الجمهورية الجزائرية الديمقراطية الشعبيـة
République algérienne démocratique et populaire
وزارة التـعليـم العالـي والبحـث العلمـــي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة عين تموشنت بلحاج بوشعيب
Université –Ain Temouchent- Belhadj Bouchaib
Faculté des Sciences et de Technologie
Département Génie Electrique

Projet de Fin d'Etudes
Pour l'obtention du diplôme de Master en :
Domaine : Sciences et Technologie
Filière : Télécommunications
Spécialité : Réseaux et Télécommunications
Thème

Implémentation de la VoIP sur une architecture MPLS/VPN

Présenté Par :
1) Mr Mokhtari Abdelghani Issam Eddine
2) Mr Bessam Wassim Ibrahim

Devant le jury composé de :

Dr BENCHERIF Kaddour	MCA	UAT.B.B (Ain Temouchent)	Président
Dr DEBBAL Mohammed	MCA	UAT.B.B (Ain Temouchent)	Examinateur
Dr SLIMANE Zohra	MCA	UAT.B.B (Ain Temouchent)	Encadrante

Année Universitaire 2020/2021

Remerciements

Nous adressons en premier lieu notre éternelle reconnaissance à ALLAH le tout puissant, pour nous avoir guidé vers le droit chemin, et nous avoir permis d'en arriver là, sans lui rien n'aurait été possible.

Un grand merci à nos parents qui nous ont toujours soutenu et encouragé. Ils illustrent notre plus grande source d'inspiration.

Nos profonds remercîments notre maitre de mémoire Mdm. SLIMANE Zohra, pour le soutien qu'elle nous a apporté et la confiance accordé tout au long de la rédaction de ce mémoire.

Nous tenons à remercier les membres du jury,
Dr BENCHERIF Kaddour, Dr DEBBAL Mohammed,
Dr SLIMANE Zohra
De nous honorer de leurs présence d'avoir accepté d'examiner et d'évaluer notre mémoire.

Enfin nos remercîments vont à toutes les personnes qui ont pu participer de près ou de loin à notre aide et encouragement.

Dédicace

C'est avec le cœur rempli d'émotions de tout un parcoure vécu et un combat d'une vie que je dédie ce mémoire :

***À mes parents** à qui je dois la vie et tout ce que j'ai entrepris, leurs présence et dévouement sans relâche aux quotidiens, spécialement à ma mère l'être le plus admirable, l'exemple de la réussite et la persévérance la seule et l'unique femme qui a fait de moi un homme, je remercie le dieu tout puissant de m'avoir fait le cadeau d'une mère pareil je te serai éternellement redevable pour tes sacrifices, ton amour, ta bienveillance ton assistance, merci du fond du cœur de m'avoir toujours poussé vers le haut quand je demeurais au plus bas, merci pour tes encouragements , de ta motivation, tes conseils qui sont en or de m'avoir transmis ta sagesse et appris les leçons de la vie.*

Merci de m'accompagner, de veiller sur moi et d'avoir cru en moi, tout le mérite te revient, ma réussite je te la doit. Puisse le tout puissant te garder pour moi, santé et longe vie heureuse

***À mon grand-père paix à ton âme. MR MEGHACHOU ABDELAZIZ**, tu étais mon mentor, depuis tout petit tu misais toutes tes espérances sur moi, tu m'as toujours ouvert les yeux et poussé à donner la meilleure image de moi. Tes encouragements et ton épaulement, je suis fière d'être ton petit fils, je te serai éternellement reconnaissant pour ma réussite, que dieu t'apporte la paix et t'accueille dans son vaste paradis*

***À ma sœur** (Rania) pour sa présence, sa gentillesse et sa bienveillance, merci de m'avoir soutenu durant toute ma période estudiantine, d'être de*

bons conseils et de savoir me remonter le moral, pour ton amour et ta maturité, je suis fière de toi, merci infiniment de ton dévouement que dieu te garde pour moi

À tous mes amis et mes porches (morad) *d'une manière ou d'une autre tu as su impacter ma vie à jamais, dans la meilleure direction, merci pour ta bonté et ta clémence de m'avoir permis de réaliser mes souhaits, et accordé ta confiance, c'est grâce à toi si je suis arrivé là où j'en suis, je te dois ma réussite, merci du fond du cœur*

À (Rafik sayah) *merci infiniment d'avoir était la quand j'en avais besoin de, m'avoir fourni de l'aide. Je t'en suis reconnaissant pour ta générosité, tes précieux conseils en tant qu'amis et instituteur, tu as participé à ma réussite, permet moi de t'exprimer toute ma gratitude cher frère*

À (chahrazed yakhou) *je t'en suis redevable pour l'aide et l'effort fournie matin et soir, tu as*
participé et influencé énormément sur l'avancement de mon travail, merci pour tous tes conseils
bien orientés, je suis reconnaissant d'avoir croisé ton chemin, ton dévouement restera précieux que
je ne reséquerai pas d'oublier.

Une dédicace particulaire à mon binôme (mokhtari abdelghani) : *durant ce temps de préparation de mémoire, cette période a été riche en émotions pour moi, des hauts et des bas, j'ai beaucoup appris de toi, merci pour ton fairplay, t'a sincérité, ta compréhension, t'a générosité et la personne que tu es, merci d'avoir partagé avec moi tes effort cher ami. J'ai été ravi de travailler avec toi et je te souhaite le meilleur pour ton avenir.*

Wassim

Dédicace

Je dédie ce modeste travail :

A mes parents, mes estimes pour eux sont immenses, je vous remercie pour tout ce que vous avez fait pour moi.
Nul mot ne pourra exprimer mes sentiments et ma recevabilité envers vous,
Que dieu vous préserve une longue vie heureuse.
A mes chers frères Bounouar , Mokhtar, et Akram
A mon binôme Wassim
A tous mes amis
A Toute ma famille, Tous ceux que j'aime, qui m'aiment et me comblez de conseils
A tous ceux qui, un jour, ont pensé à moi, les plus beaux mots ne sauraient exprimer ma gratitude.

Abdelghani

Résumé :

La concentration des réseaux de communication basés sur IP ainsi que l'émergence du regroupement de la voix et de l'image a favorisé cette tendance. Dans ce contexte, VoIP occupe une place de plus en plus primordiale, et maintenant, c'est devenu un challenge intéressant pour le développement de la communication.

Les fournisseurs de services de voix sur IP (VoIP) mettent en œuvre différents protocoles dans leurs réseaux centraux qui doivent se coordonner pour fournir, prendre en charge et offrir des services vocaux aux clients finaux, tout ceci imposent de fournir une qualité de service irréprochable pour assurer le bon fonctionnement d'une architecture réseau, d'où l'utilité du protocole MPLS.

Notre travail consiste à déployer une plateforme VoIP sur une architecture MPLS /VPN de façon à mettre en place ce protocole afin d'optimiser la qualité de service et apporter la fiabilité.

On a mis en œuvre un site local nommé Agence 1 est également autorisé à fournir des services aux utilisateurs sur des sites distants Appelés Agence 2, l'ensemble forme un réseau WAN.

Après avoir implémenté la plate-forme matérielle sous GNS3 et Vmware, la solution

Déployée compte sur le Call Manager Express qui est basé sur Cisco (CME), choix manipulé par la disponibilité du matériel qui offre la possibilité de réaliser une œuvre expérimentale dans des situations concrètes.

Des tests d'appel entre deux utilisateurs situés respectivement dans le site Agence 1 et Agence 2 ont été effectués avec succès.

Mots clés :

Internet protocol, VoIP, réseau WAN, CME, protocole GNS3, Vmaware

Abstract:

The concentration of communication networks based on IP as well as the emergence of the combination of voice and image has favored this trend. In this context, VoIP (Voice over Internet Protocol) is becoming more and more important, and now it has become an interesting challenge for the development of communication.

Voice over Internet Protocol (VoIP) service providers implement different protocols in their core networks that must coordinate to provide, support and deliver voice services to end customers, all of this imposes to provide an impeccable quality of service to ensure the proper functioning of a network architecture, hence the usefulness of MPLS protocol.

Our work consists in deploying a VoIP platform on an MPLS/VPN architecture in order to implement this protocol to optimize the quality of service and provide reliability.

We implemented a local site named Agency 1 is also allowed to provide services to users on remote sites called Agency 2, the whole forms a WAN network.

After implementing the hardware platform under GNS3 and Vmware, the solution

Deployed relies on the Call Manager Express which is based on Cisco (CME), a choice manipulated by the availability of the hardware that offers the possibility to realize an experimental work in concrete situations.

Tests of call between two users located respectively in the site Agency 1 and Agency 2 have been carried out successfully.

Key words :

Internet protocol , VoIP, WAN network, CME, GNS3 protocol, Vmaware

ملخص

أدى تركيز شبكات الاتصال القائمة على بروتوكول الإنترنت وكذلك ظهور إعادة تجميع الصوت والصورة إلى تعزيز هذا الاتجاه. في هذا السياق، يحتل VoIP مكانًا أساسيًا بشكل متزايد، والآن، أصبح تحديًا مثيرًا للاهتمام لتطوير الاتصالات.

يقوم مقدمو خدمات نقل الصوت عبر بروتوكول الإنترنت (VoIP) بتنفيذ بروتوكولات مختلفة في شبكاتهم الأساسية والتي يجب أن تنسق لتوفير الخدمات الصوتية ودعمها وتقديمها للعملاء النهائيين، كل هذا يتطلب توفير جودة خدمة لا يمكن تعويضها لضمان حسن سير بنية الشبكة، وبالتالي فائدة بروتوكول MPLS

يتكون عملنا من نشر منصة VoIP على بنية MPLS / VPN من أجل تنفيذ هذا البروتوكول من أجل تحسين جودة الخدمة وتوفير الموثوقية.

قمنا بتنفيذ موقع محلي يسمى Agency 1 مخوّل أيضًا بتقديم خدمات للمستخدمين في المواقع البعيدة Called Agency 2 ، وكلها تشكل شبكة WAN.

بعد تنفيذ النظام الأساسي للأجهزة ضمن GNS3 و Vmware ، الحل

يعتمد النشر على Call Manager Express الذي يعتمد على Cisco (CME) ، وهو خيار يتم التلاعب به من خلال توفر المعدات التي توفر إمكانية تنفيذ عمل تجريبي في مواقف ملموسة.

تم إجراء اختبارات الاتصال بين مستخدمين موجودين على التوالي في موقعي الوكالة 1 والوكالة 2 بنجاح.

الكلمات الدالة:

بروتوكول الإنترنت، VoIP ، شبكة WAN، CME ، بروتوكول GNS3، Vmaware

Acronymes

A

ADSL = Asymmetric digital subscriber link

ARP = Address Resolution Protocol

B

BGP = Border Gateway Protocol

D

DSCP = Differenciated Code Point

DoD = Direct outward Dialing

DNS = Domain Name System

DiffServ = Differenciated Service (service différencié)

DSCP = Differenciated Code Point

F

FTP = File Transfer Protocol

H

HDLC = High Data Link Control

http = Hyper Text Transfer Protocol

I

IAX = Inter-Asterisk Exchange

ICMP = Internet Control Message Protocol IETF = Internet Engineering Task Force

IP = Internet Protocol Security

IPBX = autocommutateur téléphonique utilise le protocole Internet (IP)

IPv4 = Internet Protocol version 4

ITU-T = International telecommunication Union

L

LDP = protocole d'allocation d'étiquettes)

LER = Label Edge Router

LFIB = Label Forwarding Information Base)

LIB = Label Information Base)

LSP = Label Switching Path

LSR = label Switch Router

M

MPLS = Multi Protocol Label Switching

N

NAT = Network Address Translation

O

OS = Operating System

P

PPP = Point to point protocol

PABX = Private Automatic Branch exchange PBX = Private Branch exchange

PSTN = Public Switched Telephone Network

Q

QoS = Quality of Service

R

RFC = Requests For Comment

RSVP = Protocole de réservation de ressource

RSVP-TE = réservation de ressources avec ingénierie du trafic

RTC = Réseau Téléphonique Commuté

RTCP = Real-time Transport Control Protocol RTP = Real-Time Transport Protocol

S

SIP = Session Initiation Protocol

SLA = Service Level Agreement

SPF = Sender Policy Framework

T

TCP = Transport Control Protocol TDM = Time Division Multiplexing

TOS = Type Of Service (type de service)

TTL = (Time To Live)

U

UAC = User Agent Client UAS = User Agent Server

UDP = User Datagram Protocol URL = Uniform Resource Locator

V

VoIP = Voice over Internet Protocol

VPN = Virtual Private Network

VRF = (VPN routing and forwarding)

W

WAN =World Area Network

Table des matières

Liste des figures

CHAPITRE I : VoIP

CHAPITRE II : MPLS (Multiprotocol Label Switching)

CHAPITRE III : Simulation sous GNS3

Introduction générale

Introduction générale

Au long de ces dernières années, Internet a influencé le développement de nouvelles variétés d'applications. Qui ont des besoins garantissant en termes de bande passante et de sécurité de service. En plus des données traditionnelles et transporter la voix et les données multimédia. Les ressources nécessaires pour ces nouveaux services ont entraîné une transformation de l'infrastructure d'Internet, d'une infrastructure par paquets à une infrastructure en cellules, a introduit de l'incertitude dans un réseau jusque-là déterministe.

L'augmentation de la connectivité des réseaux et l'intégration de plusieurs services dans un même système de communication a engendré une croissance significative de la complexité du métier de concepteur d'architectures de réseaux.

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

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

La mise en œuvre d'un réseau basé sur une plateforme IP/MPLS œuvrant dans la voix sur IP est le projet de fin d'étude que nous avons développé dans ce mémoire, qui est axé sur les trois chapitres suivants :

- Le premier chapitre est une introduction au domaine de la voix sur IP pour bien assimiler le principe.
- Le chapitre suivant est une présentation des concepts de base de la technologie MPLS et leurs mécanismes de fonctionnement, finissant par son influence sur la voix sur IP
- Le troisième chapitre nous présenterons une application pratique dans laquelle nous avons émulé un cœur de réseau utilisant la technologie IP MPLS sur la VoIP.

CHAPITRE I :
VoIP

I.1.Introduction

Les dernières décennies, ont connu une expansion rapide de l'utilisation des technologies de l'information et de la communication dans pratiquement tous les domaines. Tout le monde s'offre le luxe d'envoyer et de recevoir n'importe quel type de données (texte, image, voix, vidéo…etc.) en temps réel et à une qualité optimale. Cette évolution a eu lieu grâce au développement de nouvelles approches de traitement et de communication de l'information, une panoplie de standards et de normes ont vu le jour, grâce au travail acharné des organismes internationaux dans le domaine des télécommunications et de l'électronique.

La transmission de la voix en utilisant le protocole d'internet (IP : Internet Protocole), fait partie de ces approches qui ont bouleversé le monde des télécommunications et qui ont laissé une touche sur la qualité de service offerte aux utilisateurs des nouvelles technologies. En fait, jusqu'à la septième décennie du vingtième siècle, la transmission de la voix est basée sur des méthodes analogiques. La téléphonie traditionnelle par exemple emploie des lignes téléphoniques physiques, elle offre aux utilisateurs la possibilité d'émettre et de recevoir des appels téléphoniques vers des stations fixes et portables. Dans les années 80, la première évolution a été le passage à la transmission numérique TDM

L'essor de l'internet et sa démocratisation a permet l'élargissement géographique des réseaux internet, qui utilisent le protocole internet. Les réseaux intranet ont ainsi opté à leurs interconnexions via ce nouveau protocole. Dans ce contexte l'exploitation du réseau internet pour acheminer de la voix est devenu un enjeu majeur de la communauté scientifique. L'an 1996 a connu la naissance de la première version du standard de la transmission de la voix sur IP. Contrairement aux réseaux téléphoniques Commutés (RTC), la transmission de la voix sur IP permet le Transport de conversations téléphoniques sur n'importe quel type de réseau numérique ou Analogique, acceptant le protocole TCP/IP.

Dans ce chapitre, on s'intéresse à la voix sur IP, son fonctionnement, ses principes et l'impact de cette technologie sur la qualité de service. L'objectif de ce chapitre est d'étudier les techniques du transport de la voix sur les différents réseaux et le passage à la transmission de la voix sur IP. Nous commençons notre chapitre par l'architecture de la VoIP , de ses éléments et son principe de fonctionnement. Nous détaillerons ensuite les protocoles de signalisation et de transport ainsi que leurs principes de fonctionnement. Les avantages et inconvénients de chaque méthode sont enfin présentés et analysés. La deuxième partie de ce chapitre est consacrée à la qualité de service, nous expliquons l'impact positif de la voix sur IP sur la qualité de service **[1].**

I.2. Protocole TCP/IP

Le sigle TCP/IP représente l'ensemble des protocoles de transport et de contrôle de l'information sur les réseaux intranet et internet. Sur le plan historique, ce standard a été à l'origine destiné au secteur militaire, les premières recherches ont été effectuées par des militaires. En 1983, le premier standard TCP/IP a vu le jour, son exploitation se limite tout de même au secteur militaire. Peu à peu, les domaines d'application du protocole TCP/IP s'étendent au secteur universitaire, commercial et même grand public.

Divers sont les avantages de l'utilisation de ce protocole. On peut citer par exemple :

L'interopérabilité : grâce aux recherches et processus de standardisation, le TCP/IP est implémenté sur les équipements des grandes sociétés des télécommunications.

La gestion du réseau : le TCP/IP s'offre un nombre très important de protocoles de gestion de réseau, rendant ainsi cette opération très fiable.

L'extension du réseau internet : le fait que les réseaux internet sont basés sur le protocole TCP/IP rend son utilisation est plus que recommandable.

I.2.1. Architecture du protocole TCP/IP

Étant donné que le protocole TCP / IP a été créé à la demande du ministère américain de la Défense, il est généralement appelé modèle DoD .La plupart des descriptions du protocole TCP/IP définissent une architecture de protocole à quatre niveaux fonctionnels (du bas en haut) :

- **Couche d'accès au réseau :** cette couche comprend les routines d'accès au réseau physique. Le niveau le plus bas de l'architecture du protocole TCP/IP n'est autre que les connexions câblées de la couche physique, les circuits d'interface électrique (émetteurs-récepteurs), les cartes de couplage et les protocoles d'accès au réseau.

La couche d'accès au réseau TCP / IP intègre généralement les fonctions des deux couches inférieures du modèle de référence OSI (liaison de données et physique). Les utilisateurs ignorent souvent cette couche car la conception de TCP / IP cache les fonctions des couches inférieures. Ceci est dû au fait que ce protocole est une partie intégrante de l'Unix, à cet effet, cette couche apparait généralement comme une combinaison de pilotes, de périphériques et de programmes associés.

- Couche Internet : Cette couche définis les datagrammes et elle est responsable de l'opération de routage des données. La couche Internet doit fournir les adresses logiques pour les interfaces physiques. Les protocoles ARP et RARP sont employés pour fournir un mappage entre les adresses logiques et les adresses physiques fournies par la couche d'accès au réseau. Le protocole ICMP fait partie également de la couche internet, celui-ci est responsable du diagnostic et de la résolution des situations particulières liées au protocole IP. La couche Internet est également responsable du routage des paquets de données et des datagrammes entre les hôtes. Cette couche est utilisée par les couches supérieures du modèle DoD **[1]**.

- **Couche de transport hôte à hôte (TCP / UDP) :** Elle Fournit les services de transmission de données de bout en bout. Cette couche définit la connexion entre deux hôtes sur le réseau. Le modèle DoD comprend deux protocoles d'hôte à hôte:

- **Le protocole TCP :** ce protocole est responsable de la fiabilité des services de transmission de données et de la détection et la correction des erreurs. Il permet également des connexions simultanées. Vous pouvez établir plusieurs connexions TCP sur l'hôte et envoyer des données en même temps. Le TCP autorise les connexions en duplex intégral.
- **Le protocole UDP :** Ce protocole est non fiable pour les applications qui ne nécessitent pas de fiabilité TCP.

- **Couche Application :** La couche application est le summum de l'architecture TCP / IP. Elle permet aux applications d'utiliser des protocoles de couche hôte à hôte (TCP et UDP) pour transférer leurs données. Parmi les protocoles d'application les plus utilisés (orientés utilisateur), on peut citer les protocoles :

- TELNET : celui-ci est un protocole de terminal réseau (émulation de terminal), qui permet d'ouvrir des sessions à distance sur le réseau.
- FTP est un protocole de transfert de fichiers
- SMTP
- DNS ce protocole est également connu sous le nom de service de noms, il permet aux adresses IP d'être mappées aux noms attribués aux hôtes du réseau.
- RIP ce protocole est utilisé pour gérer les fonctions de routage.
- NFS il permet de partager des fichiers entre les différents hôtes sur le réseau.

I.2.2. Les fonctions du protocole IP

Le protocole Internet RFC 791 fournit les services de transfert de paquets de données de base sur lesquels les réseaux TCP / IP sont construits. Tous les protocoles des couches supérieures et inférieures à IP utilisent des protocoles Internet pour transmettre les données. Autrement dit toutes les données (entrantes et sortantes) quelle que soit leur destination finale TCP / IP sont transmises via IP.

La couche IP repose sur le matériel réseau sous-jacent pour la transmission. IP peut être exploité par plusieurs technologies différentes : Ethernet, Token Ring, FDDI, ATM…etc.

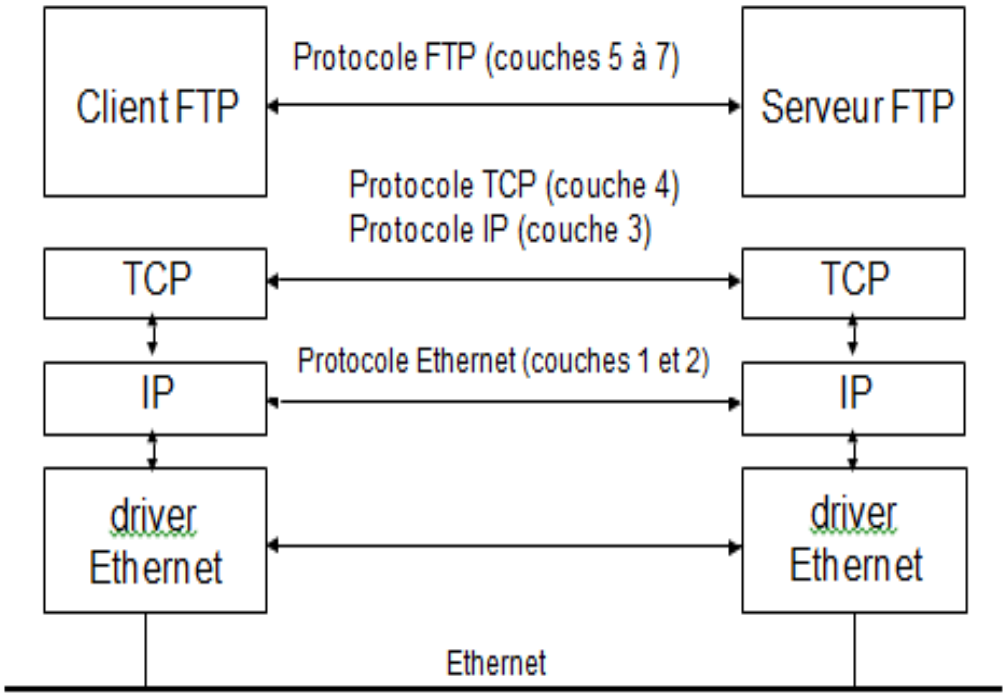

Figure I. 1.Schéma des fonctions de l'IP **[1]**

Les fonctions du protocole IP comprennent :

- La Définition du datagramme.
- La Définition du plan d'adresses Internet.
- Le Flux de données entre la couche d'accès réseau et l'hôte de la machine vers la couche de transmission de la machine hôte.
- Le routage des datagrammes vers des ordinateurs distants.
- La fragmentation et le réassemblage des datagrammes.

Le protocole IP est principalement un protocole non orienté connexion, et le routage de chaque datagramme est indépendant des autres protocoles. Si le protocole Internet nécessite des services orientés connexion, le protocole Internet déléguera la tâche d'établir une connexion aux protocoles d'autres couches. Les réseaux IP utilisent des méthodes de livraison au mieux, c'est-à-dire la meilleure livraison possible des datagrammes, mais cette livraison ne peut pas être garantie.

Le protocole IP s'appuie également sur d'autres couches de protocoles pour assurer la détection et la correction des erreurs éventuelles. Le protocole ne contient qu'une somme de contrôle d'en-tête et il n'y a pas de code de vérification des données (code de détection et de correction d'erreur). D'autres protocoles des couches de l'architecture TCP / IP permettent d'effectuer cette vérification si nécessaire **[1].**

I.2.2.1 Format du datagramme IP

Les datagrammes IP contiennent des en-têtes IP suivis de données IP provenant de protocoles de niveau supérieur.

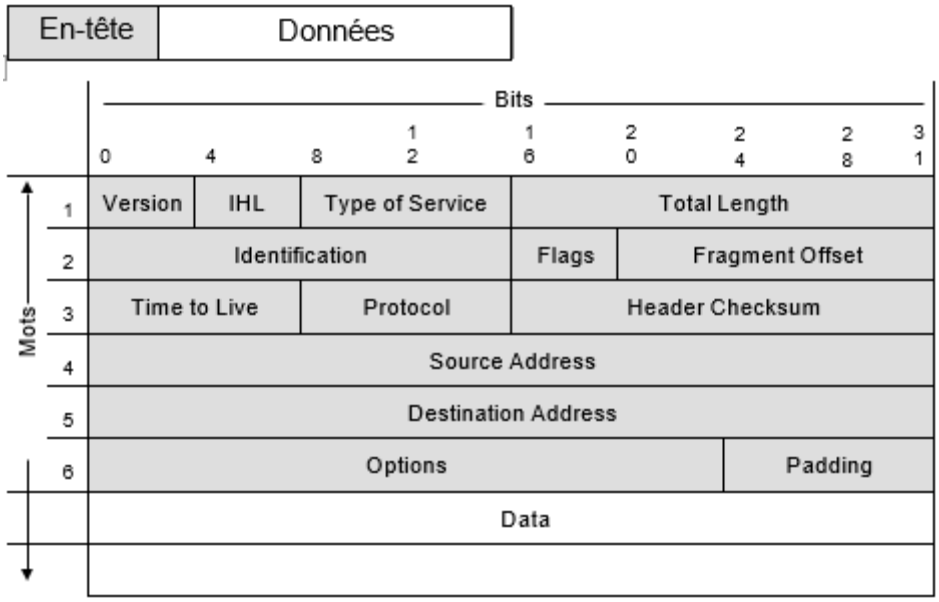

Figure I. 2. Format du datagramme **[1]**

Par défaut, la longueur de l'en-tête est de 5 mots de 32 bits chacun (20 octets), le sixième mot est facultatif. La longueur de l'en-tête étant variable, elle contient un champ appelé (IHL). L'en-tête contient toutes les informations nécessaires pour transmettre le paquet de données.

La longueur du champ *Version* est de 4 bits, indiquant le format de l'en-tête IP: le numéro de version actuel est 4 (IPv4), le numéro de version par défaut est 4. La prochaine version est la version 6 (IPv6) et autorise les adresses IP de 128 bits. L'expéditeur, le destinataire et tous les routeurs intermédiaires utilisent ce champ pour déterminer le format de l'en-tête IP.

Le champ (TOS) informe le réseau de la qualité de service requise pour spécifier la priorité, le délai, le débit et la fiabilité. La plupart des implémentations de TCP / IP et des protocoles de routage ignorent ce champ, mais il pourrait jouer un rôle plus important à l'avenir.

Le champ contient la longueur de l'en-tête et des données IP (en octets). Internet ne limite pas les datagrammes à une taille spécifique, mais il est recommandé que les réseaux et les passerelles puissent prendre en charge des datagrammes de 576 octets (données de 512 octets + en-tête de 64 octets

et données spécifiques au protocole) sans fragmentation. La taille des datagrammes IP sur la plupart des réseaux et des hôtes dépasse rarement 16 Ko.

La durée de vie (en secondes), elle représente le temps de survie le plus long d'un datagramme sur le réseau. Cette valeur est décrémentée au niveau de chaque routeur. Lorsque le champ TTL est égale à 0, le temporisateur TTL s'expire et le datagramme IP est Rejeté par le routeur (pas l'hôte cible). Le champ TTL a une double fonction :

- Limiter la durée de vie des segments TCP.
- Eliminer les boucles de routage Internet.

Lorsque le temporisateur TTL s'expire, un message ICMP en avertit la source. La valeurpar défaut utilisée est égale à 32 ou 64.

Le protocole IP utilise l'adresse de destination contenue dans le cinquième mot de l'en-tête pour envoyer des datagrammes. L'adresse cible est une adresse IP de 32 bits standard, qui est utilisée pour identifier le réseau cible et l'hôte connecté au réseau.

Si l'adresse de destination correspond à l'adresse de l'hôte connecté au réseau local, le paquet de données est directement transmis à la destination, sinon il est envoyé à la passerelle afin avant d'être retransmis à l'hôte. Le routage correspond à la sélection d'une passerelle pour la transmission de données, le protocole IP détermine ensuite la route appropriée pour chaque paquet.

I.2.2.2. Acheminement des datagrammes

Les passerelles Internet sont souvent appelés routeurs IP car elles utilisent des protocoles Internet pour acheminer les paquets de données entre les réseaux. Dans la terminologie TCP / IP traditionnelle, il n'y a que deux types de machines périphériques de réseau :

- Les passerelles
- Les machines-hôtes.

La passerelle transmet les paquets de données entre les réseaux, mais pas l'hôte. Cependant, si un hôte est connecté à plusieurs réseaux (appelé hôte à connexions multiples), il peut transférer des paquets de données entre les réseaux. Lorsqu'un hôte à connexions multiples transmet des paquets de données, son fonctionnement est le même que celui d'une passerelle et agit comme une passerelle **[1].**

I.2.2.3. Fragmentation des datagrammes

Lorsqu'une passerelle interconnecte des réseaux physiques différents, il est parfois nécessaire de diviser le datagramme en éléments de plus petite taille pour passer d'un réseau à l'autre. Chaque type de réseau se caractérise par une unité de transfert maximale MTU, celle-ci correspondant au plus grand paquet que celui-ci puisse transférer. Si la longueur du datagramme provenant d'un réseau est supérieure à la MTU de l'autre réseau, il est alors nécessaire de diviser le datagramme en fragments de plus petite taille afin de permettre la transmission des données. Cette procédure se nomme la fragmentation.

Type de réseau	MTU (en octets)
Ethernet IEEE 802.3	1 500
Token-RingFDDI	1 492
IEEE 802.4	4 440 à 17 940
	4 352
	8 166

Figure I. 3.caractérisation de type de réseau par unité de transfert **[1]**

Le deuxième mot de l'en-tête contient des informations qui identifient chaque fragment du datagramme et fournissent des informations sur le processus de recombinaison des différents fragments dans le datagramme d'origine.

Le champ d'identification indique le datagramme auquel appartient le fragment, et le champ de décalage de fragment (le décalage du fragment, exprimé en multiples de 8 octets) spécifie quelle partie du datagramme correspond au fragment. Le champ Flags a un bit "More Fragments bit", qui indique au protocole IP s'il a assemblé tous les éléments du datagramme (MF = 0) ou non. La réorganisation est effectuée par le module IP de destination et non pas par le routeur intermédiaire **[1].**

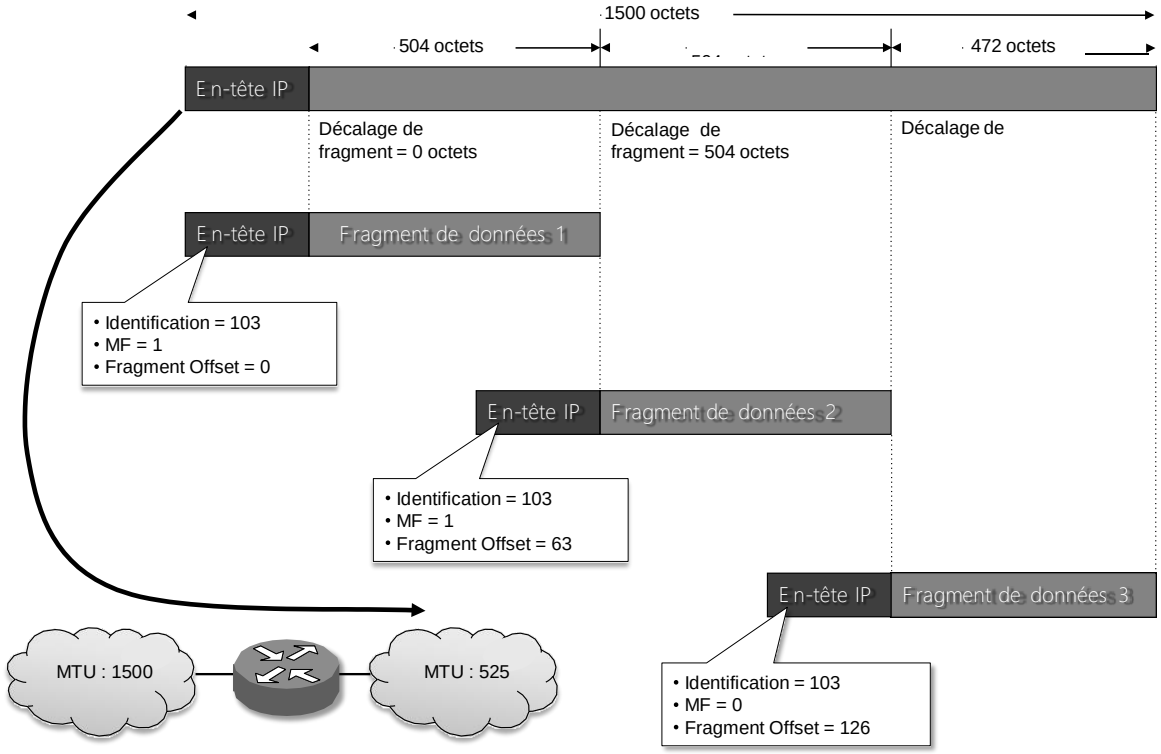

Figure I. 4.Fragmentation des datagrammes **[1]**

I.2.2.4. Transmission de datagrammes à la couche Transport

Le champ de protocole indique quel protocole de couche supérieure recevra les données IP. Ce champ est utilisé pour multiplexer / démultiplexer des données dans des protocoles de niveau supérieur. Chaque protocole a un numéro de protocole unique, permettant au protocole IP de l'identifier. Par exemple, la valeur du champ «Protocole» est égale à 6 pour TCP, 17 pour UDP et 1 pour ICMP. Sous Unix, ces valeurs sont stockées dans un fichier spécial **[1].**

I.3. VoIP (Voice Over IP)

I.3.1.Définition

La voix sur IP est une approche d'établissement et de gestion des communications vocales via le réseau Internet. Le principe de cette technologie est contraire à la téléphonie analogique filaire, qui est basée sur le raccordement aux réseaux téléphoniques commutés (RTC) et à des centraux téléphoniques dédiés. La voix sur IP réalise le trafic de conversations téléphoniques sur tout le réseau, Analogique ou numérique, acceptant le protocole TCP/IP (Ethernet, RNIS, PPP, etc.).

La VoIP est une technique qui permet de transporter, à l'aide du protocole IP. Cette technologie convertit le signal vocal en un signal digital qui traverse le réseau internet. Ces paquets sont ensuite acheminés dans le bon ordre en respectant un délai précis pour la reproduction correcte de la voix **[2].**

I.3.2. Principe de fonctionnement

Les signaux vocaux sont découpés en minuscules unités appelées "paquets" et sont transmis vers le destinataire à travers le réseau 'maillé ' quel que soit le chemin. Pour atteindre sa destination, chaque paquet est numéroté et reçoit l'adresse du destinataire, on appelle ça l'encapsulation des paquets. Les paquets suivent donc leur propre route en fonction de l'encombrement du réseau Internet. Dans une situation ou une ligne est en panne, les paquets déjà envoyé changent automatiquement de route pour arriver à leur point de destination. Une fois arrivés, les paquets sont remis dans leur ordre initial d'émission. Rien n'est transparent car tout ceci se déroule à la vitesse de la lumière. Néanmoins, si une multiplicité de paquets prennent du temps à parvenir, c'est l'ensemble des paquets précédents qui mettra un temps d'attente à parvenir en attendant le paquet manquant, ce qui des fois s'interprète chez l'usager par un délai à la réception de la voix. Il est question de délai de latence ou temps de latence.

Dans les réseaux Internet les signaux vocaux transmis par paquet ne sont plus : "spécifiques – voix", mais sont pris en compte comme des données particulières à transmettre (communication de point à point) au même niveau que la vidéo (ou l'on parle de streaming) ou divers fichier. Ces paquets à transmettre incluent des adresses réseau de l'expéditeur et du destinataire, ils vont être acheminés par des routeurs et des serveurs avec des routes divergentes afin de parvenir à une destination finale, à l'arrivée des paquets, ces derniers doivent être classés par ordre de la transmission d'origine pour réaliser une bonne lecture de la voix. Chaque paquet envoyé dans le réseau est constitué de :

- Une Entête indiquant sa source et sa destination.
- Un numéro de séquence.
- Un bloc de données.
- Un Code de vérification des erreurs.

I.3.3. Architecture de la voix sur IP

En tant que nouvelle technologie de communication, la voix sur IP n'a pas de norme unifiée. En fait, chaque fabricant introduit ses normes et ses fonctions dans ses solutions. Les trois principaux protocoles sont H.323, SIP (Session Initiation Protocol) et MGCP / MEGACO. Par conséquent, il existe plusieurs méthodes pour fournir des services de téléphonie et de visiophonie via un réseau IP.

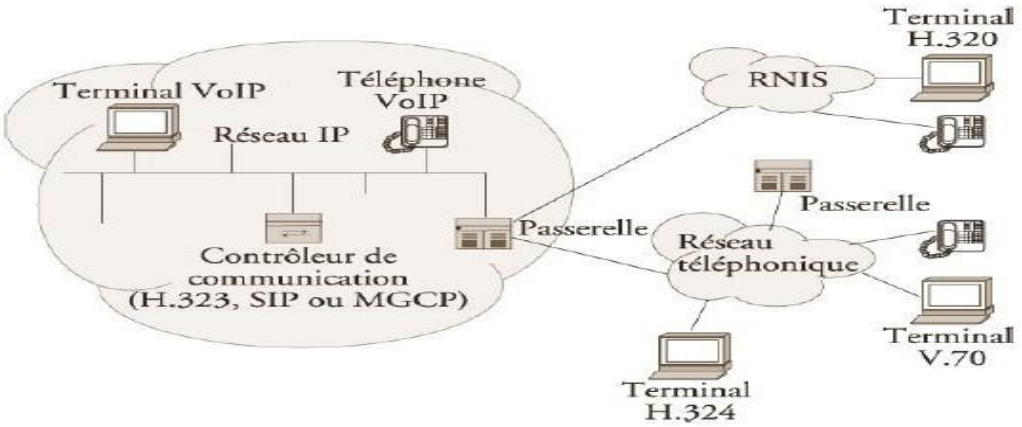

Figure I. 5.Architecture générale de la voix sur IP **[3]**

En général, la figure 1.5 décrit la topologie d'un réseau téléphonique IP. Il comprend toujours des terminaux, des serveurs de communication et des passerelles vers d'autres réseaux. Chaque norme a ses propres caractéristiques pour assurer plus ou moins de qualité de service. Le réseau peut également être expulsé sur le terminal ou sur un contrôleur de passerelle commutateur appelé Gatekeeper. Ci-dessous les éléments communs aux différents types d'architecture :

- **Le Routeur** : il est utilisé pour acheminer les paquets de données entre deux réseaux. En raison de l'ajout d'une carte dédiée qui prend en charge le protocole VoIP, certains routeurs peuvent simuler à des Gatekeeper.

- **La Passerelle :** elle est utilisée pour connecter le réseau de commutation et le réseau IP.

- **Le PABX :** C'est le commutateur du réseau téléphonique traditionnel. De cette manière, une liaison peut être établie entre la passerelle ou le routeur et le PSTN (réseau téléphonique commuté). Cependant, si l'ensemble du réseau devient IP, le matériel deviendra obsolète.

- **Le Terminal :** il appartient généralement au type logiciel ou matériel.
  Le téléphone logiciel est installé sur le PC de l'utilisateur. L'interface audio peut être un microphone et des haut-parleurs insérés dans la carte son, bien que des écouteurs soient recommandés.

- **Le Téléphone matériel :** C'est un téléphone IP qui utilise la technologie vocale IP, permettant de passer des appels téléphoniques via un réseau IP au lieu du réseau PSTN ordinaire. Les appels peuvent provenir par le réseau internet comme par un réseau privé.

Le terminal peut exploiter les protocoles comme le SIP ou l'un des protocoles propriétaires comme celui utilisée par Skype **[3].**

I.3.3.1. Les architectures utilisées

La VoIP utilise généralement 3 architectures : PC 2 PC, PC 2 téléphone et enfin téléphone 2 téléphone VoIP.

- **L'architecture PC 2 PC**

Cette architecture nécessite deux ordinateurs, chacun équipé d'un téléphone logiciel (logiciel de communication), et il est connecté au réseau Internet via un fournisseur d'accès Internet, qui fournit un support physique pour la transmission de paquets de données ou dans le cas d'un réseau. PBX (logiciel Asterisk)

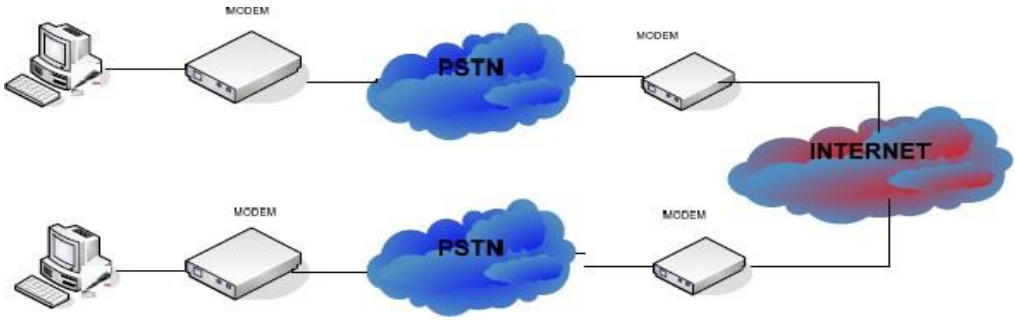

Figure I. 6.Scenario PC 2 PC **[4]**

- **L'architecture PC 2 Phone (architecture Phone 2 PC)**

Cette architecture assure l'interconnexion de deux types de réseaux différents: un participant utilise un PC connecté au réseau Internet selon le fournisseur d'accès Internet et l'autre utilise un téléphone ordinaire connecté au réseau téléphonique commuté. En fait, le canal d'un réseau à un autre nécessite une passerelle dédiée pour convertir les paquets de données entre les réseaux.

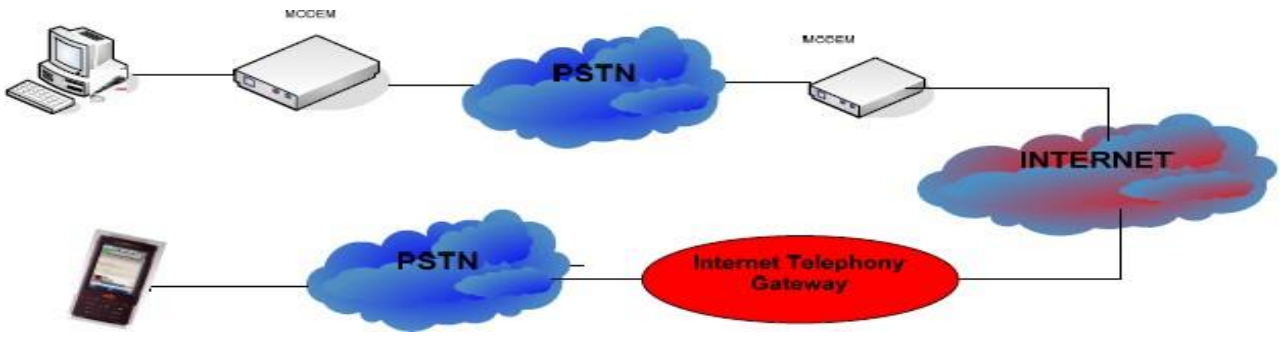

Figure I. 7.Scenario Phone 2 PC **[4]**

- **L'architecture Phone 2 Phone**

La configuration ne se limite pas à l'interconnexion du PBX, tous les éléments peuvent se toucher. Le réseau IP doit pouvoir supporter un certain niveau de qualité de service. Afin de convertir la voix IP en voix et vice versa, une passerelle doit être utilisée de chaque côté entre le réseau téléphonique et le réseau de paquets IP

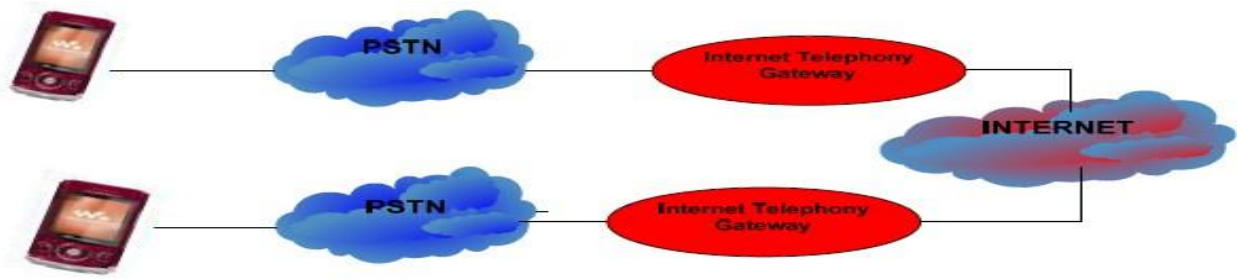

Figure I. 8.Architecture Phone 2 Phone **[4]**

- **Autre type d'architecture VoIP**

Dans ce type d'architecture, les réseaux IP, les réseaux téléphoniques et le RNIS existent à la fois. Dans ce cas, une

passerelle est nécessaire pour connecter ces trois réseaux. Le réseau IP a besoin d'un contrôleur de communication (H323, SIP, MGCP). Le terminal H320 est connecté au RNIS Des terminaux H324 et V70 peuvent être ajoutés au réseau téléphonique. Sur le réseau IP, il peut y avoir des terminaux VoIP et des téléphones VoIP **[4].**

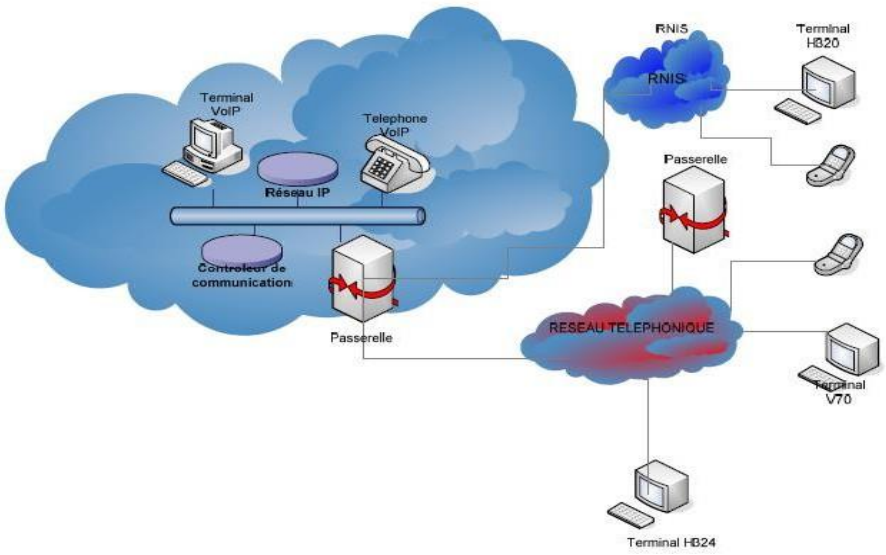

Figure I. 9.Architecture incluant trois réseaux **[4]**

I.3.4. Les protocoles de signalisation

I.3.4.1. Protocole H.323

a) Définition

Le protocole H.323 est le protocole de signalisation défini par l'ITU-T en 1996 réalisant l'établissement, la libération et la modification de sessions multimédia (voix, vidéo, données). Ce protocole est une version améliorée du protocole Q.931 du RNIS, fonctionnement est basé sur le transport en mode paquet de l'information. Il endosse une collecte de services complémentaires similaires à ceux qui sont misent en œuvre dans le réseau RNIS. En premier H.323 était conçu pour la transmission de la voix sur un réseau local (LAN), mais de plus en plus avec l'amélioration des techniques, la norme H.323 est développée pour être appliquée dans des réseaux d'ordinateurs assez grands (Internet, Intranet).

b) Architecture et composants

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

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

La figure I.10 défini les composants de l'architecture H.323.

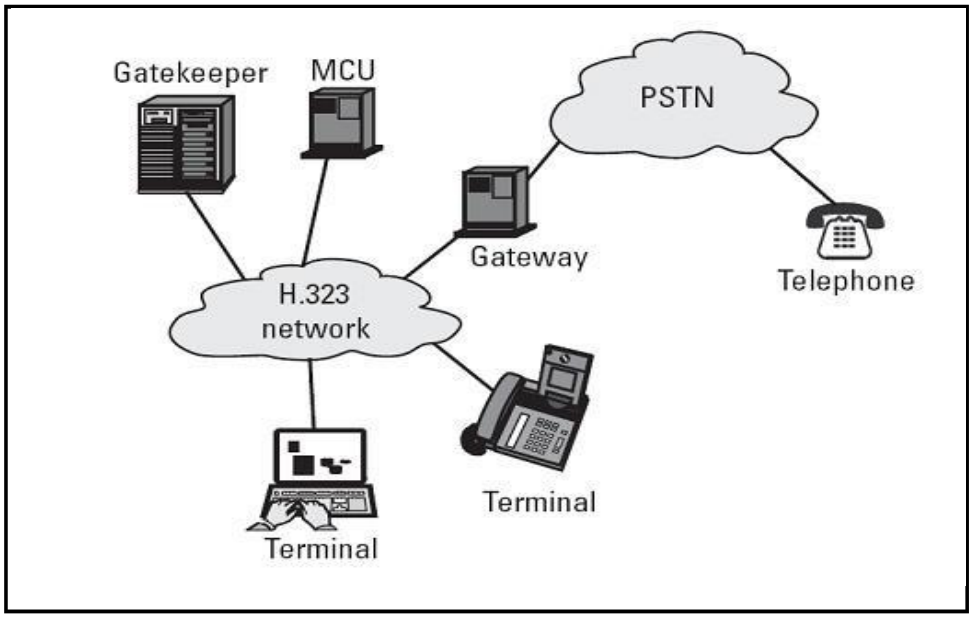

Figure I. 10.Les composants de l'architecture H.323. **[5]**

Le terminal H.323 est le nœud du réseau de la VoIP, il a la faculté de se connecter sur le réseau pour :

- concrétiser un appel avec un second terminal de la VoIP ou différent réseau.
- Accepter un appel de d'un second terminal.
- mettre fin à un appel.

Le Gatekeeper est un élément de l'architecture de la VoIP qui dirige la registration, L'admission ainsi que le statut des terminaux ou des passerelles. Il fait également la gestion de la zone, le traitement d'appel et le signalement d'appel.

Le MCU représente une station sur le réseau qui donne les possibilités pour au moins trois terminaux et passages pour participer à une conférence multipoints. Le MCU administre les ressources de la conférence, négocie avec les terminaux pour choisir les codecs audio et vidéo à mettre en place et dirige les flux de données. Le MCU s'affecte d'un contrôleur multipoints obligatoire (MC) ainsi que des processeurs multipoints optionnels (MP). Le MC caractérise les possibilités communes des terminaux en utilisant le protocole H.245, ceci dit il n'exécute pas le multiplexage d'audio, de la vidéo et des données. Le multiplexage de médias est manipulé par le MP sous la supervision de MC.

Les Passerelle (Gateways) H.323 garantissent l'interconnexion avec les différents réseaux, lesmodems H.324, les téléphones classiques, etc...). Elles sont responsables de la correspondance de signalisation de Q.931, et de celle des signaux de contrôle et la cohésion entre les médias (multiplexage, correspondance des débits, transcodageaudio) **[5].**

c)Avantages et inconvénients de la technologie H323

La technologie H.323 représente les avantages et inconvénients cités ci-dessous :

- **La gestion de la bande passante :** le protocole H.323 garantit le fonctionnement normal des applications clés sur le LAN en définissant des restrictions de flux audio/vidéo, permettant ainsi une bonne gestion de la bande passante. Chaque terminal H.323 peut effectuer un ajustement de la bande passante et une modification du débit en fonction du comportement du réseau en temps réel (retard, perte de paquets et gigue).
- **La prise en charge multipoint :** le protocole H.323 permet des conférences multipoint via une structure centralisée (telle que MCU ou en mode ad hoc.
- **La prise en charge de la multidiffusion**, le protocole H.323 permet également la transmission de multidiffusion.
- **L'interopérabilité du protocole H.323**. En fait ce protocole permet aux utilisateurs de ne

pas se soucier des méthodes de communication et de négocier de manière transparente les paramètres (codec, débit binaire, etc.).

- **La flexibilité:** les conférences H.323 peuvent inclure des terminaux hétérogènes (salles de visioconférence, PC, téléphones, etc.). En raison de différentes situations, elles peuvent partager la voix, la vidéo et même des données conformes T.120, grâce à la spécification T.120.

La liste non exhaustive des avantages du protocole H323, n'inclut en aucun cas les inconvénients de ce protocole. Ceux-ci comprennent entre autre la complexité de la mise en œuvre et la structure du système d'intégration des services téléphoniques et Internet. Le manque de modularité et de flexibilité **[7].**

I.3.4.2. Protocole SIP

A. Définition

Le protocole SIP est un protocole standardisé par l'IETF, qui a été conçu pour créer, modifier et terminer les sessions multimédias. Il est chargé de vérifier et de localiser plusieurs participants. Il est également chargé de négocier les types de supports que différents participants peuvent utiliser en encapsulant les messages SDP. Le protocole SIP n'a rien à voir avec la transmission de données, il ne contient pas de données échangées pendant la session, telles que l'audio ou la vidéo.

Le protocole SIP étant un standard ouvert pour la VoIP, il est interopérable et vise à devenir un standard pour les télécommunications multimédias (voix, image, etc.). Par conséquent, il n'est pas seulement utilisé pour la VoIP, mais également pour de nombreuses autres applications, telles que la visiophonie, la messagerie instantanée ect **[6].**

B. Architecture et composants du protocole SIP

Le protocole SIP est basé sur deux types de composantes, les agents utilisateurs (UAS, UAC) et un réseau de serveurs (Registrar, Proxy).

U.A.S : est une application de type serveur qui connecte l'utilisateur quand une demande SIP est reçue. Également est un agent de la partie appelée.

U.A.C : cet élément définit l'agent de la part appelante. C'est une application de type client qui fait l'initiation des requêtes.

Le Registrar est un serveur qui administre les requêtes REGISTER envoyées par les Users Agents afin de signaler leur positionnement courant. Ces requêtes comportent donc une adresse IP liée à un URI, qui sera enregistré dans une base de données.

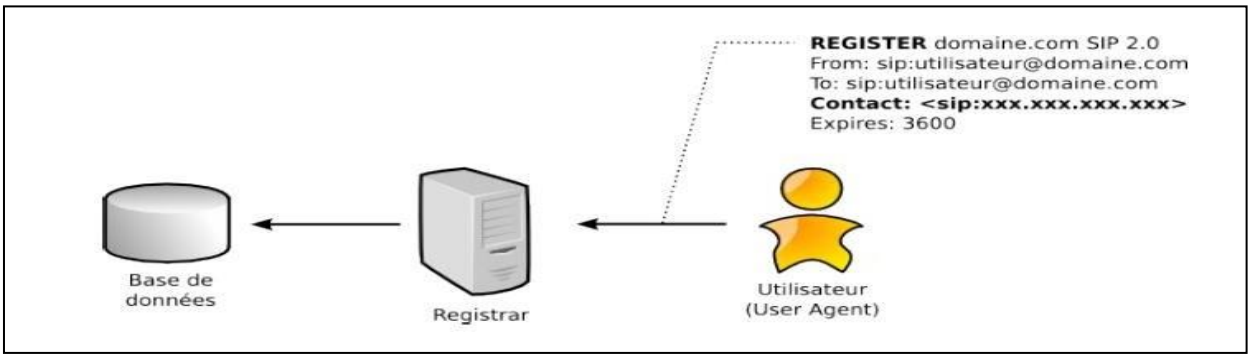

Figure I. 11.Enregistrement d'un utilisateur. **[6]**

Le proxy SIP : il sert de médiateur entre deux User Agents qui ignorent leurs localisations respectives (adresse IP). En effet, l'association URI-Adresse IP est enregistrée préalablement dans une base de données par un. Le Proxy a le pouvoir donc d'interroger cette base de données pour faire circuler les messages vers le destinataire.

Le Proxy a pour rôle de relayer uniquement les messages SIP pour établir, contrôler et mettre fin à la session. Une fois la session établie, les données, comme exemple le flux RTP pour la VoIP, ne transitent pas par le serveur Proxy. Leurs trafics sont établis directement entre les User Agents **[6].**

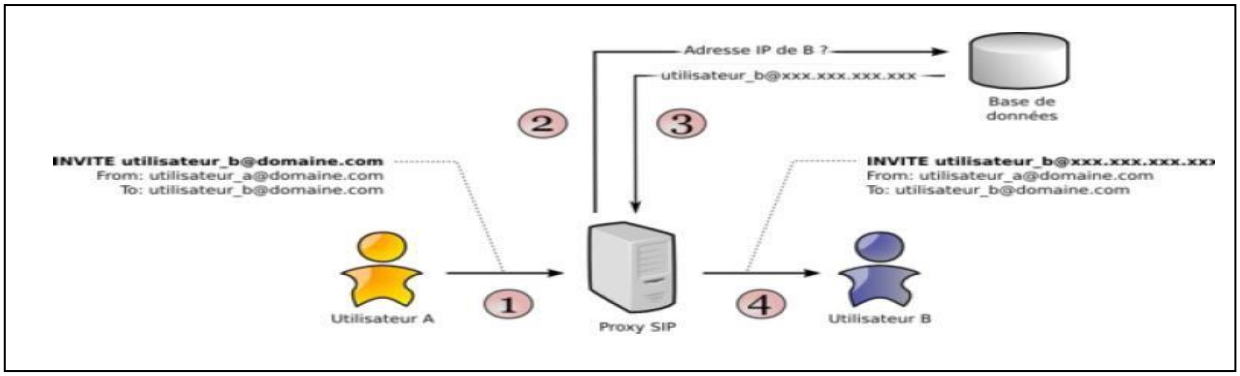

Figure I. 12.Principe du protocole SIP. **[6]**

C. Avantage et inconvénients du protocole SIP

Le protocole SIP offre de nombreux avantages, ceci est dû au fait qu'il est :

- Les protocoles et les documents officiels du SIP sont répertoriés en détail, tout le monde peut les télécharger.
- standard : l'IETF normalise ce protocole et son développement continu en créant ou en développant d'autres protocoles utilisés avec SIP.
- Simple: Le SIP est très simple, très similaire à HTTP.
- Flexible: Le SIP est utilisé pour tous les types de sessions multimédia (voix, vidéo, musique, etc.).

Ces avantages n'ont pas empêché la communauté scientifique à fournir d'énormes efforts, pour pallier aux insuffisances citées ci-dessous du protocole SIP :

- L'implémentation du protocole SIP: si celle-ci est incorrecte ou incomplète dans l'agent utilisateur, l'annulation de l'opération est inévitable.
- La limitation du nombre d'utilisateurs : le SIP est toujours connu et utilisé par le public et ne peut bénéficier de l'influence du réseau **[6].**

I.3.4.3. Le protocole MGCP

Le protocole MGCP est un protocole asymétrique (client-serveur) pour la voix sur IP. Il est différent des protocoles symétriques (client-serveur) SIP et H323. Ceux-ci ont les caractéristiques d'un protocole structuré en mode peer-to-peer ; ce qui signifie que chaque terminal est indépendant, donc il peut établir la communication (appel) et les services associés. Le terminal SIP / H323 a une autonomie.

En examinant les tendances et les attentes de l'entreprise en matière de télécommunications, nous avons constaté que peu de ces terminaux ISDM sont utilisés dans le réseau. La plupart des téléphones clients sont des téléphones simples (analogiques) qui ne fournissent que des fonctions d'appel de base et sont eux-mêmes contrôlés par un commutateur (PABX) pour gérer les services d'appel spécifiques.

Il est donc nécessaire d'avoir un protocole VoIP apte à fonctionner de la même manière, afin de laisser le contrôle des fonctions à l'opérateur et de fournir les services de base (appel, réponse, raccroché) uniquement du côté de l'abonné. Par conséquent, la gestion du service d'appel est centralisée et fournie côté serveur, tandis que le client ne gère que les fonctions d'appel de base et recevra des instructions du serveur. Ce type de processus est très utile dans les environnements où les opérateurs souhaitent garder le contrôle des services des abonnés.

- **Architecture du protocole MGCP**

Le protocole MGCP a une architecture qui repose sur deux entités :

- **Terminaux MGCP:** Ils sont situés côté client et sont les passerelles chargées de recevoir et de renvoyer les instructions du contrôleur central (call agent).

- **Le call agent :** il s'occupe du réseau MGCP, et il est responsable de la commande et de la fourniture des instructions à la passerelle MGCP. L'agent d'appel et le terminal communiqueront en utilisant les ports UDP 2727 (call d'appel) et 2427 (terminal) pour échanger des transactions. Comme dans le SIP et le H323. Le flux vocal est également géré.

Le protocole MGCP est un complément à H323 ou SIP, traitant de l'interconnexion des terminaux IP et PSTN. Le MGCP n'intervient qu'en périphérie du cœur du réseau.

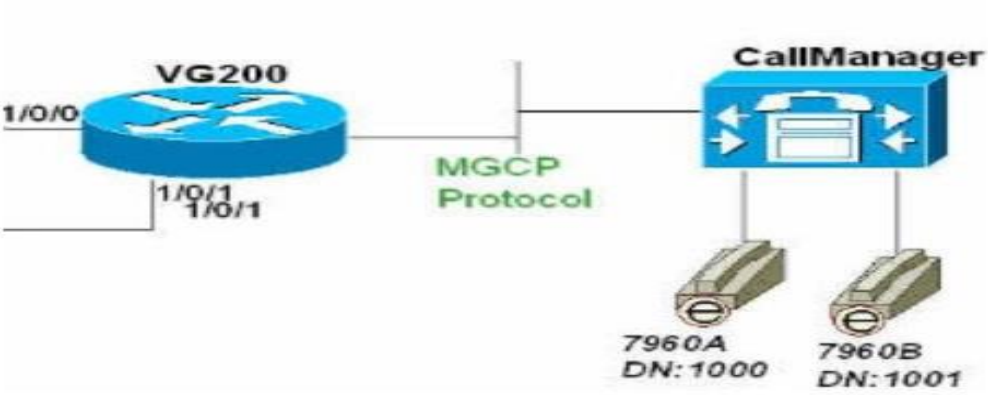

Figure I. 13.Architecture de la MGCP **[8]**

I.3.4.4. Le protocole MEGACO/H.248

Le protocole H.248 est nommé MEGACO, il est l'exploit des efforts de l'ITUet de l'IETF. Ce protocole dérive du MGCP. Comparé à celui-ci, le H248 apporte les améliorations suivantes :

- Il peut supporter des services multimédias et des vidéoconférences.
- L'Utilisation des codages en modes textes.
- La possibilité d'inclure UDP, TCP et SCTP.

La figure ci-dessous représente la structure du MGCP et H.248/MEGACO dans leréseau NGN (réseau de nouvelle génération)

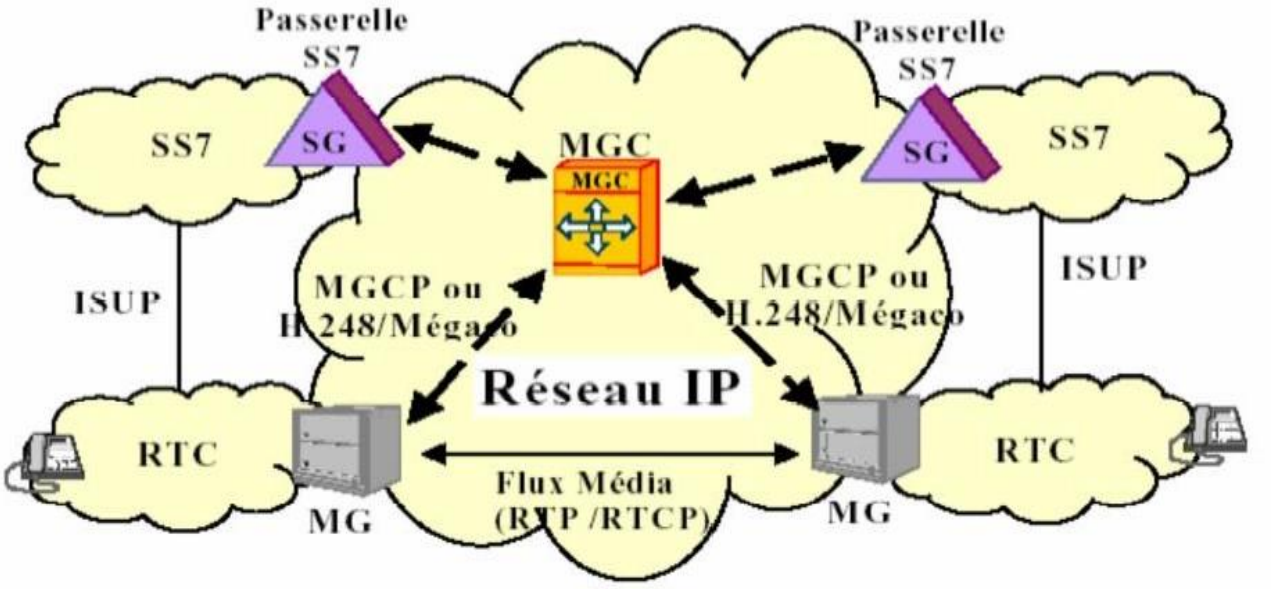

Figure I. 14.Architecture de H.248 / MEGACO **[8]**

MG : une media Gateway qui convertie des flux médias entre les différents réseaux.

- **Le MGC :** il administre l'état d'appel pour les communications entre le soft switch et une media Gateway.

- **La terminaison :** elle est une entité logique dans une MG, décrivant des ports connectes à celle-ci, qui ont la possibilité d'envoyer ou de recevoir un ou divers flux médias. Elle est représentée par un ensemble de caractéristiques qui sont groupes dans une collection de descripteurs intégré dans des commandes.

Chaque terminaison décrit un seul contexte et choisit par un indicateur de terminaison unique (Terminaison ID) indiqué par le MG.

I.3.4.5. Le protocole IAX, le protocole d'Asterisk pour la NAT

L'IAX est un protocole de signalisation qui peut remplacer le protocole SIP. C'est le protocole sur lequel Asterisk est basé, bien qu'il puisse prendre en charge d'autres protocoles VoIP majeurs, tels que SIP. Il permet la communication entre le client et le serveur et entre les serveurs. Il est plus puissant que SIP car il est conçu pour contrôler et transmettre des flux multimédias avec des débits inférieurs

- **Le fonctionnement du protocole IAX**

L'IAX utilise un seul port UDP, tandis que le port 4569 (IAX1) utilise le port 5036), ce qui marque l'une des plus grandes différences par rapport au protocole SIP. En effet, outre sa fiabilité, le protocole SIP est également connu pour ses principales limitations, difficiles à réaliser après le NAT **[8].**

I.3.5. Les protocoles de transport

Les protocoles RTP / RTCP sont deux protocoles utilisés pour le streaming multimédia sur les réseaux IP. L'utilisation du multiplexage statistique pour transmettre la voix introduit une gigue, qui doit être compensée par le récepteur. Les routeurs IP sont des équipements de multiplexage statistique, de sorte que toutes les applications voix et vidéo IP doivent résoudre ce problème de gigue. Le RTP est conçu pour permettre au récepteur de compenser la gigue et les changements de séquence de paquets. Le RTP peut être utilisé pour tout type de données en temps réel. Il définit un format de données spécial pour les paquets de données IP.

• Informations sur le type de données transférées (charge utile)

• Horodatage

•numéro de série

Quoiqu'il permet la transmission des informations sur la qualité effective de la transmission (gigue mesurée, taux moyen de perte de paquets, etc.). Le protocole RTP / RTCP ne peut pas contrôler entièrement la qualité de service. Les réseaux IP peuvent perturber, retarder ou modifier l'ordre des paquets RTP. Généralement, le RTP est utilisé en plus du protocole UDP. Celui-ci utilise uniquement des sommes de contrôle pour garantir l'intégrité des données. Il ne gère pas la récupération des données perdues **[5].**

I.4.Qualité de service

I.4.1.Paramètres de la qualité de service

La Qualité de Service ou (QoS) est la capacité à bien participer à un type de trafic fourni, en termes de :

- La disponibilité (accès à des services partagés).
- La vitesse (téléchargement ...).
- Le délai de propagation (pour les applications interactives ou téléphoniques).
- Le taux de perte de paquets (la perte n'a aucun effet sur la voix et la vidéo, mais est essentielle pour le téléchargement) **[9].**

a. Latence

La latence ou le délai de transmission indique le temps de transmission écoulé entre l'envoie et la réception d'un paquet de données. La transmission est subdivisée selon les délais suivants:

- **Le délai de transit :** il représente le temps nécessaire pour livrer le paquet de données au récepteur, et il se compose des éléments suivants:
- **Le délai de traitement :** il s'agit du temps nécessaire au routeur pour analyser les paquets de données à partir de l'interface entrante, les vérifier et les placer dans la file d'attente de l'interface sortante.
- **Le délai de la mise en file d'attente :** C'est le temps pour que le paquet passe par la file d'attente de sortie du routeur pendant sa durée de vie. Cela dépend du nombre et de la taille des paquets de données déjà dans la file d'attente d'envoi, de la bande passante de l'interface et du mécanisme de file d'attente utilisé.
- **Le délai de sérialisation :** c'est le temps de la mise de la trame sur le support de transmission.
- **Le délai de propagation :** Il s'agit de l'heure à laquelle la trame est mise en place sur le support de transmission.

b. La perte de paquets

La perte de paquets est un paramètre qui représente le pourcentage d'unités de données qui ne peuvent pas atteindre le récepteur dans un intervalle de temps donné. Cette perte de paquets est causée par la mémoire tampon complète (mémoire) de l'interface complète dans le routeur. Par conséquent, ils se débarrasseront d'un certain pourcentage de paquets entrants en fonction du seuil défini, libérant ainsi automatiquement la bande passante. S'il n'y a pas de moyen fiable de récupérer des paquets de données perdus, la perte de paquets de données IP provoquera une sensation d'interruption et de déconnexion de session.

c. La gigue

Il s'agit de la variation de bout en bout du délai de transmission (latence). En d'autres termes, cela est dû au fait que tous les paquets contenant des échantillons vocaux ne traverseront pas le réseau à la même vitesse. Cela peut provoquer une distorsion ou un hachage du son, compressant ainsi la gigue qui utilise généralement des tampons. Cela n'a rien à voir avec le temps d'expédition. La valeur de la gigue varie de quelques millisecondes à des dizaines de millisecondes.

d. La bande passante

La gestion de la bande passante permet de contrôler le trafic sur le réseau afin qu'il ne dépasse pas la capacité du réseau (risque de congestion du réseau). Grace à cette gestion, on peut également allouer de la bande passante pour certains types de trafic **[8].**

I.4.2. Méthodes de l'optimisation de la qualité de service

Après plus d'un siècle de service, les téléphones analogiques sont progressivement remplacés par une nouvelle génération de téléphones : VoIP.

Si un téléphone analogique convertit la voix en un signal électrique transmis via un réseau câblé de cuivre dédié, la VoIP emploie le réseau Internet pour transmettre son signal comme des données. Par rapport au fil de cuivre, la "Voix sur Internet" offre aux utilisateurs certains avantages (réduction des coûts, mobilité accrue, acheminement des appels amélioré, etc.). Cependant certains défauts de la qualité de service peuvent nuire à la voix sur IP: interruption de la communication, sons inaudibles, robotiques ou distants, fissures, coupures ...etc. Cinq solutions peuvent être envisagées pour améliorer la qualité de service sur ce type de réseau :

a) Vérification de la stabilité du réseau internet

L'instabilité du réseau entraîne des retards de communication, une perte de paquets ou une gigue. Pour vérifier l'état de la connexion, vous pouvez utiliser des outils en ligne, qui peuvent vous donner des résultats immédiats:

- **Fast.com:** Il s'agit d'un outil de mesure fourni par NetFlix.
- **TesDebit.fr:** fournit une analyse complète de votre réseau.
- **Speed test RingOver:** le propre outil de Ringover peut mesurer les données de base des appels VoIP.
- **La commande Ping**

Le Ping permet de mesurer le retard global de l'installation, c'est-à-dire le temps nécessaire à un paquet pour atteindre sa destination. Ce nombre doit être aussi bas que possible.

- **Le Jitter**

Le Jitter ou la gigue mesure l'irrégularité des paquets de données arrivant à la destination du même signal (à partir de la même conversation). Plus l'irrégularité est grande, plus les paquets de données seront perdus. Pour les appels VoIP de haute qualité, la gigue doit être inférieure à 20 millisecondes. Comparé au wifi ou à la 4G sur des réseaux moins stables (comme l'ADSL), Ethernet offre une meilleure expérience VoIP. En effet, la perte de données causée par le câble Ethernet est très faible (et peut être corrigée grâce au protocole Opus). Dans les connexions wifi et 4G, ces pertes sont généralement plus sévères, surtout lorsque l'appareil est éloigné du signal

b) Le Contrôle de la puissance de l'appareil

Les ombres ou les sons du robot dans la conversation peuvent également être causés par le fonctionnement lent de l'ordinateur. En effet, les applications VoIP nécessitent une certaine quantité de RAM pour fonctionner correctement, en particulier lors de l'utilisation simultanée d'autres logiciels

c) Le choix d'un casque performant

Si l'environnement de travail est bruyant (comme dans un centre d'appels, un espace ouvert ou un voyage d'affaires), la conversation peut être perturbée par le bruit ambiant. De plus, en utilisant le câble jack, le son peut être ressenti loin de l'enceinte

Il est ainsi fortement recommandé d'utiliser un casque USB (de préférence avec une option de réduction du bruit) pour assurer un appel confortable. Par exemple, dans un espace ouvert bruyant, les meilleurs écouteurs sont les écouteurs à réduction de bruit Jabra.

d) Vérification de la connexion internet côté utilisateur

Dans ce cas, s'il s'agit d'une mesure en temps réel, la cause du problème sonore peut être déterminée directement dans l'application.

e) Inspection de la technologie d'encapsulation de la voix de l'application VoIP (codec)

La qualité sonore dépend également du codec, qui est un appareil utilisé pour encapsuler les communications et transmettre sur Internet. Les opérateurs VoIP utilisent généralement d'anciens codecs (tels que G711 ou G729), qui sont très sensibles aux changements de la vitesse de connexion Internet, ce qui peut provoquer des coupures et des fissures. Ceux-ci consomment beaucoup de bande passante et le temps de réponse peut être plus long.

Afin de garantir la meilleure qualité sonore, nous recommandons que la bande passante de transmission dédiée à chaque utilisateur soit de 100 kbit et la bande passante de réception de 100 kbit **[10].**

I.4.3. Gestion de la qualité de service :

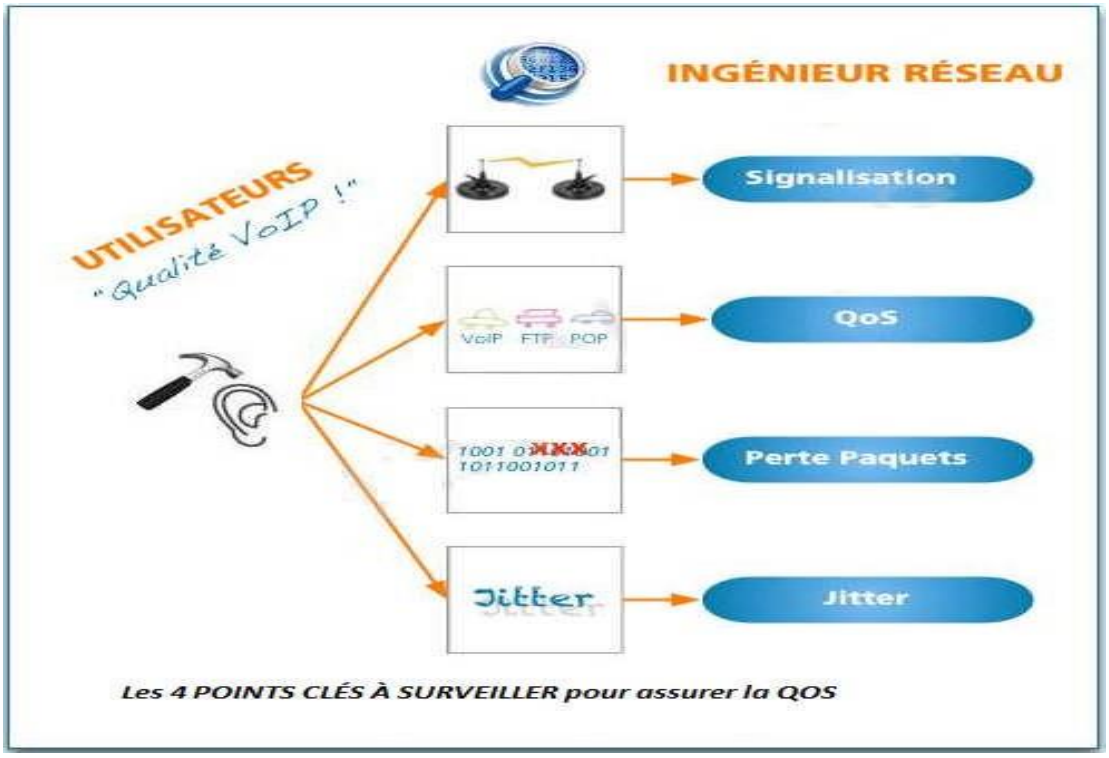

Figure I. 15.Les Quatres Points à surveiller pour assurer la Qos **[10]**

Comme la montre la figure ci-dessus, la première cause qui affecte la VoIP est liée aux problèmes de la signalisation. Par exemple, un signal SIP de type "appel occupé". La deuxième cause est en termes de QoS. En raison de la convergence des données vocales, les données peuvent être rassemblées dans différents segments du réseau. Un mauvais ajustement de la qualité de service affectera considérablement la qualité vocale des conversations des utilisateurs. La troisième cause est la perte de paquet de données entre l'expéditeur et le destinataire. Contrairement à d'autres protocoles moins sensibles, la perte de paquets de données dans un flux VoIP affectera immédiatement la qualité audio de la conversation.

Enfin, la quatrième cause est due à des changements dans le temps de transmission des paquets de données d'un téléphone à un autre, qui doit être réduit au minimum. L'utilisation correcte du tampon de gigue est essentielle.

Ces 4 indicateurs essentiels permettent une gestion sereine de la qualité sonore de la VoIP dans l'entreprise. Un système veillant au respect et au contrôle des quatre points cités repose sur :

a) **La classification:**
   Celle-ci est effectuée lorsque le routeur arrive au niveau du paquet permet de détecter le niveau de service, d'identifier le paquet reçu sur le nœud et de l'associer au micro flux. La classification est basée sur les caractéristiques suivantes (adresse source, adresse de destination, port source, port de destination et le type de protocole (UDP ou TCP)).
b) **Mesure :** Il est défini dans le routeur puis transmis au module de rejet de marquage et de mise en forme.
c) **Marquage :** Dans cette étape, le champ DSCP sera attribué et la priorité à appliquer à chaque flux sera sélectionnée. Si le flux dépasse le contrat SLA, le flux au-delà de ces priorités sera marqué comme niveau de priorité inférieur
d) **Lissage et rejet des paquets (shapper/drapper) :** Lorsque le SLA autorise le flux de classe, le lissage sera effectué. Lorsque le flux de paquets de données dépasse le contrat SLA, ces paquets de données seront rejetés **[10].**

I.5.Conclusion

La voix sur IP est l'une des plus éminentes évolutions dans le domaine des télécommunications et sans doute une solution assez avantageuse pour effectuer des conversations. Contribuant à l'aboutissement de l'implémentation mais aussi représente un atout concernant la fiabilité et le coût, chaque standard possède ses propres caractéristiques pour garantir une bonne qualité de service.

Néanmoins la normalisation n'a pas atteint la maturité suffisante pour sa généralisation au niveau des réseaux IP ce qui laisse à raisonner qu'une bonne qualité exige un investissement supplémentaire et minutieux pour garantir la continuité de service et de haute qualité. Suivant l'environnement du site à équiper de la VoIP, il s'impose de combiner les différents mécanismes et protocoles adéquats pour mettre en place une stratégie assurant la capacité à fournir un service conforme à des exigences en matière de temps de réponse et de bande passante.

CHAPITRE II :
MPLS
(Multiprotocol Label Switching)

II.1.Introduction

Ces dernières années, la multiplication des réseaux d'accès a marqué l'évolution des réseaux de télécommunications, de plus en plus de services Internet sont disponibles pour les particuliers et les petites entreprises (via l'accès aux connexions des fournisseurs, le travail à distance, les services à valeur ajoutée tels que la messagerie électronique, les serveurs Web hébergés, les VPN, etc.). Ce groupe de personnes, généralement appelé SOHO, est la cible des grands acteurs (opérateurs, constructeurs, etc.) de l'industrie des réseaux. Les tendances actuelles s'orientent vers la mutualisation de voix, données, vidéo.

Ceci est basé sur l'encapsulation de multiples protocoles de connexion des PC et des modems Cependant ces applications sont difficiles à mettre en place, à cause du travail de configuration et de formation des utilisateurs qui doit être assuré par les opérateurs En combinant la technologie VPN avec différents protocoles d'encapsulation, différentes propositions ont été avancées.

Tout cela a été accompagné d'une augmentation du trafic de données transitant par Internet. L'extension de la table de routage et le traitement de la taille du segment IP peuvent consommer beaucoup de ressources CPU, limitant ainsi la capacité du routeur et causant des problèmes avec l'architecture typique du réseau IP. Dans les réseaux IP traditionnels, les paquets de données sont acheminés en fonction de l'adresse de destination contenue dans l'en-tête de niveau 3. Chaque routeur détermine le saut suivant, puis interroge sa table de routage pour déterminer l'interface sortante à laquelle le paquet de données est envoyé. Le mécanisme de recherche de table de routage consomme du temps CPU et avec la croissance de l'échelle du réseau, la table de routage du routeur augmente également. Par conséquent, il est nécessaire de trouver un moyen plus efficace pour acheminer les paquets de données. C'est pour cette raison que la technologie MPLS semble être la solution la plus mature sur le marché aujourd'hui. La possibilité d'obtenir une QoS garantie contractuellement est un facteur important à prendre en compte par les décideurs. Nous verrons dans ce chapitre comment et pourquoi tout cela est possible.

II.2.Protocole MPLS

II.2.1.Définition

Le protocole MPLS, est une technologie de transmission de données pour les réseaux WAN à très hautes performances. Le MPLS s'appuie sur des labels pour transmettre les paquets d'un nœud à un autre, au lieu d'utiliser les informations contenues dans les en-têtes de la couche réseau et transport. Par conséquent, il évite la complexité que nécessite la recherche des routes dans les tables de routage, il simplifie également les décisions de qualité de service. Le MPLS peut encapsuler plusieurs protocoles réseau, d'où sa qualification comme un multi-protocole.

Le label inséré par le MPLS est échangé entre les routeurs, afin qu'ils puissent créer des mappages label-label. Ils sont attachés aux paquets de données IP. Cela permet aux routeurs de transmettre des

paquets de données uniquement en référence à l'étiquette du label sans voir le contenu du paquet de données. C'est ce qu'on appelle la commutation d'étiquettes au lieu du routage de couche réseau **[11].**

II.2.2. Évolution de l'IP vers MPLS

Dans le cadre du routage traditionnel, chaque routeur maintient un algorithme de routage de couche 3. Lorsqu'un paquet de données traverse le réseau, chaque routeur décide indépendamment d'envoyer le paquet de données. Le routeur utilise les informations contenues dans l'en-tête de paquet et les informations de routage obtenues à partir de la table de routage construite, pour sélectionner un "next-hop" avant d'envoyer le paquet.

Dans un réseau IP, ce processus consiste à faire correspondre l'adresse IP de destination stockée dans l'en-tête de chaque paquet avec le chemin le plus spécifique obtenue à partir de la table de routage IP. Dans un environnement traditionnel sans connexion, cette activité se reproduit à chaque nœud le long du chemin de bout en bout. L'analyse et la classification des en-têtes de couche 3 peuvent être gourmandes en ressources processeur.

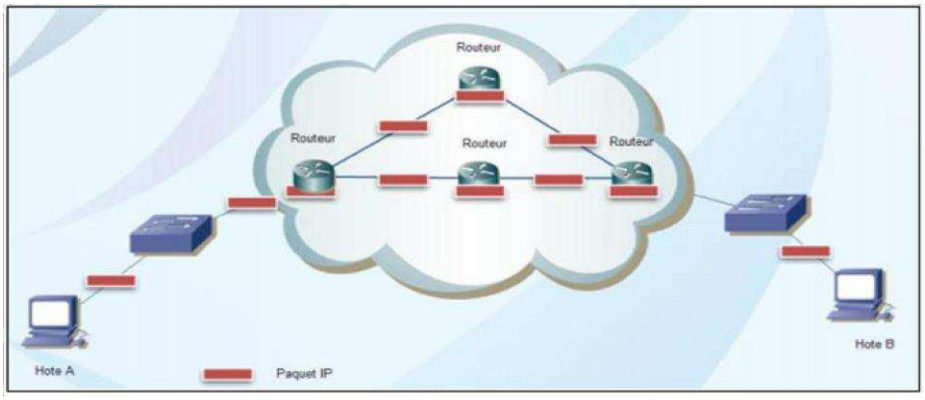

Figure II. 1.Modèle de routage IP **[12]**

Par conséquent, il est essentiel de trouver une méthode de transmission de paquets plus efficace. La technologie MPLS est une technologie qui détermine à l'avance le meilleur chemin à travers le réseau. Ensuite, lorsque le paquet de données est envoyé dans le réseau MPLS, le dispositif à la périphérie du réseau utilise les informations de l'en-tête de couche 3 pour attribuer le paquet de données à l'un des chemins prédéterminés. Cette affectation est utilisée pour ajouter des balises (également appelées étiquette, référence ou libellé). Lorsque le paquet de données traverse le réseau, le label sera envoyé avec le paquet de données.

Le routeur dans le chemin du paquet utilise les informations du label pour déterminer le routeur de saut suivant.

L'insertion de label se fait au dispositif à la périphérie du réseau, parce que le processus d'analyse et de classification de l'en-tête de la troisième couche se produit uniquement aux points d'entrée et de sortie de l'environnement MPLS **[12].**

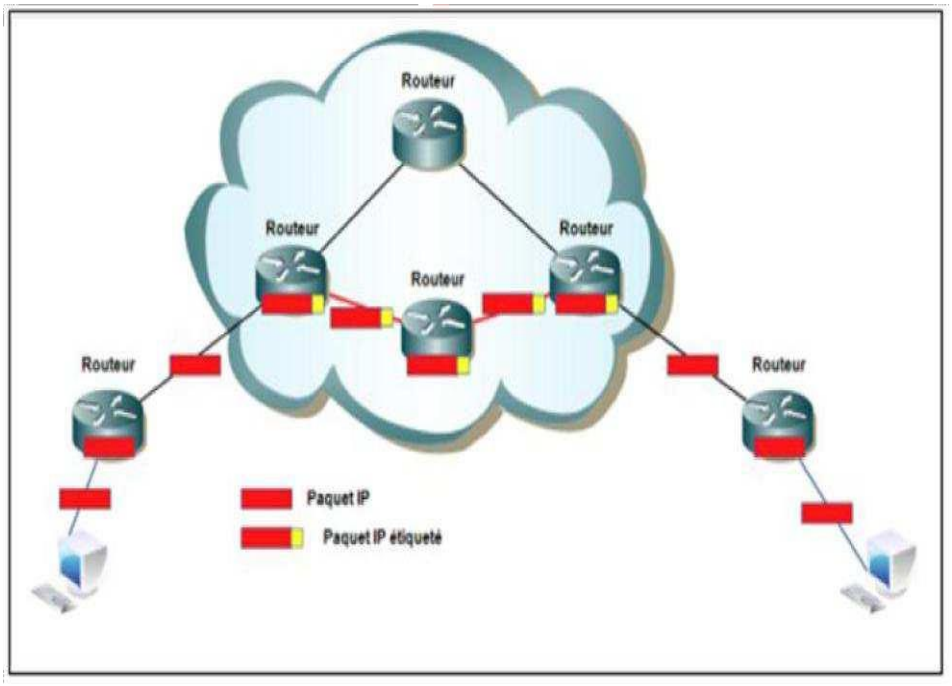

Figure II. 2. Routage IP où MPLS est appliqué **[12]**

II.2.3. Architecture du protocole MPLS

II.2.3.1 Structure fonctionnelle du protocole MPLS

Le protocole MPLS est fondé sur les deux plans suivants:

- **Le plan de contrôle**

Le plan de contrôle se compose d'un ensemble de protocoles de routage et de protocoles de signalisation classiques. Il est responsable de l'établissement, de la maintenance et de la distribution des tables de routage et des tables d'échange. Pour cela, le plan de contrôle utilise des protocoles de routage classiques tels qu'IS-IS ou OSPF pour créer une topologie de nœuds. Le protocole de signalisation est spécialement développé pour les réseaux MPLS, tels que LDP, MP-BGP ou RSVP.

Dans un réseau MPLS, on trouve deux méthodes pour créer et attribuer les étiquettes. Ces méthodes sont le «routage implicite» et le «routage explicite». Ces deux méthodes sont utilisées pour définir le LSP. La méthode du "routage implicite" est basée sur un routage saut par saut, où (hop by hop) contenant un LSP choisit indépendamment le prochain saut pour une FEC. Le routage explicite est la méthode où le premier routeur I-LSR détermine la liste des nœuds ou des routeurs LSR à suivre pour livrer le paquet.

- **Le plan de données**

Le plan de données permet de transporter les paquets étiquetés à travers le réseau MPLS en fonction des tables de commutation. Il s'agit du routage des données en ajoutant un en-tête aux paquets arrivant dans le domaine MPLS. Le plan de données est indépendant des algorithmes de routage et d'échange des labels utilise une table de commutation appelée LFIB pour transférer les paquets labélisés avec les étiquettes correctes. Cette table est renseignée par des protocoles d'échange d'étiquettes tels que le protocole LDP.

Selon les informations du label apprises par le protocole LDP, le routeur LSR construit deux tables, telles que LIB et LFIB. D'une manière générale, LIB contient toutes les étiquettes apprises des voisins LSR, tandis que LFIB est utilisé pour marquer l'échange réel de paquets. La table LFIB est un sous-ensemble de la base [LIB] **[13].**

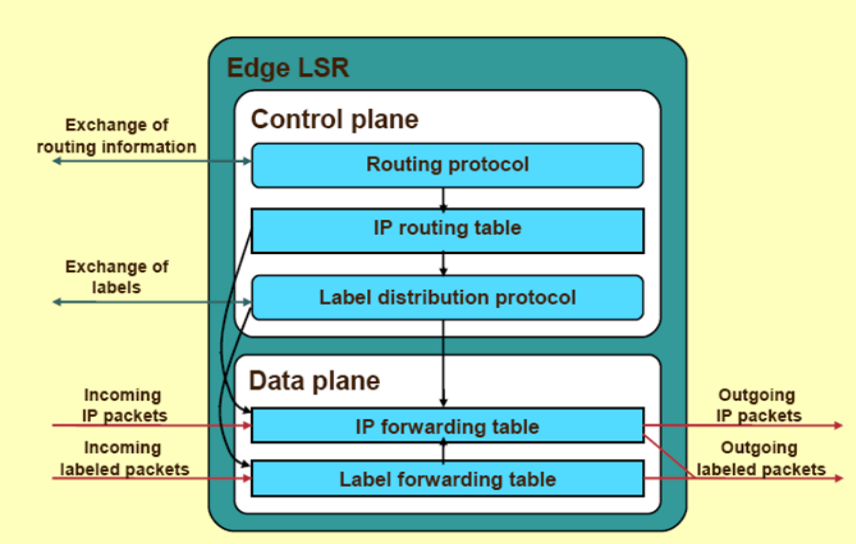

Figure II. 3.Architecture d'un routeur Edge LSR **[13]**

II.2.3.2.Les composants

II.2.3.2.1.format d'un label

Le label est un index codé de 32 bits inséré par le LER, qui identifie le chemin que le paquet de données doit suivre une fois qu'il entre dans le nuage MPLS. Le label est directement encapsulée et transmise dans le paquet de données, puis insérée entre

l'en-tête de niveau 2 (adresse MAC) et l'en-tête de niveau 3 (adresse IP). Chaque paquet de données doit suivre le processus basé sur le changement d'étiquette.

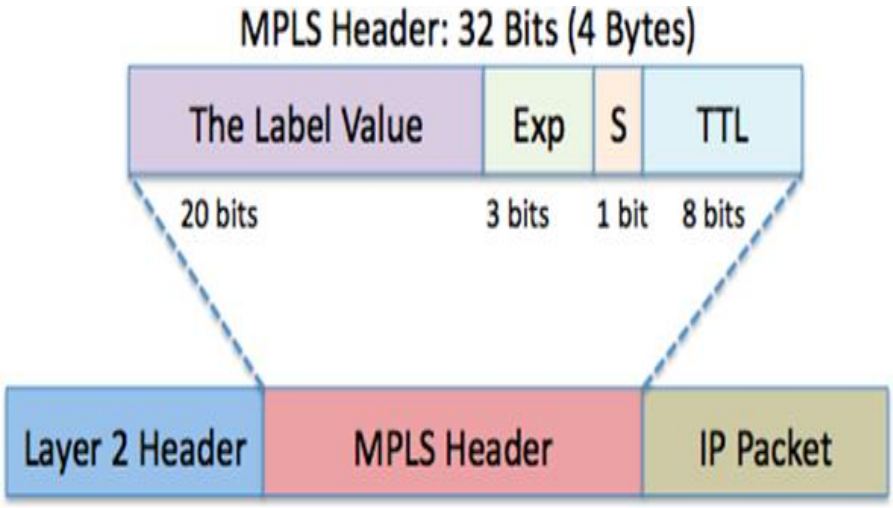

Figure II. 4.Format générique d'une étiquette MPLS **[14]**

- **LABEL :** A 20 bits, c'est le code binaire du label à convertir dans le domaine MPLS. La valeur attribuée au label correspond à la classe d'équivalence de transmission (FEC).

EXP : Sur 3 bits, c'est un champ expérimental qui n'a pas encore été normalisé et peut être utilisé pour gérer la qualité de service afin de coder le numéro de service.

- **EXP :** Sur 3 bits, c'est un champ expérimental, qui n'a pas encore été normalisé et peut être utilisé pour Gérer la qualité de service afin de coder le numéro de service.
- **STACK :** ce bit est utilisé pour spécifier si la balise est la dernière de la liste, parce que les étiquettes peuvent être empilées dans le même emballage. Par conséquent, il est nécessaire d'indiquer au routeur s'il y a d'autres balises à lire. Dans le cas courant d'une seule label, le bit sera positionné à 1.
- **TTL :** Sur 8 bits, le TTL représente le cycle de vie des paquets de données dans le nuage MPLS. Le TTL permet d'éviter les boucles sur le réseau

D'après le type de protocole de niveau 2 porté dans le paquet de données, le label est implémenté de différentes manières :

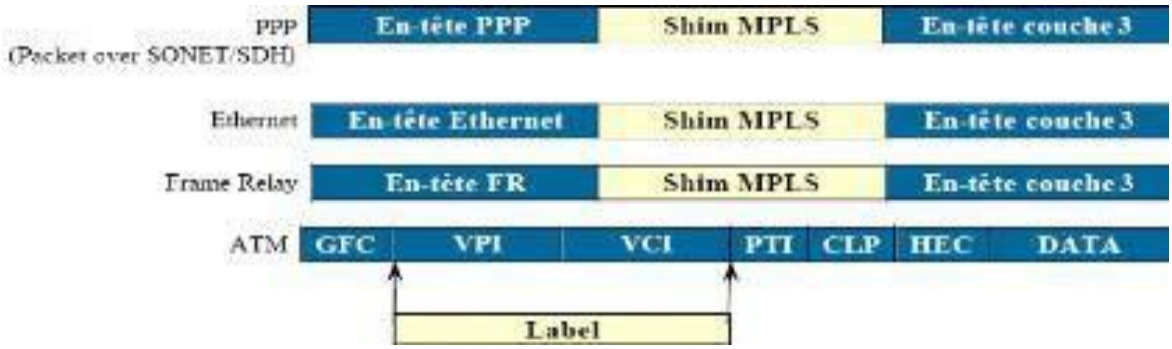

Figure II. 5.Encapsulation des labels dans des différentes trames **[14]**

Pour ATM, le label n'est pas inséré entre les en-têtes de niveau 2 et de niveau 3, mais Directement dans le champ VPI / VCI de la trame ATM.

FRAME RELAY, le principe est le même que ATM, le label est le même Inséré dans le champ DLCI de l'en-tête FR

Pour les protocoles Ethernet, HDLC et PPP contrairement aux protocoles ATM et FR, le label occupe un champ séparé et est ajoutée à la trame susmentionnée entre l'en-tête de deuxième niveau et le en-tête de troisième niveau **[14].**

II.2.3.2.2.Forward Equivalence Class (FEC)

Parler de changement de label est vraiment important car il s'agit de marquer (taguer) les trames IP afin que chaque nœud du réseau puisse les identifier. Dans la définition la plus stricte, ces balises sont considérées comme des identifiants de longueur fixe pour connaitre à quelle catégorie appartiennent le paquet de données. le label placée sur un paquet représente la classe équivalente de transmission (FEC) à laquelle il appartient, c'est-à-dire un groupe de paquets ou de trames qui les traitent. Par conséquent, les paquets de données appartenant à la même FEC utiliseront le même chemin dans le domaine MPLS. Cette opération n'est effectuée qu'une seule fois à l'entrée du réseau.

II.2.3.2.3.Label-Switched Paths (LSP)

Le LSP est une série de labels (ou d'étiquettes) insérées entre la couche 2 et la couche 3 de la couche OSI dans le paquet de données à transmettre. Il est unidirectionnel, ce qui signifie que le trafic de retour doit utiliser un autre LSP.

II.2.3.2.4.Label Edge Router (LER), Label Switching Router (LSR)

Dans un réseau MPLS, les paquets de données entrants se voient attribuer des étiquettes par des routeurs dédiés de type LER, qui peuvent prendre en charge plusieurs ports connectés à différents

réseaux (ATM, Frame Relay ou Ethernet). Ensuite, le paquet de données est envoyé via le chemin défini, et chaque routeur large bande situé au cœur du réseau MPLS de type LSR prendra une décision basée sur le contenu du label le long du chemin.

II.2.3.2.5.Label Information Base (LIB)

Chaque LSR construira lui-même une table pour comprendre comment transmettre les paquets de données. Cette table est appelée la base d'informations de label (LIB).

II.2.3.2.6.Label Distribution Protocol (LDP)

Le LDP est un protocole permettant d'apporter aux LSR les informations nécessaires d'association des labels dans un réseau MPLS. Il est également utilisé pour associer les labels aux FEC, ce qui crée des LSP**.**

Le LDP est un protocole permettant d'apporter aux LSR les informations nécessaires d'association des labels dans un réseau MPLS. Il est également utilisé pour associer les labels aux FEC, ce qui crée des LSP **[15].**

II.2.4. Principe de fonctionnement

Le MPLS est une technologie orientée connexion, elle est basée sur la commutation des étiquettes. Cela repose sur la transmission de données basée sur LSP et FEC, ces données sont gérées par LIB dérivé de LDP via LER et LSR. Le LSR et le LER sont des éléments physiques utilisés dans les réseaux MPLS. Les premier et dernier routeurs appelés routeurs de terminaux sont des LER et les LSR sont des routeurs au cœur du réseau MPLS. Le LER peut être connecté à un ou plusieurs réseaux de sortie différents, tels que ATM, relais de trame ou Ethernet, et ils jouent un rôle de base dans l'attribution et la suppression des étiquettes pour le trafic entrant et sortant du réseau MPLS **[12].**

II.2.5. Distribution des labels

L'attribution des labels au niveau du routeur fait partie du plan de contrôle, plus précisément de la signalisation. Cette attribution est effectuée par un protocole dédié, tel que le protocole LDP ou RSVP-TE. Ainsi que deux modes de distribution d'étiquettes peuvent coexister en un Domaine MPLS, ces modes sont cités ci-dessous :

- **Downstream on demande "aval à la demande" :** ce mode est appelé mode passif car seul le routeur upstream (routeur amont sur la source) data) trouvera un nouveau FEC, il établira une connexion avec le routeur en aval (le routeur en aval contribue à la source de données), et lui demandera de fournir le label correspondant au FEC trouvé.

Figure II. 6.Principe du Downstream on demande **[14]**

- **Unsolicited downstream "Aval non sollicité" :** ce mode est considéré comme proactif, car une fois que le routeur aval découvre un nouveau FEC et met à jour ses labels, il en informe le routeur upstream afin que ce dernier puisse mettre à jour sa table de commutation

Figure II. 7. Principe du Downstream unsolicited **[14]**

Chaque LSP transporte une ou plusieurs classes de flux, cette classe peut être définie en fonction de plusieurs paramètres qui relève généralement de la QoS. Les paquets ayant la même classe sont associés au même FEC, mais dans le cas où la QoS n'est pas spécifiée et lorsque un LSP est partagé par plusieurs éléments de FEC, ce LSP se termine au nœud (ou avant) où les éléments de FEC ne peuvent plus partager le même chemin. Pour cela le LDP spécifie précisément les paquets pouvant être transposés sur chaque LSP, en fournissant une spécification de numéro de FEC dans chaque LSP.

Le protocole LDP prend en charge deux méthodes de distribution d'étiquettes partagées Phase de découverte et d'établissement de la session LDP / TDP:

Un identifiant LDP (6 octets) est utilisé pour identifier un espace de label LSR, chaque routeur MPLS a un identifiant unique de 4 octets, et les deux autres sont utilisés pour identifier un espace de label spécifique dans le LSR.

LSR multidiffuse périodiquement le message "HELLO" en UDP contenant l'ID LSR sur le port 646. Lors de la réception du LSR pour établir une relation de voisin, il répond avec le même message "HELLO" pour confirmer l'existence, c'est la réunion du déclencheur LDP.

Une fois le voisin établi, une connexion TCP fiable est réalisée entre les deux pairs. C'est à partir de cette étape que la progression des deux modes a divergé, ou le mode "downstream en demande", le simple message "LABEL REQUEST" du LSR upstream est envoyé au LSR downstream, et le LSR downstream répond par le message

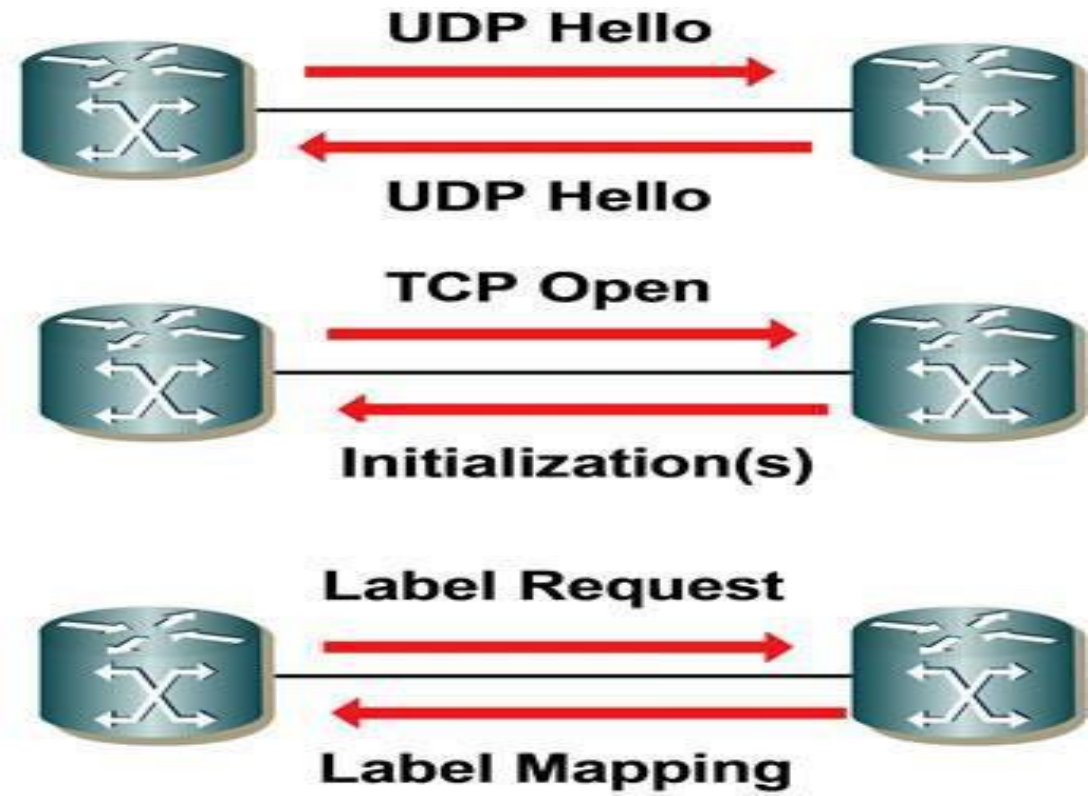

Figure II. 8.Session LDP en mode Dowenstream on demand **[14]**

Pour le mode " Unsolicited downstream ", une fois qu'une session LDP est établie, le LSR diffuse en multicast son " LABEL MAPPING " vers tous ses voisins (voisins qui ont des sessions LDP avec lui) **[14].**

II.3.VPN MPLS

Un réseau privé virtuel correspond à une connexion permanente, distante et sécurisée entre deux sites d'une organisation, qui autorise la transmission de données en toute sécurité. Il permet d'échanger des données entre deux sites distants sur un réseau partagé ou public dans un mode qui simule une liaison dédiée point à point.

Il est courant que les entreprises regroupent plusieurs emplacements géographiques (parfois loin) et elle espère interconnecter son réseau informatique via le WAN.

La solution la plus connue consiste à utiliser un lien dédié à l'entreprise pour se connecter au site. Cependant, le coût de ces liaisons est une éventuelle infaisabilité technique, par exemple, des sites séparés par des centaines de kilomètres ont conduit à rechercher des solutions plus abordables.

Les fournisseurs d'accès Internet disposent de réseaux fédérateurs étendus et couvrent la plupart du temps la majeure partie du territoire. Ainsi, les entreprises peuvent plus facilement lier leurs sites à ces réseaux fédérateurs et mettre en place des solutions VPN.

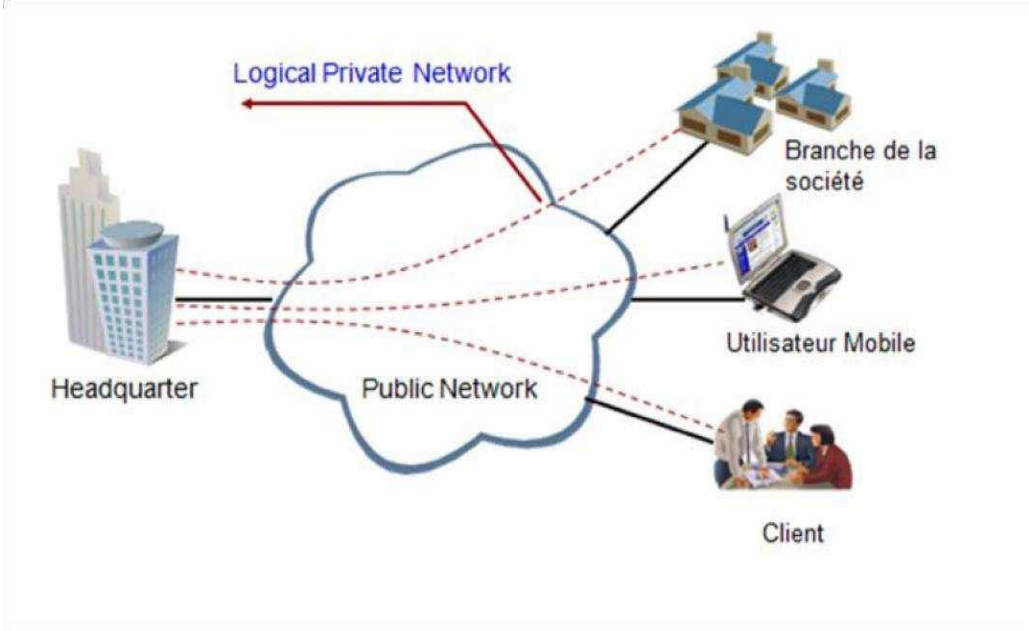

Figure II. 9.Schéma d'un accès VPN **[12]**

II.3.1. Principe de fonctionnement d'un VPN

Le réseau VPN peut isoler le trafic entre les sites qui ne font pas partie du même VPN, et est complètement transparent pour ces sites entre eux. Il est basé sur le principe du tunnel, permettant aux informations de l'entreprise de circuler en toute sécurité d'un bout à l'autre du tunnel sans qu'il soit

nécessaire de désigner explicitement un routeur intermédiaire. Cela donne aux utilisateurs l'impression qu'ils sont directement connectés à leur réseau d'entreprise. Les protocoles de tunneling (PPTP, L2TP, IPSec, etc.) permettent le chiffrement des paquets de données qui doivent être envoyés dans le tunnel. À la réception, le protocole de tunnelisation déchiffre le paquet, permettant l'accès au message d'origine, à la source et à d'autres informations.

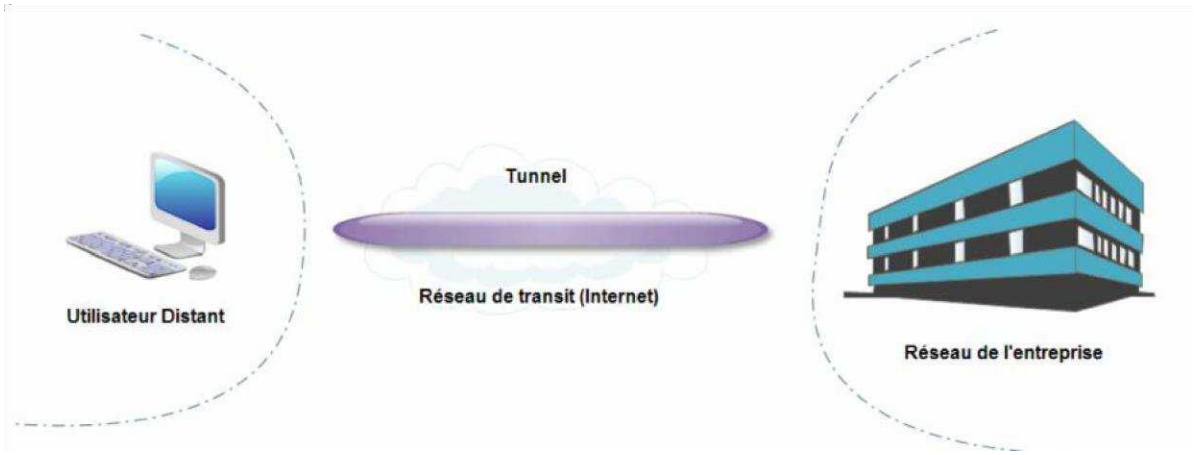

Figure II. 10.Tunnel dans VPN. **[12]**

II.3.2. Terminologies MPLS VPN

Dans un environnement MPLS VPN, le nom du routeur est différent du nom utilisé dans le réseau MPLS, en fonction de son rôle

II.3.2. 1.Routeur P

Les routeurs P (*Provider*) constitue le cœur du réseau dorsal MPLS et ne connaît rien au concept de VPN. Ils acheminent simplement les données via la commutation d'étiquettes.

II.3.2. 2.Routeur PE

Les routeurs PE (*Provider Edge*) se trouvant à la frontière du réseau Backbone MPLS et ont par définition une ou plusieurs interfaces connectées au routeur client Routeur CE

II.3.2. 3.Routeur CE

Les routeurs CE (*Customer Edge*) appartiennent au client et n'ont aucune connaissance des VPN ou même de la notion de label. Tout routeur peut être un routeurCE.

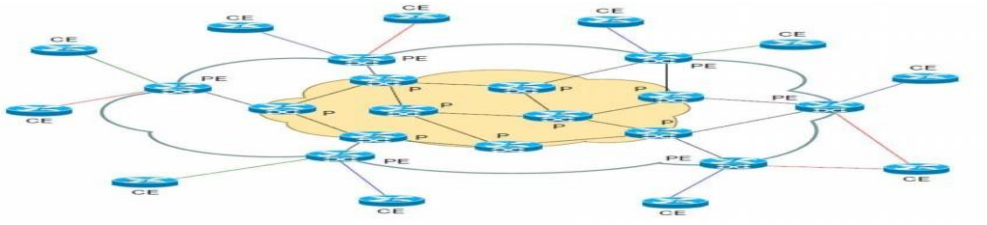

Figure II. 11.Positionnement des routeurs P, PE et CE dans un réseau MPLS **[12]**

II.3.3.L2VPN

L'architecture de MPLS L2VPN peut être divisée en AC, VC et Tunnel.AC est un lien ou un circuit indépendant reliant CE et PE. CA peut être une interface physique ou une interface virtuelle. Les attributs AC incluent des paramètres d'interface, tels que le type d'encapsulation, la MTU et le type de lien spécifié. VC fait référence à la connexion logique entre deux PE.

L2VPN est construit avec pseudowire (PW). Cette technologie fournit un format intermédiaire commun pour la transmission de plusieurs types de services sur le réseau à commutation de paquets (PSN). Le tunnel est utilisé pour transmettre de manière transparente les données utilisateur. Les tunnels couramment utilisés dans la technologie VPN MPLS sont:

- **Tunnel LSP**

Le LSP transmet des paquets de données par commutation d'étiquettes. Si le tunnel LSP est utilisé, l'en-tête IP n'est analysé que sur le PE, pas sur chaque périphérique à travers lequel le paquet VPN passe.

- **Tunnel MPLS TE**

Le tunnel, comme la combinaison de la technologie MPLS et TE, aide à équilibrer le trafic réseau en établissant des tunnels LSP le long des nœuds désignés et en supprimant les nœuds encombrés.

- **Tunnel GRE**

Cependant, si le PE prend en charge la fonction MPLS, le dispositif central du réseau CORE, à savoir P, ne fournit que des fonctions IP pures, et le LSP ne peut pas agir comme un tunnel. Dans ce cas, GRE peut être utilisé comme tunnel VPN backbone

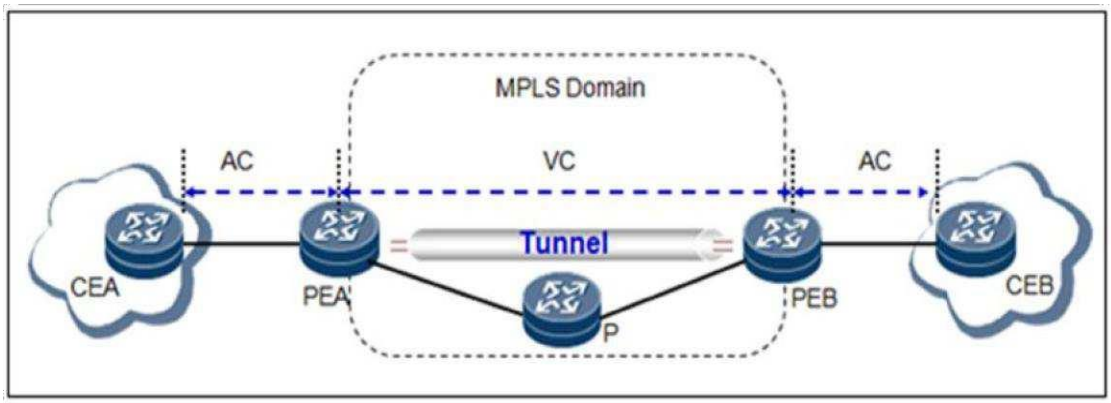

Figure II. 12.Architecture du MPLS L2VPN **[12]**

II.3.3.1.Virtual Private Wire Service VPWS

VPWS est un service point à point. Dans VPWS, deux sites peuvent communiquer comme s'ils étaient directement liés par un lien. Cependant, au niveau du fournisseur de services, plus de deux sites ne peuvent pas communiquer en même temps. PE fournit une interconnexion logique, de sorte qu'une paire de CE semble être reliée par un seul circuit logique de couche 2.

PE agit comme un commutateur de circuit de couche 2 et mappe ensuite ces circuits aux tunnels du réseau SP. Ces tunnels peuvent être spécifiques à un VPWS particulier, ou ils peuvent être partagés entre plusieurs services. VPWS peut prendre en charge plusieurs services, tels qu'Ethernet,

Chaque PE, comme ATM et Frame Relay, est responsable de l'attribution des trames VPWS appropriées pour une transmission correcte vers la destination prévue. Le pseudo-fil est une connexion entre deux PE, utilisée pour connecter deux services de terminal pseudo-fil (PWES)

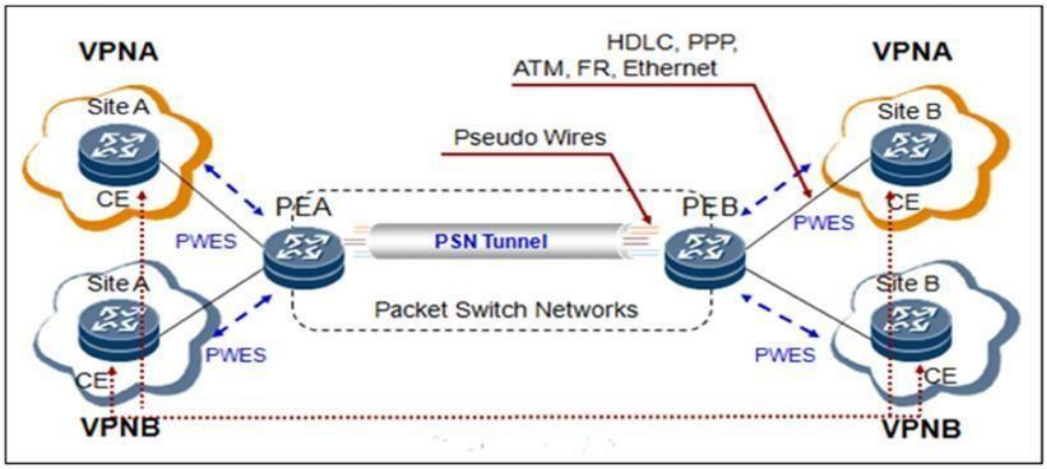

Figure II. 13.Fonctionnement d'un VPWS. **[12]**

*II.3.3.2.*Virtual Private LAN Service VPLS

VPLS est également connu sous le nom de service LAN transparent ou de service de réseau privé virtuel commuté (VPSNS). Contrairement à VPWS, VPLS permet aux fournisseurs de services de fournir des services Ethernet point à multipoint aux clients via le réseau dorsal MPLS. Le réseau pseudowire est utilisé pour connecter tous les PE qui prennent en charge un VPN VPLS donné.

Dans VPLS, chaque CE a une ou plusieurs interfaces LAN, qui conduisent au "Backbone virtuel". Deux CE sont connectés au même réseau dorsal virtuel si et seulement s'ils sont membres de la même instance VPLS (le même VPN). Lorsque le CE transmet une trame, le PE récepteur vérifie le champ d'adresse MAC de destination pour déterminer comment transmettre la trame.

Du point de vue du client, toutes les CE semblent être connectés à un commutateur public.

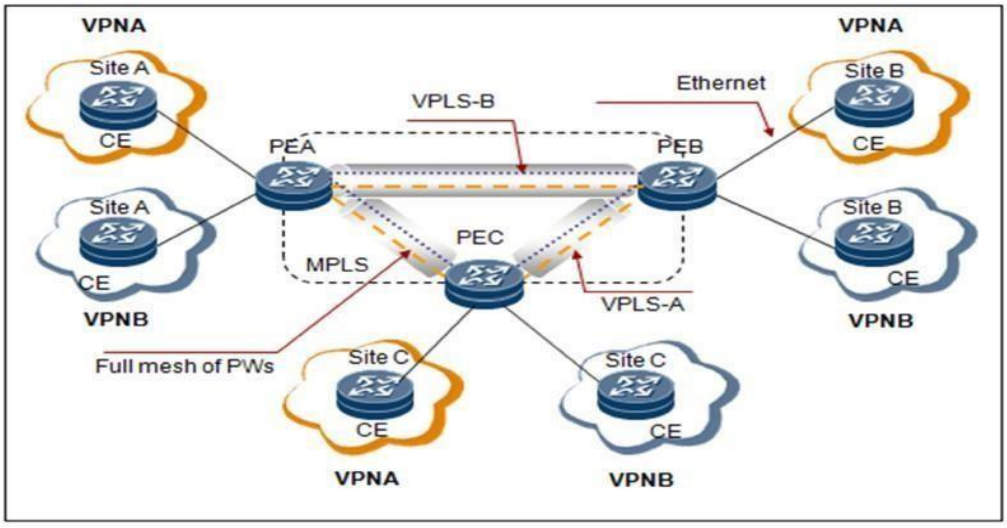

Figure II. 14.Fonctionnement d'un VPLS **[12]**

II.3.4.MPLS L3VPN

MPLS VPN BGP est une technologie VPN à trois couches qui utilise BGP pour distribuer des routes VPN et MPLS pour transférer des paquets VPN vers le réseau fédérateur du fournisseur de services (SP). MPLS VPN BGP est de plus en plus utilisé en raison de son évolutivité et de sa flexibilité et permettant au SP de déployer MPLS QoS et MPLS TE. MPLS VPN BGP a de nombreuses applications complexes, telles qu'Inter-AS MPLS BGP VPN, HoVPN, etc.

MPLS L3VPN est composé d'un routeur CE, d'un routeur PE et d'un routeur P. PE et P sont situés dans le réseau de l'opérateur.

Le réseau d'utilisateurs se compose de sites VPN situés à différents endroits géographiques. Chaque site VPN est connecté au réseau via un routeur CE, et chaque CE est connecté au PE via une liaison unique ou une liaison double.

Un VPN est généralement attribué aux sites des utilisateurs à différents endroits pour leur permettre de communiquer. Cependant, MPLS L3VPN peut également isoler un site, ou au contraire, distribuer un accès mutuel entre plusieurs sites.

MPLS L3VPN a une forte flexibilité d'isolation des utilisateurs, qui peut répondre aux exigences de sécurité de service et à un réseau flexible

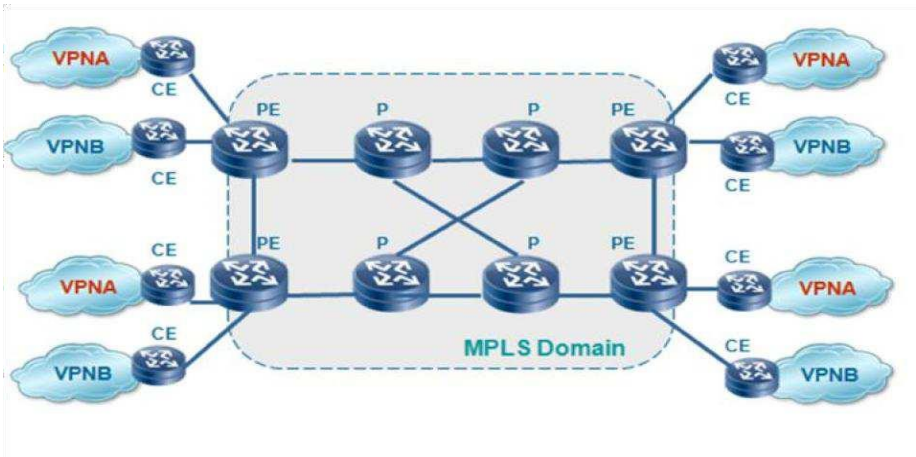

Figure II. 15.Architecture du MPLS L3VPN **[12]**.

II.3.4.1.Routeurs virtuels (VRF)

Le concept de VPN consiste à isoler le trafic entre les sites clients qui ne font pas partie du même VPN. Afin de réaliser cette séparation, les routeurs PE peuvent utiliser le concept de VRF pour gérer plusieurs tables de routage. VRF se compose d'une table de routage spécifique, de tables FIB et FEC, indépendantes des autres VRF et tables de routage. Chaque VRF est spécifié par le nom sur le routeur PE. Le nom est attribué localement et n'a aucune signification pour les autres routeurs... Chaque interface PE connectée au site client est connectée à un VRF spécifique. Lors de la réception d'un paquet IP sur l'interface client, le routeur PE vérifie la table VRF connectée à l'interface, donc il ne fait pas référence à sa table de routage globale. La possibilité d'utiliser plusieurs tables de routage indépendantes permet de gérer le plan d'adressage à travers le site.

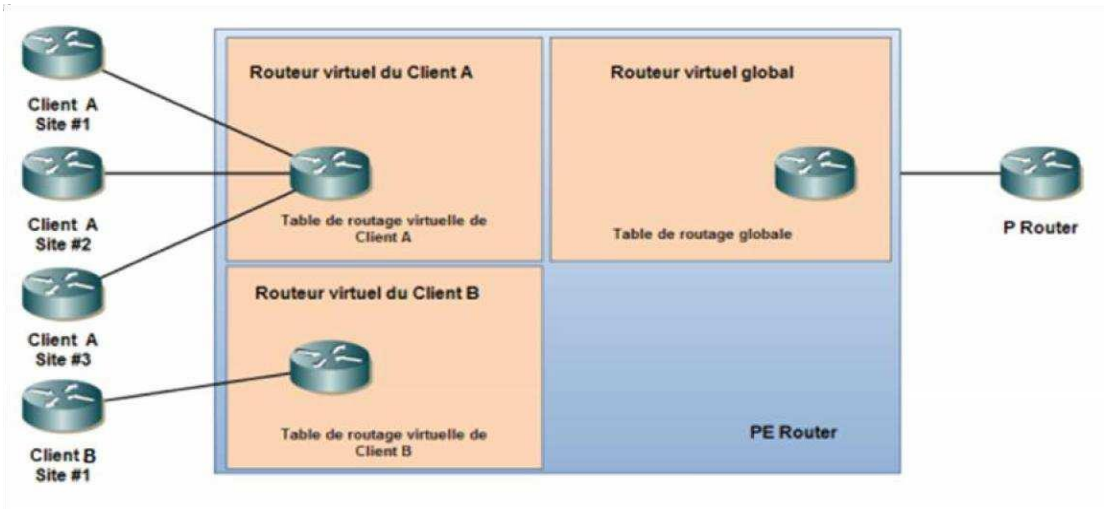

Figure II. 16.Utilisations des tables de routage virtuelles par le PE. **[12]**

II.3.4.2.Multiprotocol BGP

Afin d'acheminer correctement les paquets de données destinés à être connectés au routeur PE-1 sur le site CE-1, le routeur PE-2 échange des routes correspondant à différents VPN pour construire sa table VRF et connaître la route VPN du PE -router. 1. Utilisez le protocole MP-BGP, pour échanger des routes VPN. Le protocole MP-BGP est une extension du protocole BGP 4 et permet l'échange de routes multicast et de routes VPNv4. MP-BGP utilise des termes similaires à BGP en termes de peering:

- ✓ **MP-iBGP:** entre routeurs dans le même AS.
- ✓ **MP-eBGP:** situé entre les routeurs de 2 AS différents.

II.3.4.3.Route Distinguisher RD

Lors de la création d'un VRF sur PE, RD doit être configuré. Par conséquent, la route locale (route statique, bouclage sur PE) ou la route apprise par le CE connecté au PE sera dérivée dans la mise à jour MP-BGP avec ce RD.

Grâce à RD, les sites appartenant à des VPN différents pourront utiliser le même plan d'adressage. Par conséquent, les routes échangées entre les PE sont uniques en termes de mises à jour BGP. Cependant, il est recommandé de choisir le RD de VRF

- **VPNv4**

Les routeurs PE ont des informations de routage spécifiques à chaque CE. Ces informations contiennent l'adresse IPv4, qui est convertie en une adresse VPNv4 en ajoutant RD. Si plusieurs VPN utilisent la même adresse IPv4, le PE la convertira en une adresse VPNv4 unique.

VPNv4 est une adresse de 12 octets qui commence par 8 octets du Route Distinguisher attaché à chaque adresse de sous-réseau IPv4 (4 octets) d'un VRF donné.

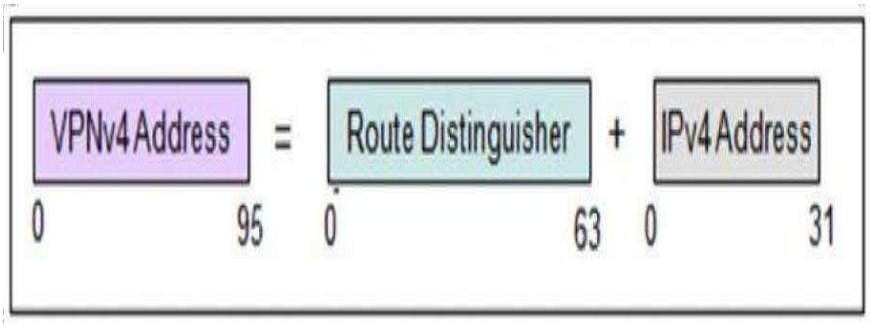

Figure II. 17.Adresse VPNv4. **[12]**

II.3.4.4.Route Target RT

RD garantit l'unicité des routes VPNv4 échangées entre les PE, mais ne définit pas comment les routes seront insérées dans le VRF du routeur PE. RTs (Route Target) est une communauté étendue de BGP qui n'est rien de plus qu'un filtre appliqué au routage VPNv4.

Chaque route VPNv4 est associée à une ou plusieurs cibles de route d'exportation. Le PE de sortie utilise la "cible de route d'importation" pour déterminer si la route reçue du PE d'entrée peut être placée dans le VRF

La cible de routage d'importation est configurée dans chaque VRF. Si cible de routage d'importation Correspondant à la cible de la route d'exportation, le routage est configuré dans VRF.

II.3.5.Protocoles utilisés

II.3.5.1. Protocole OSPF

Si cible de routage d'importation Correspondant à la cible de la route d'exportation, le routage est configuré dans VRF OSPF (Open Shortest Path First) est un protocole de routage d'état de lien interne (LSRP), ce qui signifie que chaque routeur transmet son état de lien pour mapper l'état du réseau et ensuite construire sa table de routage.

Cette méthode a été créée par l'IETF en 1988 et est actuellement l'IGP plus commun. Les principales caractéristiques d'OSPF :

- L'émission de mises à jour déclenchées par des changements de topologie.

- La connaissance précise et complète de la topologie du réseau.

- Chaque nœud connaît l'existence de ses voisins à condition de :

  - ✓ avoir le même masque de sous-réseau.
  - ✓ se situe dans la même zone.
  - ✓ Avoir la même clé d'authentification OSPF.
  - ✓ Avoir la même minuterie (Hello time et dead time).
  - ✓ Utiliser l'arbre du chemin le plus court en premier (arbre SPF et algorithme du premier chemin le plus court SPF) également connu sous le nom d'algorithme de Dijkstra pour calculer le meilleur chemin en termes de coût pour générer sa table de routage.

- Envoyer des mises à jour de topologie via des adresses de multidiffusion et de non-diffusion.

- Réduire l'utilisation de la bande passante.

- Besoin d'un routeur plus puissant.

- Métriques utilisées: le coût (chaque lien a un coût) est calculé de la manière suivante:

  - Coût = référence / bande passante.

Sachez que la valeur de référence par défaut est de 100 000 [Kb / s]. Le but est de choisir le bon chemin caractérisé par la plus petite métrique.

- Protocole en couches: offre la possibilité de diviser le réseau en d'autres sous-réseaux, ce que l'on appelle la zone peut contenir plusieurs routeurs

II.3.5.2.BGP

BGP est un protocole utilisé pour échanger des informations de routage entre pairs (pairs adjacents) dans un réseau de système autonome. Un système autonome est un réseau ou un groupe de réseaux avec les mêmes règles de routage (par exemple, le réseau d'un fournisseur de services Internet). BGP est généralement un protocole utilisé entre les hôtes de passerelle sur Internet. Cette La table de routage contient une liste de routeurs connus, les adresses qu'ils peuvent atteindre, Ainsi qu'une métrique associée au chemin de chaque routeur afin de sélectionner le meilleur chemin disponible.

Un hôte utilisant BGP utilise le protocole TCP pour communiquer uniquement lorsque l'hôte détecte une modification et envoie des mises à jour à sa table de routage. Seule la partie affectée de la table de routage est envoyée.

BGP est un PVP, qui maintient les chemins de différents hôtes, réseaux et routeurs de passerelle, et détermine les décisions de routage en fonction de ceux-ci. Il n'utilise pas les métriques IGP pour prendre des décisions de routage, mais détermine uniquement le routage en fonction des chemins et des politiques réseaux.
La dernière version de BGP-4 permet aux administrateurs de déclarer et de configurer des indicateurs de coût en fonction des politiques de routage. **[12]**

II.4. Ingénierie du trafic (TE)

Désigne toutes les technologies qui optimisent l'utilisation des ressources réseau en tenant compte de la bande passante disponible sur la liaison dans le processus de routage pour éviter la congestion. Ceci est dû à l'algorithme spécial CSPF (Constrained Shortest Path First), car ce dernier permet de reconstruire la topologie du réseau en fonction des contraintes de bande passante, réduisant ainsi au maximum la congestion et optimisant le trafic.
Cet algorithme a été implémenté par de nombreux protocoles existants, tels que:

- Routage: évoluer vers ISIS-TE et OSPF-TE comme ISIS et OSPF.
- Signalisation (réservation de bande passante sur les routeurs): RSVP évolue vers RSVP-TE **[14].**

II.6.Conclusion

Le MPLS apporte les avantages d'un mode de connexion non orienté connexion au protocole IP, et en même temps préservant la souplesse de routage, il permet également : De réduire le temps de transport réseau, concurrent des routeurs gigabit (voire Tera) actuels ; ingénierie du trafic, permet la haute disponibilité et la prévention de la congestion dans les réseaux IP ; environnement la mise en œuvre de la QoS permet de fournir des services vocaux de haute qualité et une gestion flexible sur les réseaux IP VPN.
MPLS améliore les performances du réseau et fournit une qualité de service, De plus, il peut utilisez n'importe quel protocole de couche 2.
Puisque les réseaux IP/MPLS existent dans tous les domaines, ils ont un bel avenir.
Réseau d'opérateurs. En effet, ces réseaux permettent de faire face aux limitations suivantes:
Un protocole de routage IP pur qui met en œuvre le principe d'échangeTags, ces réseaux sont aussi des solutions prometteuses car ils permettent l'intégration.

Nouvelles technologies simples basées sur la virtualisation des services réseau, telles que VPLS, pour offrir aux clients des remises virtuelles. Par conséquent, la virtualisation est innover les concepts de base des réseaux d'opérateurs, Le MPLS semble intéressant comme future technologie L'unité, et beaucoup de travail est fait pour faciliter les choix.

Grâce à son mécanisme avancé de commutation d'étiquettes et à sa simplicité lorsqu'il est mis en œuvre sur des réseaux existants, MPLS est devenu la technologie phare du futur allie flexibilité, évolutivité et performance, baisser le coût.

CHAPITRE III
Simulation sous GNS3

III.1.Introduction

Nous avons créé un modèle à l'aide de l'émulateur GNS3 de Cisco pour simuler une solution VoIP sur MPLS.

III.2.Choix des outils de simulation

Il existe de nos jours différents toute une panoplie de logiciels de simulation de réseau, bien que quelques-uns prennent en charge la mise en œuvre de l'architecture MPLS, c'est pourquoi notre choix se base principalement sur GNS3.

III.2.1. Présentation du logiciel GNS3

Le logiciel GNS3 est rien qu'en fait l'interface graphique de l'outil Dynamips sous-jacent, qui peut émuler une machine virtuelle Cisco. Il faut insister sur le terme émulation, car ces machines s'appuient sur le véritable IOS fourni par Cisco, elles disposent donc de toutes les fonctions d'origine.

Par conséquent, le logiciel peut être opposé à Packet Tracer, qui est un simulateur fourni par Cisco dans le cadre de son programme académique et est donc limité aux fonctions mises en œuvre par les développeurs de logiciels. Les performances des machines ainsi créées ne sont certes pas à la hauteur des vraies machines physiques, mais elles sont tout de même suffisantes pour mettre en œuvre des configurations relativement basiques et appréhender les concepts de base des équipements Cisco.

il se compose de :

GNS3 représente une interface graphique, permettant d'établir des liens entre plusieurs autres programmes et des présentations conviviales. Les principales procédures sur lesquelles GNS3 est basé sont

• Dynamips : émulateur Cisco IOS.

• Dynagen : L'interface texte de Dynamips.

• Qemu : émulateur système général (utilisé pour simuler ASA, PIX, JunOS ou IDS).

• Vmware : un puissant simulateur de système (utilisé pour simuler les systèmes d'exploitation Windows ou Linux).

De plus, certains utilitaires utiles sont distribués avec le programme d'installation de GNS3 notamment

• Putty : afin de se connecter aux systèmes émulés en console série ou SSH/telnet.

III.3.Description du modèle

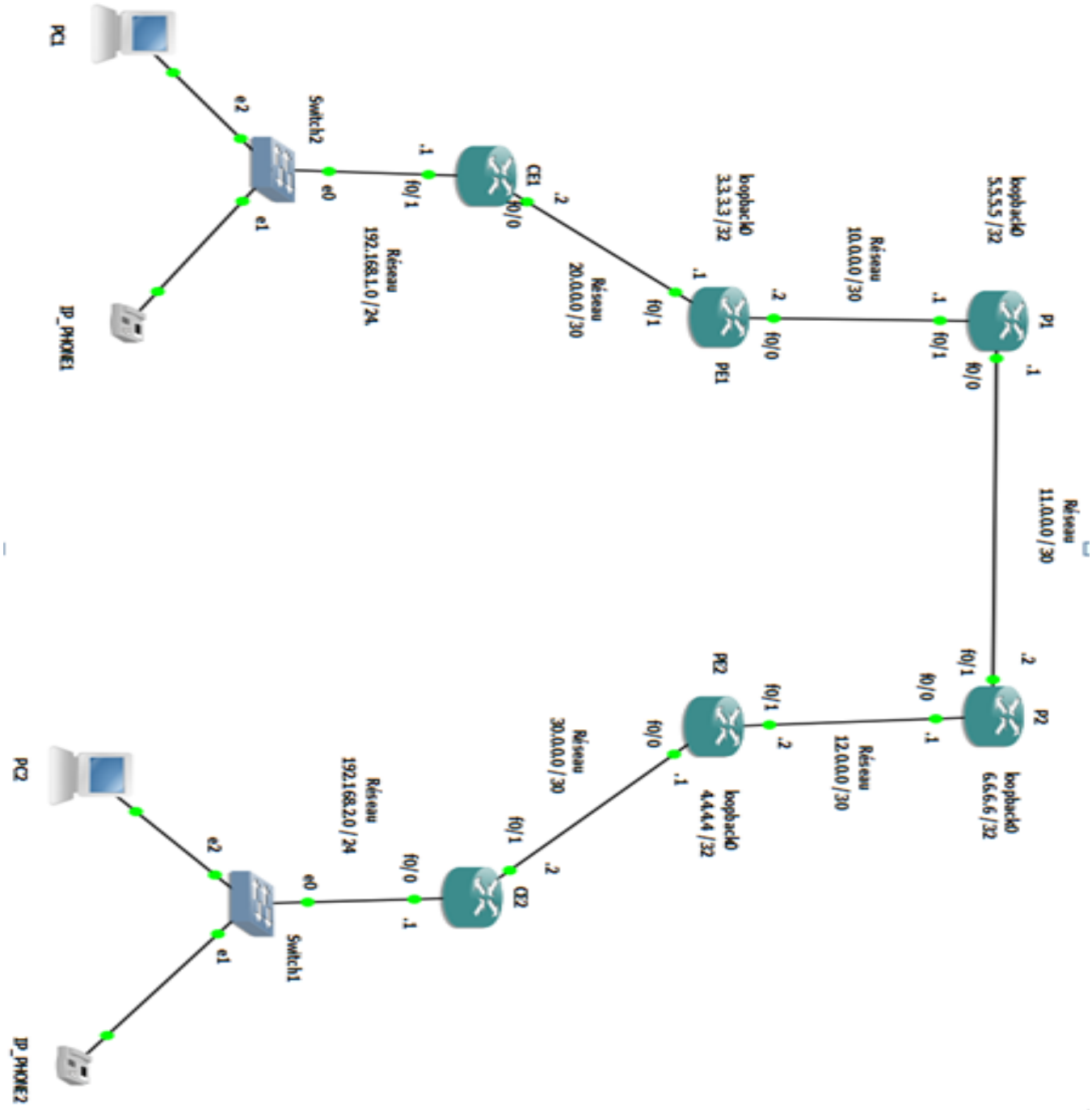

Figure III. 1.Schéma du modèle réalisé

- La figure ci-dessus est l'architecture que l'on a utilisée dans tout le long de ce chapitre.

Elle est composée de :

- 2 Routeurs représentant le CORE MPLS **(P1, P2)** ;
- 2 Routeurs représentant l'Edge MPLS **(PE1, PE2)** ;
- 2 Routeurs représentants les clients **(CE1, CE2)** ;
- 2 Switch Ethernet **(Switch1 et Swich2)** ;
- 2 PC **(PC1et PC2)**
- 2 IP Phones **(IPPhone1 et IPPhone2)** ;

- Nous avons choisi pour ce modèle les technologies suivantes:

  - OSPF pour la communication intra-nuage
  - RIP en guise de protocole CE-PE.
  - MP-BGP pour le VPN

- **Plan d'adressage :**

Routeur	**Interface**	**Adresse IP**	**Masque**
CE1	F0/0	20.0.0.2	255.255.255.252
	F0/1	192.168.1.1	255.255.255.0
CE2	F0/0	192.168.2.1	255.255.255.0
	F0/1	30.0.0.2	255.255.255.252
PE1	F0/0	10.0.0.2	255.255.255.252
	F0/1	20.0.0.1	255.255.255.252
	Loopback0	3.3.3.3	255.255.255.255
PE2	F0/0	30.0.0.1	255.255.255.252
	F0/1	12.0.0.2	255.255.255.252
	Loopback0	4.4.4.4	255.255.255.255
P1	F0/0	11.0.0.1	255.255.255.252
	F0/1	10.0.0.1	255.255.255.252
	Loopback0	5.5.5.5	255.255.255.255
P2	F0/0	12.0.0.1	255.255.255.252

	F0/1	11.0.0.2	255.255.255.252
	Loopback0	6.6.6.6	255.255.255.255

Figure III. 2.Plan d'adressage

III.4.Configuration et simulation

III.4.1.Configuration de MPLS/VPN

III.4.1.1 .Configuration des adresses IP sur les interfaces des routeurs

```
PE1(config)#int f0/0
PE1(config-if)#ip address 10.0.0.2 255.255.255.252
PE1(config-if)#no shutdown
PE1(config-if)#exit
PE1(config)#int f0/1
PE1(config-if)#ip address 20.0.0.1 255.255.255.252
PE1(config-if)#no shutdown
PE1(config-if)#exit
PE1(config)#int loopback 0
PE1(config-if)#ip address 3.3.3.3 255.255.255.255
PE1(config-if)#no shutdown
PE1(config-if)#exit
```

Figure III. 3.Configuration des adresses IP sur le routeur PE 1

On exécute les mêmes démarches de configuration sur les routeurs : CE1, CE2, P1, P2, PE2.

III.4.1.2.Configuration du protocole OSPF dans le nuage MPLS

On active le protocole OSPF sur les routeurs : PE1, P1, P2, PE2

```
PE1(config)#router ospf 1
PE1(config-router)#network 10.0.0.0 0.0.0.3 area 0
PE1(config-router)#network 3.3.3.3 0.0.0.0 area 0
```

Figure III. 4.Configuration OSPF sur le routeur PE 1

On exécute les mêmes démarches de configuration sur les routeurs P1, P2, PE2.

On a fait un ping du routeur PE1 vers le routeur PE2 pour tester la bonne configuration du protocole OSPF

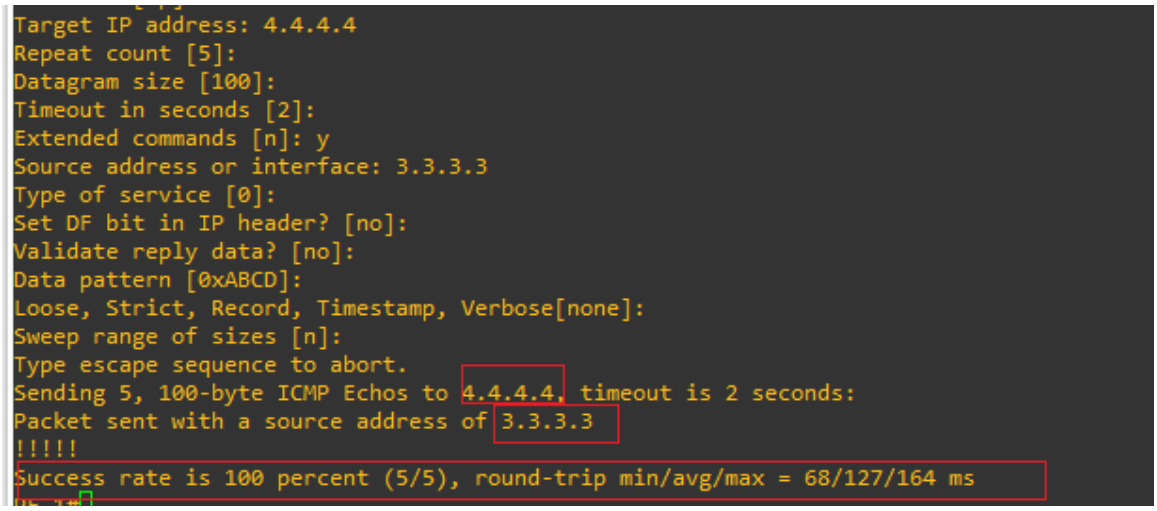

Figure III. 5.Ping du PE1 vers PE2

III.4.1.3.Configuration du protocole RIP

On active le protocole RIP avec les routeurs : CE1,CE2 , PE1, PE2

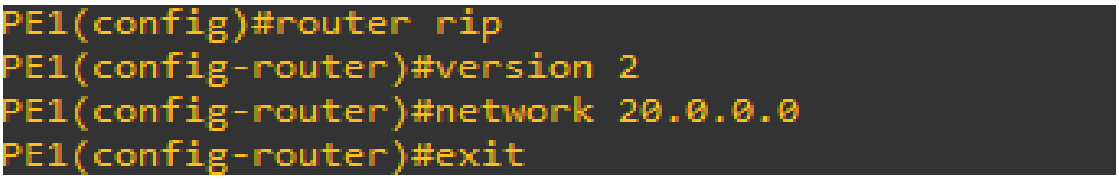

Figure III. 6.Configuration RIP sur le router PE1

On exécute les mêmes démarches de configuration sur les routeurs : CE1, CE2, PE2.

III.4.1.4.Activation du MPLS

Nous allons dès à présent configurer MPLS dans le backbone par son activation sur toutes les interfaces des routeurs P du fait qu'elles sont toutes interconnectées avec le réseau MPLS en ce qui concerne les routeurs PE il faut uniquement le déclarer sur les interfaces interconnectées avec ce réseau.

```
PE1(config)#ip cef
PE1(config)#int f0/1
PE1(config-if)#mpls ip
PE1(config-if)#mpls label protocol ldp
PE1(config-if)#exit
```

Figure III. 7.Activation du MPLS. Sur le Router PE1

On exécute les mêmes démarches de configuration sur les routeurs : P1, P2, PE2.

III.4.1.5.Configuration de MP-BGP sur les routeurs PE1 et PE2

```
PE1(config)#router bgp 700
PE1(config-router)#neighbor 4.4.4.4 remote-as 700
PE1(config-router)#neighbor 4.4.4.4 update-source loopback 0
PE1(config-router)#address-family vpnv4
PE1(config-router-af)#neighbor 4.4.4.4 activate
PE1(config-router-af)#exit
PE1(config-router)#exit
```

Figure III. 8.Configuration MP-BGP sur le routeur PE1.

On exécute les mêmes démarches de configuration sur le routeur PE2.

On a exécuté la commande « Show ip bgp vpnv4 all summary » pour s'assurer que les routeurs PE1 et PE2 sont bien des voisins par le protocole BGP

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 3.3.3.3, local AS number 700
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
4.4.4.4         4   700      55      55        1    0    0 00:46:16        0
```

Figure III. 9.PE1 et PE2 sont des routeurs voisins par protocole BGP (sur le routeur PE 1)

III.4.1.6.Création des VRF sur les interfaces des routeurs PE1 et PE2

- On va donner les adresses IP (que nous avons attribué dans les interfaces physiques en les mettant dans le VRF)
- On va implémenter le protocole RIP dans le VRF (en retirant la déclaration qui était faite de façon globale puis on va l'insérer dans l'instance au rip qui contient le VRF

```
PE1(config)#ip vrf ce1
PE1(config-vrf)#exit
PE1(config)#int f0/1
PE1(config-if)#no ip address
PE1(config-if)#ip vrf forwarding ce1
PE1(config-if)#ip address 20.0.0.1 255.255.255.252
PE1(config-if)#exit
PE1(config)#router rip
PE1(config-router)#no network 20.0.0.0
PE1(config-router)#address-family ipv4 vrf ce1
PE1(config-router-af)#network 20.0.0.0
PE1(config-router-af)#exit
```

Figure III. 10.Configuration VRF sur le routeur PE1

On exécute les mêmes démarches de configuration sur le routeur PE2.

III.4.1.7.Distribution des routes

```
PE1(config)#ip vrf ce1
PE1(config-vrf)#rd 700:1
PE1(config-vrf)#route-target both 700:1
PE1(config-vrf)#exit
PE1(config)#router rip
PE1(config-router)#address-family ipv4 vrf ce1
PE1(config-router-af)#redistribute bgp 700 metric transparent
PE1(config-router-af)#exit
PE1(config-router)#exit
PE1(config)#router bgp 700
PE1(config-router)#address-family ipv4 vrf ce1
PE1(config-router-af)#redistribute rip
PE1(config-router-af)#exit
```

Figure III. 11.Configuration de la redistribution de route sur le routeur PE1.

On exécute les mêmes démarches de configuration sur le routeur PE2.

III.4.1.8.Test et confirmation

On attribue au deux pc deux adresses IP, pour tester la configuration de MPLS/VPN avec un ping.

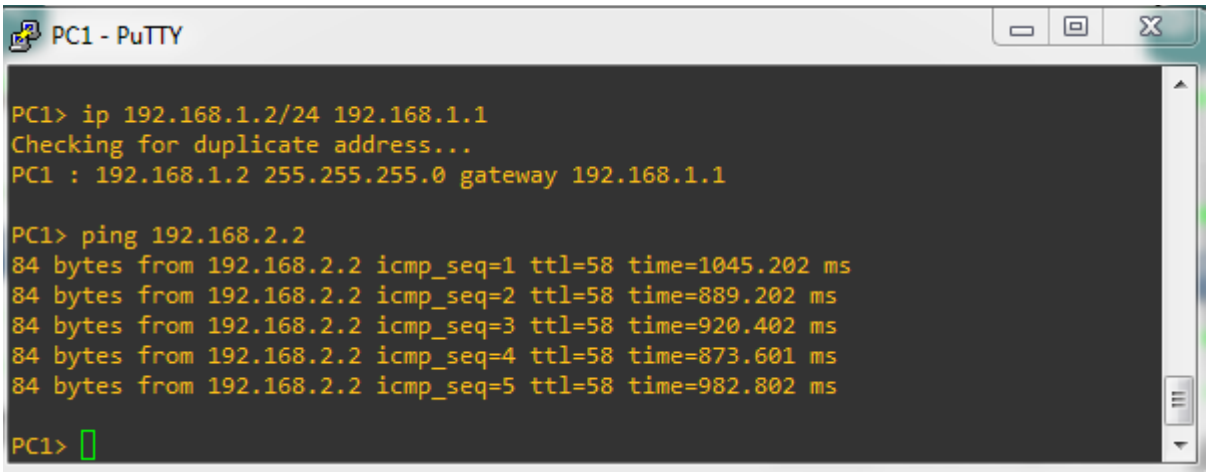

Figure III. 12.Ping du PC1 vers PC2

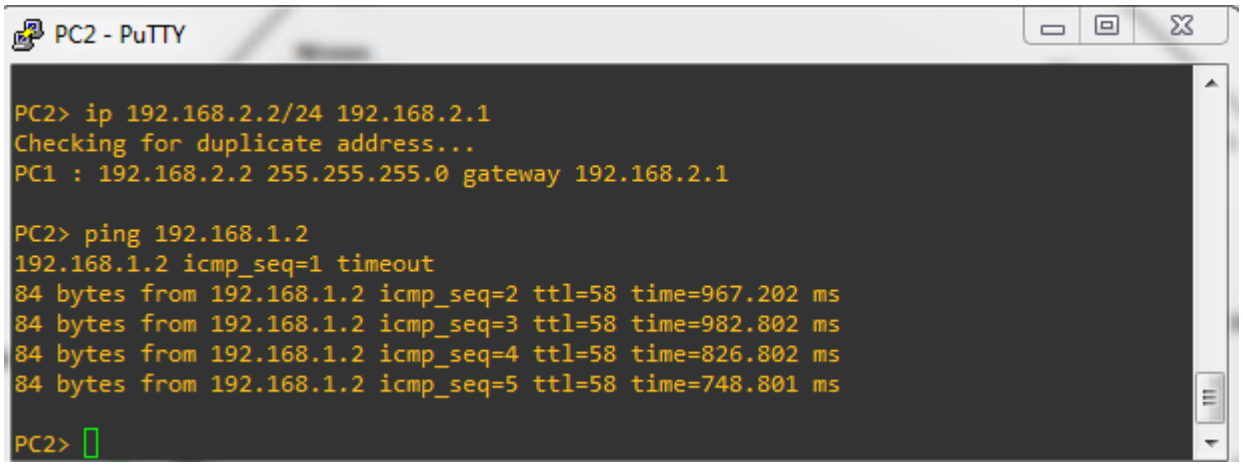

Figure III. 13.Ping du PC2 vers PC1

On remarque bien selon la Figure III. 12 et la Figure III. 13 que MPLS/VPN fonctionne

III.4.2.Configuration de la VoIP

III.4.2.1.Activation du serveur DHCP

On vient de de configurer l'activation du service DHCP qui permettra aux routeurs CE1 et CE2 d'attribuer les paramètres IP ainsi que la création des pools voic pour l'affectation automatique des adresses IP aux téléphones IP et PC

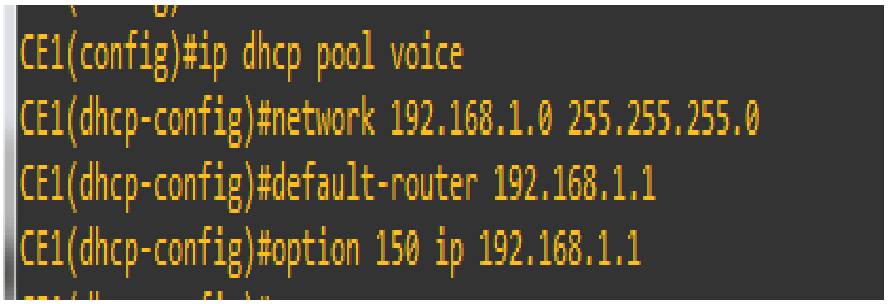

Figure III. 14.Configuration du serveur DHCP sur le routeur CE1.

On exécute les mêmes démarches de configuration sur le routeur CE2.

III.4.2.2. 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.

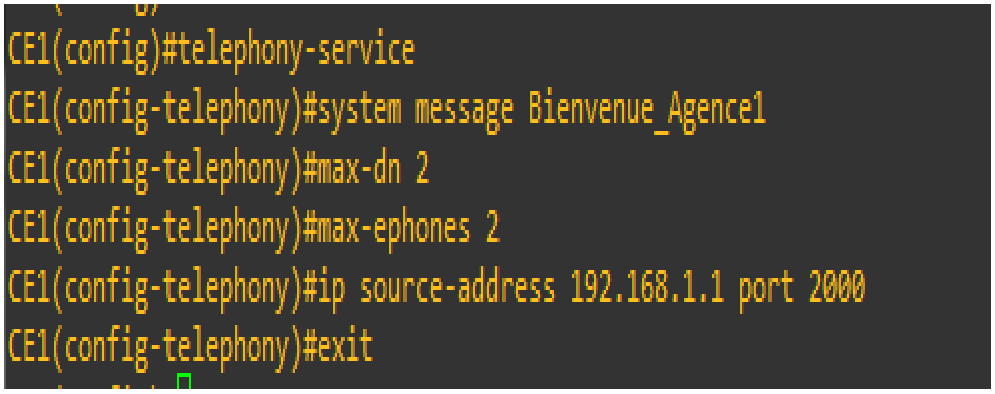

Figure III. 15.Activation du gestionnaire de communication VoIP sur le routeur MPLS

On exécute les mêmes démarches de configuration sur le routeur CE2.

III.4.2.3. Création des lignes et affectation aux téléphones IP

```
CE1(config)#ephone-dn 1 dual-line
CE1(config-ephone-dn)#number 100
CE1(config-ephone-dn)#name Abdelghani
CE1(config-ephone-dn)#label Abdelghani
CE1(config-ephone-dn)#description Bureau de Abdelghani
CE1(config-ephone-dn)#exit
CE1(config)#ephone-dn 2 dual-line
CE1(config-ephone-dn)#number 101
CE1(config-ephone-dn)#name User
CE1(config-ephone-dn)#label User
CE1(config-ephone-dn)#exit
CE1(config)#ephone 1
CE1(config-ephone)#mac-address 48E2.44A3.1B29
CE1(config-ephone)#button 1:1 3:2
CE1(config-ephone)#exit
```

Figure III. 16.Création des lignes et affectation aux téléphones IP sur le routeur CE1

On exécute les mêmes démarches de configuration sur le routeur CE2.

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

Figure III. 17.Les 2 téléphones IP configurées

Il s'impose de configurer les routeurs des deux agences 1 et 2 pour qu'ils puissent identifier les numéros d'appels d'agence distante en passant par le réseau MPLS/VPN.

```
CE1(config)#dial-peer voice 1 voip
CE1(config-dial-peer)#session target ipv4:30.0.0.2
CE1(config-dial-peer)#destination-pattern 2..
CE1(config-dial-peer)#exit
```

Figure III. 18.Identification les numéros d'appels d'agence 2 sur le router CE1

On exécute les mêmes démarches de configuration sur le routeur CE2.

III.4.2.4. Test et confirmation

Nous allons lancer l'appel depuis Ip phone 1 (Abdelghani) vers Ip phone 2 (Wassim) et on remarque que l'IP phone 2 sonne

Figure III. 19.Illustration du lancement d'appel du téléphone 1 vers téléphone 2

La communication est opérationnelle aussitôt que Ip phone 2 (Wassim) décroche l'appel.

Figure III. 20.Illustration de la réussite d'établissement de l'appel

III.5.Conclusion

La voix sur IP est la principale technologie de communication des entreprises, apporte des avantages économiques très réels, un autre avantage est l'intégration du téléphone comme une application pouvant interagir avec le système d'information de l'entreprise.

Le but de ce chapitre est de montrer la dernière partie de notre projet, y compris la VoIP est implémentée dans l'architecture MPLS/VPN. De nombreuses étapes ont été franchies complètement pour obtenir un bon fonctionnement de l'architecture.

Conclusion générale
Et perspectives

Conclusion générale et perspectives

Dans ce projet de fin d'études, nous avons étudié la qualité de service dans l'environnement VoIP et expliqué en détail les différents mécanismes permettant d'atteindre une bonne qualité de service. Notre premier objectif est de mettre en place une solution de la voix sur IP, de la faire fonctionner et de la mettre en production pour tester la qualité vocale de ses appels. Une fois mis en place, nous sommes tenus de mettre en place un mécanisme de qualité de service. Sur cette base, nous devons développer une stratégie de qualité de service pour permettre à notre infrastructure réseau d'améliorer la qualité de ses principaux produits (dont la voix sur IP). Nous étions bien motivés par le fait d'avoir l'opportunité d'étudier et de réaliser une solution pratique qui nous a permis de toucher et découvrir beaucoup de technologies et principalement le travail sous l'environnement du Protocol MPLS que nous avons décortiquer tous les aspects de fonctionnent avec les Protocol de routage nécessaire afin de le faire ouvrer sur technologie VoIP et assurer la qualité de transmission des paquets ainsi que la bande passante. Après avoir cueillis suffisamment d'informations,

On a simulé deux réseaux distants en utilisant GNS3 afin d'intégrer six routeurs Cisco 3725, deux switches Ethernet, deux IP phones, une machine virtuelle et une machine réel fonctionnant sous Windows 8.1 par VMware. La phase suivante était d'effectuer des appels VoIP entre deux utilisateurs distants, et de capturer la communication à l'entrée et à la sortie pour d'éventuels tests.

Les différents tests recueillis grâce à l'émulation de notre infrastructure réseau ont donné des résultats concluants tout ceci a causé quelques problèmes à notre PC, sachant qu'il est doté d'un processeur Intel® Core™ i3-4005M CPU @ 1.70GHz et d'une RAM de 4,00 Go et d'un système d'exploitation de 64 bits (sous Windows 7 Professionnel lors de notre simulation).
Nous avons par la suite installé une machine virtuelle GNS3 VM dans VMware Workstation.

Ce dernier travaille avec GNS3 nous a permet justement de soulager le PC du trafic entre VMware et GNS3. Ça n'a pas été suffisant on a dû remplacer la ram de 4g par une ram de 8go pour mettre en œuvre notre infrastructure réseau et d'y intégrer les protocoles de routage OSPF, RIP et BGP dans un premier temps. Par la suite, nous avons essayé d'améliorer les critères de qualité de services en intégrant le protocole MPLS, et cela aussi a été fait sans problèmes. Sachant qu'on n'a intégré le protocole MPLS que sur quatre routeurs, ce qui signifie qu'on n'a soulagé que deux routeurs et malgré cela nous avons noté des progrès considérables en ce qui concerne les paramètres de QoS.

Mais une fois qu'on a essayé de changer de routeur, d'intégrer des routeurs plus récents, comme CISC 7200, disposants de ports Gigabit Ethernet, notre PC ne les a pas supportés.

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.

Nous recommandons d'utiliser un routeur plus puissant pour de bons résultats et une meilleure progression, d'autant plus que pour assurer la couverture des différents pays à travers le monde. SD WAN s'imposent pour avoir plus de contrôle d'un quelconque réseau.

Références bibliographiques :

[1] Christian Bulfon http://www.gipsa-lab.grenoble-inp.fr/~christian.bulfone/MIASHS-L3/PDF/2-Le_protocole_IP.pdf 2018/2019

[2] Ouadouri Kamilia. <Etude et implémentation de la qualité de service sur VoIP. UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU 2015/2016 >

[3] ADNANE.N et MERSELN < Etude et Mise en Place D'une Solution VoIP Sécurisée. Cas d'étude : Entreprise Portuaire de Béjaïa.> Université Abderrahmane Mira de Bejaïa 2016/2017

[4] RA-HARINANJA Dia. <ANALYSE DE PERFORMANCE DE LA VOIX SUR IP BASEE SUR LA PLATE-FORME RASPBERRY PI>UNIVERSITE D'ANTANANARIVO 2017/2018

[5] ABDELLAOUI.M, BENHAMOU .A <Application mobile de la voIP sur un réseau Wifi> Université Abou Bekr Belkaid Tlemcen 2013/2014

[6] MEBARKI Nour El Houda. <Etude et simulation d'une transmission de la voix sur IP(VoIP). UNIVERSITE BADJI MOKHTAR ANNABA > 2018/2019

[7] Amziane.A Agdour.H <Mise en place et sécurisation d'une plateforme VoIP basée sur la solutionopen source Asterisk.> UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU 2015/2016

[8] ALKADE.H OGOUBI.K < Mise en œuvre d'une solution de gestion de la qualité de service Voix sur IP (VoIP)> UNIVERSITE BELHADJ BOUCHAIB 2019/2020

[9] Dridi.M <Optimisation d'une infrastructure IP-MPLS d'un opérateur et intégration de l'IPv6> UNIVERSITE VERTUELLE DE TUNIS 2017/2018

[10] www.ringover.fr/blog/ameliorer-qualite-appels-voip 4 mars 2020

[11] DJAMAH.B BNECHAABANE.M. <Implémentation de MPLS sur le backbone d'un fournisseur de service> Université Mouloud MAMMERI de Tizi-Ouzou 2017/2018

[12] ZERROUKI.H ADJABI.M. <Utilisation de la technologie MPLS dans le réseau 4G.> UNIVRESITE ZIANE ACHOUR DJELFA 2018/2019

[13] RAVOAVAHY Andriamparany Arnaud. <ANALYSE DE PERFORMANCE DE LA VOIP SUR UN BACKBONE MPLS AVEC TRAFFIC ENGINEERING> UNIVERSITE D'ANTANANARIVO 2012/2013

[14] OULD LAMARA.S TAKILT.M.<IMPLEMENTATION DU SDN DANS UNE STRUCTURE IP/MPLS> UNIVERSITE DE MOULOUD MAMMERI DE TIZI-OUZOU 2017/2018

[15] BENHAMZA.A TORKHANI.S<Simulation et développement d'une solution d'automatisation MPLS chez un fournisseur d'accès internet GlobalNet> UNIVERSITE VERTUELLE DE TUNIS 2017/2018