Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Virtuelle de Tunis

MEMOIRE
DE STAGE DE FIN D'ETUDES

Pour l'obtention du

«Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR)»

Présenté par :Dridi Mahmoud

Optimisation d'une infrastructure IP-MPLS d'un opérateur et intégration de l'IPv6

Soutenu le : 12/7/2018

Devant le jury :

Président : Mr.(Mme.)**M. Mohamed SAKOUHI**

Encadreur : Mr.(Mme.)**M. Khaled Ghorbel**

Rapporteur : Mr.(Mme.)**Mme. Imene AMMARI**

Membre : Mr.(Mme.).....

Année Universitaire : 2017 / 2018

Dédicace

A mes très honorables parents

Je consacre mes dédicaces de ce projet fin d'étude à mon père et à ma mère « Latifa », pour l'amour qu'ils m'ont encore apporté, leurs immenses aides et tout le support qu'ils m'ont porté.

Aucun hommage ne serait suffisant pour exprimer mon respect, ma gratitude, et mon grand amour pour les sacrifices qu'ils ont consentis pour mon parcours d'éducation et mon contentement.

Veuillez découvrir ici, mes chers, dans cet humble projet, l'aboutissement de tant de dévouement ainsi que l'expression de ma gratitude et de mon amour sincère.

Que Dieu leurs fait offrir tout le bonheur du monde et leurs offre-le paradis et la prospérité et une longue vie afin que je puisse un jour compenser de plaisir leurs vieux jours.

A ma chère fiancée « Fadwa »

Pour son fidèle amour et son soutien sentimental et spirituel. C'est la générosité et la tendresse. Elle représente pour moi l'amitié et l'amour de ma vie. Elle demeurera éternellement gravée dans ma mémoire. Puisse Dieu l'accorder la santé. Qu'elle restera toujours à mes côtés.

A mes frères

Je leurs remercie pour tous les efforts qu'ils m'ont cédés pendant mon parcours d'études. Que Dieu leurs accorde le ravissement et la joie.

A tous mes amis

je leurs avoue mes sincères remerciements. Que Dieu leurs protège, et leurs fait offrir tout le bonheur du monde.

Dridi Mahmoud

Remerciements

Initialement, je remercie **Mr Hichem Harhira**, Directeur Technique de **NextStep IT** qui m'a donné l'occasion d'achever mon projet avec l'équipe de NextStep IT.

Je tiens dans la suite à remercier **Mr Boulbeba labiadh**, Directeur Commercial de NextStep IT, je lui suis redevable de m'avoir accueilli dans son équipe où j'ai pu exécuter ce projet.

Ma gratitude va similairement au personnel de **NEXTSTEP IT** qui a participé à l'achèvement de ce projet. Je les remercie pour leur patience, pour leurs conseils, et pour tout le temps qu'ils m'ont consacré.

Nos remerciements s'adressent spécialement à **Mr Hichem Maalaoui** Directeur Général de NextStepIT.

Je remercie profondément pour ces recommandations avisées mon superviseur **Mr khaled ghorbel** qui m'a fait l'honneur d'être mon encadrant et qu'il a agréé de suivre les détails de l'avancement de mon projet. Je suis aussi, reconnaissant pour son fréquent partage de ses connaissances. Pour sa réception chaleureuse et son esprit de coopération et pour l'intérêt et l'attention qu'il a tenue à mon travail. Grâce aussi à sa confiance j'ai pu atteindre parfaitement mes missions, et mes devoirs. Aussi grâce à son aide inappréciable dans les moments les plus délicats et pour son suivi de particularités de déroulement de mon travail, de même que son assistance et ses instructions.

Finalement, je tenais à remercier **les membres de jury** qui vont évaluer mon travail et qui ont bien voulu m'honorer par leur présence.

Dridi Mahmoud

Avant-Propos

Ce projet est le résultat de missions achevées pendant mon stage de fin de formation, stage effectué pour l'obtention du Diplôme **en mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux**.
Ce stage, m'a permis de mettre en pratique les connaissances acquises durant le parcours universitaire et m'a apporté une expertise spécialiste me préparant au futur. Ce stage a été réalisé au sein du **NextStep IT** qui est l'une des pionner sociétés de d'IT.

Dès le commencement du stage, il m'a été demandé d'effectuer une nouvelle idée qui comporte la recherche et la mise en œuvre d'une solution idéale d'une structure réseau privée et sécurisée.

Pendant ce stage, mon activité se récapitule à apprendre les notions de la technologie MPLS. Il est devenu réalisable d'assurer une qualité de service opérante avec un contrôle amélioré sur VPN. En outre, c'est réalisable de créer une ligne de *backup* en cas d'interruption de la ligne principale et de mener une étude sur l'assimilation de l'IPv6.

Cette procédure m'a permis développer des nouvelles perceptions conceptuelles et pratiques.
L'aboutissement pratique apporté est un réseau IP-MPLS optimisé, efficace et sécurisé.
Vous apercevez donc dans ce projet fin d'étude, la suite de ce stage qui me qualifie simultanément à une formation profonde et à une jouissance personnelle.

Table des matières

Table des figures

Introduction Générale

INTRODUCTION GENERALE

L’internet est aujourd'hui une infrastructure d'information très répandue, le prototype initial de ce qu'on appelle souvent l'infrastructure d'information nationale (ou mondiale ou galactique). Son histoire est complexe et impose de nombreux aspects - technologiques, organisationnels et communautaires. Notamment, son influence s'étend non seulement aux domaines techniques des communications informatiques, mais aussi à l'ensemble de la société, alors que nous nous orientons vers l'utilisation croissante des outils en ligne pour accomplir le E-commerce, l'acquisition de l'information et les opérations communautaires et les services d’hébergements.

Par conséquent, avec la progression rapide de ces services et l’apparition de la notion de IOT le besoin de connexion à haute débit était très important pour cela MPLS serait simple le remède la plus appropriée pour ces réseaux car elle permet d’associer très facilement de nouvelles technologies dans un cœur réseau existant.

Désormais, la mise en œuvre d’un backbone MPLS et la mise en place d’ une solution de backup avec l’intégration de l’IPv6 et la configuration de la qualité de service est le travail que j’ai développé dans ce PFE qui s’est déroulé au sein du département système informatique du NextStep IT. Eventuellement, dans ce contexte qu’elle nous a confié la réalisation du projet intitulé :« Optimisation d’une Infrastructure IP-MPLS d’un Opérateur et Intégration de l’IPv6 »Ce projet est composé de trois chapitres :

Dans le premier chapitre, **« Présentation de l’entreprise de l’accueil »,** nous présenterons l’entreprise d’accueil, le cadre général du projet et la problématique de notre projet. Au cours du second chapitre, **« Etat de l’art »,** nous allons étudier les concepts de bases de la technologie MPLS, dans la seconde partie de ce chapitre nous présenterons la résolution et l’optimisation du problème de la redondance avec une solution de secours et nous finissons la dernière partie de ce chapitre par l’intégration de l’IPv6.

Dans le troisième chapitre, **« Réalisation »** nous présentons une émulation d’un cœur du réseau IP-MPLS en offrant une solution de backup(ADSL) puis l’intégration de l’IPv6 en assurant la performance de ce réseau élaboré.

Le rapport se termine par une conclusion générale sur la totalité du travail accompli durant le stage et une partie Néographie.

Chapitre 1 :

Présentation de l’entreprise

Introduction

Ce premier chapitre est réservé pour présenter l'entreprise d'accueil « NextStepIT» qui est une société d'informatique tunisienne qui sert à aider les entreprises d'avoir une infrastructure IT capable d'améliorer leur rentabilité augmenter la satisfaction de ces clients et réduire le risque opérationnel, riche par sa large expérience et sa grande équipe d'ingénieurs et des techniciens certifiés (en CCNA, CCNA Voice, CCNA Security , CCNP, CCIE Routing and Switching ….)

Figure 1: Qualification de NextStep –IT

I. Organigramme de NextStep IT

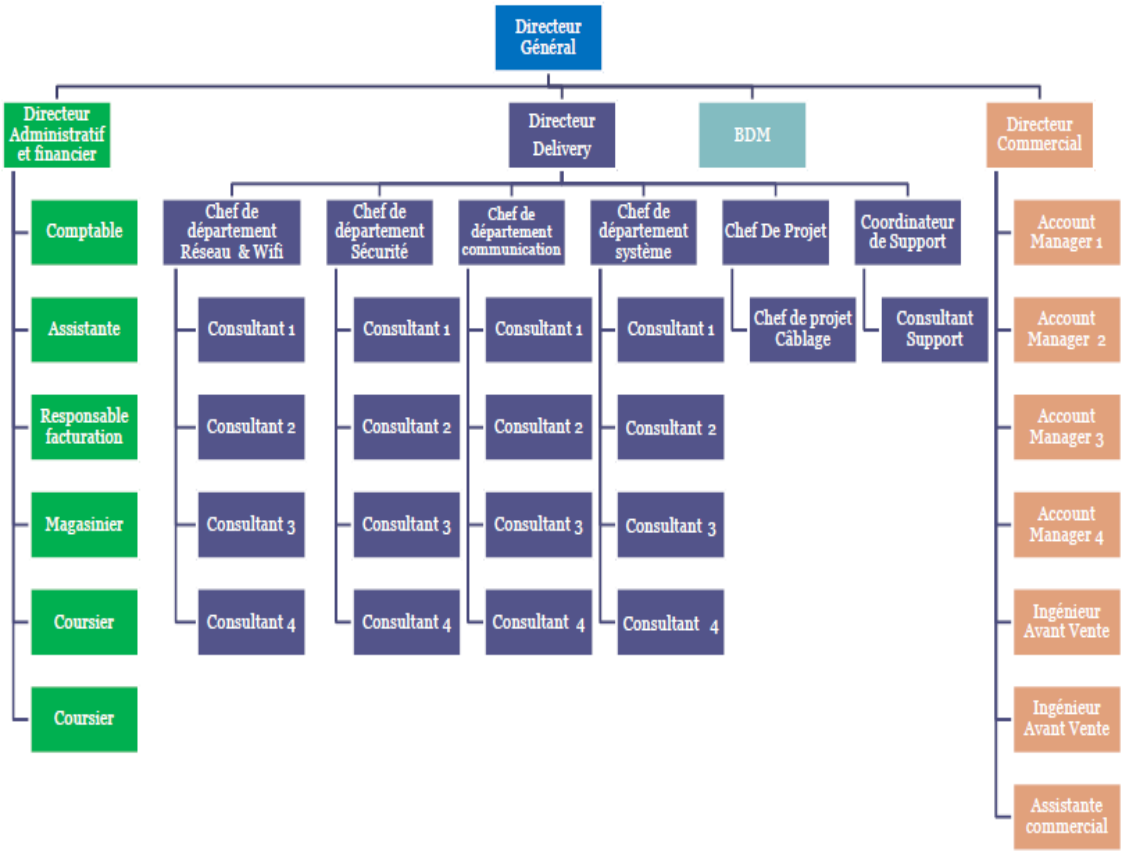

Figure 2: Organigramme de NextStep

II. Activités du NextStep IT

NextStep-IT fourni des divers services :

- Audit
- Etude et conseil
- Intégration
- Assistance

III. Cadre du projet

Ce travail s'inscrit dans le cadre de la préparation du projet de fin de formation, il nous a permis de mettre en pratique les connaissances acquises tout le long de notre formation. En plus il nous a fourni l'occasion d'apprendre à s'intégrer dans la vie professionnelle, de faire

face aux différentes situations et problématiques rencontrées et de présenter les solutions les plus adéquates. Afin de mener ce travail à terme, et pour une durée de quatre mois, nous avons été accueillies au sein de NextStep IT.

IV. Contexte du travail

Après la description du cadre général du déroulement du projet, place maintenant à détailler la problématique, ainsi qu'une description du projet, le travail demandé et les objectifs visés par ce travail.

IV.1 Problématique

Le réseau se compose de plusieurs sites distants classés en trois parties :

- Siège
- Agence de site A.
- Agence de site B

Ces différents sites sont liés au siège via le backbone MPLS de la Tunisie Telecom et en utilisant un routage dynamique basé sur le protocole OSPF ainsi qu'un routage statique pour configurer certaines routes spécifiques.

Les lignes d'interconnexion WAN utilisées sont :

- Des fibres optiques.
- Des lignes ADSL (Backup).

IV.2 Contexte spécifique de projet

La technologie MPLS offre des choix de connectivité dans les réseaux étendus et les avantages sont multiples en termes de fiabilité et efficacité. Cependant, on peut améliorer notre architecture MPLS surtout vis-à-vis client.

En fait, L'opérateur doit jouer un rôle dans la configuration du réseau global. Tout en utilisant le routage dynamique, vous devez garder à l'esprit que vous et votre fournisseur devrez travailler ensemble pour le routage du trafic MPLS. Si vous voulez un contrôle total de votre réseau MPLS peut ne pas être pour vous. En plus, un réseau MPLS n'offre aucune protection de données inhérente et une mise en œuvre incorrecte peut ouvrir votre réseau à des

Vulnérabilités. Absence totale de l'IPv6 sur le nuage IP-MPLS, avec la demande de quelques clients.

IV.3 Description du projet

Ce projet consiste à résoudre ces points en coordinations avec l'équipe IT de NextStep.

IV.4 Planification

- Etude de l'existant et préparation d'un réseau IP-MPLS simple avec un CPE Siège et 2 CPE agences.
- Résolution et optimisation du problème de la redondance.
- Intégration de l'IPv6.
- Optimisation du filtrage.
- Configuration des politiques de service adéquat au besoin de client
- Le pilotage de réseau se fait par le client lui-même

Conclusion

Dans ce présent chapitre, nous avons présenté l'entreprise d'accueil NextStep. De même nous avons présenté le cadre de notre projet et son contexte général, par la suite nous avons suivi le travail qui nous a été demandé tout au long de ce projet.

Chapitre 2 :

Etude de l’état de l’art

Introduction

Les critères qui définissent la qualité de de service manifestent essentiellement par la disponibilité de services (connectivité) et un taux de latence minimale. Grace à la technologie MPLS, il est devenu réalisable de garantir des services tel que VPN, QOS…tout ça avec un débit de haute niveau . Tout au long de ce chapitre nous allons déterminer l'architecture MPLS en argumentant son principe de fonctionnement et son architecture et en précisant des applications qu'elle propose et des méthodes a fin de l'améliorer.

I.1 Architecture MPLS

L'architecture MPLS décrit les mécanismes permettant d'effectuer une commutation d'étiquette, qui combine les avantages du transfert de paquets basés sur la commutation de couche 2 avec les avantages du routage de couche 3. Similaire aux réseaux de couche 2 (par exemple, Frame Relay ou ATM), MPLS assigne des étiquettes aux paquets pour le transport à travers des réseaux à base de paquets ou de cellules. Le mécanisme d'acheminement dans tout le réseau est un échange d'étiquettes, dans lequel les unités de données (par exemple, un paquet ou une cellule) portent une courte étiquette de longueur fixe indiquant aux nœuds de commutation le chemin et la transmission des données. L'objectif est d'associer la puissance de la commutation de la couche liaison avec la souplesse du routage de la couche réseau donc la vitesse de transmission des données.

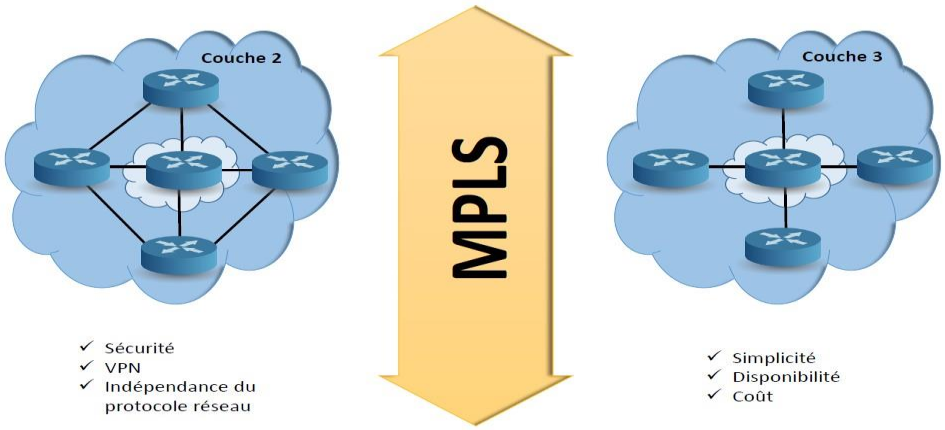

Figure 3: Positionnement de MPLS dans le modèle OSI

De la même façon que pour des réseaux de couche liaison, MPLS attribue des labels à des paquets pour les transporter sur des réseaux basés sur la commutation de labels ou de cellules.

I.2 Structure fonctionnelle MPLS

L'architecture MPLS est divisée en deux composants distincts :

- Le composant de transmission également appelé plan de données
- Le composant de contrôle également appelé plan de contrôle

Le composant de données utilise une base de données d'acheminement de labels maintenue par routeur LSR pour effectuer le transfert de paquets de données sur la base d'étiquettes transportées par des paquet. Le composant de contrôle est responsable de la création et de la maintenance des informations de transmission d'étiquettes (appelées liaisons) entre un groupe de LSR interconnectés.

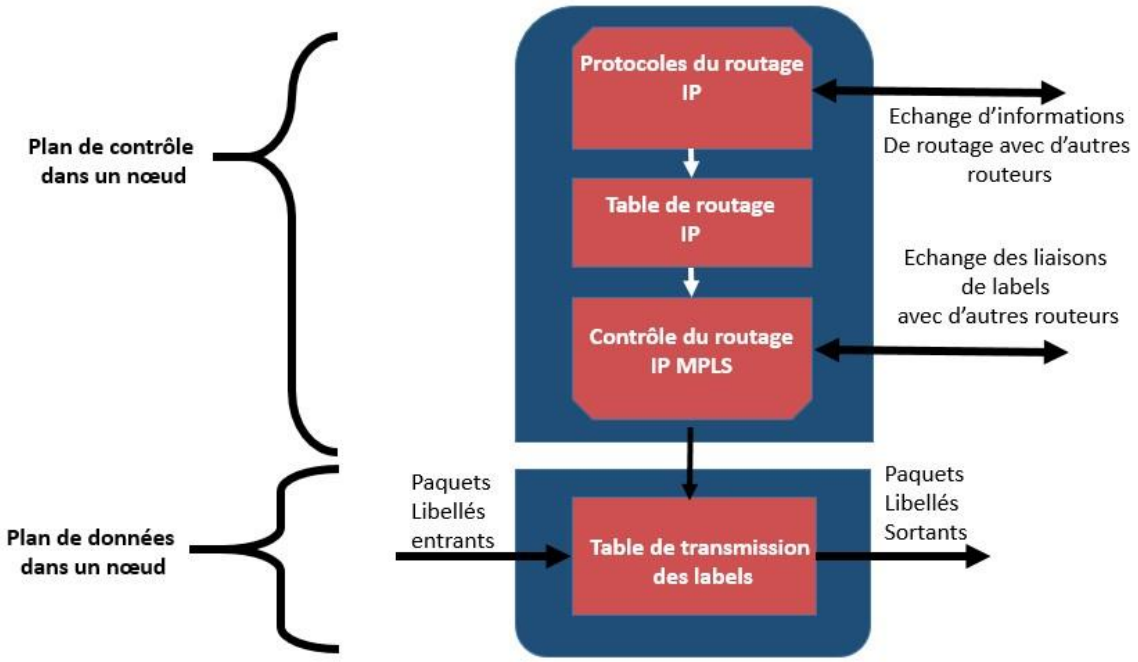

Figure 4: L'architecture de la base d'un nœud MPLS réalisant le routage d'IP

I.3 Composant du réseau MPLS

Plusieurs notions ont été créées pour expliquer les dispositifs qui constituent l'architecture. Ces nouveaux termes désignent les fonctionnalités de chaque dispositif dans la structure de la technologie MPLS.

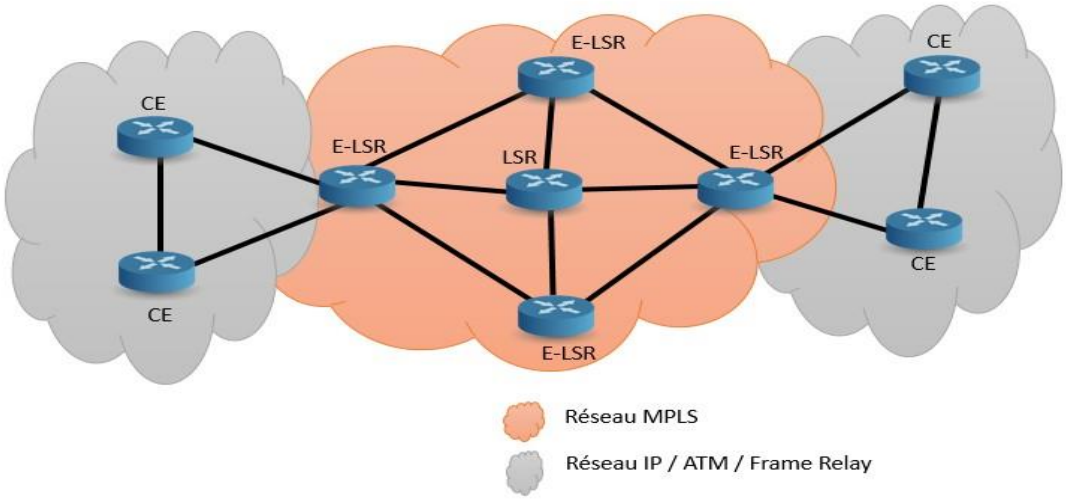

Figure 5: Les composants du réseau MPLS

Comme dans la figure 6, Il existe plusieurs types des composants :

On va tout d'abord parler de **routeur commutateur d'étiquette** (**LSR)** . Un routeur de commutation d'étiquette (LSR) présente le cœur d'un réseau à commutation par étiquette. Les réseaux à commutation d'étiquettes sont constitués de chemins prédéterminés, appelés chemins à commutation par étiquette (LSP), qui résultent de l'établissement de session entre la source et la destination par le processus MPLS (Multi-Protocol Label Switching). Les routeurs LSR prennent en charge MPLS, ce qui assure que tous les paquets acheminés sur une route spécifique resteront dans le même chemin sur un backbone.

Il existe d'autre type de LSR ce qu'on appelle Un **Edge LSR** ou**Provider Edge Router** , ''PE'' est un routeur de bordure qui réalise l'imposition de label (parfois également appelée action push) ou la disposition de label (également appelée action pop) à la périphérie du réseau MPLS.

L'imposition de label se manifeste à donner un label ou ensemble de labels a des paquets, au point d'entrée à l'infrastructure MPLS. La disposition de label est l'intervention inverse ; elle a

pour objectif de dissocier le label de paquet egress qui sera transmis à un voisin situé hors du domaine MPLS.

Label Distribution Protocol LDP est l'ensemble de procédures utilisées par les LSR pour établir des LSP. Il assure le mappage entre les informations de routage de la couche réseau directement vers les chemins de commutation de couche de liaison de données.

Un LSP : Label Switched Path est un chemin à commutation par étiquette (LSP) est un chemin unidirectionnel à travers le réseau MPLS

Une FEC: Forwarding Equivalent Class, est une représentation d'un ensemble de paquets à pour but d'indiquer les classes de transfert de paquets.

I.4 Principe de fonctionnement de MPLS

L'architecture MPLS est basée sur la commutation de label(d'étiquette). La figure suivante indique globalement ce principe.

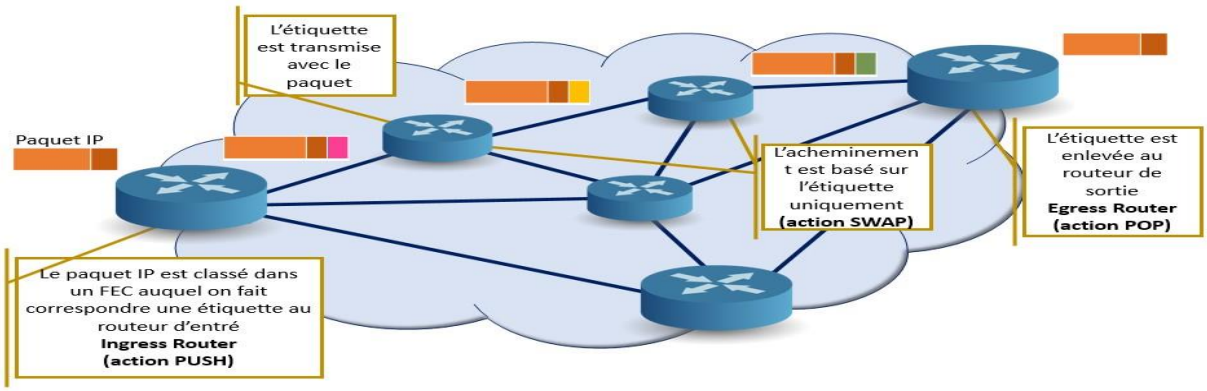

Figure 6: Principe de fonctionnement de MPLS

Lorsqu'un paquet entre dans le routeur ingress, MPLS assigne les paquets avec des étiquettes pour la transmission de données à travers le réseau. Les étiquettes de l'en-tête MPLS sont introduites dans le paquet de données à attribuer. Ces étiquettes de longueur fixe portent les informations, qui permettent à chaque routeur de commutation de traiter et d'envoyer les paquets à la destination. Au fur et à mesure que chaque nœud transfère le paquet, il passe l'étiquette en cours pour l'étiquette la plus appropriée au nœud suivant pour acheminer le paquet. Quand un paquet abouti le routeur de sortie, les étiquettes sont retirées et le paquet est transmis au réseau IP de destination. Ce mécanisme permet la commutation de paquets à très haut débit à travers le domaine MPLS de base.

I.5 Avantages de MPLS

Aujourd'hui, les ASIC de produits peuvent réaliser plusieurs dizaines de millions de examens de routage IP par seconde, relativement à bas prix et facilement. Cependant, ils constituent encore une partie importante du coût d'un routeur. L'exact Matching est toujours beaucoup moins cher et plus facile à mettre en place. Un commutateur Ethernet (qui effectue un Matching exact) peut représenter 1/4 du coût et 4 fois la capacité d'un périphérique similaire. Alors, pourquoi les gens s'intéressent-ils toujours de MPLS ? C'est pour trois raisons : Implémentation de l'ingénierie du trafic, la possibilité de contrôler où et comment le trafic est routé sur votre réseau, de gérer la capacité, de hiérarchiser les différents services et d'éviter la congestion et pour la mise en œuvre de réseaux multi services. Aussi pour sa capacité à fournir des services de transfert de données, ainsi que des services de routage IP, à travers la même infrastructure de réseau à commutation par paquets. Et, probablement pour son amélioration de la résilience du réseau avec MPLS Fast Reroute.

II. Dynamic Multipoint VPN

Introduction

DMVPN (Dynamic Multipoint VPN) est une technique de routage que nous pouvons utiliser pour créer un réseau VPN avec plusieurs sites sans être obliger à configurer d'une manière statique tous les périphériques. C'est un réseau "hub and spoke" où les spokes pourront communiquer directement entre eux sans passer par le hub. Le cryptage est pris en charge via IPSec, ce qui fait de DMVPN un choix populaire pour la connexion de différents sites à l'aide de connexions Internet régulières. C'est un excellent backup ou une alternative aux réseaux privés comme VPN MPLS.

Il y a quatre indispensables piliers pour qu'on puisse parler du DMVPN : GRE multipoint (mGRE), NHRP (Next Hop Resolution Protocol), Routage (RIP, EIGRP, OSPF, BGP, etc.), IPSec (non obligatoire mais recommandé)

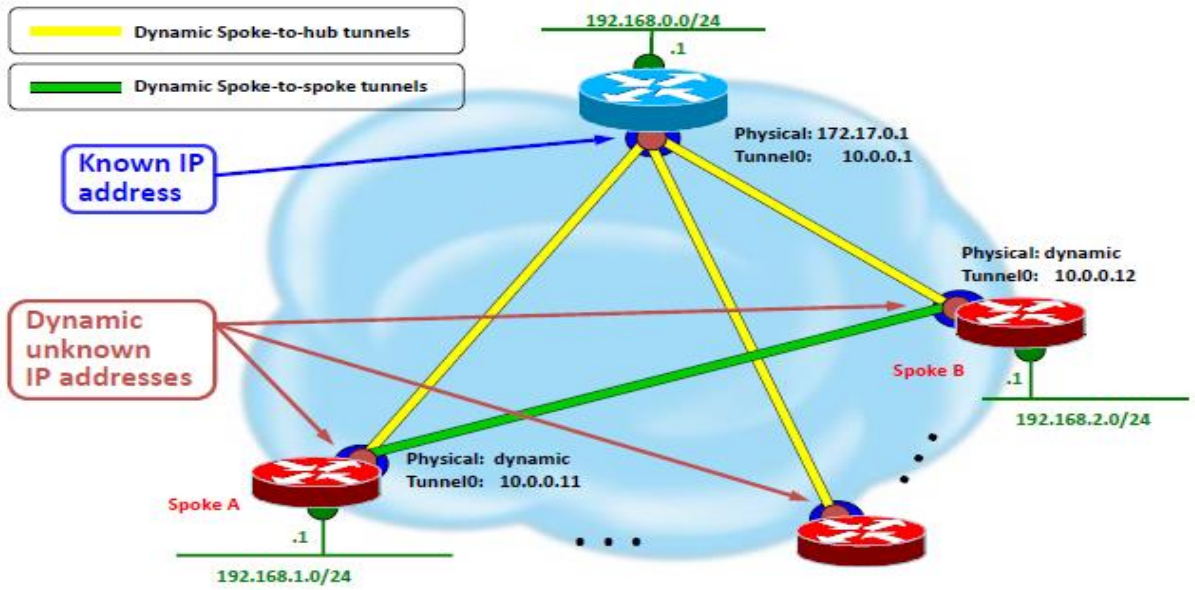

Figure9: Architecture DMVPN

II.1 Next Hop Resolution Protocol (NHRP)

Nous avons besoin de l'aide pour notre routeur branch1 à comprendre quelle est l'adresse IP publique du routeur branch2, nous le faisons avec un protocole appelé NHRP (Next Hop Resolution Protocol défini dans le document RFC 2332). En fait, Un routeur sera le serveur NHRP.Tous les autres routeurs seront des clients NHRP.Les clients NHRP s'enregistrent auprès du serveur NHRP et signalent leur adresse IP publique. Le serveur NHRP assure le suivi de toutes les adresses IP publiques dans son cache. Quand un routeur veut acheminer quelque chose à un autre routeur, il demandera au serveur NHRP l'adresse IP publique de l'autre routeur.

Puisque NHRP utilise ce modèle de serveur et de client, il est logique d'utiliser une topologie pour le GRE multipoint. Notre routeur hub sera le serveur NHRP et tous les autres routeurs seront les spokes.

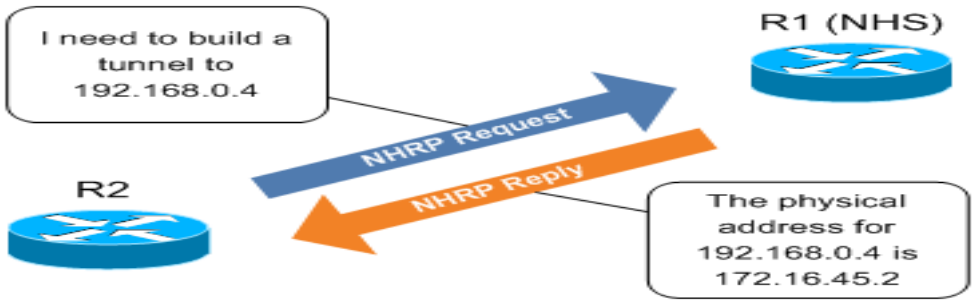

Figure 7:L'echange des messages de protocoles NHRP

II.1.1 Fonctionnement – Hub to spoke

On a deux acteurs :

- DMVPN Hub / NHRP Servers (NHS).
- DMVPN Spokes / NHRP Clients (NHC).

Employer NHRP afin que les spokes soit en mesure de s'inscrire auprès du hub. Le hub est l'unique routeur qui se sert d'une interface mGRE, l'ensemble des spokes adopteront des interfaces fréquentes de tunnel point à point GRE. Cela indique qu'il n'y aura pas de communication directe entre les spokes, tout le trafic doit passer par le hub !

II.1.2 Fonctionnement – Spoke to Spoke

Les inconvénients de la première phase est qu'il n y a pas un tunnel direct spoke to spoke. Dans la phase deux tous les spokes routeurs utilisent mGRE. Donc on obtient un tunnel direct spoke to spoke. Finalement, quand un spoke routeur veut communiquer avec un autre, il envoie vers le hub une demande NHRP afin de trouver une adresse NBMA IP d'un autre spoke.

II.2 NHRP Important messages

II.2.1 NHRP Registration Request

- Les Spokes enregistrent leurs IP NBMA et VPN au serveur NHS(hub)
- Important l'établisement des tunnels entre le hub et les spokes en phase 1

II.2.2 NHRP Resolution Request

- Les Spokes réquirent les mappings NBMA-to-VPN des autres spokes
- Necessaire pour construire les spoke-to-spokes tunnels

II.2.3 NHRP Redirect

- Permet la redirection de message entre deux spoke.

- Joue le même rôle que IP redirect.
- Permettre l'établissement de tunnel spoke to spoke au cours de la phase 3.

II.3 Avantages du VPN multipoint dynamique (DMVPN)

Dynamic multipoint VPN utilisent mGRE (Multipoint GRE), et NHRP (Next Hop Resolution Protocol), pour former des tunnels à la volée, ce qui fournit des avantages majeurs tel que :

- Réduction de la configuration et déploiement sans contact.
- Prend en charge IP Multicast et les protocoles de routage dynamique tel que (EIGRP, OSPF).
- Prend en charge les homologues distants avec des adresses attribuées dynamiquement
- Les spokes pourront communiquer directement entre eux
- Utilisable avec ou sans chiffrement IPSec.

III. Intégration de l'IPv6

Introduction

Étant donné que l'Internet est devenu une infrastructure globale déterminante pour la croissance socio-économique et qu'il se développe plus précipitamment dans les pays en cours de développement il existe un certain nombre de facteurs clés pour accélérer la migration vers le protocole IPv6 dans ces pays. Par exemple IPv6 permet un accès Internet mobile plus vaste, maintient le développement des entreprises et trace la voie à de services innovants (en particulier dans les domaines de la voix la vidéo et d'autres applications multimédias). Comme l'épuisement d'IPv4 devient de plus en plus nécessaire les opérateurs de réseaux du monde entier se penchent de plus près sur la migration vers IPv6.

III.1 Système d’adressage

Le format et la représentation des adresses sont les changements les plus repérables pour l’utilisateur expérimenté et l’ingénieur réseau dans cette nouvelle version de protocole Bien que les principes soient vivement identiques à ceux employés dans IPv4, cet adressage apparait

clairement plus compliqué. Il est intéressant d'en assimiler l'idée et les réglementations d'attribution avant d'aborder les formes protocolaires.

Une adresse IPv4 est codée sur 32 bits (4 octet) et une adresse IPv6 est codée sur 128 bits ce qui donnait des milliards de milliards de milliards d'adresses quelque chose qui repousse l'imagination.

Il y a trois types d’adresses :

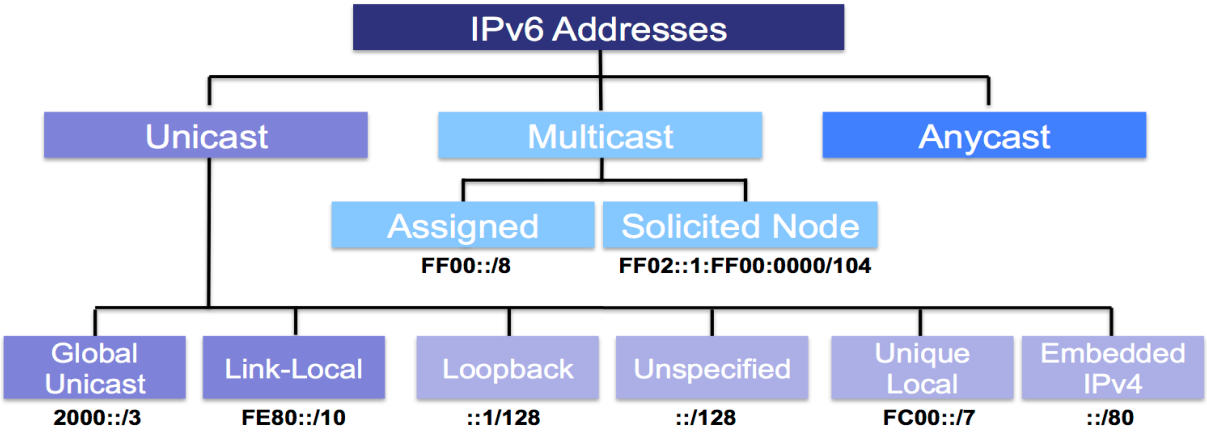

Figure 8: Les types d’adresses IPv6

- Unicast (monodiffusion) : identifiant pour une seule interface. Un paquet transmis à une adresse d'émission individuel est fourni à l'interface détectée par cette adresse.
- Multicast (multidiffusion) : identifiant pour un ensemble d’interfaces. Un paquet envoyé à une adresse de diffusion groupée est livré à toutes les interfaces identifiées par cette adresse.

- Anycast : identifiant pour un ensemble d'interfaces (appartenant normalement à des nœuds différents). Un paquet envoyé à une adresse d'émission à la cantonade est fourni à une des interfaces identifiées par cette adresse.

Une interface a la possibilité d'avoir plusieurs adresses de nature différents (unicast, anycast et multicast).Il n'y a pas d'adresses de diffusion, parce que leur fonction est faite par les adresses multicast. En outre, la fonctionnalité broadcast est pénalisante, parce qu'elle requiert un certain traitement pour chaque nœud bien que ce dernier va ignorer le paquet publié en broadcast. Le multicast cible certains nœuds uniquement ce qui est plus économique.

L'adressage IPv6 permet de regrouper les adresses hiérarchiquement, par réseau, par fournisseur d'accès, géographiquement, par établissement, etc. De tels regroupements permettront sans doute de baisser la dimension des tables de routage et de donner un coup de boost le traitement au niveau des routeurs multicast cible certains nœuds uniquement ce qui est plus économique.

III.2 Plan d'adressage

III.2.1 Adresses globales d'ensemble unicast

Plusieurs façons de hiérarchiser les adresses IP ont été offerts. La dernière proposition à l'IETF est dite 'Aggregatable Global Unicast Address Format' ou plan d'adressage agrégé.

Ce plan hiérarchise une adresse IP de la manière suivante :

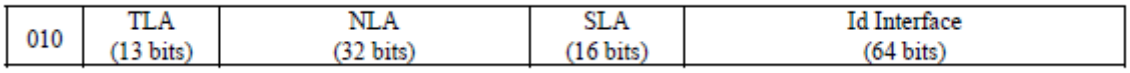

Figure 9: Plan d'adressage agrégé

- Un champ égal à 010(pour indiquer une adresse unicast)
- TLA (top Level Aggregator) : les TLA identifient les grands opérateurs internationaux
- NLA (Next Level Aggregation) : les NLA déterminent les fournisseurs d'accès intermédiaires échangeant leur inter connectivité des éléments d'interconnexion. NLA constitute un identificateur de site (ou domaine).
- SLA (Site Level Aggregator) : offre un moyen de hiérarchiser la stratégie d'adressage de site (définir les sous-réseaux)
- Identificateur interfaces.

III.2.2 Adresses unicast de lien local

Cette adresse est configurée sur une interface unique pour des taches telles que la découverte des voisins ou l'envoi des messages vers une destination précise.

Figure 10: Adresse lien local

III.2.3 Adresses unicast de site local

Ces adresses sont destinées à l'utilisation sur un site unique sans l'utilisation d'un préfixe global. Par exemple, un site non encore connecté à Internet peut utiliser ces adresses, ce qui lui évitera de demander un préfixe de réseau.

C'est en quelque sorte des adresses IP privées. Les routeurs ne doivent pas transmettre des paquets avec ce type d'adresses à l'extérieur du site concerné. de nombreux sous-réseaux peuvent être identifiés au sein d'un site .

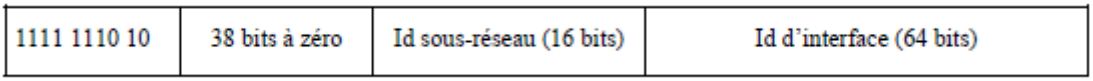

Figure 11: Adresse site local

III.2.4 Adresse anycast

L'adresse anycast est fourni pour permettre le paquet à suivre l'interface la plus près ayant cette adresse d'après la mesure de parcours en fonction de nombre de saut à traverser et taux de latence du protocole de routage utilisé.

Les adresses anycast sont syntaxiquement indistinguables des adresses unicast. Quand une adresse unicast est destinés à plus 'une interface. Elle devient une adresse anycast et le nœud auquel cette adresse est attribuée doit être installé afin d'apprendre qu'il est question d'une adresse anycast. Une utilisation programmée pour les adresses anycast est l'authentification des groupes des routeurs propriété d'une société offrant un accès à le web, ce qui offre la possibilité de banaliser l'accessibilité aux routeurs de cette firme. L'expérience de l'usage considérable des adresses anycast demeure actuellement suffisamment réduit.

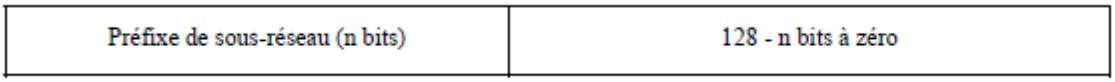

Figure 12: Adresse anycast pour les retours de sous-réseaux

III.2.5 Adresses multicast

Une adresse multicast définit une association de nœuds (interfaces). Un même nœud peut appartenir à multiples groupes multicast.

1111 1111	Flag (4 bits)	Scope (4 bits)	Identificateur de groupe (112 bits)

Figure 13: Adresse multicast

- Flag (drapeau) : contient 0000 pour une adresse permanente (qui est affectée par une autorité compétente de l'IETF) et 0001 pour une adresse temporaire.
- Scope : spécifie quelle partie du réseau l'adresse (adresse unicast ou multicast) est valide. Il définit la "taille" d'une région topologique.

IV. Virtual Routing and Forwarding

Introduction

Une **VRF**, **V**irtual **R**outing and **F**orwarding, est une table contenant un ensemble de sites avec des demandes de connexion similaire. Sa notion demeure similaire que VPN ; elle implique l'isolation du trafic entre sites clients n'appartenant pas aux mêmes VPN. Pour avoir cet isolement, les routeurs PE ont l'avantage de manager de nombreuses tables de routage à la faveur de la notion de VRF.

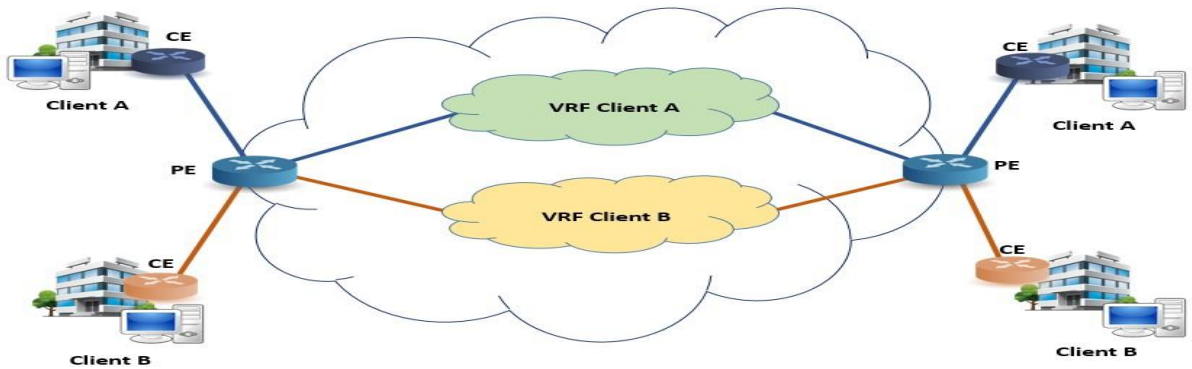

Figure 14: VRF Virtual Routing and Forwarding

La VRF se repose sur trois parties d'une table de routage, d'une **FIB**, **F**orwarding **I**nformation **B**ase, et d'une table CEF particulière et chaque VRF est indépendant de la table de routage globale.

V. Qualité de Service

Introduction

La qualité de service ou Quality of service (QoS) est l'aptitude de entraîner dans de très bonnes engagements un sorte de trafic fourni, en expressions de disponibilité(accès à un service partagé), débit(téléchargement ...),délais de propagation(pour les applications interactives ou la téléphonie, taux de perte de paquets(pertes sans influence pour la voix et la vidéo, mais critiques pour le téléchargement).... La qualité de service est une notion de gestion qui a comme but de conforter les ressources d'un réseau et de garantir de bonnes performances aux applications critiques. Elle permet donc aux FSI de s'engager clairement auprès de leurs consommateurs sur les particularités de transport des informations applicatives (Voix, Data…) sur leurs infrastructures IP.

V.1 Les mécanismes de la qualité de service

On peut distinguer les mécanismes suivants :

- trafic shaping signifie de choisir des mesures pour garantir que la circulation ne dépasse en aucun cas plusieurs valeurs prédéterminées. Quasiment, cette obligation s'exécute en mettant en attente certains paquets pour imposer un certain trafic.
- Le trafic policing est une opération qui consiste à vérifier que le trafic émis est bien conforme à la description qui en a été faite par la source.

Il existe deux modèles de gestion de qualité de services : IntServ et DiffServ :

- IntServ : Le modèle IntServ définit une architecture capable de prendre en charge la QOS sans impacter le protocole IP. Elle offre la possibilité de réserver des ressources obligatoires à les échanges pendant toute la durée du chemin qu'emprunter ont les paquets.

- DiffServ : Ce modèle propose d'abandonner le traitement du trafic ayant l'aspect de flots pour le caractériser sous forme de classes.

V.2 Trafic shaping

Le Trafic shaping est une technique de gestion de réseau qui retarde certains types de paquets dans le but d'optimiser les performances et de garantir la bande passante utilisable. Plus particulièrement, le trafic shaping désigne toute action sur un flux réseau qui impose un délai supplémentaire à ces paquets pour donner une priorité a un autre flux plus critique.

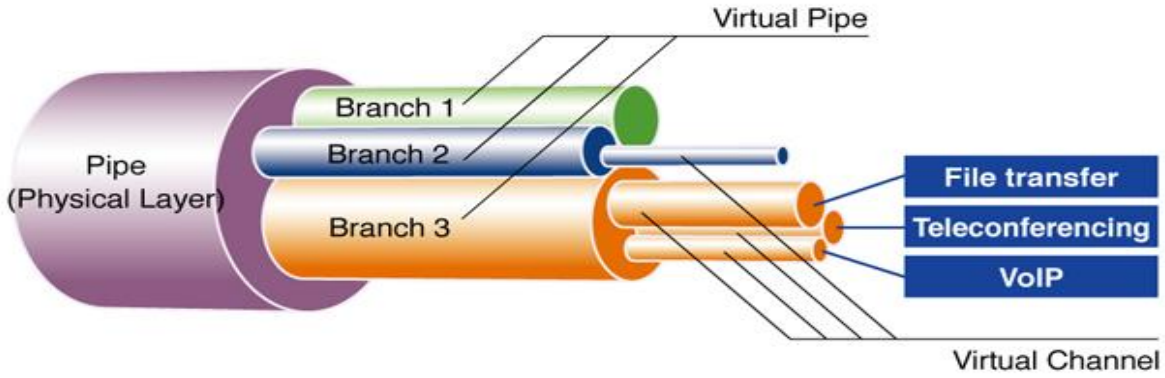

Figure 15 : Concept de trafic shaping

V.3 Per-tunnel QOS

Dans un réseau DMVPN, il est probable que vos routeurs à rayons soient connectés en utilisant une variété de connexions. Vous utilisez peut-être des connexions DSL, câblées ou sans fil sur différents sites. Avec toutes ces différentes connexions, il n'est pas possible d'utiliser une seule stratégie QoS et de l'appliquer à tous les routeurs en étoile. Vous ne souhaitez pas non plus créer de stratégie de QoS unique pour chaque routeur si vous disposez de centaines de routeurs en étoile. La QS de Per-Tunnel nous permet de créer différentes stratégies QoS et nous pouvons les appliquer à différents « groupes » NHRP. Les routeurs à plusieurs rayons peuvent être assignés au même groupe, mais chaque routeur sera **mesuré individuellement**.

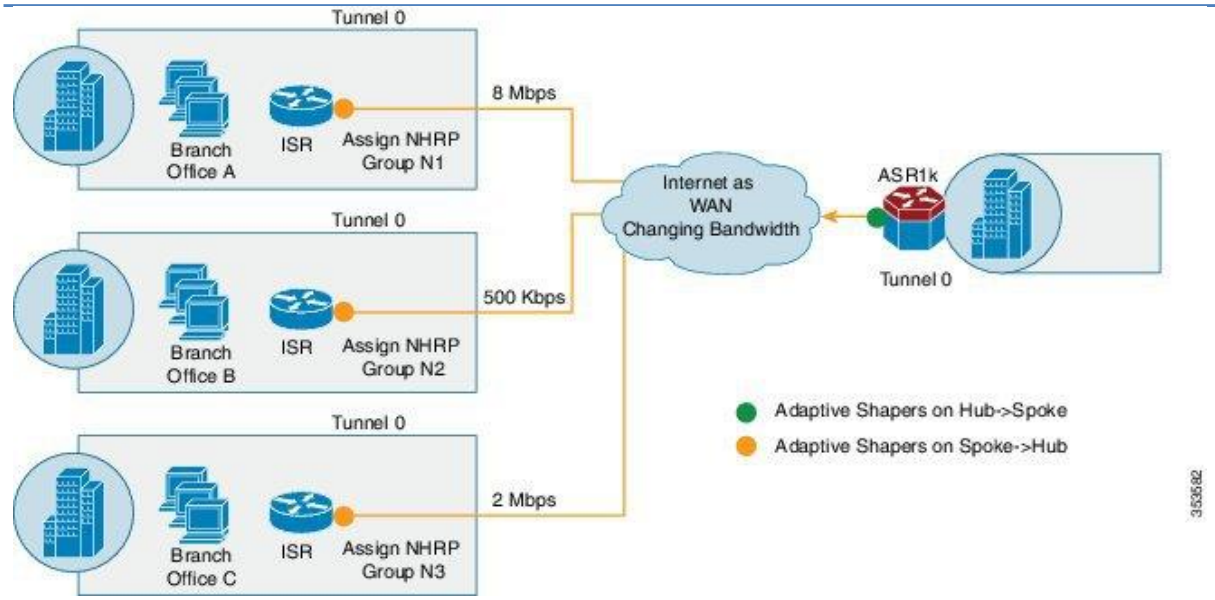

Figure 16:concept de per-tunnel Qos

VI. VPN

Introduction

Les organisations ont historiquement besoin de louer des lignes telles que les lignes T1 or Une ligne louée comme T1 fournit une connexion dédiée offrant beaucoup de bande passante, mais elle ne fournit généralement pas de cryptage ou d'authentification mais simplement que leur travail consiste à fournir une connectivité, et non un cryptage ou une authentification.

La technologie VPN existe pour assurer la sécurité. Le coût peut également jouer un rôle lorsque vous décidez comment relier un deux sites ou plus. Les lignes louées sont très chères. Les entreprises sont souvent obligées de se contenter d'une option moins chère : acheter l'accès Internet localement dans chaque pays, puis utiliser un VPN entre leurs différents sites nationaux ou internationaux pour sécuriser les données. Enfaite Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet.

Les données envoyées au travers VPN sont cryptées, ceci assure aux usagers qu'en cas d'interception malveillante les informations soient illisibles.

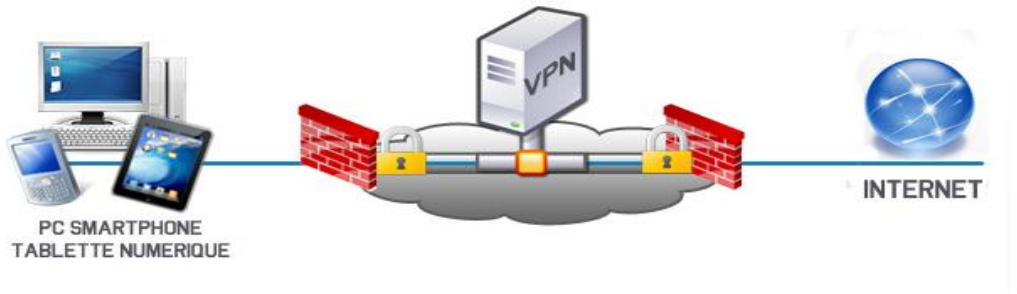

Figure 17: Concept de réseau VPN

VI.1 IPSEC

"IPSEC, définit par la RFC 2401, est un protocole dont l'objectif est de protéger l'échange de données au niveau de la couche réseau. Il constitue l'intérêt de rester en simultané commun aux règles Ipv4 et Ipv6. Il assure la confidentialité l'authentification l'intégrité, la protection contre le rejeu et la gestion des clés.

IPSEC fait appel à deux mécanismes de sécurité pour le trafic IP :

- AH (Authentification Header).
- ESP (Encapsulation Security Payload).

VI.1.1 AH (authentification header)

Il a pour vocation de garantir :

- L'authentification : les datagrammes IP réceptionnés sont identifiés par l'hôte dont l'adresse IP est notifiée comme adresse source dans les entêtes.
- L'unicité (optionnelle) : un datagramme ayant été émis légitimement et enregistré par un attaquant ne peut être réutilisé par ce dernier.
- L'intégrité : les champs suivants du datagramme IP n'ont pas été altérées depuis leur émission.

VI.1.2 ESP (Encapsulating Security Payload)

ESP est le deuxième protocole de protection des données qui permet de garantir :

- La confidentialité: la partie donnée des datagrammes IP transmis est chiffrée.

- L’authentification : les datagrammes IP réceptionnés sont identifiés par l'hôte dont le numéro ipv4 est notifiée comme adresse source dans les entêtes.
- L’unicité.
- L’intégrité : les informations n'ont pas été altérées depuis leur émission.

VI.1.3 Le mode « tunnel »

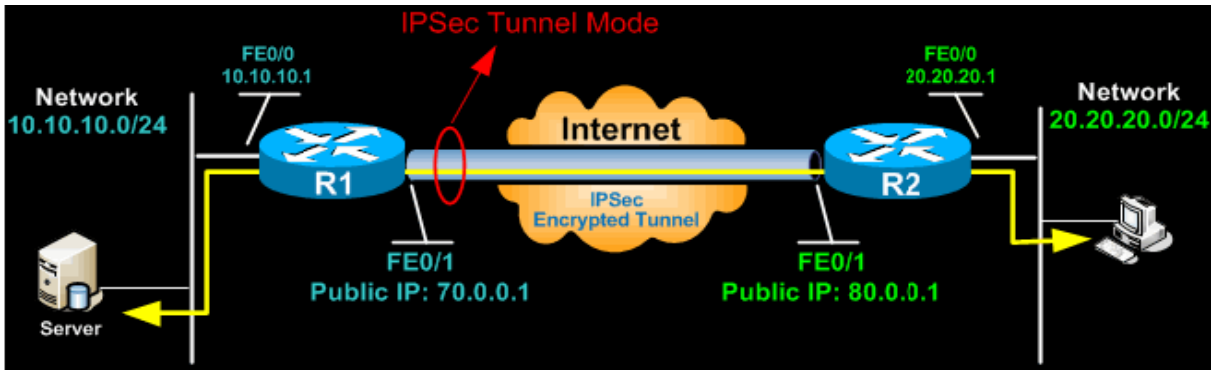

Figure 18:VPN en mode tunnel end-to-end

Le mode tunnel IPSec est le mode par défaut. En mode tunnel, tout le paquet IP d'origine est protégé par IPSec. Cela signifie que IPSec enveloppe le paquet d'origine, le crypte, ajoute un nouvel en-tête IP et l'envoie de l'autre côté du tunnel VPN (homologue IPSec). Le mode tunnel est le plus souvent utilisé entre des passerelles (routeurs Cisco ou pare-feu ASA) ou à une station terminale vers une passerelle, la passerelle agissante en tant que proxy pour les hôtes situés derrière elle.En mode tunnel, un en-tête IPSec (en-tête AH ou ESP) est inséré entre l'en-tête IP et le protocole de couche supérieure. Entre AH et ESP, ESP est le plus souvent utilisé dans la configuration du tunnel VPN IPSec.

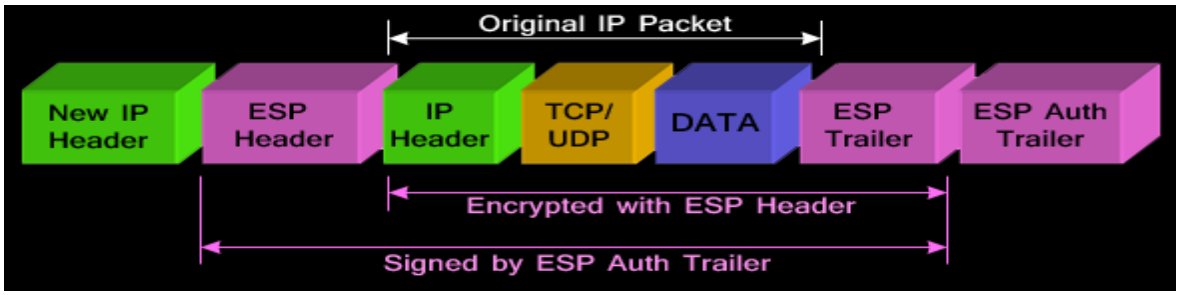

Figure 19: Paquet IPsec protégé en mode Tunnel

VI. VPN MPLS

Au milieu des applications les plus grandes du protocole MPLS est de réussir à concevoir des réseaux privés virtuels (VPN).En sens contraire à un réseau IPSec, les informations circulantes entre les différents sites d'un réseau ne transitent pas via Internet. Passer d'un réseau classique à un réseau MPLS/VPN vous fournit une simplicité de développement, une sécurisation de vos données et de la qualité de service (QoS). Le principe de vpn MPLS consiste à créer des labels la première étiquette (extérieur) identifie le parcours vers le LSR destination, et change à chaque bond, la deuxième (intérieur) spécifie le VPN-ID attribué au VPN et n'est pas altéré entre le LSR source et le LSR destination.

Les composants des VPLS sont :

- le CE routeur (Customer Edge router) : routeur client connecté au backbone IP.
- le PE routeur (Provider Edge router) : routeur backbone de périphérie auquel sont connectés des CE.
- le P (Provider device) : routeur ou commutateur de cœur de backbone.

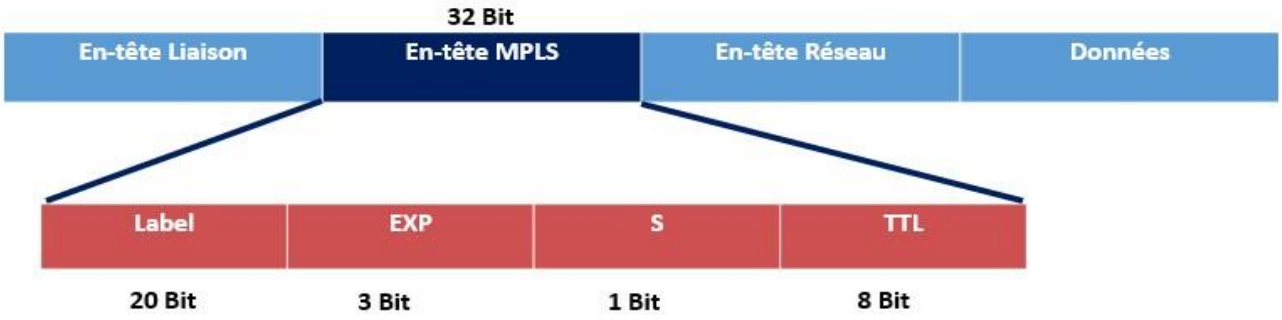

Figure 20: Positionnement du label dans l'entête MPLS

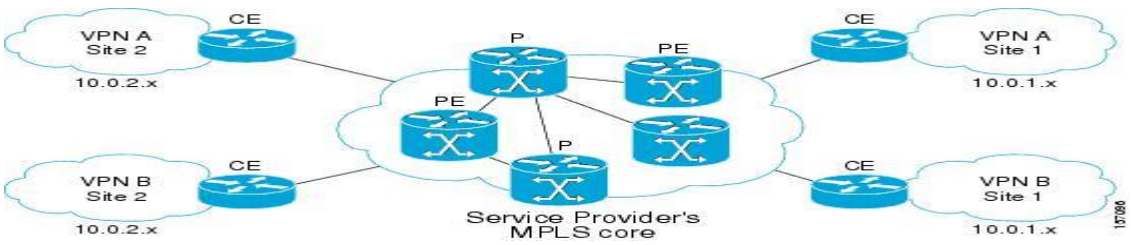

Figure 21: Architecture de réseau MPLS

VII. Backup ADSL

Introduction

Avec l'explosion du nombre d'applications temps réel déployées dans les réseaux, la récupération rapide lors des pannes est de plus en plus désirée pour assurer la continuité des services de communications. Différentes techniques de résistance aux pannes ont été développées pour éviter et réduire le temps de coupure des communications. Ces techniques ont pour rôle de déterminer des chemins de secours capables de recevoir et de router le trafic des communications affectées par une panne.

VII.1 Lien de backup

Avec une demande de la solution de secours par le client lors du panne du la ligne principale MPLS, nous avons proposé d'ajouter une ligne de backup ADSL. Cette solution de secours sert à ajouter un lien internet avec des tunnel DMVPN. ces tunnel secondaires sont activés lors de coupure des tunnel principales.

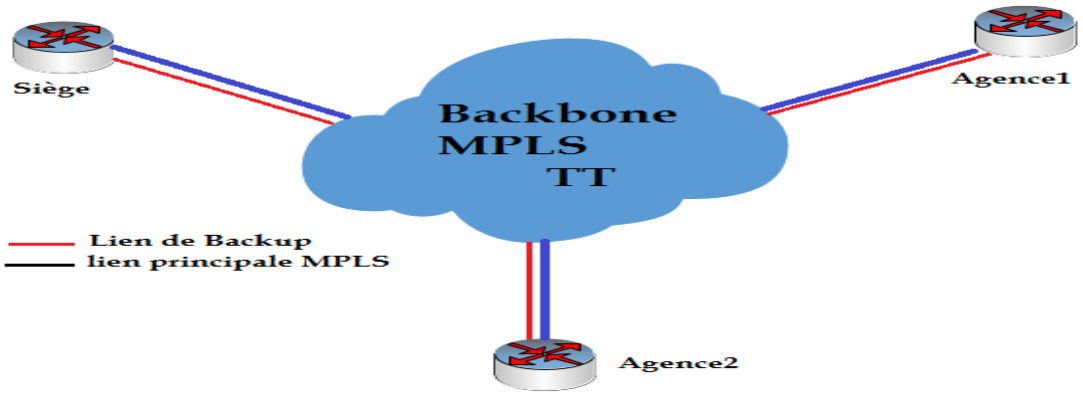

Figure 22: Solution de secours du backbone MPLS

Chapitre 3 : Conception

I. Exigences de conception

Notre solution doit répondre aux exigences suivantes:

- Routage dynamique: la solution doit prendre en charge le routage dynamique sur la nouvelle infrastructure VPN pour assurer un basculement rapide sur les défaillances VPN MPLS / VPN ou Internet.
- Configuration primaire / de sauvegarde flexible: Internet VPN sera utilisé comme chemin de sauvegarde jusqu'à ce qu'il ait été testé de manière approfondie. Il pourrait devenir l'option de connectivité principale à l'avenir.
- Flux de trafic optimal: le trafic vers / depuis les sites accessibles uniquement via Internet VPN (en raison de défaillances MPLS / VPN locales) ne doit pas traverser l'infrastructure MPLS / VPN. Le trafic entre un site MPLS / VPN uniquement et un site Internet VPN uniquement devrait traverser le site central.
- Topologie Hub-and-spoke ou peer-to-peer: Le VPN Internet sera utilisé dans une topologie en étoile (hub = site central). La topologie sera migrée vers un réseau de superposition pair-à-pair (any-to-any) lorsque le VPN Internet deviendra la solution de connectivité WAN principale.
- Modifications minimes de la configuration: le déploiement de la connectivité VPN Internet ne doit pas nécessiter de modifications majeures de la configuration de l'équipement de site distant existant. Les routeurs de site centraux devront probablement être reconfigurés pour tirer parti de la nouvelle infrastructure.
- Interruption minimale: l'introduction de la connectivité VPN Internet ne doit pas perturber la connectivité réseau WAN existante.
- Dépendance minimale sur le fournisseur MPLS / VPN: Une fois l'infrastructure VPN Internet établie et intégrée à l'infrastructure MPLS / VPN existante (qui peut nécessiter des modifications de configuration sur les routeurs CPE gérés par SP), les modifications du flux de trafic ne doivent pas nécessiter de intervention sur les routeurs CPE gérés par SP.

II. Vue d'ensemble de la solution

Internet VPN sera implémenté avec la technologie DMVPN pour répondre aux futures exigences de la topologie peer-to-peer. Chaque routeur de site central sera un routeur concentrateur dans son propre sous-réseau DMVPN (un routeur concentrateur par sous-réseau DMVPN), les routeurs de site distant disposant de deux tunnels DMVPN (un pour chaque routeur concentrateur de site central).

MPLS sera implémenté avec la technologie DMVPN pour répondre aux futures exigences de la topologie peer-to-peer. Chaque routeur de site central sera un routeur concentrateur dans son propre sous-réseau DMVPN (un routeur concentrateur par sous-réseau DMVPN), les routeurs de site distant disposant de deux tunnels DMVPN (un pour chaque routeur concentrateur de site central).

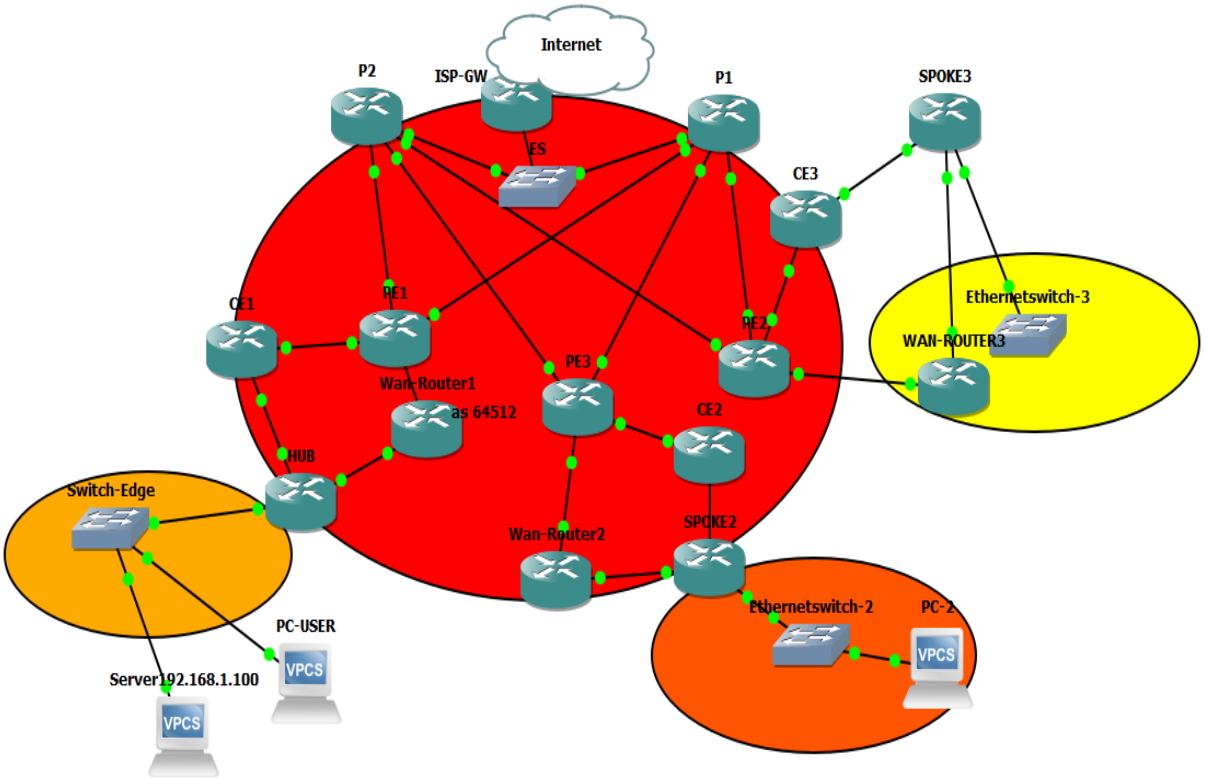

Figure 23 : Concept de l'architecture

Chapitre 4 : Réalisation

Introduction

Après l'analyse de l'état actuel du réseau et l'étude théorique de la technologie MPLS, je propose une nouvelle architecture qui parait adéquate et plus optimisée.Pour bien dégager les avantages de cette nouvelle architecture, je vais la simuler avec gns3 et la tester avec les mêmes paramètres utilisés auparavant.

I Présentation de l'environnement du travail

I.1 Choix des matériels

Les matériels que nous avons exploités sont :

- Routeur Cisco c7200 :

  Les routeurs Cisco de la série 7200 sont les routeurs Cisco mono processeurs les plus rapides ; ils sont parfaitement adaptés aux entreprises et prestataires de services déployant des MPLS, des systèmes groupés à large bande, des dispositifs d'extrémité des réseaux WAN, des VPN de sécurité IP et une intégration vidéo/audio/données. La gamme 7200, de conception modulaire, dispose d'option de connectivité et de fonctions de gestion.

Figure 24: Routeur Cisco c7200

- Commutateurs : il s'agit d'un élément actif agissant au couche liaison de données du modèle OSI. Il examine les trames arrivant sur ses ports d'entrée et filtre les données les orienter seulement sur les ports adéquats. Si bien que le commutateur permet d'allier les caractéristiques du pont en matière de filtrage et du concentrateur en terme de liaison des équipements réseaux.

Figure 25: Commutateur Switch

I.2 Outil d'implémentation GNS3

- **GNS3** : Graphical Network Simulator est un émulateur graphique des réseaux qui nous offre un moyen de émuler des topologies vastes.
  Pour fournir des simulations complètes et précises, GNS3 est fortement lié à :
- Dynamips : est un émulateur IOS Cisco.
- Dynagen : est une extrémité avant à base de texte pour Dynamips.
- Qemu : est un émulateur de machine source et virtualiseur.
- VirtualBox : est un logiciel de virtualisation libre et puissant.
- GNS3 est un excellent outil complémentaire à des véritables laboratoires pour les ingénieurs réseau, les administrateurs…

II Configuration IP-MPLS

II.1 Présentation de la topologie adoptée

Nous avons commancé par l'élaboration de la topologie qui fait la description du le backbone adopté au sein de Tunisie Télécom comme étant un fournisseur de réseau IP-MPLS. Ensuite nous avons configuré les étapes nécessaires afin de garantir un échange fonctionnel entre les routeurs PE et P.

Nous présentons la stratégie d'adressage employé dans ce backbone :

PE1	WANROUTER-S	**172.33.1.0/30**
PE1	CE1	**10.1.1.0/30**
PE1	P1	**172.16.1.0/30**
PE1	P2	**172.16.4.0/30**
PE2	WAN-ROUTER3	**172.33.3.0/30**
PE2	CE3	**10.1.3.0/30**
PE2	P1	**172.16.2.0/30**
PE2	P2	**172.16.6.0/30**
PE3	WAN-ROUTER2	**172.33.2.0/30**
PE3	CE2	**10.1.2.0/30**
PE3	P1	**172.16.3.0/30**
PE3	P2	**172.16.5.0/30**
P1	P2	**172.16.7.0/28**
P1	ISP	**172.16.7.0/28**

Routeur	Loopback
PE1	1.1.1.1/32
PE2	2.2.2.2/32
PE3	3.3.3.3/32
ISP	100.100.100.100/32
CE1	111.111.111.111/32
CE2	222.222.222.222/32
CE3	225.225.225.225/32

III Etapes de configuration

III.1 Configuration du nom du routeur

Nous avons démarré notre travail par l'affectation d'un nom significatif pour l'authentification à chaque routeur. Dans cette figure nous découvrons l'attribution du nom pour le routeur « PE1 ».

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname PE1
PE1(config)#exit
```

Figure 26: Configuration du nom du routeur

III.2 Configuration du protocole OSPF sur PE

Dans le backbone MPLS, afin de garantir les échanges entre les équipements de backbone, nous avons employé le protocole de routage interne OSPF. Il prend en charge les protocoles de la couche réseau tels qu'IPv4 et IPv6. Ce protocole est déclenché avec la commande : « router ospf 1 ». Nous avons reconnu uniquement les réseaux directement connectés au routeur y compris son adresse de Loopback.

```
PE1#sh run | sec ospf
router ospf 1
 network 1.1.1.1 0.0.0.0 area 0
 network 172.16.1.0 0.0.0.3 area 0
 network 172.16.4.0 0.0.0.3 area 0
 network 172.33.1.0 0.0.0.3 area 0
PE1#
```

Figure 27: Configuration du protocole sur PE1

III.2.1 Vérification du protocole OSPF sur PE

Toute configuration nécessite une vérification, pour cela nous avons vérifié le fonctionnement du protocole OSPF avec la commande « show ip route ospf » qui permet d'afficher la table de routage du routeur PE1. Ce protocole est reconnu par la lettre O.

```
PE1#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/3] via 172.16.4.1, 00:23:23, GigabitEthernet3/0
                 [110/3] via 172.16.1.1, 00:24:03, GigabitEthernet1/0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/3] via 172.16.4.1, 00:23:38, GigabitEthernet3/0
                 [110/3] via 172.16.1.1, 00:23:53, GigabitEthernet1/0
      100.0.0.0/32 is subnetted, 1 subnets
O        100.100.100.100 [110/3] via 172.16.4.1, 00:23:23, GigabitEthernet3/0
                         [110/3] via 172.16.1.1, 00:23:23, GigabitEthernet1/0
      172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
O        172.16.2.0/30 [110/2] via 172.16.1.1, 00:24:03, GigabitEthernet1/0
O        172.16.3.0/30 [110/2] via 172.16.1.1, 00:24:03, GigabitEthernet1/0
O        172.16.5.0/30 [110/2] via 172.16.4.1, 00:23:38, GigabitEthernet3/0
O        172.16.6.0/30 [110/2] via 172.16.4.1, 00:23:38, GigabitEthernet3/0
O        172.16.7.0/29 [110/2] via 172.16.4.1, 00:23:33, GigabitEthernet3/0
                       [110/2] via 172.16.1.1, 00:24:03, GigabitEthernet1/0
      172.33.0.0/16 is variably subnetted, 4 subnets, 2 masks
O        172.33.2.0/30 [110/3] via 172.16.4.1, 00:23:38, GigabitEthernet3/0
                       [110/3] via 172.16.1.1, 00:23:53, GigabitEthernet1/0
O        172.33.3.0/30 [110/3] via 172.16.4.1, 00:23:23, GigabitEthernet3/0
                       [110/3] via 172.16.1.1, 00:24:03, GigabitEthernet1/0
      196.238.14.0/30 is subnetted, 1 subnets
O E2     196.238.14.0 [110/20] via 172.33.1.1, 00:23:43, FastEthernet0/0
      196.238.16.0/30 is subnetted, 1 subnets
O E2     196.238.16.0 [110/20] via 172.16.4.1, 00:23:38, GigabitEthernet3/0
```

Figure 28:Vérification du protocole OSPF sur PE1

Cette table nous dévoile tous les réseaux configurés avec OSPF, tel que l'adresse réseau 172.16.0.0 et 172.33.0.0, aussi le cout de ce protocole qui est égale à 110.

III.3 Activation MPLS

Nous avons suivi 3 phases pour garantir une connexion efficace dans le backbone MPLS, pour cela nous avons configuré le protocole IP MPLS. La phase initiale a pour objectif d'assembler une table de routage 'Cisco Express Forwarding' par la commande « ipcef ». Ensuite nous avons activé le protocole MPLS par la commande « mplsip », et la dernière étape permet d'activer le protocole LDP qui sert à affecter des labels aux paquets IP entrants dans le trafic par la commande « mpls label protocol ldp ».

```
PE1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#ip cef
PE1(config)#mpls ip
PE1(config)#mpls label protocol ldp
PE1(config)#exit
```

Figure 29 : Activation MPLS sur PE1

III.4 Activation MPLS sur les interfaces

Afin d'accomplir la configuration du protocole MPLS, il faut le mettre en fonction sur toutes les interfaces d'un routeur qui sont associées au backbone MPLS. Donc il suffit d'ajouter la commande « mplsip » sur tous les liens.

```
PE1#sh run int g1/0
Building configuration...

Current configuration : 127 bytes
!
interface GigabitEthernet1/0
 ip address 172.16.1.2 255.255.255.252
 negotiation auto
 mpls ip
 mpls label protocol ldp
end

PE1#
```

Figure 30: Activation MPLS sur les interfaces

III.5 Activation du protocole BGP sur PE

MP-BGP est un protocole de routage externe qui offre la possibilité de signer la communication entre deux systèmes autonomes sur un réseau partagé par tous les clients. Alors, nous avons activé ce protocole entre les trois routeurs de bordures PE1, PE2 et PE3 avec la commande « router bgp 64512 » en spécifiant le numéro d'AS afin d'assurer la communication entre eux.

La commande « addresse-family-vpnv4 » permet d'activer la mode de configuration pour les spécificités du VPN et la commande « neighbor » employée pour indiquer les adresses des routeurs voisins. Les commandes nécessaires pour la configuration sont mentionnées dans la figure ci-dessous.

```
PE1#sh run | sec bgp
  redistribute bgp 64512 metric 1024 1 255 1 1500
router bgp 64512
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 64512
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 64512
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 100.100.100.100 remote-as 64512
 neighbor 100.100.100.100 update-source Loopback0
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  neighbor 100.100.100.100 activate
  neighbor 100.100.100.100 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf ClientSiege
  redistribute eigrp 1 metric 1
 exit-address-family
```

Figure 31: Activation du protocole BGP sur PE1

III.5.1 Vérification du protocole BGP sur PE

La commande « show ip bgp summary » présente la table de routage de protocole BGP, dont laquelle nous tombons sur les adresses Loopback des routeurs voisins, PE2 et PE3 ainsi le nombre de sessions établis entre eux.

```
PE1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 64512
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4        64512      31      47        1    0    0 00:33:16        0
3.3.3.3         4        64512      30      47        1    0    0 00:33:17        0
100.100.100.100 4        64512      25      47        1    0    0 00:32:54        0
PE1#
```

Figure 32:Vérification du protocole BGP sur PE1

III.5.2 Test de vérification de MPLS et VPN

Après toutes les configurations réalisées dans le backbone IP/MPLS, il nous faut vérifier l'état de marche adéquate de celui-ci, donc nous faisons deux essais principaux :

Le premier est réalisé par la commande « show mplsforwarding-table » qui offre la possibilité de consulter la base TIB des routeurs formés dynamiquement par l'intermédiaire du protocole LDP.

```
PE1#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         16         2.2.2.2/32       0             Gi1/0      172.16.1.1
           18         2.2.2.2/32       0             Gi3/0      172.16.4.1
17         17         172.33.3.0/30    0             Gi1/0      172.16.1.1
           21         172.33.3.0/30    0             Gi3/0      172.16.4.1
18         Pop Label  172.16.7.0/29    0             Gi1/0      172.16.1.1
           Pop Label  172.16.7.0/29    0             Gi3/0      172.16.4.1
19         Pop Label  172.16.6.0/30    0             Gi3/0      172.16.4.1
20         Pop Label  172.16.3.0/30    0             Gi1/0      172.16.1.1
21         Pop Label  172.16.2.0/30    0             Gi1/0      172.16.1.1
22         19         3.3.3.3/32       0             Gi1/0      172.16.1.1
           17         3.3.3.3/32       0             Gi3/0      172.16.4.1
23         Pop Label  172.16.5.0/30    0             Gi3/0      172.16.4.1
24         21         172.33.2.0/30    0             Gi1/0      172.16.1.1
           24         172.33.2.0/30    0             Gi3/0      172.16.4.1
25         25         196.238.16.0/30  0             Gi1/0      172.16.1.1
           27         196.238.16.0/30  0             Gi3/0      172.16.4.1
26         No Label   196.238.14.0/30  195602        Fa0/0      172.33.1.1
27         27         100.100.100.100/32   \
                                       0             Gi1/0      172.16.1.1
           16         100.100.100.100/32   \
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
                                       0             Gi3/0      172.16.4.1
28         28         196.238.17.0/30  0             Gi1/0      172.16.1.1
           26         196.238.17.0/30  0             Gi3/0      172.16.4.1
29         No Label   10.1.1.0/30[V]   76438         aggregate/ClientSiege
34         No Label   192.168.1.0/24[V]    \
                                       0             Gi2/0      10.1.1.2
35         No Label   172.31.1.0/30[V] 56856         Gi2/0      10.1.1.2
PE1#
```

Figure 33:Vérification de la base TIB

La commande « show bgp vpnv4 unicast all » permet d'afficher les tables de routage VRF trouvées sur le routeur PE1, ainsi les liens attaché à chaque VRF.

```
PE1#show bgp vpnv4 unicast all
BGP table version is 38, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf ClientSiege)
 *>i 4.2.2.2/32      100.100.100.100          0    100      0 i
 *>  10.1.1.0/30     0.0.0.0                  0         32768 ?
 *>i 10.1.2.0/30     3.3.3.3                  0    100      0 ?
 *>i 10.1.3.0/30     2.2.2.2                  0    100      0 ?
 *>  172.31.1.0/30   10.1.1.2                 1         32768 ?
 *>i 172.31.2.0/30   3.3.3.3                  1    100      0 ?
 *>i 172.31.3.0/24   2.2.2.2                  1    100      0 ?
 *>  192.168.1.0     10.1.1.2                 1         32768 ?
 *>i 192.168.2.0     3.3.3.3                  1    100      0 ?
 *>i 192.168.3.0     2.2.2.2                  1    100      0 ?
PE1#
```

Figure 34:Vérification de VPN

III.6 La notion du VRF : Virtuel Routing Forwarding

```
ip vrf ClientSiege
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 ip vrf forwarding ClientSiege
```

Figure 35: Création d'un VRF sur PE1

Nous avons associé à chaque interface du routeur, seulement qui sont liées au réseau IP, la table de routage vrf au qu'elle appartienne avec la commande « ip vrf forwarding Client Siege». Voici la configuration de l'interface GigabitEthernet2/0 du routeur Edge PE1.

```
PE1#sh run int g2/0
Building configuration...

Current configuration : 122 bytes
!
interface GigabitEthernet2/0
 ip vrf forwarding ClientSiege
 ip address 10.1.1.1 255.255.255.252
 negotiation auto
end
```

Figure 36: Configuration d'un VRF sur l'interface du PE1

III.7 Configuration du protocole EIGRP sur PE

Le protocole EIGRP (EnhancedInterior Gateway Routing Protocol) est utilisé sur les routeurs pour créer dynamiquement les tables de routage IP. Grace à ce protocole, le routeur connait la topologie du réseau et utilise le chemin le plus adapté pour envoyer des paquets IP vers n'importe quelle destination de ce réseau. Ce qui suit explique comment activer ce protocole sur les routeurs.

```
router eigrp 1
 !
 address-family ipv4 vrf ClientSiege autonomous-system 1
  redistribute bgp 64512 metric 1024 1 255 1 1500
  network 10.0.0.0
 exit-address-family
  redistribute eigrp 1 metric 1
```

Figure 37: Configuration du protocole EIGRP surPE1

III.7.1 Vérification de configuration

Pour tester l'activité du processus VRF, nous avons consulté la table de routage de ce dernier avec la commande « sh ip route vrf A ». La figure ci-dessous présente tous les liens connectés au processus VRF soit par le protocole BGP, soit par le protocole EIGRP.

```
PE1#sh ip route vrf ClientSiege

Routing Table: ClientSiege
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
B        4.2.2.2 [200/0] via 100.100.100.100, 00:56:45
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet2/0
L        10.1.1.1/32 is directly connected, GigabitEthernet2/0
B        10.1.2.0/30 [200/0] via 3.3.3.3, 00:56:45
B        10.1.3.0/30 [200/0] via 2.2.2.2, 00:56:45
      172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
D        172.31.1.0/30 [90/28416] via 10.1.1.2, 00:58:46, GigabitEthernet2/0
B        172.31.2.0/30 [200/1] via 3.3.3.3, 00:56:45
B        172.31.3.0/24 [200/1] via 2.2.2.2, 00:56:45
D EX  192.168.1.0/24 [170/1706752] via 10.1.1.2, 00:58:46, GigabitEthernet2/0
B     192.168.2.0/24 [200/1] via 3.3.3.3, 00:56:45
B     192.168.3.0/24 [200/1] via 2.2.2.2, 00:56:45
```

Figure 38: Verification des routes des sites distants

III.7.2 Redistribution des protocoles

La configuration des protocoles de routage comme BGP et EIGRP se réalise pour œuvrer un bon échange entre les processus VRF. Pour cela nous avons injecté le protocole BGP dans EIGRP et vice et versa afin d'assurer la redistribution des nouvelles routes entre les CPE. La commande « redistribute » permet de garantir cette redistribution des liens.

```
  redistribute bgp 64512 metric 1024 1 255 1 1500
router bgp 64512
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 64512
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 64512
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 100.100.100.100 remote-as 64512
 neighbor 100.100.100.100 update-source Loopback0
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  neighbor 100.100.100.100 activate
  neighbor 100.100.100.100 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf ClientSiege
  redistribute eigrp 1 metric 1
 exit-address-family
```

Figure 39: Redistribution des protocoles

III.8 Mise en place de la solution de secours

Dans notre projet, nous avons configuré une solution de secours (lien de backup) avec un basculement automatique lors de la panne du la ligne principale MPLS.

```
HUB#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

D     192.168.2.0/24 [90/25605120] via 10.30.30.2, 00:02:10, Tunnel2
D     192.168.3.0/24 [90/25605120] via 10.30.30.3, 00:02:00, Tunnel2
      196.238.16.0/30 is subnetted, 1 subnets
D EX     196.238.16.0
           [170/1709056] via 196.238.14.2, 00:06:46, FastEthernet4/0
      196.238.17.0/30 is subnetted, 1 subnets
D EX     196.238.17.0
           [170/1709056] via 196.238.14.2, 00:06:45, FastEthernet4/0
```

Figure 40 : Basculement

```
PE1#sh ip route ospf | sec 172.33.0.0
     172.33.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.33.2.0/30 [110/3] via 172.16.4.1, 00:15:32, GigabitEthernet3/0
                      [110/3] via 172.16.1.1, 00:15:37, GigabitEthernet1/0
O       172.33.3.0/30 [110/3] via 172.16.4.1, 00:15:32, GigabitEthernet3/0
                      [110/3] via 172.16.1.1, 00:15:47, GigabitEthernet1/0

PE1#
```

Figure 41 : Réseau de backup

```
HUB#sh ip int  brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.31.1.2      YES NVRAM  administratively down down
GigabitEthernet1/0     unassigned      YES NVRAM  administratively down down
GigabitEthernet2/0     unassigned      YES NVRAM  administratively down down
FastEthernet3/0        192.168.1.1     YES NVRAM  up                    up
FastEthernet4/0        196.238.14.1    YES NVRAM  up                    up
Tunnel1                10.20.20.1      YES NVRAM  up                    down
Tunnel2                10.30.30.1      YES NVRAM  up                    up
HUB#
```

Figure 42 : Basulement vers le backup

III.9 Intégration de l'IPv6

L'IPv6 est la solution qui s'impose pour corriger certains défauts trouvés dans l'IPv4 afin d'améliorer les performances et anticiper les futures fonctionnalités du réseau.

La mise en place d'IPv6 implique la mise en œuvre de processus d'interopérabilité avec la technologie IPv4 configurée au sein du notre backbone MPLS.

```
HUB#sh run | sec ipv6
ipv6 unicast-routing
ipv6 cef
 ipv6 address 2001:1234::2/64
 ipv6 enable
 ipv6 eigrp 1
 ipv6 address 2001:1111::1/64
 ipv6 enable
ipv6 router eigrp 1
 eigrp router-id 225.225.225.225
```

Figure 43: Activation et configuration de l'IPv6

Comme indique la figure ci-dessus la commande « ipv6 unicast-routing » permet d'activer la transmission d'IPv6 datagrammes unicast.

```
HUB#sh run int f3/0
Building configuration...

Current configuration : 211 bytes
!
interface FastEthernet3/0
 description ***GW-Siege***
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex full
 ipv6 address 2001:1111::1/64
 ipv6 enable
 service-policy input Traffic-VERS-SITES
end
```

Figure 44: Activation et configuration de l'IPv6

```
HUB#sh ipv6 route
IPv6 Routing Table - default - 14 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
EX  ::/0 [170/1709056]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
C   2001:1111::/64 [0/0]
     via FastEthernet3/0, directly connected
L   2001:1111::1/128 [0/0]
     via FastEthernet3/0, receive
C   2001:1234::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:1234::2/128 [0/0]
     via FastEthernet0/0, receive
D   2001:1235::/64 [90/26885120]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
D   2001:1236::/64 [90/26885120]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
EX  2001:2222::/64 [170/26882560]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
EX  2001:3333::/64 [170/26882560]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
EX  2002:1234::/48 [170/26882560]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
D   2002:1234::/64 [90/26882560]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
EX  2002:1235::/48 [170/26882560]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
D   2002:1235::/64 [90/26882560]
     via FE80::C805:32FF:FE0C:0, FastEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Figure 45 : Vérification des routes

```
CE1#sh run int tun 1
Building configuration...

Current configuration : 180 bytes
!
interface Tunnel1
 no ip address
 ipv6 address 2002:1235::1/64
 ipv6 enable
 ipv6 eigrp 1
 tunnel source GigabitEthernet2/0
 tunnel mode ipv6ip
 tunnel destination 10.1.3.2
end
```

Figure 46 : Création d'un Tunnel

```
CE1#ping ipv6
CE1#ping ipv6 2001:3333::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:3333::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/96/164 ms
```

Figure 47 : Test de connectivité

III.10 Qualité de service

Cette étape consiste a marquer le trafic selon des access-lists .

```
Extended IP access list voice
    10 permit ip host 192.168.1.11 any
    20 permit ip host 192.168.1.12 any
    30 permit ip host 192.168.1.13 any
    40 permit ip host 192.168.1.14 any
    50 permit ip host 192.168.1.15 any
    60 permit ip host 192.168.1.16 any
    70 permit ip host 192.160.1.17 any
    80 permit ip host 192.168.1.18 any
    90 permit ip host 192.168.1.19 any
    100 permit ip host 192.168.1.20 any
```

Figure 48: Access-List Voice

```
 match dscp af43
class-map match-all voip-in
 match access-group name voice
```

Figure 49 : Comparaison de Traffic

```
policy-map Traffic-VERS-SITES
 class voip-in
  set dscp af43
 class Servers-In
  set dscp af41
 class Users-in
  set dscp af32
```

Figure 50 : Marquage de Traffic

```
interface FastEthernet3/0
 description ***GW-Siege***
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex full
 ipv6 address 2001:1111::1/64
 ipv6 enable
 service-policy input Traffic-VERS-SITES
end
```

Figure 51: Activation de la politique au Traffic entrant

Chaque traficsortant sera traité suivant le marquage grâce au politique à la sortie .

```
class-map match-any voip
  description ***Traffic Voix***
 match protocol h323
 match dscp af43
```

Figure 52: Comparaison de marquage

Chaque trafic filtré sera attribué a la bande passant définit

```
policy-map TRAFFIC
  class voip
    bandwidth percent 20
  class SERVERS
    bandwidth percent 40
  class users
    bandwidth percent 30
policy-map COM
  class class-default
    shape average 100000000
     service-policy TRAFFIC
policy-map Traffic-in
policy-map Agence1
  class class-default
    shape average 10000000
     service-policy TRAFFIC
policy-map Agence2
  class class-default
    shape average 5000000
     service-policy TRAFFIC
```

Figure 53 : Nested policy maps

On va maintenant tester notre politique en pingeant a partir le vlan serveur vers l agence 2

```
VPCS> ip 192.168.1.100 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.100 255.255.255.0 gateway 192.168.1.1

VPCS> ping 192.168.2.1 -c 1000
84 bytes from 192.168.2.1 icmp_seq=1 ttl=254 time=259.189 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=254 time=86.737 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=254 time=66.176 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=254 time=119.820 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=254 time=92.747 ms
84 bytes from 192.168.2.1 icmp_seq=6 ttl=254 time=145.888 ms
84 bytes from 192.168.2.1 icmp_seq=7 ttl=254 time=99.264 ms
84 bytes from 192.168.2.1 icmp_seq=8 ttl=254 time=78.208 ms
```

Figure 54: Ping de réseau agence a partir le vlan serveur

```
UB#sh policy-map interface
FastEthernet3/0

 Service-policy input: Traffic-VERS-SITES

   Class-map: voip-in (match-all)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: access-group name voice
     QoS Set
       dscp af43
         Packets marked 0

   Class-map: Servers-In (match-all)
     39 packets, 3822 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: access-group name servers
     QoS Set
       dscp af41
         Packets marked 43

   Class-map: Users-in (match-all)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: access-group name users
     QoS Set
       dscp af32
         Packets marked 0

   Class-map: class-default (match-any)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: any
UB#
```

Figure 55: Marquage de traffic au niveau de segument serveurs

III.11 DMVPN

III.11.1 CONFIGURATION DU HUB

```
interface Tunnel1
 ip address 10.20.20.1 255.255.255.0
 no ip redirects
 ip mtu 1416
 no ip next-hop-self eigrp 10
 no ip split-horizon eigrp 10
 ip nhrp map multicast dynamic
 ip nhrp map group Agence2 service-policy output Agence1
 ip nhrp map group Agence3 service-policy output Agence2
 ip nhrp network-id 1
 ip nhrp holdtime 3600
 delay 10
 tunnel source 172.31.1.2
 tunnel mode gre multipoint
 tunnel protection ipsec profile dmvpn
end
```

Figure 56 : Interface tunnel1 en hub

III.11.2 CONFIGURATION DU SPOKE

```
interface Tunnel1
 ip address 10.20.20.2 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp group Agence2
 ip nhrp map 10.20.20.1 172.31.1.2
 ip nhrp map multicast 172.31.1.2
 ip nhrp network-id 1
 ip nhrp nhs 10.20.20.1
 delay 2
 tunnel source 172.31.2.2
 tunnel mode gre multipoint
 tunnel protection ipsec profile dmvpn
end
```

Figure 57 : Interface tunnel1 en spoke2

Nous mappons de façon manuelle en NHRP l'adresse publique de serveur NHS pour réalisation du tunnel perpétuel entre le spoke et le hub.

```
interface Tunnel1
 ip address 10.20.20.2 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp group Agence2
 ip nhrp map 10.20.20.1 172.31.1.2
 ip nhrp map multicast 172.31.1.2
 ip nhrp network-id 1
 ip nhrp nhs 10.20.20.1
 delay 2
 tunnel source 172.31.2.2
 tunnel mode gre multipoint
 tunnel protection ipsec profile dmvpn
end
```

Figure 58 : Mappage de serveur NHRP

Nous identifions le serveur NHRP qui sera le hub R1

```
interface Tunnel1
 ip address 10.20.20.2 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp group Agence2
 ip nhrp map 10.20.20.1 172.31.1.2
 ip nhrp map multicast 172.31.1.2
 ip nhrp network-id 1
 ip nhrp nhs 10.20.20.1
 delay 2
 tunnel source 172.31.2.2
 tunnel mode gre multipoint
 tunnel protection ipsec profile dmvpn
```

Figure 59:Définition de résolveur NHRP

Nous désactivons le mécanisme Split-Horizon puis on demande à EIGRP de ne pas réécrire l'adresse de Next-hop avec celle du routeur qui annonce afin d'établir un lien dynamique directe l'aide d'NHRP.

```
interface Tunnel1
ip address 10.20.20.1 255.255.255.0
no ip redirects
ip mtu 1416
no ip next-hop-self eigrp 10
no ip split-horizon eigrp 10
ip nhrp map multicast dynamic
ip nhrp map group Agence2 service-policy output Agence1
ip nhrp map group Agence3 service-policy output Agence2
ip nhrp network-id 1
ip nhrp holdtime 3600
delay 10
tunnel source 172.31.1.2
tunnel mode gre multipoint
tunnel protection ipsec profile dmvpn
```

Figure 60: Adaptation de protocole EIGRP au exigence de DMVPN

```
router eigrp 10
 network 10.20.20.0 0.0.0.255
 network 192.168.1.0
 distance eigrp 10 100
```

Figure 61: Activation et partage eigrp dans le tunnel.

III.12 IPSEC

On va maintenant appliquer un mécanisme de sécurité (IPSEC) pour sécuriser notre tunnel DMVPN.

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
```

Figure 62: Création de la policy ISAKMP

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key Pfe*2018 address 0.0.0.0
crypto isakmp keepalive 10 periodic
!
```

Figure 63: Configuration de la clé ISAKMP

Figure 64: Configuration du transform set IPsec

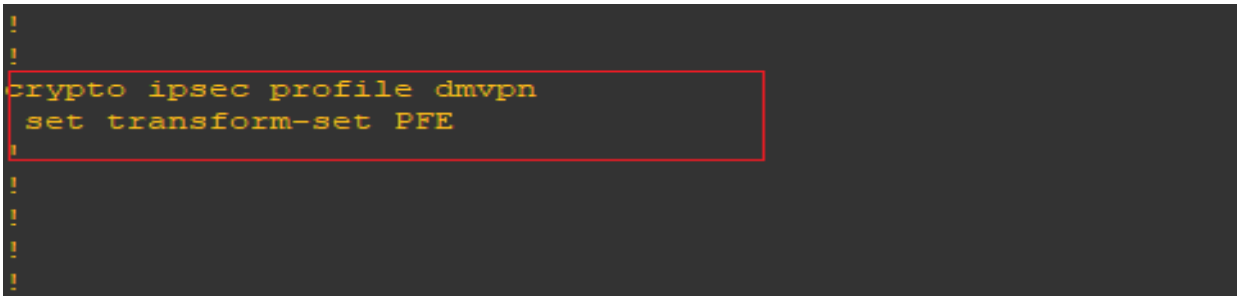

Figure 65: Configuration du profile IPSEC

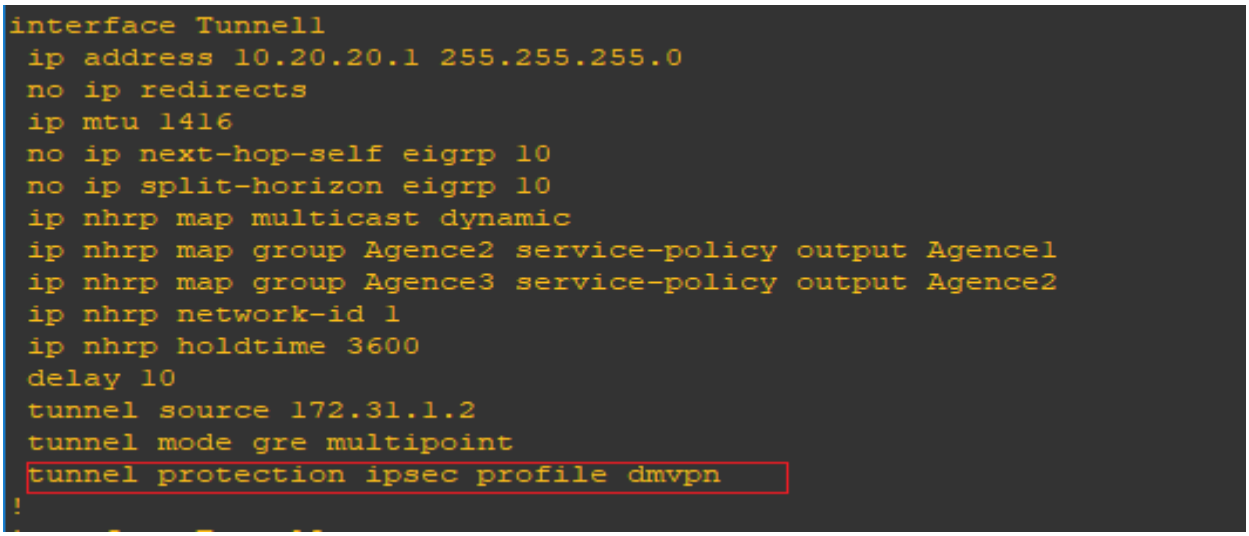

Figure 66: Affectation du profile dans le tunnel.

Vérifions la configuration de notre IPSEC :

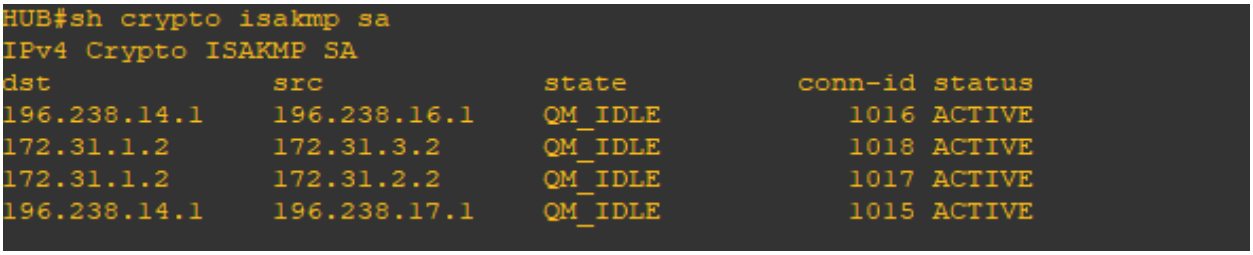

Figure 67 : IPSec activé

Le tunnel permanent NHRP est établi entre le routeur de siège et le routeur d'agence 2.

```
SPOKE2#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 172.31.1.2            10.20.20.1    UP 00:02:15     S
```

Figure 68 : Dmvpn fonctionnel

CONCLUSION GENERALE

Certaines mesures, dans le domaine des réseaux informatiques des entreprises, tels que la congestion et les délais participent à affaiblir ses performances. L'établissement de la qualité de service dans le réseau MPLS des entreprises, précisément les consommatrices des applications Triple Play (voix, données et vidéo..), devient une nécessite à y appliquer afin d'en contribuer. Dans ce cadre, s'intègre notre projet de fin de formation ayant pour objectif l'optimisation d'une infrastructure IP-MPLS d'un opérateur et l'intégration de l'IPv6.

Durant ces quatre mois du stage de projet fin de formation, déroulé au sein de NextStep-IT, nous avons bien configuré premièrement un réseau IP-MPLS avec un plan d'adressage spécifique et des protocoles de routage déterminés. En addition, nous paramétré une solution de secours en cas de panne de ce réseau. Et finalement, nous avons intégré l'IPv6 pour parer à l'épuisement des adresses IPv4, actuellement utilisées à travers le monde, qui s'accélère en raison de la croissance mondiale d'Internet. La nouveauté majeure de l'IPv6 est l'utilisation d'adresses plus longues qu'avec l'IPv4. Avec l'IPv6 on passe d'environ 4,2 milliards d'adresses à 340 sextillions (340*1034) d'adresses, ce qui permettra d'interconnecter tous les équipements possibles sur Internet, donnant de nouveaux cas d'application.

Ce travail a nécessité une large connaissance dans le monde des réseaux, plus particulièrement le réseau MPLS, la qualité de service, l'intégration de l'IPv6 et encore une maitrise des notions de routage avec des nouveaux protocoles tels que l'OSPF, BGP et EIGRP.

Néographie

https://fr.slideshare.net/aymenbouzid/mpls-49163305 ,Aymen Bouzid,09/06/2015

https://fr.scribd.com/document/237902029/Optimisation-Backbone-IP-MPLS , Nizar Saâda,05/02/2014

https://www.arcep.fr/uploads/tx_gspublication/Cahiers_11_ARCEP-nov2014.pdf , Ingrid Appenzeller, Jean-François Hernandez,11/10/2014

http://abcdrfc.free.fr/rfc-vf/pdf/rfc3513.pdf , Groupe de travail Réseau,04/2013

http://docplayer.fr/5335799-Introduction-a-ipv6-i-introduction-ii-classes-d-adresses-ipv4.html Marc Hébert,2016

https://fr.scribd.com/document/75440745/partie1-adahy ,Adahy Arthur GhislainKouakou

https://fr.scribd.com/document/254700705/Chap8IPv6-pdf, Fouad Boutat

http://docplayer.fr/5335799-Introduction-a-ipv6-i-introduction-ii-classes-d-adresses-ipv4.html Marc Hébert,2016

https://fr.scribd.com/document/253700692/Rapport-Reseau-2-v2 , Mahdi Alain Allani

http://abdelhamid-djeffal.net/web_documents/ipv6.pdf ,Dr A. DJEFFAL,2015/2016

https://www.memoireonline.com/03/11/4293/m_Mise-en-oeuvre-dun-coeur-de-reseau-IPMPLS13.html , Amine Amine,2011

http://pf-mh.uvt.rnu.tn/805/1/solution-communication-tunisie-telecom.pdf Anouar JELASSI

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.4208&rep=rep1&type=pdf , Mohamed Aymen Chalouf,13/12/2009

https://www.memoireonline.com/10/12/6146/m_Etude-des-protocoles-de-securite-dans-le-reseau-internet35.html ,NZALANKUMBU DIALEMBA,2007

service-dans-inter-reseau-via-le-protocole-BGP-Cas-d3.html

https://networklessons.com/cisco/ccie-routing-switching/dmvpn-per-tunnel-qos/

https://www.cisco.com/c/fr_ca/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.pdf

http://www.networklife.net/2014/10/introduction-au-dmvpn/

http://packetlife.net/blog/2008/jul/23/dynamic-multipoint-vpn-dmvpn/

http://blog.ipspace.net/2013/09/combining-dmvpn-with-existing-mplsvpn.html

https://gloriuscity.files.wordpress.com/2014/05/expose-dmvpn.pdf