REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

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

Mémoire de Master

Présenté par

BOUTICHE Imene

ZAIDI Lilia Amira

Filière : Télécommunications

Spécialité : Réseaux et télécommunications

Implémentation de la ToIP sur une architecture MPLS/VPN

Soutenu le 13 /07 /2023 devant le jury composé de :

HAROUNE	Radia	MAA	UMBB	Président
SEDJELMACI	Ibticeme	MAA	UMBB	Examinateur
MECHID	Samira	MAA	UMBB	Rapporteur

Année Universitaire : 2022/2023

Dédicaces

Je rends grâce à Dieu de m'avoir donné le courage et la volonté. Ainsi que la conscience d'avoir pu terminer mes études.

Je dédie ce modeste travail :

À mes très chères : À celui qui m'a toujours appris comment réfléchir avant d'agir, à celui qui m'a soutenu tout au long de ma vie scolaire, à celui qui n'a jamais épargné un effort pour mon bien, mon cher père.

À celle qui est toujours à côté de mon cœur, à celle qui m'apprit le vrai Sens de la vie, à celle qui n'a hésité aucun moment à m'encouragé, ma chère mère.

A ma 2éme mère, qui me donne toujours l'espoir de vivre et qui n'a jamais cessé de prier pour moi.

À ma sœur : KHADIDJA
À mon frère : AMAR
À tous mes amis les plus sincères.

À ma chère binôme : LILIA AMIRA
À tous les enseignants et étudiants de département génie électrique.
A tous mes collègues de
Promo RT 2023
Et bien sûr a toute la famille "BOUTICHE" et à tous ceux
Que me connaît

Imene

Dédicaces

Je rends grâce à Allah, le Miséricordieux, qui m'a accordé la force et la persévérance nécessaires pour accomplir ce travail et terminer mes études.

À chaque fois qu'on achève une étape importante dans notre vie, on fait une pause pour regarder en arrière et se rappeler toutes ces personnes qui ont partagé avec nous tous les bons moments de notre existence, mais surtout les mauvais. Ces personnes qui nous ont aidés sans le leur dire, soutenus sans réserve, aimés sans compter, ces personnes à qui notre bonheur devient directement le leur, à qui un malheur en nous, en eux se transforme en pleurs.

Je dédie ce modeste travail à :

***Mes très chers parents**, source de vie, d'amour et d'affection, qui ont toujours été les étoiles de mon ciel et ont illuminé mon chemin depuis ma naissance, je ne les remercierai jamais assez que Dieu me les garde.*

*Ma grand-mère, mes chers frères, **Ahmed**, **Riadh** et **Samy***

*Mes cousins et toute la famille **"ZAIDI"** et la famille **"DJELLOULI".***

*Ma chère binôme **Imene**, pour m'avoir supportée au long de cette année et avoir tout donné pour que nous achevons ce travail.*

Mes chères amies.

Toute ma promotion 2023 de la spécialité Réseaux et Télécommunications sans exception.

Toutes les personnes que j'ai aimées, j'aime et j'aimerai toujours, et à tous ceux qui m'aiment...

Lilia Amira

Remerciements

Louange à Allah le miséricordieux de nous avoir donné le courage, la force et la volonté pour la réalisation de ce mémoire.

Nous remercions chaleureusement et spécialement notre promotrice, Mme S. MECHID, qui a accepté de nous encadrer pour la réalisation de ce modeste travail et qui nous a orientés dans notre travail. Nous exprimons nos profonds remerciements pour son aide, ses conseils et sa compréhension.

Nous remercions également les membres du jury qui nous ont fait l'honneur de nous recevoir, de nous écouter et d'apprécier notre présent mémoire.

Un grand merci pour M^lle^ A.TAFAT qui a accepté de nous aider dans notre projet.

Nous ne saurons oublier le grand mérite des enseignants qui ont contribué à notre cursus, particulièrement ceux du département "Ingénierie des Systèmes Electriques" et qu'ils trouvent ici le témoignage de notre profonde reconnaissance.

Enfin, que toute personne qui, d'une façon ou d'une autre, a contribué à la réalisation de cette étude trouve ici le témoignage de nos plus vives gratitudes.

Résumé :

La téléphonie sur IP (ToIP) est une technologie qui s'impose progressivement dans tous les secteurs, elle consiste à faire transiter les communications téléphoniques par le réseau IP.

Aujourd'hui, cette technologie est de plus en plus déployée dans les universités et les laboratoires de recherche, grâce à ses avantages tels que la réduction des coûts en utilisant internet pour transmettre des appels vocaux et vidéo, faciliter la gestion des appels téléphoniques etc.…

L'objectif de ce travail est d'optimiser les communications et de faciliter la gestion des appels téléphoniques au sein d'une entreprise en offrant une haute qualité de service tout en garantissant la sécurité des données. En effet, l'utilisation d'un réseau MPLS VPN permet de garantir une bande passante suffisante pour les communications vocales et de prioriser le trafic en temps réel. De plus, l'architecture MPLS VPN offre une sécurité accrue grâce à la segmentation du réseau et à l'utilisation de tunnels VPN pour protéger les données circulant sur le réseau.

L'utilisation d'une architecture MPLS VPN pour la mise en place du ToIP offre une solution sécurisée, fiable et évolutive pour répondre aux besoins des entreprises en termes de communications vocales sur IP.

Mots clés : IP, ToIP, Architecture MPLS VPN, tunnels VPN.

Abstract:

IP telephony (ToIP) is a technology that is gradually becoming more prevalent in all sectors, involving the transmission of telephone communications through the IP network.

Today, this technology is increasingly being deployed in universities and research laboratories, thanks to its advantages such as cost reduction by using the internet to transmit voice and video calls, facilitating the management of telephone calls, etc.

The objective of this work is to optimize communications and facilitate the management of telephone calls within a company by offering high-quality service while ensuring data security. Indeed, the use of an MPLS VPN network guarantees sufficient bandwidth for voice communications and prioritizes real-time traffic.

The MPLS VPN architecture offers increased security through network segmentation and the use of VPN tunnels to protect data circulating on the network. In summary, using an MPLS VPN architecture for implementing ToIP offers a secure, reliable, and scalable solution to meet companies' needs for IP voice communications.

Keywords: IP, ToIP, MPLS VPN architecture, VPN tunnels.

ملخص :

الهاتف عبر بروتوكول الانترنت (ToIP) هي تقنية تنتشر تدريجيا في جميع القطاعات، وتتضمن نقل الاتصالات الهاتفية عبر شبكة (IP). واليوم، يتم نشر هذه التقنية بشكل متزايد في الجامعات والمخابر البحثية، بفضل مزاياها مثل تخفيض التكاليف باستخدام الانترنت لنقل المكالمات الهاتفية، إلخ.

والهدف من هذا العمل هو تحسين الاتصالات وتسهيل إدارة المكالمات الهاتفية داخل الشركة عن طريق تقديم خدمة عالية الجودة مع ضمان أمن البيانات. في الواقع، يضمن استخدام شبكة (MPLS/VPN) ضمان نطاق ترددي كاف للاتصالات الصوتية وإعطاء الأولوية لحركة المرور في الوقت الفعلي. بالإضافة الى ذلك، توفر بنية (MPLS/VPN) مزيدا من الأمان من خلال تجزئة الشبكة واستخدام أنفاق (VPN) لحماية البيانات التي تنتقل عبر الشبكة.

يوفر استخدام بنية (MPLS/VPN) لتمرير (ToIP) حلا امنا وموثوقا وقابلا للتطور لتلبية حاجات الشركات في مجال الاتصالات الصوتية عبر (IP).

الكلمات المفتاحية : أنفاق VPN، بنية MPLS VPN، ToIP، IP.

Chapitre I : Généralités sur le routage

Chapitre II : "ToIP" La Téléphonie sur IP

Chapitre III : "MPLS" Multi Protocol Label Switching

Chapitre IV : Simulation sous GNS3

Chapitre II : "ToIP" La Téléphonie sur IP

Chapitre IV : Simulation sous GNS3

A

AS : Autonomous System

ATM : Asynchronous Transfer Mode

B

BGP : Border Gateway Network

BS : Bit Stack

C

CE : Customer Edge

CoS : Class of Service

CME : Call Manager Express

CR-LDP : Constraint based Routing Over Label Distribution Protocol

CSC : Common Signaling Channel

D

DHCP : Dynamic Host Configuration Protocol

E

eBGP : exterior Border Gateway Network

EGP : Exterior Gateway Protocol

EIGRP : Extended Interior Gateway Routing Protocol

F

FAI : Fournisseur d'accès à Internet

FEC : Forwarding Equivalence Class

FIB : Forwarding Information Base

FR : Frame Relay

G

GRE : Generic Routing Encapsulation

H

HDLC : High-Level Data Link Control

I

iBGP : Interior Border Gateway Network

IETF: Internet Engineering Task Force

IGP: Interior Gateway protocol

IGRP: Interior Gateway Routing Protocol

IP : Internet Protocol

IS-IS : Système Intermédiaire à système Intermédiaire

L

LAN : Local Area Network

LDP : Label Distribution Protocol

LER : Label Edge Router

LFIB : Label Forwarding Information Base

LIB : Label Information Base

LSP : Label Switch Path

LSR : Label Switching Router

L2VPN : Layer 2 Virtual Private Network

L3VPN : Layer 3 Virtual Private Network

M

MAC : Media Access Control

MGCP : Media Gateway Control Protocol

MPLS : Multi-Protocol Label Switching

MPLS-TE : Multi-Protocol Label Switching- Traffic-Engineering

MP-BGP : Multi-Protocol-Border Gateway Protocol

MP-eBGP : Multi-Protocol-external Border Gateway Protocol

MP-iBGP : Multi-Protocol-internal Border Gateway Protocol

O

OSI : Open Systems Interconnection

OSPF : Open Shortest Path First

OSPF-TE : Open Shortest Path First-Traffic Engineering

P

P : Provider router

PE : Provider Edge router

PSTN : Public switched Telephone Network

Q

QoS : Quality of Service

R

RD : Route Distinguisher

RIP : Routing Information Protocol

RIPv1 : Routing Information Protocol Version 1

RIPv2 : Routing Information Protocol Version 2

RSVP : ReSerVation Protocol

RSVP-TE : ReSerVation Protocol-Traffic Engineering

RT : Route Target

RTC : Réseau téléphonique commuté

RTCP : Real Time Transport Control Protocol

RTP : Real Time Transport Protocol

S

SIP : Session Initiation Protocol

SLA : Service Level Agreement

T

TCP : Transmission Control Protocol

TDP : Tag Distribution Protocol

TE : Traffic-Engineering

ToIP : Telephony over Internet Protocol

TTL : Time To Live

U

UA : User Agent

UA : User Agent Client

UDP : User Datagram Protocol

URI : Uniform Resource Identifier

V

VCI : Virtual Channel Identifier

VoIP : Voice over Internet Protocol

VPI : Virtual Path Identifier

VPLS : Virtual Private LAN Services

VPN : Virtual Private Network

VPWS : Virtual Private Wire Service

VRF : Virtual Routing and Forwarding

W

WAN : Wide Area Network

Introduction Générale

Introduction générale

L'évolution du domaine des télécommunications a connu une transformation importante avec l'avènement de la technologie ToIP (Téléphonie sur IP). Cette technologie a permis de transmettre des données, de la voix et de la vidéo sur un même réseau. Cependant, pour garantir une qualité de service (QoS) et une sécurité optimale, il est nécessaire d'implémenter la ToIP sur une architecture MPLS VPN.

La mise en place d'une ToIP garantissant la QoS et la sécurité des communications est une problématique complexe. En effet, les réseaux IP sont soumis à des perturbations telles que les congestions, les retards et les pertes de paquets qui peuvent affecter la qualité des communications. De plus, les communications doivent être sécurisées pour éviter toute interception ou intrusion malveillante.

Pour répondre à cette problématique, il est nécessaire d'implémenter une architecture MPLS VPN qui permettra d'assurer une QoS optimale en réservant des ressources pour les communications vocales et en garantissant un débit minimal. De plus, cette architecture permettra de sécuriser les communications en utilisant des tunnels VPN pour chiffrer les données.

Nous avons mis en place ce travail au sein d'Algérie Télécom, qui est une société nationale algérienne spécialisée dans le domaine des télécommunications. Elle offre une gamme complète de services tels que l'accès Internet haut débit, la téléphonie fixe et mobile ainsi que l'hébergement web.

Ce mémoire est organisé en quatre chapitres, présentés comme suit :

Le premier chapitre sera consacré au routage, qui est un élément clé de la communication entre les différents réseaux informatiques. Il permet de déterminer le chemin optimal pour acheminer les données d'un point à un autre. Nous allons explorer les différentes formes de routage, notamment le routage statique consiste à configurer manuellement les routes dans la table de routage du routeur, tandis que le routage dynamique utilise des protocoles de routage pour échanger des informations entre les routeurs et mettre à jour automatiquement la table de routage. Nous allons également étudier en détail deux protocoles de routage largement utilisés : OSPF (Open Shortest Path First) et BGP (Border Gateway Protocol).

Le deuxième chapitre de notre étude portera sur la téléphonie sur IP (ToIP). La ToIP est une technologie qui permet de faire passer les appels téléphoniques sur un réseau IP. Elle fonctionne en convertissant la voix analogique en paquets numériques qui sont ensuite transmis sur le réseau IP. Pour cela, il est nécessaire d'utiliser des protocoles spécifiques tels que SIP

(Session Initiation Protocol) ou H.323, qui permettent d'initier et de gérer les sessions de communication. Nous allons également aborder les notions de qualité de service (QoS) qui est un élément important dans la mise en place d'une solution ToIP pour garantir une qualité de voix optimale.

Le troisième chapitre de notre étude approfondie sur les réseaux informatiques se concentrera sur la technologie MPLS, également connue sous le nom de Multi Protocol Label Switching. Cette technologie est largement utilisée dans les réseaux modernes pour améliorer la vitesse et l'efficacité de la commutation de paquets. En effet, MPLS permet de créer des tunnels entre deux points du réseau en ajoutant une étiquette à chaque paquet pour indiquer le chemin à suivre vers sa destination finale. Cette méthode est plus rapide que les méthodes traditionnelles de commutation de paquets, car elle évite les traitements complexes des adresses IP et des tables de routage. Nous allons nous intéresser aux applications les plus importantes de MPLS, notamment la création de réseaux privés virtuels (VPN) sécurisés sur un réseau public comme internet. Les VPN sont largement utilisés par les entreprises pour connecter leurs différents sites distants en toute sécurité. Avec MPLS, il est possible d'isoler le trafic VPN en utilisant des étiquettes spécifiques pour chaque tunnel. Ainsi, même si le trafic passe par un réseau public non sécurisé comme internet, il reste protégé contre les attaques externes. Pour mettre en place un réseau MPLS VPN, il faut configurer les routeurs pour prendre en charge le protocole MPLS et définir les différents tunnels qui seront utilisés pour acheminer les données entre les différents sites du VPN. Cette configuration peut être complexe et nécessite une expertise technique avancée. Cependant, une fois mis en place correctement, un réseau MPLS VPN offre une sécurité accrue et une meilleure performance que d'autres solutions VPN traditionnelles.

Dans le dernier chapitre qui sera consacré à la simulation, nous allons utiliser GNS3 pour simuler notre infrastructure réseau. Nous allons configurer notre réseau en utilisant les connaissances acquises dans les chapitres précédents et tester notre solution ToIP.

L'implémentation de la ToIP sur une architecture MPLS VPN est un projet complexe qui nécessite une compréhension approfondie du routage, de la ToIP et de MPLS. Ensuivant les connaissances acquises dans ce projet, nous pouvons mettre en place une solution ToIP efficace qui offre des avantages tels que la réduction des coûts et l'amélioration de la qualité des appels à travers la simulation sous GNS3.

Chapitre I

Généralités sur Le routage

I.1 Introduction

Les échanges au sein d'un réseau informatique dépendent principalement du processus de routage, dont les protocoles constituent la base. Sans eux, aucun échange ne serait possible. Toutefois, l'expansion d'internet et l'émergence de services convergents ont entraîné des problèmes de performance menaçant la stabilité et la rentabilité du réseau. Les chercheurs ont donc développé des solutions allant d'une simple amélioration à un changement radical dans les technologies existantes en se concentrant sur les protocoles de routage, qui ont un impact direct sur les performances du réseau.

I.2 Routage IP

Le routage est le processus de sélection du chemin optimal pour acheminer des données d'un réseau à un autre. Il implique l'utilisation de protocoles de routage pour déterminer la meilleure route possible en fonction de facteurs tels que la distance, la bande passante, le coût et les conditions du réseau. Le routage est essentiel pour assurer une communication efficace et fiable entre les différents réseaux et périphériques connectés à Internet. On dispose deux types de routage [1][2] :

I.2.1 Routage statique

Le routage statique est un routage où chaque route a été saisie manuellement par l'administrateur. Il est utilisé dans les tout petits réseaux. Il est facile à gérer lorsque le nombre de routes reste limité. Lorsqu'une route est en panne, l'intervention de l'administrateur est obligatoire pour saisir une route de secours [3].

I.2.2 Routage dynamique

Le routage dynamique est un routage où les routes sont calculées et saisies grâce à un protocole de routage. Il est utilisé dans les plus grands réseaux. Il est plus difficile à mettre en place, mais plus facile à maintenir. Lorsqu'une route est en panne, il recalcule automatiquement un autre chemin [3].

I.3 Système autonome AS

Un système autonome est un ensemble de routeurs qui partagent des politiques de routage similaires et qui sont gérés dans un même domaine administratif [4].

I.4 Table de routage

La table de routage est une structure de donnée qui est stockée sur les routeurs pour déterminer le chemin qu'empruntera un paquet de données. Elle garde une trace des routes vers une destination spécifique du réseau. Elle peut établir une correspondance entre le réseau de destination et l'adresse du routeur suivant, permettant d'atteindre la destination finale. Une route a quatre composants principaux, qui sont [5] :

- Réseau cible (Le réseau de destination).
- Masque de sous-réseau.
- Adresse de la passerelle ou de l'interface.
- Une métrique de route qui représente la valeur d'une route par rapport à d'autres routes. La gamme complète des composants métriques peut être trouvée à [6] :
  - Le nombre de sauts (RIP)
  - La bande passante (EIGRP)
  - Latence ou bien le délai (EIGRP)
  - La charge (EIGRP)
  - La fiabilité (EIGRP)
  - Le coût (OSPF)

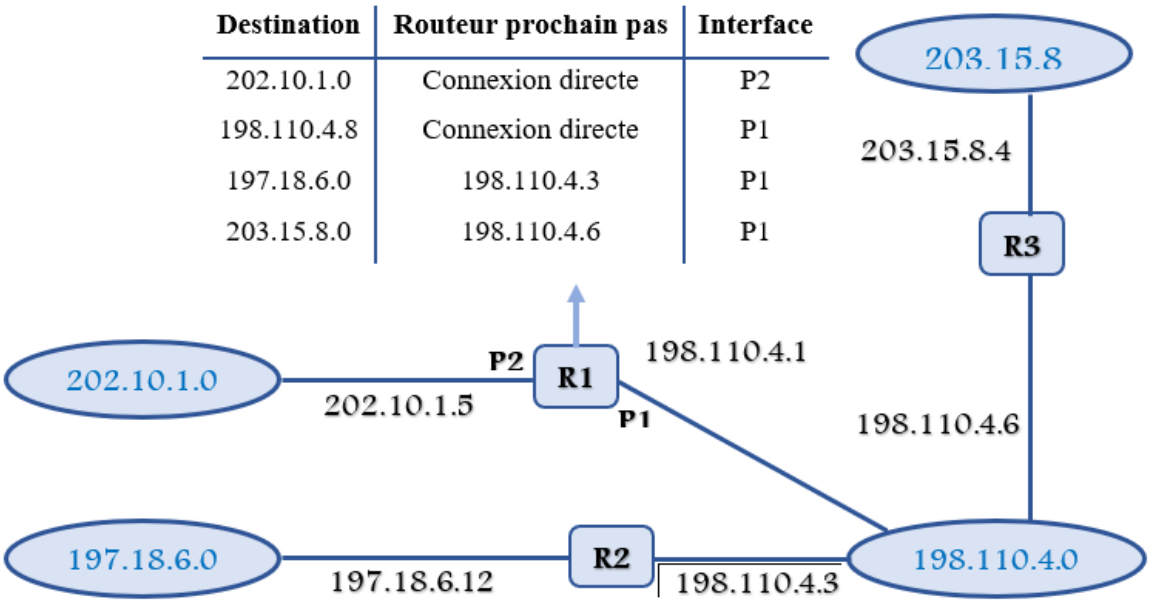

Figure I.1. *Exemple d'une table de routage [7]*

I.5 Classification des protocoles de routage dynamique

Tous les protocoles de routage exécutent les mêmes fonctions de base. Ils déterminent la meilleure route vers chaque destination et distribuent au voisinage les informations d'acheminement entre les systèmes d'un réseau. Les modalités d'exécution de ces fonctions, en particulier les procédures de sélection des meilleures routes permettent de distinguer les différents protocoles [8].

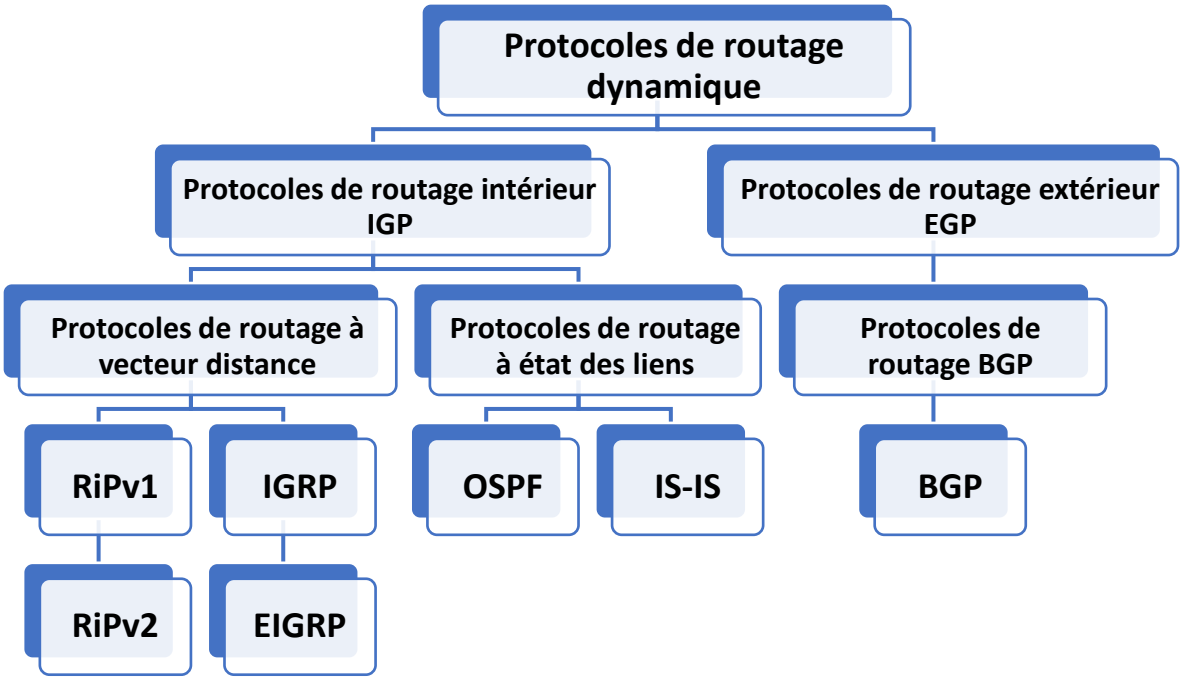

Figure I.2. *Classification des protocoles de routage dynamique*

I.5.1 Classification par mécanisme de travail et algorithme

Les protocoles de routage dynamique peuvent être classés en protocoles de routage vectoriel à distance et en protocoles de routage d'état de liaison selon leurs mécanismes de travail et algorithmes [9].

❖ **Protocoles de routage de vecteur de distance**

Les protocoles de routage à vecteur de distances sont des protocoles permettant de construire des tables de routage où aucun routeur ne possède la vision globale du réseau, la diffusion des routes se faisant de proche en proche. Le terme « vecteur de distance » vient du fait que le protocole manipule des vecteurs (des tableaux) de distances vers les autres nœuds du réseau. La distance en question est le nombre de sauts permettant d'atteindre les routeurs voisins. Ces protocoles s'appuient sur l'algorithme de Ford-Bellman [7].

❖ **Protocoles de routage à l'état de lien**

Dans les protocoles à l'état de lien, chaque routeur communique tous les autres routeurs en échangeant des informations, permettant à chaque routeur de construire une vue complète de la topologie du réseau et de sa table de routage avec les meilleures routes à l'esprit.

Tous les paquets sont transmis via la meilleure route. Les métriques utilisées sont :

- Qualité du lien.
- Sa taille.
- Le type de flux à envoyer (transmettre).
- Des limites de QoS appliquées
- Les coûts financiers.

Cette méthode de routage génère une table de routage plus rapidement que le routage à vecteur de distance.

I.5.2 Classification par aire de travail

Par zone de travail, les protocoles de routage dynamique peuvent être classés en protocoles de passerelle intérieure et en protocoles de passerelle extérieure.

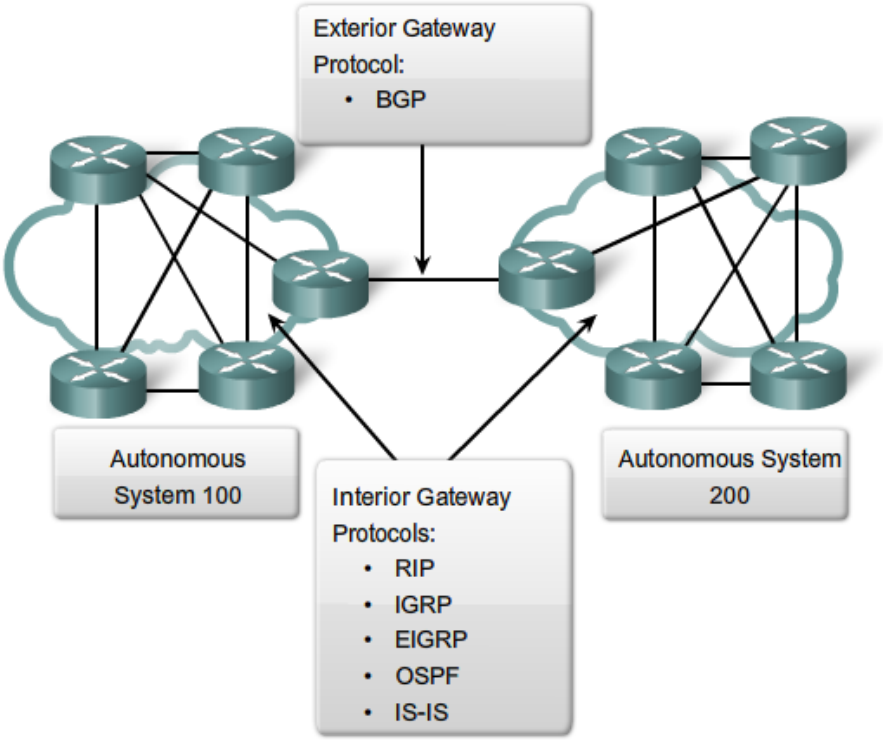

Figure I.3. *IGP et EGP [10]*

❖ **Interior Gateway Protocol (IGP)**

Interior Gateway Protocol (IGP) est un protocole de routage responsable du routage dans un système autonome. Il est chargé de s'assurer que chaque routeur dans un domaine suit la même manière de représenter les informations de routage et les mêmes règles pour la publication et le traitement des informations. Il est principalement utilisé pour découvrir et calculer des itinéraires.

Les protocoles de passerelle intérieure comprennent :

1- RIP (Routing Information Protocol)

Le protocole RIP (Routing Information Protocol) est un protocole de routage à vecteur de distance utilisé pour échanger des informations de routage entre les routeurs d'un réseau. Il utilise une métrique basée sur le nombre de sauts pour déterminer la meilleure route vers une destination.

- **Versions de RIP**

Il existe actuellement deux versions à ce jour, RIPv1 ainsi que RIPv2

✓ **RIPv1**

RIPv1 est défini dans la RFC 1058. Cette version ne prend pas en charge les masque des sous réseaux de longueur variable ni de l'authentification des routeurs. Les routes sont envoyées en broadcaste.

✓ **RIPv2**

RIPv2 est défini dans la RFC 2453. Cette version, développée en 1993, a été conçue pour permettre au protocole de répondre aux contraintes des réseaux actuels (découpages des réseaux IP en sous-réseaux, authentification par mot de passe). Avec cette version, les routes sont envoyées à l'adresse multicast 224.0.0.9.

2- IGRP (Interior Gateway Routing Protocol)

Il s'agit d'un protocole propriétaire de Cisco qui surmonte (pallier) les défauts de RIP, a une seule métrique et a un nombre limité de sauts. Il utilise des diffusions de mise à jour périodiques comme RIP, mais en 90 secondes au lieu des 30 secondes de RIP, il a donc moins d'impact sur le réseau. Son processus d'acheminement et le choix d'une route est basé sur la prise en compte des paramètres suivants :

- Bande passante (largeur de bande)
- Lien de charge (charge sur les liens)
- Topologie de latence (délais sur la topologie)
- Fiabilité du chemin.
- Taille maximale des paquets.

IGRP peut partager le trafic (répartition de la charge) sur des chemins de coût presque égal (load splitting) sans risque de boucles [11].

- **Versions d'IGRP :**

On peut citer une seule version existante :

✓ **EIGRP (Enhanced Interior Gateway Routing Protocol)**

Enhanced IGRP représente une évolution de l'IGRP. Ceci est le résultat des changements dans le réseau et des diverses requêtes qu'on attend d'IGRP. EIGRP intègre la fonctionnalité d'un protocole d'état de lien (Link-State Protocol) avec un protocole de vecteur de distance (Distance-Vector Protocol). Il comprend l'algorithme DUAL (Diffusing-Update Algorithme) développé par le Dr Garcia-Luna Aceves de SRI International [11].

3- OSPF (Open Shortest Path First)

OSPF (Open Shortest Path First) est un protocole de routage à état de lien qui utilise le coût de la bande passante pour déterminer le chemin le plus court entre deux nœuds dans un réseau. Il est largement utilisé dans les réseaux d'entreprise et les fournisseurs de services Internet.

➢ **Fonctionnement du protocole OSPF**

Le protocole OSPF échange des informations sur les liens entre les routeurs du réseau. Chaque routeur OSPF maintient une base de données topologique qui contient des informations sur tous les liens du réseau, y compris leur coût et leur état. Les routeurs OSPF utilisent cette base de données pour calculer le chemin le plus court vers toutes les destinations du réseau [12].

Le protocole OSPF utilise des messages Hello pour découvrir et maintenir la connectivité entre les routeurs voisins. Les routeurs échangent également des messages Link State Advertisement (LSA) pour partager des informations sur leur état et leurs liens avec d'autres routeurs OSPF [13].

Les routeurs OSPF sont organisés en domaines, qui sont des groupes logiques de routeurs qui partagent une base de données topologique commune. Les domaines peuvent être connectés à d'autres domaines via des passerelles d'interconnexion (Area Border Routers ou ABR) [13].

4- IS-IS (Système Intermédiaire à système Intermédiaire)

Intermediate System to Intermediate System (IS-IS) est un protocole de routage d'état de liaison présentant des similitudes avec OSPF. Il s'agit d'un protocole de passerelle intérieure (IGP) qui est principalement implémenté pour le routage au sein de grands domaines de réseau de fournisseurs de services. Il propose trois modes d'utilisation possibles du protocole IS-IS [9] :

- Mode OSI uniquement.
- Mode IP uniquement.
- Le mode double prend en charge deux formats d'adresse en même temps.

Quel que soit le mode d'utilisation choisi, le protocole repose sur un routage à deux niveaux hiérarchiques, le niveau L1 et le niveau L2, où chaque niveau est associé à une base de topologie (LSDB) distincte.

❖ **EGP (Exterior Gateway Protocol)**

Exterior gateway protocol (EGP) est conçu pour être utilisé entre des réseaux contrôlés par deux organisations différentes. Les EGP sont généralement utilisés entre les fournisseurs de services Internet (FSI) ou entre une entreprise et un FSI.

Un EGP doit isoler les systèmes autonomes. Parce que les systèmes autonomes sont gérés par différentes administrations, les réseaux doivent avoir un protocole pour communiquer entre différents systèmes.

1- **BGP (Border Gateway Protocol)**

Le Border Gateway Protocol est un protocole de communication. Il se charge dynamiquement de calculer les meilleurs chemins vers une destination et de les propager à travers les réseaux IP [14].

C'est un protocole de routage complexe qui est au cœur du fonctionnement d'Internet. Son objectif principal est d'échanger des informations de routage et d'assurer l'accessibilité de

réseaux, appelés préfixes, entre les AS. Comme il circule sur TCP, il est considéré comme appartenant à la couche application du modèle OSI.

- **Les types d'entité BGP**

Il existe deux versions de BGP : Interior BGP (iBGP) et Exterior BGP (eBGP) comme le montre la figure I.4. iBGP est utilisé à l'intérieur d'un AS alors que eBGP est utilisé entre deux AS [15].

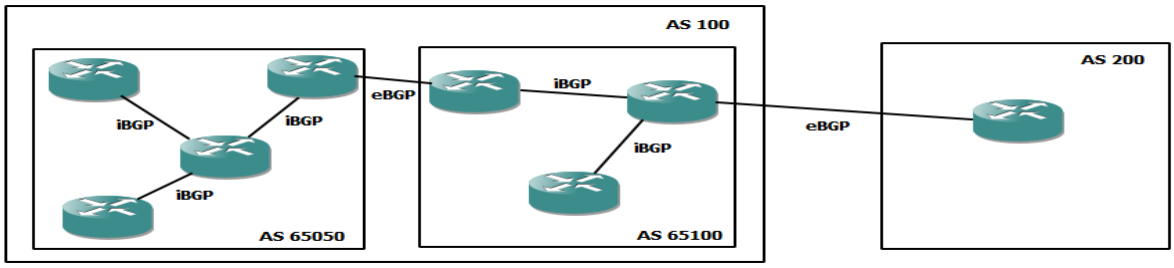

Figure I.4. *Réseau utilisant iBGP et eBGP [14]*

- Les connexions iBGP sont généralement établies entre des adresses logiques qui ne sont pas liées à une interface physique spécifique. En cas de panne d'un lien physique, la session iBGP reste active si une alternative est disponible et qu'un protocole de routage interne dynamique (comme OSPF) est utilisé.
- Les connexions eBGP sont établies soit sur des connexions point-à-point, soit sur des réseaux locaux. Si la liaison physique est interrompue, la session eBGP est également rompue et tous les préfixes appris par cette session sont supprimés et retirés de la table de routage.

- **Utilisation du BGP**

BGP est principalement utilisé [15] :

- Entre les opérateurs et fournisseurs d'accès à Internet pour l'échange de routes.
- La majorité des utilisateurs d'Internet ont une seule connexion à leur fournisseur d'accès. Dans ce cas, BGP n'est pas nécessaire car une route par défaut est suffisante.

Toutefois, les entreprises qui sont connectées à plusieurs fournisseurs d'accès (multihoming) peuvent bénéficier d'un numéro de système autonome et établir des sessions BGP avec chaque fournisseur.

En plus d'Internet, il est possible d'utiliser BGP pour interconnecter des réseaux IP privés, tels que des réseaux locaux qui utilisent OSPF.

- **Les décisions de routage de BGP**

BGP est un protocole de routage qui utilise des chemins, des règles et des stratégies réseau configurées par un administrateur pour prendre des décisions de routage. La table BGP est créée en comparant les routes reçues pour chaque préfixe et en choisissant la meilleure route. Seul le meilleur chemin est utilisé dans la table de routage et annoncé aux voisins. BGP utilise plusieurs critères pour choisir une route parmi d'autres [15].

- **Origin (origine) :** Le choix du chemin préféré dépend de la manière dont ils sont connus via le protocole BGP.
- **Local preference (Préférence locale):** L'attribut de préférence local est utilisé pour sélectionner le point de sortie pour un itinéraire spécifique.
- **AS-path (Chemin- AS) :** Préférence du chemin avec les moins d'AS traversés.
- **Le MED (Multi-exit discriminator):** Est une préférence basée sur la métrique (nombre de sauts et coût) communiquée par l'AS d'origine.
- **Next hop (Prochain saut) :** Si le routeur ne dispose pas d'informations de routage pour déterminer la prochaine adresse IP à atteindre, l'itinéraire sera supprimé.
- **Community (Communauté) :** Il fournit un moyen de regrouper des destinations.
- **Router ID :** Le choix du chemin dépend de l'identifiant du routeur(l'id), qui est unique au sein d'un même système autonome.

I.6 Les fonctions de base des protocoles de routage

En règle générale, un routeur détermine le chemin que doit emprunter un paquet entre deux liaisons à l'aide des deux fonctions de base suivantes :

- La détermination du chemin.
- La commutation.

I.6.1 La détermination du chemin

La détermination du chemin se produit au niveau de la couche réseau. La fonction de détermination du chemin permet à un routeur d'évaluer le chemin vers une destination donnée et de déterminer le meilleur chemin pour traiter le paquet. Les routeurs utilisent des tables de routage pour déterminer le meilleur chemin, puis utilisent des fonctions de commutation pour transférer les paquets.

I.6.2 La commutation

La fonction de commutation est un processus interne utilisé par les routeurs pour accepter des paquets sur une interface et les transmettre à une seconde interface sur le même routeur. La responsabilité principale de la fonction de commutation est d'encapsuler le paquet de données dans un type de trame approprié pour la liaison suivante.

Les routeurs utilisent la partie réseau de l'adresse pour choisir un chemin pour transmettre le paquet au routeur suivant sur le chemin, une fois qu'il atteint le routeur local, il utilise la partie hôte pour déterminer le port vers lequel il va envoyer les paquets.

I.7 Conclusion

En conclusion, le routage IP est un élément clé de la communication sur Internet (les réseaux informatiques). Il permet de diriger les paquets de données vers leur destination en utilisant des tables de routage et des protocoles de routage tels que OSPF, BGP et RIP.

Le routage IP est également important dans la mise en place de la ToIP (Téléphonie sur IP), car il permet de faire transiter les appels téléphoniques via des réseaux IP.

Chapitre II

« ToIP »

La Téléphonie

Sur IP

II.1 Introduction

ToIP (Telephony over Internet Protocol) est une technologie qui peut transmettre des communications vocales ou des appels téléphoniques sur Internet. Il est apparu dans les années 1990 et a connu un développement important au cours des dernières décennies.

L'histoire de la ToIP remonte aux années 1990, lorsque les premiers protocoles VoIP ont été développés. Au fil du temps, ces protocoles ont évolué pour offrir une meilleure qualité de service et des fonctionnalités plus avancées [16].

Aujourd'hui, la ToIP est largement utilisée par les entreprises et les particuliers du monde entier. Elle offre des avantages tels que la possibilité d'utiliser un réseau unique pour la transmission de la voix et des données, l'intégration facile de fonctionnalités avancées telles que la messagerie vocale et le renvoi d'appel, et surtout la réduction des coûts d'appel.

L'objectif principal de la ToIP est de remplacer le réseau téléphonique traditionnel par un réseau basé sur Internet, offrant ainsi une plus grande flexibilité et une meilleure qualité de service. Il permet également de réduire les coûts de communication, en particulier pour les entreprises qui nécessitent de grandes infrastructures de téléphonie.

II.2 Téléphonie sur IP

II.2.1 Définition

Dans la téléphonie IP, la voix et les données sont transmises de manière transparente sur une seule infrastructure IP. Cela évite le besoin d'un réseau de téléphonie dédié et tire parti d'un réseau IP existant tel que LAN, WAN ou intranet pour permettre la communication vocale à l'aide du protocole IP. Contrairement au RTC, qui transmet des signaux sur un réseau à commutation de circuits, la téléphonie IP utilise la commutation par paquets [16]. La numérisation de la voix produit un signal numérique, qui est découpé en plusieurs paquets qui traversent le réseau IP pour atteindre leur destination prévue. L'application du destinataire effectue la transformation inverse, convertissant les paquets en voix. Avec la téléphonie IP, les entreprises peuvent unifier leurs réseaux RTC et informatiques, rationalisant ainsi la communication sur un seul réseau [17].

II.2.2 Principe de fonctionnement de la téléphonie sur IP

La téléphonie sur IP fonctionne sur le principe de la conversion de la voix d'un signal analogique en un signal numérique. Le signal numérisé est compressé à l'aide de codecs sélectionnés pour réduire la quantité d'informations transmises, comme les silences. Ces

signaux compressés sont divisés en paquets, auxquels sont ajoutés des en-têtes spécifiques au réseau comme IP, UDP, RTP, etc. Les paquets sont ensuite envoyés sur le réseau.

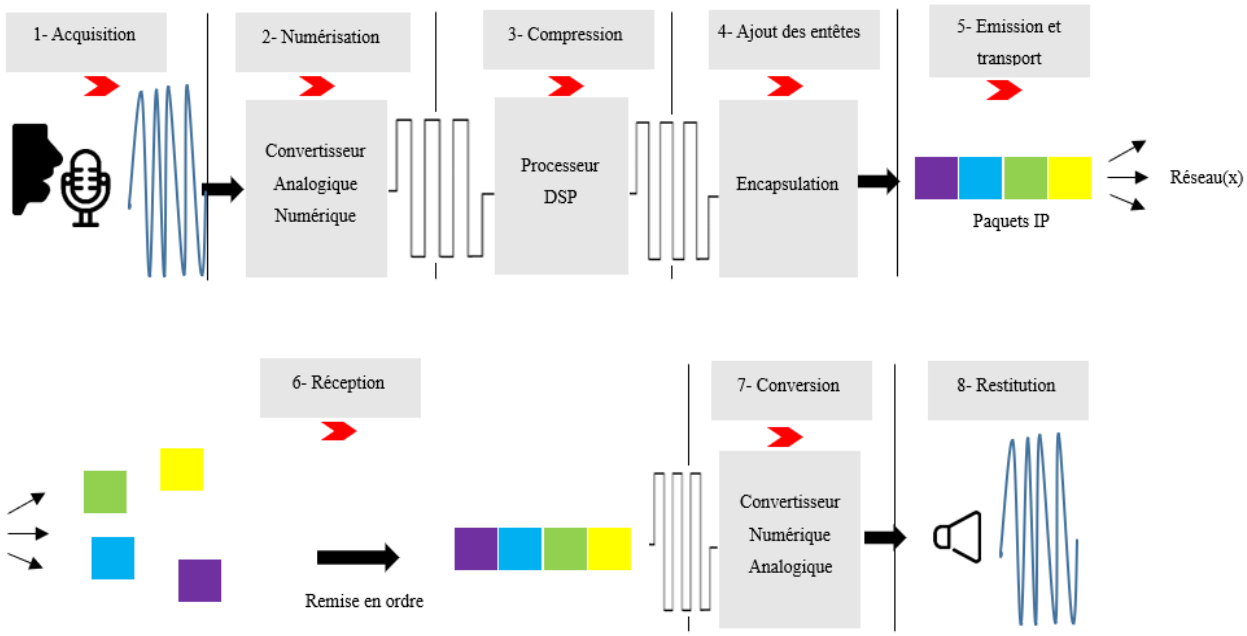

Figure II.1. *Traitement de la voix dans un réseau IP [18]*

Lorsqu'ils atteignent leur destination, les paquets entrants sont reconstruits en supprimant les en-têtes. Le signal de données résultant est ensuite décompressé et transformé en un signal analogique qui permet à l'utilisateur d'écouter le message initial.

La ToIP représente une progression des capacités de la VoIP et repose sur deux principes fondamentaux :

- La segmentation du flux vocal numérique en une série de paquets.
- Mouvement à travers le réseau IP [9].

II.2.3 Les architectures de la ToIP

Il existe différentes façons de mettre en place la téléphonie sur IP dans une entreprise, selon le niveau de convergence souhaité et en prenant en considération diverses contraintes telles que le budget ou l'équipement disponible.

- **Architecture Full IP**

L'architecture Full IP pour la Téléphonie sur IP (ToIP) implique l'utilisation exclusive de la technologie IP pour toutes les communications téléphoniques.

L'architecture Full IP repose uniquement sur des protocoles IP pour les appels, les messages vocaux, la messagerie instantanée, la visioconférence et toutes les autres formes de communications [19].

Cette approche présente de nombreux avantages, tels qu'une plus grande flexibilité, une meilleure qualité de communication et une réduction des coûts. Elle permet également une meilleure intégration avec d'autres technologies, comme les applications web et les services cloud [20].

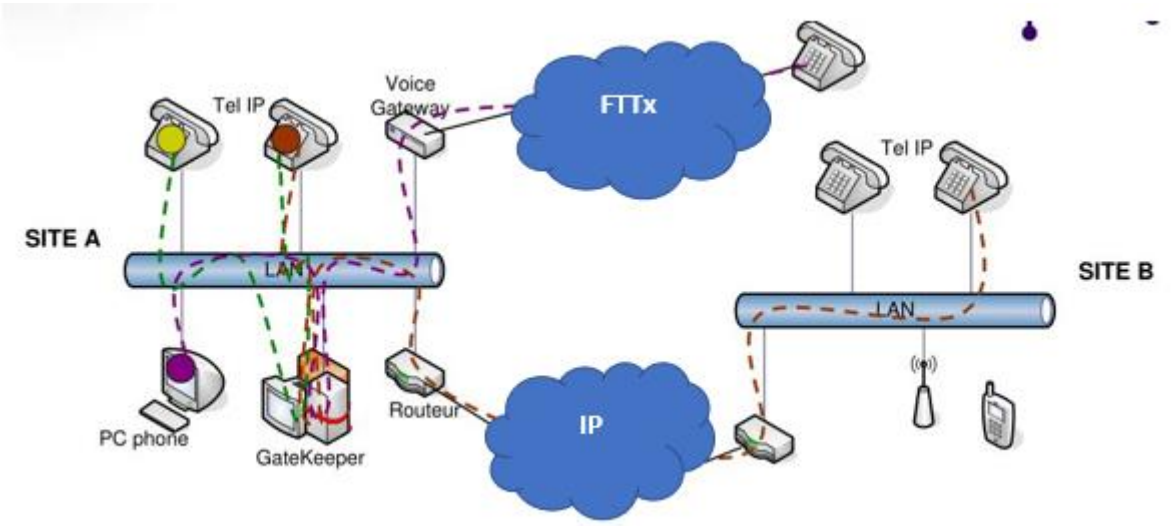

Figure II.2. *Architecture Full IP*

- **Architecture Hybride**

L'un des avantages de cette solution est qu'elle n'implique pas la modification de l'infrastructure existante, tout en bénéficiant des avantages de la voix sur IP pour les communications inter-sites. Pour mettre en place cette solution, il est possible d'ajouter un boîtier externe appelé " passerelles intégrées " au PABX, ou d'utiliser les fonctionnalités de passerelle (Gateway) intégrées aux routeurs de nouvelle génération sous forme de carte.

Cependant, les fonctionnalités de téléphonie liées aux protocoles de signalisation propres au PABX sont généralement perdues lors du passage par les passerelles intégrées. Cette approche peut être utilisée pour le transport inter-sites, constituant ainsi la première étape de la migration vers le full-IP [21].

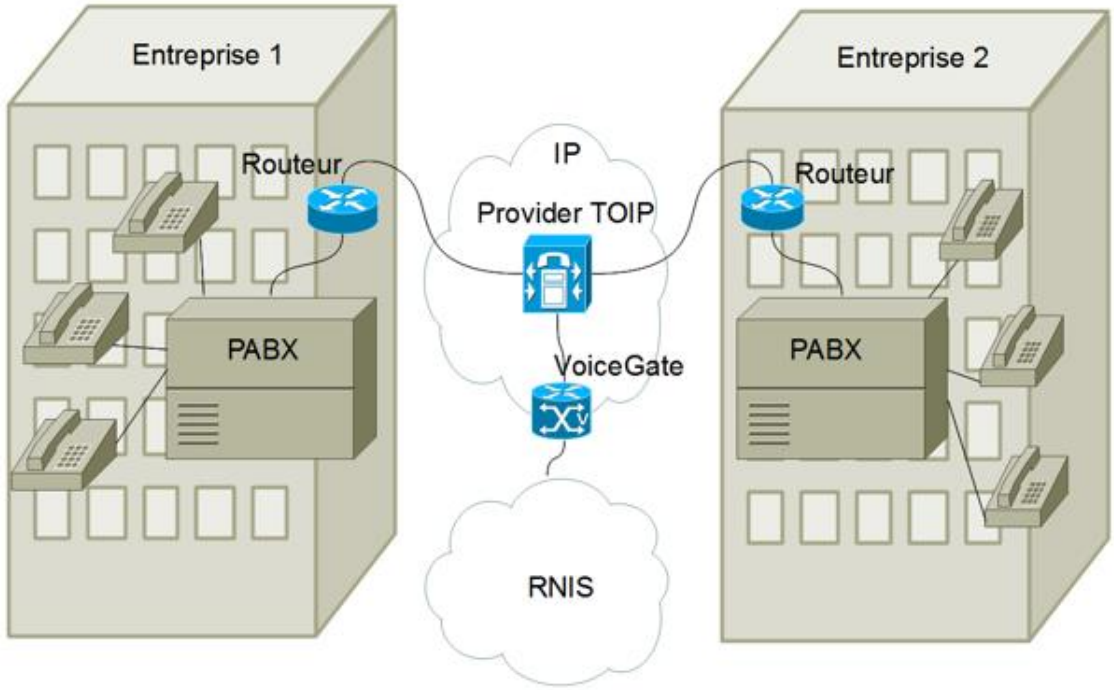

Figure II.3. *Architecture Hybride [22]*

- **Architecture Centrex**

Le centrex IP, également connu sous le nom de "téléphonie dans le Cloud" ou "téléphonie hébergée", est une solution dématérialisée basée sur les technologies VoIP qui convient parfaitement aux normes téléphoniques des entreprises. Cette solution offre de nombreux avantages et représente une nouvelle façon d'aborder les communications internes et externes d'une entreprise. Avec la téléphonie dans le Cloud, les appels téléphoniques sont acheminés via le protocole Internet de l'entreprise, tout comme les autres données informatiques. L'infrastructure du centrex est hébergée physiquement chez l'opérateur téléphonique de l'entreprise, qui mutualise son système entre ses différents clients tout en cloisonnant numériquement les informations en transit pour garantir la sécurité et la confidentialité des données stockées [23].

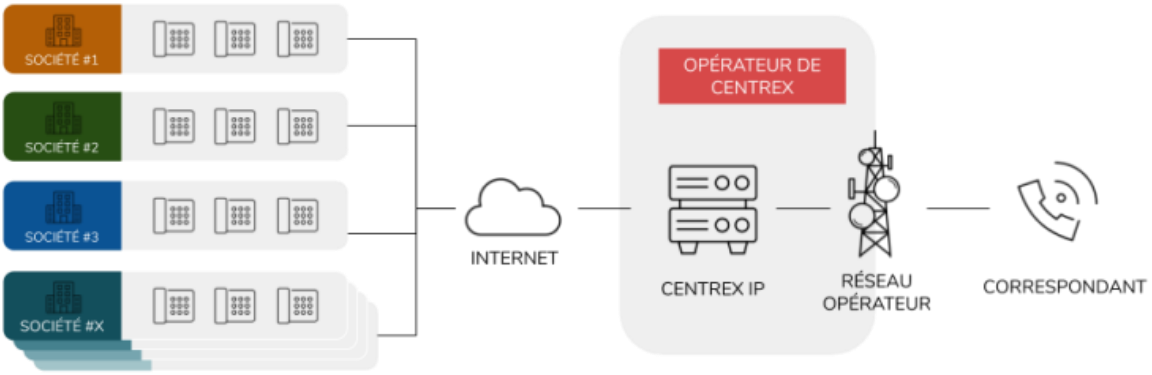

Figure II.4. *Architecture Centrex [23]*

II.2.4 Les différents types de la ToIP

- **Téléphonie entre deux ordinateurs (pc to pc)**

Dans ce modèle, chaque ordinateur est pourvu d'une carte son, d'un microphone et d'un haut-parleur. Il se connecte directement au réseau internet via un modem ou une carte NIC. Les ordinateurs doivent installer un logiciel VoIP pour passer des appels [23].

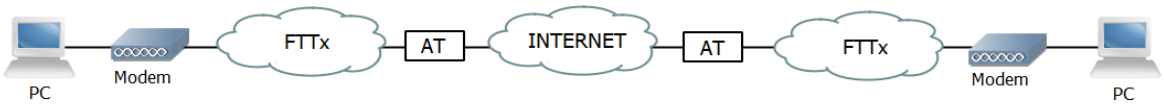

Figure II.5. Téléphonie pc to pc

- **Téléphonie entre PC et poste téléphonique (pc to phone)**

Ce modèle offre une fonctionnalité plus étendue que la simple connexion PC à PC. Il permet aux utilisateurs de passer des appels entre le réseau IP et le réseau RTC grâce à une passerelle qui assure la connexion entre les deux réseaux [23].

Figure II.6. *Téléphonie pc to phone*

- **Téléphonie entre deux postes téléphonique (phone to phone)**

Le type de communication PC à téléphone a été étendu pour utiliser le réseau internet au lieu des réseaux PSTN. Lorsqu'un appel est effectué, le réseau PSTN se connecte à la

passerelle la plus proche, qui convertit ensuite le numéro de téléphone en adresse IP pour acheminer les paquets vers leur destination [23].

Figure II.7. *Téléphonie phone to phone*

II.3 Les différents protocoles utilisés en ToIP

II.3.1 Les protocoles de signalisation

La signalisation désigne la transmission d'un ensemble de signaux et d'informations de contrôle échangés entre les intervenants d'une communication. Ces intervenants peuvent être des entités en bout de liaison (terminaux) ou des entités intermédiaires de contrôle et de gestion des communications. Leurs échanges permettent l'initiation, la négociation, l'établissement, le maintien et la fermeture de la connexion.

Dans le cas typique d'une application de téléphonie, lorsqu'une personne en appelle une autre, elle n'a initialement pas de données à lui transmettre, mais veut simplement être mise en relation avec son correspondant. Cette mise en relation nécessite d'abord de localiser l'appel, puis de faire sonner son poste, afin de lui signaler l'appel. Pour la localisation comme pour l'avertissement d'appel, on parle de signalisation.

En ToIP, il existe plusieurs protocoles de signalisation tels que : SIP, H.323, MGCP, IAX, MEGACO… [24].

- **Le protocole H323**

En 1996, l'UIT-T a introduit le protocole de signalisation H.323 pour permettre la configuration, la modification et la terminaison de sessions multimédias, y compris la voix, la vidéo et les données. Ce protocole est une version avancée du protocole Q.931 du RNIS et fonctionne en transmettant des informations en mode paquet. Il fournit également des services supplémentaires proches de ceux offerts par le réseau RNIS. Alors qu'il était initialement destiné à la transmission vocale sur LAN, H.323 a évolué pour englober des réseaux informatiques à plus grande échelle tels qu'Internet et Intranet.

Architecture et composants

La norme H.323 est constituée de quatre composants principaux :

- Terminal.
- Gatekeeper.
- Passerelle.
- MCU.

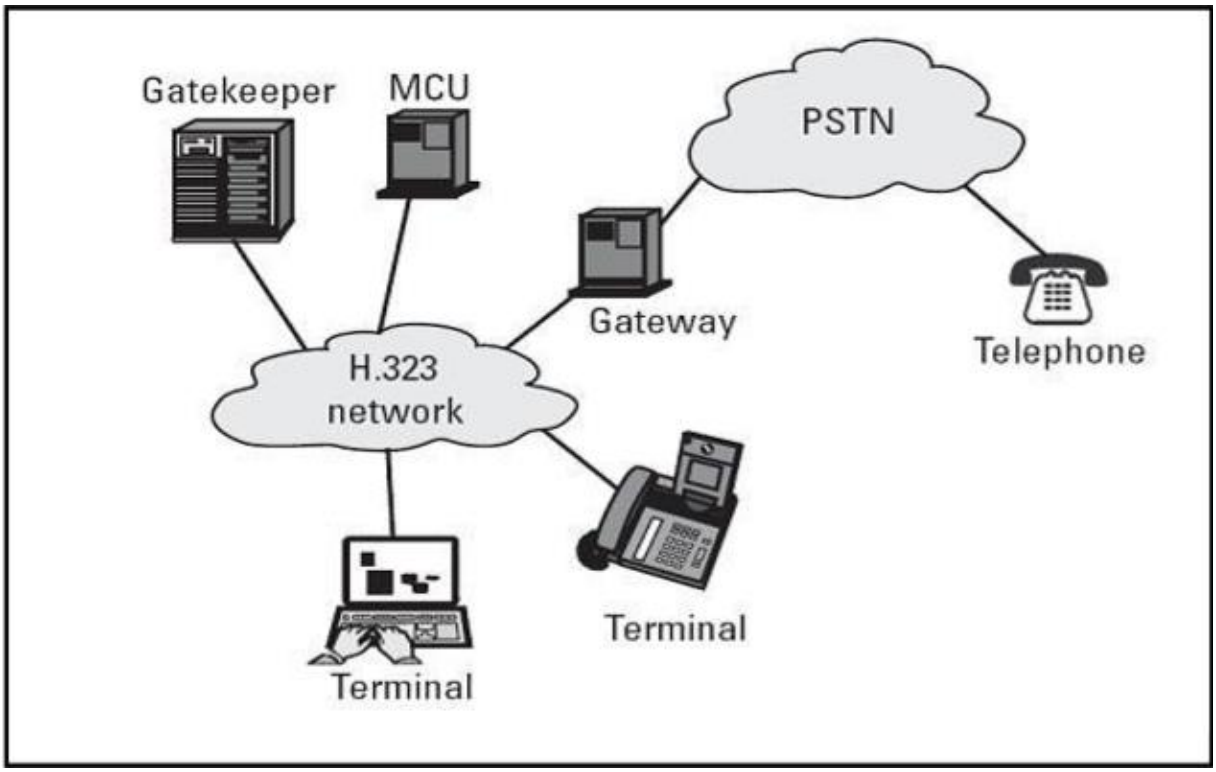

Figure II.8. *Les composants de l'architecture H.323 [23]*

- **Le Gatekeeper** : Est un composant clé de l'architecture de la VOIP qui assure la gestion de l'enregistrement, de l'admission et du statut des terminaux et passerelles. Il est également responsable de la gestion de la zone, du traitement des appels et du signalement d'appels.
- **Le terminal H.323** : Est considéré comme le point central du réseau de la VoIP, car il permet de se connecter au réseau pour effectuer des appels avec d'autres terminaux de la VoIP ou d'autre réseaux, accepter des appels entrants et mettre fin à des appels.
- **Le MCU** : Est une station sur le réseau qui permet à au moins trois terminaux de participer à une conférence multipoints. Il gère les ressources de la conférence, négocie avec les terminaux pour choisir les codecs audio et vidéo à utiliser et dirige les flux de données. Le MCU est composé d'un contrôleur multipoints optionnels (MC) et de processeurs multipoints optionnels (MP). Le MC utilise le protocole H.245

pour déterminer les capacités communes des terminaux, mais ne gère pas le multiplexage des médias. C'est le rôle du MP, sous la supervision du MC.

- **Les passerelles H.323** assurent la connectivité avec divers réseaux, modems H.324, téléphones traditionnels, etc. Elles gèrent la signalisation Q.931 et les signaux de contrôle, ainsi que la coordination des médias (multiplexage, adaptation des débits et transcodage audio) [23].

- **Le protocole SIP**

Le protocole SIP est un protocole conçu pour l'internet qui permet l'établissement de sessions multimédia entre plusieurs utilisateurs ou systèmes. Il est basé sur une architecture client/serveur et utilise des adresses URI (Uniform Resource Identifier) pour localiser les terminaux, déterminer leur disponibilité et leurs capacités, ainsi que gérer et contrôler la session. Les principaux acteurs de cette architecture sont détaillés ci-dessous.

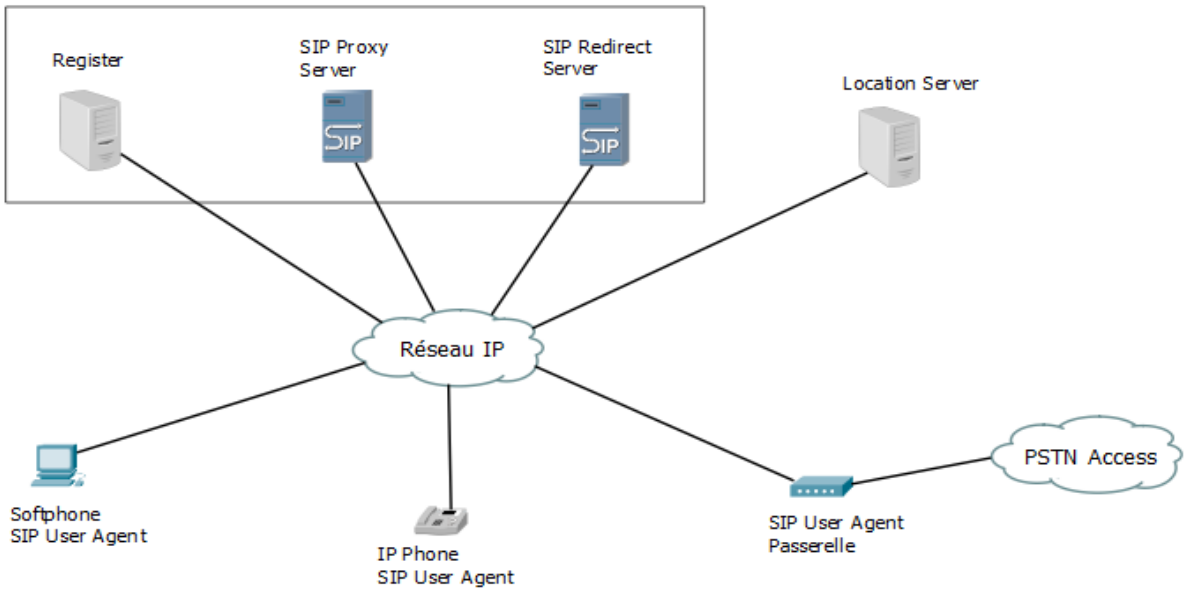

Figure II.9. *Architecture SIP. [25]*

➢ **Terminal Utilisateur**

Le terminal, également appelé UA (User Agent), est l'outil dont dispose l'utilisateur pour passer et recevoir des appels. Il peut être sous la forme d'un composant logiciel (un programme lancé à partir d'un ordinateur). Il est composé de deux sous-entités : la partie cliente (UAC – User Agent Client) qui envoie les requêtes et la partie serveur (UAS – User Agent Server) qui reçoit et traite les requêtes. Lorsqu'une entité UA envoie une requête, c'est l'UAS qui répond à l'appel. La communication entre deux entités UA se fait par le biais d'un dialogue.

➢ **Serveur d'Enregistrement**

Lorsqu'un terminal est activé dans un réseau, il envoie une requête REGISTER au serveur d'enregistrement pour lui signaler sa présence. Le serveur de localisation stocke alors cette information en associant l'identifiant de l'utilisateur à sa position.

➢ **Serveur de Localisation**

Le serveur de localisation (Location Server) complète le rôle du serveur d'enregistrement en fournissant la capacité de localiser les abonnés. Il stocke une base de données contenant les informations sur tous les abonnés qu'il gère.

➢ **Serveur de Redirection**

Le serveur de redirection joue le rôle d'un intermédiaire entre le terminal client et le serveur de localisation. Il est appelé par le terminal client pour trouver la position actuelle d'un utilisateur auprès du serveur de localisation.

➢ **Serveur Proxy**

Le serveur proxy est chargé de diriger les messages SIP [26].

- **Le protocole MGCP**

Le protocole MGCP (Media Gateway Control Protocol) est une norme établie par le groupe MeGaCo de l'IETF. Il permet de gérer les passerelles multimédia qui assurent la conversion de la voix et de la vidéo dans les réseaux IP et RTC. Le CALL Agent est l'élément clé du protocole MGCP, car il contrôle les passerelles et garantit leur bon fonctionnement.

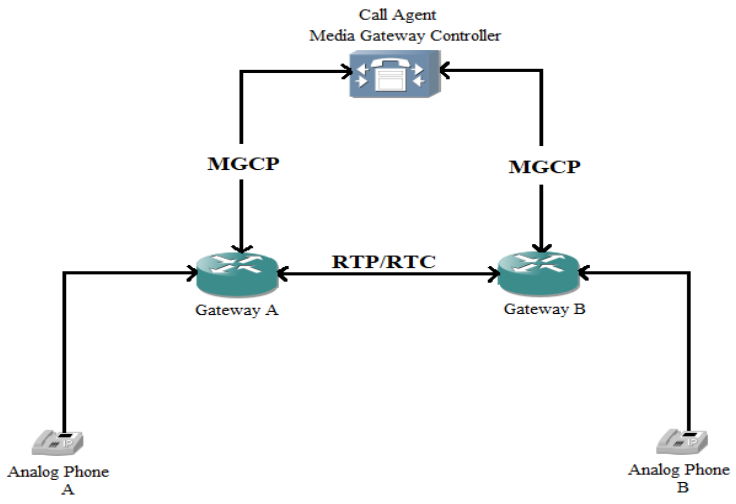

Figure II.10. *Architecture MGCP*

- **Comparaison entre les protocoles**

	H323	**SIP**	**MGCP**
Complexité	Elevée	Faible	Elevée
Implémentation de nouveaux service	NON	OUI	NON
Adapté à internet	NON	OUI	NON
Protocole de transport	TCP	TCP ou UDP	TCP ou UDP
Coûts	Elevée	Faible	Modéré
Avantages	-Maturité du protocole : Actuellement version 4 pour la définition. -Les premières mises en œuvre de V3 commencent juste à apparaître beaucoup de constructeurs Utilisent H323 -Peut supporter autre chose que IP. -Existe aussi sur ATM.	-Simple à mettre en œuvre, messages écrits en clair. -Interopérabilité très bonne Grâce à CPL (Call Processing Language) qui utilise XML, il est très facile d'ajouter des services intelligents de redirection Très bonne. -Possibilité de gestion de la mobilité utilisé pour la téléphonie 3G (UMTS).	-Permet d'utiliser des téléphones « idiots ». -Indépendant des protocoles de signalisation supérieurs (H323, SIP). -Bien pour les opérateurs voulant faire du RTC-IP-RTC.
Inconvénients	-Protocole très complexe, manque d'interopérabilité, difficultés avec les firewalls. -Support des fonctions avancées du téléphone. Pas dans l'esprit « Internet ».	-Pas encore de grande référence -Service supplémentaire de téléphonie inexistant.	-Pas encore de grande référence -Service supplémentaire de téléphonie inexistant.

Tableau II.1. *Comparaison entre les différents protocoles [27] [28]*

II.3.2 Les protocoles de transport

- **Le protocole TCP**

Le protocole TCP garantit la fiabilité des données transportées grâce à l'utilisation d'un mécanisme d'accusé de réception. Cependant, il n'est pas très rapide en termes de temps de réponse.

- **Le protocole UDP**

Le protocole de datagramme utilisateur (UDP) est plus facile à utiliser que TCP et offre une meilleure performance en envoyant des paquets sans nécessiter de confirmation de réception.

- **Le protocole RTP**

Le protocole RTP est conçu pour le transport de flux en temps réel, qui sont encapsulés dans des paquets UDP. Cela est dû au fait que les exigences pour le transport de la voix sont différentes de celles pour le transport de données.

- **Le protocole RTCP**

Le protocole RTCP (Real Time Control Protocol) est un moyen de surveiller et de gérer les flux de données et la bande passante. Il permet d'évaluer la qualité de service des sessions entre les participants en véhiculant des informations telles que le délai, la gigue, les paquets reçus et perdus. Ces quantités sont essentielles pour évaluer la qualité de toute transmission et réception temps réel.

II.4 Qualité de service

L'utilisation de mécanismes ou de technologies fonctionnant sur un réseau à capacité limitée pour gérer le trafic et garantir l'exécution des applications essentielles est appelée qualité de service (QoS). Il donne aux organisations la possibilité de réguler leur trafic réseau en donnant la priorité à des applications hautes performances particulières.

Les réseaux qui prennent en charge des systèmes gourmands en ressources sont généralement soumis à des protocoles de qualité de service (QoS). La qualité de service est essentielle pour une variété de services, notamment la télévision sur protocole Internet (IPTV), la vidéoconférence, la vidéo à la demande (VOD) et la voix sur IP (VoIP).

II.4.1 Paramètres de la qualité de service

Les paramètres clés pour mesurer la qualité de service dans un réseau ToIP sont :

- **Latence :** Est le temps mis par un paquet pour voyager de sa source à sa destination dans une communication réseau. Il est important que ce temps soit inférieur à 150 ms [5] car l'oreille humaine peut détecter des latences allant jusqu'à 250 ms. Cette fonction est considérée comme la plus critique en termes de qualité de service [29].
- **Gigue :** Est la variation de l'heure d'arrivée des paquets de données, causée par divers facteurs tels que la congestion du réseau ou la perte de synchronisation. Pour assurer une communication efficace, la gigue doit être inférieure à 100 ms. Les tampons de gigue sont utilisés pour compenser cette fluctuation et peuvent être implémentés côté récepteur pour atténuer son impact sur les flux multimédias. Cependant, cela introduit une latence au début de la lecture du flux [29].
- **Perte de paquets :** Est un indicateur qui mesure le nombre de paquets perdus après la transmission. Les paquets de données vocales sont particulièrement sensibles à toute perte de paquets, car cela peut considérablement réduire la qualité audio. Si la perte de paquets dépasse 3%, cela signifie que la qualité audio sera considérablement réduite.

II.4.2 Les fonctionnalités de QoS (Qualité de Service)

La QoS fournit un service réseau meilleur (et plus prévisible) en fournissant les fonctionnalités suivantes :

- Prise en charge de la bande passante dédiée
- Amélioration des caractéristiques de perte
- Éviter et gérer la congestion du réseau
- Façonner le trafic réseau
- Établir les priorités en matière de trafic sur l'ensemble du réseau

Qualité de service pour voix sur IP traite de divers concepts et caractéristiques de la QoS applicables à la VoIP [29].

II.4.3 Les normes de la QoS dans la ToIP

Les normes qui définissent la qualité de service QoS dans la ToIP incluent :

- **Le protocole DiffServ (Differentiated Services)**

Le protocole DiffServ peut classer et traiter différemment les paquets de données selon leur priorité. Cette norme utilise des marquages sur les paquets pour indiquer leur niveau de priorité et permet ainsi aux routeurs et commutateurs d'appliquer des politiques de gestion du trafic en conséquence [30].

- **Le protocole RSVP (Resource Reservation Protocol)**

RSVP est une norme de qualité de service pour la ToIP qui permet aux applications d'indiquer leurs besoins en bande passante et aux routeurs et commutateurs d'allouer les ressources nécessaires en conséquence. Ce protocole permet de réserver des ressources pour assurer une qualité stable des communications vocales [31].

- **Le protocole MPLS (Multiprotocol Label Switching)**

MPLS est une norme de qualité de service pour la ToIP qui permet d'acheminer le trafic sur des chemins prédéfinis en utilisant des étiquettes plutôt que des adresses IP. Cette norme permet également d'appliquer des politiques de gestion du trafic en fonction des étiquettes utilisées [32].

II.5 Conclusion

La technologie ToIP offre de nombreux avantages en termes de coûts et de fonctionnalités, mais elle présente également des risques en matière de sécurité et de fiabilité du réseau. Les entreprises doivent être conscientes des vulnérabilités potentielles liées à l'utilisation des protocoles IP sur internet et prendre les mesures nécessaires pour protéger leur système téléphonique contre les menaces potentielles afin d'assurer un fonctionnement fiable et sécurisé.

L'utilisation de MPLS / VPN dans les solutions ToIP peut aider à atténuer ces risques en offrant une sécurité renforcée, une qualité de service améliorée, une évolutivité accrue et une gestion centralisée du réseau.

Chapitre III

« MPLS »

Multi Protocol

Label Switching

III.1 Introduction

Dans les années 1990, une technologie de mise en réseau révolutionnaire a été développée appelée MPLS (Multiprotocol Label Switching). Il utilise des étiquettes au lieu d'adresses IP pour acheminer les paquets de manière plus efficace. Cette solution innovante améliore la sécurité, la gestion du trafic et la qualité de service sur le réseau.

Grâce à la technologie MPLS, les réseaux privés virtuels (VPN) sont souvent mis en place pour les entreprises. En utilisant cette méthode, les entreprises sont en mesure d'interconnecter en toute sécurité leurs différents sites distants via un réseau privé qui s'exécute sur l'infrastructure accessible au public d'un fournisseur de services internet. Les informations sont contenues dans des paquets MPLS et sont dirigées à travers le système au moyen de tunnels virtuels.

L'isolation du trafic entre différents clients permet une sécurité renforcée avec les VPN MPLS, offrant des avantages par rapport aux autres types de VPN qui incluent également une meilleure qualité de service grâce à la gestion du trafic.

III.2 Présentation des réseaux MPLS

Le MPLS (Multi-Protocol Label Switching) est un système de transfert de données qui utilise des labels (étiquettes) pour commuter les informations. Ces étiquettes sont ajoutées au début du réseau MPLS et retirées à la fin. Cette opération se situe entre la couche de liaison de données (niveau 2) et la couche réseau (niveau 3), ce qui lui confère une classification de protocole de niveau 2,5 [33].

La figure suivante, indique clairement l'emplacement de protocole MPLS dans le modèle OSI (ISO en français) :

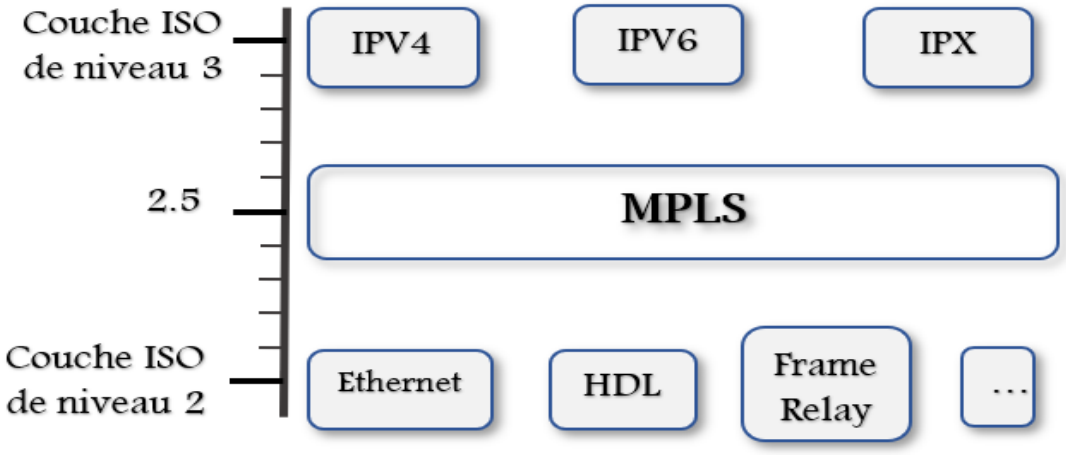

Figure III.1. *MPLS dans le modèle OSI [34]*

III.3 Architecture MPLS

III.3.1 Les composantes de MPLS

- **LSP (Label-Switched Paths)**

Le LSP est constitué d'une suite d'étiquettes insérées entre la couche 2 et la couche 3 du modèle OSI, dans le but de transmettre des paquets de données. Il fonctionne dans un seul sens, ce qui implique que le trafic de retour doit emprunter un autre LSP.

- **LSR (Label Switching Router)**

LSR est un élément central du réseau MPLS qui assure la commutation des étiquettes et participe à la création du chemin emprunté par les paquets. Les fonctions principales de ce routeur LSR incluent l'échange d'informations de routage, l'échange des étiquettes et l'acheminement des paquets.

- **LER (Label Edge Router)**

Le LER est un LSR qui sert d'interface entre un réseau MPLS et un réseau externe, ce qui en fait une passerelle d'accès au réseau MPLS. Il dispose généralement d'interfaces compatibles avec le protocole MPLS et d'autres avec le protocole IP. Il existe deux types de LER :

- INGRESS LER : Routeur qui responsable de la gestion du trafic entrant dans un réseau MPLS
- EGRESS LER : Routeur qui gère le trafic sortant du réseau MPLS.

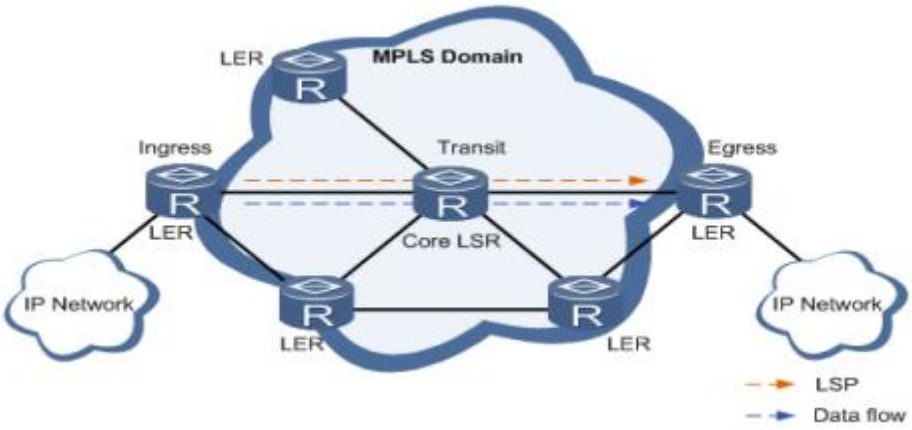

Figure III.2. *Structure du réseau MPLS [35]*

- **FEC (Forwarding Equivalence Classes)**

Un groupe d'adresses IP partageant le même préfixe ou la même classe de service est associé à un label MPLS unique par le biais du processus de MPLS.

III.3.2 Principe de fonctionnement de l'architecture MPLS

Le MPLS fonctionne en ajoutant un label à l'en-tête IP d'un paquet lorsqu'il entre dans le domaine MPLS via un LER. Ce label est utilisé pour acheminer le paquet à travers le réseau en utilisant des valeurs de label successives. Une fois que le paquet a traversé le cœur de réseau (les LSR), le LER de sortie retire le label pour retrouver le paquet IP d'origine. Cependant, ce processus implique plusieurs mécanismes, notamment l'association d'un paquet IP à une FEC lorsqu'il arrive à un Ingress LER et la mise en œuvre d'un protocole de routage pour découvrir un chemin jusqu'à l'Egress LER. Cette opération ne se réalise qu'une seule fois, et tous les paquets appartenant à la même FEC seront acheminés suivant ce chemin ou LSP. Ainsi, la fonction de routage se fait uniquement au niveau de l'Ingress LER, tandis que tous les paquets appartenant à la même FEC subissent une commutation basée sur l'utilisation des labels pour être acheminés à travers ce chemin découvert, appelé commutation de label [36].

Afin de garantir une transmission efficace des paquets par les LSR, l'Ingress LER leur attribue une étiquette ou label (label imposition ou label pushing). Ensuite, chaque LSR peut consulter sa table de commutation (LFIB) pour déterminer que tout paquet entrant avec un label spécifique appartient à une certaine FEC et doit être commuté vers une interface de sortie donnée en lui attribuant un nouveau label (label swapping). Cette opération est effectuée par tous les LSR du LSP jusqu'à ce que l'Egress LER supprime le label (label popping) et achemine le paquet de retour dans le monde IP.

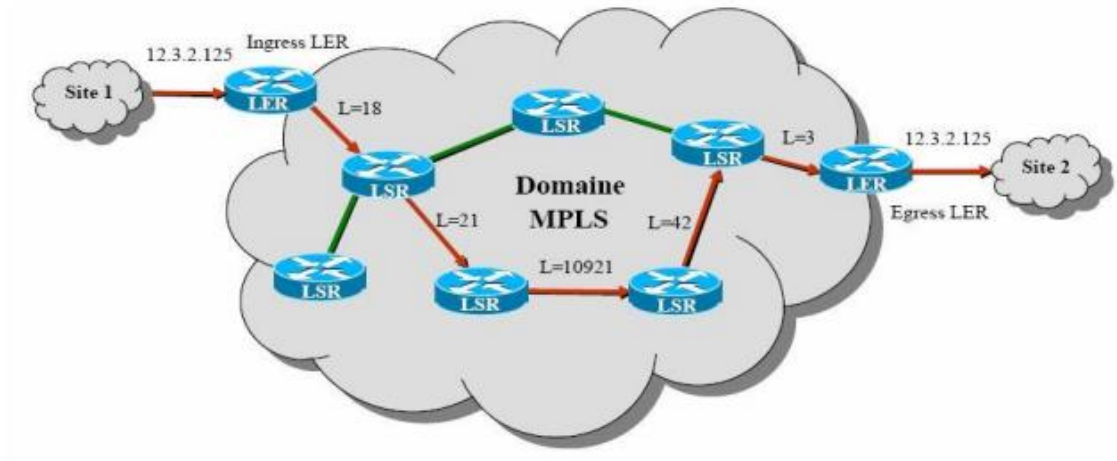

Figure III.3. *Exemple d'un réseau MPLS [35]*

III.3.3 Structure fonctionnelle de MPLS

L'architecture MPLS est capable de prendre en charge plusieurs protocoles, ce qui explique pourquoi elle se compose de deux plans principaux pour la commutation dans le réseau BACKBONE.

- **Plan de contrôle**

La responsabilité de gérer et de maintenir les étiquettes dans chaque routeur du réseau MPLS incombe à un plan de contrôle. Ce plan utilise des protocoles de routage conventionnels tels qu'OSPF ou RIP pour établir la topologie des nœuds du réseau MPLS, ainsi que des protocoles spécialement conçus pour le MPLS tels que le Label Distribution Protocol (LDP), MP-BGP que nous étudierons par la suite [37][38].

- **Plan de données**

Le mécanisme de transmission des données est totalement distinct de la signalisation et repose sur une table de commutation nommée Label Forwarding Information Base (LFIB). Cette dernière permet d'acheminer les paquets labellisés en utilisant les labels appropriés [39].

Exemple : De la figure III.4

- Réception du label 30 pour les paquets à destination du 20.0.0.0/8.
- Génération d'un label 46 pour ces paquets et expédition de l'information aux autres routeurs.
- Insertion de l'information dans la LFIB.

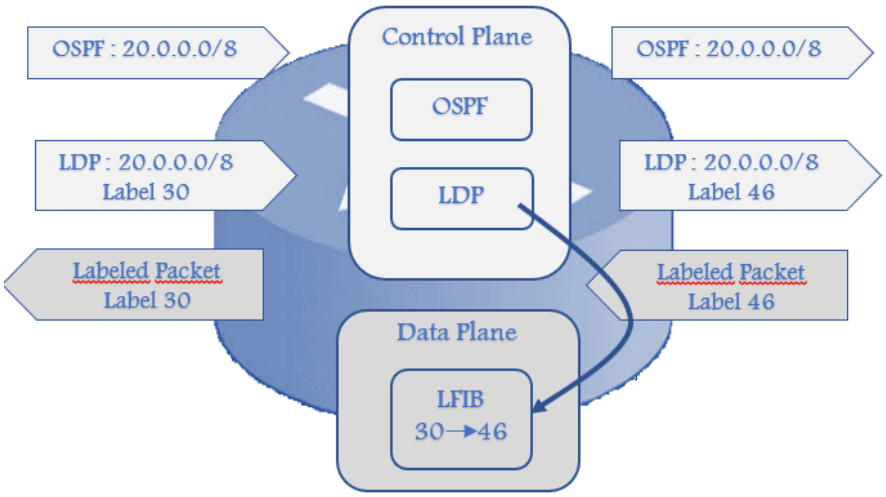

Figure III.4. *Structure fonctionnelle du routeur MPLS*

Les LSR, qui agissent à la fois comme des commutateurs pour les données utilisateur et comme des routeurs pour la signalisation, créent trois bases de données d'informations pour diriger les paquets.

- **LIB (Label Information Base)**

La table LIB est la première table créée par le routeur MPLS et sert de base de données pour LDP. Elle répertorie les labels attribués par les LSR voisins pour chaque sous-réseau IP. Cette table permet de connaître les labels attribués à un sous-réseau par chaque LSR voisin et contient tous les chemins possibles pour atteindre la destination.

- **FIB (Forwarding Information Base)**

Le FIB est la source de données qui permet de diriger les paquets non étiquetés vers leur destination via le routage IP classique. Si le label du prochain saut est valide pour le réseau de destination IP, alors le paquet sera étiqueté et acheminé.

- **LFIB (Label Forwarding Information Base)**

La table LFIB est une combinaison entre la table de routage IP et la table LIB, elle est utilisée pour commuter les paquets labellisés. Dans le réseau MPLS, chaque sous-réseau IP est appris par un protocole IGP qui détermine le prochain saut pour l'atteindre. Ainsi, pour atteindre un sous-réseau IP donné, le routeur LSR sélectionne le label d'entrée correspondant dans la table LIB et choisit comme label de sortie celui annoncé par le routeur voisin déterminé par le protocole IGP [40].

III.3.4 Construction de structures de données

La construction des structures de données implémentées par chaque routeur LSR doit suivre les étapes suivantes [41] :

- Développement de tables de routage via des protocoles de routage : Le LSR attribue une étiquette indépendamment à chaque destination dans sa table de routage
- Enregistrer l'attribution d'étiquettes significatives localement dans LIB.
- Enregistrer les actions à effectuer par ces balises et leurs prochains sauts dans la table « LFIB ».
- Le LSR envoie des informations sur sa "LIB" à ses voisins.
- Les informations reçues dans sa « LIB » sont enregistrées par chaque LSR.
- Les informations reçues du prochain bond dans la « FIB » sont enregistrées.

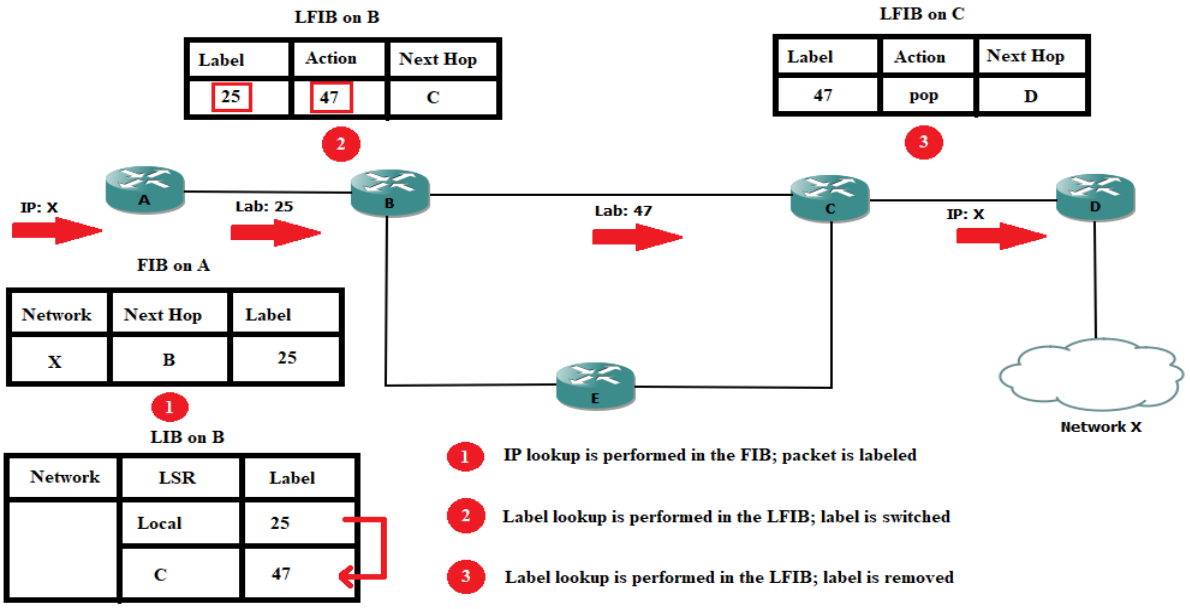

Figure III.5. *Construction des structures de données [41]*

III.4 Les labels

III.4.1 Format de label

Le label est un code de 32 bits attribué par le LER pour identifier le chemin à suivre par le paquet de données dans le nuage MPLS. Ce code est inclus directement dans le paquet de données, entre l'en-tête de niveau 2 (adresse MAC) et l'en-tête de niveau 3 (adresse IP). Le processus d'étiquetage est essentiel pour guider chaque paquet de données vers sa destination finale [42].

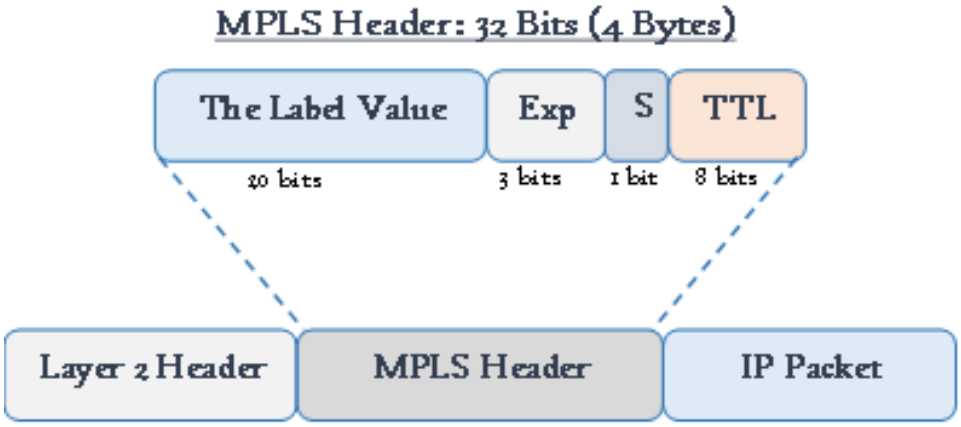

Figure III.6. *Format générique d'une étiquette MPLS [43]*

- **Label (20 bits) :** La valeur qui représente le label contient des informations sur le protocole de la couche 2 et d'autres détails nécessaires pour transférer les données.
- **Expo ou CoS (3 bits) :** Pour la classe de service du paquet (Class of Service).

- **Un bit Stack (BS) :** Indicateur de fin de pile (égal à 1 s'il s'agit du dernier label).
- **TTL (Time To Live) :** Sur 8 bits, représente la durée de vie du paquet. Ce champ TTL est identique à celui utilisé pour IP.

III.4.2 Distribution et gestion des labels MPLS

Il existe deux méthodes pour initier la communication entre les nœuds MPLS afin D'échanger les labels :

- **Descente à la demande (Downstream-on-demand)**

La figure démontre qu'un LSR peut solliciter un label de liaison pour une FEC spécifique en adressant sa demande au nœud MPLS du prochain saut de cette FEC.

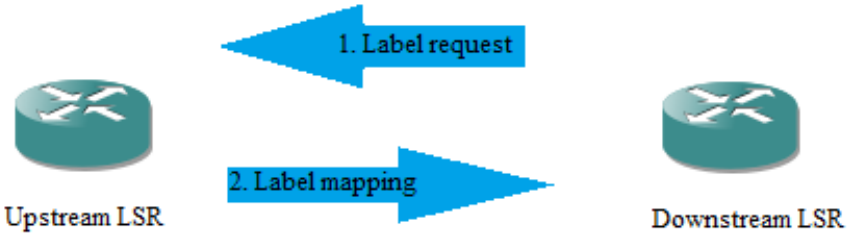

Figure III.7. *Mode downstream-on-demand [44]*

- **Descente systématique (Unsolicited downstream)**

Chaque LSR distribue automatiquement les labels associés à une FEC sans attendre une demande des LSR adjacents.

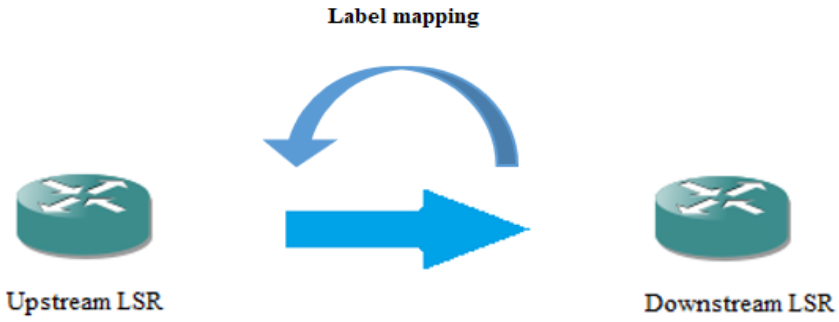

Figure III.8. *Unsolicited downstream [44]*

Il est possible d'utiliser simultanément ces deux techniques de distribution dans un même réseau. Cependant, une entente doit être conclue entre les LSR en amont et en aval quant à la technique à utiliser [44].

III.4.3 Mode de rétention des labels

L'architecture MPLS se compose de deux types de rétention de labels :

- **Mode conservatif**

Les LSR en mode DOWNSTREAM ON DEMAND utilisent uniquement les étiquettes acquises à partir de leurs PROCHAINS HOP pour chaque FEC, sans tenir compte de tous les autres. Bien que cette approche consomme moins de mémoire, elle entraîne une convergence plus lente.

- **Mode libéral**

L'utilisation d'un LSR en mode (DOWN STREAM UNSOLICITED) garantit que toutes les étiquettes annoncées, qu'elles soient utilisées ou non, sont conservées. Ce mode de fonctionnement favorise une convergence rapide. Cependant, il nécessite une quantité importante de mémoire.

III.4.4 Les opérations sur les labels

Les opérations push, swap et pop sont des opérations clés dans le fonctionnement de MPLS (Multiprotocol Label Switching). Voici un détail sur chacune de ces opérations :

- **Insérer/Empiler (Push)** : L'opération push consiste à ajouter une étiquette MPLS à un paquet IP. Cette étiquette est placée au début du paquet, juste après l'en-tête IP. Lorsqu'un routeur MPLS reçoit un paquet IP sans étiquette, il peut utiliser l'opération push pour ajouter une étiquette et ainsi créer un nouveau chemin pour ce paquet.

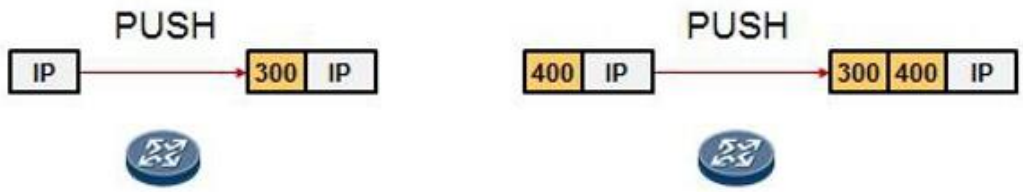

Figure III.9. *L'opération push [45]*

- **Échanger (Swap)** : L'opération swap consiste à remplacer une étiquette MPLS existante par une nouvelle étiquette. Cela se produit lorsque le paquet atteint un routeur MPLS qui doit changer le chemin du paquet en fonction de sa destination finale. Le routeur remplace alors l'étiquette actuelle par une nouvelle étiquette correspondant au nouveau chemin.

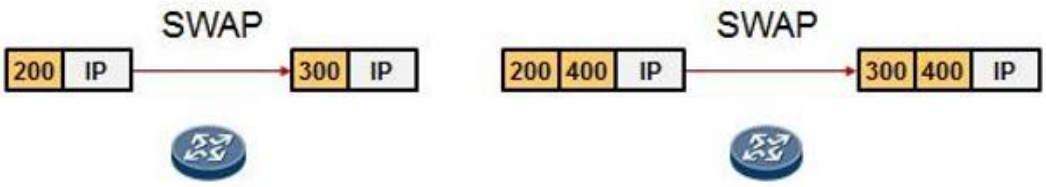

Figure III.10. *L'opération swap [45]*

- **Supprimer (Pop)** : L'opération pop consiste à retirer l'étiquette MPLS d'un paquet et à renvoyer le paquet vers son chemin d'origine (c'est-à-dire le chemin IP). Cela se produit lorsque le paquet atteint sa destination finale ou lorsqu'il rencontre un routeur qui ne prend pas en charge MPLS.

Figure III.11. *L'opération pop [45]*

En résumé, les opérations push, swap et pop sont utilisées pour créer des chemins de communication efficaces dans les réseaux MPLS en ajoutant, modifiant ou supprimant des étiquettes MPLS sur les paquets IP en transit [46].

III.4.5 Les protocoles de distribution des labels

- **TDP (Tag distribution Protocol)**

Le protocole TDP est utilisé pour distribuer des étiquettes de commutation dans les réseaux MPLS basés sur Cisco. Il utilise un processus de découverte pour identifier les routeurs voisins et établir des sessions de distribution d'étiquettes. Une fois que la session est établie, les routeurs peuvent échanger des informations sur les étiquettes à utiliser pour acheminer le trafic.

- **LDP (Label distribution Protocol)**

Le protocole LDP, quant à lui, est un protocole standardisé qui peut être utilisé dans tous les réseaux MPLS. Il utilise également un processus de découverte pour identifier les routeurs voisins et établir des sessions de distribution d'étiquettes. Une fois que la session est

établie, les routeurs peuvent échanger des informations sur les étiquettes à utiliser pour acheminer le trafic [47].

III.5 Le routage MPLS

Le routage dans MPLS se fait de deux manières :

III.5.1 Routage implicite

Aussi connu sous le nom de routage de saut par saut (hop by hop), le routage implicite dans MPLS consiste à utiliser les informations de routage existantes pour acheminer les paquets [48]. Les routeurs MPLS utilisent les tables de routage IP pour déterminer le chemin à suivre pour acheminer les paquets. Une fois que le chemin est déterminé, une étiquette est ajoutée au paquet pour identifier le chemin à suivre [49].

III.5.2 Routage explicite

Le routage explicite dans MPLS consiste à spécifier explicitement le chemin à suivre pour acheminer les paquets [39]. Cela se fait en créant des tunnels MPLS entre les routeurs. Les tunnels sont créés en ajoutant une étiquette spécifique au paquet qui indique le chemin à suivre. Les tunnels peuvent être configurés manuellement ou automatiquement en utilisant des protocoles de signalisation tels que LDP (Label Distribution Protocol) ou RSVP-TE (Resource Reservation Protocol - Traffic Engineering) [50].

III.6 MPLS-VPN (Virtual Private Network)

Le protocole MPLS est largement utilisé pour créer des réseaux privés virtuels (VPN), qui permettent de connecter plusieurs sites d'un client via une infrastructure réseau. Pour garantir l'isolation des flux de chaque client, le label MPLS est composé de deux labels au lieu d'un seul. Cette fonctionnalité est essentielle pour la création de VPNs clients [51].

- **Label extérieur :** Identifie le chemin vers le LSR destination, et change à chaque saut.
- **Label intérieur :** Spécifie le VPN-ID attribué au VPN et n'est pas modifié entre le LSR source et le LSR destination.

Figure III.12. *Labels MPLS*

III.6.1 Les différentes composantes des VPNs MPLS

Comme montre la figure III.14, les composantes des VPN sont [52] :

- **CE routeur (Customer Edge router) :** Est un routeur client qui est relié au backbone.
- **PE routeur (Provider Edge router) :** Est un routeur de périphérie qui est connecté à des CE. Au niveau des PE, il est possible de déclarer l'appartenance d'un CE à un VPN spécifique.
- **P (Provider) :** Le routeur central du réseau principal est responsable de la gestion des transferts de données entre les différents points du réseau.

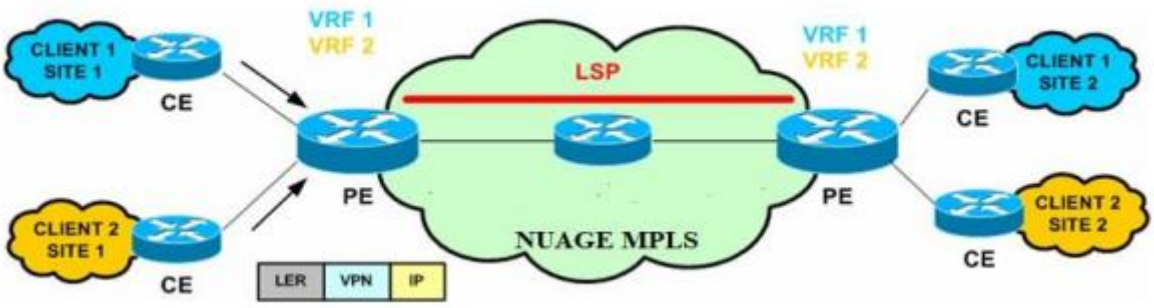

Figure III.13. *Un schéma général d'une architecture VPN [53]*

III.6.2 Gestion des VPNs

L'opérateur gère les VPN dans le backbone en utilisant les PE, comme illustré dans la Figure III.12. Chaque interface utilisateur est associée de manière statique à une VRF (Virtual Routing and Forwarding Table), également connue sous le nom de LIB dans la norme MPLS. La VRF est une table de routage qui est liée à un VPN et qui fournit des informations sur les routes vers les réseaux IP appartenant à ce VPN [52].

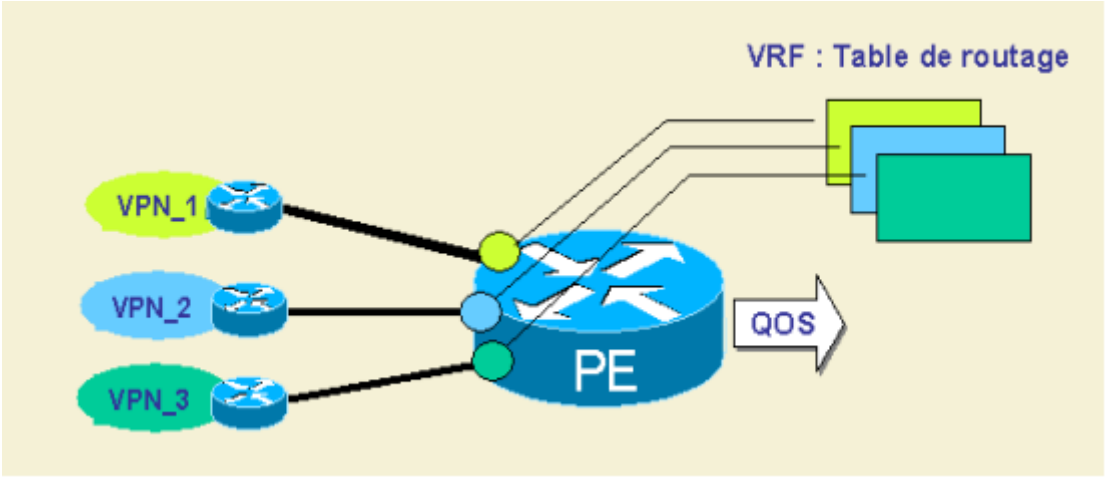

Figure III.14. *Gestion des VPNs par PE [53]*

III.6.3 Utilisation des VRF dans les VPN

Les réseaux virtuels sont caractérisés par [54] :

- Un routeur peut contenir plusieurs VRF.
- Assure la sécurité d'accès aux ressources.
- Chaque VRF dispose de sa propre table de routage.
- Permet la mise en place de VPNs.
- La connexion entre les ressources de VRFs s'établit par l'utilisation du BGP.
- Les VRF permettent de réutiliser l'espace d'adressage IP (Overlapping) entre des Domaines de routage isolés (le cas d'offrir la même adresse IP pour 2 clients Indépendants). Voir la figure III.15

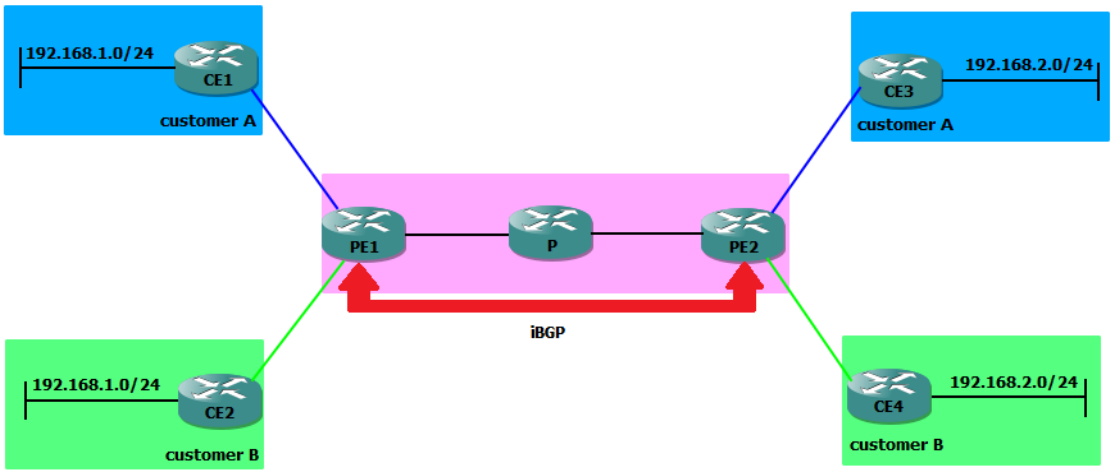

Figure III.15. *OverLapping*

III.6.4 L2VPN

Est une technologie qui permet de connecter des réseaux locaux (LAN) distants via un réseau étendu (WAN). Elle permet de créer un tunnel sécurisé entre deux sites distants, en utilisant des protocoles tels que MPLS, VPLS, LDP ou BGP pour acheminer les paquets de données.

Les L2VPN sont souvent utilisés pour connecter des succursales d'entreprise à leur siège social, pour fournir une connectivité entre les centres de données ou pour offrir des services VPN aux clients [42].

Le tunnel est utilisé pour transmettre de façon transparente les données utilisateur. Les tunnels couramment utilisés dans la technologie MPLS VPN sont :

- **Tunnel LSP (Label Switched Path)** : Est un chemin prédéfini dans le réseau MPLS qui permet d'acheminer les paquets de données d'un point à un autre par commutation d'étiquettes. Les tunnels LSP sont créés pour établir une connexion entre deux points d'un réseau et peuvent être utilisés pour transporter différents types de trafic, y compris les données L2VPN. Si les tunnels LSP sont adoptés l'en-tête de paquet IP est analysé uniquement sur le PE plutôt que d'être analysé sur chaque appareil par lequel un paquet VPN passe.
- **Tunnel MPLS TE (Traffic Engineering)** : Est un mécanisme qui permet d'améliorer l'utilisation des ressources du réseau MPLS en acheminant le trafic sur des chemins spécifiques au lieu de ceux par défaut. Les tunnels MPLS TE sont créés pour acheminer le trafic en fonction de critères tels que la bande passante, la qualité de service ou la redondance.
- **Tunnel GRE (Generic Routing Encapsulation)** : Est un protocole qui permet d'encapsuler des paquets IP dans d'autres paquets IP pour créer un tunnel virtuel entre deux points du réseau. Les tunnels GRE peuvent être utilisés pour transporter différents types de trafic, y compris les données L2VPN, et sont souvent utilisés dans les réseaux VPN pour créer des connexions sécurisées entre des sites distants.

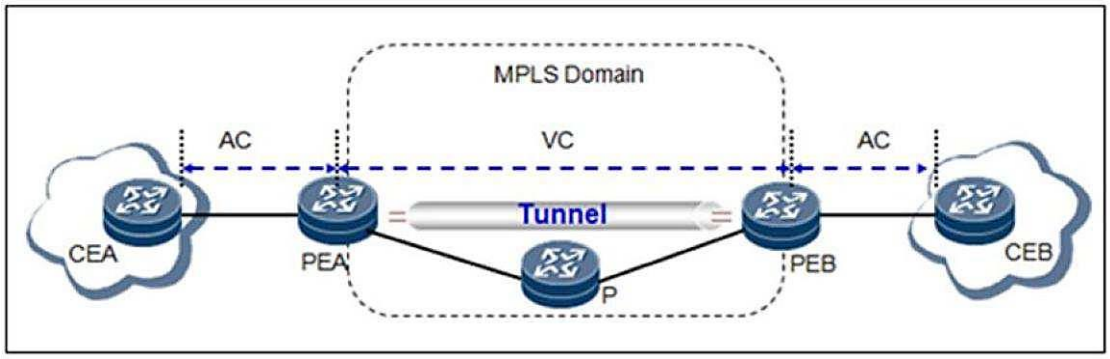

Figure III.16. *Architecture du MPLS L2VPN [44]*

- **VPWS (Virtual Private Wire Service)**

VPWS est un service de réseau privé virtuel qui permet de connecter deux sites distants via un réseau MPLS en émulant une liaison point à point. Cependant, plus de deux sites ne peuvent communiquer en même temps, au niveau du fournisseur de services. Les équipements des deux sites sont connectés à des PE (Provider Edge) différents qui se chargent d'acheminer les paquets entre eux en utilisant des labels MPLS [54].

VPWS est souvent utilisé pour connecter deux datacenters ou pour fournir une liaison WAN dédiée entre deux sites distants. Il offre une bande passante garantie et une qualité de service élevée, ainsi qu'une sécurité renforcée grâce à l'utilisation d'un tunnel VPN.

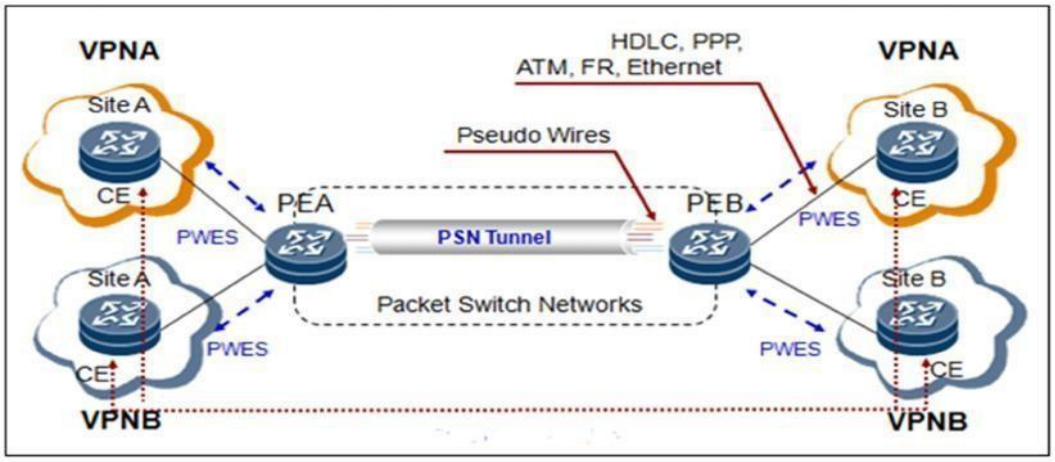

Figure III.17. *Fonctionnement d'un VPWS [44]*

- **VPLS (Virtual Private LAN Service)**

VPLS est également appelé service LAN transparent, contrairement à VPWS, il s'agit d'un service de réseau privé virtuel qui permet de connecter plusieurs sites distants via un réseau MPLS (Multiprotocol Label Switching) en simulant un seul LAN (Local Area Network). Les équipements de chaque site sont connectés à un fournisseur de périphérie PE (Provider Edge) qui est responsable du routage des paquets vers d'autres PE du réseau à l'aide d'étiquettes MPLS. Ainsi les sites peuvent communiquer entre eux comme s'ils étaient sur le même réseau local [55].

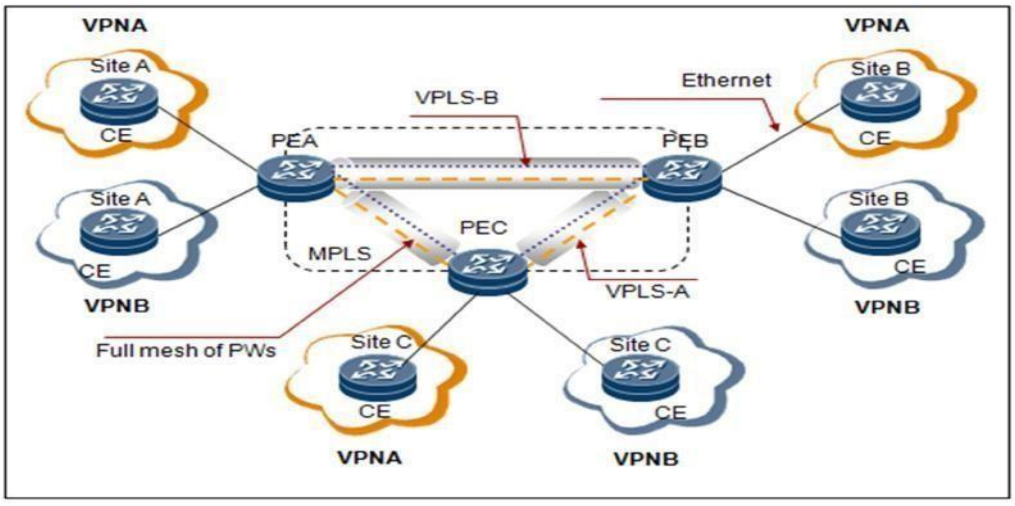

Figure III.18. *Fonctionnement d'un VPLS [44]*

III.6.5L3VPN

L3VPN est une technologie VPN couche 3 qui permet de créer des réseaux privés virtuels en utilisant le protocole MPLS [56]. Elle permet aux entreprises d'utiliser des protocoles de couche 3 tels que IP pour connecter des réseaux locaux (LAN) distants, tout en garantissant la sécurité et la qualité de service. Les L3VPN sont souvent utilisés pour fournir une connectivité sécurisée VPN à distance aux clients ou pour connecter des sites d'entreprise distants [57].

MPLS L3VPN se compose de routeur CE, routeur PE et de routeur P. PE et P sont situés dans les réseaux d'opérateurs.

Un réseau d'utilisateurs se compose de sites VPN dans différents emplacements géographiques. Chaque site VPN est connecté aux réseaux via un routeur CE et chaque CE est connecté à un PE via des liaisons simples ou doubles.

Les sites d'utilisateurs à différents emplacements sont généralement attribués à un VPN pour leur permettre de communiquer. Mais MPLS L3VPN permet aussi d'isoler un site ou au contraire d'allouer des accès mutuels entre plusieurs sites.

MPLS L3VPN offre une forte flexibilité d'isolation des utilisateurs pour répondre aux besoins de sécurité des services et la mise en réseau flexible.

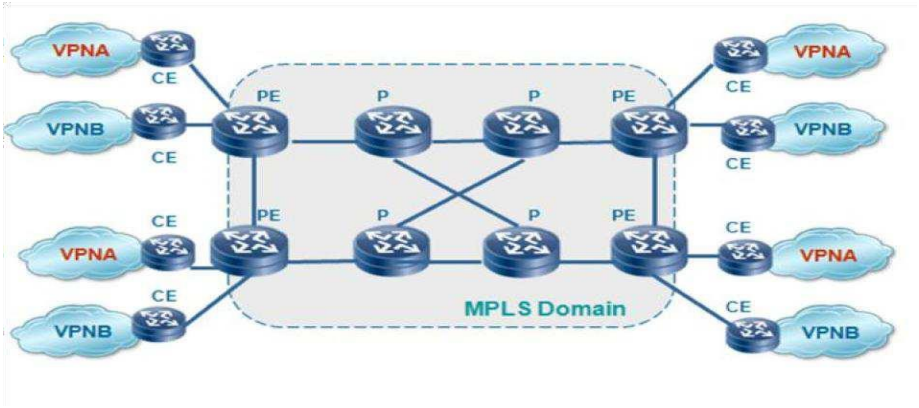

Figure III.19. *Architecture du MPLS L3VPN [44]*

III.6.5.1 VRF (Virtual Routing and Forwarding)

La notion même de VPN consiste à isoler le trafic entre des sites clients qui n'appartiennent pas aux mêmes VPN. Pour réaliser cette séparation, les routeurs PE ont la capacité de gérer plusieurs tables de routage grâce au concept de VRF (VPN Routing and Forwarding). Une VRF est constituée d'une table de routage spécifique, d'une table FIB, d'une table FEC indépendante des VRF et d'une table de routage. Chaque VRF est désignée par un

nom sur les routeurs PE. Les noms sont affectés localement, et n'ont aucune signification pour les autres routeurs. Chaque interface PE reliée à un site client est rattachée à une VRF particulière. Lors de la réception de paquets IP sur l'interface client, le routeur PE vérifie la table VRF à laquelle l'interface est connectée, et ne consulte donc pas sa table de routage globale. Cette possibilité d'utiliser plusieurs tables de routage indépendantes permet de gérer un plan d'adressage par site [58].

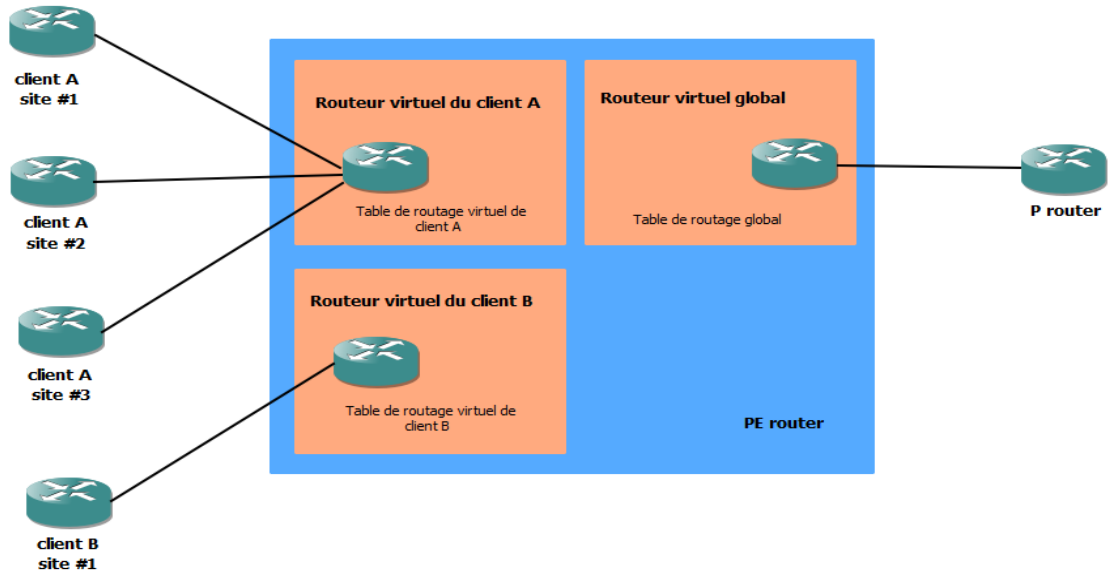

Figure III.20. *Utilisations des tables de routage virtuelles par le PE [44]*

III.6.5.2 MP-BGP (MultiProtocol-Border Gateway Protocol)

Le protocole MP-BGP est une extension du protocole BGP 4, permet l'échange de routes multicast et VPNv4. MP-BGP adopte une terminologie similaire à BGP concernant la symétrie :

- MP-iBGP : Entre routeurs d'un même AS.
- MP-eBGP : Entre routeurs situés dans 2 AS différents

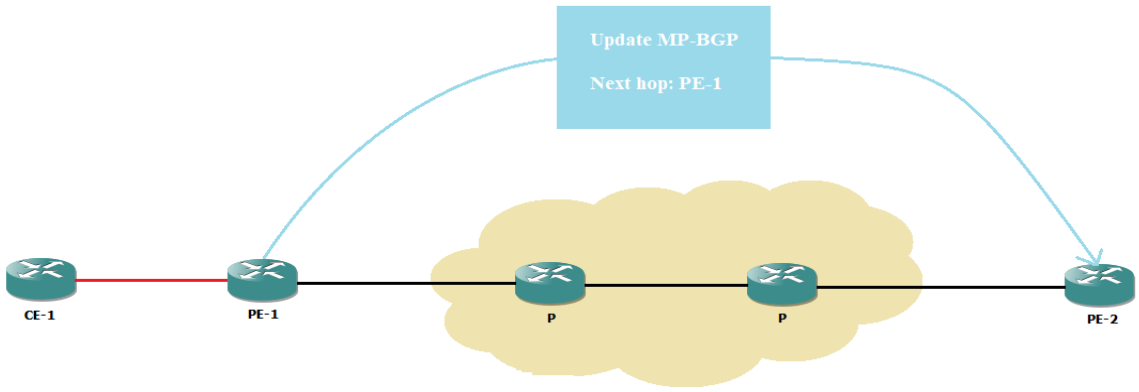

Figure III.21. *Updates MP-BGP*

III.6.5.3 RD (Route Distinguisher)

RD est un identifiant unique utilisé pour distinguer les routes VPN dans le réseau MPLS L3VPN. Il est ajouté au préfixe IP pour créer une adresse IP unique pour chaque route VPN [59].

Lors de la création d'une VRF sur un PE, un RD doit être configuré. Les routes apprises soit localement (routes statiques, Loopback sur le PE), soit par les CE rattachés au PE seront ainsi exportées dans les updates MP-BGP avec ce RD.

Grâce au RD, des sites appartenant à différents VPNs auront la possibilité d'utiliser les mêmes plans d'adressage. Ainsi, les routes échangées entre PE sont uniques au niveau des updates BGP. Cependant, il est recommandé de choisir un RD par VRF [60].

- **VPNv4**

Le routeur PE possède des informations de routage propre à chaque CE. Ces informations consistent en des adresses IPv4 qui seront converties en adresses VPNv4 en ajoutant RD. Si plusieurs VPNs utilisent la même adresse IPv4, PE la traduit en une seule adresse VPNv4.

VPNv4 est une adresse de 12 octets, commençant par un identificateur de route (Route Distinguisher) de 8 octets ajouté à chaque adresse de sous-réseau IPv4 (4 octets) d'un VRF donné [42].

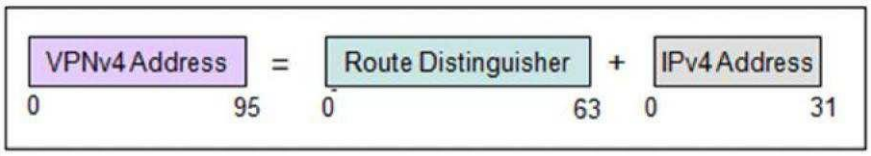

Figure III.22. *Adresse VPNv4*

III.6.5.4 RT (Route Target)

RT est un identifiant qui permet aux routeurs MPLS L3VPN d'identifier les routes VPN qui doivent être importées ou exportées à partir d'un VRF spécifique. Les RT sont utilisés pour contrôler la distribution des routes VPN entre différents VRF d'un même routeur [61].

Le RD permet de garantir l'unicité des routes VPNv4 échangées entre PE, mais ne définit pas la manière dont les routes vont être insérées dans les VRF des routeurs PE. Les RT (Route Target) qui est une communauté étendue de BGP (extended community), ne sont rien de plus que des sortes de filtres appliqués sur les routes VPNv4.

A chaque route VPNv4 est associé une ou plusieurs Export Route Target. L'egress PE utilise l'Import Route Target pour déterminer si la route reçue du ingress PE peut être placée dans le VRF.

L'Import Route Target est configuré dans chaque VRF. Si l'Import Route Target correspond à l'Export Route Target, la route est configurée dans le VRF.

III.6.6 Les types de MPLS L3VPN

Les types de MPLS L3VPN incluent [62] :

- **Layer 3 MPLS VPN** : permet la création de tunnels VPN entre les sites distants à l'aide de protocoles de routage tels que OSPF ou BGP.
- **MPLS Traffic Engineering (MPLS TE)** : permet la gestion du trafic sur un réseau MPLS à l'aide des tunnels LSP (Label Switched Path).
- **Carrier Supporting Carrier (CSC) :** permet aux fournisseurs de services de fournir des services VPN à leurs clients en utilisant un autre fournisseur de services comme opérateur (transporteur).

III.7 Conclusion

En conclusion, VPN et MPLS sont des outils essentiels pour les entreprises qui cherchent à améliorer la connectivité et la sécurité. Les VPN permettent aux entreprises de créer des connexions sécurisées entre les sites, tandis que le MPLS permet d'acheminer efficacement le trafic sur le WAN. En combinant ces technologies avec d'autres solutions de mise en réseau, les entreprises peuvent créer des réseaux performants et fiables qui répondent à leurs besoins spécifiques.

Ils offrent une solution puissante aux entreprises et aux particuliers qui ont besoin de communications fiables, sécurisées et efficaces.

Chapitre IV

Simulation sous GNS3

IV.1 Introduction

Ce chapitre présente une application pratique de l'implémentation de la ToIP sur une architecture MPLS VPN à l'aide du simulateur GNS3. Nous montrons comment configurer les équipements pour prendre en charge le trafic vocal et garantir une QoS adéquate, ainsi que comment tester notre configuration en effectuant des appels vocaux entre différents sites du VPN.

IV.2 Choix des outils de simulation

Il y a actuellement de nombreux logiciels de simulation réseau disponibles tel que GNS3, Cisco Packet Tracer, mais peu d'entre eux prennent en charge l'architecture MPLS. C'est pourquoi nous avons principalement choisi GNS3.

IV.2.1 Présentation du logiciel GNS3

GNS3 est un logiciel open-source de simulation de réseaux informatiques. Il permet aux utilisateurs de créer des topologies de réseau virtuelles en utilisant des images d'appareils réseau réels, tels que des routeurs, des commutateurs et des pares-feux. Les utilisateurs peuvent configurer ces appareils pour simuler différents scénarios de réseau et tester leur fonctionnement.

Figure IV.1. *Logo de GNS3*

IV.2.2 VMware Workstation

VMware Workstation permet aux utilisateurs de configurer des machines virtuelles (VM) sur une seule machine physique, et les utiliser simultanément avec la machine réelle. Chaque machine virtuelle peut exécuter son propre système d'exploitation, y compris les versions de Microsoft Windows, Linux, etc.

IV.2.3 Cisco IP Communicator

Cisco IP Communicator est une application Windows Softphone Windows qui vous permet d'utiliser votre ordinateur personnel pour effectuer des appels vocaux et vidéo haut de gamme. En offrant les dernières technologies de communication IP, il est facile d'acquérir, de déployer et d'utiliser.

IV.2.4 Serveur TFTP (Trivial File Transfer Protocol)

TFTP Server est un client TFTP gratuit qui permet d'envoyer et de recevoir plusieurs fichiers simultanément vers différents périphériques de réseau. Ainsi, TFTP Server est dédié aux administrateurs réseau souhaitant utiliser le protocole TFTP pour transférer de nouveaux firmwares vers leurs routeurs et leurs commutateurs réseau.

Est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP.

IV.2.5 Les plates-formes utilisées

- *Routeur Cisco 3745*

Le routeur Cisco 3745 est un routeur modulaire de la gamme Cisco 3700 Series. Il est conçu pour les réseaux d'entreprise et offre des fonctionnalités avancées telles que le routage IP, le routage basé sur les politiques, la sécurité intégrée, la qualité de service (QoS) et la prise en charge de nombreux protocoles de réseau.

Le C3745 dispose de plusieurs emplacements pour modules d'extension, ce qui permet aux utilisateurs de personnaliser les fonctionnalités du routeur en ajoutant des cartes d'interface réseau supplémentaires ou d'autres modules spécialisés tels que des modules de voix ou des modules VPN.

IV.3 Configuration et simulation

La figure IV.2 présente l'architecture que l'on a utilisée tout le long de ce chapitre.

Elle est composée de :

- 2 Routeurs représentant le CORE MPLS (P, P1) ;
- 2 Routeurs représentant l'Edge MPLS (PE, PE1) ;
- 4 Routeurs représentants les clients (cust-A, cust-A1, cust-B, cust-B1) ;
- 4 Switches Ethernet (Switch1, Switch2, Switch3, Switch4);
- 2 PC (PC1 et PC2)

- 5 IP Phones (IPPhone1, IPPhone2, IPPhone3, IPPhone4 et IPPhone5) ;

Nous avons choisi pour ce modèle les technologies suivantes :

- OSPF pour la communication dans le réseau MPLS ;
- Routage statique entre CE-PE ;
- MP-BGP pour le VPN.

Plan d'adressage :

Routeur	Interface	Adresse IP	Masque
CUST-A	F1/0	192.168.4.1	255.255.255.0
	F0/0	192.168.0.1	255.255.255.252
CUST-A1	F1/0	192.168.1.2	255.255.255.252
	F0/0	192.168.5.1	255.255.255.0
PE	F1/0	10.1.1.1	255.255.255.252
	F1/1	10.1.4.1	255.255.255.252
	Loopback0	1.1.1.1	255.255.255.255
PE1	F0/0	10.1.2.2	255.255.255.252
	F2/0	10.1.3.2	255.255.255.252
	Loopback0	3.3.3.3	255.255.255.255
P	F0/0	10.1.1.2	255.255.255.252
	F1/0	10.1.2.1	255.255.255.252
	Loopback0	2.2.2.2	255.255.255.255
P1	F0/0	10.1.3.1	255.255.255.252
	F1/0	10.1.4.2	255.255.255.252
	Loopback0	4.4.4.4	255.255.255.255
PC1	Vmnet3	192.168.4.3	255.255.255.0
PC2	Vmnet4	192.168.5.2	255.255.255.0

Tableau IV.1. *Plan d'adressage*

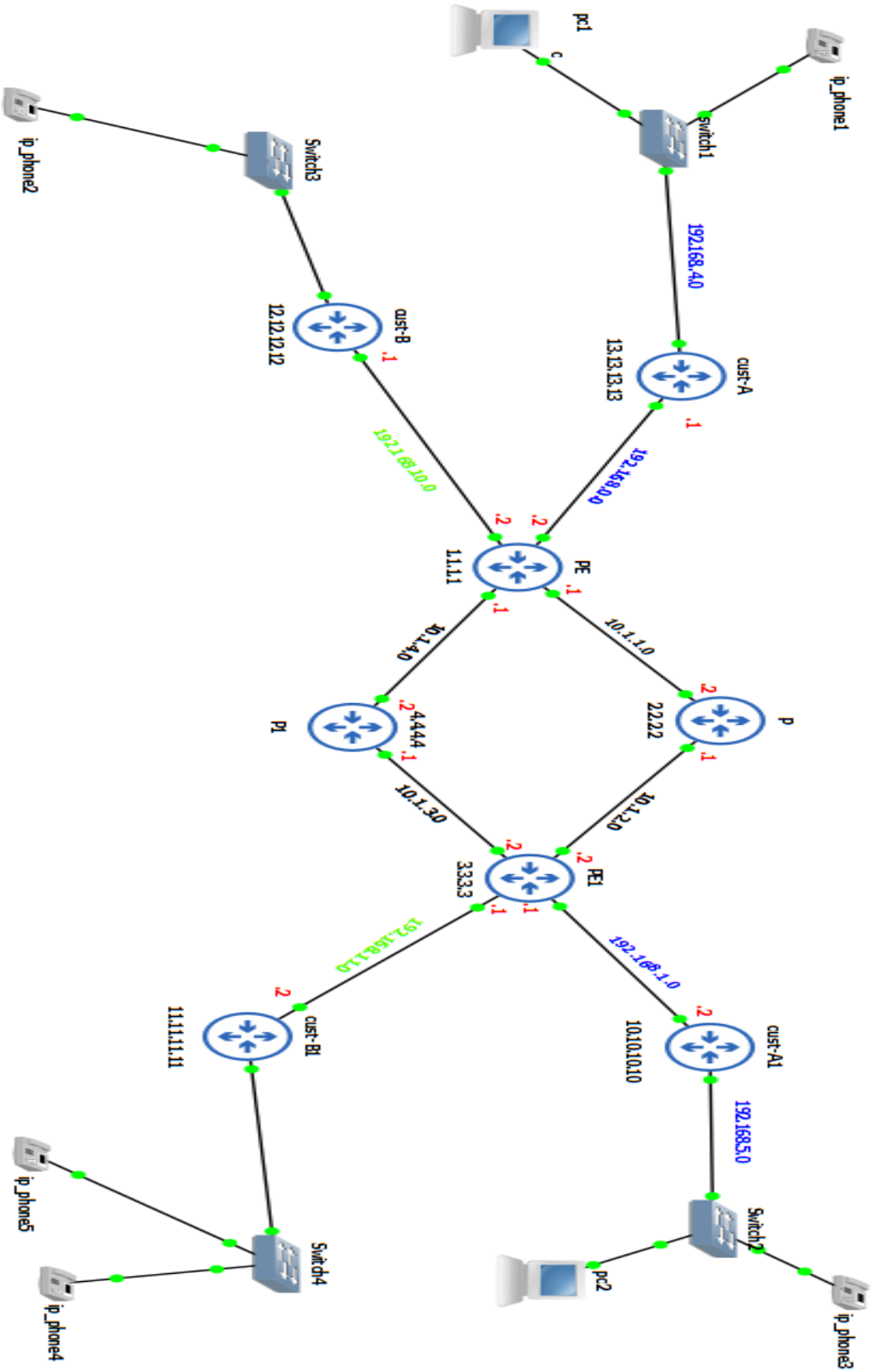

Figure IV.2. *Lab utilisé*

IV.3.1 Configuration de MPLS/VPN

IV.3.1.1 Configuration du protocole OSPF dans le réseau MPLS

On active le protocole OSPF sur les routeurs : **PE**, **P**, **P1**, **PE1.**

```
PE(config)#
PE(config)#router ospf 100
PE(config-router)#network 10.1.1.0 0.0.0.3 area 0
PE(config-router)#network 10.1.4.0 0.0.0.3 area 0
PE(config-router)#network 1.1.1.1 0.0.0.0 area 0
PE(config-router)#exit
PE(config)#
```

Figure IV.3. *Configuration OSPF sur le routeur PE*

Les étapes de configuration sont répétées sur les routeurs : **P**, **P1**, **PE1**.

Pour vérifier que le protocole OSPF est activé dans les routeurs : P, P1, PE et PE1, On utilise la commande **« show ip ospf neighbor ».**

```
PE(config)#
PE(config)#do show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           1   FULL/BDR        00:00:38    10.1.4.2        FastEthernet1/1
2.2.2.2           1   FULL/BDR        00:00:32    10.1.1.2        FastEthernet1/0
PE(config)#
PE(config)#
```

Figure IV.4. *OSPF est activé dans le routeur PE*

IV.3.1.2 Activation du MPLS

On active MPLS dans les interfaces qui relient les routeurs **PE**, **P**.

```
PE(config)#ip cef
PE(config)#
PE(config)#mpls label protocol ldp
PE(config)#mpls ldp ro
PE(config)#mpls ldp router-id loo
PE(config)#mpls ldp router-id loopback 0
PE(config)#int f1/0
PE(config-if)#mpls ip
PE(config-if)#int f1/1
PE(config-if)#mpls ip
PE(config-if)#ex
```

Figure IV.5. *Activation du MPLS sur le routeur PE*

Après le redémarrage des routeurs on vérifie les voisins LDP en tapant la commande **« show mpls ldp neighbor »**.

```
PE(config)#do show mpls ldp nei
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 2.2.2.2.42116 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 32/30; Downstream
        Up time: 00:17:22
        LDP discovery sources:
          FastEthernet1/0, Src IP addr: 10.1.1.2
        Addresses bound to peer LDP Ident:
          10.1.1.2        10.1.2.1        2.2.2.2
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 4.4.4.4.48327 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 32/29; Downstream
        Up time: 00:16:32
        LDP discovery sources:
          FastEthernet1/1, Src IP addr: 10.1.4.2
        Addresses bound to peer LDP Ident:
          10.1.3.1        10.1.4.2        4.4.4.4
```

Figure IV.6. *L'activation de MPLS sur le routeur PE est vérifiée*

IV.3.1.3 Configuration de MP-BGP sur les routeurs PE et PE1

On configure **MP-BGP** sur les routeurs **PE** et **PE1** en utilisant la commande **"neighbor** <adresse IP> remote-as <numéro d'AS>".

D'où on va mettre l'adresse de loopback au lieu de l'adresse de l'interface ce qui permet d'assurer que la communication entre les différents routeurs se fait au maniéré efficace et fiable.

```
PE(config)#router bgp 100
PE(config-router)#neighbor 3.3.3.3 remote-as 100
PE(config-router)#neighbor 3.3.3.3 update-source loopback 0
PE(config-router)#
```

Figure IV.7. *Configuration MP-BGP sur le routeur PE*

Les étapes de configuration sont répétées sur le routeur **PE1**.

Pour vérifier que les routeurs **PE** et **PE1** sont connectés en tant que voisine via le protocole BGP, la commande **« show ip bgp neighbor »** a été exécutée.

```
PE#show ip bgp nei
BGP neighbor is 3.3.3.3,  remote AS 100, internal link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
```

Figure IV.8. *PE et PE1 sont des routeurs voisins par protocole BGP*

IV.3.1.4 Création des VRF sur les interfaces des routeurs PE et PE1

Les adresses IP que nous avons assignées aux interfaces physiques seront fournies en les incluant dans le VRF.

On va implémenter le routage statique dans le VRF.

```
PE(config)#ip vrf cust-A
PE(config-vrf)#rd 100:50
PE(config-vrf)#route-t
PE(config-vrf)#route-target import 100:50
PE(config-vrf)#route-target export 100:50
PE(config-vrf)#exit
PE(config)#int f0/0
PE(config-if)#ip vrf forwarding cust-A
% Interface FastEthernet0/0 IPv4 disabled and address(es) removed due to enabling
VRF cust-A
PE(config-if)#ip add 192.168.0.2 255.255.255.252
PE(config-if)#no sh
PE(config-if)#ex
PE(config)#ip route vrf cust-A 13.13.13.13 255.255.255.255 192.168.0.1
PE(config)#
```

Figure IV.9. *Configuration VRF sur le routeur PE*

Les étapes de configuration sont répétées sur le routeur **PE1**.

IV.3.1.5 Distribution des routes

```
PE(config)#router bgp 100
PE(config-router)#address-family vpnv4
PE(config-router-af)#nei 3.3.3.3 activate
PE(config-router-af)#exit
PE(config-router)#address-family ipv4 vrf cust-A
PE(config-router-af)#redistribute connected
PE(config-router-af)#redistribute static
PE(config-router-af)#exit
```

Figure IV.10. *Configuration de la redistribution de route sur le routeur PE*

IV.3.1.6 Test et confirmation

Pour vérifier la connectivité entre les clients (**cust-A** et **cust-A1**), on va tester le ping.

```
cust-A#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 600/796/864 ms
cust-A#
```

Figure IV.11. *Ping du cust-A vers cust-A1*

```
cust-A1#ping 13.13.13.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 13.13.13.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 504/678/800 ms
cust-A1#
```

Figure IV.12. *Ping du cust-A1 vers cust-A*

On remarque bien selon la **Figure IV.11** et la **Figure IV.12** que MPLS/VPN fonctionne.

IV.3.2 Configuration de la ToIP

IV.3.2.1 Activation du serveur DHCP

Le DHCP (Dynamic Host Configuration Protocol) est un protocole qui permet aux téléphones IP d'obtenir automatiquement une adresse IP.

Pour activer le service **DHCP** sur les routeurs **cust-A, cust-A1**, **cust-B** et **cust-B1**, il faut utiliser la commande **« ip dhcp pool »** suivie du nom du pool de **DHCP** que l'on souhaite créer, on a choisi le nom **« voice ».**

Ensuite, on va définir toutes les adresses réseau que l'on souhaite attribuer aux clients **DHCP** en utilisant la commande **« network »** suivie de l'adresse réseau correspondante. Il est également possible de configurer des options **DHCP** supplémentaires telle que le **DNS** en utilisant la commande **« dns-server ».**

```
cust-A(config)#ip dhcp pool voice
cust-A(dhcp-config)#network 192.168.4.0
cust-A(dhcp-config)#default-router 192.168.4.1
cust-A(dhcp-config)#dn
cust-A(dhcp-config)#dns-server 192.168.4.1
cust-A(dhcp-config)#exit
```

Figure IV.13. *Configuration du serveur DHCP sur le routeur cust-A*

Les étapes de configuration sont répétées sur les routeurs **cust-A1**, **cust-B** et **cust-B1**.

IV.3.2.2 Activation du gestionnaire de communication VoIP (Call Manager Express)

Nous allons indiquer le nombre maximum des ephones qui peuvent être spécifiés dans le réseau et le nombre maximum de ephone-dn qui peuvent être définit dans le système.

```
cust-A(config)#telephony-service
cust-A(config-telephony)#max-dn 2
cust-A(config-telephony)#max-ephones 2
cust-A(config-telephony)#system message ToIP over MPLS VPN
cust-A(config-telephony)#auto assign 1 to 2
cust-A(config-telephony)#ip source-address 192.168.4.1 port 2000
%Error deleting flash:SEPDEFAULT.cnf (File not found)
%Error deleting flash:XMLDefault.cnf.xml (File not found)
cust-A(config-telephony)#exit
```

Figure IV.14. *Activation du gestionnaire de communication VoIP sur le routeur client*

Les étapes de configuration sont répétées sur les routeurs **cust-A1**, **cust-B** et **cust-B1**.

IV.3.2.3 Création des lignes et affectation aux téléphones IP

Pour créer une ligne, il faut définir le numéro, le nom et les paramètres avancés tels que la qualité audio ou la redirection d'appel en cas d'absence.

```
cust-A(config)#ephone-dn 1
cust-A(config-ephone-dn)#
*Mar  1 01:13:02.731: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state t
o up
cust-A(config-ephone-dn)#number 100
cust-A(config-ephone-dn)#name imene
cust-A(config-ephone-dn)#label imene-btc
cust-A(config-ephone-dn)#exit
```

Figure IV.15. *Création des lignes et affectation aux téléphones IP sur le routeur cust-A*

Les étapes de configuration sont répétées sur les routeurs cust-A1, cust-B et cust-B1.

On remarque que les informations attribuées dans la configuration sont réellement affichées sur les 2 téléphones IP.

Figure IV.16. *Deux téléphones IP configurés*

Il s'impose de configurer les routeurs clients pour qu'ils puissent identifier les numéros d'appels en passant par le réseau MPLS/VPN.

```
cust-A(config)#dial-peer voice 1 voip
cust-A(config-dial-peer)#destination-pattern 200
cust-A(config-dial-peer)#session protocol sipv2
cust-A(config-dial-peer)#session target ipv4:192.168.1.2
cust-A(config-dial-peer)#exit
cust-A(config)#
```

Figure IV.17. *Identification les numéros d'appels d'ip phone 3 sur le router cust-A*

IV.3.2.4 Test et confirmation

Une fois que les téléphones IP sont configurés, il est important de tester leur fonctionnement, en lançant un appel depuis ip_phone 1 (Imene-btc) vers ip_phone 3 (lilya-zd).

Figure IV.18. *Illustration du lancement d'appel du ip_phone 1 vers ip_phone 3*

On remarque que l'ip_phone 3 (lilya-zd) sonne.

Figure IV.19. *Illustration de la réussite d'établissement de l'appel*

La communication est opérationnelle aussitôt que ip phone 3 (lilya-zd) décroche l'appel.

IV.4 Conclusion

En conclusion, la mise en place de la ToIP sur une architecture MPLS VPN est une étape importante pour les entreprises qui cherchent à améliorer leur communication interne et externe. Grâce à l'utilisation de GNS3, nous avons pu simuler cette configuration et tester avec succès les appels VoIP. Cela démontre l'efficacité de cette solution pour améliorer la qualité des communications tout en réduisant les coûts liés aux appels téléphoniques traditionnels. En somme, la ToIP sur une architecture MPLS VPN est un choix judicieux pour les entreprises souhaitant optimiser leur communication et leur productivité.

Conclusion Générale

Conclusion générale

Après avoir étudié en détail le thème de notre projet de fin d'études « Implémentation de la ToIP sur une architecture MPLS/VPN », nous pouvons conclure que cette solution est très bénéfique pour les entreprises qui cherchent à améliorer leur communication interne et externe.

Nous avons réalisé une simulation sous GNS3 pour mettre en pratique nos connaissances théoriques.

En conclusion, l'implémentation de la ToIP sur une architecture MPLS/VPN nécessite une expertise dans plusieurs domaines tels que la téléphonie classique, les réseaux IP, les réseaux MPLS/VPN, la sécurité et la mobilité. Il est donc important pour l'entreprise de choisir une solution pertinente et cohérente en ayant une bonne connaissance du monde des opérateurs. Cela nécessite une planification minutieuse et une expertise technique pour garantir le succès du projet.

Nous pensons également que notre travail peut être un bon repère et un référentiel pour tout autre projet visant à approfondir et déployer différents outils pour les environnements MPLS.

Le développement d'un tel projet n'est jamais totalement achevé et certaines idées n'ont pas pu être réalisées en raison des contraintes de temps et des moyens. Comme perspectives de notre travail, nous proposons :

- Installez Cisco Unified Video Advantage pour transférer des images et des vidéos, car nous n'avons pas pu le télécharger en raison de son coût élevé et de la nécessité d'une carte de débit ou d'un contrat de travail avec CISCO pour l'acheter.
- Utiliser Cisco Unified Call Manager qui est une version améliorée de CME avec des avantages tels que la sécurité et la prise en charge plus de numéros de téléphone

Références bibliographiques

Références bibliographiques

[1] Collectif cisco, **«** Cisco networking academy program: CCNA 1 and 2 companion guide », 3rd edition, 2005, ISBN 1-58713-150-1.

[2] « Difference Between Static and Dynamic Routing », site web : https://techdifferences.com/ (consulté le 12/02/2023).

[3] Claude Servin, « Réseaux et Télécoms », Préface de Jean-Pierre Arnaud, Livre -2003- Edition Dunod.

[4] Cisco press, « Routing TCP/IP », 2nd edition, 2006, ISBN-10: 1-58705-202-4.

[5] Cisco, CCNA, routage, table-routage-cisco-ios. Site web : https://cisco.goffinet.org/ (consulté le 15/02/2023)

[6] Cours Cisco, CCNA, synthèse sur les protocoles de routage dynamique, classification des protocoles de routage. Site web : https://cisco.goffinet.org/ (consulté le 15/02/2023)

[7] Nouali.K Moumou.D, « Mise en place d'une solution ToIP sous le réseau Intranet d'Algérie Télécom », Université Mouloud Mammeri De Tizi-Ouzou, 2017/2018.

[8] Vacamps Andrés, « Cisco protocoles, concept de routage et sécurité », 2011, 2ième module de préparation aux certifications, ISBN 2746056755.

[9] BOUABID Amel « Choix d'un protocole de routage dynamique dans un réseau d'entreprise : Cas de CEVITAL. », Université Abderrahmane Mira de Béjaïa, 2012/2013

[10] « IGP Versus EGP Routing Protocols » site web : https://www.researchgate.net/ (consulté le 16/02/2023)

[11] Protocoles de routage dynamique « Types de protocoles de routage », sur le site « https://formip.com », (consulté le 16/02/2023).

[12] « Quelle est la différence entre RIP et OSPF ? ». site web : https://community.fs.com/ (consulté le 16/02/2023)

[13] « Introduction à OSPF ». site web : https://reussirsonccna.fr/ (consulté le 17/02/2023)

[14] « About PEERING - The BGP Testbed ». Site web : https://peering.usc.edu/ (consulté le 16/02/2023)

[15] Y. Rekhter, T.LI S. Hares, « **RFC 4271: A Border Getway Protocol 4** », 2006.

[17] Bachiri soumia, belarbi baraka, « déploiement d'une application de TOIP », Université Abou Bakr Belkaid– Tlemcen,2015, p11.

[18] Ahmed Aouadi « Mise en place d'une solution open Source VoIP et Visioconférence multi-sites sécurisée », Université virtuelle de tunis, 2014/2015

[19] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[20] Ressources de formation sur la téléphonie sur IP ToIP avec exemple pratique - Cours Divers. Site web : https://www.cours-gratuit.com/ (consulté le 15/03/2023)

[21] Evariste Wababusho, « Etude et conception d'un système de communication ToIP au sein de l'OCC/Bukavu », Université libre des grands lacs/ULPGL Goma - Licence 2019, p24.

[22] Patrick.C, Laurent.G et Angel.A, « Une plateforme pédagogique pour illustrer les différentes architectures de ToIP », IUT 2010.

[23] Abdellaoui.M, Benahmou.A, « Application mobile de la voIP sur un réseau Wifi » - Université Abdou Bekr Belkaid- Tlemcen -2014.

[24] Mezhoudi.Y, « Voix sur IP sécurisée », Université Mohamed Khider de biskra, 2017.

[25] Soulemanou Nsangou Moungnutou « Etude d'une offre technique innovante de téléphonie sur IP à Camtel Cameroun », Université de Maroua Cameroun – 2012.

[26] Hamani saïd, « étude et simulation d'un réseau de téléphonie sur IP (TOIP) », Université M'Hamed Bougara-Boumerdes,2019

[27] « VoIP Protocols: SIP and H323 ». Site web : https://www.ciscopress.com/ (Consulté le 20/03/2023)

[28] « Le TOIP, Téléphonie Sur IP. » Futura-Sciences. Site web : https://www.futura-sciences.com/ (Consulté le 20/03/2023)

[29] « Quality of Service for Voice over IP - Cisco ». Site web : https://www.cisco.com (consulté le 21/03/2023)

[30] D. Grossman, « RFC 3260 : New Terminology and Clarifications for Diffserv », 1998.

[31] R. Braden, « RFC 2205 : Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification », 1997.

[32] E. Rosen, « RFC 3031 : Multiprotocol Label Switching Architecture », 2001.

[33] S. BELLALI, « Conception et déploiement d'une solution SDN au sein d'un réseau IP/MPLS », université USTHB, 2016.

[34] Mohand Yazid SAIDI « Méthodes de contrôle distribué du placement de LSP de secours pour la protection des communications unicast et multicast dans un réseau MPLS », Université de Rennes 1- 2008.

[35] Frédéric Launay « Principe du SDN dans une architecture réseau classique », Université de poitiers, 2018.

[36] M. Théodore Gildas ZINKPE, « Gestion du trafic d'un réseau d'entreprise par le MPLS : Cas du Ministère de l'Economie et des Finances » école Polytechnique d'Abomey-Calavi, 2010 – 2011.

[37] Ould Lamara.S, Takilt.M, « Implémentation du SDN dans une structure IP/MPLS » Université Mouloud Mammeri Tizi-Ouzou,2017-2018.

[38] Randa B. « Etude et simulation d'un réseau IP-MPLS sous GNS3 » Université Mouloud Mammeri.2018.

[39] MEGRI Hmanou, SALHI Noureddine « Etude, Conception et Évaluation d'une Architecture MPLS/VPN Désignée pour une Infrastructure Opérateur » Université A. MIRA, 2014/2015.

[40] Ravoavahy.A « Analyse de performance de la VoIP sur un backbone MPLS avec traffic engeneering », université Antananarivo,06 août 2014.

[41] AMINE.A « Mise en œuvre d'un cœur de réseau IP/MPLS », université de Bechar 2011.

[42] Mokhtari.A Bessam.W, « Implémentation de la VoIP sur une architecture MPLS/VPN », université Belhadj Bouchaib, 2020/2021.

[43] Ould Lamara.S, Takilt.M, « Implémentation du SDN dans une structure IP/MPLS » Université Mouloud Mammeri Tizi-Ouzou,2017-2018.

[44] Zerrouki.H, Adjabi.M, « Utilisation de la technologie MPLS dans le réseau 4G », Université ziane achour de djelfa, : 2018-2019.

[45] zhushigeng (Vinsoney), « Processing of MPLS Labels » 2019. Site web : https://forum.huawei.com (consulté le 14/04/2023)

[46] « Processing of MPLS Labels » site web: https://forum.huawei.com (consulté le 15/04/2023)

[47] Jean-Marie BONNIN. « Protocole LDP » (Site web : https://www.techniquesingenieur.fr/) Consulté le 14/04/2023

[48] Cisco, « MPLS Basics », site web : https://www.cisco.com/ (Consulté le 10/04/2023)

[49] Juniper Networks, « MPLS Overview », site web : https://www.juniper.net/ (consulté le 11/04/2023)

[50] E. Rosen, « RFC 3031 : Multiprotocol Label Switching Architecture », 2001.

[51] « Introduction to Cisco MPLS VPN », site web : https://www.cisco.com/ (consulté le 18/04/2023).

[52] « Multi Protocol Label Switching ». site web : https://igm.univ-mlv.fr/ (consulté le 15/04/ 2023).

[53] Ghislain SOH TCHENDJOU, « Conception et mise en place d'une architecture VPN/MPLS avec gestion de la GOS. Cas de Matrix Télecoms », Université de Maroua Institut Supérieur du Sahel, 2015.

[54] « Juniper Networks : Understanding VPWS and VPLS VPNs ». site web : https://www.juniper.net/ (consulté le 16/04/2023)

[55] « Cisco : What is VPLS ? ». site web : https://www.cisco.com/ (consulté le 16/04/2023)

[56] I. Pepelnjak, J. Guichard et J. Apcar, « MPLS and VPN Architectures », 2001, ISBN 1587050021.

[57] K. Reddy, « Building MPLS-Based Broadband Access VPNs », 2005, ISBN 1587051362.

[58] FILLOT, Christophe. « Cour MPLS », Université de technologies Compiègne, 2013.

[59] « Understanding MPLS VPNs, Part I : Introduction to MPLS VPNs ». site web : https://www.cisco.com/ (consulté le 23/04/2023)

[60] David Sunny, « MPLS L2VPN/L3VPN », Huawei technologies co. 2009.

[61] « Understanding MPLS VPNs, Part II : Route Target Distribution ». site web : https://www.cisco.com/ (consulté le 24/04/2023)

[62] E. Rosen, « RFC 4364 : BGP/MPLS IP Virtual Private Networks (VPNs) », 2006.