Université Kasdi Merbah Ouargla

Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'Informatique des Technologies de l'Information

Mémoire

MASTER PROFESSIONNEL

Domaine : Mathématique et informatique

Filière : Informatique

Spécialité : Réseau Convergence et Sécurité

Présenté par : Guemmoula lazhar
Douib larouci

Thème

La sécurité dans les réseaux MPLS basés sur la commutation par étiquette

Soutenu publiquement en : 29/06/2017

Devant le jury :

Mr DJIDIAI Hmida (président)	Université Kasdi Merbah
Mr BOUHANI A.Elkader (Examinateur)	Université Kasdi Merbah
Mr MAHDJOUB M.Bachir (Encadreur)	Université Kasdi Merbah

Année universitaire: 2016/2017

Sommaire

Liste des Figures :

Remerciements

Nous remercions DIEU le tout puissant, maître des cieux et de la terre, qui nous a éclairé le chemin et permis de mener à bien ce travail.

Tout d'abord nous tenons surtout à adresser nos plus vifs remerciements à M. MAHDJOUB MOHAMED BACHIR, qui nous a permis de réaliser ce travail sous sa direction. Nous n'oublierons jamais ses conseils judicieux.

Un merci pour tous mes enseignants qui nous a Permis de travailler dans un environnement Sain et paisible.

Aux membres du jury pour avoir accepté d'évaluer notre travail. Un grand merci à toutes les personnes qui nous ont soutenues de près ou de loin au cours de la réalisation de ce travail.

Dédicaces

A ma mère et mon père que DIEU les gardent.

A mes sœurs, et mon frère.

A tous ceux qui m'aime

A Mon binôme qui est vraiment considéré comme mon frère

A tous ceux qui sont proches de mon cœur.

A tous mes amies.

larouci

Dédicaces

A ma mère et mon père que DIEU les gardent.

A mes sœurs, mes frères, et ma famille.

Ma femme, qui a toujours m'encourage pour réussir dans mes études.

Mes enfants qui me donnent tous joie et bonheur à ma vie

Mon binôme qui est vraiment considéré comme mon frère

A tous ceux qui m'aime

A tous ceux qui sont proches de mon cœur.

A tous mes amis.

lazhar

Résumé

MPLS (**M**ulti **P**rotocol **L**abel **S**witching) spécifié des mécanismes pour gérer les flux de trafic de différentes granularités, telles que les flux entre les différents matériels, machines, ou même flux entre les différentes applications, Indépendante des protocoles de couche 2 et 3, et offre un moyen pour mapper des adresses *IP* aux étiquettes simples, de longueur fixe utilisée pour le transfert de paquets en utilisant des technologies de commutation de paquets différents.

L'une des façons de protéger l'infrastructure du MPLS est de séparer les ressources utilisées par les services MPLS, des ressources utilisées à d'autres fins. Dans un réseau MPLS, il est possible de séparer les ressources utilisées pour le plan de commande de celles utilisées pour le plan de données. Cela signifie que les ressources de ce dernier peuvent être protégées et isolées physiquement de tout autre équipement pour protéger les données des utilisateurs tandis que le plan de commande utilise les ressources du réseau qui peuvent être consultées par les opérateurs pour configurer le réseau.

Dans notre travail nous avons fournit un aperçu général sur les réseaux NGN, sur les réseaux MPLS, sa structure, son architecture, ainsi que les différentes fonctionnalités qu'il assure, nous avons présenté aussi la tolérance aux fautes et la sécurité dans un réseau MPLS ainsi ses principales composants, les défaillances, les différents mécanismes et techniques de récupération utilisés pour protéger l'infrastructure MPLS des pannes, ensuite s'articuler aux travaux connexes sur le rétablissement de l'échec et la tolérance aux pannes dans les réseaux MPLS, la sécurité MPLS et les principales questions de sécurité avec différentes attaques, mécanismes et techniques de sécurité MPLS, étude de cas du BackBone Network IP MPLS de télécommunication.

Mots clés : MPLS (Multiprotocol Label Switching), sécurité, liaison, transmission, routage, adresse IP, routeurs, paquet, étiquette

Abstract

MPLS (**M**ulti **P**rotocol **L**abel **S**witching) specified mechanisms to manage traffic flows of different granularities, such as flows between different hardware, machines, or even flow between different applications, independent of layer 2 and 3 protocols, and offers a means to map IP addresses to simple, fixed-length labels used for packet forwarding using different packet switching technologies.

One way to protect the MPLS infrastructure is to separate the resources used by MPLS services from resources used for other purposes. In an MPLS network, it is possible to separate the resources used for the control plane Of those used for the data plan. This means that its resources can be protected and physically isolated from any other equipment to protect user data while the control plane uses network resources that can be accessed by operators to configure the network.

In our work we have provided a general overview of NGN networks, MPLS networks, structure, architecture, fault tolerance and security in an MPLS network and its functionalities. Main components,

failures, recovery mechanisms and techniques used to protect the MPLS infrastructure from failures, and related work on failure recovery and fault tolerance in MPLS networks, MPLS security and Main security issues with different attacks, mechanisms and security techniques MPLS, case study of the BackBone Network IP MPLS telecommunication.
Keywords: MPLS (Multiprotocol Label Switching), security, link, transmission, routing, IP address, routers, package, tag

الملخص

يقوم متعدد البروتوكولات بإدارة التدفقات مختلفة الحجم، مثل التدفقات بين الأجهزة المختلفة، والآلات، أو حتى التدفق بين التطبيقات المختلفة، بشكل مستقل عن بروتوكولات الطبقة 2 و3 ، ويوفر وسيلة للتعيين بدل عناوين IP باستعمال علامات بسيطة، ذات طول ثابت مستخدمة في إعادة توجيه الرزم باستخدام تكنولوجيات مختلفة لتحويل الرزم.

إحدى الطرق لحماية البنية التحتية لمتعدد البروتوكولات هي فصل الموارد المستعملة من قبل خدمات متعدد البروتوكولات عن الموارد المستعملة لأغراض أخرى. وفي شبكة متعدد البروتوكولات، يمكن فصل الموارد المستخدمة لمستوى التحكم عن تلك المستخدمة في خطة البيانات. وهذا يعني أن مواردها يمكن حمايتها وعزلها عن أي معدات أخرى لحماية بيانات المستخدم في حين أن مستوى التحكم يستخدم موارد الشبكة التي يمكن الوصول إليها من قبل المشغلين لتكوين الشبكة.

وقد قدمنا في عملنا هذا لمحة عامة عن شبكات الجيل الجديدNGN وشبكات MPLS وهيكلها وهندستها، والأمان في شبكةMPLS ووظائفها. كذلك المكونات الرئيسية وتحمل الاخطاء وآليات الاسترداد والتقنيات المستخدمة لحماية البنية التحتيةMPLS من الاعطاب، والأعمال ذات الصلة على شبكات , MPLS والقضايا الأمنية الرئيسية مع الارتدادات المختلفة والآليات وتقنيات الأمن ، دراسة حالة الشبكة الحلقية الرئيسية للاتصالات.IP MPLS

كلمات مفتاحية: (متعدد البروتوكولات تسمية التبديل)، الأمن، صلة، نقل، والتوجيه، عنوان IP، الموجهات، حزمة، العلامة

INTRODUCTION GENERALE

Au cours de ces dernières années, Internet a évolué et a inspiré le développement de nouvelles variétés d'applications. Ces applications ont des besoins garantissant en termes de bande passante et de sécurité de service. En plus des données traditionnelles, Internet doit maintenant transporter voix et données multimédia. Les ressources nécessaires pour ces nouveaux services, en termes de débit et de bande passante, ont entraîné une transformation de l'infrastructure d'Internet. Cette transformation du réseau, d'une infrastructure par paquets à une infrastructure en cellules.

L'augmentation de la connectivité des réseaux et l'intégration de plusieurs services dans un même système de communication (intégration de voix et données, téléphonie mobile, développements de la téléphonie sur plates-formes IP, etc.) a engendré une croissance significative de la complexité du métier de concepteur d'architectures de réseaux.

D'une part, sur des aspects de dimensionnement matériel puisque les structures de communication doivent fédérer un nombre croissant de points de raccordement. D'autre part, la convergence des médias où l'on cherche à faire passer sur un même support physique les données, la voix, la vidéo, entraîne l'ajout de nouveaux équipements.

Avec l'évolution rapide des technologies de transports à haut débit, il devient évident qu'ATM n'est plus une solution d'avenir pour les réseaux IP, car il est difficile d'intégrer d'autres technologies dans une signalisation ATM, lorsque le débit augmente et qu'on ne sait plus construire de cartes capables de segmenter et de réassembler des paquets en cellules à la vitesse des liens. MPLS est donc une solution prometteuse parce qu'elle permet d'intégrer très facilement de nouvelles technologies dans les réseaux existant.

La sécurité dans les réseaux MPLS basés sur la commutation par étiquette est le projet de fin d'étude que nous avons développé dans ce mémoire, qui est axé sur les trois chapitres suivants :

Le premier chapitre est une introduction aux réseaux de nouvelle génération (NGN) comme un bon exemple des réseaux basés sur le MPLS.

Le chapitre suivant Survol sur les réseaux MPLS

Le troisième chapitre est une présentation des Tolérances aux fautes et Sécurité dans MPLS, et étude de cas du BackBone Network IP MPLS de télécommunication.

Chapitre I :Les Réseaux de Nouvelle Génération-NGN (Next Generation Network)

1. Introduction :

L'émergence des solutions mobiles alliées aux nouvelles technologies d'accès (fibre optique, DSL...), ainsi que la poursuite sans fin de la capacité et de l'efficacité du réseau à amener les opérateurs à la recherche d'alternatives pour leurs infrastructures existantes et cela pour répondre à la demande accrue de réduction des coûts et amélioration de la sécurité, à faire évoluer leurs réseaux fixes ou mobiles d'une technologie basée sur la commutation de circuits à une technologie reposant sur la commutation de paquets. Compte tenu des réalités de l'industrie de la communication, tels que l'explosion du trafic IP, et la convergence des réseaux, en 2004 l'*UIT-T* a proposé un concept innovant pour les réseaux futurs: Les *réseaux de la prochaine génération* dite aussi *Réseaux de Nouvelle Génération* (*NGN* ou *Next Generation Network* en anglais).

Cette première partie s'oriente vers l'introduction de notre mémoire qui fournit des informations de base sur les réseaux *NGN*, en abordant une description générale du concept de *NGN*, leurs caractéristiques et les différents types constituant ce réseau, une présentation de son architecture fonctionnelle suivi par la description concise de certaines technologies de base nécessaires à la réalisation de l'infrastructure *NGN* envisagée. Ainsi que les différents services offerts par cette technologie.

2. Définition du NGN (Next Generation Network) :

Un Réseau de Nouvelle Génération est un réseau à base de paquets qui peut être utilisé pour la téléphonie et les données à la fois, et qui supporte la mobilité. Initialement, le terme *Next Generation Network* a été utilisé pour se référer à la transformation du réseau de base IP. Parfois, un *NGN* est appelé un *réseau tout-IP*.

L'*International Telecommunication Union* (*ITU*) a défini un *NGN* comme : un réseau capable de fournir les services de télécommunication aux utilisateurs et en mesure de faire usage de la large bande multiples à base de paquets, technologies QoS de transport et dans lequel les fonctions liées aux services sont indépendantes des technologies liées au transport sous-jacentes. Il permet un accès illimité pour les utilisateurs aux réseaux et aux prestataires et aux services de leur choix. Il prend en charge la mobilité généralisée qui permet la fourniture cohérente et partout de services aux utilisateurs [1].

3. Caractéristiques du NGN :

Les réseaux NGN sont définis sur la base de leur technologique sous-jacent, comme il est mentionné dans la définition de l'ITU. Les caractéristiques du NGN peuvent avoir un impact sur les modèles d'affaires et de

la structure du marché traditionnel, ainsi que sur la réglementation [2]. Parmi les principales caractéristiques nous allons citer :

3.1. Réseaux basé IP:

Les réseaux *NGN* couvrent généralement la migration à partir de plusieurs réseaux de base existants à des réseaux IP pour fournir tous les services. Cela signifie que toutes les informations sont transmises par l'intermédiaire des paquets. Les paquets peuvent prendre des routes différentes pour la même destination, et par conséquent, ne nécessite pas la création d'un chemin dédié de bout en bout comme dans le cas de communications *PSTN*.

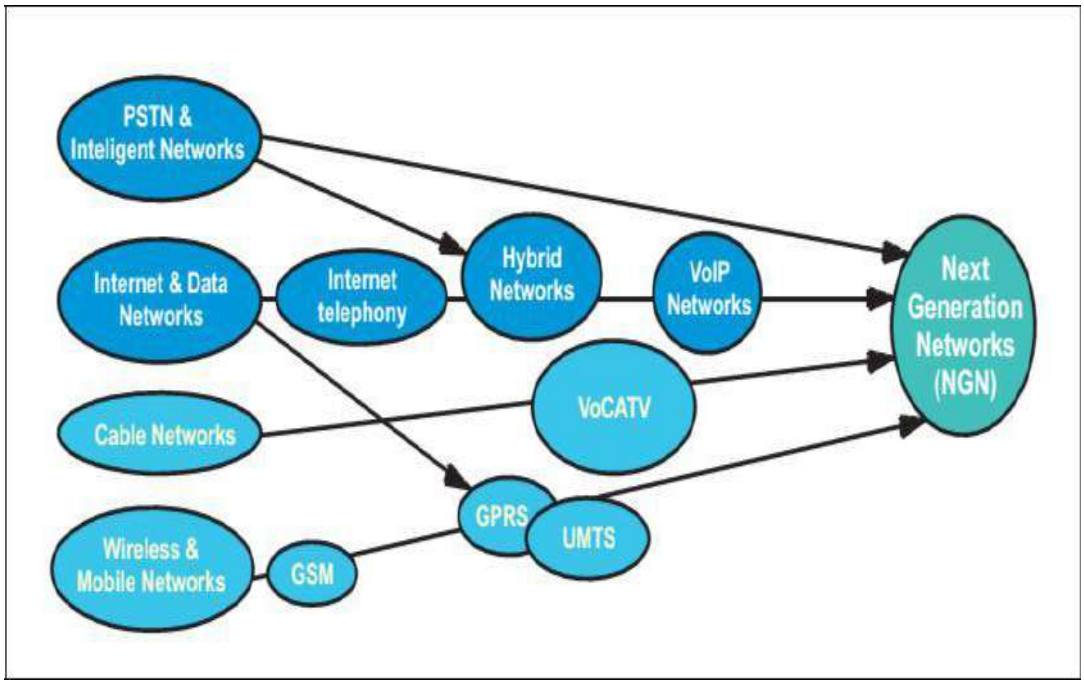

Figure1. 1 MIGRATION VERS LE NGN [3]

3.2. Réseaux basé paquets, à usage multiples:

Alors que les réseaux traditionnellement distincts sont utilisés pour fournir une voix, des applications de données et de vidéo, chacune nécessitant des dispositifs d'accès distincts. Différents types de *NGN* applications peuvent être transformés en paquets, étiquetés et livrés simultanément sur un certain nombre de différentes technologies de transport, permettant le passage de réseaux à usage unique (un réseau, d'un service), aux réseaux à usage multiple (un réseau, de nombreux services).

3.3. La séparation de la couche de transport et de service:

Elle constitue le facteur commun essentiel entre *NGN* et la convergence, ce qui porte sur le changement radical dans la relation entre les couches de réseau (Infrastructures de transport, les services de transport et de contrôle, les services de contenu et applications). Dans prochaine fonctions liées aux services réseaux de nouvelle génération sont indépendants de sous-jacente liée aux technologies de transport (Figure 1.2). Le découplage des applications et réseaux permet aux applications être définis directement au niveau de service et fourni de façon transparente sur différentes plates-formes, ce qui permet pour l'entrée sur le marché des fournisseurs de services (*Service Provider –SP-*) multiples sur une base non discriminatoire.

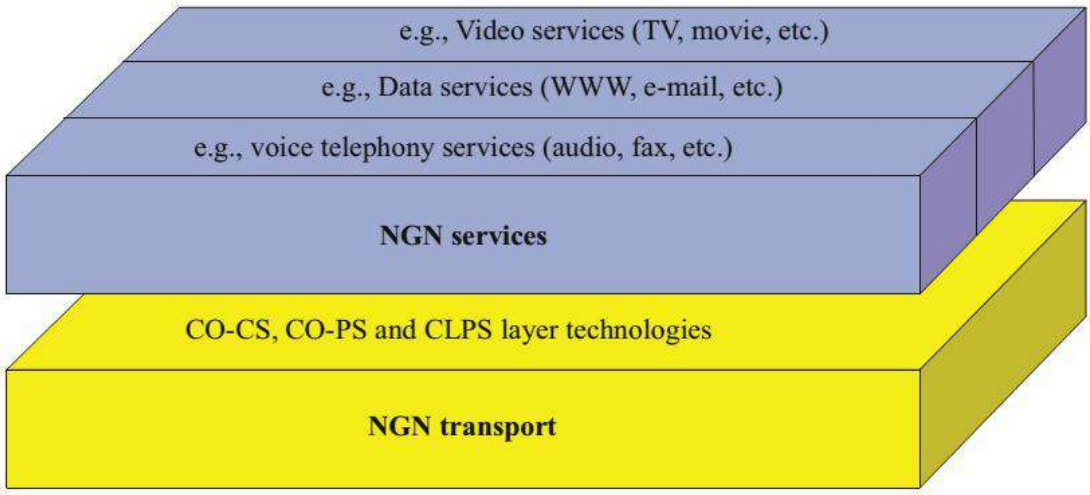

Figure1. 2 SÉPARATION DES PLANS FONCTIONNELS SOURCE: NEXT GENERATION NETWORKS ARCHITECTURE by ITU-T

4. Types du NGN :

Il existe trois types de réseau *NGN* sont : *NGN class 4, NGN Class 5* et *NGN Multimédia* [4]. Nous allons les introduire en détails dans cette section:

4.1. Les NGN Class 4 et Class 5:

Les *NGN Class 4* et *Class 5* sont des architectures de réseau offrant uniquement les services de téléphonie. Il s'agit donc de *NGN téléphonie*.

Dans le *RTC*, un commutateur class 4 est un centre de transit. Un commutateur class 5 est un commutateur d'accès aussi appelé centre à autonomie d'acheminement. Le NGN class 4 (respectivement, NGN class 5) émule donc le réseau téléphonique au niveau transit (respectivement, au niveau accès) en transportant la voix sur un mode paquet.

4.2. Le NGN Multimédia:

Le *NGN Multimédia* est une architecture offrant les services multimédia (ex. messagerie vocale/vidéo, conférence audio/vidéo) puisque l'usager a un terminal IP multimédia. Cette solution est plus intéressante que les précédentes puis qu'elle permet à l'opérateur d'innover en termes de services par rapport à une solution *NGN téléphonie* qui se cantonne à offrir des services de téléphonie.

Le *NGN Class 4* permet :

Le remplacement des centres de transit téléphoniques (*Class 4 Switch*). La croissance du trafic téléphonique en transit.

Le *NGN Class 5* permet :

Le remplacement des centres téléphoniques d'accès (*Class 5 Switch*). La croissance du trafic téléphonique à l'accès.

La voix sur DSL/ Voix sur le câble. Le *NGN Multimédia* permet de :
Offrir des services multimédia à des usagers disposant d'un accès à large bande tel que xDSL, câble, Wi-Fi / WiMax, EDGE /UMTS, etc.

5. Les deux grandes familles de réseaux NGN:

Avant d'entamer l'architecture *NGN*, nous allons d'abord introduire les deux grandes familles de réseaux: les *réseaux sans signalisation* et les *réseaux avec signalisation*.

5.1. Les réseaux sans signalisation:

Les *réseaux sans signalisation* vont d'une communication simple d'individu à individu jusqu'à Internet. L'information est véhiculée dans des paquets, qui portent l'adresse complète du destinataire, de telle sorte que ces paquets se suffisent à eux-mêmes pour atteindre ce dernier [5].

5.2. Les réseaux avec signalisation:

Les réseaux avec signalisation sont nombreux dans le monde des télécommunications. Le premier d'entre eux est le réseau téléphonique, où la gestion de la signalisation par des opératrices ayant été remplacée par une signalisation automatique par la suite, utilisant le protocole *CCITT n° 7*, les réseaux à commutation de type *X.25* puis *Frame Relay* et *ATM* proviennent d'idées émanant du secteur des télécommunications.

Dans un réseau avec signalisation, aucune information ne peut transiter d'un émetteur vers un récepteur tant que la communication n'a pas été signalée au récepteur. Dans pratiquement tous les cas, on profite de

la signalisation pour mettre en place dans le réseau un chemin, sur lequel des ressources peuvent être réservées [5].

Dans chacune de ces familles, deux grandes possibilités s'offrent aux architectes réseau, ce qui donne quatre architectures.

6. Architectures NGN:

Les quatre architectures possibles pour réaliser le *NGN* sont illustrées dans la figure ci-dessous [5] :
La partie haute de la figure regroupe les deux possibilités de la famille sans signalisation, le *surdimensionnement* et les *priorités*. Alors que, la partie basse regroupe celles de la famille avec signalisation, le chemin *MPLS/GMPLS* et le *contrôle par des signalisations* provenant du monde de l'informatique, notamment *SIP (Session Initiation Protocol)*.

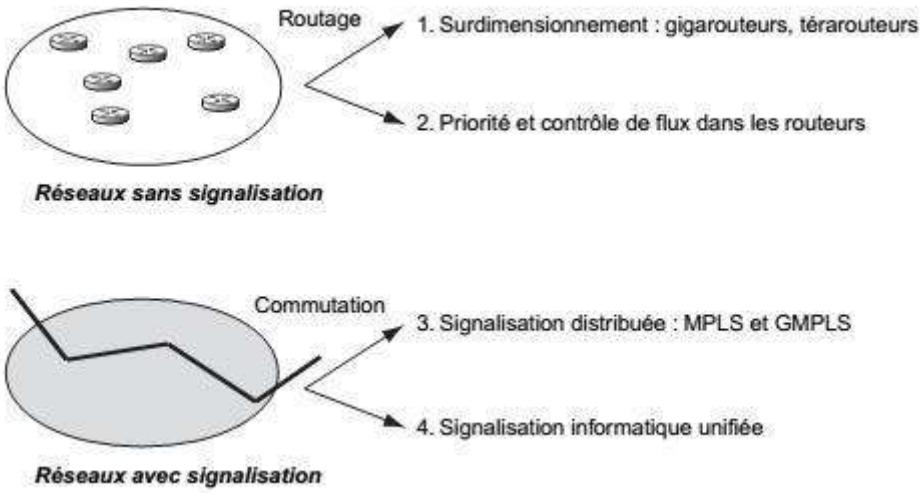

Figure1. 3 LES QUATRE ARCHITECTURES DU NGN [5]

6.1. Le surdimensionnement :

La première de ces solutions concerne un réseau IP natif dans lequel les artères du réseau ainsi que les nœuds de transfert, les routeurs dans le cas présent, sont surdimensionnés. Cette possibilité est réaliste puisque les progrès technologiques depuis le début des années 2000 conduisent à un débit des tuyaux de communication qui augmente plus vite que la demande des utilisateurs. Les routeurs suivent le même chemin avec les gigarouteurs et même les térarouteurs dans lesquels un million voire un milliard de paquets peuvent être routés chaque seconde. En 2004, la capacité totale des réseaux était utilisée approximativement à 50 % au moment des pointes de trafic. Le surdimensionnement est assez couramment utilisé mais son coût est élevé. En effet, les équipements de transmission permettant de dépasser le gigabit par seconde ce qui restent très chers.

6.2. Les priorités :

Avec routage, une seconde solution s'est mise en place à partir de l'idée suivante : au lieu de surdimensionné le réseau pour l'ensemble des utilisateurs, pourquoi ne pas le surdimensionné uniquement pour les applications qui ont besoin d'une forte qualité de service ? En adoptant un environnement avec priorités et en limitant le nombre de flots utilisant la plus haute priorité, les clients prioritaires auront l'impression d'avoir un réseau surdimensionné, comme s'il leur était quasiment dédié, et obtiendront en conséquence une très bonne qualité de service.

Cette solution nécessite qu'il n'y ait pas de congestion pour les clients les plus prioritaires et impose donc de trouver un moyen de limiter le nombre de ces derniers. La solution la plus souvent évoquée consiste à imposer aux clients prioritaires un tarif suffisamment dissuasif pour que leur nombre soit limité. On avance la valeur de 15 % de l'ensemble des ressources d'un réseau affectées aux clients prioritaires. Cette valeur provient de modèles mathématiques, qui montrent que la probabilité de congestion dans les moments de pointe reste négligeable.
Une architecture *NGN* pourrait consister à choisir une technologie IP native avec une gestion des priorités de type *DiffServ* en limitant le nombre de clients dans la classe Premium ou *EF* (*Expedited Forwarding*).

6.3. MPLS-GMPLS :

Dans les réseaux avec signalisation, une première solution provient de *MPLS-GMPLS*, présentée en détail au chapitre 2. Elle revient à tracer des circuits virtuels, ou *LSP* (*Label Switched Path*), sur lesquels circulent des paquets IP encapsulés dans différents types de trames, mais plus spécifiquement ATM et Ethernet. L'avantage de cette solution est l'ingénierie de performance qu'on peut lui appliquer, permettant de bien dimensionner les chemins.

Les extensions *GMPLS* avec des commutations diverses, comme les commutations en longueur d'onde. Y'en d'autre innovation, concerne la *commutation par éclat (*ou *burst-switching* en anglais*)*, c'est-à-dire par un ensemble de paquets représentant une transmission de quelques dizaines de millisecondes. Cette solution peut se placer entre la commutation de paquets et la commutation en longueur d'onde.

L'idée est de commuter un ensemble de paquets sur un chemin mais pour une durée non pas de quelques nanosecondes mais, comme nous venons de l'indiquer, de quelques dizaines de millisecondes. La commutation d'un seul paquet demande en effet beaucoup de temps de supervision puisqu'il faut modifier les chemins de chaque paquet.

Dans une commutation en longueur d'onde, la bande passante est très mal utilisée puisque les applications travaillent aveuglement. La *commutation par éclat* est un bon compromis entre ces deux techniques, qui se

rapproche de la commutation de paquets lorsque les éclats sont très courts et de la commutation en longueur d'onde lorsqu'ils sont très longs.

6.4. La signalisation informatique unifiée:

Dans le cas de *MPLS/GMPLS*, la signalisation est essentiellement due à la mise en place d'un chemin, le *LSP* (*Label Switched Path*). Le futur s'intéresse aussi à la convergence des applications afin qu'elles puissent s'exécuter aussi bien sur les réseaux fixes que mobiles. L'utilisation de la signalisation applicative *SIP* a déjà été introduite pour *l'IMS* (*IP Multimédia Subsystem*), qui marque la convergence fixe/mobile.

7. Services du NGN :

Une variété de services, ont été liée aux initiatives *NGN*, parmi ces services fournis nous citons [6] :

- **Services de ressources spécialisées**: par exemple, la fourniture et la gestion des transcodeurs, ponts multimédia, multipoint de conférence, des unités de conversion de médias, unités de reconnaissance vocale, etc.

- **Services de traitement et de stockage**: par exemple, la fourniture et la gestion du stockage de l'information, unités pour la messagerie, serveurs de fichiers, serveurs de terminaux, plates-formes de système d'exploitation, etc.

- **Services de middleware** : par exemple, le courtage, la sécurité, les licences, les transactions, etc.

- **Services spécifiques à l'application** : par exemple, des applications d'entreprise, les applications e-commerce, la chaîne d'approvisionnement des applications de gestion, jeux vidéo interactifs, etc.

- **Services de fourniture de contenu qui fournissent de l'information ou du contenu de courtier** : par exemple, la formation électroniques, les services d'information de poussée, etc.

- **Interfonctionnement des services :** pour les interactions avec d'autres types d'applications, de services, réseaux, protocoles ou formats (par exemple, traduction EDI).

- **Services de gestion :** à entretenir, exploiter et gérer les communications / informatique réseaux et services.

8. Le protocole Internet (Internet Protocol IP) NGN :

NGN tente de redéfinir l'infrastructure de réseau basé sur l'Internet actuel et des réseaux *RTPC* / *RNIS*, par conséquent, en tant que protocole de réseau dominant dans le monde, le protocole Internet est sélectionné en tant que protocole de réseau pour acheminer des données et fournir des services / applications de la périphérie du réseau à l'âme dans un *NGN* infrastructure.

Actuellement, il existe deux méthodes de base utilisées pour transmettre des données: *commutation de circuits* et *commutation de paquets*.

8.1. Commutation de circuits:

Dans un réseau de commutation de circuits, comme *RTC / RNIS*, le système décide puis établit le chemin (circuit) pour la transmission de données, ce chemin est toujours en service, dédié et exclusif, et ne sera pas fermé jusqu'à la conversation se termine. Ainsi, l'ensemble du message est transmis entre deux nœuds par une voie dédiée dans l'ordre et avec un débit binaire constant [7].

8.2. Commutation de paquets :

Dans un réseau de commutation de paquets, les données sont encapsulées dans de petits segments appelés *paquets* par le protocole réseau utilisé. Chaque paquet contient des données utiles et liées à des informations de contrôle, et se déplace grâce à des itinéraires identiques ou différents. Au nœud destination, les paquets reçus sont remonté par le protocole de réseau en constituent les données d'origine à nouveau. Cependant, il est noté qu'il existe deux types de réseaux à commutation de paquets: *sans connexion et orienté connexion* [7]**.**

8.2.1. Commutation de paquets sans connexion :

Les paquets encapsulé par les protocoles sans connexion comme IP, qui sont appelés *datagramme*, contient les informations sur leurs source et destination. Un datagramme peut trouver leur propre route vers la destination, en acheminons des voies différentes, ce que peut entraîner dans différents retards.

8.2.2. Commutation de paquets orienté connexion :

La commutation de paquets orienté connexion est également appelé *commutation de circuits virtuelle (virtual circuit switching)*, pour émuler la commutation de circuits dans des réseaux de commutation de paquets afin de combiner le meilleur de ces deux types de réseaux. Similaire à commutation de circuits, un réseau de commutation de circuit virtuel établie une connexion avant que la transmission des données commence, et les paquets sont livrés dans l'ordre par cette voie dédiée, mais ses débits pourraient être différents. Les exemples pour la commutation de circuit virtuel comprennent : *ATM*, *TCP*, et *MPLS* [8] [9].

MPLS, a été conçus pour transporter à la fois des données pour les nœuds de commutation de circuits et pour les nœuds de commutation de paquets. *MPLS* est un élément important permettant aux services *NGN* en fournissant des réseaux basés sur IP [10]. En vira en détails le fonctionnement et les techniques de MPLS dans le chapitre 2.

9. Conclusion :

Ce chapitre fournit un aperçu général sur les réseaux *NGN*. Le concept de *NGN* reflète la tendance future de la convergence des réseaux dans l'industrie des télécommunications, et répond aux exigences de la télécommunication industrielle sur les réseaux futurs en redéfinissant l'architecture du réseau de manière significative pour réduire les coûts opérationnels ainsi que pour améliorer la capacité du réseau à fond. Les *NGN* offrent les capacités, en termes de protocole, de gestion, et d'infrastructure pour déployer et créer de nouveaux services multimédia en mode paquet sur les réseaux.

En bref, selon les initiatives de *l'UIT-T* et *Cisco, NGN* est un réseau IP basé sur des paquets conçus à fournir des services / applications intégrées sur une infrastructure de réseau commune. Il fournit un certain nombre de nouvelles fonctionnalités avancées ainsi que le maintien compatible avec les systèmes existants grâce à plusieurs technologies de base telles que le *MPLS* qui sera présenté en détails dans le chapitre suivant.

Chapitre II: Survol sur les réseaux MPLS

1. Introduction :

L'idée de *MultiProtocol Label Switching (MPLS)* vient d'un groupe d'ingénieurs d'*Epsilon Networks*, mais la technologie n'était prévue pour fonctionner que sur *ATM* ce qui limite sa place sur le marché. *Cisco System*, a proposé ensuite l'idée de ne pas limiter *MPLS* sur *ATM* par la création de "*Tag Switching*", qui sera ensuite renommé en "*Label Switching*", puis il est standardisé par *l'IETF* en tant que *MPLS*, qui utilise des étiquettes (références) attachées aux paquets réseau pour les transmettre à travers le réseau.

Ce chapitre représente une introduction à la technologie *MPLS*. Nous allons y trouver un bref aperçu des applications les plus importantes de *MPLS* ainsi que leur structure, architecture et fonctionnalités.

2. Définition du MPLS:

MPLS est un mécanisme de transport de données basé sur la commutation d'étiquettes, où les labels sont insérés à l'entrée du réseau MPLS et retirés à sa sortie. À la base, cette insertion s'opère entre la couche de liaison de données et la couche réseau afin de transporter des protocoles comme IP [11].

Les étiquettes *MPLS* sont annoncés entre les routeurs afin qu'ils puissent construire une cartographie étiquette à étiquette. Ces étiquettes sont attachées aux paquets *IP*, permettant aux routeurs de transmettre le trafic en regardant l'étiquette et non l'adresse *IP* de destination. Les paquets sont transmis par commutation d'étiquettes plutôt que par la commutation *IP* [12].

C'est pourquoi *MPLS* est qualifié de protocole de couche "2,5" comme il représenté dans la *figure 2.1*. Ce protocole a ensuite évolué pour fournir un service unifié de transport de données pour les clients en utilisant une technique de commutation de paquets. *MPLS* peut être utilisé pour transporter pratiquement tout type de trafic, par exemple la voix ou les paquets *IPv4*, *IPv6* et même les trames *Ethernet* ou *ATM* [11].

MPLS permet un déploiement à grande échelle pour acheminer différents types de trafic tout en respectant les contraintes de fonctionnement associées et sur une unique infrastructure illustrée dans la figure 2.1.

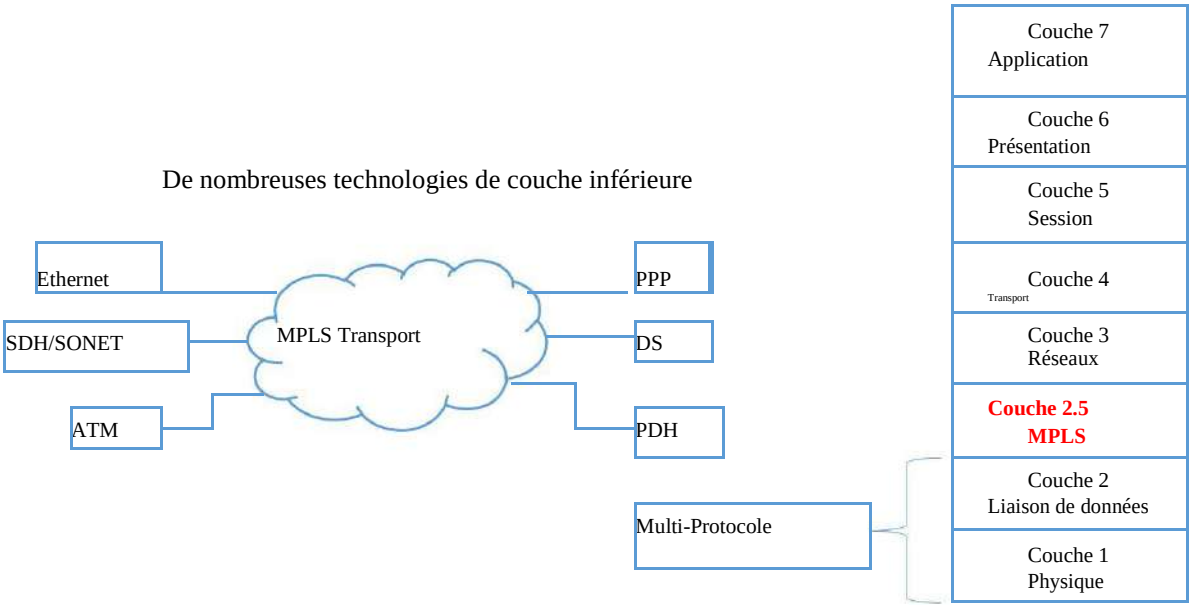

Figure 2. 1 POSITIONNEMENT DE MPLS DANS LE MODELE OSI

3. Caractéristiques MPLS :

MPLS est l'aboutissement logique de toutes les propositions qui ont été faites dans les années 1990. L'idée de l'*IETF* a été de proposer une norme commune pour transporter des paquets *IP* sur des sous-réseaux travaillant en mode commuté. Les nœuds sont des routeurs-commutateurs capables de remonter soit au niveau *IP* pour effectuer un routage, soit au niveau trame pour effectuer une commutation.

Les caractéristiques les plus importantes de la norme *MPLS* sont les suivantes [5]:

Spécification des mécanismes pour transporter des flots de paquets *IP* avec diverses granularités des flots entre deux points, deux machines ou deux applications. La granularité désigne la grosseur du flot, qui peut intégrer plus ou moins de flots utilisateur.

Indépendance du niveau trame et du niveau paquet, bien que seul le transport de paquets *IP* soit réellement pris en compte.

Mise en relation de l'adresse *IP* du destinataire avec une étiquette d'entrée dans le réseau.

Utilisation des protocoles de routage de type *OSPF* (*Open Shortest Path First*) et de signalisation comme *RSVP* (*Resource reSerVation* Protocol).

Utilisation de différents types de trames.

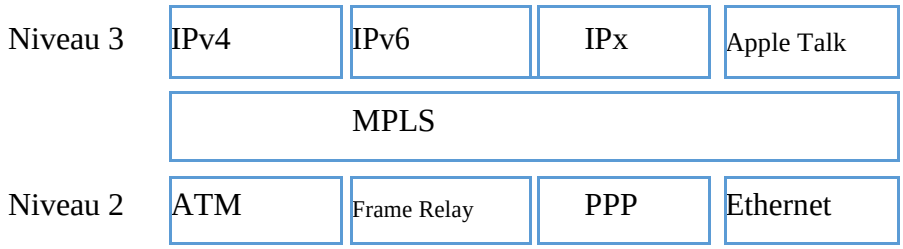

Figure 2. 2 L'INDÉPENDANCE DU MPLS DU NIVEAU TRAME ET DU NIVEAU PAQUET

Aussi nous pouvons citer quelques caractéristiques supplémentaires du *MPLS* qui méritent d'être soulignées :

- Assignation des étiquettes faite par le nœud qui émet un message vers le nœud destinataire.
- Granularité variable des étiquettes.
- l'ensemble des étiquettes géré selon la méthode « dernier arrivé premier servi ».
- Possibilité de hiérarchiser les demandes.
- Utilisation d'un temporisateur *TTL*.
- Encapsulation d'une étiquette dans la trame incluant un *TTL* et une qualité de service (*QoS).*

4. Terminologie MPLS :

Avant de rentrer dans les détails du MPLS, il est nécessaire de citer les éléments constituant un réseau MPLS :

4.1 FEC (Forwarding Equivalency Classes)

Dans MPLS, le routage s'effectue par l'intermédiaire de classes d'équivalence. Une classe représente un flot ou un ensemble de flots ayant les mêmes propriétés, notamment le même préfixe dans l'adresse *IP*.

Toutes les trames d'une *FEC* sont traitées de la même manière dans les nœuds du réseau *MPLS*. Elles sont introduites dans une *FEC* au nœud d'entrée et ne peuvent plus être distinguées à l'intérieur de la classe des autres flots [5].

4.2 L'étiquette MPLS (MPLS Label) :

Une étiquette *MPLS* est un court identifiant de longueur fixe qui permet d'identifier localement et d'une manière unique un seul *FEC*. Le format de l'étiquette *MPLS* est illustré dans la figure suivante [13]:

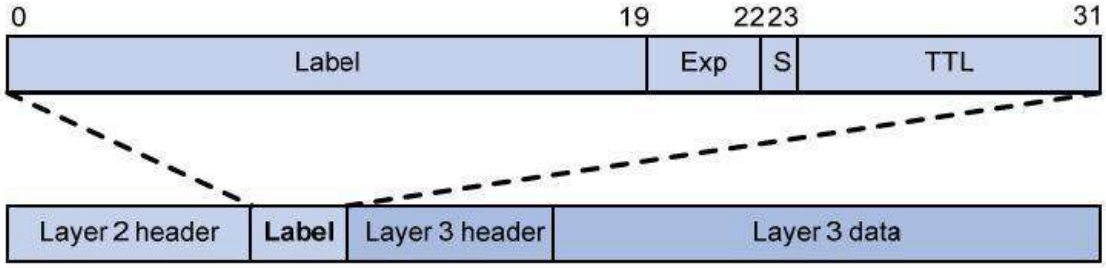

Figure 2. 3 FORMAT D'UNE ÉTIQUETTE MPLS

Comme le montre la figure ci-dessus, une étiquette *MPLS* est encapsulée entre l'en-tête d'un trame de couche 2 et l'en-tête d'un paquet de couche 3.

L'entête *MPLS* inclut les quatre champs suivants [13]:

Label : la valeur d'étiquette *MPLS* sur 20 bits.

Exemple : sur 3 bits, ils sont utilisés généralement pour définir la *classe de service (CoS)*, pour définir la *QoS*.

S : indique s'il y a empilement des étiquettes. Il mit à 1 pour l'entrée la plus ancienne dans la pile et à 0 pour toutes les autres entrées. C.-à-d. S = 1 lorsque le dernier étiquette de la pile est atteint.

Time To Live (TTL) : ce champ a le même rôle que le *TTL* de l'entête *IP*. Étant donné que l'entête *IP* n'est pas analysé par les *LSR*, la valeur du *TTL* est recopiée dans l'entête *MPLS* à l'entrée du réseau par *l'Ingress LER*. Ensuite, à chaque commutation par un *LSR*, le *TTL* est modifié. La valeur *TTL* de l'entête *MPLS* est ensuite recopiée dans l'entête *IP* à la sortie du réseau *MPLS* par *l'Egress LER*.

4.3. LSR (Label Switched Router) et LER (Label Edge Router):

Les nœuds qui participent à *MPLS* sont classifiés en *LER* et *LSR* :

4.3.1 Un routeur de commutation d'étiquettes (LSR)

Un routeur de commutation d'étiquettes, aussi appelé *Provider Router,* est un routeur dans le cœur du réseau et qui participe à la mise en place du circuit virtuel par lequel les trames sont acheminées.

4.3.2 Un routeur de bord d'étiquette (LER)

Un routeur de bord d'étiquette, aussi appelé *Provider Edge Router,* est un *LSR* qui se trouve sur le bord d'un réseau *MPLS* et qui est relié à un autre réseau, un nœud d'accès au réseau *MPLS*. Un *LER* peut avoir des ports multiples permettant d'accéder à plusieurs réseaux distincts, chacun pouvant avoir sa propre technique de commutation [5]. Les *LER* jouent un rôle important dans la mise en place des étiquettes. Nous distinguons deux types *LER* :

4.3.2.1 Ingress-LER (Ingress Label Edge Router) :

C'est un routeur se situant à l'entrée du réseau *MPLS* et dans lequel nous allons attribuer des étiquettes pour le flux arrivant du réseau du client.

4.3.2.2 Egress-LER (Egress Label Edge Router):

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

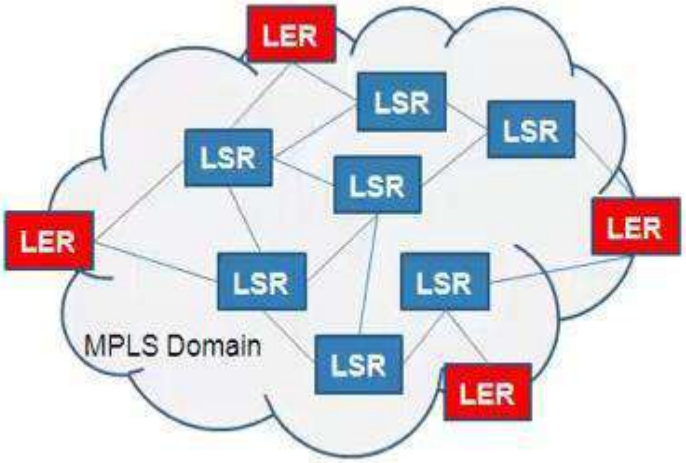

Figure 2. 4 LES NŒUDS QUI PARTICIPENT À MPLS : LSR ET LER

4.4 LSP (Label Switched Path) :

Un domaine *MPLS* est déterminé par un ensemble de nœuds *MPLS* sur lesquels sont déterminés les *FEC*.

Les *LSP* sont les chemins déterminés par les étiquettes positionnées par la signalisation. Donc, un chemin à commutation d'étiquettes (*LSP*) est le chemin duquel les paquets d'un *FEC* travers un réseau *MPLS* [5].

Un *LSP* est un chemin unidirectionnel de l'entrée à la sortie d'un réseau *MPLS*. Sur un *LSP*, dans le sens de transfert des paquets, deux *LSR* voisins sont appelés les *upstream LSR* and *downstream LSR* respectivement. Sur la *figure 2.5*, le *LSR* B est l'*upstream LSR* de *LSR* A et *LSR* A est le *downstream LSR* de *LSR* B.

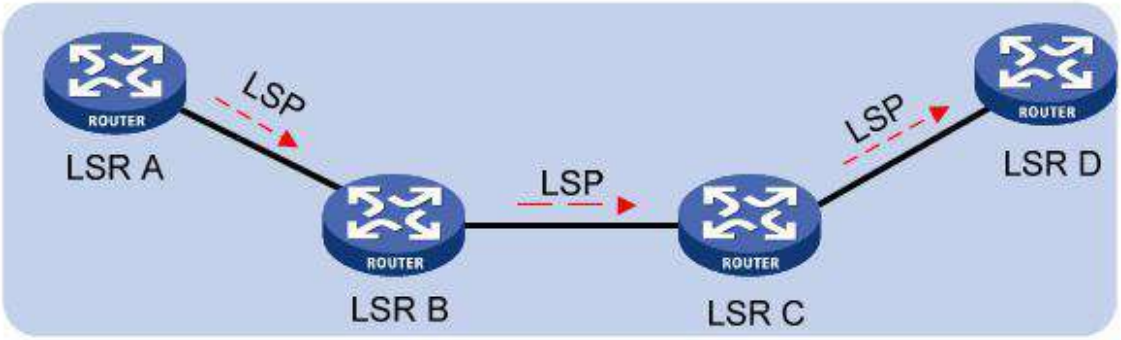

Figure 2. 5 DIAGRAMME POUR LSP

Les *LSP* sont déterminés sur un domaine avant l'arrivée des données dans le cas le plus classique. Deux options sont utilisées à cette fin [5] :

Le *routage saut par saut (hop-by-hop)* : Dans ce cas, les *LSR* sélectionnent les prochains sauts indépendamment les uns des autres. Le *LSR* utilise pour cela un protocole de routage comme *OSPF* ou pour des sous-réseaux de type *ATM*.

Le *routage explicite* (identique au routage par la source) : Dans ce cas, le *LER* d'entrée du domaine *MPLS* spécifie la liste des nœuds par lesquels la signalisation a été routée. Le choix de ce chemin pouvant avoir été contraint par des demandes de qualité de service. Le chemin suivi par les trames dans un sens de la communication peut être différent dans l'autre sens.

5. Structure MPLS :

Comme le montre la *figure 2.6*, l'élément essentiel d'un réseau *MPLS* est *LSR*. Les *LSRs* dans le même domaine de routage forment un domaine *MPLS*.

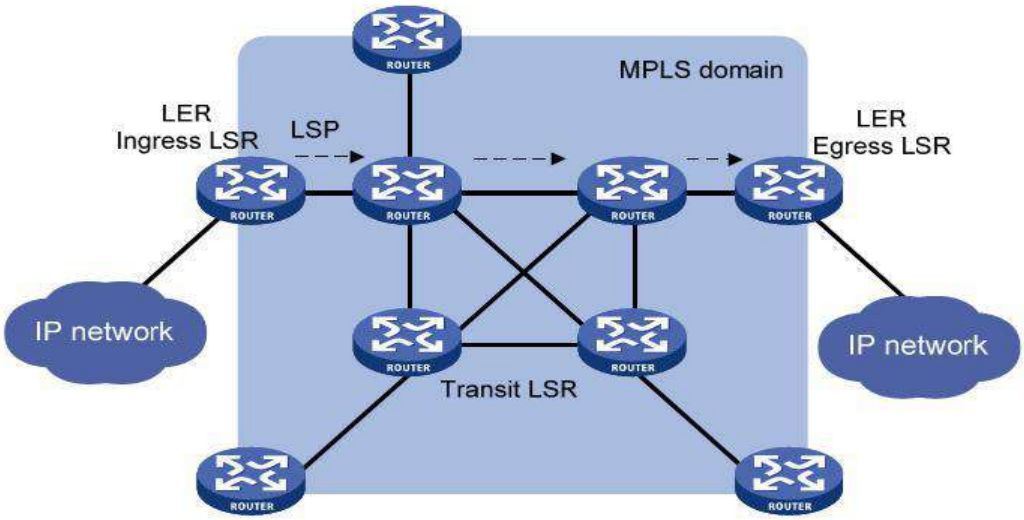

Figure 2. 6 DIAGRAMME POUR LA STRUCTURE D'UN RÉSEAUX MPLS

Un domaine *MPLS* comprend les types de *LSRs* suivants, comme il est illustré dans la *figure 2.7* :

LSR d'entrée (*Ingress LSR «Push »* : pour recevoir et étiqueter les paquets reçus dans le domaine de la technologie *MPLS*.

LSR de transit «Swap» : pour l'acheminement des paquets du *LSP* à leurs *LER* selon les étiquettes ;

LSR de sortie (Egress LSR « Pop» : pour enlever les étiquettes des paquets IP et les transmettre leurs réseaux destinations.

La figure suivante illustre ce mécanisme :

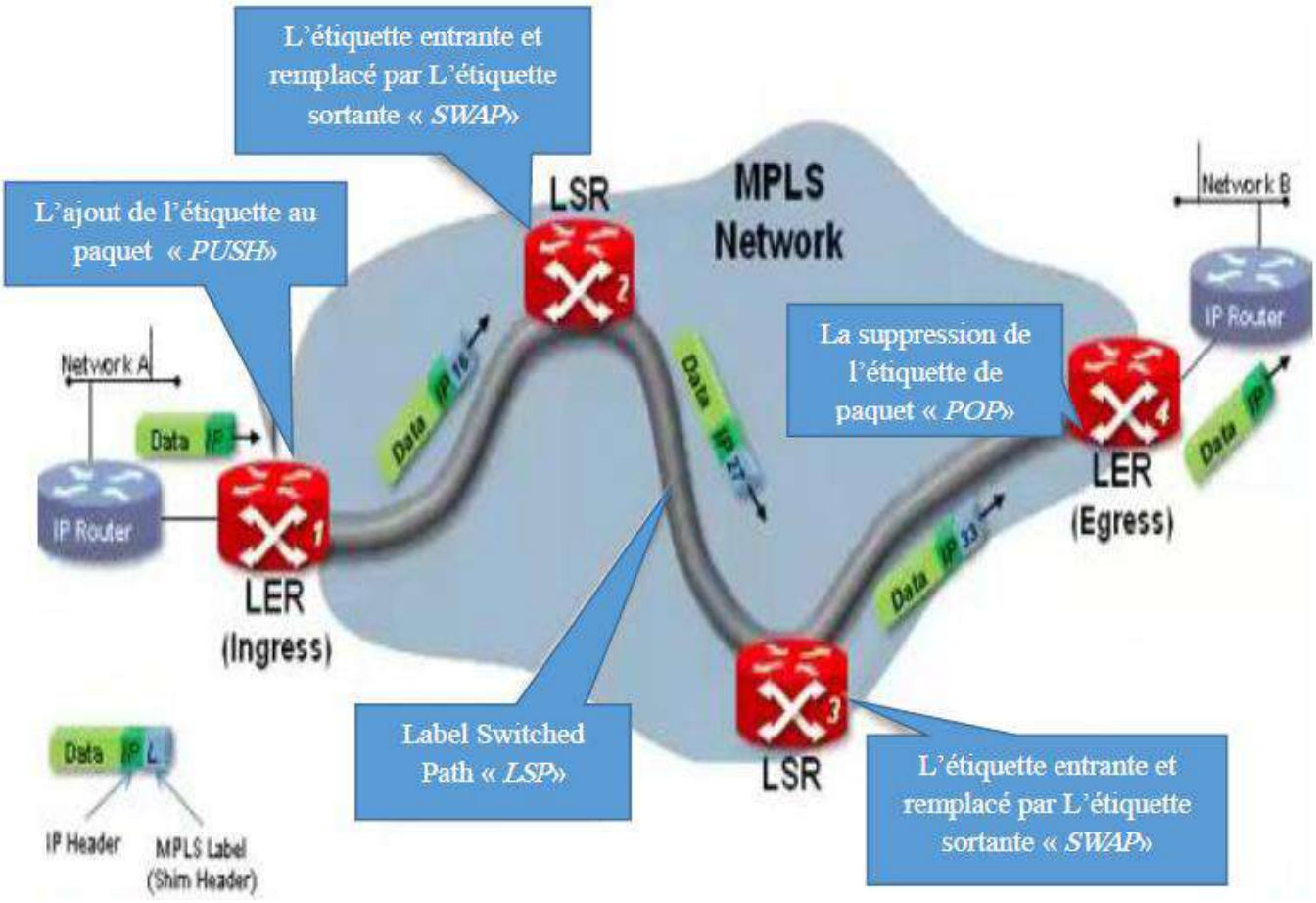

Figure 2. 7 TRAITEMENT DE LA COMMUTATION DANS LE CORE MPLS

En d'autres termes, le LSR de transit effectue le transfert d'étiquettes *MPLS* sur la base de paquets, et les *LSRs* de l'entrée et de sortie traitent la commutation entre *MPLS* et *IP*.

6. L'Architecture MPLS:

L'architecture *MPLS* est divisée en deux composants distincts : le composant de transmission, également appelé « *plan des données, data plane* » et le composant de contrôle appelé « *plan de contrôle, control plane* » [14].

6.1 Plan de contrôle (Control Plane):

Le plan de contrôle construit une table de routage (*Routing Information Base –RIB-*) qui est basé sur le protocole de routage. Différents protocoles de routage, tels que *OSPF*, *IGRP*, *EIGRP*, *IS-IS*, *RIP* et *BGP* peuvent être utilisés dans le plan de contrôle. Le plan de contrôle utilise un protocole d'échange d'étiquettes pour créer et maintenir les étiquettes en interne et d'échanger ces étiquettes avec d'autres nœuds *MPLS*. Les protocoles d'échange d'étiquettes comprennent le protocole *LDP* , l'ancien protocole de Cisco *TDP* et le *BGP* (utilisé par *VPN MPLS*). Le *RSVP* est utilisé par *MPLS* pour accomplir l'échange d'étiquette.

Échange des informations de routage

Échange des informations d'étiquettes

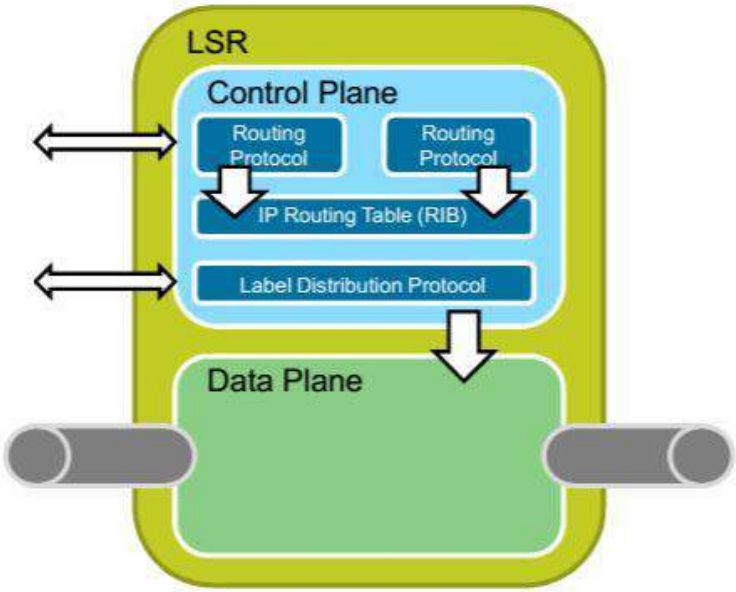

Figure 2. 8 L'ARCHITECTURE MPLS : PLAN DE CONTRÔLE

Le plan de contrôle s'appuie également sur deux tables, une base d'informations de transmission (*Forwarding Information Base –FIB-*) à partir des informations dans le *RIB* et une base d'informations de transmission des étiquettes (*Label Forwarding Information Base – LFIB-*) sur la base du protocole d'échange d'étiquettes et de *RIB*. Le tableau *LFIB* comprend les valeurs des étiquettes et les associations avec l'interface de sortie pour chaque préfix réseau.

6.2 Plan de données (Data Plane):

Le plan de données prend soin de l'expédition sur la base des adresses ou des étiquettes de destination.

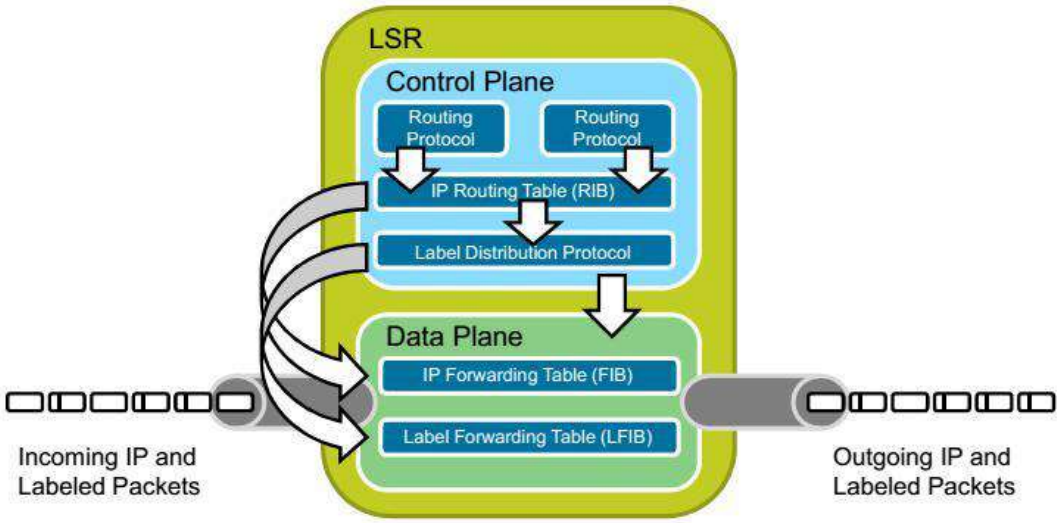

Figure 2. 9 ARCHITECTURE MPLS : PLAN DES DONNÉES

Le plan de données est également connu sous le plan d'acheminement. C'est un moteur d'acheminement simple qui est indépendant du type de protocole de routage ou de protocole d'échange de étiquète utilisé. Le plan de données transmet des paquets à l'interface appropriée sur la base des informations contenues dans les tableaux *FIB* et *LFIB*.

6.3 Structure de Transfère (Forwarding Structures):

Le plan de données sur un routeur est chargé de la transmission des paquets sur la base de décisions effectuées par les protocoles de routage, qui s'étendent dans le plan de contrôle de routeur. Le plan de données sur un routeur *MPLS* se compose de deux structures de transmission:

La base d'informations de transmission (*Forwarding Information Base -FIB-) :*

Quand un routeur est activé, le *FIB* est utilisé pour transmettre des paquets *IP* sur la base de décisions prises par les protocoles de routage. Le *FIB* est peuplé une table de routage qui comprend les réseaux de destination, les sauts suivants, les interfaces de sortie et les pointeurs vers les adresses de la couche 2. Le *FIB* sur un routeur *MPLS* autorisé contient également une étiquette sortante, si une interface de sortie est activée pour *MPLS*. La recherche *FIB* est faite quand un paquet *IP* est reçu, et en basant sur le résultat, le routeur peut envoyer un paquet *IP* ou une étiquette peut être imposée.

La base d'informations de transmission des étiquettes (Label *Forwarding Information Base -LFIB-) :*

Le *LFIB* est utilisé quand un paquet étiqueté est reçu. Il contient l'étiquette entrant et sortant, l'interface de sortie et les informations de prochain saut. Quand une recherche *LFIB* est faite, le résultat peut être le fait d'échanger une étiquette et envoyer un paquet étiqueté ou de supprimer une étiquette et envoyer un paquet IP.

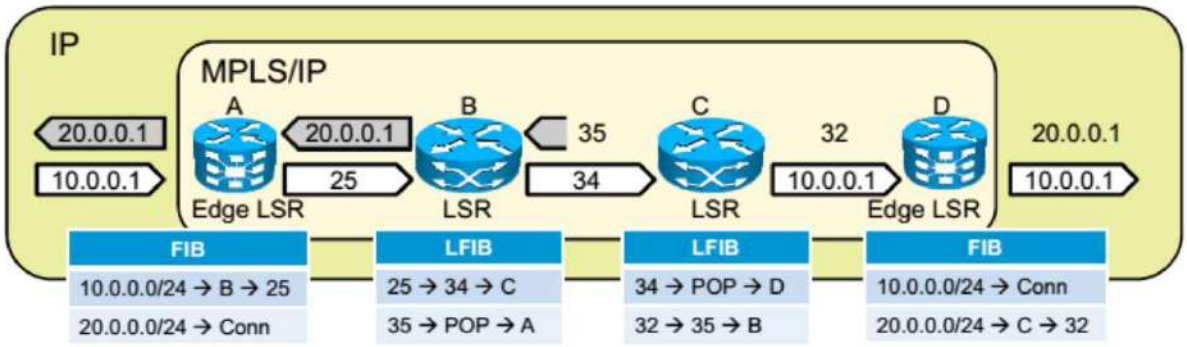

Figure 2. 10 STRUCTURE DE TRANSFER DANS UN CORE IP/MPL

Ces combinaisons de transmission de paquets sont possibles:

Un paquet *IP* reçu (*FIB*) est transmis sur la base de l'adresse de destination *IP* et il est envoyé comme paquet *IP*.

Un paquet *IP* reçu (*FIB*) est transmis sur la base de l'adresse de destination IP et il est envoyé en tant que paquet étiqueté.

Un paquet étiqueté reçu (*LFIB*) est transmis sur la base de l'étiquette, l'étiquette est échangée et le paquet étiqueté est envoyé.

Un paquet étiqueté reçu (*LFIB*) est transmis sur la base de l'étiquette, l'étiquette est enlevée et le paquet IP est envoyé.

6.4. Exemple d'Architecture MPLS:

La *figure 2.11*, illustre un exemple de protocoles utilisés dans le plan de contrôle *MPLS* et le *LFIB* dans le plan de données. Dans l'exemple d'architecture *LSR*, le plan de contrôle utilise ces protocoles:
Un protocole de routage *OSPF* qui reçoit et envoie des informations sur le réseau IP 10.0.0.0/8.
Un protocole d'échange d'étiquettes *LDP* qui reçoit l'étiquette 24 utilisée pour les paquets avec l'adresse de destination 10.0.0.0/8.
Une étiquette local 17 est générée et est envoyée aux voisins en upstream afin que ces voisins puissent étiquetés les paquets avec l'étiquette appropriée.

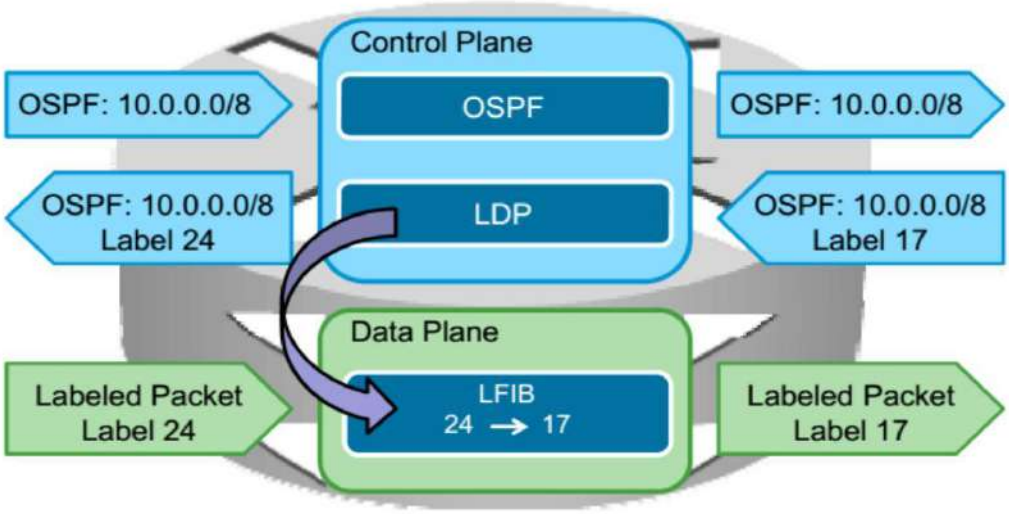

Figure 2. 11 EXEMPLE D'ARCHITECTURE MPLS

Le plan de données utilise un *LFIB* pour transmettre les paquets basés sur les étiquettes comme suit : Le *LFIB* reçoit une entrée de *LDP*, où l'étiquette 24 est mappée à l'étiquette 17. Lorsque le plan de données reçoit un paquet marqué avec un 24, il remplace l'étiquette 24 avec l'étiquette 17 et transmet le paquet par l'intermédiaire des interfaces appropriées.

7. Fonctionnement de MPLS:

La transmission des données s'effectue sur des chemins nommés *LSP*. Ils sont établis avant la transmission des données (*control-driven*) ou à la détection d'un flot (*data-driven*) qui souhaite traverser le réseau. Les étiquettes incluses dans les trames sont distribuées en utilisant un protocole de signalisation, le plus important de ces protocoles est le *LDP*, mais nous utilisons aussi le *RSVP*, éventuellement associé à un protocole de routage, comme *BGP* ou *OSPF*. Les trames acheminant les paquets *IP* transportent les étiquettes d'une nœud vers une nœud [5].
Une étiquette d'entrée permet donc de déterminer la *FEC* par laquelle le flot transite. Cette solution ressemble à la notion de circuit virtuel dans *l'ATM*, où les circuits virtuels sont multiplexés. Ici, nous

avons un multiplexage de tous les circuits virtuels à l'intérieur d'une *FEC*, de telle sorte que, nous ne puissions plus distinguer les circuits virtuels [5].

Le *LSR* examine l'étiquette et envoie la trame dans la direction indiquée. Nous voyons bien ainsi le rôle capital joué par les *LER*, qui assignent aux flots de paquets des étiquettes qui permettent de commuter les trames sur le bon circuit virtuel. L'étiquette n'a de signification que localement, puisqu'il est modifiée sur la liaison suivante [5].

Une fois le paquet classifié dans une *FEC*, une étiquette est assignée à la trame qui va le transporter. Cette étiquette détermine le point de sortie par le chaînage des étiquettes, dans

le cas des trames classiques, comme *LAP-F* du *Frame Relay* ou *ATM*, l'étiquette est positionnée dans le *DLCI* ou dans le *VPI/VCI* [5].

La signalisation nécessaire pour déposer la valeur des étiquettes du chemin déterminé par une *FEC*, peut être gérée soit à chaque flot, soit par un environnement de contrôle indépendant des flots utilisateur. Cette dernière solution est préférable dans le cas de grands réseaux, du fait de ses capacités de passage à l'échelle.

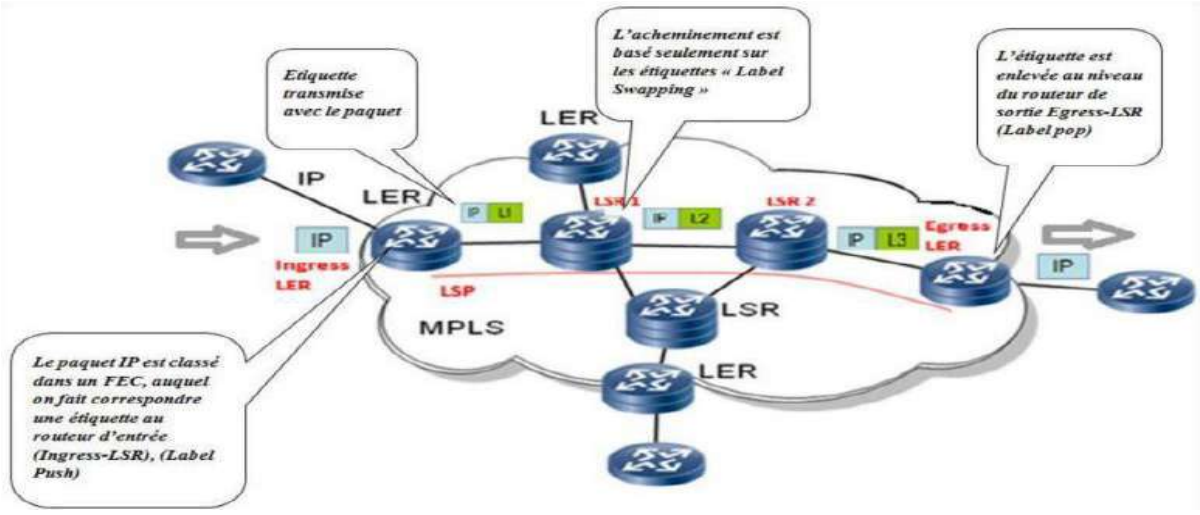

Figure 2. 12 LES PRINCIPALES ÉTAPES DE COMMUTATION PAQUET MPLS

Les étiquettes peuvent être distribuées par :

Un routage unicast vers une destination particulière. Une gestion du trafic, ou *TE* (*Traffic Engineering*).

Un multicast.

Un réseau privé virtuel. Une qualité de service.

7.1.Distribution des étiquètes :

MPLS normalise plusieurs méthodes pour réaliser la distribution des étiquettes. La distribution indique que chaque nœud possède ses propres étiquettes et qu'il doit les mettre en correspondance avec les étiquettes de ses voisins [5]. Les méthodes de distribution des référe étiquettes sont les suivantes :

Topology-based : est fondée sur la topologie, elle utilise les messages destinés à la gestion du routage comme *OSPF* et *BGP*.

Request-based : est fondée sur le flot, elle utilise une requête de demande d'ouverture d'un chemin pour un flot *IP*. C'est le cas de *RSVP*.

Traffic-based : est fondée sur le trafic, à la réception d'un paquet, une étiquette est assignée à la trame qui le transporte.

Les méthodes fondées sur la topologie et sur le flot correspondent à un, tandis que celles fondées sur le trafic correspondent à des données.

Les protocoles de routage, dont *IGP*, ont été améliorés pour transporter une étiquette supplémentaire. De même le protocole *RSVP* comporte une version associée à *MPLS* qui lui permet de transporter une étiquette, Où la nouvelle version est *RSVP-TE*, qui permet l'ouverture des chemins en tenant compte des ressources du réseau.

L'IETF a également normalisé un nouveau protocole de signalisation, *LDP*, pour gérer la distribution des étiquettes. Des extensions de ce protocole, comme *CR-LDP* (*Constraint-based Routing-LDP*) permettent de choisir les routes suivies par les clients des *FEC* avec une qualité de service prédéfinie.

Les principaux protocoles de signalisation sont les suivants :

LDP, qui fait correspondre les adresses *IP* unicast et les étiquettes.

RSVP-TE et *CR-LDP*, qui ouvrent les routes avec une qualité de service.

PIM (*Protocol Independent Multicast*), qui fait correspondre les adresses *IP* multicast et les étiquettes associées ;

BGP, qui est utilisé pour déterminer les étiquettes dans le cadre de réseaux virtuels privés.

7.2.Agrégation de flots:

Les flots provenant de différentes interfaces peuvent être rassemblés et commutés sur une même étiquette, s'ils vont vers la même direction de sortie. Cela correspond à une *agrégation de flots*, cette technique est déjà exploitée sur les réseaux *ATM*, dans lesquels un circuit peut agréger plusieurs flots venant de différents nœuds d'entrée vers un point commun, où les flots sont désagrégés [5].

L'agrégation de flots a pour objectif de réduire le nombre des étiquettes utilisés ou, c'est-à-dire, d'empêcher les tables de commutation de devenir trop importantes.

7.3 Signalisation :

Comme expliqué précédemment, plusieurs mécanismes de distribution des étiquettes, appelés *signalisation*, peuvent être implémentés dans les nœuds d'un réseau *MPLS*, notamment les suivants:

Demande d'étiquette: un *LSR* émet une demande d'étiquette à ses voisins vers le downstream, qu'il peut être lié à la valeur d'une *FEC*. Ce mécanisme peut être utilisé d'un nœud vers un nœud jusqu'au nœud de sortie du réseau *MPLS*.

Correspondance d'étiquette: en réponse à une demande d'étiquette d'un nœud upstream, un *LSR* envoie une référence provenant d'un mécanisme de correspondance déjà mise en place, pour aller jusqu'au nœud de sortie.

La figure suivante donne une illustration de ces deux mécanismes.

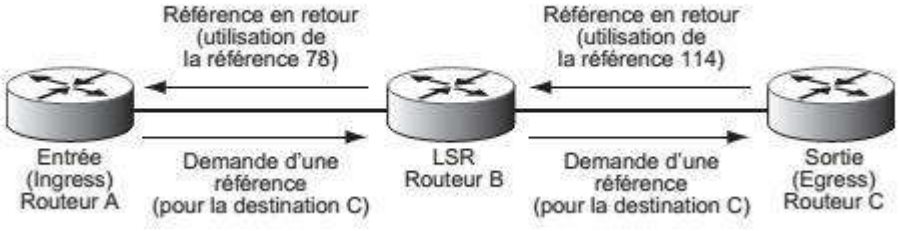

Figure 2. 13 MÉCANISME DE SIGNALISATION MPLS

7.4 LDP (Label Distribution Protocol) :

Le *LDP* est le protocole de distribution des étiquettes qui tend à devenir le standard le plus utilisé dans *MPLS*. Ce protocole tient compte des adresses unicast et multicast. Le routage est explicite et est géré par les nœuds de sortie, quant aux échanges, ils s'effectuent sous le protocole *TCP* pour assurer une qualité acceptable.

Deux classes de messages sont acceptées, celle des messages adjacents et celle des messages indiquant les étiquettes. La première permet d'interroger les nœuds qui peuvent être atteints directement à partir du nœud origine, et La seconde transmet les valeurs de l'étiquette lorsqu'il y a accord entre les nœuds adjacents. Ces messages sont encodés sous la forme classique, qui permet de décrire un objet : nous indiquons dans un premier champ le type d'objet, dans un deuxième la longueur totale du message décrivant l'objet et dans un troisième la valeur de l'objet. Cet encodage s'appelle le *TLV* (*Type Length Value*).

Le routage s'effectue, comme nous l'avons vu, par *FEC*. La granularité des étiquettes, c'est-à-dire la taille des flots qui utilisent une même étiquette, résulte de la taille des *FEC*: s'il y a peu de *FEC*, les flots sont importants et la granularité est forte. Et s'il y a beaucoup de *FEC*, les flots sont faibles, et la granularité est fine.

La destination peut aussi être une application particulière sur une machine donnée, ce qui donne une forte granularité. Ce dernier cas est illustré par la *figure 2.14*.

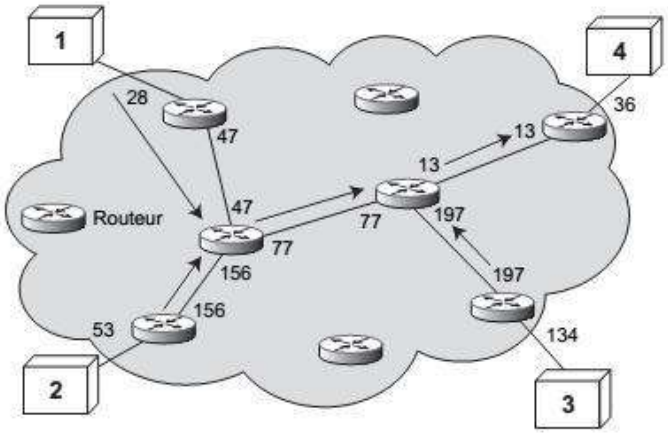

Figure 2. 14 CLASS D'ÉQUIVALENCE FEC DANS RÉSEAUX MPLS

8. Avantages et Tendance de MPLS :

Dans les routeurs *modernes*, la commutation d'étiquettes *MPLS* n'est pas plus rapide que le routage *IP*, mais MPLS n'est pas utilisé uniquement en raison de ses performances de commutation. Il existe plusieurs autres avantages MPLS [14] :

MPLS diminue les frais généraux de transfert sur les routeurs de cœur. MPLS prend en charge plusieurs applications utiles: *VPN*, et *QoS*.

MPLS soutient la transmission de protocoles non-IP, car les technologies *MPLS* sont applicables à n'importe quel protocole de couche réseau.

la possibilité de transporter les paquets *IP* sur plusieurs types de réseaux commutés. Il est ainsi possible de passer d'un réseau *ATM* à un réseau *Ethernet* ou à un réseau *Frame Relay*. En d'autres termes, il peut s'agir de n'importe quel type de trame, à partir du moment où une étiquette peut y être incluse [5].

La différence essentielle entre *MPLS* et les technologies *WAN* traditionnelles se résume par la manière dont les étiquettes sont attribué [5] ;

En utilisant les étiquettes plutôt que les informations contenues dans l'en-tête *d'IP*, le traitement impliqué dans le routage de paquets est rendu simple et rapide ;

Permet un déploiement à grande échelle pour acheminer différent types de trafic tout en représentant les contraintes de fonctionnement associées et sur une unique infrastructure.

MPLS est devenu populaire et a vu de nombreuses implémentations et déploiements par des fournisseurs de services. L'idée originale pour inventer *MPLS* était une meilleure intégration des *IP* dans les réseaux *ATM*. Cependant, *MPLS* a connu un succès qui a surpris beaucoup de gens dans l'industrie des réseaux, et en particulièrement l'énorme succès de *VPN MPLS* de l'industrie. Les fournisseurs de services ont rapidement reconnu les grands bénéfices de *VPN MPLS* et le déployé rapidement. Aujourd'hui, tout transport sur MPLS connaît un intérêt croissant dans l'industrie

9. Conclusion :

Ce chapitre nous introduit dans le monde du *MPLS* et nous a donné un aperçu général sur *MPLS*, son structure, son architecture, ainsi que les différentes fonctionnalités qu'elle assure, nous citons :

Spécification des mécanismes pour gérer les flux de trafic de différentes granularités, telles que les flux entre les différents matériels, machines, ou même flux entre les différentes applications.

Indépendante des protocoles de couche 2 et 3.

Offre d'un moyen pour mapper des adresses *IP* aux étiquettes simples, de longueur fixe utilisée pour le transfert de paquets en utilisant des technologies de commutation de paquets différents.

MPLS est une infrastructure critique et pour cela nous allons présenter, dans le chapitre suivant, un état de l'art sur la tolérance aux fautes et les mécanismes de sécurité dans un réseau *MPLS*.

Chapitre III :Tolérance aux fautes et Sécurité dans MPLS

1. Introduction

Ce chapitre, présente la tolérance aux fautes et la sécurité dans un réseau *MPLS* et de ses principales composants. Dans la première section, nous allons voir les défaillances, les différents mécanismes et techniques de récupération utilisés pour protéger l'infrastructure *MPLS* des pannes, pour passer ensuite, aux travaux connexes sur le rétablissement de l'échec, des approches utilisées pour soutenir la tolérance de pannes dans les réseaux *MPLS*. Dans la deuxième section, nous allons voir la sécurité *MPLS* et les principales questions de sécurité avec différentes attaques, mécanismes et techniques de sécurité *MPLS*.

2. Les principales défaillances du réseau :

Les principales défaillances du réseau sont essentiellement de trois types [15] :

2.1 Défaillance d'un Nœud :

Défaillance d'un nœud due à une panne de l'équipement ou des dommages matériels résultant d'un événement comme un feu d'accident, inondation, tremblement de terre; en conséquence, tout ou partie des liens de communication relier au nœud affecté peuvent être échoué.

2.2 Défaillance d'un Lien :

Défaillance d'un Lien due à une coupure du câble à fibres. Le câble porteur de trafic d'un bureau de télécommunication à un autre est enterré environ trois pieds sous terre dans un conduit, mais en raison des activités de construction, des coupures de câble accidentelles se produisent fréquemment, en dépit des efforts accrus de soins de réseau et d'entretien.

2.3 Panne de logiciel :

Une panne de logiciel peut influer sur une grande partie du réseau donné. Si l'application logicielle dans un routeur par exemple est endommagée ou ne fonctionne pas correctement, alors cela affectera les autres composants de réseau qui sont connectés à ce dernier.

Afin d'éviter ces problèmes, il faut que les routeurs et les autres éléments du système de réseau tolèrent les défaillances de nœud ou un lien dans le réseau. Par conséquent, un système qui est capable de continuer à fonctionner correctement en cas de défaillance de certaines de ses parties est appelée un système de tolérance de fautes.

3. Tolérance aux fautes :

La tolérance aux fautes est l'aptitude d'un système informatique à accomplir sa fonction malgré la présence des fautes [16], qu'il s'agisse de dégradations physiques du matériel, de défauts logiciels, d'attaques malveillantes, d'erreurs d'interaction homme-machine. En bref, la tolérance aux fautes permet à un système de

continuer à délivrer un service conforme à sa spécification et d'éviter les défaillances du système malgré la présence des fautes [17].

4. Problèmes de MPLS :

MPLS est une procédure compliquée, car les défaillances dans le réseau *MPLS* causent énormément de perte de données [18], qui sont résultant un effet négatif sur les applications et les services critiques de l'entreprise [19]. Dans *MPLS*, la défaillance de composants de réseau est motivée par des raisons différentes tels que le matériel, les erreurs logicielles, coupure de fibre [20], pannes de courant, nœuds malveillants et adversaires [21], architectural et vices de procédure [22]. De multiples défaillances simultanées sont motivées dans *MPLS* comme sa topologie qui se compose de liens multiples. Une panne générale qui se produit dans le réseau *MPLS* est «trou noir». Cet échec se produit dans le réseau en raison de la résiliation anormale d'un *LSP* intérieur d'un réseau *MPLS*. L'échec peut également être motivé par un tunnel *MPLS* échoué et brisé. Retarder la convergence des protocoles de routage vers les erreurs de configuration à des bugs dans la mise en œuvre de routeur individu est une conséquence grave de l'échec de trou noir [22].

Les échecs sont de nature complexe, en raison de l'architecture multicouche de *MPLS*.
Ce dernier, est dépendant de couche physique de transmission, d'où, la défaillance d'un seul composant peut conduire à une défaillance simultanée de plusieurs composants.
Dans MPLS, la survie du réseau peut être assurée qu'en prenant en considération la tolérance de panne comme un facteur de qualité de service, où les défaillances des liens ou des nœuds cause des problèmes importants [23].
Défauts dans les résultats de réseau MPLS en grande perte de paquets, la mauvaise qualité du service et dégrade les performances du réseau. Donc défauts doivent être découvertes et récupérées dès que plus tôt. La tolérance aux pannes est définie comme la capacité du réseau à répondre et à récupérer rapidement de l'échec. Les techniques de récupération des défauts peuvent libérer le réseau de défauts et peut faire la faute de réseau MPLS plus tolérant. La mise en œuvre de la technique de protection de chemin en redondance permet implicitement réseau ressources. Ainsi, lors de la conception technique à tolérance de panne, le facteur de capacité d'attribution d'actions doit être considéré [24] La technique de récupération de l'échec encourt un temps de retard et ce retard peut varier d'une approche à l'autre. Ce facteur de retard influence sur la topologie du réseau et la technique de récupération [25].
Dans la suite de ce chapitre, une structure fondamentale de MPLS est décrite. Puis, nous passons à quelques problèmes rencontrés généralement dans le réseau.

5. Tolérance aux fautes dans MPLS:

Il est très important que lors d'un défaut sur la voie existante, le flux de données doit être transféré immédiatement sur un chemin alternatif, sinon une grande quantité de données sera perdue par le nœud défaillant. Pour cette raison, MPLS fournit des mécanismes qui peuvent détecter au début le défaut dans le réseau et aussi des techniques qui sont utilisées pour passer le flux influencé dans un chemin alternatif vers la destination.

5.1 La détection d'un défaut dans MPLS :

Le défaut dans un chemin peut être détecté avec le contrôle utilisé entre les *LSR* voisins. Par exemple, *KeepAlive* messages peuvent être utilisés et sont échangés périodiquement entre tous les routeurs voisins dans le chemin. Le *LSR* qui détecte la panne peut être en mesure de passer le flux du chemin alternatif. Si le *LSR* n'est pas en place pour réagir immédiatement, il doit envoyer des messages d'indication de défaut (Failure Indication Signal –FIS-) afin d'informer les autres *LSR* et *Ingress LSR*. Lorsque le routeur responsable de rediriger le trafic reçoit des messages du *FIS*, la procédure de récupération de l'échec doit commencer. Les messages du *FIS* sont transmis avec une priorité élevée afin de garantir la propagation rapide vers *LSR* qui est en charge de restaurer le flux influencé [26].

5.2 Techniques de récupération dans MPLS :

L'IETF a défini deux modèles de récupération du réseau *MPLS* sont : le modèle de *réacheminement* et la *commutation de protection*.

5.2.1. Réacheminement (Rerouting ou la protection dynamique) :

Dans le réacheminement, le chemin alternatif est calculé dynamiquement après la détection d'un défaut. Après l'établissement de *LSP* alternatif, le flux de données est commuté vers le nouveau chemin.
Le réacheminement est défini comme la création de nouveaux chemins ou des segments de chemin sur la demande de restauration du trafic après l'apparition d'un défaut. Les nouveaux chemins peuvent être basés sur des informations sur les défauts, des politiques de routage, des configurations prédéfinies et des informations sur la topologie du réseau. Ainsi, lors de la détection d'un défaut, les chemins ou les segments de chemin sont établis au moyen de signalisation afin de contourner le défaut. À cet effet, un chemin de remplacement ou de secours en dehors de le chemin primaire est nécessaire.

5.2.2. La commutation de protection (Protection switching) :

La commutation de protection fournit la restauration rapide par rapport à la technique de réacheminement, parce que le chemin alternatif est déjà préconfiguré, donc elle est effectuée immédiatement après le défaut est détecté.
Elle préétablit un chemin ou un segment de chemin alternatif sur la base des politiques de réseau, de routage, des exigences en matière de restauration de la transmission sur le chemin et des considérations administratives. Lorsqu'un défaut est détecté, le trafic de protection est commuté sur le chemin alternatif.

Dans le modèle de restauration rapide, le *LSP* de sauvegarde est créé et configuré à l'avance, donc la réservation de la bande passante doit être faite.

Il existe deux mécanismes de commutation de protection sont : la *réparation locale* (ou protection de lien/nœud) et la *réparation globale* (ou protection de chemin).

5.2.2.1 La réparation globale :

Dans la réparation globale, la protection est activée sur la base de bout en bout, indépendamment du lieu de la défaillance, comme la montre la figure ci-dessous. Autrement dit, une variante ou un LSP de secours est préétablie à partir de la pénétration de routeurs de sortie de la voie à protéger. Dans ce cas, la voie alternative fournit une protection contre toutes les liaisons et nœuds utilisés dans le chemin qui est en train de routée les données. Quand une panne est détectée, le LSR doit envoyer des messages du FIS à la pénétration LSR, puis le processus de récupération va commencer [26]. Nous remarquons que dans la réparation globale un signal de défaillance se propage à la source (routeur d'entrée) avant la commutation du trafic vers le chemin de sauvegarde, ce qui gaspille un temps précieux parce que la notification d'échec doit traverser l'ensemble du réseau MPLS (Domain).

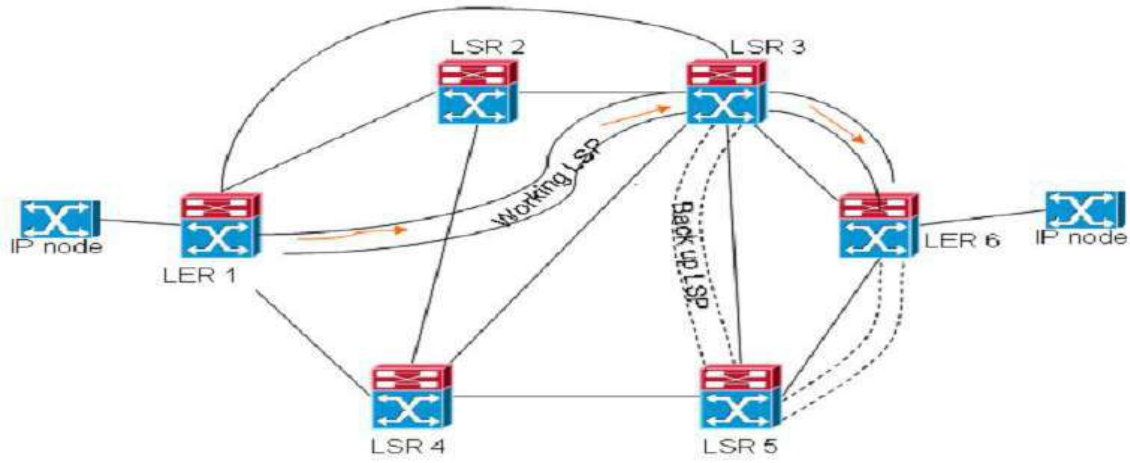

Figure 3. 1 LA RÉPARATION GLOBALE

5.2.2.2 La réparation locale:

La voie alternative peut être locale, cela signifie que la réparation est effectuée contre une défaillance d'un lien simple ou d'un nœud. Dans ce cas, les messages du *FIS* ne sont pas utilisés, comme le montre la *figure 3.2* [26]. Et ce, dans une très courte distance de l'échec, minimisant ainsi les retards et la perte totale du paquet.

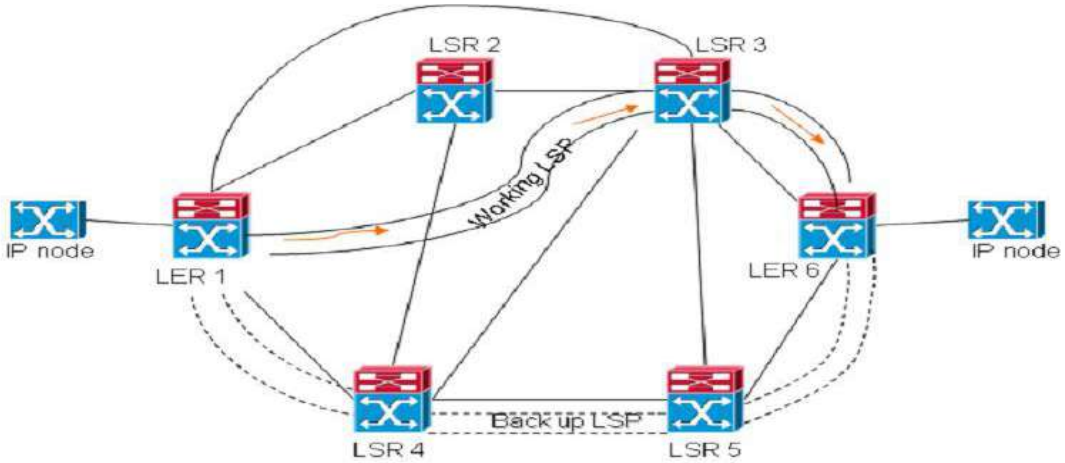

Figure 3. 2 LA RÉPARATION LOCALE

Si une réparation locale est tentée de protéger un ensemble de *LSP*, chaque *LSR* intermédiaire doit avoir la capacité d'initier un *LSP* alternatives préétablis. En effet, il est impossible de prédire où un incident peut se produire dans un *LSP*. Un coût très élevé doit être payé en termes de calculs complexes avec une signalisation vaste nécessaire pour établir des *LSPs* alternatifs de chaque *LSR* intermédiaire.

5.3 Les facteurs de restauration dans MPLS :

Les critères les plus importants à prendre en considération lors de l'utilisation du mécanisme de restauration dans MPLS sont: la *perte de paquets*, le *temps de restauration*, la *vulnérabilité* et la *qualité de la protection*. Dans ce qui suit, nous résumerons les facteurs de notre intérêt [15] :

***La perte de paquets*:** Les systèmes de restauration peuvent introduire des pertes de paquets lors de la commutation ou d'une reprise de sauvegarde *LSP*. Par conséquent, les débits atteints pour le service sont gravement touchés. Alors, les systèmes de récupération devraient garantir un minimum ou, si possible pas de pertes de paquets pendant la période de restauration.

***Le réacheminement du Paquet*:** les systèmes de restauration peuvent exiger des paquets réorganisés lors de la commutation de ou vers le *LSP* de travail. La réorganisation de paquet est principalement nécessaire à la sortie du réseau *MPLS*.

***L'utilisation des ressources*:** afin de fournir la tolérance de fautes dans un réseau *MPLS*, en particulier la protection pré-planifiée, une bande passante redondante doit être réservée et utilisée efficacement.

***Le temps de restauration*:** c'est le temps depuis le début de détection de panne, jusqu'au moment où les paquets commencent à apparaitre dans le chemin alternative.

Après avoir présenté les différentes techniques de restauration, de réacheminement et de commutation de protection, nous allons présenter dans ce qui suit, la sécurité dans un réseau *MPLS*, ses différentes techniques et les stratégies de défense à utiliser.

6. Sécurité dans MPLS :

Avec le déploiement croissant de *MPLS*, les problèmes de sécurité ont été soulevés. L'architecture de base des réseaux *MPLS* ne supporte pas les mécanismes de sécurité à cause de l'émergence de technologie *MPLS* vers une livraison de paquets à haute vitesse.

Dans les réseaux MPLS, seuls les deux routeurs d'entrée et de sortie sont responsables de la vérification de l'entête des paquets IP reçus. En générale le réseau MPLS porte sur des questions de sécurité tels que: la confidentialité, l'intégrité des données et la disponibilité [31].

6.1 Confidentialité:

La confidentialité assure que les informations ne soient pas accessibles par des personnes (ou entités) non autorisées. Dans les réseaux *MPLS*, elle peut se référer par exemple à la confidentialité de *LIB* (*Label Information Base*) et la confidentialité de trafic passant par l'infrastructure.

Les *MPLS* faut veiller à ce qu'aucun des paquets étiqueté soient acceptés à partir de l'extérieur de l'infrastructure MPLS, afin d'éviter l'introduction des paquets par des intrus qui détermine la valeur d'une étiquette.

MPLS est communément annoncé comme offrant une bonne fonctionnalité MPLS *VPN*. Mais contrairement à la technologie *VPN* qui utilise par exemple *l'IPSec*, *MPLS VPN* n'assure pas la confidentialité des données, mais il permet d'utiliser les protocoles chiffrés comme l'HTTPS, et l'IPSec.

Une caractéristique intéressante de *MPLS* est que permet aux opérateurs de réseau de cacher les détails sur leur cœur *MPLS*. Même si un paquet traversant le réseau, seulement ses étiquettes sont l'objet de manipulations.

6.2 Intégrité des données:

L'intégrité des données est le fait que l'information n'a pas été modifiée ou détruite d'une manière non autorisée. *MPLS* repose sur la confiance aux décisions de transfert de paquets faites par *LIB*. Les mises à jour des informations du *LDP* ne doivent être acceptées qu'à partir des sources fiables. Cela peut être assuré par deux mécanismes :

Tout d'abord, les mises à jour du *LDP* ne doivent être acceptées qu'à partir de l'interface sur lesquelles un autre *LSR* est connu. En d'autres termes, les mises à jour du *LDP* ne devraient pas être acceptées par les clients à l'extérieur du noyau *MPLS*.

Ensuite, si les routeurs de cœur ne sont pas approuvés ou sont supposés être vulnérables aux attaques, les mécanismes d'authentification doivent être en place pour protéger le *LDP*.

6.3 Disponibilité:

La disponibilité est la propriété d'un système ou d'une ressource système d'être accessible ou utilisable à la demande d'une entité autorisée. Ainsi, les opérateurs de réseaux doivent entretenir les appareils au sein de l'infrastructure de base.

7. Les menaces de sécurité dans MPLS :

Cette section aborde les diverses menaces de sécurité réseau qui peuvent mettre en danger le réseau *MPLS*. Plusieurs types d'attaques existent, nous citons: les *attaques sur le plan de contrôle*, les *attaques sur le plan des données* et les attaques *de l'intérieurs du cœur MPLS* [32].

7.1 Attaques sur le plan de contrôle :

Cette catégorie englobe les attaques sur les structures de contrôle exploitées par le fournisseur de service du noyau *MPLS*. Parmi ces attaques, nous citons :

7.1.1. Création LSP par un élément non autorisé :

L'élément non autorisé peut être une *CE* (*CustumerEdge*) locale ou un routeur dans un autre domaine. Un élément non autorisé peut générer la signalisation des étiquettes *MPLS*, cela peut entraîner dans le plan de contrôle, dans l'état de transmission en cas de succès, ainsi que une réservation inutile de la bande passante du réseau. Cela peut également, entraîner un vol de service ou même risquer l'ensemble du réseau.

7.1.2. Interception du message LSP:

Cette menace peut être accomplie par le trafic de surveillance du réseau après une intrusion physique. Ainsi sans intrusion physique, il pourrait être accompli avec une modification non autorisée de logiciels. Aussi, de nombreuses technologies telles que les micro-ondes terrestres, satellite ou fibre optique pourraient être interceptés sans intrusion physique. En cas de succès, il pourrait fournir des informations menant à l'étiquette.

7.1.3. Les attaques contre LDP :

LDP est le protocole de contrôle utilisé pour mettre en place les tunnels *MPLS* sans *TE* (Traffic Engineering). Il existe deux types importants d'attaque contre le *LDP* sont:
Un élément de réseau non autorisé peut établir une session *LDP* en envoyant des messages *LDP Hello* et *LDP Init*, conduisant à la mise en place potentielle d'un *LSP*, ainsi que le *LDP*.
Une attaque peut lancer un *DoS (Denial of Service)* attaque sous la forme d'une tempête des messages *LDP Hello* ou *LDP TCP SYN*, conduisant à l'utilisation du des ressources de routeur cible.

7.1.4. Attaques sur l'équipement d'un fournisseur de service via les interfaces de gestion :

Cela comprend l'accès non autorisé à l'infrastructure d'un équipement d'un fournisseur de service, par exemple : pour reconfigurer le matériel ou l'extrait d'informations (statistiques, topologie, etc.) appartenant au réseau.

7.1.5. Connexion croisée du trafic entre les utilisateurs :

Ceci se rapporte à l'événement dans lequel la contrainte de séparation entre les utilisateurs est violée. Cela inclut plusieurs cas:

Un site étant relié dans le *VPN* mauvais.

Un trafic reproduit et envoyé à un utilisateur non autorisé. Deux ou plusieurs *VPN* incorrectement fusionnées.

Une *VPN* point à point reliant les deux mauvais points.

Tout paquet ou trame étant mal livrés en dehors de la *VPN* auquel il appartient.

Un inter connexion de *VPN* peut être causé par le fournisseur de service, par l'erreur de l'équipement de fournisseur ou par l'action malveillante d'un attaquant. La violation peut être physiques, par exemple les liens *PE-CE* mal connectés, ou logique, par exemple une mauvaise configuration de l'appareil.

7.2 Attaques sur le plan des données :

Cette catégorie englobe les attaques sur le fournisseur de service ou l'utilisateur final de données.

Du point de l'utilisateur final du réseau MPLS, une partie pourrait être le plan de contrôle du trafic, par exemple, les protocoles de routage en cours d'exécution à partir du site de l'utilisateur A à site d'utilisateur B via *IP* ou *non-IP* connexions, qui peuvent être un certain type de *VPN*.

7.2.1. Observation non autorisée de données sur la circulation :

Cela peut entraîner une exposition de confidentialité d'informations, il peut aussi être une première étape d'autres attaques (décrit ci-dessous) dans lequel les données enregistrées sont à jour et réinsérées ou simplement seront rejouées plus tard.

7.2.2. Modification des données de trafic :

Ceci se rapporte à la modification du contenu de paquets lorsqu'ils traversent le noyau *MPLS*.

7.2.3. Insertion non autorisée du trafic de données:

Spoofing se réfère à l'envoi des paquets vers une destination ou l'insertion des paquets dans un flux de données qui ne font pas partie, afin de les avoir accepté par le destinataire comme légitime.

7.2.4. Suppression non autorisée de données :

Ceci se rapporte à provoquer des paquets à être rejeter par le réseau *MPLS*. C'est un type spécifique de l'attaque *DOS*.

7.2.5. Analyse non autorisé du trafic:

Ceci se rapporte à espionner les paquets de fournisseur des services ou d'utilisateurs en examinant les aspects ou les méta-aspects qui peuvent être visibles même lorsque les paquets eux-mêmes sont cryptés. Un attaquant pourrait récupérer les informations utiles au moment du l'acheminement dans le réseau, sur la base de la quantité et la taille des paquets, l'adresses source et destination, …etc.

7.2.6. Attaques par déni de service :

Les dénis de service (DoS) sont ceux dans lesquels un attaquant qui tente de perturber ou empêcher l'utilisation d'un service par son légitime utilisateurs, en prenant les périphériques réseau hors service, en modifiant leur configuration ou en les surcharger par des demandes de service.

7.3 Attaque de l'intérieur du cœur MPLS:

La chaîne de modèle de confiance signifie que les réseaux *MPLS* sont particulièrement vulnérables aux attaques de l'intérieur. Ceux-ci peuvent être lancés par toute personne maligne ayant accès à tout *LSR* dans le domaine de la confiance. Ces attaques pourraient également être lancées par le logiciel compromis au sein du domaine de la confiance.

La protection contre ce type d'attaque peut être obtenue par la sécurité stricte des mises à niveau de logiciels et d'un accès par des procédures de contrôle. Dans certains cas, les processus de changement de configuration d'homologation peuvent aussi être justifiés. Les outils logiciels pourraient être utilisés pour vérifier les configurations pour la cohérence et la conformité. Ils peuvent également être utilisés pour surveiller et signaler les comportements et l'activité réseau afin de repérer rapidement les irrégularités qui peuvent être le résultat d'une attaque de l'intérieur.

8. Techniques de défense pour un réseau MPLS :

Les techniques défensives discutées dans le présent chapitre visent à décrire les méthodes par lesquelles certaines menaces de sécurité peuvent être abordées. Ces techniques décrites ici incluent *l'authentification*, le *cryptage*, le *contrôle d'accès*, le *filtrage*, le *pare-feu*, *l'isolement*, l'*agrégation* et d'autres [32].

8.1 Authentification :

Pour éviter les problèmes de sécurité découlant de certaines attaques *DoS* ou à partir de malveillant ou d'une mauvaise configuration accidentelle, il est essentiel que les dispositifs dans le *MPLS* n'acceptent que les connexions ou les messages de contrôle à partir de sources valides. L'authentification se réfère à des procédés pour faire en sorte que les sources de messages soient correctement identifiées par les dispositifs MPLS avec lequel ils communiquent. Il existe plusieurs stratégies dans *MPLS* pour assurer l'authentification, nous citons :

8.1.1. Système de gestion de l'authentification :

Le système de gestion de l'authentification comprend l'authentification d'un *PE* à une gestionnaire de réseau qui est gérée de manière centralisée ou à un serveur d'annuaire. Il comprend également une authentification de *CE* vers le serveur de configuration, lorsqu'un système de serveur de configuration est utilisé. Elle devrait être bidirectionnelle.

8.1.2. Authentification point à point :

L'authentification point à point comprend l'authentification par les pairs dans le réseau des protocoles de contrôle (par exemple, *LDP*, *BGP*, etc.) et d'autres pairs. L'authentification devrait être bidirectionnel, notamment *PE* ou *CE* du serveur de configuration pour être certain qu'il est en communication avec le bon serveur.

8.1.3. Les techniques cryptographiques pour authentifier l'identité :

Les techniques cryptographiques offrent plusieurs mécanismes d'authentification, d'identité des dispositifs ou des individus. Ceux-ci comprennent l'utilisation des clés secrètes partagées, des clés uniques générées par les dispositifs accessoires ou logiciels, des paires de nom d'utilisateur et mot de passe et une gamme des clés public-privé. Une autre approche consiste à utiliser un système d'autorité de certification hiérarchique et de fournir des certificats numériques.

8.2 Techniques cryptographiques :

Il existe plusieurs techniques cryptographiques utilisées dans *MPLS*, nous citons:

8.2.1 IPSec dans MPLS :

IPSec est le protocole de sécurité de choix pour la protection de la couche *IP*. Il offre une sécurité robuste pour le trafic *IP* entre les paires de dispositifs. Le trafic non-IP, tels que le routage IS-IS doivent être convertis en *IP* (par exemple, par l'encapsulation) afin d'utiliser *IPSec*. Lorsque le *MPLS* encapsule le trafic *IP*, *IPSec* couvre le chiffrement de la couche *IP* du client.

Dans le modèle *MPLS*, *IPsec* peut être utilisé pour protéger le trafic *IP* entre les *SPE*, entre un *PE* et un *CE* ou de *CE* à *CE*. De même, il peut utiliser une variété d'algorithmes d'intégrité ou de confidentialité avec diverses longueurs de clés, telles que le cryptage *AES*. Il y a compromis entre la longueur de clé, la charge de calcul, et le niveau de sécurité du chiffrement.

8.2.2 Encryptions pour la configuration et la gestion des périphériques :

Pour la configuration et la gestion des dispositifs *MPLS*, le cryptage et l'authentification de la connexion de gestion à un niveau comparable à celle fournie par *IPsec* est souhaitable. Plusieurs méthodes de transport de trafic et de gestion de dispositif de *MPLS* offrent l'authentification, l'intégrité des données et la confidentialité, nous citons :

Secure SHell (SSH) : elle offre une protection pour *Telnet* pour permettre la configuration à distant.
Transport Layer Security (TLS) : elle repose sur *HTTPS*, elle est largement utilisé pour sécuriser la communication et peuvent ainsi fournir un soutien pour la plupart sur *XML* et les approches de gestion des périphériques basés sur *SOAP* ;
IPSec: elle fournit des services de sécurité, y compris l'intégrité des données et la confidentialité de la couche réseau.

8.3 Techniques de contrôle d'accès :

Les techniques de contrôle d'accès comprennent le paquet par paquet offre l'accès au moyen de filtres et pare-feu sur les paquets *IPv4* et *IPv6*, ainsi que par des moyens d'admission d'une session pour le contrôle, la signalisation ou le protocole de gestion.
Dans cette section nous distinguons deux techniques, le *filtrage* et le *pare-feu*.

8.3.1 Filtrage :

Il est relativement fréquent pour les routeurs de filtrer les paquets. Ces routeurs peuvent regarder dans l'entête des paquets. Les paquets répondant aux critères associés à un filtre particulier peuvent être soit rejetés, soit bénéficier d'un traitement spécial. Aujourd'hui, non seulement les routeurs, mais aussi les hôtes ont des filtres et chaque instance de *IPSec* possède également un filtre.

8.3.2 Pare-feu:

Les pare-feu fournissent un mécanisme pour contrôler le trafic passant entre différentes zones de confiance dans *MPLS* ou entre une grande zone et une zone non sécurisée. Les pare-feu fournissent généralement beaucoup plus de fonctionnalités que les filtres, car ils peuvent être en mesure d'appliquer, analyser et détailler les fonctions logiques du flux, et pas seulement les paquets individuels. Ils peuvent offrir une variété de services complexes, comme protection contre les attaques DoS, la détection de virus, etc. Comme avec d'autres techniques de contrôle d'accès, la valeur de pare-feu dépend d'une compréhension claire des topologies du cœur de réseau *MPLS*, les réseaux d'utilisateurs et le modèle de menace.

8.4 Contrôle d'accès aux interfaces de gestion :

La plupart des problèmes de sécurité liés à des interfaces de gestion peuvent être adressés par l'utilisation de techniques d'authentification. Cependant, des techniques de sécurité supplémentaires peuvent être considérées en contrôlant l'accès à la gestion interfaces dans d'autres façons.

Les interfaces de gestion, en particulier les ports *MPLS*, peuvent être configurés de sorte qu'ils ne soient accessibles en dehors du domaine *MPLS*, à travers un système qui est physiquement ou logiquement séparé du reste de l'infrastructure *MPLS*. Les techniques de filtrage ou de pare-feu peuvent être utilisées pour restreindre la circulation non autorisée.

8.5. Utilisation de l'infrastructure isolée :

L'une des façons de protéger l'infrastructure du *MPLS* est de séparer les ressources des utilisées par les services *MPLS* des ressources utilisées à d'autres fins. Dans certains cas, cela peut impliquer l'utilisation des équipements physiquement séparés pour les services *VPN*, ou même un réseau physiquement séparé. Par exemple, *IP VPN* à base de *PE* peuvent être exécutés sur un squelette séparé, non connecté à Internet, comme ils peuvent utiliser des routeurs de bordure distincte à partir de ceux qui soutiennent le service Internet. Des adresses *IPv4* privées sont parfois utilisées pour fournir une séparation supplémentaire.

Dans un réseau *MPLS*, il est possible de séparer les ressources utilisée pour le plan de commande des celles utilisées pour le plan de données. Cela signifie que les ressources de ce dernier peuvent être protégées et isolées physiquement de tout autre équipement pour protéger les données des utilisateurs tandis que le plan de commande utilise les ressources du réseau qui peuvent être consultées par les opérateurs pour configurer le réseau.

8.6. Utilisation de l'infrastructure agrégée :

En général, il est impossible d'utiliser un ensemble complètement séparé de ressources pour le soutien de chaque service. En fait, l'un des principales raisons pour les services *MPLS* est qu'il permet le partage des ressources entre plusieurs services et plusieurs utilisateurs. Ainsi, même si certains services utilisent un réseau distinct, il y aura encore plusieurs utilisateurs *MPLS* partageant les mêmes ressources réseau. Dans certains cas, les services *MPLS* partagent des ressources réseau avec des services Internet ou d'autres services.

Il est donc important pour les services *MPLS* de fournir la protection entre les ressources utilisées par les différentes parties. Ainsi l'utilisateur doit être protégé contre les possibilités d'inconduite par d'autres utilisateurs. Cela nécessite plusieurs mesures de sécurité à mettre en œuvre. Les possibilités incluent, par exemple l'utilisation d'un routeur ou d'un routeur virtuel logique pour définir le matériel ou les limites des ressources du logiciel par service ou par utilisateur, il aide la limitation du débit par *Virtual Routing and Forwarding (VRF)* ou par connexion Internet, pour fournir une protection de la bande passante ; ou à l'aide de la réservation de ressources pour le trafic de plan de commande.

8.7. Service de processus de contrôle de la qualité fournisseur :

Le déploiement de services VPN fournisseur provisionné nécessite en général une quantité relativement grande de la configuration par le fournisseur des services. Par exemple, le fournisseur de service doit configurer VPN qui appartient à chaque site, ainsi que la qualité de service et des garanties LSR. Cette grande quantité de configuration requise conduit à la possibilité d'une erreur de configuration.
L'authentification CE-à-CE peut être utilisée pour détecter une mauvaise configuration et le cryptage CE-à-CE peut également limiter les dommages en cas de mauvaise configuration.

8.8. Déploiement du service de test MPLS :

Ceci se rapporte à des solutions qui peuvent être facilement testées pour assurer le fait qu'ils soient correctement configurés. Par exemple, pour une connexion point-a-point, en vérifiant que la connectivité destinée travaille assez et qu'elle assure qu'il n'y a pas de connexion non intentionnelle à une autre place.

8.9. Vérification de la connectivité :

Afin de se protéger contre une mauvaise connexion accidentelle ou délibérée, des mécanismes peuvent être mis en place pour vérifier à la fois la connectivité de bout en bout et les ressources saut par saut. Ces mécanismes peuvent retracer les itinéraires de *LSP* à la fois dans le plan de commande et le plan de données. Il convient de noter que si le plan de contrôle est attaqué par une menace, ses mécanismes de contrôle et de connectivité peuvent également être attaqués. Cela peut cacher les défauts grâce à de faux positifs ou perturber les services fonctionnant grâce à des faux négatifs.

9.Etude de cas du BackBone Network IP MPLS de télécommunication:

Pour Faire cet étude nous essayons d'aboutir à un opérateur de télécommunication mais malheureusement la confidentialité des données et l'installation et la mise en place des réseaux MPLS qui sont effectués par le fournisseur du matériel même la configuration des routeurs, pour cela nous seulement décrivons les routeurs installés ainsi présentons une architecture similaire :

9.1. Les routeurs installés:

Figure 3. 3 Routeur Juniper M960

Le routeur Juniper MX960: offre aux entreprises et aux fournisseurs de services des niveaux optimaux de performances, de fiabilité et d'évolutivité. Il dispose d'une capacité système atteignant 10,56 Tbits/s dans un format trois fois inférieur à celui d'un rack de télécommunications standard et prend en charge les interfaces 10 GbE, 40 GbE et 100 GbE haute densité, ainsi que les technologies héritées SONET/SDH, ATM et PDH.

Le routeur MX960 hautes performances est doté de fonctionnalités de routage, de commutation, de sécurité et de service très évolutives, qui ouvrent la voie à des applications génératrices de revenus, à la consolidation des réseaux et à la convergence des services. Le routeur prend notamment en charge un large éventail de services VPN de couche 2 et 3 ainsi que des fonctions de passerelle de réseau haut débit avancées. Il propose également des services de routage, de commutation et de sécurité intégrés.

le MX960 est déployé dans les réseaux stratégiques d'entreprises et de fournisseurs de services du monde entier. Il aide les opérateurs de réseaux à transformer leurs réseaux (et leurs entreprises) afin de prospérer dans notre monde hyper-connecté.

9.2. Architecture BackBone Network IP MPLS:

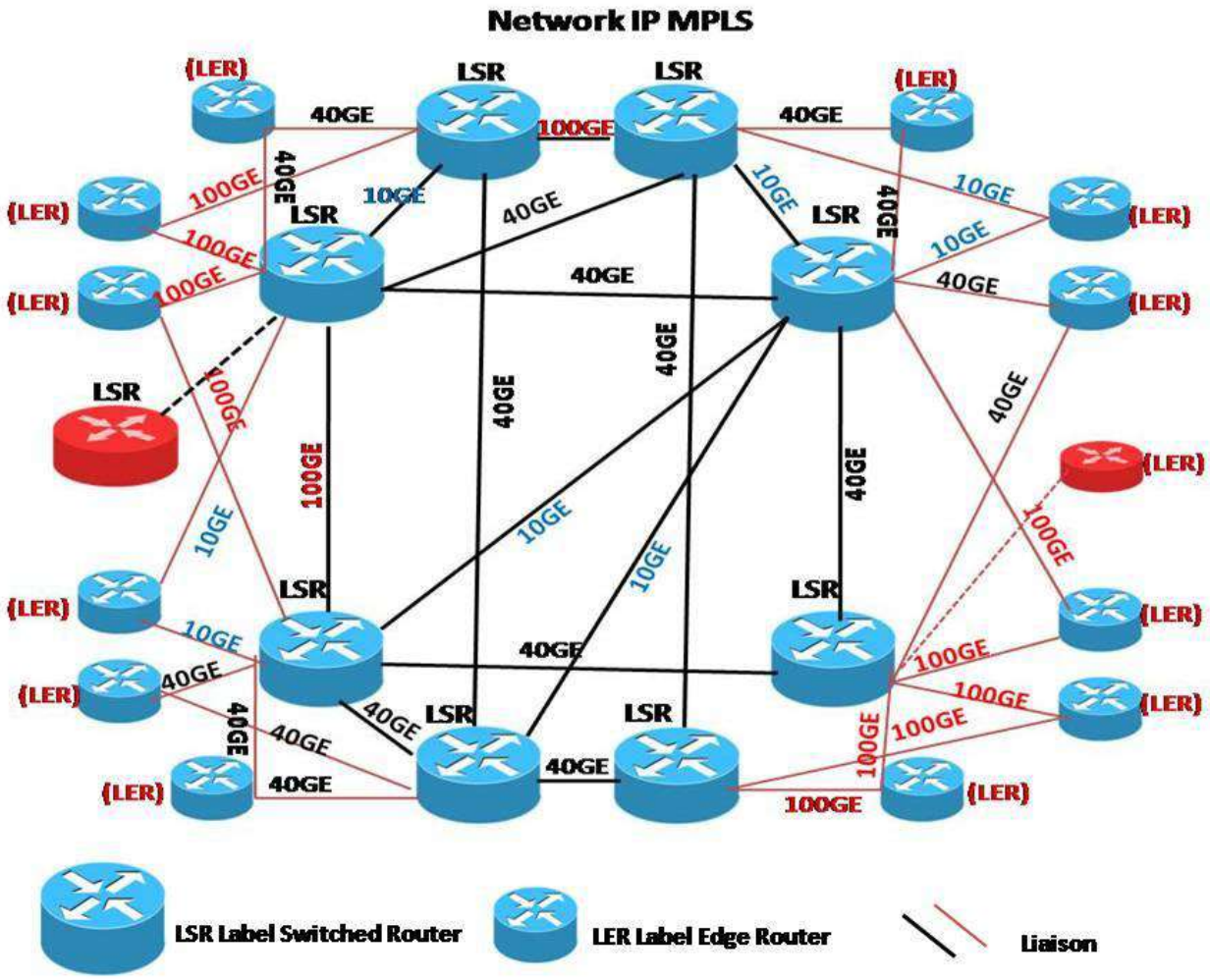

Figure 3. 4 Network IP MPLS

NB:

-Installation des LSR au cœur (core) du réseau MPLS.

-Installation des LER au bord (Edge) du réseau MPLS et qui sont relier avec les routeurs IP des clients CE.

-Le réseau peut être extensible.

9.3.MPLS en pratique :

Après vous avoir introduit les principes de la technologie MPLS, nous avons maintenant présenter un protocole de distribution de label RSVP-TE utilisé pour créer des LSP respectant des contraintes de QoS. Enfin nous allons analyser le fonctionnement d'un service trés utilisé dans les réseaux IP/MPLS : le Virtual LAN Private Services. [35].

9.3.1. ReSerVation Protocol Traffic Engineering RSVP-TE

Le protocole RSVP-TE est un protocole permettant de reserver des ressources dans un routeur afin d'introduire de la QoS dans un réseau. RSVP-TE est un protocole de distribution de labels qui permet d'établir des LSP suivants des contraintes de QoS. RSVP-TE utilise le mode de distribution "DownStream on Demand", et chaque noeud MPLS utilise le protocole UDP pour envoyer des messages RSVP-TE aux autres routeurs MPLS, RSVP-TE va permettre de réserver les ressources nécessaires au LSP dans les LSR et LER lors de l'établissement du chemin. De plus, il va permettre de détecter rapidement les "nodes failure" ou panne de lien ou de routeur. Enfin, cette détection rapide des "nodes failure" permet d'introduire la technologie "FRR ou Fast ReRoute" qui permet de rerouter très rapidement un LSP lorsqu'un noeud ou un lien tombe en panne.
Nous allons maintenant voir les messages qui sont échangés lors de l'établissement d'un LSP grâce au protocole RSVP-TE Figure 3. 5 . [35].

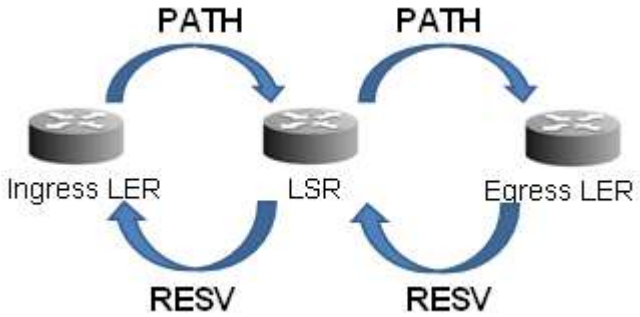

Figure 3. 5 Etablissement LSP

Lorsqu'un Ingress LER veut établir un LSP jusqu'au Egress LER. Le premier envoi un message "PATH" vers le deuxième, qui est le message de demande d'établissement d'un LSP. Ce message est acheminé de proche en proche du Ingress LER vers le Egress LER. Le message "PATH" du protocole RSVP-TE contient les informations suivantes :

- Paramètres de la FEC : adresse réseaux (source et/ou destination), paramètres de QoS caractérisant les paquets associés à cette FEC.
- Priorité d'établissement du LSP : cette priorité d'établissement va servir dans le cas ou le LSP n'arrive pas à être établi par manque de ressource dans le réseau. Le protocole RSVP-TE va comparé la priorité d'établissement de ce LSP à la priorité de maintien des LSP déjà établi. Si il existe des LSP dont la priorité de maintien est plus faible que la priorité d'établissement du LSP à établir, alors les LSP déjà établi vont être "déconnecté" afin de libérer des ressources qui permettront l'établissement du LSP en cours d'établissement.
- Priorité de maintien du LSP : elle définit l'importance qu'il y'a à maintenir ce LSP connecté dans le réseau. Cette priorité est utilisé dans le cas ou il y'a un manque de ressource dans le réseau (description de la priorité d'établissement).
- Objet Record Route : cette objet (ou champ) contient les adresses IP des routeurs qui participent à l'établissement du LSP. Chaque routeur, lorsqu'il voit passer le message "PATH" va ajouter son adresse dans cette objet. Ceci va être utile pour détecter d'éventuel boucle lors de l'établissement du LSP. Cette objet à été ajouter dans l'extension RSVP-TE
- Objet Label Request : objet qui témoigne que ce message "PATH" fait office de demande d'établissement de LSP. Cette objet à été ajouter dans l'extension RSVP-TE.
- Objet contenant les paramètres de QoS du LSP : ce sont les informations qui servent au routeur pour reserver les ressources nécessaires à ce LSP. Cette objet était déjà présent dans le protocole RSVP

Lorsque le Egress LER reçoit le message "PATH", il va répondre par un message "RESV" qui va se propager de proche en proche jusqu'au Ingress LER. Une fois que le Ingress LER à reçu ce message, le LSP est établi et les ressources sont nécessaires sont alloués dans chaque noeud MPLS qui compose le LSP. Le message "RESV" contient les informations suivantes :

- Paramètres de la FEC : adresse réseaux (source et/ou destination), paramètres de QoS caractérisant les paquets associés à cette FEC
- Objet label : contient le numéro de label associé à la FEC par le routeur suivant
- Objet Record Route
- Style de réservation :
    - Fixed Filter : Le LSP aura une bande passante reservé uniquement pour lui
    - Shared Explicit : Le LSP aura une bande passante partagé avec plusieurs LSP qui sont précisés dans le message "RESV".
- Objet contenant les paramètres de QoS du LSP : ce sont les informations qui servent au routeur pour reserver les ressources nécessaires à ce LSP. Cette objet était déjà présent dans le protocole RSVP

A n'importe quel moment pendant l'établissement d'un LSP, l'établissement peut échoué et un message d'erreur est envoyé au Ingress LER. Cette annulation de l'établissement peut par exemple avoir lieu par manque de ressources.

9.3.2. Virtual LAN Private Services:

La technologie VPLS permet à un opérateur d'offrir à un client une offre de VPN de niveau 2. Ainsi, un client peut interconnecter plusieurs sites distants en ayant l'impression que tous les sites sont sur un même LAN. Les clients souscrivant à une offre VPLS sont maître de leur stratégie de routage au sein de leur LAN, car l'opérateur leur offre une connectivité de niveau 2. Dans le schéma ci-dessous, nous n'utiliserons plus le nommage des routeurs propres à MPLS (LSR, LER), mais nous utiliserons une dénomination utilisé par les opérateurs lorsqu'ils décrivent leur réseaux en terme d'accès à des services Figure 3.6, On a donc les routeurs suivants :

- P : Provider Router, ce sont les routeurs de coeur de réseau (backbone)
- PE : Provider Edge Router, ce sont les routeurs aux extrémités du réseau de l'opérateur
- CE : Customer Edge, ce sont les routeurs présent dans le réseaux du client. Ils sont interconnectés avec un ou plusieurs PE.

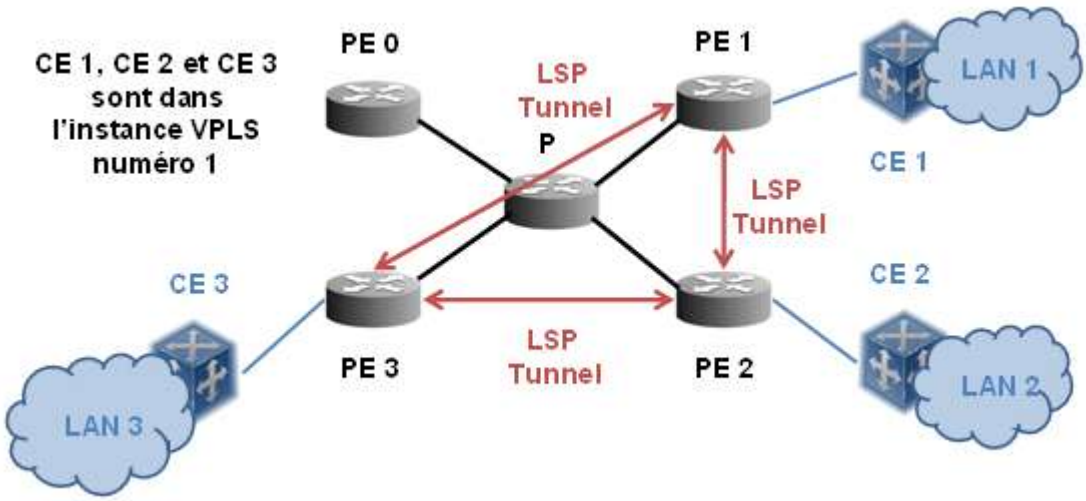

Figure 3. 6 Instance VPLS

Afin d'établir un service VPLS, des Tunnel LSP seront établi entre tous les PE qui interconnecte les CE d'un même client. Ces Tunnels LSP serviront à encapsuler les trames Ethernet qui circuleront. Ainsi lorsqu'un PE reçoit des données via un des LSP Tunnels qui le relie aux autres PE d'une même instance VPLS, il sais qu'il s'agit d'une trame Ethernet encapsulé à destination de l'instance VPLS numéro 1 (dans notre schéma). De façon plus simple, on peut dire que le réseau MPLS forme un switch pour chaque instance VPLS, ou chaque PE est un port du switch. De ce fait, chaque PE possède une table

d'adresse MAC par instance VPLS afin d'avoir une correspondance entre l'adresse MAC d'une machine et son PE de raccordement. Les entrées dans cette table d'adresse MAC ont une durée de vie, comme dans le cas d'une table ARP dans un LAN classique. On peut en déduire le fonctionnement du VPLS, si un PE reçoit une trame à destination d'une adresse MAC inconnu, il va envoyer la trame à travers les Tunnels LSP vers tous les PE qui sont dans l'instance VPLS de l'émetteur de la trame.

Les réseaux IP/MPLS sont présent dans tous les réseaux d'opérateurs, il permet aux opérateurs de répondre à tous leurs besoins en terme de fonctionnalités et ce sans changer leur réseaux IP existants. Les réseaux IP/MPLS reprennent tous les principes intéressant d'autres protocoles comme l'ATM :

- Création de chemin (circuit en ATM)
- Commutation rapide grâce aux labels (VPI/VCI en ATM)
- Gestion de la QoS et du Traffic Engineering dans le réseau (QoS, Traffic Shaping en ATM)

Ainsi, c'est toutes ces fonctionnalités qui permettent aux réseaux IP/MPLS de supporter des services réseaux variés et fiables :

- Etablissement des VPN via VPLS
- Etablissement de lignes point à point virtuels : VLL. Ces "Virtual Leased Lines" peuvent servir à encapsuler divers protocoles comme du TDM, de l'ATM, de l'Ethernet ou du Frame Relay.

10. Conclusion :

Dans ce chapitre, nous avons introduit des informations de base sur la tolérance aux fautes dans les réseaux *MPLS* et les stratégies de sécurité pour *MPLS*.
La revue de la littérature sur tolérance aux fautes dans les réseaux *MPLS*, montre que de nombreuses approches ont été proposées pour le protéger contre les défaillances. Il existe deux principales techniques utilisées pour la restauration des réseaux *MPLS* sont la commutation de protection et le réacheminement. Chacune de ces techniques à des avantages et des inconvénients en termes de perte de paquets, de temps de récupération, de réorganisation des paquets et d'utilisation de la bande passante.

La technique à laquelle nous nous sommes intéressés est celle de la commutation de protection car elle fonctionne mieux que la technique dynamique dans les applications sensibles au temps, nous avons également exploré les questions de sécurité MPLS en introduisant les menaces de sécurité ainsi que les différentes stratégies de défense. Le problème de sécurité dans le réseau MPLS est une question qui évolue et qui n'a pas encore été normalisé, enfin une étude de cas du BackBone Network IP MPLS de télécommunication, les routeurs installés et les liaisons entre différents types de routeurs.

Conclusion générale

Actuellement les opérateurs de télécommunication misent beaucoup d'investissements sur les réseaux de télécommunication modernes, vue leurs utilités, leur facilité d'utilisation et d'intégration de nouveau gammes de services et leur exploitation à faible coût.

Le MPLS offre aux opérateurs télécom des services adéquats à leurs attentes, au niveau de la garantie de transfert et la disponibilité de la bande passante. La gestion des flux de trafic, l'optimisation de la détermination de l'acheminement des paquets, la garantie de la bande passante constituent des améliorations conséquentes par rapport aux technologies utilisées pour les trafics traditionnels.

La norme *MPLS* est l'aboutissement logique de toutes les propositions qui ont été faites comme une norme commune pour transporter des paquets *IP* sur des sous-réseaux travaillant en mode commuté. Les nœuds sont des routeurs-commutateurs capables de remonter soit au niveau *IP* pour effectuer un routage, soit au niveau trame pour effectuer une commutation.

Références

[1] L'International Telecommunication Union (ITU) , La Recommandation UIT-T Y.2001, la commission d'etude 13 (2005-2008) de l'UIT-T, 17 /12/ 2004.

[2] a. D. Organisation for Economic Co-operation et Ministerial Council Meeting, «CONVERGENCE AND NEXTGENERATION NETWORKS,» the future of internet economy, Korea, 2008.

[3] «NGN (Next Generation Networks,» Technical university in Prague, Prague.

[4] Simon ZNATY et Jean-Louis, «Architecture NGN Du NGN Téléphonie au NGN Multimédia,» DAUPHIN EFORT.

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

[6] CRIMI et J.,C, Next Generation Network (NGN) Services, Telcordia Technologies, 2002.

[7] L. Roberts, The evolution of packet switching, Proceedings of the Institute for Electrical and Electronic Engineers 1978, 66 (11), 1307 – 1313., 1978.

[8] K. Thurber, Circuit Switching, IEEE Computer, 12(6), 8 – 9., 1979.

[9] Z. &. C. D. R. Haas, A case for packet switching in high-performance wide-area networks, Proceedings of the ACM workshop on Frontiers in computer communications technology , 402 – 409, 1987.

[10] Y. &. L. J. Kang, The implementation of the premium services for MPLS IP VPNs, Proceedings of the 7th International Conference on Advanced Communication Technology , 1107 – 1110, 2005.

[11] U. M. Oscar, ETUDE COMPARATIVE DU TRANSFERT DE DONNEES PAR LES PROTOCOLES MPLS ET ATM DANS UN RESEAU MAN, INSTITUT SUPERIEUR DES TECHNIQUES APPLIQUEES, 2013.

[12] L. D. Ghein, MPLS Fundamentals, Cisco Systems, Inc., 2007.

[13] W. Stallings, «MPLS,» *The Internet Protocole Journale,* vol. 4, n° %13, 2001.

[14] C. S. Learning, Implementing Cisco Service Provider Next-Generation Core Network Services, Cisco, 2012.

[15] S. A. Alouneh, On Fault-Tolerance and Security in MPLS Netowrks, Concordia University, Canada., 2008 .

[16] J. Arlat, Y. Crouzet, Y. Deswarte, J.-C. Fabre, J. C. Laprie et D. Powell, Encyclopédie de l'Informatique et des Systèmes d'Information, chapitre Tolérance aux fautes, Vuibert, 2006, p. pages 241–270.

[17] M. Marouf, Ordonnancement temps réel dur multiprocesseur tolérant aux fautes appliqué à la robotique mobile, French: Ecole Nationale Supérieure des Mines de Paris, 2012.

[18] J. Liuo et R. Lu, Monitoring Network through SNMP-based System, vol. Vol.5, International Journal of Intelligent Engineering and Systems, 2012.

[19] M. Hadjiona, C. Georgiou, M. Papa et V. Vassiliou, A Hybrid Fault Tolerant Algorithm for MPLS Networks, 2008.

[20] J. Wu1, C. Guo, P. Yan et J. Zhou, Traffic Balance after Link Failures Using Few Weight Changes, International Journal of Intelligent Engineering and Systems 2, 2008, pp. 40-47.

[21] O. Klopfenstein, Robust pre-provisioning of local protection resources in MPLS networks, 2007.

[22] J. T. Park, S. Member, IEEE, J. W. Nah et W. H. Lee, Dynamic Path Management with Resilience Constraints under Multiple Link Failures in MPLS/GMPLS Networks, vol. 5, IEEE Transactions On Dependable And Secure Computing , july sept 2008.

[23] S. Alouneh, A. En-nouaary et A. Agarwal, A Multiple LSPs Approach to Secure Data in MPLS Networks, vol. 2, Journal Of Networks, august 2007.

[24] E. R. Naganathan et S. Rajagopalan, Effective Traffic Management in MPLS using Traffic Flow Analysis Based ACO Algorithm, vol. 72, European Journal of Scientific Research ISSN 1450-216X, 2012, pp. 482-489.

[25] M. HossienYaghmae et F. Jafari, A New Fault Tolerant Routing Algorithm For GMPLS/MPLS Networks, 2004.

[26] V. Sharma et H. F., Framework for Multi-Protocol Label Switching (MPLS)-based Recovery, RFC 3469, 2003.

[27] K. Makam, C.Huang et V.Sharma, Building reliable MPLS Networks Using a Path Protection Mechanism, IEEE Communication Magazine, March 2002, pp. 156-162.

[28] T.Saad, B.Alawieh et H. Mouftah, Tunneling Techniques for End-to-End VPNS generic Deployment in an Optical Testbed Environment, IEEE Communication Magazine, 2006, pp. 124-132.

[29] J.Chung, S.Panguluru, L.Dongfang et R.Garcia, Muliple LSP Routing Network Security for MPLS Networking, IEE-MWSCAS, 2002 , pp. 605-608 .

[30] Security of the MPLS Architecture, Cisco Press, 2001.

[31] I. PLC, MPLS SECURITY OVERVIEW, DECEMBER 2007.

[32] I. E. T. F. (IETF) et L. Fang, Security Framework for MPLS and GMPLS Networks, Request for Comments: 5920 ISSN: 2070-1721 éd., Cisco Systems, Inc., July 2010.

[33] J. informatique, 2006.

[34] C. N. Academy, *CCNA V5*, San Franscisco: CISCO, 2014.

[35] Les réseaux IP/MPLS Yazid KARKAB