin bidirectionnel est exécutée lorsqu'un message RESV est transmis de la même manière que dans un chemin unidirectionnel. La configuration de la ligne pour le chemin amont est exécutée lorsque le message Path est transféré. Ceci est caractéristique de la configuration de l'étiquette dans le cas d'un chemin bidirectionnel.

En utilisant cette procédure de signalisation, il devient possible d'établir un chemin bidirectionnel en seulement un aller-retour du message Path et du message RESV **[14]**.

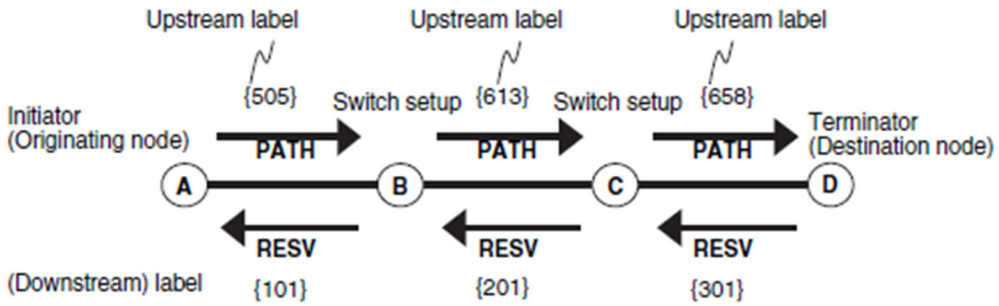

Figure 29 : Etiquette en amont

2.2 Routage GMPLS

Le routage est l'une des fonctions les plus importantes d'un système de gestion de réseau optique est de déterminer les ressources qui doivent être assignées pour prendre en charge un nouveau flux de trafic. GMPLS utilise le routage IP avec des extensions pour l'ingénierie de trafic (TE) afin d'effectuer cette fonction, en utilisant un routage contraint pour tenir compte des restrictions que la couche physique ou l'opérateur de réseau peut imposer. Par exemple, la diversité de routage pour les chemins qui partagent une ressource de protection commune.

Les protocoles de routage **Open Shortest Path First** (OSPF) et **Intermediate System-to-Intermediate System** (IS-IS) ont été étendus pour prendre en charge les fonctionnalités de routage GMPLS.

2.2.1 Extension OSPF

Dans un réseau GMPLS, l'OSPF utilisé dans le réseau IP est étendu **[15]**. Dans cette extension OSPF, des concepts tels que le lien d'ingénierie de trafic (TE), la hiérarchisation du LSP, les liens non numérotés, l'agrégation de liens et la LSA (annonce d'état de lien) ont été introduits **[16]**.

2.2.1.1 Ingénierie de trafic et la hiérarchisation de l'LSP

Dans un réseau GMPLS, un LSP de couche inférieure peut devenir un lien d'un LSP de couche supérieure, créant ainsi une hiérarchie. Par exemple, lorsqu'un LSP est établi sur un

chemin TDM, ce chemin devient un lien fixe dans le réseau. Lorsque le LSP de couche inférieure est établi, le nœud d'origine du LSP est annoncé en tant que lien de couche supérieure dans le réseau. Ce type de LSP est appelé un lien TE **[12]**.

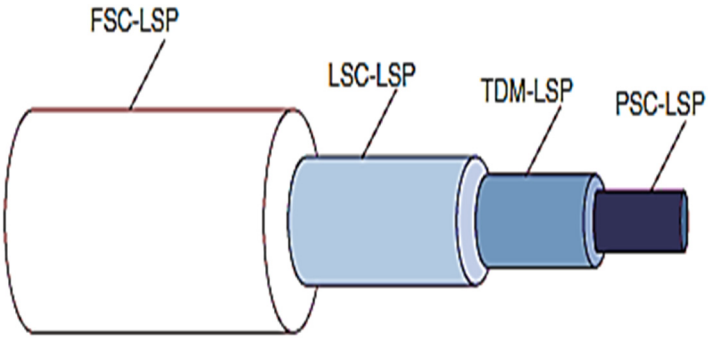

Figure 30 : Hiérarchisation des LSP

La figure 31 illustre le concept du lien TE. Un chemin TDM est représenté par une ligne en pointillés dans la figure 31(b). Alors qu'il existe un chemin direct entre A et C, il n'y en a pas entre B et C. Dans ce cas, le lien TE prend une topologie telle que celle présentée dans la figure 31(a). Le LSP TDM agit comme un lien TE entre le paquet et la couche TDM. Lorsque le LSP PSC est établi, la route est sélectionnée en se basant sur la topologie construite par les liens TE. Bien que le lien TE soit abstrait, il est utilisé pour l'ingénierie du trafic et la sélection de la route lors de l'établissement du LSP, en se référant simplement à la topologie sans tenir compte de la structure physique. En général, dans la topologie d'un réseau GMPLS, un lien physique, comme une fibre optique, est également considéré comme un lien TE, sans distinction entre les liens physiques et abstraits **[12]**.

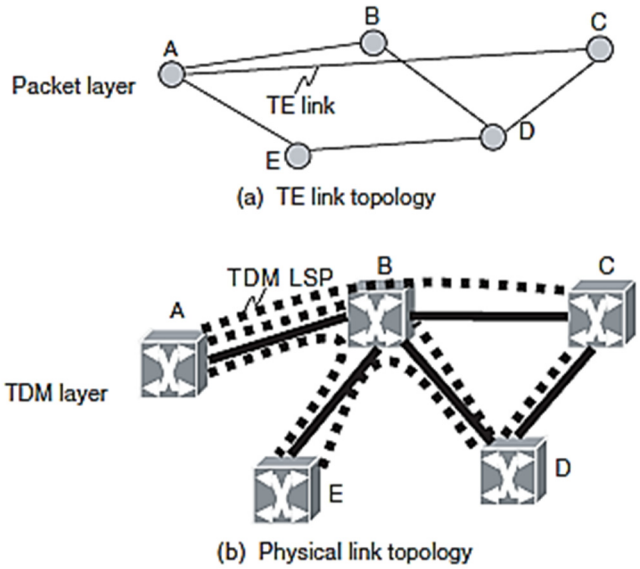

Figure 31 : Concept d'ingénierie de trafic

2.2.1.2 Lien non numéroté

L'interface d'un lien dans un réseau MPLS est généralement assignée à une adresse IP. Selon cette adresse IP, il est possible d'identifier le lien à l'intérieur du réseau. Cependant, dans un réseau GMPLS, étant donné qu'il est possible d'accueillir plus de 100 longueurs d'onde par fibre optique, le nombre d'adresses IP requis devient énorme si une adresse IP est assignée à chaque interface de ces longueurs d'onde. De plus, comme l'LSP de chaque couche est annoncée à la couche supérieure en tant que lien TE, l'approvisionnement en adresses IP peut être épuisé si une adresse IP est assignée à chaque lien TE. Par conséquent, dans GMPLS, pour identifier le lien, un identificateur de lien (ID de lien) qui est assigné à l'interface du lien a été introduit. Bien qu'une adresse IP doive encore être assignée globalement, cet ID de lien est bon s'il est unique juste à l'intérieur du routeur. Il est possible d'identifier le lien à l'intérieur du réseau à partir d'une combinaison de l'ID du routeur et de l'ID du lien. Un lien qui est exprimé par une combinaison de l'ID du routeur et de l'ID du lien est appelé un "lien non numéroté", ce qui signifie qu'une adresse IP n'est pas assignée à chaque interface du lien. Ainsi, dans GMPLS, si le nombre de longueurs d'onde ou de liens TE augmente, il n'y a pas de problème de pénurie d'adresses IP **[12]**.

2.2.1.3 Agrégation de liens

L'agrégation de liens, dont le but est d'abstraire plusieurs liens de même nature en les intégrant dans un seul lien TE. Les conditions du lien de même nature sont **[17]** :

* Les liens sont établis entre les mêmes nœuds ;
* Les liens sont du même type de lien (point-à-point/point-à-multipoints) ;
* Les liens sont dans le même métrique TE ;
* Les liens sont dans la même classe de ressources.

Le but du l'agrégation de liens est d'améliorer la scalabilité du routage en réduisant la quantité d'annonces d'états de lien par le protocole de routage. Le lien agrégé est composé de ressources individuelles. Bien que la quantité d'annonces puisse être réduite en intégrant et en abstrayant les liens multiples en un seul lien TE avec l'agrégation de liens, il peut arriver que des informations de ressources individuelles soient manquantes. Par exemple, la capacité vacante maximale d'un lien regroupé est définie sur la valeur maximale de la capacité vacante pour une ressource individuelle. Il y a un compromis entre l'effet de réduire la quantité d'annonce et la capacité de maintien des informations de ressources.

2.2.1.4 Annonce d'état de lien

Dans un réseau IP/MPLS, les états de liens entre routeurs sont annoncés à l'aide d'un LSA (Link State Advertisement) **[18]**. Alors pour annoncer l'état de lien d'un lien TE dans le réseau GMPLS, un LSA "opaque" est utilisé **[19]**.

LSA opaque est annoncé selon le format **TLV** (type, longueur, valeur) stockant des informations opaques. Il existe deux types de format TLV : un est un TLV de routeur qui exprime les informations du routeur, et l'autre est un TLV de lien qui exprime les informations du lien. Le TLV de lien a des sous-TLV en dessous de lui.

Dans l'extension OSPF de GMPLS, le sous-TLV du TLV de lien a été défini de : Type-1 à Type-9, neuf types de sous-TLV ont été des extensions pour l'ingénierie de trafic MPLS **[20]**. En plus de cela, il y a les ajouts suivants : Sous-TLV=11,14,15,16 en tant qu'extensions pour GMPLS **[16]**.

• **Sous-TLV=11** : Identificateur du nœud local / à distance de lien, est utilisé pour les liaisons non numérotées.

• **Sous-TLV=14** : Type de protection de lien, indique la fiabilité du lien : non protégé, protégé, type partagé, trafic supplémentaire, amélioré (plus fiable).

• **Sous-TLV=15** : Identifiant de capacité de commutation d'interface.

• **Sous-TLV=16** : Groupe de liens partageant le risque SRLG.

2.2.2 IS-IS-TE (Intermediate system to intermediate system-Traffic Engineering)

ISIS-TE sert exactement le même objectif qu'OSPF-TE. Le choix entre ISIS-TE et OSPF-TE dépend simplement du protocole de routage, IS-IS ou OSPF, utilisé dans le plan de contrôle. En théorie, on pourrait utiliser un protocole pour distribuer la portée IP et l'autre pour distribuer les informations TE, mais cela serait inhabituel car il n'y a pas de nécessité de faire fonctionner les deux protocoles.

Pour annoncer leurs informations au réseau, les haut-parleurs ISIS utilisent des unités de données de protocole d'état de liaison composées de plusieurs TLV. ISIS-TE définit deux nouveaux types de TLV : le TLV ID de routeur d'ingénierie de trafic et le TLV d'étendue IS de portée. Les deux nouveaux TLV contiennent les mêmes informations et sont utilisés à des fins identiques aux TLV OSPF-TE Router Address et Link TLV, respectivement.

GMPLS ISIS-TE introduit quelques nouveaux sous-TLV pour le TLV d'étendue IS de portée afin de rendre possible l'annonce d'attributs de lien TE tels que les identificateurs locaux et distants pour les liens TE non numérotés, les types de protection de lien, et les SRLG **[21]**.

2.3 Gestion des liens GMPLS

Pour cela il est utilisé le protocole de gestion de lien (Link Management Protocol en anglais, abrégé LMP), qui fournit un mécanisme pour gérer plusieurs canaux de contrôle entre des paires de nœuds GMPLS. Il prend en charge la découverte des voisins en permettant aux nœuds connectés de vérifier la connexion appropriée de leurs liens de données et de corréler les propriétés de ces liens. LMP peut également être utilisé pour prendre en charge la gestion des pannes, et joue donc un rôle dans la prise en charge des capacités de protection et de restauration dans les réseaux optiques GMPLS.

2.3.1 Opérations LMP

Le protocole de gestion de lien LMP a quatre opérations :

1 – La gestion des canaux de contrôle.

2 – La corrélation des propriétés des liens.

3 – La vérification de la connectivité des liens.

4 – La gestion des pannes.

2.3.1.1 Gestion des canaux de contrôle

Pour établir une adjacence LMP entre deux nœuds, il est nécessaire d'avoir un canal de contrôle bidirectionnel fonctionnel entre eux. Ce canal de contrôle, composé de deux connexions unidirectionnelles, permet aux nœuds de découvrir les adresses IP de destination pour chaque flux de trafic de contrôle unidirectionnel. Chaque point de terminaison du canal de contrôle a attribué un identificateur unique pour permettre la distinction entre plusieurs canaux de contrôle.

Quatre types de messages sont utilisés par LMP pour créer et maintenir les canaux de contrôle. Ce sont Config, ConfigAck, ConfigNack et Hello. Les trois premiers messages sont utilisés pour annoncer et négocier les paramètres du canal de contrôle. Le message Hello est utilisé pour prendre en charge une fonction de maintien de connexion rapide qui permet à LMP de répondre aux défaillances du canal de contrôle. La configuration du canal de contrôle commence par l'envoi d'un message Config qui contient l'ID du canal et des valeurs de paramètres suggérées pour le maintien rapide de l'état de lien. Si les valeurs sont acceptées, un message ConfigAck est renvoyé avec l'ID de canal du destinataire. En cas de valeurs inacceptables, un message ConfigNack est envoyé avec des valeurs de paramètres alternatives. Une fois qu'un message ConfigAck est reçu avec succès, le canal de contrôle est établi et les points de terminaison peuvent commencer à échanger des messages Hello.

LMP prend en charge la mise en veille progressive des canaux de contrôle. L'en-tête commun des messages LMP comprend un indicateur pour indiquer la désactivation en cours du

canal de contrôle. Lorsqu'un nœud reçoit un message LMP avec cet indicateur activé, il met le canal de contrôle unidirectionnel en état inactif et cesse d'envoyer des messages *Hello* **[22]**.

2.3.1.2 Corrélation des propriétés des liens

La corrélation des propriétés des liens est réalisée par l'échange de messages de résumé de liens (LinkSummary) sur le canal de contrôle, assurant la cohérence dans les attributions des liens TE entre les nœuds adjacents. Les liens TE et les liens de données peuvent être identifiés par des adresses IPv4 ou IPv6, ou être non numérotés, et sont également caractérisés par le type de commutation d'interface et la longueur d'onde transportée. Ces messages de résumé de liens (LinkSummary) sont également utilisés pour regrouper plusieurs liens de données en liens TE, ou pour modifier, échanger ou corréler les paramètres des liens TE ou des liens de données. Lorsque les correspondances des propriétés des liens sont conformes, le destinataire envoie un message d'accusé de réception de résumé de liens (Link Summary Ack), sinon un message de refus est envoyé (Link Summary Nack). En cas de refus, il est recommandé de procéder à une vérification des liens pour les correspondances signalées comme incorrectes **[22]**.

2.3.1.3 Vérification de la connectivité des liens

Le processus de vérification commence avec le message BeginVerify transmis sur le canal de contrôle, établissant les paramètres de la session de vérification tels que l'intervalle de temps entre les messages de test, le nombre de liens de données à tester, le mécanisme de transport des messages de test et le débit de ligne du lien de données utilisé. Les messages de test sont envoyés sur le lien de données en cours de test plutôt que sur les canaux de contrôle, et sont répétés jusqu'à recevoir un message TestStatusSuccess ou TestStatusFailure du nœud de destination. Les messages de réponse d'état du test sont également répétés périodiquement jusqu'à réception d'un accusé de réception ou jusqu'à atteindre le nombre maximum de retransmissions **[22]**.

2.3.1.4 Gestion des pannes

LMP (Link Management Protocol) permet de diffuser rapidement les informations sur les pannes ou les défaillances via les canaux de contrôle, facilitant ainsi les opérations de protection et de restauration. La détection des défaillances se fait au niveau des couches inférieures dans un réseau de commutateurs optiques transparents, par exemple, à travers une indication de perte de lumière (LOL). LMP utilise le message ChannelStatus pour propager les informations sur les défaillances, où chaque nœud détectant une défaillance transmet un message ChannelStatus à son nœud amont, qui répond avec un message ChannelStatusAck. Les nœuds récepteurs corréleront les informations pour déterminer si une défaillance peut être isolée, déclenchant ainsi des mécanismes de récupération via la signalisation **[22]**.

2.3.2 LMP pour la protection et la restauration

Le groupe de travail CCAMP a récemment proposé l'utilisation de LMP (Link Management Protocol) pour propager des informations sur les défaillances, en utilisant un mécanisme de diffusion similaire à celui d'OSPF. Ils ont introduit deux nouveaux messages LMP, FaultNotify (Notification de défaut) et FaultNotifyAck (Accusé de réception de notification de défaut). Lorsqu'un nœud détecte une défaillance, il envoie des messages FaultNotify à ses voisins LMP adjacents, contenant l'identifiant du lien défaillant ou un ensemble d'identifiants SRLG, ainsi que l'ID du nœud émetteur. Le nœud récepteur vérifie si les éléments défaillants sont déjà répertoriés dans sa base de données des entités réseau défaillantes. S'ils le sont, il ne transmet pas le message, sinon il le transmet à ses voisins et envoie un message FaultNotifyAck à l'émetteur **[22].**

3 Conclusion

Dans ce chapitre, nous avons discuté des principaux concepts et des fonctionnalités du plan de contrôle GMPLS tel que la signalisation, le routage et la gestion des liens. Nous avons également exploré les différents types de messages et les protocoles utilisés pour contrôler les réseaux optiques tel que : RSVP-TE, OSPF-TE et LMP.

Dans le chapitre suivant, nous discutons les résultats de notre simulation des réseaux GMPLS sur deux modèles, à savoir le modèle Pair à Pair et modèle Amélioré appliqués sur trois villes algériennes (Alger, Oran et Constantine).

Chapitre IV :
Simulations et résultats

1 Introduction

Ce chapitre vise à étudier et à simuler le plan de contrôle de réseau GMPLS pour évaluer ses performances et optimiser son déploiement. Nous allons examiner les protocoles de signalisation, de routage et de contrôle de la bande passante, ainsi que les équipements de transmission nécessaires pour mettre en œuvre le réseau GMPLS.

Nous allons utiliser des outils de simulation pour reproduire les conditions réelles du réseau et mesurer les performances en termes de temps de réponse, de disponibilité de la bande passante, et des délais de transmission. Nous allons également tester différents scénarios de trafic et de topologie de réseau pour déterminer les exigences en matière de ressources de transmission et d'optimisation les performances.

Dans ce chapitre, nous allons adopter deux architectures différentes à savoir, le modèle Pair à Pair et modèle Amélioré pour tester notre plan de contrôle du GMPLS avec une comparaison détaillée entre les deux modèles afin d'illustrer la meilleure tout en gardant une haute qualité de service QoS. Pour la 3ème architecture (Modèle Superposé), nous n'allons pas la simuler car cette dernière nécessite des interfaces très compliquées qui n'existent pas dans notre bibliothèque du logiciel GNS3 et même pour OPNET Modeler. Elles sont également à la fois très récentes et payantes. Nous allons juste citer des théories sur ce modèle avec son fonctionnement, et nous le proposerons dans les perspectives pour les futurs travaux.

2 Réalisation du réseau GMPLS

2.1 Simulateur du réseau GMPLS

Pour notre simulation nous avons utilisé le logiciel GNS3 version 2.2.38, installé sur un ordinateur personnel fonctionnant sur Windows 10. Nous avons choisi ce dernier parce qu'est un outil puissant et flexible pour la simulation des réseaux. Il permet aux utilisateurs de concevoir, tester et expérimenter des environnements réseaux virtuels à grande échelle de manière économique, sûre et efficace.

Pour simuler notre réseau GMPLS à l'aide du GNS3, nous avons utilisé des images de routeurs de type CISCO C7200 avec la version IOS 12.4-25g.

Pour connecter nos routeurs, nous avons utilisé des liens POS comme lien de fibre optique. Les liens POS sont des liens séries utilisés pour connecter des équipements réseaux prenant en charge le protocole SONET, qui est utilisé dans les réseaux de transport à haute vitesse tels que les réseaux de fibre optique en encapsulant les paquets de données dans des trames SONET.

Pour simuler un réseau GMPLS nous avons utilisé GNS3. Ce dernier nous a permis de tester différents scénarios de déploiement et vérifier la qualité de service (QoS).

2.2 Architecture du réseau GMPLS

La topologie GMPLS utilisée dans notre simulation (Figure 32) comprend trois villes algériennes comme équipements terminaux CE (Customer Edge) : Alger, Oran et Constantine. Les équipements de bordure de réseau PE (Provider Edge) sont au nombre de trois et sont placés stratégiquement pour permettre la communication entre les équipements terminaux. Les nœuds de commutation de réseau P (Provider) sont au nombre de sept et sont situés sur la trajectoire des données entre les équipements terminaux.

L'objectif de cette topologie GMPLS est de fournir des services de transport de données pour les utilisateurs situés dans les villes d'Alger, d'Oran et de Constantine. Les équipements terminaux CE (Customer Edge) sont connectés aux équipements de bordure de réseau PE (Provider Edge) via des liens à haut débit, tandis que les nœuds de commutation de réseau P (Provider) sont utilisés pour rediriger les paquets de données en fonction des besoins de la QoS.

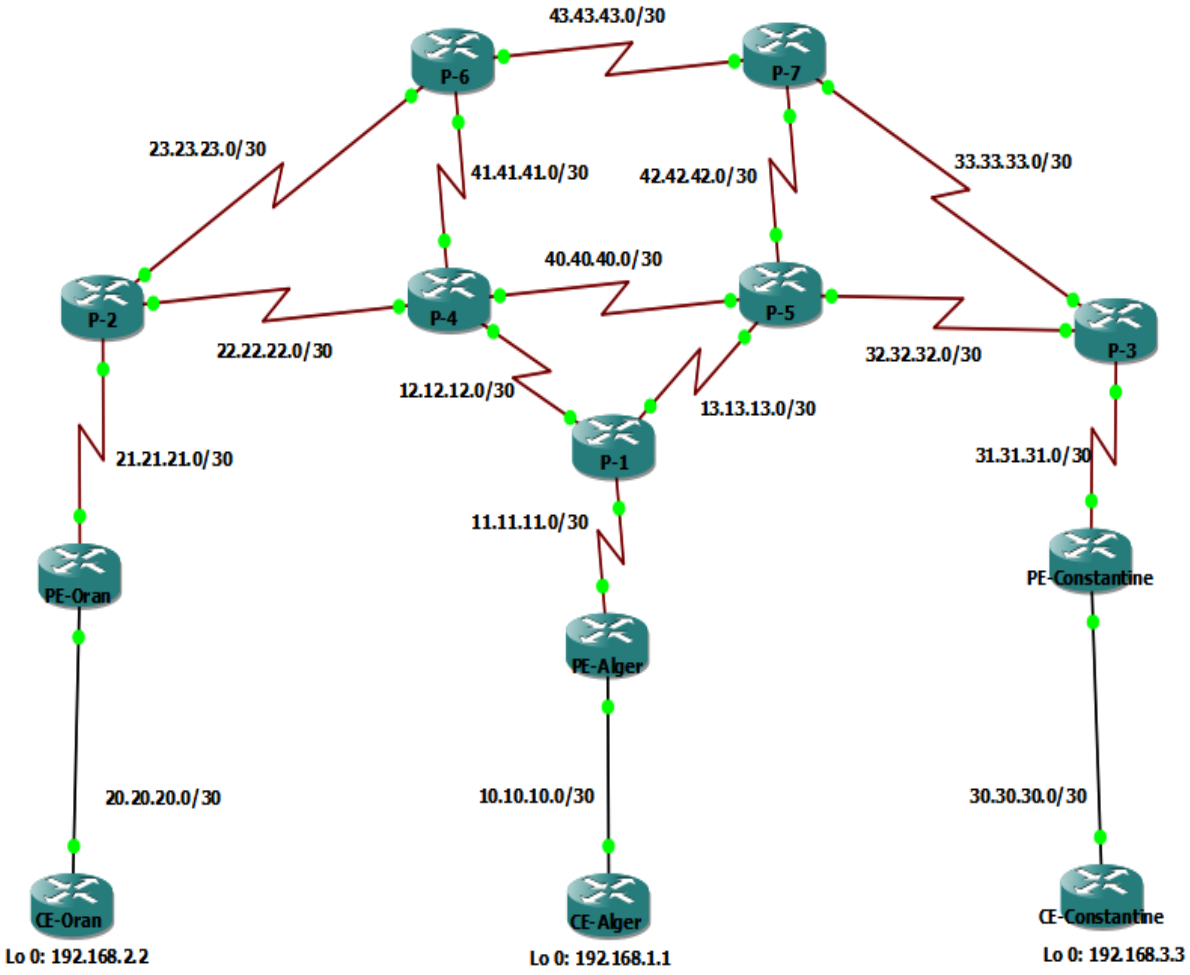

Figure 32 : Architecture réseau GMPLS

2.3 Table d'adressage

L'adressage est un mécanisme essentiel dans les réseaux informatiques, permettant l'identification et la communication entre les appareils connectés. Les adresses IP et MAC sont les principaux types d'adressage utilisés, assurant un acheminement efficace des données au sein du réseau.

Le tableau qui suit nous indique les adresses IP attribuées aux interfaces de chaque routeur.

Équipement	**Interface**	**Adresse IPv4**	**Destination**
CE-Alger	Fast Ethernet 0/0	10.10.10.1/30	PE-Alger
	Loopback 0	192.168.1.1/32	
CE-Oran	Fast Ethernet 0/0	20.20.20.1/30	PE-Oran
	Loopback 0	192.168.2.2/32	
CE-Constantine	Fast Ethernet 0/0	30.30.30.1/30	PE-Constantine
	Loopback 0	192.168.3.3/32	
PE-Alger	Fast Ethernet 0/0	10.10.10.2/30	CE-Alger
	Pos1/0	11.11.11.1/30	P-1
	Loopback 0	1.1.1.1/32	
PE-Oran	Fast Ethernet 0/0	20.20.20.2/30	CE-Oran
	Pos1/0	21.21.21.1/30	P-2
	Loopback 0	2.2.2.2/32	
PE-Constantine	Fast Ethernet 0/0	30.30.30.2/30	CE-Constantine
	Pos1/0	31.31.31.1/30	P-3
	Loopback 0	3.3.3.3/32	
P-1	Pos1/0	11.11.11.2/30	P-4
	Pos2/0	12.12.12.1/30	PE-Alger
	Pos3/0	13.13.13.1/30	P-5
	Loopback 0	4.4.4.1/32	
P-2	Pos1/0	21.21.21.2/30	PE-Oran
	Pos2/0	22.22.22.1/30	P-4
	Pos3/0	23.23.23.1/30	P-6
	Loopback 0	4.4.4.2/32	

P-3	Pos1/0	31.31.31.2/30	PE-Constantine
	Pos2/0	32.32.32.1/30	PE-5
	Pos3/0	33.33.33.1/30	PE-7
	Loopback 0	4.4.4.3/32	
P-4	Pos1/0	41.41.41.1/30	P-6
	Pos2/0	22.22.22.2/30	P-2
	Pos3/0	12.12.12.2/30	P-1
	Pos4/0	40.40.40.1/30	P-5
	Loopback 0	4.4.4.4/32	
P-5	Pos1/0	42.42.42.1/30	P-7
	Pos2/0	32.32.32.2/30	P-3
	Pos3/0	13.13.13.2/30	P-1
	Pos4/0	40.40.40.2/30	P-4
	Loopback 0	4.4.4.5/32	
P-6	Pos1/0	43.43.43.1/30	P-7
	Pos2/0	41.41.41.2/30	P-4
	Pos3/0	23.23.23.2/30	P-2
	Loopback 0	4.4.4.6/32	
P-7	Pos1/0	43.43.43.2/30	P-6
	Pos2/0	42.42.42.2/30	P-5
	Pos3/0	33.33.33.2/30	P-3
	Loopback 0	4.4.4.7/32	

Tableau 2 : Table d’adressage

3 Le Plan de contrôle GMPLS

3.1 Modèle Pair à Pair

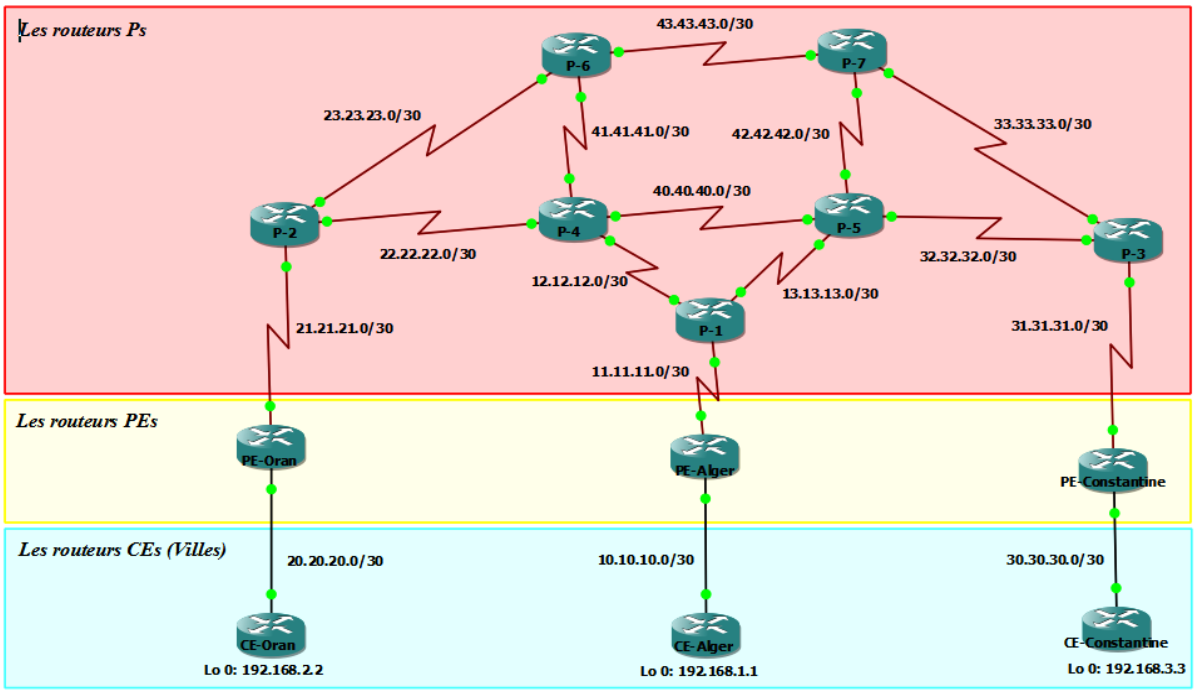

Figure 33 : Architecture modèle Pair à Pair

L'architecture modèle Pair à Pair est devenue de plus en plus populaire dans les réseaux de télécommunication en raison de sa grande évolutivité, de sa flexibilité et de sa fiabilité. Cette architecture permet à des nœuds de réseaux égaux de communiquer directement entre eux pour établir des connexions d'étiquettes commutées. Nous avons configuré des nœuds dans le réseau pour utiliser le modèle Pair à pair, et observer comment les nœuds communiquent directement les uns avec les autres pour établir des connexions d'étiquettes commutées.

3.1.1 Configuration modèle Pair à Pair

a. Configuration routage RIP dans les CE's

CE-Alger

```
router rip
version 2
network 192.168.1.1
network 10.10.10.0
```

CE-Oran

```
router rip
version 2
network 192.168.2.2
network 20.20.20.0
```

CE-Constantine

```
router rip
version 2
network 192.168.3.3
network 30.30.30.0
```

b. Configuration routage RIP dans les PE's et la redistribution OSPF

PE-Alger

```
router rip
version 2
network 10.10.10.0
network 1.1.1.1
redistribute ospf 1 metric 1
```

PE-Oran

```
router rip
version 2
network 20.20.20.0
network 2.2.2.2
redistribute ospf 2 metric 1
```

PE-Constantine

```
router rip
version 2
network 30.30.30.0
network 3.3.3.3
redistribute ospf 3 metric 1
```

c. Configuration routage OSPF dans les PE's et la redistribution RIP

PE-Alger

```
router ospf 1
network 1.1.1.1 0.0.0.0 area 0
network 11.11.11.0 0.0.0.3 area 0
network 10.10.10.0 0.0.0.3 area 0
redistribute rip metric 1 subnets
```

PE-Oran

```
router ospf 1
network 2.2.2.2 0.0.0.255 area 0
network 21.21.21.0 0.0.0.255 area 0
network 20.20.20.0 0.0.0.255 area 0
redistribute rip metric 1 subnets
```

PE-Constantine

```
router ospf 1
network 3.3.3.3 0.0.0.0 area 0
network 31.31.31.0 0.0.0.3 area 0
network 30.30.30.0 0.0.0.3 area 0
redistribute rip metric 1 subnets
```

d. Configuration routage OSPF dans les P's

P-1

```
router ospf 1
no network 4.4.4.2 0.0.0.0 area 0
network 4.4.4.1 0.0.0.0 area 0
network 11.11.11.0 0.0.0.3 area 0
network 12.12.12.0 0.0.0.3 area 0
network 13.13.13.0 0.0.0.3 area 0
```

P-2

```
router ospf 1
network 4.4.4.2 0.0.0.0 area 0
network 21.21.21.0 0.0.0.3 area 0
network 22.22.22.0 0.0.0.3 area 0
network 23.23.23.0 0.0.0.3 area 0
```

P-3

```
router ospf 1
network 4.4.4.3 0.0.0.0 area 0
network 31.31.31.0 0.0.0.3 area 0
network 32.32.32.0 0.0.0.3 area 0
network 33.33.33.0 0.0.0.3 area 0
```

P-4

```
router ospf 1
network 4.4.4.5 0.0.0.0 area 0
network 12.12.12.0 0.0.0.3 area 0
network 22.22.22.0 0.0.0.3 area 0
network 40.40.40.0 0.0.0.3 area 0
network 41.41.41.0 0.0.0.3 area 0
```

P-5

```
router ospf 1
network 4.4.4.4 0.0.0.0 area 0
network 13.13.13.0 0.0.0.3 area 0
network 32.32.32.0 0.0.0.3 area 0
network 40.40.40.0 0.0.0.3 area 0
network 42.42.42.0 0.0.0.3 area 0
```

P-6

```
router ospf 1
network 4.4.4.6 0.0.0.0 area 0
network 23.23.23.0 0.0.0.3 area 0
network 41.41.41.0 0.0.0.3 area 0
network 43.43.43.0 0.0.0.3 area 0
```

P-7

```
router ospf 1
network 4.4.4.7 0.0.0.0 area 0
network 33.33.33.0 0.0.0.3 area 0
network 42.42.42.0 0.0.0.3 area 0
network 43.43.43.0 0.0.0.3 area 0
```

e. Configuration BGP

PE-Alger

```
router bgp 1
neighbor 2.2.2.2 remote-as 1
neighbor 2.2.2.2 update-source loopback 0
address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community both
exit
router bgp 1
neighbor 3.3.3.3 remote-as 1
neighbor 3.3.3.3 update-source loopback 0
address-family vpnv4
neighbor 3.3.3.3 activate
neighbor 3.3.3.3 send-community both
```

PE-Oran

```
router bgp 1
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 update-source loopback 0
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 send-community both
exit
router bgp 1
neighbor 3.3.3.3 remote-as 1
neighbor 3.3.3.3 update-source loopback 0
address-family vpnv4
neighbor 3.3.3.3 activate
neighbor 3.3.3.3 send-community both
```

PE-Constantine

```
router bgp 1
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 update-source loopback 0
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 send-community both
exit
router bgp 1
neighbor 2.2.2.2 remote-as 1
neighbor 2.2.2.2 update-source loopback 0
address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community both
```

f. Configuration VRF (Virtual routing and forwarding)

PE-Alger

```
ip vrf NET12
int fa 0/0
no ip address
ip vrf forwarding NET12
ip address 10.10.10.2 255.255.255.252
no shutdown
exit
router rip
version 2
address-family ipv4 vrf NET12
network 10.10.10.0
network 192.168.1.1
```

PE-Oran

```
ip vrf NET12
int fa 0/0
no ip address
ip vrf forwarding NET12
ip address 20.20.20.2 255.255.255.252
no shutdown
exit
router rip
version 2
address-family ipv4 vrf NET12
network 20.20.20.0
network 192.168.2.2
```

PE-Constantine

```
ip vrf NET12
int fa 0/0
no ip address
ip vrf forwarding NET12
ip address 30.30.30.2 255.255.255.252
no shutdown
exit
router rip
version 2
address-family ipv4 vrf NET12
network 30.30.30.0
network 192.168.3.3
```

g. Configuration Traffic Engineering

PE-Alger, PE-Oran, PE-Constantine

```
conf ter
mpls traffic-eng tunnel
router ospf 1
mpls traffic-eng router-id loopback 0
mpls traffic-eng area 0
interface range pos1/0
mpls traffic-eng tunnels
ip rsvp bandwidth 1024000
```

P-1, P-2, P-3, P-6, P-7

```
conf ter
mpls traffic-eng tunnel
router ospf 1
mpls traffic-eng router-id loopback 0
mpls traffic-eng area 0
interface range pos1/0 , pos2/0 , pos3/0
mpls traffic-eng tunnels
ip rsvp bandwidth 1024000
```

P-4, P-5

```
conf ter
mpls traffic-eng tunnel
router ospf 1
mpls traffic-eng router-id loopback 0
mpls traffic-eng area 0
interface range pos1/0 , pos2/0 , pos3/0, Pos4/0
mpls traffic-eng tunnels
ip rsvp bandwidth 1024000
```

h. Configuration Routage Explicite

PE-Oran

```
ip explicit-path name OR-AL-1 enable
next-address 21.21.21.2
next-address 23.23.23.2
next-address 43.43.43.2
next-address 42.42.42.1
next-address 13.13.13.1
next-address 11.11.11.1
exit
ip explicit-path name OR-CO-1 enable
next-address 21.21.21.2
next-address 23.23.23.2
next-address 43.43.43.2
next-address 33.33.33.1
next-address 31.31.31.1
```

PE- Constantine

```
ip explicit-path name CO-AL-1 enable
next-address 31.31.31.2
next-address 33.33.33.2
next-address 42.42.42.1
next-address 13.13.13.1
next-address 11.11.11.1
exit
ip explicit-path name CO-AL-2 enable
next-address 31.31.31.2
next-address 33.33.33.2
next-address 43.43.43.1
next-address 41.41.41.1
next-address 12.12.12.1
next-address 11.11.11.1
```

i. Configuration Tunnels

PE-Alger

```
interface tunnel 12
ip unnumbered loopback 0
mpls ip
tunnel destination 2.2.2.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 0 0
tunnel mpls traffic-eng bandwidth 1024000
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 dynamic
interface tunnel 13
ip unnumbered loopback 0
mpls ip
tunnel destination 3.3.3.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 0 0
tunnel mpls traffic-eng bandwidth 1024000
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 dynamic
```

PE-Oran

```
interface tunnel 21
ip unnumbered loopback 0
mpls ip
tunnel destination 1.1.1.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 0 0
tunnel mpls traffic-eng bandwidth 1024000
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 explicit name OR-AL-1
interface tunnel 31
ip unnumbered loopback 0
mpls ip
tunnel destination 3.3.3.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 0 0
tunnel mpls traffic-eng bandwidth 1024000
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 2 explicit name OR-CO-1
```

PE- Constantine

```
interface tunnel 13
ip unnumbered loopback 0
mpls ip
tunnel destination 1.1.1.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 0 0
tunnel mpls traffic-eng bandwidth 1024000
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 explicit name CO-AL-1
interface tunnel 31
ip unnumbered loopback 0
mpls ip
tunnel destination 1.1.1.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng bandwidth 1024000
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 explicit name CO-AL-2
```

3.1.2 Découverte des voisins

Dans le GMPLS, tous les équipements du réseau doivent être connus et configurés pour pouvoir fonctionner correctement. Dans notre simulation les nœuds utilisés sont des routeurs.

Nous allons prendre l'exemple des deux routeurs (PE-Alger, P-4) un routeur de chaque niveau. Avec les voisins du nœud PE-Alger (Figure 34) sont P-1 avec LDP Ident : 4.4.4.1.

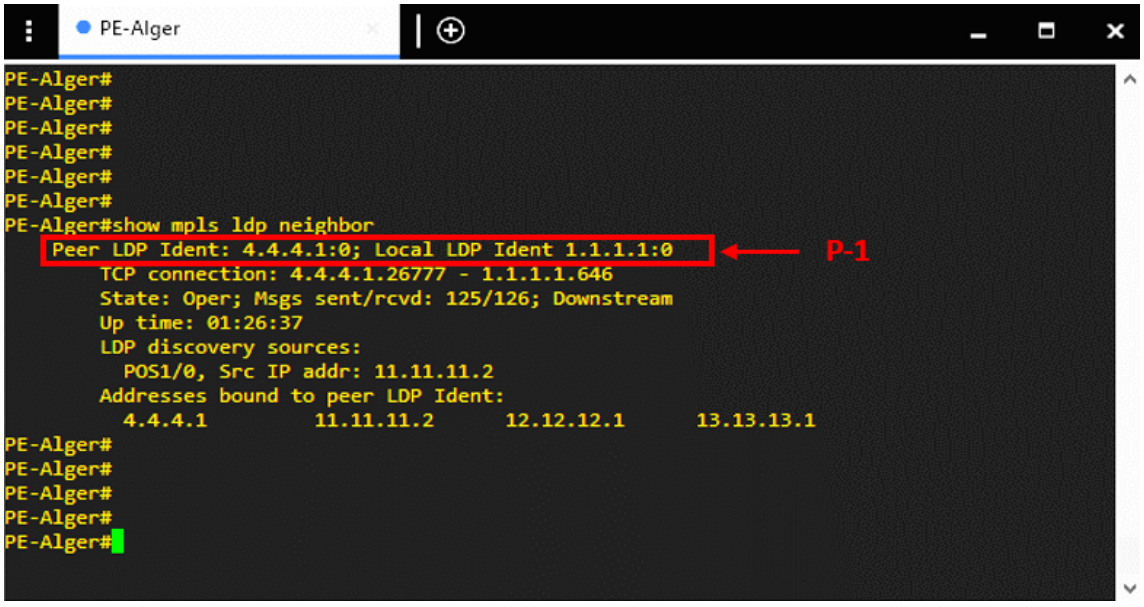

Figure 34 : Découverte des voisins pour le routeur PE-Alger dans modèle Pair à Pair

Cependant avec le routeur P-4 (Figure 35) les voisins découverts sont P-1, P-2, P-5 et P-6 avec les LDPs Ident respective 4.4.4.1, 4.4.4.2, 4.4.4.5 et 4.4.4.6.

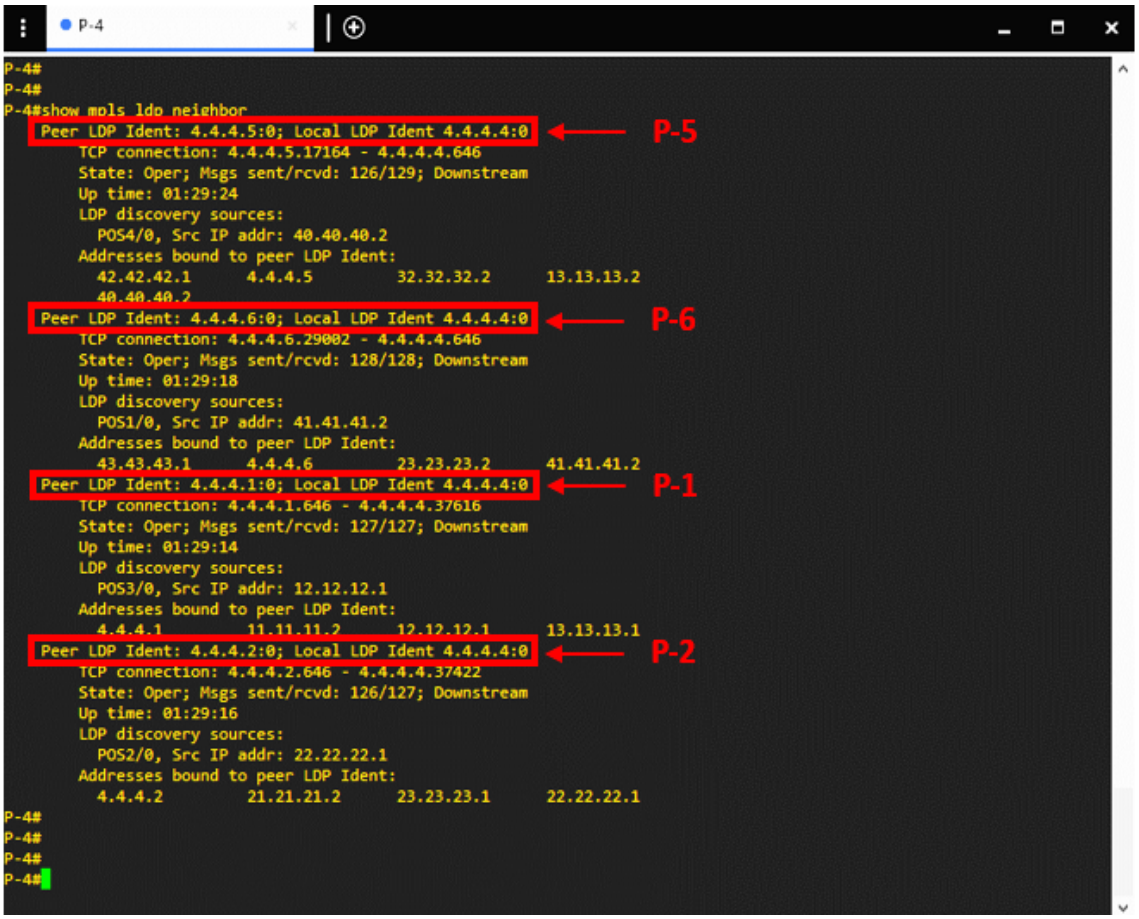

Figure 35 : Découverte des voisins pour le routeur P-4 dans le modèle Pair à Pair

3.1.3 Propagation des états de lien

La propagation des états de lien dans le GMPLS est un processus critique qui permet aux nœuds du réseau de détecter et de signaler rapidement les changements d'état de lien, pour permettre une mise à jour dynamique des tables de routage et de connexion d'étiquettes commutées. Pour ce processus nous avons utilisé le protocoles OSPF *(Open Shortest Path First)*.

Nous prenons comme exemple le routeur PE-Oran (Figure 36), nous constatons que le routeur a dans sa table de routage tous les liens OSPF de la topologie, les routeurs de la topologie utilisent les mises à jour périodiques pour échanger des informations d'état de lien entre les routeurs.

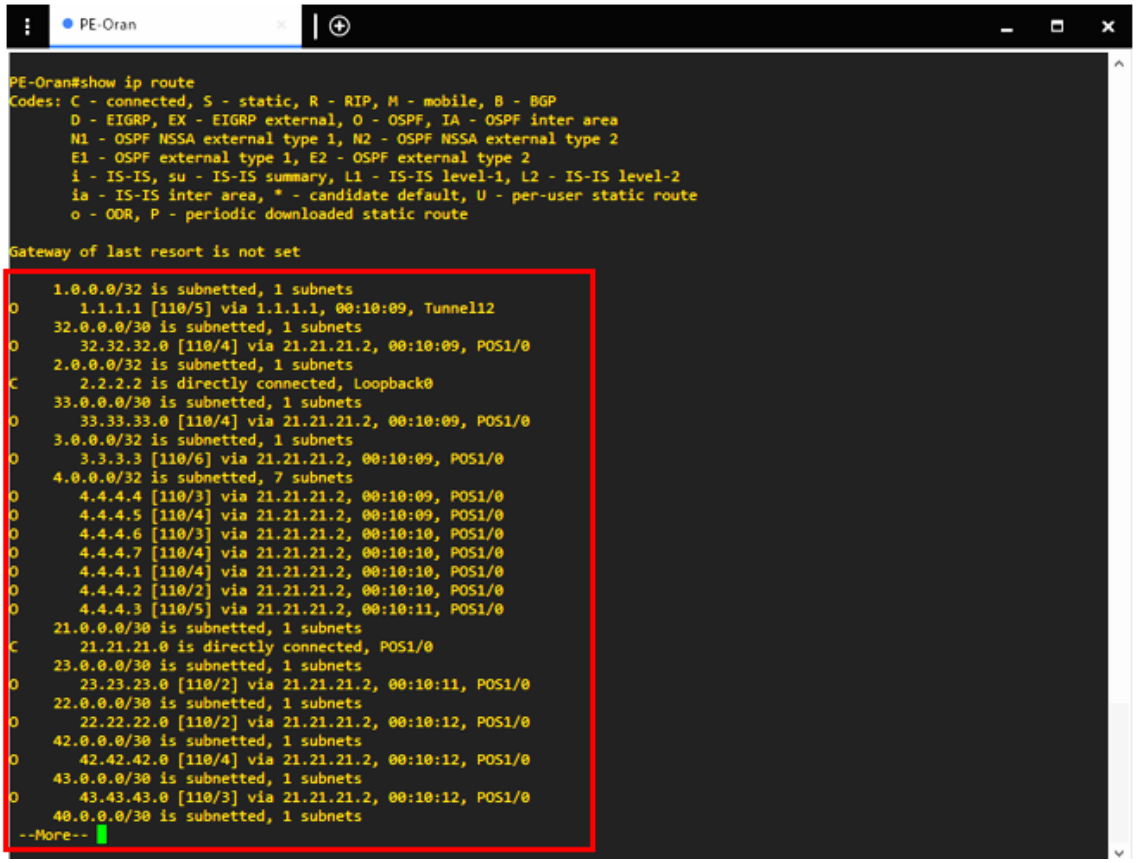

Figure 36 : Propagation des états de lien PE-Oran dans le modèle Pair à Pair

3.1.4 Gestion de l'état des liens

La gestion de l'état des liens dans le GMPLS est un processus critique qui permet de maintenir un état précis des connexions de réseau dans un environnement MPLS. Dans le GMPLS, il existe plusieurs protocoles de gestion d'état de lien, parmi eux l'OSPF.

Nous avons configuré pour le routeur PE-Oran deux routes vers le routeur PE-Alger : le premier routage est explicit et le deuxième dynamique.

Pour le routage explicit nous avons configuré une route bien précise passons par les routeurs P2, P6, P7, P5 et P1 pour atteindre le routeur PE-Alger (Figure 37). Le chemin est indiqué avec la flèche verte dans la Figure 39.

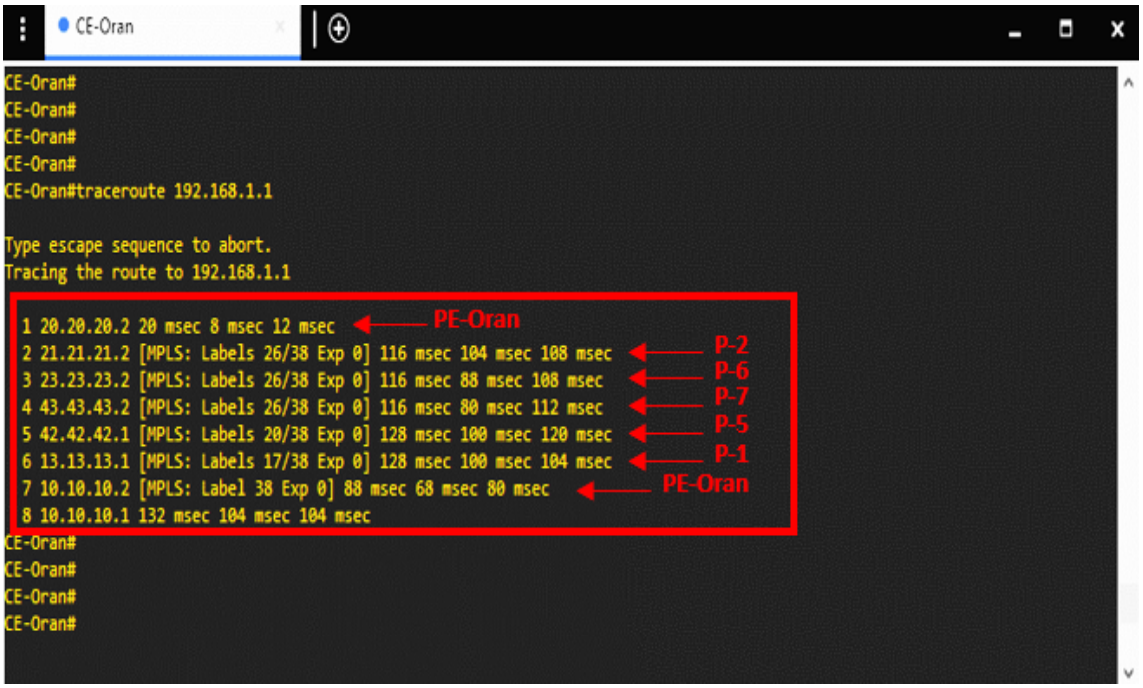

Figure 37 : Gestion de l'état des liens CE-Oran dans le modèle Pair à Pair avec un routage explicite

En cas d'arrêt d'un lien dans la route explicite, c'est le routage dynamique qui va prendre la relève pour calculer une nouvelle route vers la destination (Figure 38). Le chemin est t'indiqué avec la flèche bleue dans la Figure 39.

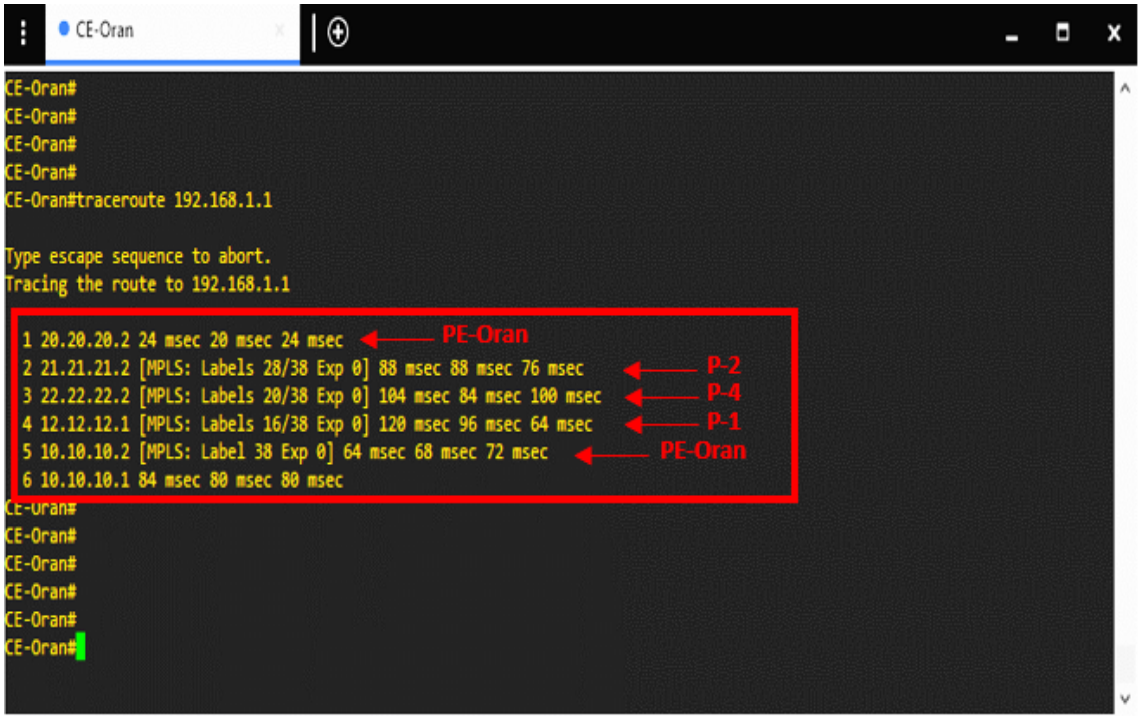

Figure 38 : Gestion de l'état des liens CE-Oran dans le modèle Pair à Pair avec un routage dynamique

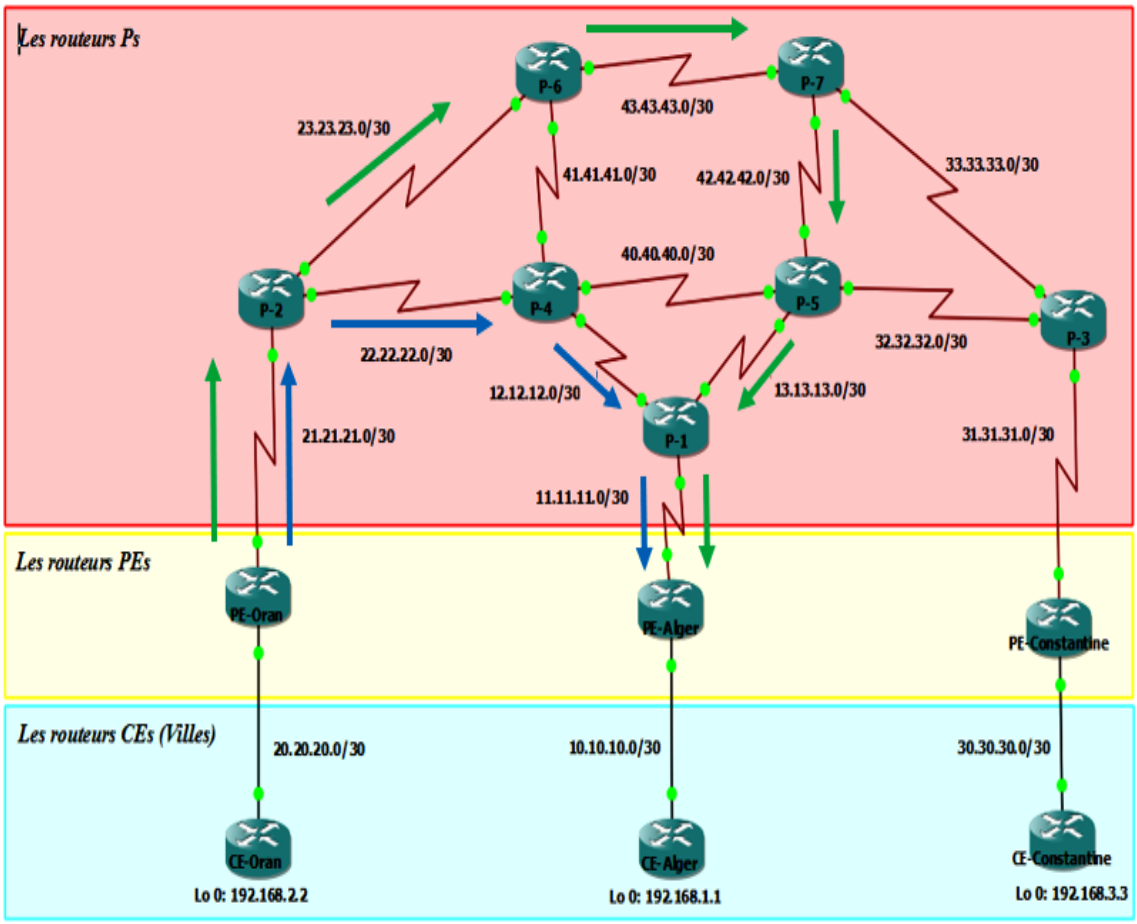

Figure 39 : Gestion de l'état des liens CE-Oran dans le modèle Pair à Pair avec un routage explicite et dynamique

3.1.5 Contrôle et gestion des routes

Dans cette simulation, nous avons utilisé RSVP-TE *(Ressource ReSerVation Protocol-Traffic Engineering)* pour réserver la bande passante. Nous avons fixé une limite de bande passante totale de 4 Go, ce qui signifie que la somme des débits de toutes les connexions actives ne peut pas dépasser cette valeur. De plus, nous avons limiter la bande passante par flux à 1 Go, ce qui signifie que chaque connexion ne peut pas utiliser plus de cette quantité de bande passante (Figure 40).

En utilisant RSVP-TE pour la réservation de la bande passante, nous pouvons garantir des performances QoS fiables pour les applications critiques, même dans des environnements de réseau à forte demande. Le protocole RSVP-TE gère et contrôle efficacement la bande passante, en allouant les ressources nécessaires pour chaque connexion de manière à éviter la congestion et les perturbations dans le réseau.

Figure 40 : Contrôle et gestion des routes pour le routeur PE-Alger dans le modèle Pair à Pair

3.1.6 Gestion des liens

Dans le modèle Pair à pair de GMPLS, la gestion des liens est assurée par les équipements de réseau eux-mêmes, qui communiquent directement entre eux pour établir des connexions de bout en bout à travers le réseau en utilisant des protocoles de signalisation tels que RSVP-TE.

En affichant la table forwarding à l'aide de la commande : **mpls forwarding-table**. Donc nous constatons une connectivité fiable entre les nœuds en attribuant les labels (Figure 41).

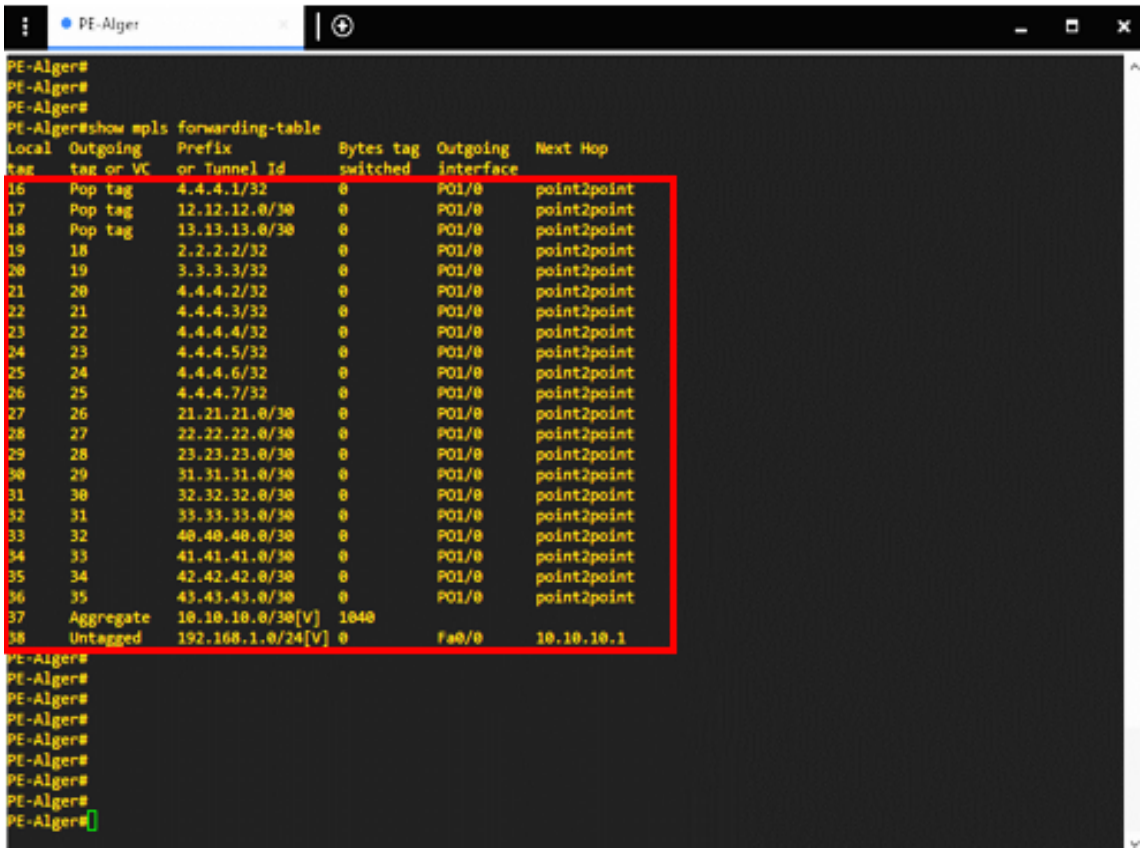

Figure 41 : Chemins empruntés dans le routeur PE-Alger dans le modèle Pair à Pair

3.1.7 Protection des liens

Pour la protection des liens, il y a plusieurs techniques, nous avons choisi la protection par commutation rapide, cette technique consiste à créer plusieurs chemins de transmission possibles pour les données, et à commuter rapidement entre ces chemins en cas de panne ou de défaillance.

Dans notre simulation la protection par commutation rapide nous l'avons appliquer au niveau du routeur PE-Oran en créant un tunnel nommé 21 entre le PE-Oran et le routeur PE-Alger avec routage explicit en définissant un chemin bien définit pour ce tunnel (Figure 42).

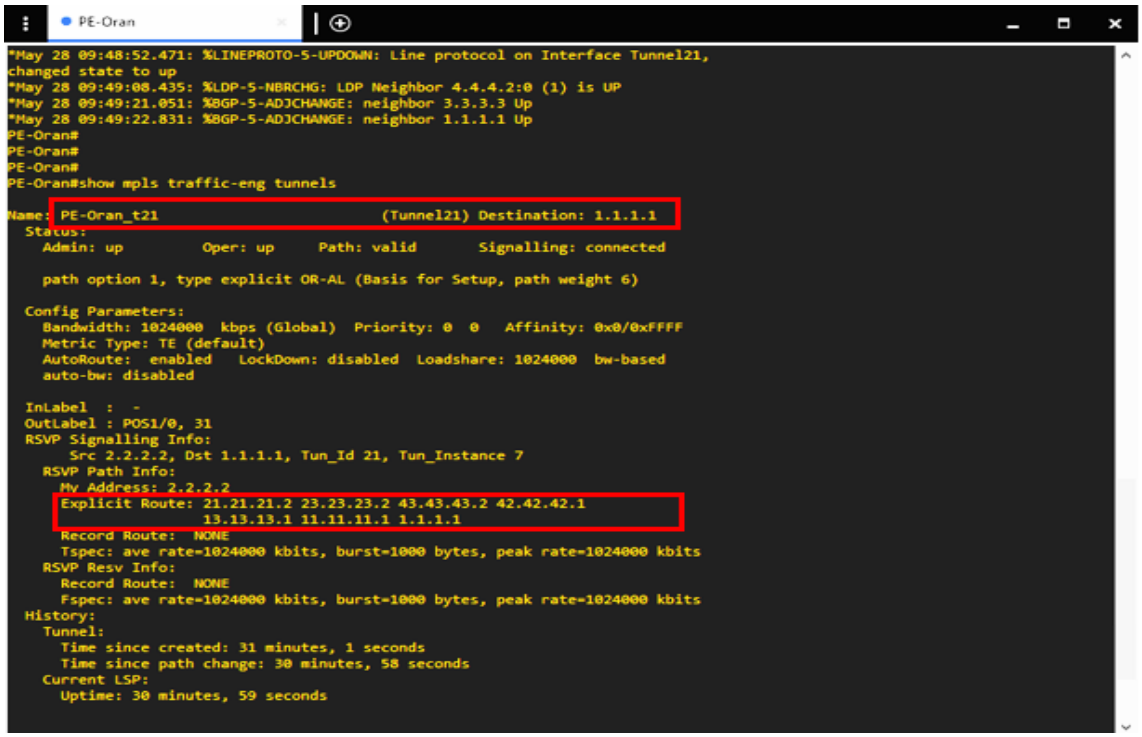

Figure 42 : Protection des liens pour PE-Oran dans le modèle Pair à Pair

3.2 Modèle Amélioré

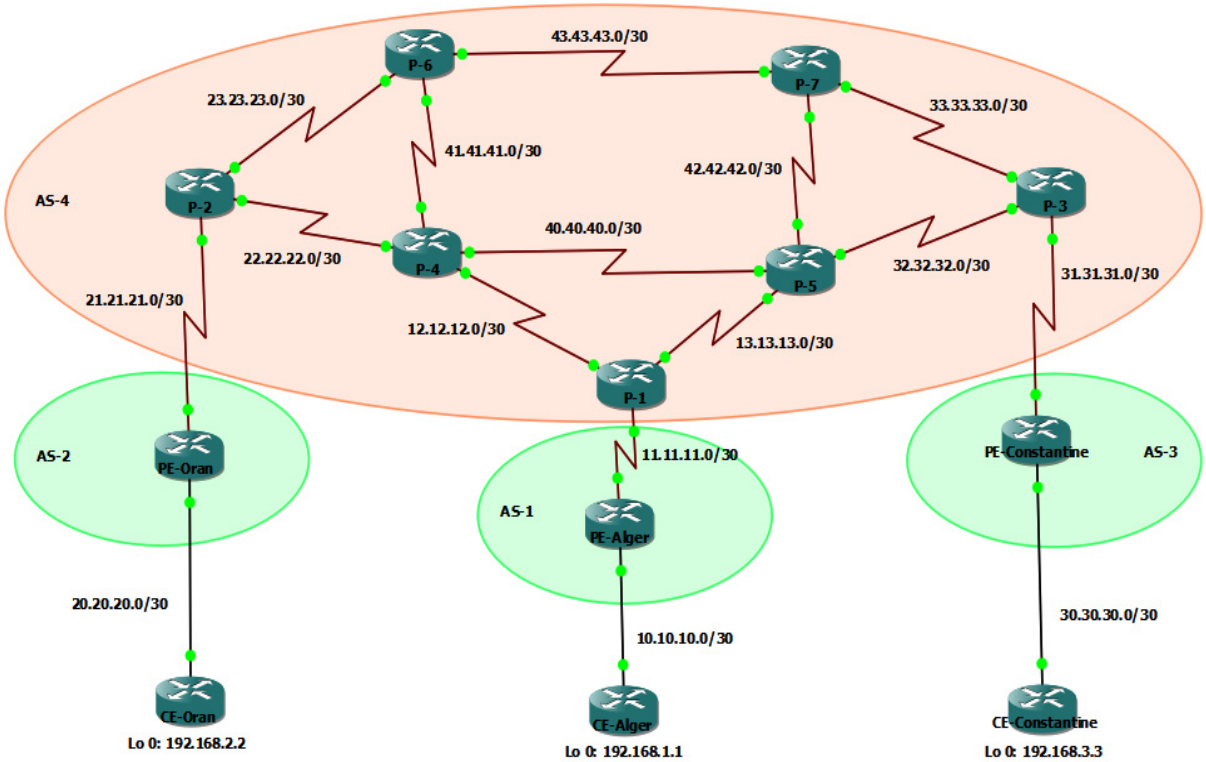

Figure 43 : Architecture modèle Amélioré

L'architecture modèle Amélioré pour le GMPLS permet une gestion centralisée des ressources et de la signalisation pour les réseaux de transport optique. Dans cette simulation, nous considérons quatre AS (*Autonomous System*) différents situés en Algérie : AS1 à Alger, AS2 à Oran, AS3 à Constantine et AS4 utilisant une connexion Internet.

Les trois premiers AS utilisent le protocole iBGP *(interior Border Gateway Protocol)* pour la communication entre les routeurs appartenant à des AS différents, tandis que le quatrième AS utilise le protocole eBGP *(external Border Gateway Protocol)* pour communiquer avec les autres AS via Internet.

L'objectif de cette simulation est de montrer comment l'architecture modèle Amélioré permet une gestion centralisée et efficace des ressources et de signalisations dans un environnement multi-domaine. Nous allons donc simuler la mise en place d'une connexion de bout en bout entre deux équipements situés dans des AS différents, en utilisant les protocoles de routage et de signalisation appropriés.

3.2.1 Configuration modèle Amélioré

La configuration du modèle Amélioré est similaire à celle du modèle Pair à pair, à une différence près : elle implique la mise en place d'une architecture en quatre systèmes autonomes (AS) distincts. Dans cette configuration, l'AS4 est le centre augmenté qui joue un rôle central en tant que point d'échange pour les autres AS, à savoir AS1, AS2 et AS3. Pour assurer une connectivité cohérente et efficace, l'iBGP (interior Border Gateway Protocol) est configuré entre les routeurs au sein de l'AS4, permettant ainsi le partage des routes internes entre eux. D'autre part, l'eBGP (exterior Border Gateway Protocol) est utilisé pour établir des connexions entre l'AS4 et les autres AS (AS1, AS2 et AS3), assurant ainsi le routage des données à travers les frontières des AS. Cette configuration augmentée permet une collaboration renforcée et une meilleure gestion du trafic entre les différents systèmes autonomes, favorisant ainsi une communication fluide et fiable à l'échelle de l'ensemble du réseau.

PE-Alger

```
router bgp 1
no bgp default ipv4-unicast
neighbor 4.4.4.1 remote-as 4
neighbor 4.4.4.1 update-source loopback 0
address-family vpnv4
neighbor 4.4.4.1 activate
neighbor 4.4.4.1 next-hop-self
```

PE-Oran

```
router bgp 2
no bgp default ipv4-unicast
neighbor 4.4.4.2 remote-as 4
neighbor 4.4.4.2 update-source loopback 0
address-family vpnv4
neighbor 4.4.4.2 activate
neighbor 4.4.4.2 next-hop-self
```

PE-Constantine

```
router bgp 3
no bgp default ipv4-unicast
neighbor 4.4.4.3 remote-as 4
neighbor 4.4.4.3 update-source loopback 0
address-family vpnv4
neighbor 4.4.4.3 activate
neighbor 4.4.4.3 next-hop-self
```

P-1

```
router bgp 4
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 update-source loopback 0
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 next-hop-self
exit
router bgp 4
no neighbor 4.4.4.3 remote-as 4
no neighbor 4.4.4.3 update-source
loopback 0
address-family vpnv4
no neighbor 4.4.4.3 activate
no neighbor 4.4.4.3 next-hop-self
exit
router bgp 4
neighbor 4.4.4.2 remote-as 4
neighbor 4.4.4.2 update-source loopback 0
address-family vpnv4
neighbor 4.4.4.2 activate
neighbor 4.4.4.2 next-hop-self
```

P-2

```
router bgp 4
neighbor 1.1.1.1 remote-as 2
neighbor 1.1.1.1 update-source loopback 0
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 next-hop-self
exit
router bgp 4
no neighbor 4.4.4.1 remote-as 4
no neighbor 4.4.4.1 update-source
loopback 0
address-family vpnv4
no neighbor 4.4.4.1 activate
no neighbor 4.4.4.1 next-hop-self
exit
router bgp 4
neighbor 4.4.4.3 remote-as 4
neighbor 4.4.4.3 update-source loopback 0
address-family vpnv4
neighbor 4.4.4.3 activate
neighbor 4.4.4.3 next-hop-self
```

P-3

```
router bgp 4
neighbor 1.1.1.1 remote-as 3
neighbor 1.1.1.1 update-source loopback 0
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 next-hop-self
exit
router bgp 4
no neighbor 4.4.4.1 remote-as 4
no neighbor 4.4.4.1 update-source
loopback 0
address-family vpnv4
no neighbor 4.4.4.1 activate
no neighbor 4.4.4.1 next-hop-self
exit
router bgp 4
neighbor 4.4.4.2 remote-as 4
neighbor 4.4.4.2 update-source loopback 0
address-family vpnv4
neighbor 4.4.4.2 activate
neighbor 4.4.4.2 next-hop-self
```

3.2.2 Découverte des voisins

Dans le modèle Amélioré, l'exécution de la commande affiche les voisins LDP du routeur P-1, résultant la découverte avec succès de trois voisins. L'identifiant du premier voisin PE-Alger est 1.1.1.1, celui de P-4 est 4.4.4.4 et celui de P-5 est 4.4.4.5. Cette fonctionnalité a permis à P-1 de communiquer efficacement avec ses voisins, ouvrant ainsi la voie à une meilleure collaboration et à un échange d'informations plus fluide (Figure 44).

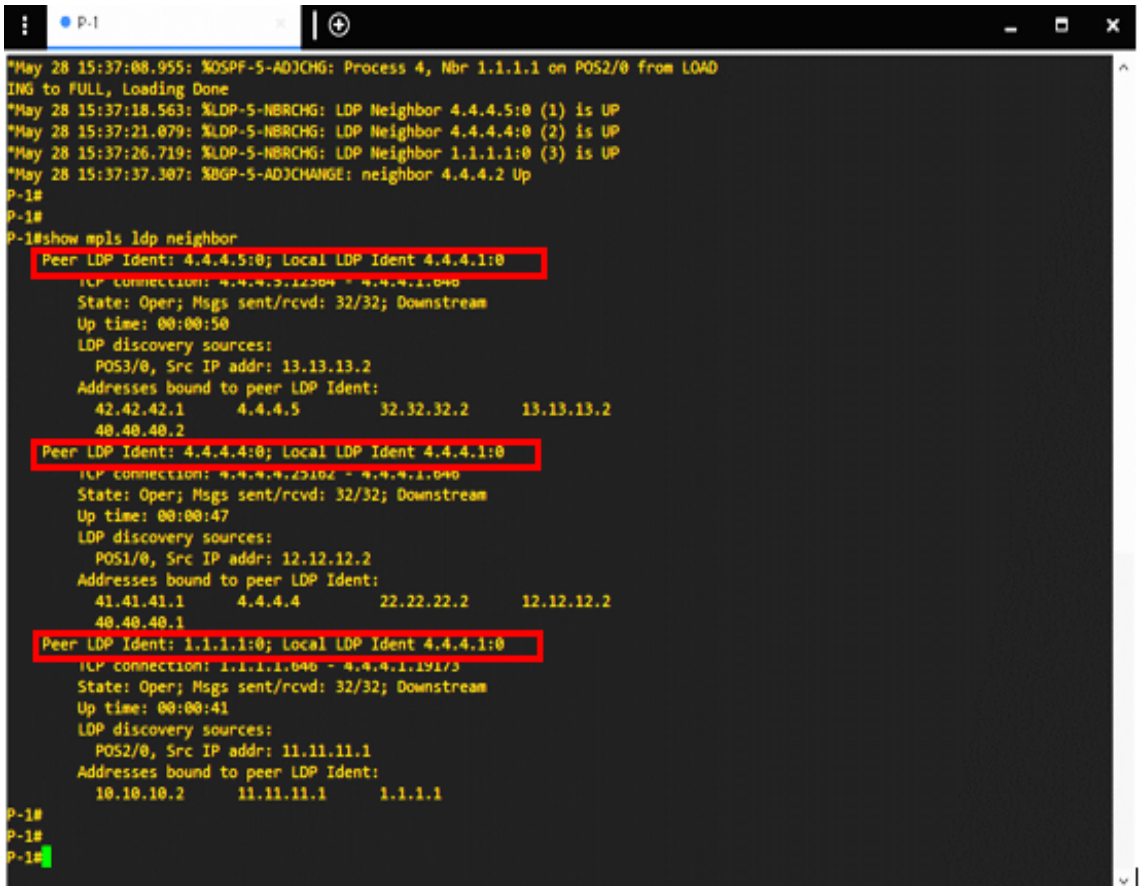

Figure 44 : Découverte des voisins pour le routeur P-1 dans modèle Amélioré

3.2.3 Propagation des états de lien

Dans notre simulation de modèle Amélioré, nous avons étudié la propagation des états de lien du routeur PE-Constantine (Figure 45). Modèle Amélioré utilise une approche améliorée pour la diffusion de ces informations cruciales. Les états de lien du routeur PE-Constantine sont diffusés de manière efficace et rapide à travers le réseau. Cette propagation optimisée permet d'assurer une synchronisation précise et en temps réel des états de lien, ce qui facilite la prise de décision et la planification des itinéraires dans le système GMPLS. En garantissant une transmission fiable et rapide de ces informations, modèle Amélioré contribue à une meilleure stabilité et performance globale du réseau, offrant ainsi une expérience utilisateur améliorée et des communications fluides entre les différents nœuds du système.

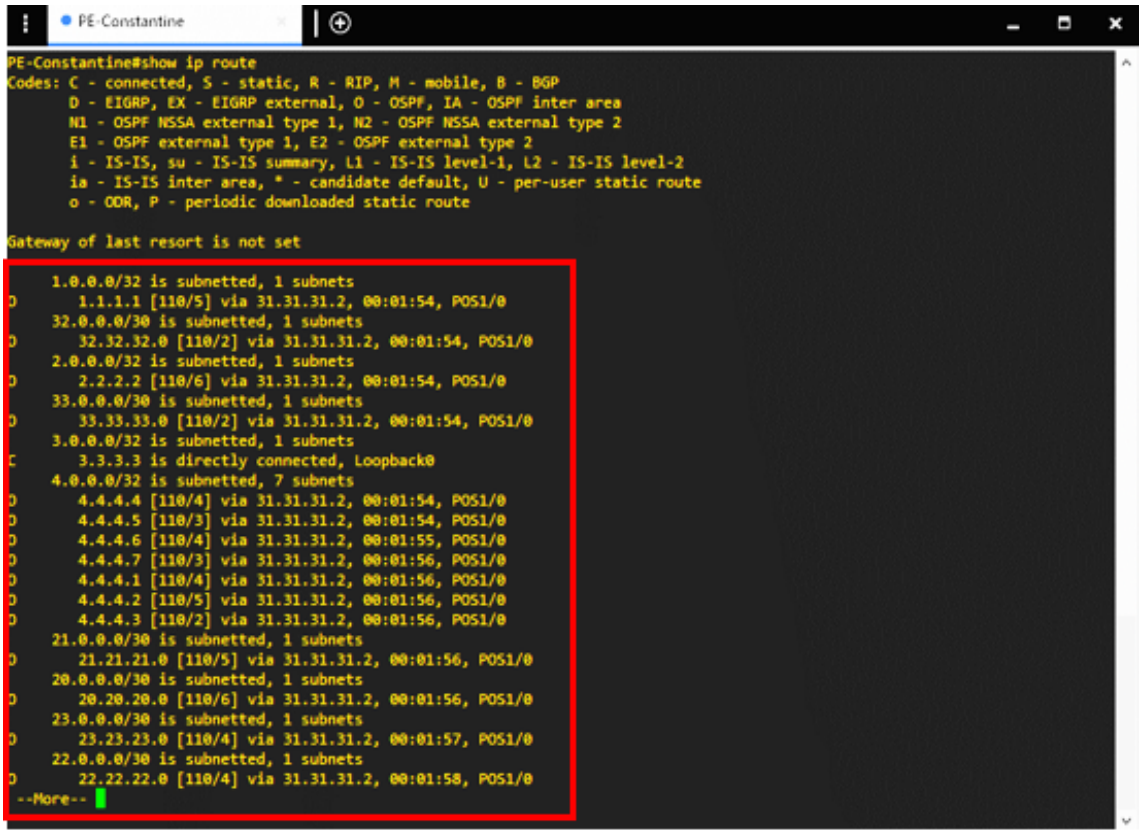

Figure 45 : Propagation des états de lien PE-Constantine dans modèle Amélioré

3.2.4 Gestion de l'état des liens

Dans notre simulation de modèle Amélioré, nous avons utilisé la commande **traceroute** pour observer la gestion de l'état des liens lors du routage de CE-Oran vers CE-Alger. Nous avons pu constater le routage explicite des paquets de données à travers les routeurs PE-Oran, P-2, P-6, P-7, P-5, P-1 et enfin PE-Alger pour atteindre la destination CE-Alger (Figure 46).

De plus, nous avons également étudié la gestion des pannes de lien et le routage dynamique dans modèle Amélioré. En cas de panne d'un lien spécifique, nous avons observé un changement de routage pour assurer la continuité de la connectivité. Le routage alternatif, dans ce cas précis, se faisait à travers les routeurs PE-Oran, P-2, P-4, P-1, et enfin PE-Alger (Figure 46).

Cette capacité à gérer de manière dynamique les pannes de lien et à rediriger le trafic vers des itinéraires alternatifs démontre la résilience et la robustesse du réseau GMPLS dans modèle Amélioré. Ces fonctionnalités de routage dynamique permettent de maintenir la connectivité et de minimiser les interruptions de service, offrant ainsi une expérience utilisateur fiable et continue.

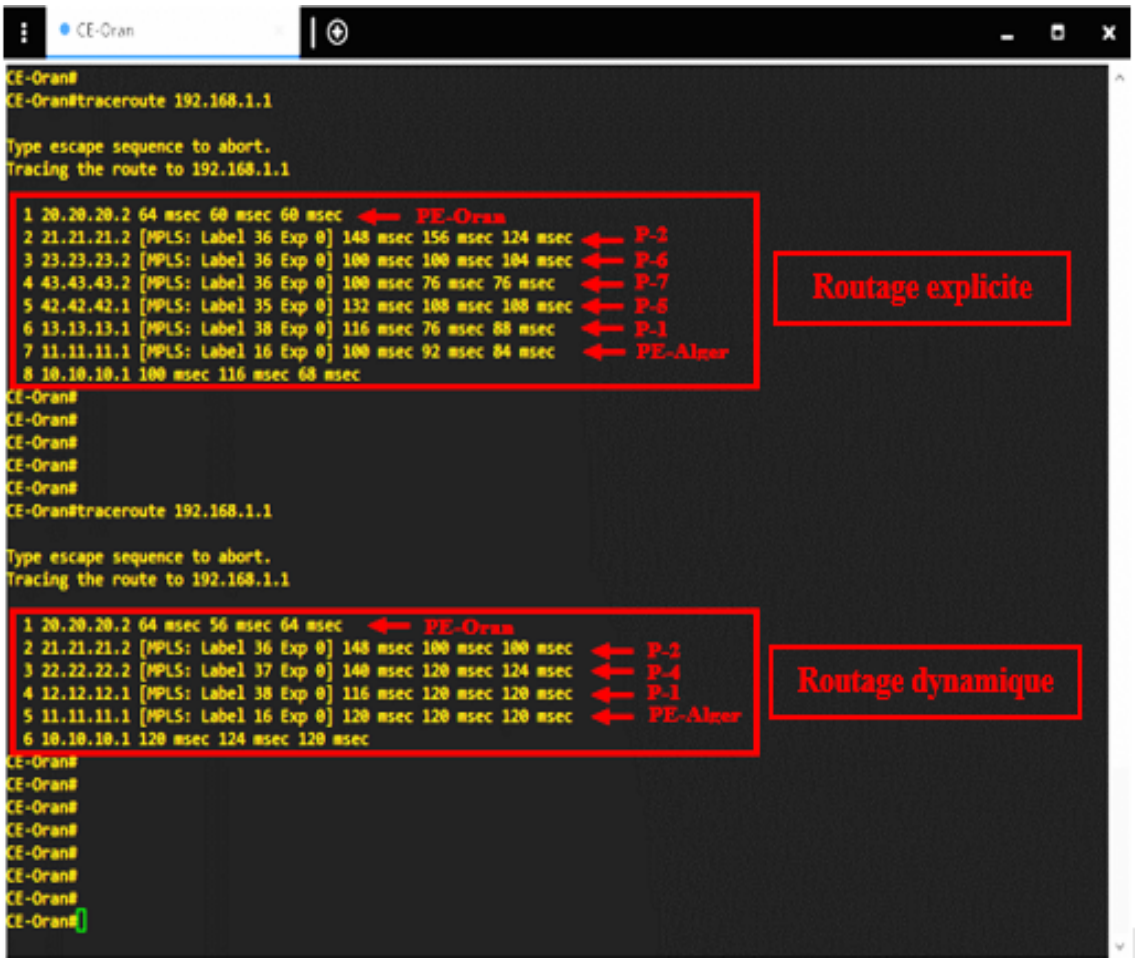

Figure 46 : Gestion de l'état des liens CE-Oran dans modèle Amélioré avec un routage explicite et dynamique

3.2.5 Contrôle et gestion des routes

Dans modèle Amélioré, le contrôle et la gestion des routes sont essentiels pour une utilisation efficace de la bande passante. Notre simulation a utilisé une bande passante totale de 4 Go, avec une allocation de 1 Go par flux de données, assurant une répartition équitable des ressources (Figure 47). Cette approche permet de choisir les chemins les plus adaptés en termes de disponibilité de la bande passante, grâce à une surveillance en temps réel de la charge et de la disponibilité des liens. Modèle Amélioré ajuste ainsi dynamiquement les itinéraires et les allocations de bande passante pour optimiser les performances du réseau, évitant la congestion et les goulots d'étranglement. Cette gestion améliore la fluidité et l'efficacité de la transmission des données, garantissant des délais de livraison optimisés et une meilleure expérience utilisateur.

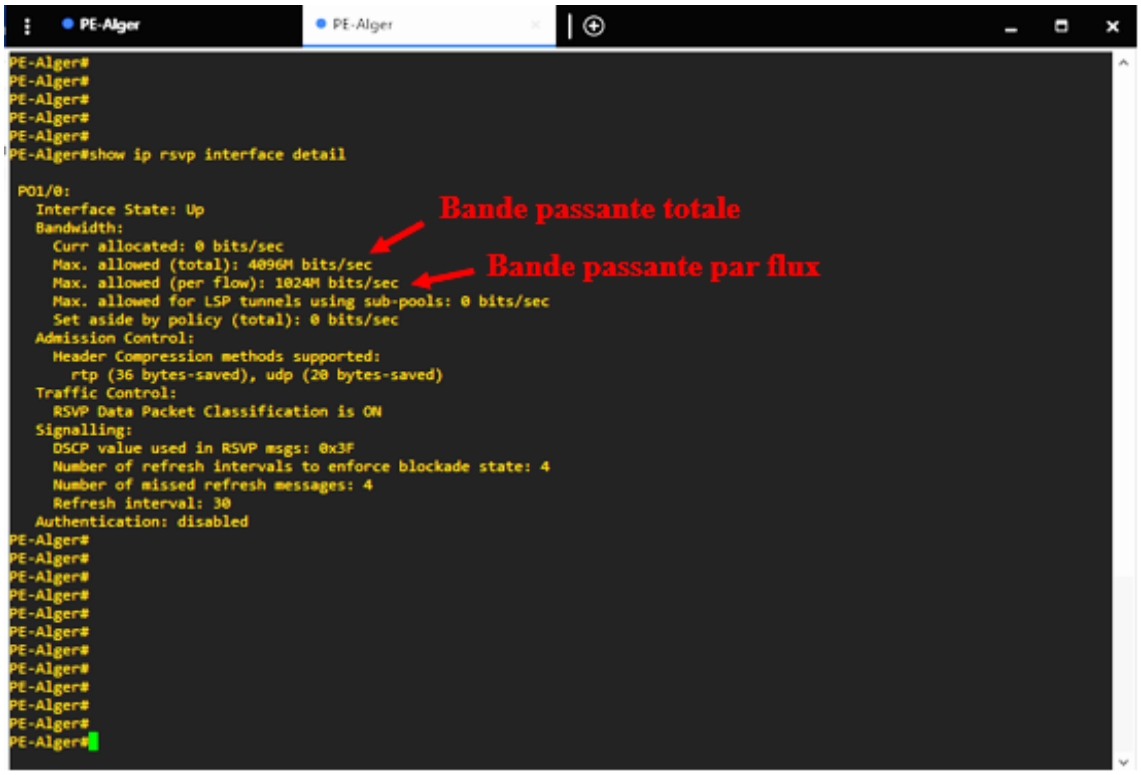

Figure 47 : Contrôle et gestion des routes pour le routeur PE-Alger dans modèle Amélioré

3.2.6 Gestion des liens

Dans modèle Amélioré, la gestion des liens est optimisée grâce à l'utilisation de labels. Les labels sont des identifiants uniques attribués aux liens et aux ressources du réseau. Ils permettent une gestion plus efficace des liens en facilitant leur identification et leur suivi.

Dans notre simulation, nous avons pu observer comment les labels étaient utilisés dans la gestion des liens. Les labels sont associés à chaque lien du réseau (Figure 48), ce qui permet de les identifier rapidement et de façon précise. Cela facilite la configuration, le suivi et la résolution des problèmes liés aux liens dans le réseau GMPLS.

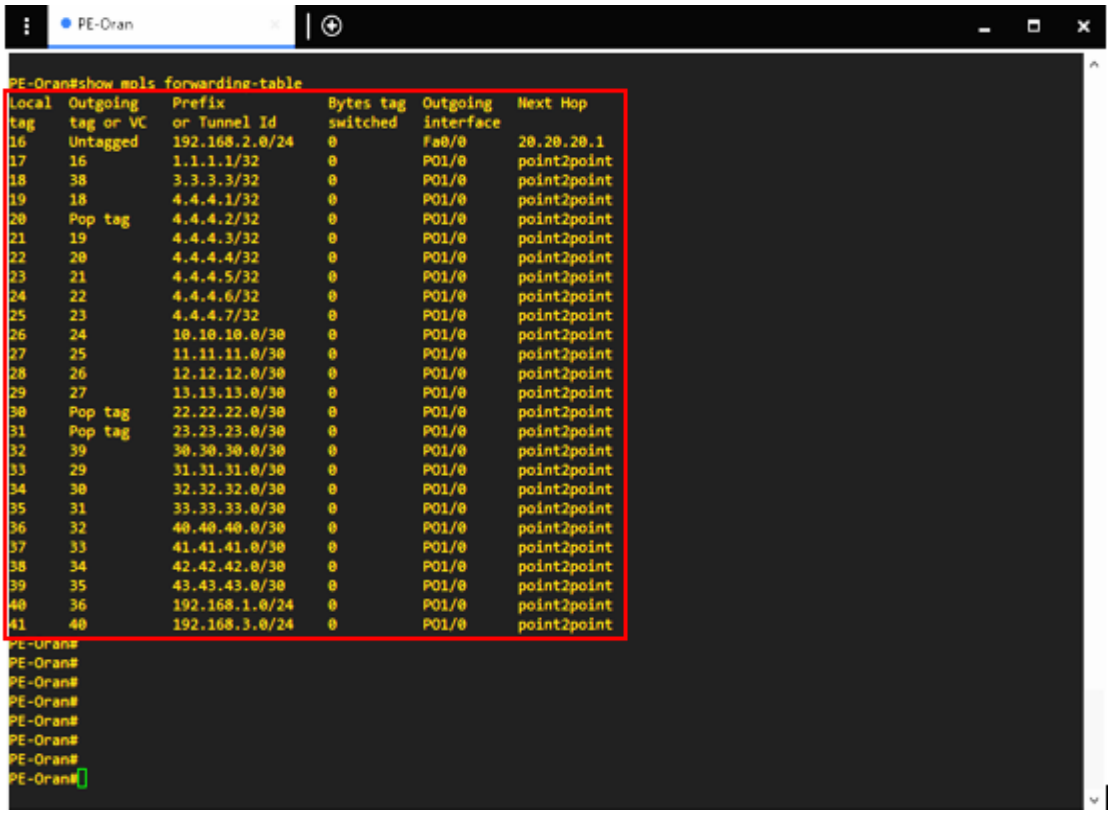

Figure 48 : Chemins empruntés dans le routeur PE-Oran dans modèle Amélioré

3.2.7 Protection des liens

Dans modèle Amélioré, la protection des liens est essentielle pour garantir la continuité des communications. Notre simulation a mis en place une stratégie de protection des liens basée sur l'utilisation de tunnels explicites et dynamiques.

Tout d'abord, nous avons configuré un tunnel explicite prioritaire, le tunnel 13 (Figure 49), reliant Constantine à Alger. Ce tunnel est dédié au trafic principal et bénéficie d'une priorité élevée. Il offre une bande passante optimale et assure une performance optimisée pour les communications entre les deux sites.

En cas de panne du tunnel 13 (Figure 49), nous avons également configuré un tunnel de secours, le tunnel 31. Ce tunnel est activé automatiquement lorsque le premier tunnel rencontre un problème. Il permet de maintenir la connectivité entre Constantine et Alger en fournissant un chemin alternatif pour acheminer les données.

Nous avons mis en place un tunnel dynamique reliant Constantine à Oran (Figure 49). Ce tunnel permet de réacheminer le trafic en temps réel, maintenu la connectivité entre Constantine et Oran.

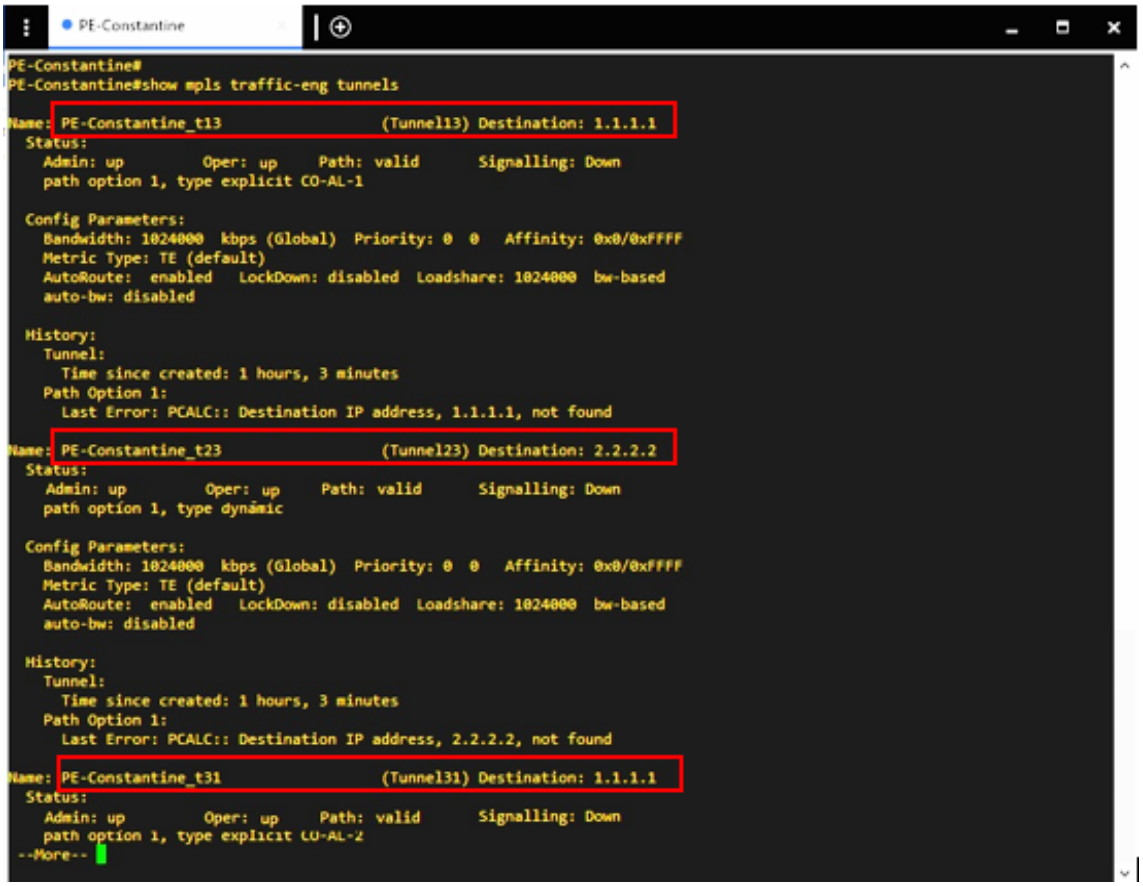

Figure 49 : Protection des liens pour PE-Constantine dans modèle Amélioré

3.3 Modèle Superposé

La topologie modèle Superposé dans GMPLS consiste à créer une couche de contrôle et de gestion supplémentaire au-dessus de l'infrastructure existante en utilisant des tunnels pour établir des communications logiques entre les nœuds. Cela permet une plus grande flexibilité et évolutivité dans le déploiement de services et l'utilisation des ressources réseau.

Dans GMPLS, le modèle Superposé utilise UNI *(User Network Interface)* qui joue un rôle essentiel dans la communication et l'interaction entre les utilisateurs finaux et le réseau GMPLS.

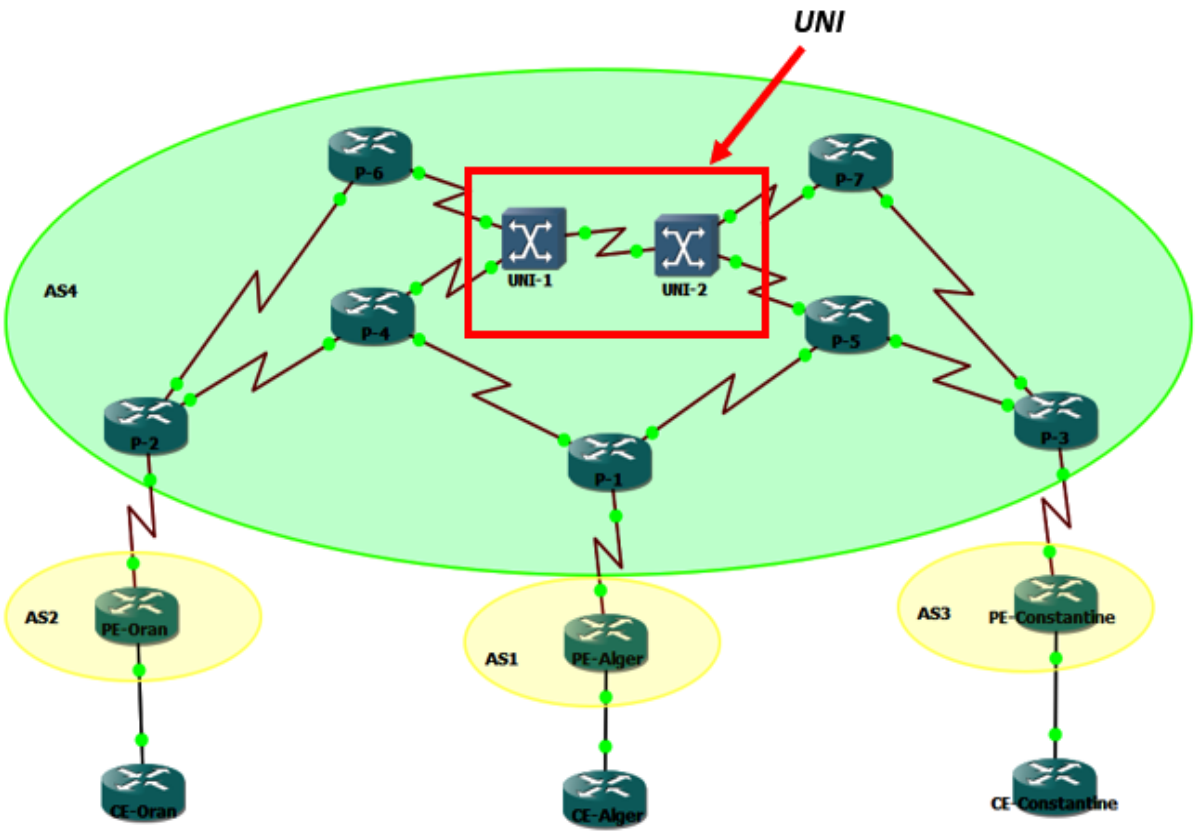

Figure 50 : Architecture modèle Superposé

Ce modèle présente une difficulté concernant l'implémentation des interfaces dans notre simulateur GNS3 et vu que l'indisponibilité de la série du routeur NCS 5500 dans notre bibliothèque GNS3 et le Net, nous avons focalisé juste sur les deux architectures précédentes.

3.3.1 Découverte des voisins

Dans le modèle Superposé du GMPLS, la découverte des voisins peut être réalisée à l'aide de protocoles de signalisation GMPLS, de protocoles de routage ou de mécanismes de contrôle de voisinage. Ces mécanismes permettent aux nœuds d'échanger des informations d'adjacence, d'établir des connexions, de partager des informations de connectivité et d'identifier les voisins directement dans la topologie du réseau.

3.3.2 Propagation des états de lien

La propagation des états de lien consiste à diffuser et mettre à jour les informations sur l'état des liens du réseau entre les nœuds. Les protocoles de routage, tels que l'OSPF ou IS-IS *(Intermediate* System - *Intermediate System)*, permettent aux nœuds de partager les mises à jour périodiques ou déclenchées concernant l'état des liens. Les protocoles de signalisation GMPLS, comme RSVP-TE, sont utilisés pour informer les autres nœuds des changements d'état des liens. L'objectif est de maintenir une vision cohérente et à jour de la topologie et de l'état des

liens afin de faciliter les décisions de routage, d'établissement de connexions et de réservation de ressources dans le réseau Superposé GMPLS.

3.3.3 Gestion de l'état des liens

Dans Superposé GMPLS, les protocoles de routage permettent l'échange d'informations sur l'état des liens, la détection des changements d'état et la mise à jour de la base de données topologique. Les protocoles de signalisation GMPLS facilitent la négociation des paramètres de connexion, la vérification de l'état des ressources et la mise à jour de l'état des liens en fonction des demandes de trafic et des changements de disponibilité. Les mécanismes de monitoring surveillent l'état des liens et déclenchent des mises à jour en cas de changements. La coordination des ressources gère les conflits potentiels lors de la réservation des ressources et maintient la cohérence des informations de l'état des liens lors de la planification des chemins et de la répartition des ressources.

3.3.4 Contrôle et gestion des routes

Dans le modèle Superposé de GMPLS, les protocoles de routage traditionnels, tels que l'OSPF et IS-IS, sont utilisés pour calculer les chemins optimaux et partager les informations de routage entre les nœuds. RSVP-TE, jouent un rôle clé dans la mise à jour des routes en cas de changements. Des mécanismes de contrôle de trafic sont employés pour gérer la distribution des flux sur les routes disponibles, en utilisant des techniques de répartition de charge, de QoS et de la gestion des priorités. Les mécanismes de gestion des politiques permettent de définir et d'appliquer des règles spécifiques aux routes, incluant des politiques de routage, de filtrage et de sécurité.

3.3.5 Gestion des liens

La gestion des liens dans le modèle Superposé de GMPLS implique la surveillance, la mise à jour et la coordination de l'état des liens du réseau. Cela comprend la détection des changements d'état des liens physiques et virtuels, la propagation des mises à jour d'état, la résolution des conflits et la coordination des ressources.

L'objectif est d'assurer une vision cohérente et à jour de la topologie et de l'état des liens, facilitant ainsi la prise de décisions de routage et la gestion efficace des ressources dans le réseau Superposé GMPLS.

3.3.6 Protection des liens

La protection des liens dans le modèle Superposé GMPLS vise à assurer la disponibilité et la résilience du réseau en cas de défaillance des liens physiques ou virtuels. Cela est réalisé par la mise en place de chemins de secours, la commutation rapide vers des liens de secours préconfigurés, la restauration des connexions à travers de nouvelles routes et l'utilisation de la diversité des chemins. Ces techniques garantissent la continuité du service et offrent des options de routage alternatives en cas de défaillance, assurant ainsi la fiabilité du réseau.

Notez bien que cette architecture sera adoptée dans les travaux futurs (perspectives).

4 Qualité de service dans le GMPLS

4.1 Latence

La latence dans le GMPLS se réfère au délai ou à la durée de transmission des données à travers le réseau.

Dans notre simulation, nous avons mesuré les latences entre les sites CE-Oran et CE-Alger en utilisant des commandes ping. Nous avons configuré un chemin explicite spécifique entre ces sites, en appliquant différents paramètres. Nous avons varié le nombre de pings envoyés, allant de 100 à 1000, et la taille des paquets, fixée à 1000 octets. En effectuant ces mesures, nous avons pu obtenir des informations sur les délais de transmission des données entre les sites, ce qui nous permet d'évaluer les performances du réseau GMPLS. Ces résultats nous permettent de mieux comprendre la latence dans le contexte de notre simulation et de prendre des décisions éclairées concernant la configuration et l'optimisation du réseau GMPLS.

Au cours de notre simulation, nous avons observé une différence de latence entre les deux modèles, modèle Pair à Pair et modèle Amélioré. Dans le modèle Pair à Pair, nous avons enregistré une variation de latence entre un maximum de 102 ms et un minimum de 98 ms (Figure 51). Cependant, dans modèle Amélioré, cette latence était légèrement inférieure, oscillant entre un maximum de 101 ms et un minimum de 97 ms (Figure 52). Néanmoins, une constatation importante est que, quelle que soit la version du modèle utilisée, la latence a finalement atteint une stabilité à la fin de notre simulation. Cette stabilisation est essentielle pour garantir des performances cohérentes et fiables, permettant ainsi une meilleure planification et une exécution plus efficace des tâches. En optimisant les temps de réponse et en réduisant les variations de latence, nous améliorons significativement l'expérience utilisateur et assurons un fonctionnement fluide de nos modèles.

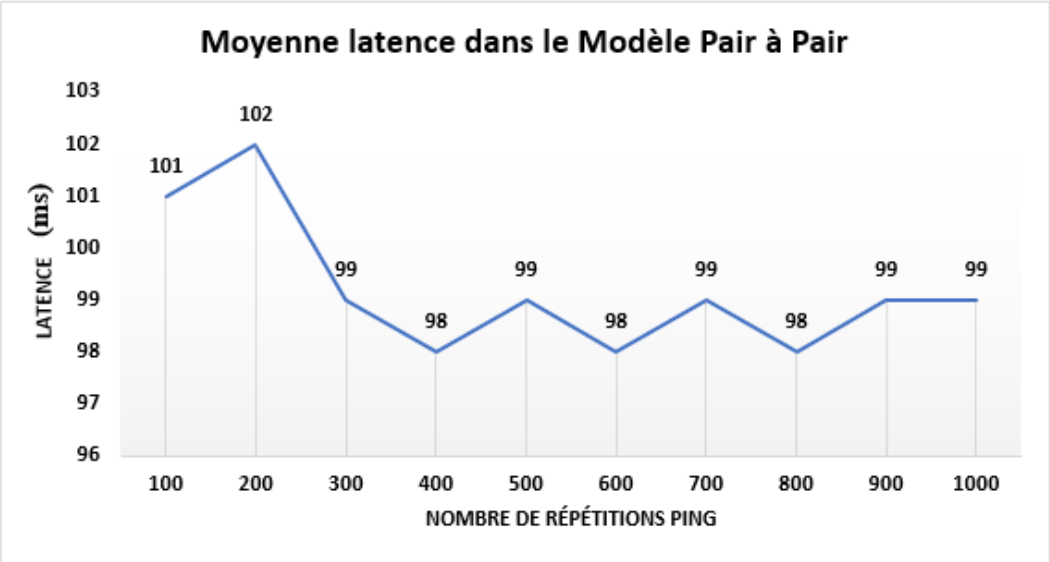

Figure 51 : Latence dans modèle Pair à Pair

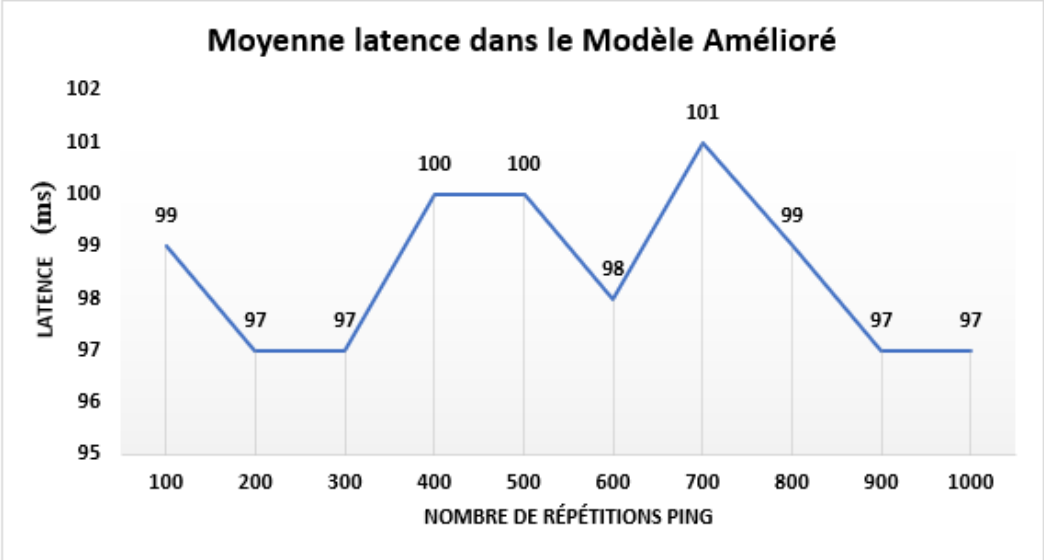

Figure 52 : Latence dans modèle Amélioré

4.2 Bande passante

À partir de notre analyse des performances, nous avons constaté une variation significative de la bande passante entre les deux modèles, modèle Pair à Pair et modèle Amélioré. Dans le modèle Pair à Pair, nous avons mesuré une bande passante variant entre un maximum de 188600 bits et un minimum de 91100 bits (Figure 53). Cependant, dans le modèle Amélioré, nous avons enregistré une bande passante plus élevée, oscillant entre un maximum de 225900 bits et un minimum de 137300 bits (Figure 54). Ces variations de la bande passante peuvent avoir un impact important sur les performances globales de nos modèles, notamment en ce qui concerne le débit de transmission des données. Une bande passante plus élevée permet un transfert plus

rapide des informations, ce qui peut contribuer à une exécution plus efficace des tâches et à une meilleure réactivité du système.

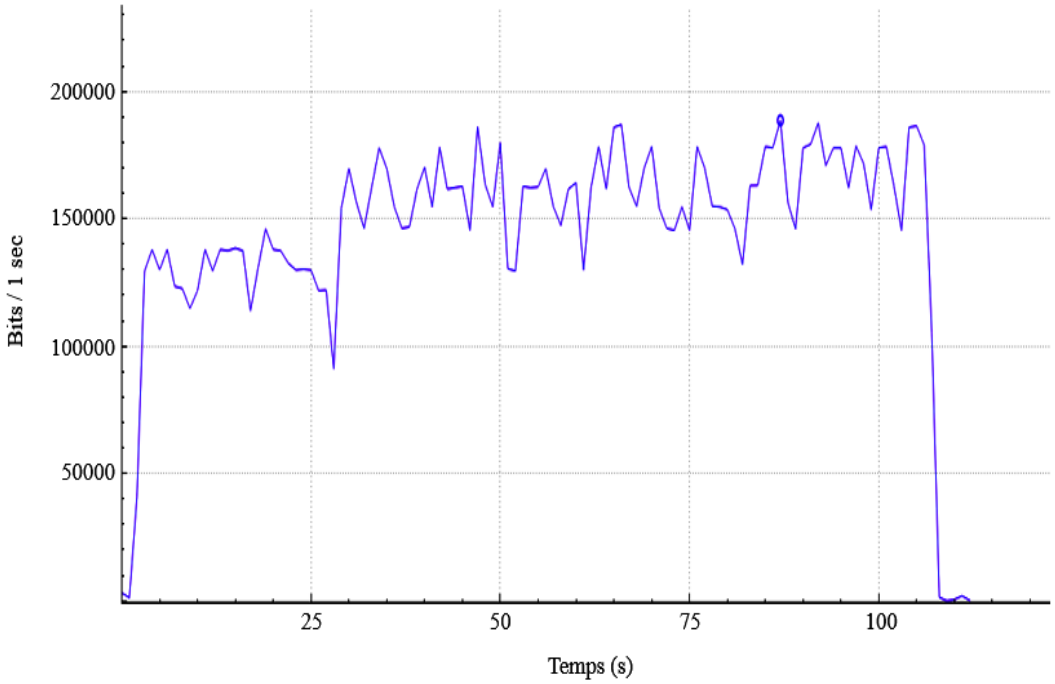

Figure 53 : Variation de la bande passante dans modèle Pair à Pair

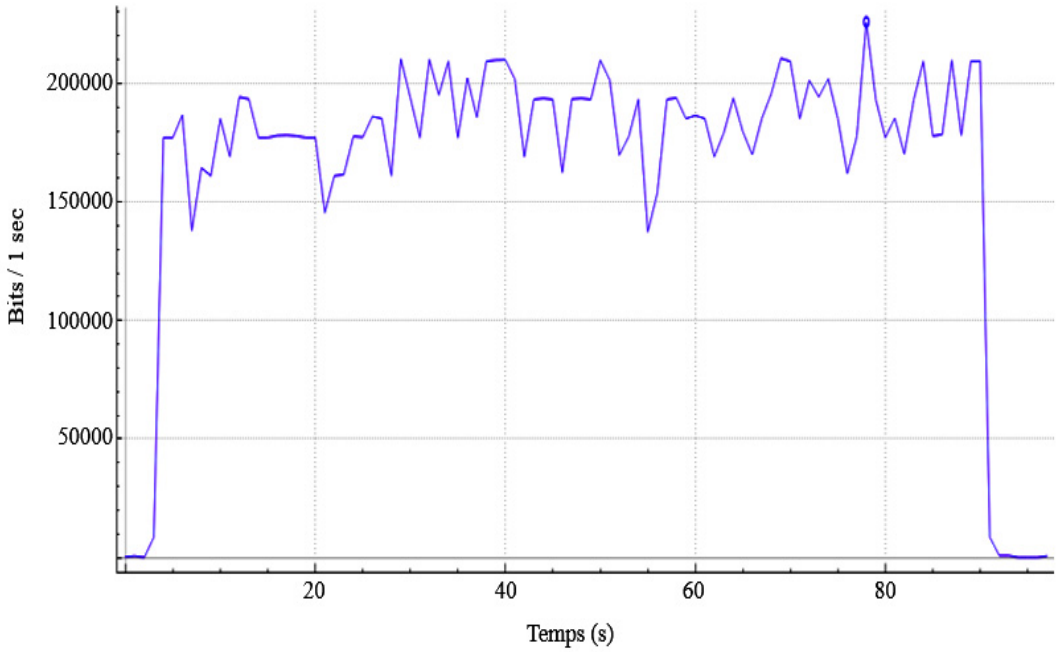

Figure 54 : Variation de la bande passante dans modèle Amélioré

5 Comparaison entre modèle Pair à Pair et modèle Amélioré

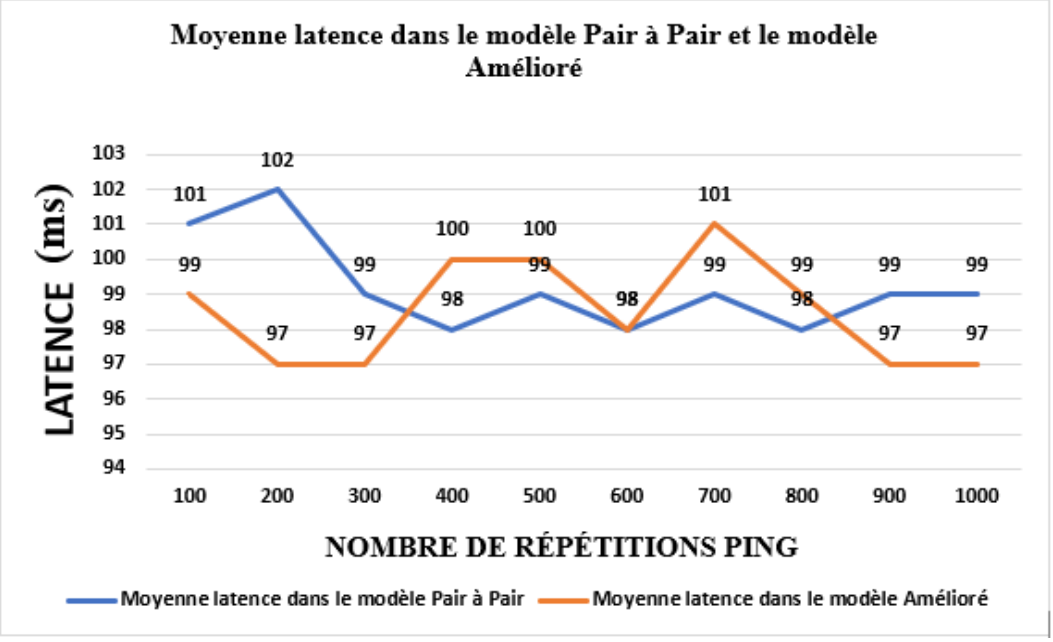

Figure 55 : Latence dans modèle Pair à Pair et modèle Amélioré

Voici un tableau comparatif des avantages et inconvénients de la bande latence dans les modèles Pair à pair et modèle Amélioré, en utilisant les valeurs résultant de notre simulation (Figure 55) :

	Modèle Pair à Pair	**Modèle Amélioré**
Avantages	- Latence moyenne plus faible (98,6 ms)	- Latence moyenne légèrement plus élevée (98,8 ms)
	- Stabilité de la latence (variance faible)	- Latence relativement stable (variance faible)
Inconvénients	- Quelques valeurs de latence légèrement élevées (101 ms)	- Quelques valeurs de latence élevées (101 ms)
	- Quelques valeurs de latence légèrement basses (98 ms)	- Quelques valeurs de latence basses (97 ms)
	- Quelques valeurs de latence légèrement supérieures à la moyenne (99 ms)	- Quelques valeurs de latence supérieures à la moyenne (100 ms)

Tableau 3 : Comparaison de la latence entre modèle Pair à Pair et modèle Amélioré

Voici un tableau comparatif des avantages et inconvénients de la bande latence dans les modèles Pair à Pair et Amélioré, en utilisant les plages de valeurs résultant de notre simulation (Figure 55) :

	Modèle Pair à Pair	**Modèle Amélioré**
Avantages	- Plage de latence plus étroite (91-100 ms)	- Plage de latence plus étendue (137-225 ms)
	- Latence moyenne relativement basse (95 ms)	- Latence moyenne relativement élevée (181 ms)
Inconvénients	- Limite inférieure de la plage de latence légèrement élevée (91 ms)	- Limite inférieure de la plage de latence relativement élevée (137 ms)
	- Limite supérieure de la plage de latence relativement élevée (100 ms)	- Limite supérieure de la plage de latence légèrement élevée (225 ms)

Tableau 4 : Comparaison de la bande passante entre modèle Pair à Pair et modèle Amélioré

Le choix entre les deux modèles dépendra des exigences spécifiques du réseau, de la nécessité d'une coordination globale des opérations, de la flexibilité locale et des compromis entre l'autonomie des nœuds et la coordination centralisée.

6 Conclusion

En conclusion de notre simulation sur la gestion de plan de contrôle du GMPLS concernant les deux architectures, à savoir le modèle Pair à Pair et le modèle Amélioré, nous avons observé des résultats prometteurs en termes de latence et de bande passante.

Dans le modèle Pair à Pair, la latence variait entre 102 ms maximum et 98 ms minimum, tandis que dans le modèle Amélioré, elle était légèrement réduite, oscillant entre 101 ms maximum et 97 ms minimum. Cela indique que le modèle Amélioré présente une amélioration importante en termes de réactivité et de temps de réponse par rapport au modèle Pair à Pair.

Pour ce qui concerne la bande passante, nous avons mesuré une plage plus large dans le modèle Amélioré, allant de 225900 bits au maximum à 137300 bits au minimum, par rapport au modèle Pair à Pair qui était de 188600 bits au maximum à 91100 bits minimum. Cette augmentation de la bande passante dans le modèle Amélioré permet un transfert plus rapide des données, offrant ainsi une meilleure capacité de transmission et une exécution plus efficace des tâches.

Donc, le modèle Amélioré présente des avantages significatifs en termes de latence réduite et de bande passante accrue par rapport au modèle Pair à Pair. Ces améliorations jouent un rôle capital dans l’amélioration des performances globales du système GMPLS, en offrant une

expérience utilisateur plus fluide et des échanges d'informations plus rapides dans la gestion du plan de contrôle.

Cependant, il convient de noter que des études supplémentaires et des analyses approfondies sont nécessaires pour évaluer pleinement les performances des deux modèles et comprendre leurs impacts sur des scénarios d'utilisation spécifiques.

Conclusion générale

Dans notre travail, nous avons fait une étude sur la gestion du plan de contrôle pour le réseau GMPLS. Nous avons réalisé plusieurs simulations concernant ce plan appliqué sur trois villes algériennes à savoir, Alger, Oran et Constantine. Nous avons employé des protocoles de signalisation et de routage pour le réseau GMPLS à savoir RSVP, l'OSPF, iBGP et eBGP appliqués sur les deux architectures (modèle Pair à Pair et modèle Amélioré). Dans notre étude, nous avons testé notre plan de contrôle GMPLS sur ces deux modèles pour mesurer les performances en termes de temps de réponse, de disponibilité de la bande passante, et les délais de transmissions. Après la simulation, nous avons élaboré une comparaison entre les deux architectures, et nous avons obtenu des meilleurs résultats en termes de latence et de bande passante pour modèle Amélioré par rapport au modèle Pair à Pair, ce que signifie que le choix d'une telle architecture joue un grand rôle pour optimiser notre plan de contrôle relatif au réseau GMPLS.

En ce qui concerne la troisième architecture le modèle Superposé, nous n'avons pas pu la réaliser en raison d'une difficulté liées l'implémentation des interfaces dans notre simulateur GNS3 et à l'indisponibilité de la série du routeur NCS 5500 dans notre bibliothèque GNS3, de plus cette série de routeurs est payante. Par conséquent, nous nous sommes concentrés uniquement sur les deux architectures.

En tant que perspective pour les futurs travaux nous souhaitons réaliser cette architecture (Modèle Superposé), afin d'établir une comparaison détaillée entre ces trois modèles.

Bibliographie

[1] : KHERICI Cheikh, *''Polycopié : cours sur les réseaux WAN",* Université Ibn Khaldoun-Tiaret, 2022.

[2] : Mazhar, Muhammad Shoaib, *''Comparative Study of WAN Services and Technologies in Enterprise Business Networks'',* 01/05/2019.

[3] : Adam Guipelbé, *"Architectures des réseaux WAN",* DIRTECH, CCNA 200-301.

[4] : El Hassan EL AMRI - Technologie WAN, *"Connexion point à point (ppp, hdlc)",* 21/01/2017.

[5] : Adam Guipelbé, *" Architectures des réseaux WAN"*, Topologies de WAN, DIRTECH, CCNA 200-301.

[6] : Guy Pujolle, *"Les Reseaux"*, avec la collaboration de Olivier Salvatori et la contribution de Jacques Nozick. 6ème édition, 2008.

[7] : Kevunie R , *" WAN : tout savoir sur le réseau étendu "* , Avril 2021.

[8] : Cours *''Introduction to WANs (Wide Area Network)''* publié sur NetworkLessons.com.

[9] : Guemmoula lazhar, Douib larouci, Mémoire *"La sécurité dans les réseaux MPLS basés sur la commutation par étiquette",* Université Kasdi Merbah Ouargla, 2017.

[10] : FOUROUR Said, THESE DE MAGISTER *"Modélisation et Optimisation dans les Réseaux MPLS",* Université d'Oran-Es Senia, 2011.

[11] : L. Berger, *"Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description"* Ed., RFC 3471, January 2003.

[12] : Taylor & Francis, Brian J. Thompson, Group, LLC, *'' GMPLS TECHNOLOGIES'', Broadband Backbone Networks and Systems''*, University of Rochester, New York, 2006.

[13] : L. Berger *"Generalized Multi-Protocol Label Switching (GMPLS) Signaling : Resource ReSerVation Protocol-Traffic Engineering (RSVP-TE) Extensions",* Ed., RFC 3473, January 2003.

[14] : David Griffith, *'' The GMPLS Control Plane Architecture for Optical Networks : Routing and Signaling for Agile High Speed Switching ''*, GMPLS SIGNALING, 2004.

[15] : Banerjee, A. et al., *''Generalized multi Protocol label Switching : an overview of routing and management enhancements''*, IEEE Commun. Mag., Vol. 39, Issue1,144–150, 2001.

[16] : Kompella, K. and Rekhter, Y., *''OSPF Extensions in Support of Generalized MPLS, IETF draft''*, Oct. 2003 (work in progress).

[17] : Kompella, K. et al., *''Link Bundling in MPLS Traffic Engineering, IETF draft''*, Dec. 2004.

[18] : Moy,J.*''OSPF Version 2, RFC 2328''*http://www.ietf.org/rfc/rfc2328.txt?number=2328.

[19] : Coltun, R., *''The OSPF Opaque LSA Option, RFC 2370''*. http://www.ietf.org/rfc/ rfc2370.txt? Numbers=2370.

[20] : Katz, D. et al., *''Traffic Engineering Extensions to OSPF Version 2, RFC3630''*, http://www.ietf.org/rfc/rfc3630.txt?number=3630.

[21] : Adrian Farrel, Igor Bryskin, and Morgan Kaufmann, *'' GMPLS architecture and applications ''*, Publishers imprint of Elsevier, 2006.

[22] : David Griffith, *'' The GMPLS Control Plane Architecture for Optical Networks : Routing and Signaling for Agile High Speed Switching, LINK MANAGEMENT PROTOCOL",* 2006.

[23] : Brian J. Thompson, *''GMPLS TECHNOLOGIES, Broadband Backbone Networks and Systems'',* University of Rochester, New York, 2006.

[24] : Taylor & Francis Group, LLC, *'' modèle PAIR À PAIR AND modèle SUPERPOSÉ''*, 2006.

Webographie

[web1] : https://www.studocu.com/row/document/universite-de-batna-1/informatique/chapitre-ii-general ite-sur-les-réseaux/5954092

[web2] : https://fr.go-travels.com/38394-definition-of-pan-817889-4592211

[web3] : https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-conn aitre/

[web4] : https://www.networkworld.com/article/2222089/a-brief-history-of-the-enterprise-wan/

[web5] : https://aws.amazon.com/fr/what-is/wan/

[web6] : https://www.wikiwand.com/fr/R%C3%A9seau_%C3%A9tendu

[web7] : https://www.wikiwand.com/fr/Commutation_de_paquets

[web8] : http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/Bordessoules-Bret/Site/Index.htm

[web9] : https://www.rfc-editor.org/rfc/rfc3032.html

[web10] : https://www.rfc-editor.org/rfc/rfc3031.html

[web11] : https://www.frameip.com/mpls/

[web12] : http://www-igm.univ-mlv.fr/~dr/XPOSE2007/ykarkab_MPLS/mpls.html#fec

[web13] : http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/Bordessoules-Bret/Site/MPLS.htm#2.1.3

[web14] : https://datatracker.ietf.org/doc/html/rfc5036

[web15] : https://www.rfc-editor.org/rfc/rfc3477

[web16] : https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-ex-series-vpn-layer2 -layer3.html

[web17] : https://www.frameip.com/vpn/#35-8211-le-protocole-mpls

[web18] : http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002/Brunet-Suarez/ HTML/chapitre2.htm

[web19] : https://www.juniper.net/documentation/fr/fr/software/junos/mpls/topics/topic-map/gmplsconfiguration.html

[web20] : http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/Bordessoules-Bret/Site/GMPLS.htm#3.2

[web21] : https://www.researchgate.net/figure/LSP-hierarchy-in-GMPLS_fig1_229015596

[web22] : https://www.rfc-editor.org/rfc/rfc3209.html

[web23] : https://telcocloudbridge.com/blog/rsvp-te-and-ospf-te-extensions-for-gmpls/

[web24] : https://www.ietf.org/rfc/inline-errata/rfc4428.html

Résumé

Le GMPLS est une extension de MPLS (Multi-Protocol Label Switching) qui permet aux LSR (Label Switched Router) de supporter plusieurs types de commutations à savoir : les paquets, le TDM (SDH/SONET), les lambdas (longueurs d'onde) ainsi que les fibres optiques. Dans le but de contrôler les composantes extérieures au standard de la couche réseau, un plan de contrôle commun a été développé pour le GMPLS. Ce plan de contrôle permet le contrôle total des équipements du réseau.

Le but de ce mémoire est de faire une étude détaillée de la gestion du plan de contrôle en tenant compte la gestion de l'état des liens grâce aux protocoles de routage tels que l'OSPF (Open Shortest Path First) et IS-IS (Intermediate System to Intermediate System Protocol), contrôle et gestion des routes à l'aide du protocole RSVP (Ressource reSerVation Protocol) ainsi que la protection des liens.

Nous allons adopter deux architectures différentes à savoir, le modèle Pair à Pair et modèle Amélioré pour tester notre plan de contrôle du GMPLS, appliqué sur trois villes algériennes : Alger, Oran et Constantine, dont une comparaison détaillée entre les deux modèles sera élaborée afin d'illustrer la meilleure tout en gardant une haute qualité de service QoS.
Mot clés : WAN ; Plan de contrôle ; MPLS, GMPLS, LSP, LSR ; RSVP-TE ; OSPF-TE.

Summary

GMPLS is an extension of MPLS (Multi-Protocol Label Switching) that allows Label Switched Routers (LSRs) to support various types of switching, including packets, TDM (SDH/SONET), lambdas (Wavelengths), and Optical Fibers. In order to control components outside the standard network layer, a common control plane has been developed for GMPLS. This control plane enables full control of network equipment.

The purpose of this thesis is to conduct a detailed study of control plane management, taking into account link state management through routing protocols such as OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System Protocol), control and management of routes using the RSVP (Resource ReSerVation Protocol), as well as link protection.

We will adopt two different architectures, namely the modèle Pair à Pair and modèle Amélioré, to test our GMPLS control plane applied to three Algerian cities: Algiers, Oran, and Constantine. A detailed comparison between the two models will be elaborated to illustrate the better one while maintaining a high quality of service (QoS).
Keywords : WAN ; Control Plane ; MPLS ; GMPLS ; LSP ; LSR ; RSVP-TE ; OSPF-TE.

ملخص

يعد GMPLS امتدادًا لبروتوكول MPLS (Multi-Protocol Label Switching) الذي يتيح لموجّهات التبديل ذات العلامات (Label Switched Router)دعم أنواع متعددة من التبديل، بما في ذلك الحزم، وTDM (SDH/SONET)، واللامبدا (الطول الموجي)، والألياف البصرية. ومن أجل التحكم في المكونات خارج المعيار الخاص بطبقة الشبكة، تم تطوير خطة تحكم مشتركة لـ GMPLSتسمح بالتحكم الكامل في معدات الشبكة.

تهدف هذه المذكرة إلى إجراء دراسة مفصلة لإدارة خطة التحكم، مع مراعاة إدارة حالة الروابط باستخدام بروتوكولات التوجيه مثل OSPF (Open Shortest Path First) وIS-IS (Intermediate System to Intermediate System Protocol)، والتحكم وإدارة المسارات باستخدام بروتوكولRSVP (Resource ReSerVation Protocol) ، بالإضافة إلى حماية الروابط.

في هذه المذكرة، سيتم اعتماد نموذجين مختلفين، وهما نموذج النظير ونموذج التعزيز لاختبار خطة التحكم لـGMPLS ، وتطبيقها على ثلاث مدن جزائرية وهي الجزائر العاصمة، وهران وقسنطينة. سيتم إعداد مقارنة مفصلة بين النموذجين لتوضيح الأفضلية مع الحفاظ على جودة عالية للخدمة .(QoS)
الكلمات المفتاحية: WAN ; Control Plane ; MPLS ; GMPLS ; LSP ; LSR ; RSVP-TE ; OSPF-TE.