

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et Technologie Houari Boumediene
Faculté d'Electronique et d'Informatique



Mémoire présenté pour l'obtention de MAGISTER

EN : ELECTRONIQUE

Spécialité : Communication Parlée

Par

Karim SAFIR

Thème

**Déploiement d'une solution VoIP avec IPv6, Gestion de la QoS et
Evaluation en Reconnaissance Vocale**

Soutenue publiquement le 14 décembre 2014, devant le jury composé de :

Mme F. Merazka	Professeur à l'USTHB	Présidente
Mr A. Amrouche	Professeur à l'USTHB	Directeur de Mémoire
Mme L. Falek	Maître de Conférences à l'USTHB	Examineur
Mr B. Fergani	Maître de Conférences à l'USTHB	Examineur

Dédicaces

Je tiens à exprimer mes sincères remerciements à monsieur Amrouche, Professeur chercheur à L'Université des Sciences et Technologie Houari Boumediene Faculté d'électronique et d'informatique pour avoir accepté d'encadrer ce mémoire et son aide précieuse pour l'accomplissement de mon travail.

Je voudrais également exprimer mes remerciements à monsieur Outemezebet, Ex directeur de l'INPTIC pour son aide et soutien.

Je tiens aussi à remercier très sincèrement, l'ensemble de jury Composé de Mme F. Merazka Professeur à l'USTHB, Mme L. Falek Maître de Conférences à l'USTHB, Mr B .Fergani Maître de Conférences a l'USTHB qui me font le grand honneur de juger ce travail.

Je tiens à remercier tout particulièrement mes collègues et amies Mustapha, Tarek, Ahmed et Farid pour leur soutien et conseille, toute au long de la durée de ce travail.

Enfin, un grand salue à ma femme et mes enfants, pour m'avoir supporté pendant cette durée du travail.

Et a toute personne qui m'a aidé pour la réalisation de ce travail

SAFIR KARIM

- **Introduction**
- **Objectif**

Chapitre 1- Convergence des Services de Télécommunication et VoIP

- **Introduction**

1.1	Convergence des systèmes de télécommunication vers le tout	1
1.1.1	Contexte général	1
a.	Le protocole IP	2
b.	Problème d'adressages	2
c.	La bande passante	2
d.	Nécessité de préparer le réseau	3
e.	Gestion de la Qualité de Service (QoS).....	3
1.1.2	Nécessité de passage vers le Protocole IPv6.....	3
1.1.3	Cas de la Voip	4
1.2	Emergence de la VoIP	5
1.2.1	Le signal Vocal	5
1.2.2	Etapes préliminaires de la communication en VoIP :.....	5
1.2.3	Les Codecs.....	8
a.	Les différents Codecs :	8
b.	Les caractéristiques des différents Codecs :	9
1.2.4	Encapsulation des paquets Voix pour le transport sur le réseau IP	10
1.2.5	Les protocoles de transport temps réel.....	12
a.	Le protocole RTP	12
b.	Le protocole RTCP.....	13
1.2.6	Encapsulation des paquets VoIP	14
1.2.7	Les En- tête VoIP.....	16
1.3	Les protocoles de signalisation pour VoIP	17
1.3.1	Le protocole H.323	17
1.3.2	Le protocole MGCP :	18
1.3.3	Le Protocole d'Initiation de Session (SIP) :	19

a. Introduction	19
b. Architecture de SIP	20
1.3.4 Le protocole Skinny	20
Conclusion.....	21

Chapitre 2 - VoIP et Contraintes

2.1 Les paramètre de la voix sur IP.....	22
2.1.1 Le Seuil de tolérance pour la VoIP.....	22
2.1.2 Les codecs et leurs débits :.....	23
2.1.3 Implications de la Bande passante de Codecs	23
2.2 Les Codecs de la VoIP.....	24
2.3 Les contraintes de la VoIP.....	25
2.3.1 Délais de transmissions	25
a. Le délai d'échantillonnage.....	26
b. Le délai de propagation	26
c. Le délai de transport	26
d. Le délai des buffers de gigue	26
2.3.2 Impacte du délai de paquitisation sur les paquets VoIP et le débit.....	27
a. Un plus grand délai de parkérisation	27
b. Taille des paquets VoIP.....	28
c. Le délai de propagation	29
2.3.3 La Gigue de phase.....	30
2.3.4 La perte des paquets.....	30
Conclusion	31

Chapitre 3 - IPv6 et Qualité de Service (QoS)

Introduction.....	32
3.1 Qualité de services (QoS)	32
3.1.2 Les Mécanismes de qualité de service	33
3.1.3 Définition.....	33
3.1.3 Service Best effort	33
3.1.4 Services garantis (IntServ)	33

Présentation.....	33
a.Le protocole RSVP (ReSerVation Protocol)	33
b.Comment fonctionne RSVP	35
3.1.5 Services différenciés (DiffServ).....	35
a. Présentation	35
b. Classification et conditionnement du trafic	36
3.1.6 Mise en œuvre de DiffServ	37
a. Principe.....	37
b. Optimisation de trafic: MPLS (Multi-Protocol Label Switching)	38
3.2 Le Protocole IPV6	38
3.2.1 Caractéristiques du nouveau protocole Internet IPv6	38
3.2.2 Description du protocole IPv6	39
3.2.3 Les avantages des en-têtes IPv6.....	41
3.2.4 Représentation des adresses IPv6	41
3.2.5 Les Types d'adresse IPv6	42
3.2.6 Attribution des adresses IPv6	42
3.2.6 Attribution des adresses IPv6	42
3.2.7 Configuration de routage avec IPv6	44
3.2.8 Protocoles associés à IPv6	45
3.3 Les Mécanismes de transition d'IPv4 à IPv6	45
3.3.1 Techniques Dual-stack (Double Pile)	45
3.3.2 Tunnels IPv6 sur IPv4 (Tunneling)	46
3.4 Apport du protocole IPv6 à la QoS :.....	47
3.4.1 Les apports d'IPv6 pour la Qualité de service	47
3.4.2 La Qualité de service (QoS)	49
3.4.3 Evolution vers DIFFSERV	50
3.4.4 La Mobilité	50
3.4.5 La Sécurité	50
3.5 Stratégie D'implémentation de la QoS pour IPv6	51

Chapitre 4 - Déploiement de VoIP avec le protocole IPv4 et IPv6

Introduction	52
4.1 L'architecture et topologie du réseau	52

4.1.1 Composante de l'architecture réseaux	52
4.1.2 Caractéristiques des équipements utilisés.....	53
4.1.3 Conception LAN pour la VOIP et architecture utilisé.....	53
4.1.4 Intérêt du VLAN Voice	54
4.1.5 Commutateur avec Power over Ethernet (PoE)	54
4.1.6 La liaison WAN	54
4.2 Déploiement de la solution VoIP avec le Protocol IPv4.....	55
4.2.1 Modèle de conception	55
4.2.2 Choix de la topologie Réseau Distant	55
4.2.3 Présentation de la solution CME (Call Manager Express).....	55
a. Les protocoles VoIP supportés par CME	56
b. Les Codecs supportés par CME	57
c. Plates formes supportées.....	58
d. Exigences pour la configuration du matérielle.....	59
e. Modèles de déploiement de la solution CME	59
4.2.4 Architecture centralisée (Dans notre cas).....	60
4.3 Etape de configuration de la solution Cisco Call Manager Express.....	61
4.3.1 Configuration des VLAN Data et Voice sur les commutateurs	61
4.3.2 Configuration du routage Inter-vlan sur le Routeurs CME et Routeur Remote.....	62
4.3.3 Activation du service Serveur DHCP sur le routeur CME.....	63
4.3.4 Création du pool Voice pour l'attribution automatique des adresses IP	
au téléphone IP.....	64
4.3.5 Création de la pool data pour l'attribution automatiques des adresses IP.....	64
4.3.6 Activation de service téléphoné sur IP.....	65
4.3.7 Creation des lignes et affectation au telephone IP avec Ephone-dn et Ephone.....	65
4.4 Déploiement de la solution et tests.....	66
4.4.1 Lancement de la solution VoIP et enregistrement des téléphones IP.....	66
4.4.2 Lancer une session VoIP et enregistrement des fichiers .WAV.....	67
4.5 Déploiement de VoIP sur IPv6	69
4.5.1 Configuration des routeurs d'extrémité Gateway et Remote en mode tunnel	69
4.5.2 Configuration des routeurs d'extrémité Gateway et Remote en mode	
Dual Stack ainsi que le router ISP	71
Conclusion.....	72

Chapitre. 5 Evaluation et test de la solution VoIP sous IPv6 proposée

INTRODUCTION.....	73
5.1 Les différentes méthodes de mesures	73
5. 1.1 L'échelle MOS	73
5. 1.2 Le E-Model	73
5.1.3 PESQ (Perceptual Evaluation of Speech Quality) :	73
5.2 Evaluation objective et subjective de la qualité de la parole	74
5. 3 Evaluation objective de la qualité de la parole.....	74
5.3.1 Speech Quality Testing – PESQ	74
5.3.2 La méthode de mesure	75
5. 3.3 Résultats des mesures avec le PESQ	75
a. Solution VoIP basée sur le protocole IPv4 et influence de la bande passante..	75
b. Solution VoIP basée sur le protocole IPv6 et influence de la bande passante:	85
5.4 Evaluation subjective de la qualité de la parole:	86
5.4.1 MOS (Mean Opinion Score)	86
5.4.2 Méthodologie	86
5.4.3 Procédure de mesure.....	87

Liste des Figures

Figure 1.1 : Exemple de transmission de la VoIP	06
Figure 1.2 : Echantillonnage d'un signal analogique.....	07
Figure 1.3: Exemple de Quantification.....	07
Figure 1.4 : L'architecture du protocole RTP.....	13
Figure 1.5 : La voix encapsulée dans des paquets IP	15
Figure 1.6 : Compression de l'en-tête RTP	16
Figure 1.7 : La pile protocole du Terminal H323.....	18
Figure 1.8 : L'architecture de SIP.....	20
Figure 2.1 : La paupérisation de la VoIP	24
Figure 2.2 : Comparaison de deux scénarios de paupérisation avec des périodes de mise en paquet différentes.....	28
Figure 2.3 : Exemple d'en-tête de couche 2.....	29
Figure 3.1 : Les équipements d'interconnexions (routeurs), sur le chemin du flot des données, répondent aux requêtes RSVP , établissent et maintiennent les connexions.....	34
Figure 3.2 : Fonctionnement de RSVP.....	35
Figure 3.3 : Le DSCP dans le champ TOS de l'en-tête IP	36
Figure 3.4 : Classification Marquage et conditionnement du trafic.....	37
Figure 3.5 : Comparaison des deux en-têtes IPv4 et IPv6.....	39
Figure 3.8 : Structure générale d'une adresse IPv6 (Global Unicast).....	43
Figure 3.9 : Organisation de l'attribution des adresses IPv6 Globale.....	44

Figure 3.10: Les types de routage IPv6.....	44
Figure 3.11: Encapsulation de trames IPv4 dans des trames IPv6.....	45
Figure 3.12 : Configuration Dual-Stack sur un routeur Cisco.....	46
Figure 3.13: Tunnels IPv6 sur IPv4.....	46
Figure 3.14 : L'en-tête IPv6 standard.....	47
Figure 3.15 : Routage IPv6.....	47
Figure 4.1 : L'architecture réseau du déploiement de la plateforme VoIP.....	52
Figure 4.2 : Exemple du déploiement avec haute disponibilité.....	54
Figure 4.3 : Déploiement de Cisco Call Manager Express.....	56
Figure 4.4: Plateforme matérielle utilisée pour le déploiement et les tests de la solution VoIP avec IPv4 et IPv6 basée sur CME.....	58
Figure 4.5: Mode site unique.....	59
Figure 4.6 : illustre un déploiement distribué typique de traitement des appels, avec une interconnexion IP WAN et une connexion de secours RTC.....	61
Figure 5.1 : Représentation des valeurs obtenue avec IPv4 et IPv6	62
Figure 5 .1 : Test N°1.....	75
Figure 5 .2 : Test N°2.....	76
Figure 5 .3 : Test N°3.....	76
Figure 5 .4 : Test N°4.....	76
Figure 5 .5 : Test N°1.....	77
Figure 5 .6 : Test N°2.....	77
Figure 5 .7 : Test N°3.....	77

Figure 5 .8 : Test N°4.....	78
Figure 5 .9 : Test N°1.....	79
Figure 5 .10 : Test N°2.....	79
Figure 5 .11 : Test N°3.....	79
Figure 5 .12 : Test N°1.....	80
Figure 5.13 :Test N°2.....	80
Figure 5.14 :Test N°3.....	81
Figure 5.15 :Test N°4.....	81
Figure 5.15 : Test N°1.....	82
Figure 5.16 : Test N°2.....	82
Figure 5.17 :Test N° 3.....	82
Figure 5.18 : Test N°4.....	83
Figure 5.19.....	83
Figure 5.20 Representation des meilleurs valeurs obtenue dans le tableau 5.1.....	85
Figure 5.21 Representation des valeurs du tableau 5.2.....	86
Figure 5.22 representation des valeurs obtenue dans le tableau 5.6.....	85
Figure 5.6 Representation des valeurs obtenue dans le tableau 5.7.....	90

Liste des Tableaux

Tableau 1.1 : Les codecs utilisables en VoIP et leurs Bandes Passantes	9
Tableau 2.1 Bilan de bande passante en fonction du codec.....	23
Tableau 2.2 : Qualité audio pour les différents codecs.....	15
Tableau 2.3 Récapitulatif des valeurs acceptables pour de la VoIP.....	25
Tableau 2.4 : Valeurs tolérées de la latence.....	27
Tableau 2.5 Des exemples d'encapsulation VoIP avec des codecs différents et des périodes de mise en paquet de 20 et 30 ms.....	29
Tableau 2.6 : Valeurs des entêtes de couche 2 en Octets.....	30
Tableau 4.1 Equipements utilisé dans l'architecture réseau.....	53
Tableau 5.1 Tableaux récapitulatif des résultats (PESQ) obtenus avec IPv4.....	83
Tableau 5.2 Tableaux récapitulatif des résultats (PESQ) obtenus avec IPv6.....	85
Tableau 5.3 : Valeur du MOS	86
Tableau 5.4 Tableaux récapitulatif de meilleures valeurs obtenues avec IPv4	88
Tableau 5.5 Tableaux récapitulatif des résultats (MOS) obtenus avec IPv6.....	88
Tableau 5.6 Récapitulatif de la valeur moyenne MOS obtenus avec IPv4.....	89
Tableau 5.7 Tableaux récapitulatif de la valeur moyenne MOS obtenus avec IPv6.....	90

Liste des Abréviations :

A :

ADSL : Asymetric Digital subscriber Line

AH : Authentication Header :

AD : Duplicate Adresse Detection

ATM :

B :

C :

CLI :Commande Line Interface

CNAME : Canonical Name

CME :Call Manager Express

COS : Class Of Service

D :

DiffServ : Differentiated Services

DSP : Digital Signal Processors

DSCP : Differentiated service Code Point.

DHCP :Dynamique Host Configuration Protocole

DTE :

DND : Neighbor Discovery

E :

ESP : Encapsulating Security Payload

ETSI

F :

FXS : Foreign eXchange Subscriber

G:

I:

IETF : Inetrnet Engineering Task Force

IPv4 :Internet Protocole Version 4

*ITU : **I**nternational **T**elecommunication **U**nion*

ICMP : Internet Contrôle Message Protocole

IntServ Le Services garantis

ISP : Internet Service Provider

K:

L:

LAN : Local Area Network

M:

MPLS : Multi-Protocol Label Switching

MAC : Media access control

MGCP : Media Gateway Control Protocol

MLD : Multicast Listener Discovery

MTU : Maximum Transfert Unit) :

MOS : Mean Opinion Score)

N:

NAT : Network Address Translation

O:

P:

PCM : Modulation par impulsions et codage

PAM : une modulation d'amplitude d'impulsion

PABX :

PESQ : Perceptual Evaluation of Speech Quality

PoE : Power over Ethernet

PHB : Per Hop Behavior e of Service (ToS)

PSQM

S:

SDP : Session Description Protocol

SAP : Session Annoucement Protocol

SCCP : Skinny Client Control Protocol

SIP : Protocole d'Initiation de Session

T:

TTL : Time To Live

V:

VoIP :Voix Over Internet Protocole

VLAN : Virtual Local Area Network

VPN :Virtual Private Network

W:

R:

RTC : réseau téléphonique commuté

RNIS : ISDN en anglais)

RSVP : Resource ReSerVation Protocol

RTP : Real Time Protocole

RFC : Request For Comment

RTCP : Real Time Control Protocol

RSVP : Resource Reservation Protocol

W :

WAN : Wide Area Network

LER : Label Edge Router :

LSR : Label Switcher Router :

UTP : blindé à paire torsadée

Q :

QoS :Qualité Of Service

I'UIT-T :

RESUME

La convergence des réseaux de communications basés sur le tout IP (Internet Protocol) a été favorisée par l'avènement de la paquetisation de la voix et de l'image. Dans ce contexte, la VoIP (Voice over Internet Protocol) prend une place de plus en plus prépondérante et est devenue de nos jours un challenge intéressant pour le développement des réseaux de communications

Dans ce mémoire de Magister, nous déployons une plate-forme VoIP utilisant le nouveau protocole entre des réseaux distants, à savoir l'IPv6.

Afin de mieux cerner la problématique du déploiement d'une solution VoIP basée sur l'IPv6, nous nous sommes intéressés d'abord aux systèmes de communication utilisant la VoIP et les différents paramètres et protocoles qui gèrent le transport de la voix. Nous nous sommes aussi focalisés sur les paramètres de qualité de services (QoS) dans des communications VoIP en implémentant différents mécanismes introduisant la qualité de service.

Nous avons opté pour une architecture centralisée où la solution VoIP est implémentée sur le site Local permettant aussi de desservir les utilisateurs sur le Site lointain appelé Remote, le tout formant ainsi un réseau WAN.

Après avoir mis en œuvre la plateforme matérielle, la solution déployée est basée sur le Call Manager Express (CME) du constructeur Cisco, choix dicté par la disponibilité du matériel offrant la possibilité d'une mise en œuvre expérimentale dans des situations concrètes.

Plusieurs mécanismes permettant le passage de l'IPv4 vers l'IPv6 ont été développés. Dans ce travail, nous avons opté pour deux mécanismes les plus utilisés à savoir : i) Dual Stack (Double pile) où le routeur prend en charge les deux protocoles IPv4 et IPv6, selon le type de trafic envoyé (paquet IPv4 ou IPv6), ii) le mode tunnel où un paquet IPv4 est encapsulé par une en-tête IPv6.

Des tests d'appel entre deux utilisateurs situés respectivement dans le site Local et Remote ont été effectués avec succès, avec respectivement IPv4 et IPv6.

Nous avons effectués dans ce travail, une étude comparative des solutions IPv4 et IPv6, à l'aide d'une communication VoIP, en utilisant des outils d'évaluation objective et subjective de la qualité de la parole, notamment le PESQ et le MOS,

Ainsi, la solution VoIP utilisant l'IPv6 apporte une amélioration certaine, quand à la QoS par rapport à la solution utilisant l'IPv4.

Introduction :

Les différents services de télécommunications (Internet, téléphonie fixe, téléphonie mobile, diffusion de la télévision) ont longtemps évolué de manière indépendante en se fondant sur des techniques dédiées.

Apparu au début des années 1990, le développement du Web a fait décoller l'utilisation d'Internet. C'est au début des années 2000, au moment de l'apparition des hauts débits chez les particuliers, via l'ADSL (Asymmetric Digital subscriber Line) et le câble, que la convergence des services a débuté. Le nombre d'utilisateurs explose alors avec la création des offres « Triple Play » qui fournissent la téléphonie fixe, la diffusion de la télévision numérique, la vidéo à la demande et l'accès Internet via une couche fédératrice, IP (Internet Protocol).

Un besoin de convergence des systèmes de télécommunications apparaît alors, d'une part le besoin d'une architecture commune et unifiée, pour tous les services fournis par les différents systèmes de télécommunications, et d'autre part une architecture intégrant toutes les communications de manière la plus transparente possible.

Une multitude de questions fait son apparition : est-il possible de gérer tous ces différents flux réseau avec un seul point de convergence ? Une réponse possible est la convergence vers un système tout IP.

Au début de l'apparition des réseaux IP et notamment le réseau mondial Internet, on a utilisé le protocole IPv4, avec une adresse codée sur 32 bits, à ce moment-là les flux réseaux n'étaient pas aussi variés et complexes, on avait à envoyer des données (DATA) de quelque kilo bits de tailles variables, mais à fur et mesure que les réseaux IP prenaient de l'ampleur et l'apparition de nouvelles applications trop gourmandes en termes de bande passante, le manque d'adresse disponible se fera sentir et la demande de numéros d'adresses ne cesse d'augmenter.

Ainsi, et en raison de la saturation possible et des limites du protocole IPv4, l'évolution vers le nouveau protocole IPv6 devient impérative, l'intégration de nouvelles fonctionnalités, comme la Qualité de service (QoS), la portabilité, la mobilité des systèmes et des périphériques, est devenue indispensable au développement de nouveaux services, tel que la VoIP. Le passage à l'IPv6 s'accompagnera donc nécessairement d'une amélioration des performances bâties sur cette version.

L'objectif de ce mémoire de magister traite de déploiement d'une plate-forme VoIP sur le nouveau protocole IPv6 entre des réseaux distants.

La motivation principale ayant conduit à ce choix, réside dans le fait que la majorité des solutions proposées dans le domaine de la VoIP sont basées sur l'IPv4.

Dans ce mémoire nous allons tenter de mettre en évidence l'apport de l'IPv6 pour améliorer la qualité des communications vocales dans le monde de la VoIP, tout en essayant d'améliorer la Qualité de service (QoS). Pour cela, une attention particulière sera portée sur un des principaux paramètres influant sur la qualité de la communication, à savoir la bande passante.

Ce projet fait appel à plusieurs notions et connaissances sur les réseaux IP, les protocoles et notamment la VoIP, QoS, IPv6 et d'autres connaissances sur les réseaux IP en général.

Nous allons d'abord étudier et mettre en œuvre une solution VoIP en IPv4 entre réseaux distants, Ensuite on va déployer une solution en IPv6 et faire des tests comparatifs.

Afin de mieux cerner la problématique du déploiement d'une solution VoIP basée sur l'IPv6, ce mémoire commence par une étude sur la VoIP et les différents paramètres et protocoles qui gèrent le transport de la voix. Dans le deuxième chapitre, nous traitons les contraintes liées aux applications temps réel tel que la VoIP. Dans le troisième chapitre, nous montrons

que l'IPv6 apporte une amélioration de la qualité de service (QoS) dans les réseaux IP, en particulier pour la VoIP. Le but de ce chapitre est de mesurer les paramètres de qualité de services sur des communications VoIP en implémentant différents mécanismes introduisant la qualité de service. Dans le quatrième chapitre, nous décrirons la plateforme matérielle et la solution déployée à la base de Call Manager Express (CME) du constructeur Cisco sur deux sites situés sur deux sites distants que l'on appellera Local et Remote, formant ainsi un réseau WAN.

Enfin, on va clôturer ce mémoire par une étude comparative entre une communication VoIP, en utilisant des outils d'évaluation de la qualité de la parole et notamment le PESQ et le MOS. Ces différentes méthodes de traitement se feront en comparant un signal d'entrée de parole qui est une phrase lue par l'initiateur de la communication (Local-User) et le signal de sortie de parole à l'autre bout du réseau WAN, la première fois en utilisant le protocole IPv4 et la seconde fois avec le protocole IPv6. Ce travail est réalisé en faisant des captures du signal vocal en mode WAV, au niveau du réseau Local et sa sortie sur le réseau Remote.

Chapitre 1 :

***Convergence des Services de Télécommunications et
VoIP***

Introduction :

Dans ce premier chapitre, nous présentons d'abord le contexte général dans lequel se situe notre travail qui concerne le déploiement d'une solution IPv6 (Internet Protocol v6) pour la VoIP (Voice over IP). Tout d'abord, nous présenterons la convergence des réseaux de communications vers le tout IP. Par la suite, nous expliquerons le déroulement d'une session de communication de voix sur un réseau IP, avec les différentes phases que nécessite cette opération.

1.1 Convergence des réseaux de communications vers le tout IP :**1.1.1 Contexte général :**

Les différents services de télécommunications (Internet, téléphonie fixe, téléphonie mobile, diffusion de la télévision) ont longtemps évolué de manière indépendante en se fondant sur des techniques dédiées. Apparu au début des années 1990, le développement du Web a fait décoller l'utilisation d'Internet. C'est au début des années 2000, au moment de l'apparition des hauts débits chez les particuliers (abonnés), via l'ADSL (Asymmetric Digital subscriber Line) et le câble, que la convergence des réseaux a débuté. Le nombre d'utilisateurs explose alors avec la création des offres « Triple Play » qui fournissent la téléphonie fixe, la diffusion de la télévision numérique, la vidéo à la demande et l'accès Internet via une couche fédératrice IP (Internet Protocole). Un besoin de convergence des systèmes de télécommunications apparaît alors : d'une part le besoin d'une architecture commune et unifiée pour tous les services fournis par les différents systèmes de télécommunications, et d'autre part une architecture intégrant toutes les communications de manière la plus transparente possible. Une réponse possible est la convergence vers un réseaux unique de communication basé sur le tout IP.

a. Le protocole IP :

De nos jours, IP est devenu la couche fédératrice d'Internet et du monde des télécommunications. Cette convergence vers IP des systèmes de communication apporterait de nombreux avantages. Tout d'abord, elle permettrait une interconnexion et une interopérabilité plus simples et plus efficaces entre tous les systèmes de télécommunications. De plus, l'évolutivité des services serait rendue plus aisée dans des systèmes où le principe est traditionnellement de proposer des mécanismes et protocoles optimisés pour un service, mais peu génériques ni évolutifs. Enfin, l'intégration de la qualité de service (QoS) de niveau IP au sein des systèmes de télécommunications serait possible. Elle permettrait une prise en charge de la QoS cohérente avec le reste du monde IP et en adéquation avec les besoins applicatifs.

b. Problème d'adressages :

Lors de l'avènement de l'IP (décrit pour la première fois dans la RFC 760 définie en janvier 1980), les concepteurs pensaient alors que seuls quelques milliers d'ordinateurs, répartis sur une douzaine de réseaux, seraient concernés. Avec IPv4 (Internet Protocole version 4), l'adressage se fait sur 32 bits. Mais, IPv4 est un protocole qui est trop restreint de par son utilisation et qui est donc coûteux en matière d'adresses gaspillées. Etant donné l'expansion de l'Internet, avec l'arrivée massive d'objets adressables, l'épuisement des adresses disponibles sous IPv4 devient une réalité à laquelle il faut trouver une solution. Par ailleurs, de par la taille des tables de routage, le traitement des paquets est fortement ralenti.

c. La bande passante :

La bande passante traditionnelle utilisée en téléphonie fixe, appelée « bande-étroite », est 300-3400 Hz. Elle résulte d'un filtre standardisé par l'ITU [ITU-T, Rec. G.712, 1992]. Or, le réseau de téléphonie, à l'origine analogique a subi un premier changement en passant à l'ère numérique, passant du Réseau Téléphonique Commuté (RTC) au Réseau Numérique à Intégration de Service (RNIS). Pour autant, ce réseau peut être défini par certaines caractéristiques comme la connexion physique, entre deux interlocuteurs, qui durant toute la durée de la conversation, reste active. Ceci n'est plus vrai avec l'apparition de la VoIP, qui permet la transmission de données sous forme de paquets.

d. Nécessité de préparer le réseau :

L'architecture de convergence doit permettre une interconnexion et une intégration de tous les services de communication. Cette interconnexion et cette intégration posent alors plusieurs problèmes en termes de prise en charge de la qualité de service (locale et de bout en bout) ou encore de routage IP. Ces aspects doivent être absolument résolus lors du développement du réseau.

e. Gestion de la Qualité de Service (QoS) :

Une prise en charge globale et cohérente de la qualité de service (QoS) est un enjeu important de la convergence. En effet, c'est la définition de ces mécanismes de QoS qui va permettre une intégration efficace des différents services quel que soit le type de réseau sous-jacent.

Cette intégration passe par l'intégration des mécanismes de gestion de la qualité de service de niveau 3 (notamment l'architecture DiffServ implantée dans les équipements qui permet d'appliquer la QoS adéquate aux différents trafics). En effet, de nombreuses applications des télécommunications instruites sur la base d'IP supposent une QoS satisfaisante.

1.1.2 Nécessité de passage vers le Protocole IPv6 :

La nécessité du passage vers IPv6 est née de la pénurie d'adresses IPv4. La convergence de tous les multimédias sur IP nécessite à la fois de connecter plus d'équipements au réseau, mais également d'assurer une communication de bout en bout entre ceux-ci. Pour ces deux problématiques, IPv6 nouveau protocole de l'Internet est incontournable. Avec une adresse IPv6 codée sur 128 bits (au lieu de 32 pour IPv4), l'espace d'adressage IPv6 devient plus large et il est possible de connecter tout terminal au réseau avec une adresse distincte. La communication entre ces terminaux est donc simplifiée, car elle ne nécessite ni translation d'adresse, ni autres proxy complexe du fait de la nature des flux.

Dès le milieu des années 1990, le réseau Internet était utilisé largement par les universités, les industries de pointes, et les gouvernements. Les principaux objectifs du protocole IPv6 sont :

- Supporter des milliards d'ordinateurs prévus, en se libérant de l'inefficacité de l'espace des adresses IP actuelles.
- Réduire les tables de routage.
- Simplifier le protocole, pour permettre aux routeurs de router plus rapidement.

- Fournir une meilleure sécurité que l'actuel protocole IP (IPv4)
- Accorder plus d'importance au type de service, et notamment aux services associés au trafic temps réel.
- Faciliter la diffusion multi-destinataires en permettant de spécifier l'envergure.
- Donner la possibilité à un ordinateur de se déplacer sans changer son adresse.
- Permettre au protocole une évolution future, c'est-à-dire anticiper sur des utilisations futures demandant des fonctions évoluées, telles que la mobilité, le multimédia etc.
- Accorder à l'IPv4 et à l'IPv6 une coexistence pacifique.

1.1.3 Cas de la VoIP :

Dans le contexte de la convergence des réseaux de communications vers le tout IP, les entreprises utilisent la technologie VoIP pour économiser de l'argent sur les coûts de communications et des améliorations fonctionnelles telles que la mobilité, la présence des fonctions liées et la messagerie unifiée. Les réseaux VoIP commencent à prendre en charge l'itinérance de téléphones basés sur Ethernet au service cellulaire. Cependant, deux problèmes fondamentaux font obstacle à l'évolutivité de la VoIP.

- Le premier problème est le manque de facto intrinsèque QoS dans de nombreux réseaux IP, à la fois au niveau du support et de l'entreprise.
- Il est difficile de transporter des paquets VoIP à travers les Pare Feu (firewalls), non seulement en raison de considérations protocolaires, mais aussi à cause de traduction d'adresses réseau NAT (Network Address Translation).
- Les problèmes de sécurité, tels que l'espionnage et le piratage, constituent un autre problème potentiel.
- La prochaine génération de réseaux VoIP basés sur IPv6 est en phase de développement pour répondre à ces questions, en particulier l'évolutivité et la fiabilité de qualité commerciale.

1.2 Emergence de la VoIP

Introduction :

La VoIP est apparue grâce à la démocratisation des connexions Internet Haut- débits et des réseaux Ethernet pour les réseaux locaux. La VoIP est d'abord un système de mise en paquets des données vocales. En effet, lorsque la connexion est établie, la parole est codée (par un Codec) est ensuite mise sous forme de paquets de données puis envoyée de la source jusqu'à la destination par le biais du réseau IP en utilisant la pile TCP/IP. Des en-têtes sont ajoutés aux paquets de données vocales par les différents protocoles employés et augmentent successivement la taille du fichier.

1.2.1 Le signal vocal :

La parole est un signal non stationnaire qui peut cependant être considéré comme quasi stationnaire sur des intervalles de durée comprise entre 10 à 40 ms.

- La parole humaine utilise la bande de fréquence 200-9000 Hz
- L'oreille humaine peut détecter des sons dans la bande de fréquence 20-20000 Hz.
- Les systèmes de téléphonie traditionnels ont été conçus pour fonctionner dans la bande 300-3400 Hz.
- Le taux d'échantillonnage de la voix numérisée a été fixé à 8000 échantillons par seconde ($F_{ech} = 8 \text{ kHz}$).

1.2.2 Etapes préliminaires de la communication en VoIP :

Comme indiqué sur la figure 1.1, la transmission d'un signal Voix sur un réseau IP passe par les étapes suivantes.

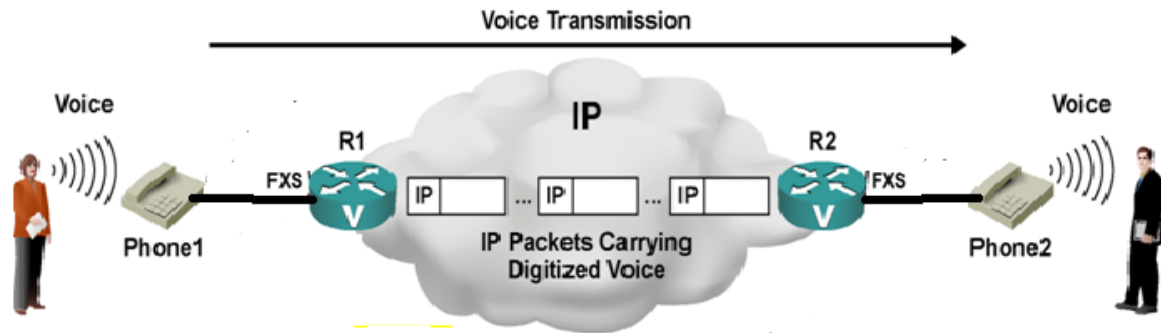


Figure 1.1 : Exemple de transmission de la VoIP

a. Etape 1 : Échantillonnage du signal analogique :

L'échantillonnage est la technique qui permet de numériser des informations analogiques. La figure 1.1 illustre la façon dont les routeurs convertissent les signaux vocaux analogiques au format numérique pour l'encapsulation dans des paquets IP. Dans le schéma, un appel est effectuée à partir d'un téléphone analogique (Phone1) connecté à un routeur (R1) vers un téléphone analogique (Téléphone 2) connectée à un autre routeur (R2). Les deux routeurs se connectent à un réseau IP. L'utilisateur du Phone1 parle dans le microphone du téléphone, et le téléphone émet un signal analogique sur le port FXS (Foreign eXchange Subscriber) du routeur R1. Le routeur R1 convertit le signal analogique reçu en un signal numérique et encapsule les bits dans les paquets IP. Le réseau IP transporte les paquets IP au routeur R2

Le module DSP sur les cartes d'interface vocale des routeurs à commande vocale effectue la conversion analogique-numérique. Le DSP échantillonne périodiquement le signal analogique en respectant le théorème de Shannon

$$F_{ech} \geq 2 f_{max}$$

avec F_{ech} : fréquence d'échantillonnage

f_{max} : valeur de la fréquence maximale du signal à échantillonner.

Le taux d'échantillonnage affecte la qualité du signal numérisé : si le taux d'échantillonnage est trop faible et ne respecte pas le théorème de Shannon, la qualité résultante est dégradée. Si le taux d'échantillonnage est plus élevé que nécessaire, il en résulte une consommation inutile de la bande passante. La figure 1.2 donne un exemple de l'échantillonnage d'un signal analogique

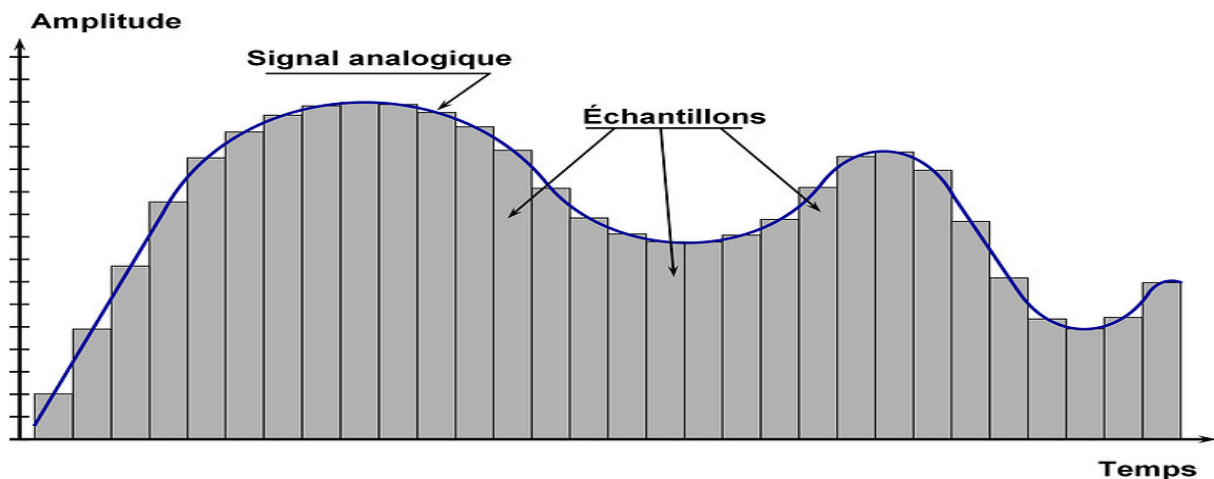


Figure 1.2 : Echantillonnage d'un signal analogique

Bien que l'oreille humaine puisse détecter des sons de 20 à 20.000 Hz, et la parole englobe les sons d'environ 200 à 9000 Hz, les voies téléphoniques que nous utilisons fonctionnent à environ 300 à 3400 Hz.

b. Etape 2 : Quantification :

La quantification est la représentation des amplitudes par une valeur discrète. Les applications de téléphonie utilisent généralement 8 bits de quantification. Comme l'échantillonnage du signal téléphonique prend 8000 échantillons par seconde, le débit nécessaire est de 64 kbps.

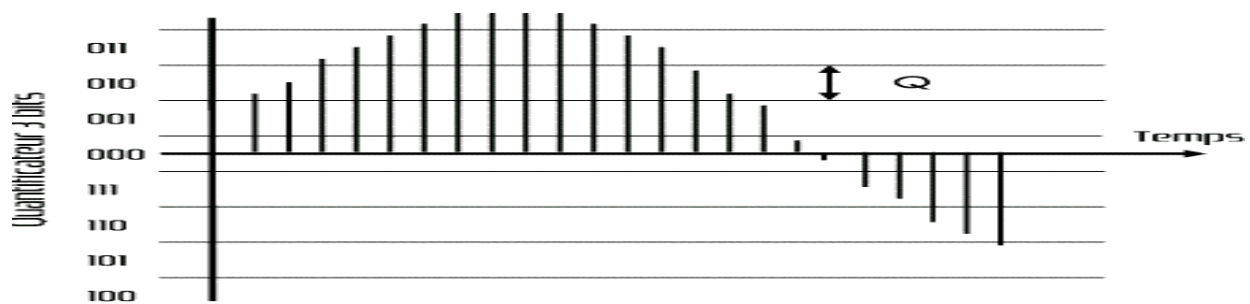


Figure 1.3 : Exemple de Quantification.

c. Etape 3 : Codage

Ce besoin de bande passante est la raison pour laquelle les réseaux traditionnels de téléphonie à commutation de circuits utilise le multiplexage par répartition lignes, combinant de multiples canaux de 64 kbps chacun (niveau du signal numérique 0 [DS-0]) dans une interface physique unique. La modulation par impulsions et codage (PCM) est une représentation numérique d'un signal analogique lorsque l'amplitude du signal est échantillonnée régulièrement à des intervalles uniformes, puis quantifiés à une série de symboles numériques en un code. La technique de base PCM est d'utiliser un codeur-décodeur (codec) pour échantillonner l'amplitude d'un signal vocal 8000 fois par seconde et ensuite stocker la valeur d'amplitude de 8 bits de données. Il existe une formule à cette procédure de stockage. Le résultat est la base de la hiérarchie du système téléphonique numérique entière.

1.2.3 Les Codecs :

a. Les différents Codecs :

Le sigle codec vient de la juxtaposition des termes Coder/Decoder. Un codec permet de coder un signal vocal dans un format adapté aux transports à travers un réseau. Il doit bien évidemment permettre également le décodage de ce signal pour le restituer à l'autre extrémité du réseau. L'objectif d'un codec est d'obtenir une bonne qualité de voix avec un débit et un délai de compression le plus faible possible. Chaque codec présente des avantages et des inconvénients. Mais pour simplifier, on peut retenir que plus un codec compresse le signal (et donc utilise moins de bande passante) moins sa qualité sera bonne. À l'inverse moins il compresse le signal plus la qualité sera bonne. Les codecs les plus souvent mis en oeuvre dans les solutions VoIP sont G.711, G.729 et G.723.1 (voir tableau 1.1).

Tableau 1.1 : Les codecs utilisables en VoIP et leurs Bandes Passantes :

Standard ITU-T	Type de Codage	Débit binaire en kb/s
G.711	PCM	64
G.722.2 (AMR-WB)	ACELP	16
G.723.1	ACELP	6,3
G.726	ADPCM	16, 24, 32, et 40
G.728	LD CELP (Low Delay CELP)	16
G.729,	CS-ACELP	8

b. Les caractéristiques des différents Codecs :

- **G.711 :**

Le **G.711** est une norme de compression audio de l'UIT, s'appuyant sur les lois de quantification A (Europe, Afrique) ou μ (Amérique du Nord, Japon).

- Échantillonnage : 8000 Hz pour une bande passante du téléphone entre 300 et 3400 Hz
- Bande passante sur le réseau : 64 kbit/s
- Type de codage : MIC (Modulation d'impulsion codée, PCM en anglais)

Son principe repose sur une grille de quantification non linéaire, permettant de diminuer le rapport signal-sur-bruit de l'erreur de quantification pour les sons de faible amplitude. La norme G.711 a été révisée en 2000. Elle est la base de transport de la voix sur le réseau téléphonique commuté (RTC) ou sur le RNIS (ISDN en anglais) et est également utilisée pour le transport de la voix avec peu de compression dans les réseaux IP, comme par exemple sur les offres de téléphonie sur les « boxes » ou sur des réseaux locaux IP. Elle est en revanche

assez peu utilisée pour faire de la téléphonie directement sur des réseaux étendus comme Internet de par l'utilisation importante de bande passante.

- **G.723.1**

Le codec G.723 est avant tout un codeur de voix. Son algorithme fait l'hypothèse que le signal traité correspond à une voix humaine occidentale. En particulier, il se révèle de qualité médiocre pour le codage de signaux non vocaux (musique, etc.). Le G.723 est normalisé pour deux taux de compression, à savoir 5.3 kbit/s et 6.4 kbit/s. Ces deux débits correspondent à deux types de codage différents, il ne s'agit pas d'un simple ajustement. La version à 6.3 kbit/s est d'une qualité légèrement supérieure à la version 5.3 kbit/s: la note MOS du 6.3 kbit/s atteint 3.9, contre 3.65 pour le 5.3 kbit/s. Ces deux codecs ont une latence algorithmique de 30 ms.

- **G.729**

La recommandation UIT-T **G.729** définit un codage de la parole à 8 kbit/s par prédiction linéaire avec excitation par séquences codées à structure algébrique conjuguée. Le codec G.729 est moins consommateur en bande passante que G711. Il est utilisé pour obtenir une téléphonie de qualité. Il est supporté par la plupart des PABX IP .

- Utilisé pour le codage de la partie audio d'une visioconférence,
- Rencontré aussi pour transporter de la voix sur IP sur les WAN .
- Utilisé préférentiellement par les opérateurs de téléphonie

Il existe aussi une version G.729A compatible avec G.729 (qui utilise aussi CS-ACELP), mais le G.729A nécessite moins de calculs.

1.2.4 Encapsulation des paquets Voix pour le transport sur le réseau IP :

- Les Protocoles :

Le transfert de données sur Internet s'effectue par paquets de données. Cette structure repose sur l'utilisation de protocoles TCP/IP (Transport Control Protocol/ Internet Protocol). Chaque document, qu'il s'agisse de texte, image ou voix, est numérisé puis réparti en paquets.

Chacun de ces paquets est alors envoyé sur Internet indépendamment des autres et essaie de prendre le chemin le plus rapide pour parvenir à sa destination.

- Le Protocole IP :

Le protocole IP est au centre du fonctionnement de l'Internet. Il fait partie de la couche Internet de la suite de protocoles TCP/IP. Il assure sans connexion un service non fiable de délivrance de paquets IP. Le service est non fiable car il n'existe aucune garantie pour que les paquets IP arrivent à destination. Certains paquets peuvent être perdus, dupliqués ou remis en désordre. On parle de remise au meilleur effort. Le protocole IP permet aux paquets de se déplacer sur le réseau Internet, indépendamment les uns des autres, sans liaison dédiée. Chacun d'entre eux, envoyé sur le réseau, se voit attribuer une adresse IP. Cette dernière est un en-tête accolé à chaque paquet et contenant certaines informations, notamment, l'adresse destinataire, sa durée de vie, le type de service désiré, etc. Le protocole IP actuellement utilisé en est la version 4 et la nouvelle version IPv6 est déjà prête à prendre le relais.

- Le Protocole TCP

Le protocole TCP est un protocole de contrôle de transmission, il fait partie de la couche transport du modèle OSI. Il est orienté connexion, c'est à dire, il simule un circuit virtuel entre les applications utilisateurs. Le protocole TCP établit un mécanisme d'acquittement et de réémission de paquets manquants. Ainsi, lorsqu'un paquet se perd et ne parvient pas au destinataire, TCP permet de prévenir l'expéditeur et lui réclame de renvoyer les informations non parvenues. Il assure d'autre part un contrôle de flux en gérant une fenêtre de congestion qui module le débit d'émission des paquets. Il permet donc de garantir une certaine fiabilité des transmissions. TCP assure un service fiable et est orienté connexion, cependant il ne convient pas à des applications temps réel à cause des longs délais engendrés par le mécanisme d'acquittement et de retransmission.

- Le Protocole UDP :

Le protocole de datagramme utilisateur (UDP) est le protocole de transport sans confirmation. UDP est un protocole simple qui permet aux applications d'échanger des datagrammes sans accusé de réception ni remise garantie. Le traitement des erreurs et la retransmission doivent être effectués par d'autres protocoles. UDP n'utilise ni fenêtrage, ni accusés de réception, il ne

re-séquence pas les messages, et ne met en place aucun contrôle de flux. Par conséquent, la fiabilité doit être assurée par les protocoles de couche application. Les messages UDP peuvent être perdus, dupliqués, remis hors séquence ou arriver trop tôt pour être traitée lors de leurs réception. UDP est un protocole particulièrement simple conçu pour des applications qui n'ont pas à assembler des séquences de segments. Son avantage est un temps d'exécution court qui permet de tenir compte des contraintes de temps réel ou de limitation d'espace mémoire sur un processeur, contraintes qui ne permettent pas l'implémentation de protocoles beaucoup plus lourds comme TCP. Dans des applications temps-réel, UDP est le plus approprié, cependant il présente des faiblesses dues au manque de fiabilité. Des protocoles de transport et de contrôle temps-réel sont utilisés au dessus du protocole UDP pour remédier à ses faiblesses et assurer sa fiabilité. Ces protocoles sont RTP et RTCP et sont détaillés dans le paragraphe suivant.

1.2.5 Les protocoles de transport temps réel :

a. Le protocole RTP :

Le groupe de l'IETF (Internet Engineering Task Force) a développé en 1993 le protocole de transport en temps réel (RTP, RFC 1889) dont le but est de transmettre sur Internet des données qui ont des propriétés temps réel (audio, vidéo, etc.). C'est un protocole de la couche application du modèle OSI qui utilise les protocoles de transport TCP ou UDP, mais, généralement, il utilise UDP qui est mieux approprié à ce genre de transmission. Le tableau 1.4 représente l'architecture du protocole RTP.

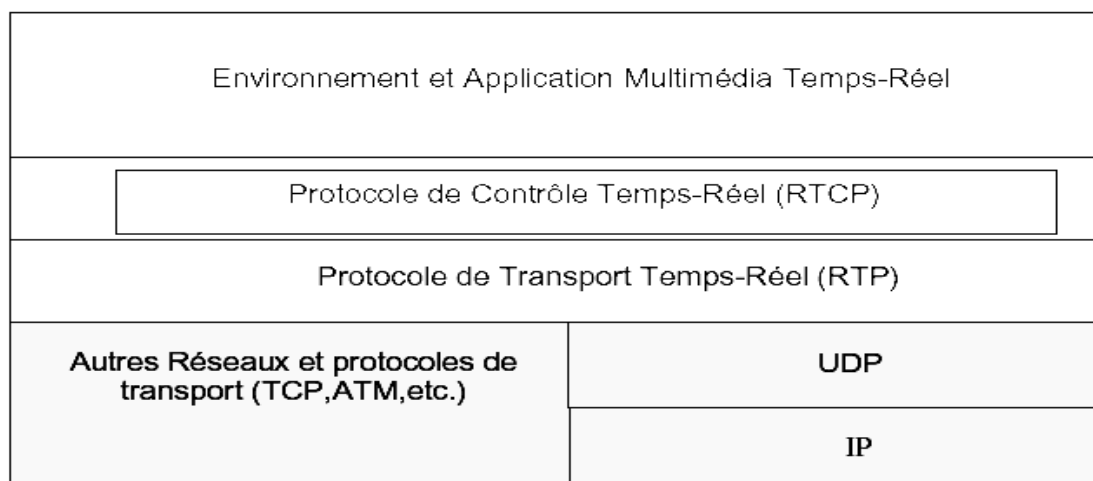


Figure 1.4 L'architecture du protocole RTP

Le rôle principal de RTP consiste à mettre en œuvre des numéros de séquence de paquets IP et des mécanismes d'horodatage (timestamp) pour permettre de reconstituer les informations de voix ou vidéo. Plus généralement, RTP permet :

- D'identifier le type de l'information transportée.
- D'ajouter des indicateurs de temps (horodater) et des numéros de séquence à l'information transportée.
- De contrôler l'arrivée à destination des paquets.

b. Le protocole RTCP :

RTCP (Real Time Control Protocol, RFC 1889) est un protocole de contrôle utilisé conjointement avec RTP pour contrôler les flux de données et la gestion de la bande passante. RTCP permet de contrôler le flux RTP, et de véhiculer périodiquement des informations de bout en bout pour renseigner sur la qualité de service de la session de chaque participant à la session. Des quantités telles que le délai, la gigue, le taux de paquets reçus et perdus sont très importants pour évaluer la qualité de service de toute transmission et réception temps réelle. C'est le protocole sous-jacent (UDP par exemple) qui permet grâce à des numéros de ports différents et consécutifs (port pair pour RTP et port impair immédiatement supérieure pour RTCP) le multiplexage des paquets de données RTP et des paquets de contrôle RTCP.

Le protocole RTCP remplit trois fonctions :

- L'information sur la qualité de service : RTCP fournit, en rétroaction des informations sur la qualité de réception des données transmises dans les paquets RTP. Cette information est utilisée par la source émettrice pour adapter le type de codage au niveau des ressources disponibles.
- L'identification permanente : RTCP transporte un identificateur original de la source RTP c'est à dire la provenance du flux, appelé *CNAME* (Canonical Name). Cet

identificateur permet une identification permanente de chacun des flux multimédia entrants.

- Le calibrage de la fréquence d'émission : La réception des feed-back et la connaissance du nom permanent servent à ajuster la fréquence d'envoi des paquets à la bande passante mise à la disponibilité de l'utilisateur situé à l'autre extrémité. Chaque paquet RTCP contient un rapport émetteur ou récepteur suivi d'une description de la source (source description).

1.2.6 Encapsulation des paquets VoIP :

La voix numérisée est encapsulée dans RTP, UDP, et IP par défaut, Une portion de 20 ms de voix est mise en un seul paquet IP. Les périphériques VoIP encapsulent la voix dans RTP et UDP avant d'ajouter l'en-tête IP. La taille de l'ensemble du paquet VoIP dépend du codec utilisé et la quantité de voix qui est mis en paquets. La longueur des échantillons peut varier, mais pour la voix, des échantillons représentant 20 ms sont la durée maximale de la charge utile. Le choix de cette durée de charge utile est un compromis entre les exigences de bande passante et de qualité. Une petite charge utile exige une bande passante proportionnellement plus élevée par bandes par canal, car la longueur d'en-tête reste à 40 octets. Toutefois, en cas d'augmentation des charges utiles, le retard global dans le système augmente, et le système est plus sensible à la perte de paquets individuels par le réseau. La figure 1.5 montre des échantillons de voix encapsulés dans des paquets IP avec UDP et RTP. Chaque exemple utilise un codec différent, et est basé sur une valeur par défaut de 20 ms de voix par paquets.

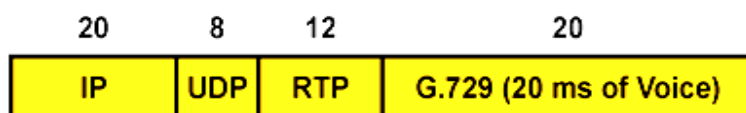
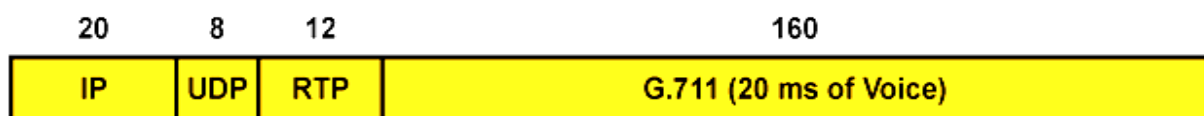


Figure 1.5 La voix encapsulée dans des paquets IP

- Le Processus d'encapsulation :
- Lorsque des signaux analogiques sont numérisés en utilisant le codec G.711, 20 ms de parole se compose de 160 échantillons, chaque échantillon est codé sur 8 bits. Le résultat est de 160 octets d'information vocale. Ces échantillons G.711 (160 octets) sont encapsulés dans avec un en-tête RTP (12 octets), un en-tête UDP (8 octets), et un en-tête IP (20 octets). Par conséquent, l'ensemble du paquet IP transportant UDP, RTP, et la charge utile vocale utilisant G.711 a une taille de 200 octets.
- En revanche, 20 ms de voix codées avec le codec G.729 est constituée de 160 échantillons, où des groupes de 10 échantillons sont représentés par un mot de code 10-bit. Le résultat est de 160 bits (20 octets) de données voix. Ces mots de code G.729 (20 octets en taille) sont encapsulés dans un en-tête RTP (12 octets), un en-tête UDP (8 octets), et un en-tête IP (20 octets). Par conséquent, l'ensemble du paquet IP transportant UDP, RTP, et la charge utile vocale en utilisant G.729 a une taille de 60 octets.

1.2.7 Les En-tête VoIP :

- La surcharge combinée des en-têtes IP, UDP et RTP est extrêmement élevée, en particulier parce que la voix se déplace dans des paquets relativement petites et à des taux élevés de paquets.
- Lorsque G.729 est utilisé, les en-têtes sont deux fois la taille de la charge utile vocale. La bande passante de voix pure du codec G.729 (8 kbps) est triplé pour l'ensemble du paquet IP. Ce total, cependant, n'est pas encore la dernière exigence de bande passante, car la couche 2 doit également être incluse. Sans l'en-tête de couche 2, un appel G.729 nécessite 24 kbps.
- Lorsque G.711 est utilisé, le rapport des en-tête sur la charge utile est plus petite en raison de la charge utile vocale plus grande. Une en-tête de 40 octets sont ajoutés à

160 octets de charge utile, de sorte que le quart de la largeur de bande G.711 codec (64 kbps) doit être ajouté. Sans les en-têtes de couche 2, un appel G.711 nécessite 80 kbps.

- En tête cRTP :

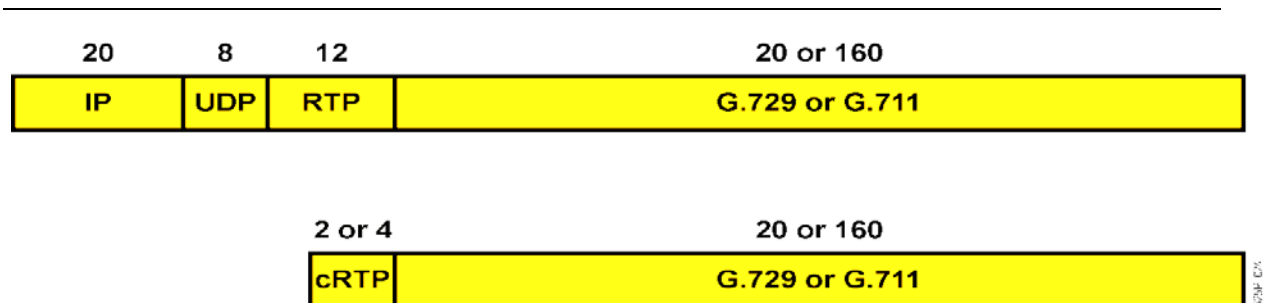


Figure 1.6 Compression de l'en-tête RTP

La figure 1.6 montre comment l'en-tête RTP est compressé, (cRTP) réduit l'énorme surcharge de la bande passante qui est causée par l'IP, UDP, et RTP-têtes. cRTP non seulement comprime la tête RTP, mais il compresse également les en-têtes IP et UDP. La compression des 40 octets d'en-têtes combinées ensemble fournit sensiblement plus de gain de compression de 12 octets d'en-tête RTP seul car la taille obtenue est à peu près le même (2-4 octets) dans les deux cas. Les champs statiques dans les en-têtes comprennent adresses IP source et destination, d'origine et de destination numéros de ports UDP, et de nombreux autres domaines dans les trois têtes.

1.3 Les protocoles de signalisation pour VoIP :

La signalisation désigne la transmission d'un ensemble de signaux et d'informations de contrôle échangés entre les intervenants d'une communication. Leurs échanges permettent l'initiation, la négociation, l'établissement, le maintien et la fermeture de la connexion.

Il convient de distinguer deux types de transferts pour comprendre à quoi correspond la signalisation :

- le transfert de données brutes :

Le transfert de données brutes concerne les échanges de données binaires d'un poste vers un autre. L'objectif de ce transfert est de reproduire à l'identique des données en les faisant transiter par un réseau.

- le transfert d'informations de contrôle :

Le transfert d'informations de contrôle concerne les échanges de types protocolaire exécutant une action prédéfinie, et donc nécessairement limitée en possibilités. L'objectif de ce transfert est d'assurer la maîtrise et la gestion du flux.

- Intérêt des Protocoles de signalisation :

1.3.1 Le protocole H.323 :

Le standard H323, développé par l'ITU-T, est défini comme étant le standard spécifiant les éléments, les protocoles et les procédures pour réaliser des communications audio, vidéo et autres données en temps réel sur les réseaux de paquets. Il décrit également les terminaux, équipements, et services nécessaires à l'établissement d'une communication multimédia sur un réseau local ne garantissant pas une qualité de service optimale. Il spécifie aussi les protocoles, les méthodes et les éléments du réseau qui sont nécessaires à l'établissement de connections multimédia point à point, multipoint et de conférences multimédia entre trois parties et plus.

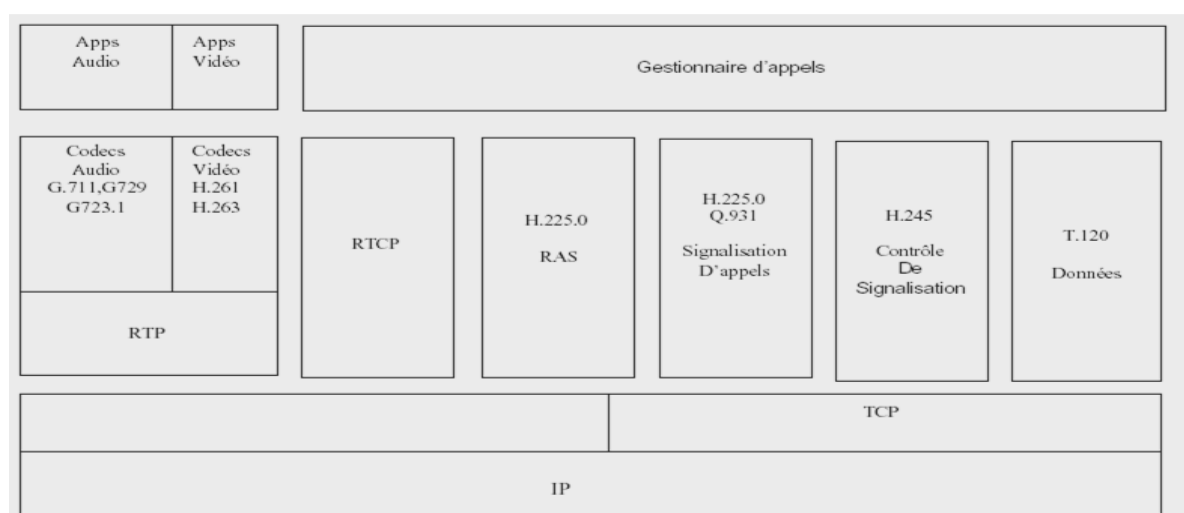


Figure 1.7 La pile protocolaire du Terminal H323

1.3.2 Le protocole MGCP :

MGCP est le sigle de **Media Gateway Control Protocol**, développé par Telecordia et Level 3 Communication ; c'est un protocole asymétrique (client-serveur) de VoIP. Il se distingue par exemple des protocoles SIP et H323 qui, eux sont symétriques (pair-à-pair). Il fonctionne au niveau applicatif et permet d'offrir une couverture plus large en fédérant toutes les signalisations, qu'elles soient de type IP ou RTC entre autres. C'est le maître d'œuvre de l'interopérabilité entre tous les protocoles de signalisation et tous les réseaux, de quelque nature qu'ils soient, qu'il s'agisse de la signalisation SS7, utilisée dans un réseau commuté, H.323 ou SIP. Le protocole MGCP est conçu pour relier et faire communiquer l'ensemble de ces réseaux. **MGCP** est aujourd'hui massivement utilisé par les fournisseurs d'accès Internet pour assurer le contrôle et l'administration à distance des boîtiers (*box*) mis à disposition de leurs abonnés

1.3.3 Le Protocole d'Initiation de Session (SIP) :

a. Introduction :

Développé par l'IETF et présenté dans la RFC 2543 en 1999 jusqu'à la nouvelle RFC 3261, le protocole d'initiation de session (SIP) est un protocole de signalisation appartenant à la couche application du modèle OSI. Son rôle est d'ouvrir, modifier et libérer les sessions entre un ou plusieurs utilisateurs. L'ouverture de ces sessions permet de réaliser de l'audio ou vidéoconférence, de l'enseignement à distance, de la voix (téléphonie) et de la diffusion multimédia sur IP. Notons qu'avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode multicast, en mode point à point ou dans un mode combinant ceux-ci. Pour ouvrir une session, l'utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de s'accorder sur la compatibilité de leur média. Ainsi, SIP peut relier des stations mobiles en transmettant ou redirigeant les requêtes vers la position courante de la station appelée. Notons que SIP possède l'avantage de ne pas être attaché à un médium particulier et est censé être indépendant du protocole de transport. De plus il peut être étendu et s'adapter aux évolutions futures. Le SIP maintient les informations suivantes entre les participants :

- La localisation des usagers
- La disponibilité des usagers, leur accessibilité, et leur intention d'accepter ou non une communication.
- Les capacités des terminaux, permettant de déterminer les types de media et leur paramètre utilisable pour la communication.
- L'établissement de session, pour 'sonner' le dispositif distant, et rétablir la session media entre l'appelant et l'appelé.
- La gestion de session, y compris le transfert des flux en cours de communication, la modification des paramètres de session, et l'invocation de services.

b. Architecture de SIP

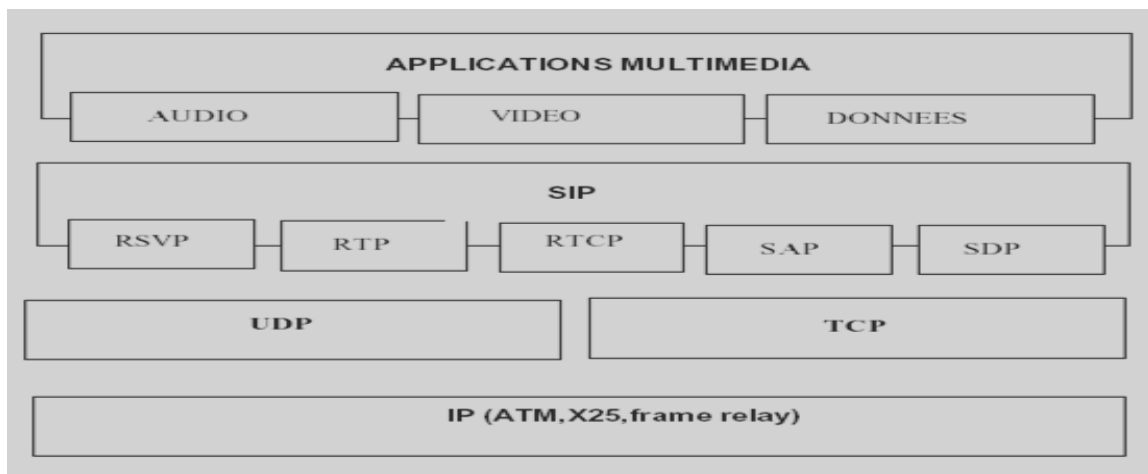


Figure 1.8 L'architecture de SIP

A chacune des couches de l'architecture SIP sont associés des protocoles tels que :

- **RSVP** : (Resource Reservation Protocol) : protocole utilisé pour réserver les ressources réseaux sur IP.

- RTP : (Real Time Transport protocol) : protocole de transport des données en temps réel
- RTCP : (Real Time Control Protocol) : protocole qui assure le contrôle de flux des données multimédia
- SAP : (Session Announcement Protocol) : protocole pour annoncer si les sessions multimédia ouvertes sont en multicast
- SDP : (Session Description Protocol) : protocole de description des sessions multimédia

1.3.4 Le protocole Skinny :

Le Skinny Client Control Protocol (*SCCP*) est un protocole de communication, développé par Cisco. Le H.323 étant trop rigoureux pour certaines utilités de la téléphonie IP (comme le renvoi d'appel, le transfert, la mise en attente), Cisco a mis en place ce protocole beaucoup plus léger qu'est le SCCP (il utilise le port 2000). L'avantage de Skinny est qu'il utilise des messages prenant très peu de bande passante c'est pourquoi il est utilisé pour les communications entre les téléphones IP et le CallManager, ainsi que pour contrôler une conférence.

Conclusion :

La voix sur IP procure des avantages certains aux entreprises et aux utilisateurs. Un seul réseau est utilisé pour la voix, la vidéo et les données, ce qui a pour conséquence de réduire les frais d'exploitations. Dans ce chapitre, nous avons présenté le principe de la VoIP. Nous avons également étudié les protocoles qui permettent ce genre d'applications. Parmi ces protocoles, nous avons étudié les protocoles de transports et de contrôles en temps réel RTP et RTCP qui utilisent le protocole UDP pour le transport de la voix et de la vidéo.

Chapitre 2

VoIP et Contraintes

2.1 Les paramètres de la voix sur IP :

Les aspects déterminants pour la qualité de la voix sur un réseau sont le traitement du signal vocal, l'intelligibilité, le délai de bout en bout et l'écho. Ils dépendent des différents composants de la chaîne de transmission, de leur paramétrage, de l'architecture générale de la chaîne, et dans le cas de la VoIP des flux concurrents. Ces aspects sont les suivants :

- Traitement du signal de parole : avant sa transmission, le signal est numérisé, codé et éventuellement compressée, avant d'être transmis.
- Le délai de bout en bout est le temps de propagation de la voix à travers le réseau de l'émetteur vers le récepteur.
- L'écho est le son émis par l'émetteur qui lui revient.

2.1.1 Le seuil de tolérance pour la VoIP :

La problématique de la qualité de la voix sur IP est particulière. La transmission de données classique (fichiers, messages, transactions, etc.) ne supporte aucune perte en ligne sous peine de graves conséquences pour l'interprétation et l'utilisation de ces données par l'équipement récepteur, mais elle supporte en revanche une dérive importante en terme de durée d'acheminement. Peu importe qu'un paquet arrive avec 100 ms de retard. Le comportement attendu pour la voix est exactement inverse, 1% ou 2% de perte de données de voix en ligne ne sont pas trop gênante pour la qualité du service de VoIP, mais en revanche une variation fréquente de 100 ms sur le délai de transit est catastrophique et rend le service inutilisable. La voix attend donc du transport IP l'inverse de ce qu'exigent les données. Cette formulation n'est qu'un raccourci, car en fait le transport de la voix exige beaucoup plus : il bénéficiera évidemment de l'intégrité exigée pour le transport des données laquelle est garantie par les réseaux modernes bien qu'il puisse s'en affranchir dans une certaine limite, mais exigera beaucoup plus au niveau des autres paramètres, notamment en ce qui concerne la stabilité du réseau dans le temps.

2.1.2 Les codecs et leurs débits :

Le paramètre débits pour les codecs (compression / décompression) est structurant en VoIP. Le codec détermine le débit de la voix et dimensionne par la même le flux de données numériques que va générer la transformation d'un échantillon temporel de voix analogique. Les codecs sont répertoriés par leur nom à l'ITU. Le tableau 2.1 donne les débits des codecs utilisés en VoIP.

Le choix du codec est un compromis entre la qualité des services souhaités et la capacité de l'infrastructure IP à délivrer une bande passante et des paramètres de QoS qui vont impacter cette qualité. Le paramètre le plus déterminant auquel nous nous intéressons pour commencer est la bande passante que l'on met en regard du nombre de communications simultanées à écouler.

Tableau 2.1 Bilan de bande passante en fonction du codec

Codec	Débit	Durée de paquetage	Bande passante
G.711	64 kbit/s	5 ms	169.6 kbit/s
G.711	64 kbit/s	10 ms	116.8 kbit/s
G.711	64 kbit/s	20 ms	90.4 kbit/s
G.711	64 kbit/s	30 ms	81.6 kbit/s
G.729	8 kbit/s	10 ms	60.8 kbit/s
G.729	8 kbit/s	20 ms	34.4 kbit/s
G.723.1	5.3 kbit/s	30 ms	22.9 kbit/s
G.723.1	6.3 kbit/s	30 ms	23.9 kbit/s

Le choix du codec G.711 permet de bénéficier, à réseau constant, de la meilleure qualité de service, tandis que les compressions G.726, G.728, G.729 et G.723 apportent avec elles des diminutions initiales de la QoS.

2.1.3 Implications de la Bande passante de Codecs :

Différents codecs produisent des qualités audio différentes, et consomment différents niveaux de bande passante. Certains utilisent plus de traitements que d'autres. Il est donc important d'utiliser le bon codec. Avant d'évoquer les différences entre les différents codecs les plus courants, introduisons un autre principe qui nous permettra précisément de calculer la bande passante utilisée. Lorsque nous avons besoin d'envoyer des données par l'intermédiaire d'un

réseau, les données sont paquets. Le 'package' contient des informations qui permettent aux données d'être envoyées vers leur destination et d'être reconstruites correctement. Le flux audio encodé a besoin d'être paquets dans les paquets RTP. En réalité, les paquets RTP ont besoin d'être paquets à l'intérieur de paquets UDP qui sont eux-mêmes paquets dans les paquets IP (voir figure 2.1). Ethernet est le type de réseau le plus répandu.

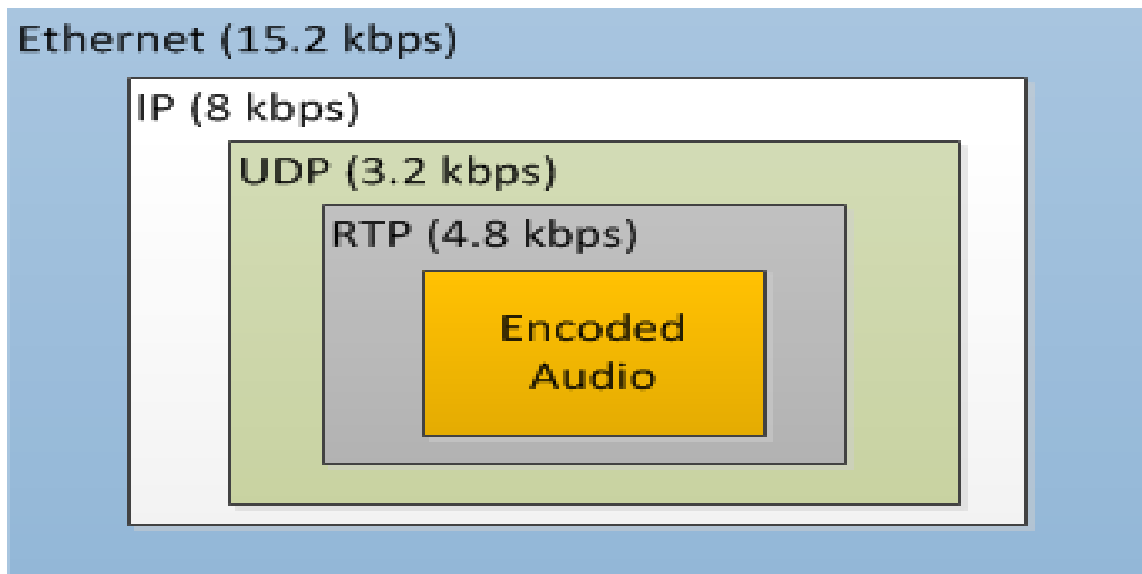


Figure 2.1 La paquetsisation de la VoIP

Quelque soit le codec utilisé, cet en-tête sera fixe et se décompose de la façon suivante:

- RTP – 4.8 kbps, UDP – 3.2 kbps, IP – 8 kbps, Ethernet (sans utilisation de QOS) – 15.2 kbps, la totalité de l'en-tête représente 31.2 kbps.

2.2 Les Codecs de la VoIP :

Maintenant que nous avons présenté les caractéristiques des codecs, voyons la différence entre les codecs les plus courants qui peuvent être utilisés dans l'encapsulation du signal audio dans un appel VoIP. Le tableau 2.2 montre la qualité audio espérée, la ressource processeur nécessaire pour encoder et décoder l'audio, la taille de base des paquets audio et

l'utilisation globale de la bande passante après avoir pris en considération l'entête globale. Un codec transforme les signaux analogiques au format numérique. Différents codecs ont différents besoins en bande passante.

Tableau 2.3: Qualité audio pour les différents codecs

Codec	Qualité Audio	Ressources CPU	Taille de base	Taille Total
G711	Elevé	Moyenne	64 kbps	95 ,2kbps
G722	Elevé	Moyenne	64 kbps	95 ,2kbps
G729	Elevé	Elevé	8 kbps	39,2kbps

2.3 Les contraintes de la VoIP :

Les contraintes de la VoIP se retrouvent en partie dans les paramètres de la QoS. En effet, la latence, la gigue et les pertes de paquets influent fortement sur la VoIP. Le tableau 2.4 dresse les critères communément admis pour une bonne transmission en VoIP.

Tableau 2.4 Récapitulatif des valeurs acceptables pour de la VoIP

	Bon	Moyen	Mauvais
Délai de transmission	$D < 150\text{ms}$	$150\text{ms} < D < 300\text{ms}$	$300\text{ms} < D$
Gigue de phase	$G < 20\text{ms}$	$20\text{ms} < G < 50\text{ms}$	$50\text{ms} < G$
Perte de données(perte de paquets)	$P < 1\%$	$1\% < P < 3\%$	$3\% < P$

2.3.1 Délai de transmissions :

Le délai de transmission est le temps que met l'information pour se déplacer d'un interlocuteur à un autre. Lorsque deux personnes sont l'une en face de l'autre, le temps de transit du signal sortant de la bouche d'un utilisateur est très faible. Lorsque les deux personnes sont à distance et communiquent par l'intermédiaire d'un réseau, la même

contrainte doit être vérifiée. Cette contrainte est de 300 ms entre le moment où le signal sort de la bouche jusqu'au moment où il arrive à l'oreille du destinataire. La valeur de 300 ms correspond à une limite supérieure. Pour ne pas avoir l'impression que le correspondant est très éloigné, surtout si le signal vocal et véhiculé en même temps que le signal vidéo, un délai de 150ms est préférable.

Le délai de transit (ou end-to-end delay dans la dénomination anglo-saxonne) est un des paramètres critiques influençant fortement la QoS d'un service de voix sur IP. C'est le temps que va mettre en moyenne un paquet IP contenant un échantillon de voix pour traverser l'infrastructure entre deux interlocuteurs. Ce temps de transit comporte quatre composantes.

a. Le délai d'échantillonnage :

C'est la durée de numérisation de la voix à l'émission puis de conversion en signal voix à la réception. Ce temps dépend du type de codec choisi et varie de quelques millisecondes avec le codec G.711 (échantillonnage 64 kbps) à plus de 50 ms en G.723 (échantillonnage 6,3 ou 5,3 kbps). C'est une des raisons pour laquelle le choix du codec impacte le score MOS d'appréciation de la clarté de la voix, indépendamment des autres caractéristiques de l'infrastructure.

b. Le délai de propagation :

C'est la durée de transmission en ligne des données numérisées. Cette durée est normalement très faible par rapport aux autres composantes du délai de transit, de l'ordre de quelques millisecondes.

c. délai de transport :

C'est la durée passée à traverser les routeurs, les commutateurs et les autres composants du réseau et de l'infrastructure de téléphonie IP. L'ordre de grandeur est de plusieurs dizaines de millisecondes, voir centaines de millisecondes.

d. Le délai des buffers de gigue :

C'est le retard introduit à la réception en vue de lisser la variation de temps de transit, et donc de réduire la gigue de phase. L'ordre de grandeur est de 50 ms. Les éléments d'infrastructure, notamment les routeurs, peuvent également mettre en oeuvre des buffers de gigue. La valeur

de la gigue va de quelques ms à quelques dizaines de ms. Voici un tableau provenant de la recommandation UIT-T G114 qui traite la qualité de la communication en fonction de la latence.

Tableau 2.5 : Valeurs tolérées de la latence

Classe	Latence	Etat de la Communication
n°1	0 à 150ms	Correct
n°2	150 à 300ms	Acceptable s'il n'y a que peu d'interactions
n°3	300 à 700 ms	Inutilisable pour une communication normale
n°4	>700ms	Utilisable uniquement en half-duplex

2.3.2 Impact du délai de paquets sur les paquets VoIP et le débit :

a. Un plus grand délai de paquets :

La voix numérisée est encapsulée dans RTP (*Real Time Protocol*), utilisé pour le transport de flux temps réel sur des réseaux IP, et dans le protocole UDP. UDP est préféré à TCP, car ce dernier met en œuvre des mécanismes destinés à garantir la fiabilité du transport (comme la retransmission des paquets en cas de perte), généralement incompatibles avec les fortes contraintes de délai des flux temps réel. Comme nous l'avons vu précédemment, à la sortie du codec sont formés des paquets RTP. Un des problèmes majeurs est de savoir qu'elle doit être la taille du paquet RTP. En effet, il y a un compromis au niveau de l'émission, car l'empaquetage est une source de délai. L'empaquetage est le temps nécessaire au remplissage d'un paquet par des données. Plus la taille du paquet est grande plus le remplissage prendra du temps, mais en contrepartie l'*overhead* (surdébit engendré par les en-têtes introduit par les différents protocoles) aura été optimisé. On a donc là aussi un compromis entre délai et bande requise. Par exemple une charge en terme d'octets de l'ordre de 160 octets pour une sortie de codec G.711 à 64 kbps. On peut noter par ailleurs que l'influence du header décroît lorsque le débit physique augmente. En effet, pour transmettre un header de 20 octets à 2 Mbps il faut 80 μ s, alors qu'à 54 Mbps, il faut 3 μ s environ.

La figure 2.2 compare deux scénarios avec des périodes de mise en paquet différentes.

1. Dans le premier scénario, portions de 20 ms de voix (160 échantillons PCM) sont mises en paquets. Le débit de paquets est l'inverse de la période de mise en paquet. Si un paquet est effectué toutes les 20 ms, 50 paquets sont générés par seconde. Pour un total de 60 ms de voix, trois paquets, chacun comportant au moins 20 ms de voix, sont nécessaires.
2. Dans le deuxième scénario, des morceaux de 30 ms de voix (240 échantillons PCM) sont mises en paquets. Cette mise en paquets se traduit par une baisse du taux de paquets de 33,3 pps. Pour la 60 ms de voix indiqué dans la figure, seuls les deux paquets (transportant 30 ms de voix chacun) sont générés, de sorte que la tête IP est réduite d'un tiers par rapport au premier scénario.

La valeur par défaut pour la période de mise en paquet sur la plupart des périphériques VoIP de Cisco est de 20 ms. Cette valeur par défaut est la valeur optimale pour la plupart des scénarios.

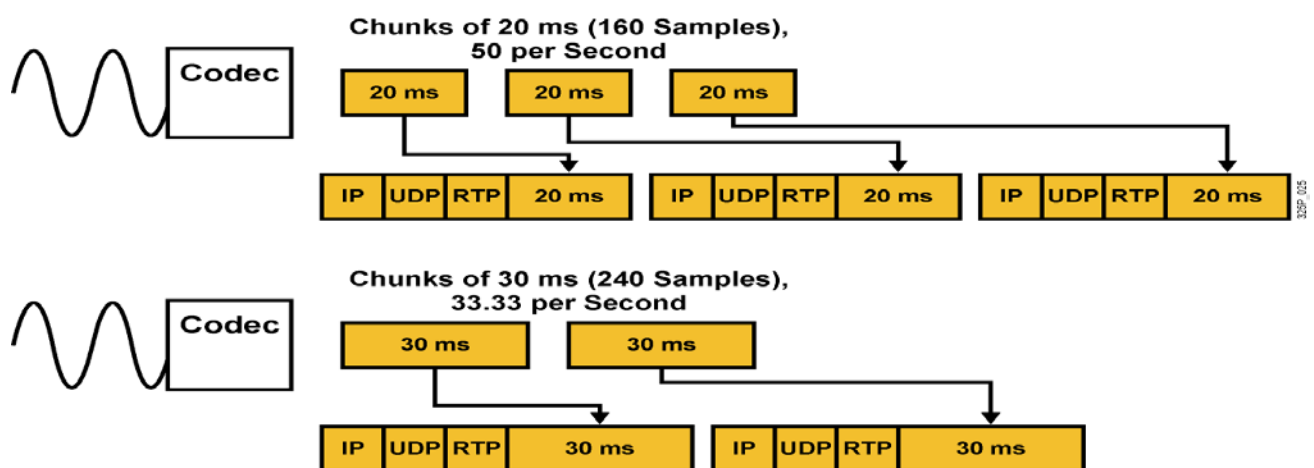


Figure 2.2 : Comparaison de deux scénarios de paquetisation avec des périodes de mise en paquet différentes.

b. Taille des paquets VoIP

La taille des paquets a une importance considérable. En effet, les entêtes se rajoutant au signal, la taille des paquets devient importante si le codec a un débit nécessaire important. Le

tableau 2.6 montre quelques exemples de taille de paquets en fonction du type de codec et de la fenêtre utilisée.

Tableau 2.6 Des exemples d'encapsulation VoIP avec des codecs différents et des périodes de mise en paquet de 20 et 30 ms.

Codec et Période de paquets	G.711 20 ms	G.711 30 ms	G.729 20 ms
Codec bandwidth (kbps)	64	64	8
Packetization size (bytes)	160	240	20
IP overhead (bytes)	40	40	40
VoIP packet size (bytes)	200	280	60
Packet rate (pps)	50	33.33	50

c. L'en-tête de couche deux pour différents liens :

Le routeur reçoit le paquet VoIP à partir du réseau Frame Relay, supprime l'en-tête Frame Relay et encapsule le paquet VoIP dans une trame Ethernet à nouveau avant de passer le paquet sur le téléphone IP de réception. La figure 2.3 montre un exemple d'entête de couche 2, alors que le tableau 2.7 met en relief les valeurs des entêtes de couche 2.

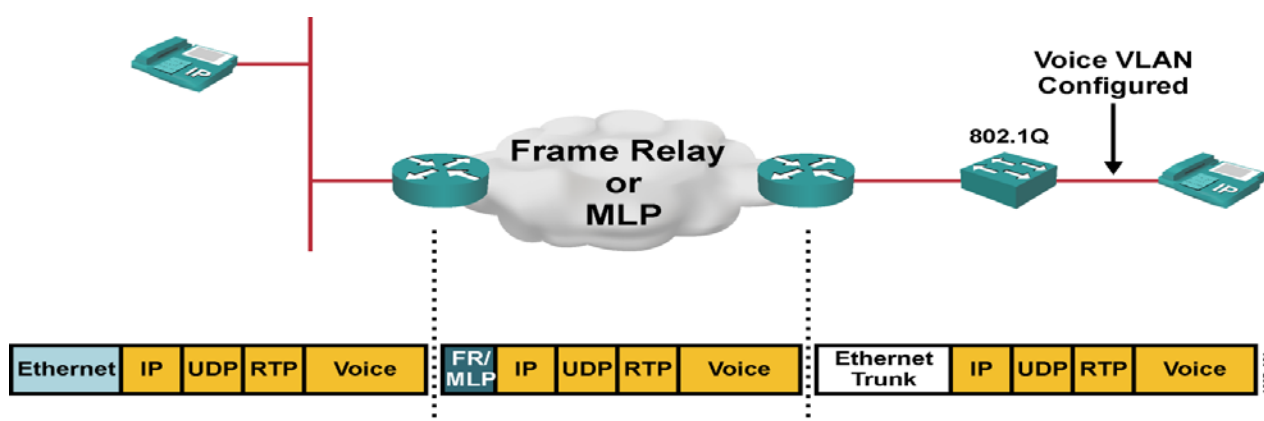


Figure 2.3 Exemple d'en-tête de couche 2.

Tableau 2.7 Valeurs des entêtes de couche 2 en Octets

Data-Link Protocol	Ethernet	Frame Relay	MLP	Ethernet Trunk

En-tête [Octets]	18	6	6	22
------------------	----	---	---	----

2.3.3 La gigue de phase :

Prenons l'exemple d'une communication, on imagine que toutes les millisecondes un paquet est envoyé de l'émetteur vers le récepteur. Pour celui qui reçoit la communication il est important qu'il reçoive les informations au même intervalle qu'elles sont parties, donc toutes les millisecondes. Le souci est, qu'en fonction de la charge du réseau il arrive que les paquets mettent plus ou moins de temps à arriver à destination ce qui crée un décalage lors de la réception et rend la communication inaudible. La variation de temps de transit, ou gigue de phase, est la conséquence du fait que tous les paquets contenant des échantillons de voix ne vont pas traverser le réseau à la même vitesse. Cela crée une déformation de la voix ou un hachage. La gigue de phase est indépendante du délai de transit. Le délai peut être court et la gigue importante ou inversement. La gigue est une conséquence de congestions passagères sur le lien. Le problème de la gigue est que les données ne sont plus transportées de manière constante ce qui crée une valeur de gigue de quelques millisecondes à plusieurs dizaines de millisecondes. Pour répondre à ce problème différentes solutions existent et notamment :

- Utilisation de buffer : Il permet de compenser de décalage créé par la gigue.
- Répéter le contenu du dernier paquet pour combler le vide.

2.3.4 La perte de paquets :

Un phénomène assez courant qui persiste sur les réseaux est la perte de paquets (données). Le souci avec la VoIP est qu'au-delà d'un certain seuil, la communication devient incompréhensible. Les pertes de paquet sont dues aux congestions sur le réseau qui entraînent des rejets de paquets, ou à une gigue excessive provoquant des rejets de paquets dans les buffers ne pouvant accueillir tous les paquets arrivés en retard. Une perte supérieure à 5% entraîne une détérioration trop importante au niveau de la qualité de service VoIP. Pour garder une qualité d'écoute correcte il ne faut pas que ces pertes excèdent 1 ou 2%. En temps normal il suffirait d'utiliser un protocole avec une garantie d'acheminement, mais avec la contrainte de temps réel il est impossible de retransmettre les données perdues sans créer une gigue trop importante.

- Pour contourner ce problème on peut aussi répartir l'information sur plusieurs paquets de façon à introduire une redondance des données. En cas de pertes de paquets, le codec dispose ainsi d'une copie du paquet à retransmettre.
- La transmission de la voix par paquets s'appuie sur le protocole RTP. Ce dernier permet de transmettre sur IP les paquets de voix en reconstituant les informations même si la couche de transport change l'ordre des paquets. Il utilise pour cela des numéros de séquence et s'appuie sur UDP.
- Les contraintes temps réel de délai de transit évoquées plus haut rendent inutile la retransmission des paquets perdus : même retransmis un datagramme RTP arriverait bien trop tard pour être d'une quelconque utilité dans le processus de reconstitution de la voix, dans la VoIP on ne retransmet donc pas les données perdues.
- Une perte de données régulière mais faible est moins gênante en voix sur IP que des pics de perte de paquets espacés mais élevés. En effet, l'écoute humaine s'habitue à une qualité moyenne mais constante et en revanche supportera peu de soudaines dégradations de la QoS.

Conclusion :

Entre les délais de transition, le temps d'encodage, les pertes supportées et la gigue de phase on se rend compte, à quel point le réseau sur lequel est utilisé la VoIP doit être configuré avec soin. Aucun paramètre ne doit être laissé au hasard aussi bien dans le choix du codec que le réglage des priorités des différents paquets. Contrairement à des données classiques il est impossible de tolérer le moindre écart du réseau sous peine d'avoir très rapidement une communication inaudible. Les options seront donc soigneusement paramétrées en fonction du débit disponible et du nombre simultané de communications VoIP. Ainsi des outils sont disponibles pour aider à la mise en place d'un réseau VoIP .

Chapitre 3

IPv6 et Qualité de Service (QoS)

Introduction :

Dans cette partie de notre travail, nous allons essayer de montrer ce que le nouveau protocole IPv6 va apporter pour améliorer la qualité de service dans les réseaux IP, et spécialement pour les applications temps réel embarqué, telles que la VoIP. Le but de ce chapitre est de mesurer les paramètres de qualité de services sur des communications VoIP en implémentant différents mécanismes qui introduisent la qualité de service (QoS) .

3.1 Qualité de services (QoS) :**3.1.1 Définition :**

La qualité de service, est un ensemble de caractéristiques et de performances de service qui sont perçues et exprimées par l'utilisateur. Elle se manifeste par des paramètres pouvant prendre des valeurs qualitatives, c'est à dire qui ne peuvent pas être mesurées directement mais perceptibles par l'utilisateur, ou bien se traduit par des valeurs quantitatives qui sont directement observées et mesurées aux points d'accès. En effet, pour IP les paquets sont tous traités de la même façon sans aucune différenciation. Ainsi, un flux "temps réel" (comme le streaming vidéo) et la messagerie sont traités avec le même service qui est le "Best Effort". Ils sont stockés dans la file d'attente selon le principe FIFO (First In First Out). C'est pour cela que le temps de transmission peut être long, et surtout il n'est pas constant, d'où l'apparition de la **gigue**, phénomène auquel la transmission multimédia et en particulier la transmission audio sont très sensible. Les protocoles RTP/RTCP permettent de régler les problèmes aux extrémités. Ce sont des protocoles de bout en bout, comme TCP qui ne traitent pas les problèmes liés à l'augmentation du trafic et au comportement des routeurs pour la résolution de cette congestion.

Depuis 1989, des propositions ont été faites au sein de l'IETF , pour offrir une qualité de service adaptée aux besoins de l'application. Le protocole RSVP (Resource ReSerVation Protocol) a été adopté. Il est intéressant de noter qu'on ne parle de la qualité de service que s'il y a une dégradation de la performance d'un réseau.

3.1.2 Les Mécanismes de qualité de service :

La transmission de la voix humaine à travers un réseau IP, nécessite des performances respectables ainsi qu'une grande stabilité. Une conversation téléphonique est gravement perturbée par d'éventuels retards ou coupures. Il faut donc veiller à ce que le flot soit le plus continu possible et que les variations restent faibles.

3.1.3 Le Service Best effort :

Les réseaux IP classiques offrent un simple service, qui est le service best effort. Un tel modèle de service permet aux routeurs d'être sans état et de ne garder aucune information à propos du trafic. Comme IP est un protocole sans connexion, le concept du contrat de trafic n'existe pas. Les congestions peuvent entraîner des pertes transitoires ou bien des pertes de longue durée. Le protocole d'extrémité TCP a été conçu pour assurer la fiabilité et la retransmission si nécessaire. Par ailleurs, comme le réseau n'effectue pas le contrôle de congestion, cette fonction doit impérativement être assurée par les équipements d'extrémités.

3.1.4 Le Services garantis (IntServ) :

1. Présentation :

Le modèle IntServ définit une architecture capable de prendre en charge la QoS en définissant des mécanismes de contrôle complémentaires, sans toucher au fonctionnement IP. C'est un modèle basé sur le protocole de signalisation RSVP.

a. Le protocole RSVP (ReSerVation Protocol) :

RSVP est un protocole de signalisation pour allouer dynamiquement de la bande passante aux applications orientées réseaux dans des environnements traditionnellement datagramme (voir figure 3.1). RSVP est utilisé dans le modèle IntServ. RSVP rend obligatoire la demande de QoS par le récepteur (l'application participante) plutôt que par l'émetteur (l'application source), il a les caractéristiques suivantes :

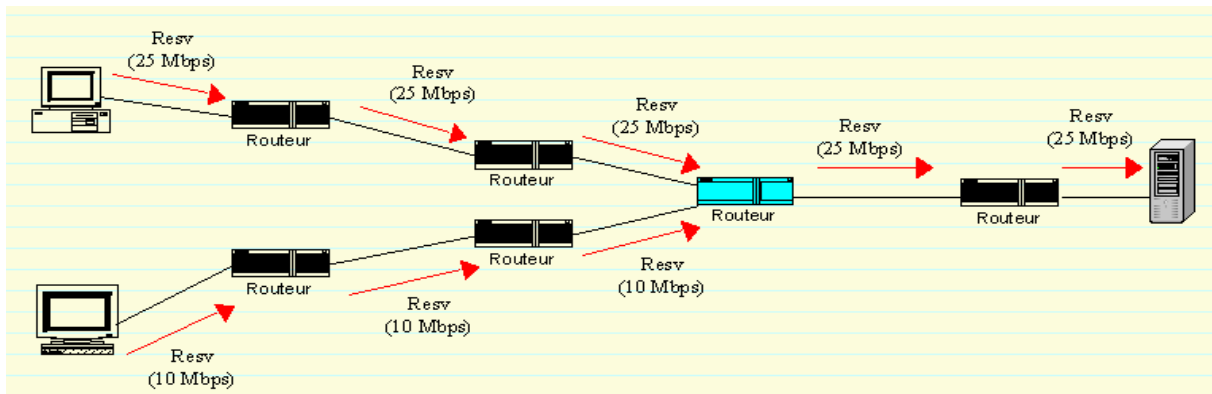


Figure 3.1 Les équipements d'interconnexions (routeurs), sur le chemin du flot des données, répondent aux requêtes RSVP , établissent et maintiennent les connexions.

- Les routeurs communiquent via RSVP pour initialiser et gérer la QoS réservée aux sessions.
- RSVP travaille au dessus de IP (IPv4 ou IPv6) et occupe la place d'un protocole de transport.
- RSVP est encapsulé dans des paquets UDP.
- RSVP passe de façon transparente les routeurs non RSVP.
- RSVP n'est pas un protocole de routage. Il est censé travailler avec les protocoles de routage unicast et multicast.
- RSVP fait des réservations de ressources pour les applications unicast et multicast et s'adapte dynamiquement aux évolutions (participants, changements de routes). Il demande des ressources dans une seule direction et traite l'émetteur et le récepteur de manière différente.
- Il est utilisé par un "host" pour le compte d'une application, pour demander une QoS au réseau (bande passante garantie, débit crête, etc.). Il est utilisé par les routeurs pour le contrôle de la QoS et l'établissement et le maintien du service demandé.
- RSVP peut être utilisée avec RTP/RTCP, mais ce n'est pas obligatoire.

b. Comment fonctionne RSVP :

Sept Types de Messages RSVP ont été prévus :

- Path: envoyé par la source pour indiquer la liste des routeurs du chemin suivi par les données;
- Resv: demande de réservation;
- PathErr: message d'erreur concernant le chemin;
- ResvErr: message d'erreur de demande de réservation;
- PathTear: indique aux routeurs d'annuler les états concernant la route;
- ResvTear: indique aux routeurs d'annuler les états de réservation (fin de session);
- ResvConf (optionnel): message de confirmation envoyé par le routeur au demandeur de la réservation;

Un message RSVP est constitué d'un en-tête et d'un nombre variable d'objets qui dépend du type du message.

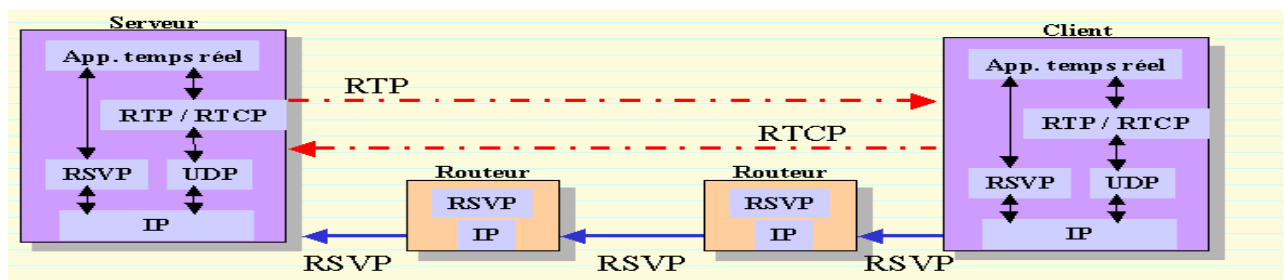


Figure 3.2 Fonctionnement de RSVP

3.1.5 Les Services différenciés (DiffServ) :

a. Présentation:

La méthode Diffserv propose d'abandonner le traitement du trafic sous forme de flux pour le caractériser sous forme de classes. Il n'est plus nécessaire de maintenir des états dans les routeurs pour chacun des flux. Ceci permet son utilisation à grande échelle. Le trafic conditionné est identifié par un champ DS ou un marquage du champ *Type of Service* (ToS)

de l'en-tête de paquet IPv4 ou l'octet *Class of Service* (COS) d'IPv6. Ce champ d'en-tête IP porte l'indice de la Classe de Service DSCP (Differentiated Service Code Point).

Les opérations de classification, contrôle et marquage sont effectuées par les Routeurs périphériques (*Edge Router*) tandis que les routeurs centraux (*Core Router*) traitent les paquets en fonction de la classe codée dans l'en-tête d'IP (champ DS) selon un comportement spécifique : le PHB (*Per Hop Behavior*) codé par le DSCP (Differentiated Service Code Point).

1. DSCP : c'est le champ qui identifie le traitement que le paquet doit recevoir. Ce champ est codé sur 6 bits et fait parti des 8 bits codant le champ TOS d'IPv4 où le champ classe de trafic d'IPv6.

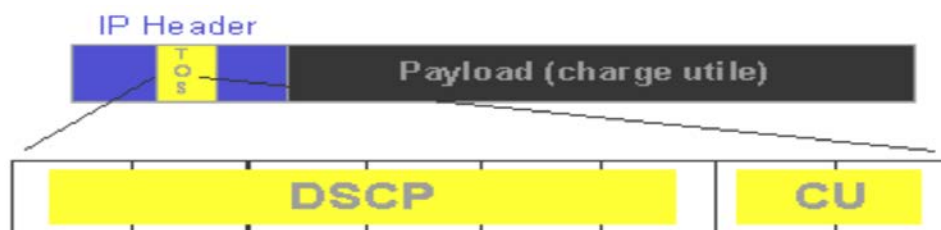


Figure 3.3 Le DSCP dans le champ TOS de l'en-tête IP

DSCP : Differentiated Service Code Point (6bits)

CU : Currently Unused (2bits)

Pour la classe EF DSCP = 101110

Pour la classe AF DSCP = 12 codes

b. Classification et conditionnement du trafic :

La classification s'effectue suivant une ou plusieurs valeurs contenues dans l'entête IP (exemple : adresse source - destination, port source - destination, *protocol ID*, etc.). Celle-ci faite, elle dirige le paquet vers la fonction de marquage appropriée comme le montre la figure 3.4 :

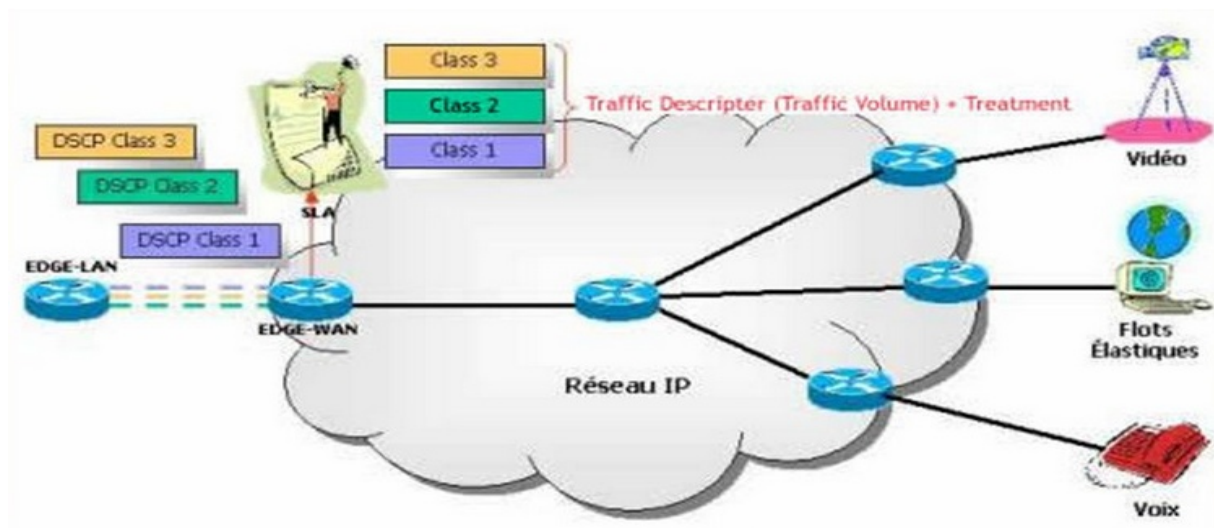


Figure 3.4 Classification Marquage et conditionnement du trafic

Une fois les paquets marqués, ils sont envoyés à leur destination puis à chaque routeur *DS-capable*. Ils reçoivent le service associé à leur classe. Il n'est pas précisé par le groupe de travail Diffserv comment le classificateur est paramétré pour effectuer cette classification ou plus exactement, qui le paramètre. Cela doit être fait manuellement, aux bons soins de l'administrateur (qui paramètre les tables de marquage des paquets en fonction d'une table d'adresse source, par exemple, donnée au *edge router*), ou par le biais d'un protocole de signalisation. RSVP pourrait d'ailleurs très bien convenir car celui-ci n'étant pas un protocole de signalisation propre à Intserv uniquement, on pourrait l'utiliser afin de signaler les classes que les routeurs auront à traiter.

3.1.6 Mise en oeuvre de DiffServ :

a. Principe DiffServ :

Le trafic entrant dans le réseau est classifié, et se voit attribué des ressources, en fonction des critères de gestion du modèle de service. Aucune réservation n'est faite, mais un dimensionnement adéquat assure qu'il aura assez de ressources dans le réseau pour les demandes de toutes les applications. Les garanties données par le modèle vont dans le sens du partage des ressources disponibles. Pour offrir un certain niveau de QoS, les classifications donnent un traitement différentiel à des applications sensées avoir des besoins plus exigeants c'est-à-dire des priorités. Une fois le mécanisme de priorité disponible, la mise en place d'une qualité de service suppose la définition des règles pour utiliser ce mécanisme. Pour garantir le

respect de ces règles, on emploie une politique qui les impose aux limites d'un périmètre. On parle de "routing policies".

b. Optimisation de trafic: MPLS (Multi-Protocol Label Switching) :

Il s'agit d'un nouveau standard de l'IETF. Dans le même esprit que l'architecture DiffServ, MPLS permet de réduire le coût des traitements associés au relayage des paquets en les reportant à la périphérie du réseau et en en réduisant la fréquence. Il apporte aussi un mécanisme de routage hiérarchique efficace, c'est-à-dire des tunnels permettant de gérer les réseaux privés virtuels (VPN). Il permet également de pouvoir acheminer tous les types d'applications, données, audio, vidéo, ainsi que de différencier le trafic selon les classes de service employées.

- Routeur d'extrémité (LER : Label Edge Router) : situé à la frontière de réseau. Il est responsable d'insérer et de retirer le Label à un paquet au moment de son entrée et de sa sortie.
- Routeur (commutateur) central (LSR : Label Switcher Router) : responsable de la commutation des paquets en fonction du Label. Dans le coeur de réseau, les LSR lisent uniquement les labels, et non les adresses des protocoles de niveau supérieur c'est à dire les adresses IP.

3.2 Le Protocole IPV6 :

3.2.1 Caractéristiques du nouveau protocole Internet IPV6 :

L'évolution d'Internet dont la taille croît massivement au fil du temps a entraîné l'apparition de deux principaux problèmes :

- La saturation d'adresses IPv4.
- L'explosion de la taille des tables de routage.

La nouvelle version du protocole Internet s'appelle IPv6. Pour s'assurer que ce protocole ait autant de puissance et de flexibilité qu'IPv4, on l'a conçu sur les mêmes bases que ce dernier. La plupart des grandes caractéristiques et options d'IPv4 se retrouvent donc également dans IPv6. Cependant, si les deux versions sont très proches au niveau de la conception, elles se

différencient au niveau des détails d'implémentation. Les principales améliorations apportées à IPv6 sont les suivantes :

- IPv6 utilise des adresses de 128 bits.
- En-tête réduit et fixe pour un routage rapide.
- Options dans des en-têtes d'extensions.
- L'utilisation des options est devenue plus souple.
- Dans IPv4, chaque option se voit d'office attribué un champ de l'en-tête, qu'elle soit utilisée ou non. IPv6, par contre, utilise des en-têtes optionnels, qui n'existent que si l'option correspondante est utilisée.
- IPv6 permet d'allouer des ressources du réseau à une communication.
- Support de l'IPsec (en-têtes d'extensions spécifiques).
- Support de la QoS (Identifiants du flux dans l'en-tête).

3.2.2 Description du protocole IPv6 :

Le protocole IPv6 est composé des en-têtes suivantes :

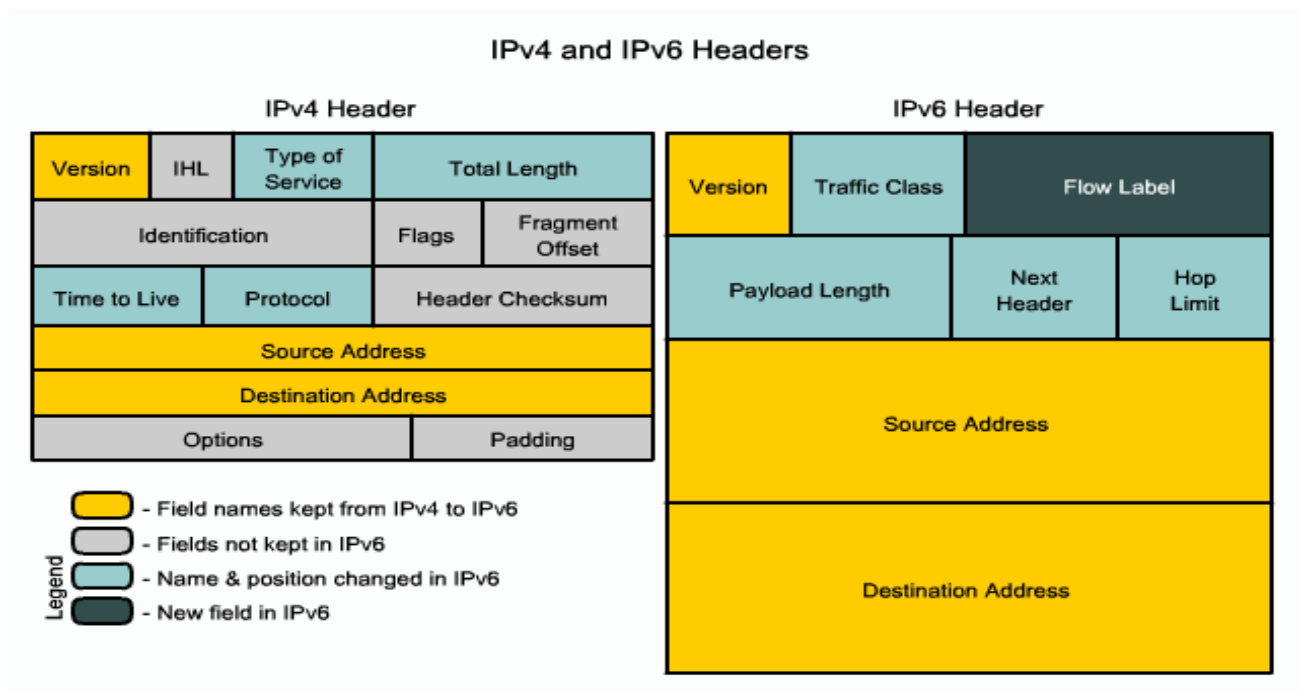


Figure 3.5 Comparaison des deux en-têtes IPv4 et IPv6

- Version :

Ce champ est identique à la pile IPv4, il sert justement à identifier le protocole de couche 3 du modèle OSI.

- Classe (Traffic Class) :

Le champ "Classe" est codé sur 8 bits. Il définit la priorité du datagramme afin que des nœuds origines et des routeurs transmetteurs puissent identifier et distinguer la classe ou la priorité du paquet IPv6 en question.

- Label (Flow Label) :

Le champ "Label" est codé sur 20 bits. Il peut être utilisé par une source pour nommer des séquences de paquets pour lesquels un traitement spécial de la part des routeurs IPv6 est demandé. Ce traitement spécial pourrait être une qualité de service différente du service par défaut ou un service "temps réel".

- Longueur (Payload Length) :

Le champ "Longueur" est codé sur 16 bits. Il indique le nombre d'octet des données qui suivent cet en-tête IPv6. Il faut noter que les options de l'en-tête IPv6 sont considérés comme de la donnée et font donc partie du calcul du champ "Longueur".

- Entête suivante (Next Header) :

Le champ "en-tête suivante" est codé sur 8 bits. Il identifie le type de données ou de l'option qui se trouve derrière l'entête IPv6.

- Saut maximum (Hop Limit) :

Le champ "Saut maximum" est codé sur 8 bits. Il indique le nombre de routeur maximum que le datagramme pourra traverser. Identiquement au champ "TTL" de l'entête IPv4, il est décrémenté de 1 par chaque nœud que le paquet traverse.

- Adresse source (Source Address) :

Le champ "Adresse source" est codé sur 128 bits. Il représente l'adresse IP de l'émetteur.

- Adresse destination (Destination Address) :

Le champ "Adresse destination" est codé sur 128 bits. Il représente l'adresse IP du destinataire.

- En-têtes d'extension :

Pour ne pas avoir un en-tête IPv6 trop long et trop lourd à traiter, une série de champs des datagrammes IPv4 ont été mis en option dans des en-têtes d'extension. C'est l'émetteur qui choisit quelles extensions inclure dans le paquet.

3.2.3 Les avantages des en-têtes IPv6 :

- Grande flexibilité.
- L'émetteur n'utilise que les extensions qu'il estime utile.
- Il est possible de définir un grand nombre de nouveaux en-têtes d'extension.

Un en-tête d'extension commence toujours par un champ d'un octet nommé " prochain en-tête " (next header) indiquant le type du prochain en-tête d'extension (59 si aucun).

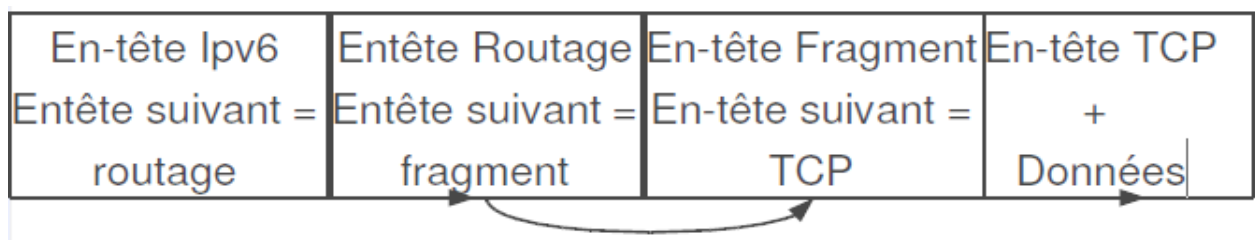


Figure 3.6 : Le Chaînage d'extensions IPv6

3.2.4 Représentation des adresses IPv6 :

Notation : "**x:x:x:x:x:x:x**" où x représente les valeurs hexadécimales des 8 portions de 16 bits de l'adresse.

Exemples d'adresse :

2001:0660:7401:0200:0000:0000:0edf:bdd7

3ffe:0104:0103:00a0:0a00:20ff: fe0a:3ff7

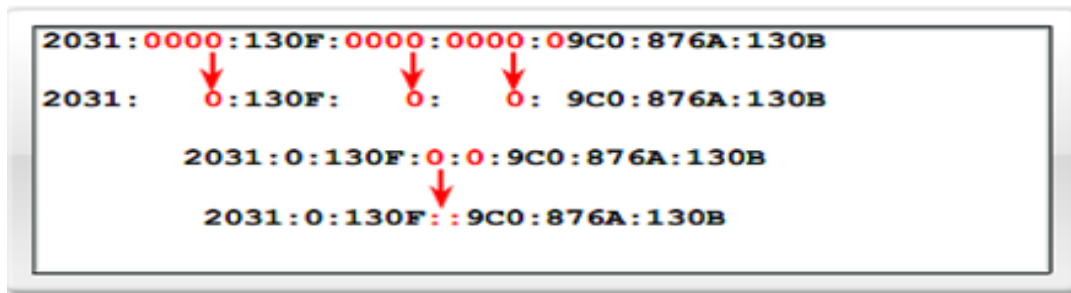


Figure 3.7: Représentation des adresses IPv6: forme abrégée

3.2.5 Les type d'adresse IPv6 :

- Unicast :

Une adresse unicast désigne une interface unique. Un datagramme envoyé vers une telle adresse est reçu par l'interface identifiée par l'adresse.

- Multicast :

Une adresse multicast désigne un ensemble d'interfaces. Un datagramme envoyé vers une telle adresse est reçu par toutes les interfaces identifiées par l'adresse

- Anycast

Une adresse anycast désigne un ensemble d'interfaces. Un datagramme envoyé vers une telle adresse sera reçu par une seule des interfaces désignées par l'adresse. L'interface qui reçoit le datagramme est celle située le plus près de l'émetteur.

3.2 6 Attribution des adresses IPv6 :

Les modes d'attribution d'une adresse IPv6 sont les suivants :

2. Stateless ou le mode non administré :

- Link local Neighbors Discovery .
- Stateless Auto-configuration .

3. Stateful ou le mode administré :

- Configuration Manuelle.
- DHCPv6

Dans les méthodes Stateless, la machine qui se configure ne reçoit du routeur qu' au maximum les 64 premiers bits de l'adresses IPv6. Il lui reste à définir les 64 derniers afin de constituer son adresse complète. Pour cela deux techniques existent:

- Génération selon le format EUI-64, basé sur l'adresse MAC de l'interface Ethernet utilisée (où celle d'une interface disponible sur la machine).
- Génération « aléatoire » des 64 derniers bits.

Afin d'éviter une duplication d'adresse dans le réseau, chaque machine qui se configure une adresse procédera à une vérification de duplication d'adresse (DAD = Duplicate Address Detection) en profitant d'ICMPv6 et plus précisément du principe de Neighbor Solicitation (remplaçant de ARP). L'idée est simple, si une station demande sur le réseau qui est la machine disposant de son adresse, et que personne ne répond, la station émettrice considère que c'est son adresse.

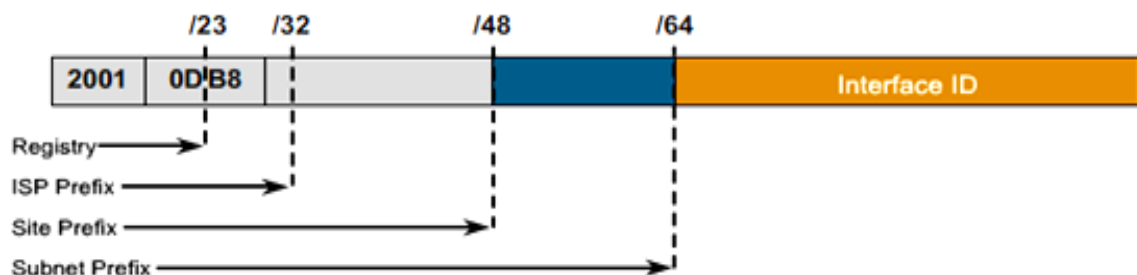


Figure 3.8 : Structure générale d'une adresse IPv6 (Global Unicast)

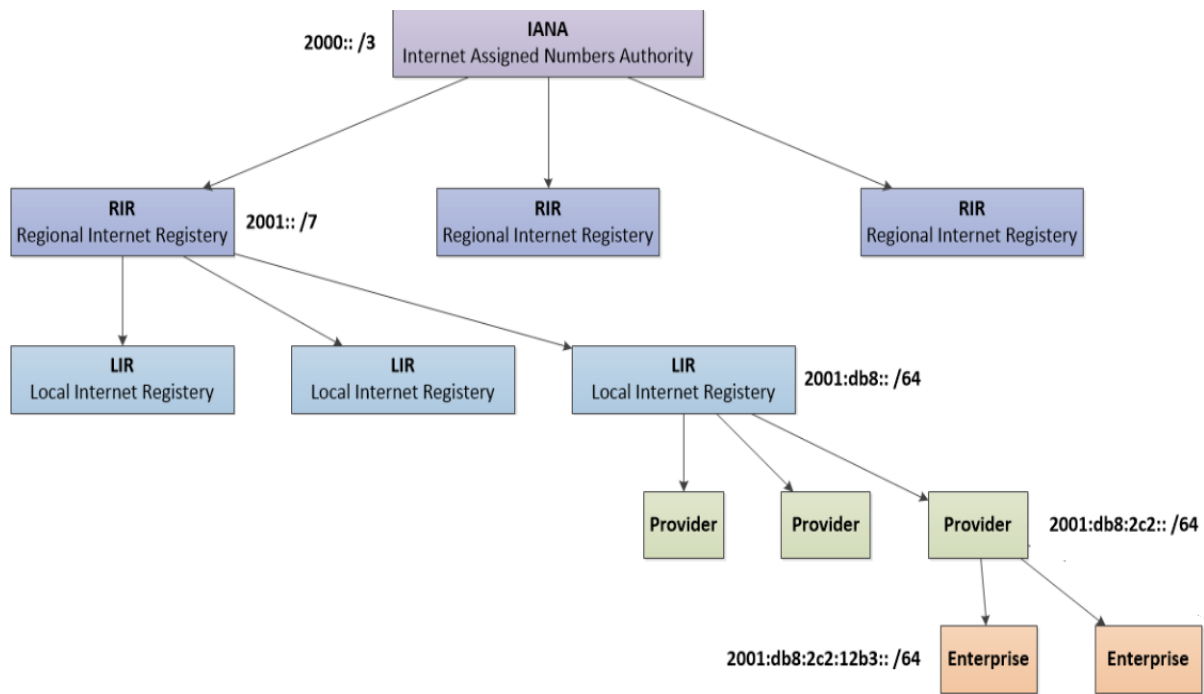


Figure 3.9 : Organisation de l'attribution des adresses IPv6 Globale

3.2.7 Configuration de routage avec IPv6 :

Les différentes méthodes de routage utilisé dans IPv6 sont :

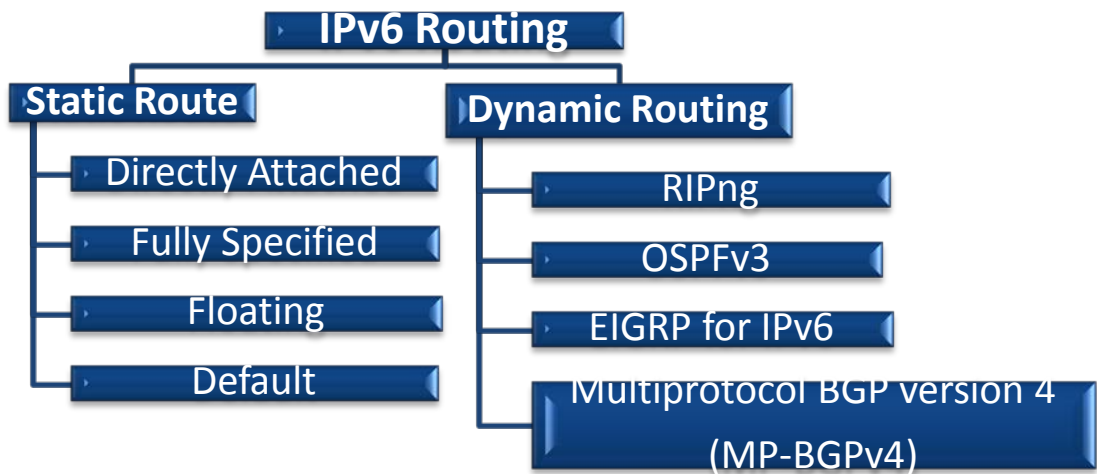


Figure 3.10: Les types de routage IPv6

3.2.8 Les Protocoles associés à IPv6 :

- ND (Neighbor Discovery) : découverte des voisins
- MLD (Multicast Listener Discovery) Gestion des groupes multicast basés sur IGMPv2

- MLDv2 équivalent d'IGMPv3 d' IPv4.
- ICMPv6 : Le protocole de contrôle d'IP a été revu pour Ipv4, ICMP sert à la détection d'erreurs, aux tests, à la configuration automatique des équipements. Ces fonctions sont mieux définies par IPv6. De plus, ICMPv6 intègre les fonctions de gestion des groupes de multicast et celles du protocole ARP.

3.3 Les Mécanismes de transition d'IPv4 à IPv6 :

Le principal objectif de la transition vers IPv6 est double. Il doit permettre à des stations de travail implémentant IPv6 et/ou IPv4 de communiquer entre-elles ainsi qu'à des stations et des routeurs IPv6 d'être déployés sur l'Internet de manière incrémentale et à grande échelle. A ceci, un troisième objectif sous-jacent consiste à proposer une transition la plus simple possible pour tous les utilisateurs finaux, les administrateurs de réseaux et les opérateurs réseaux.

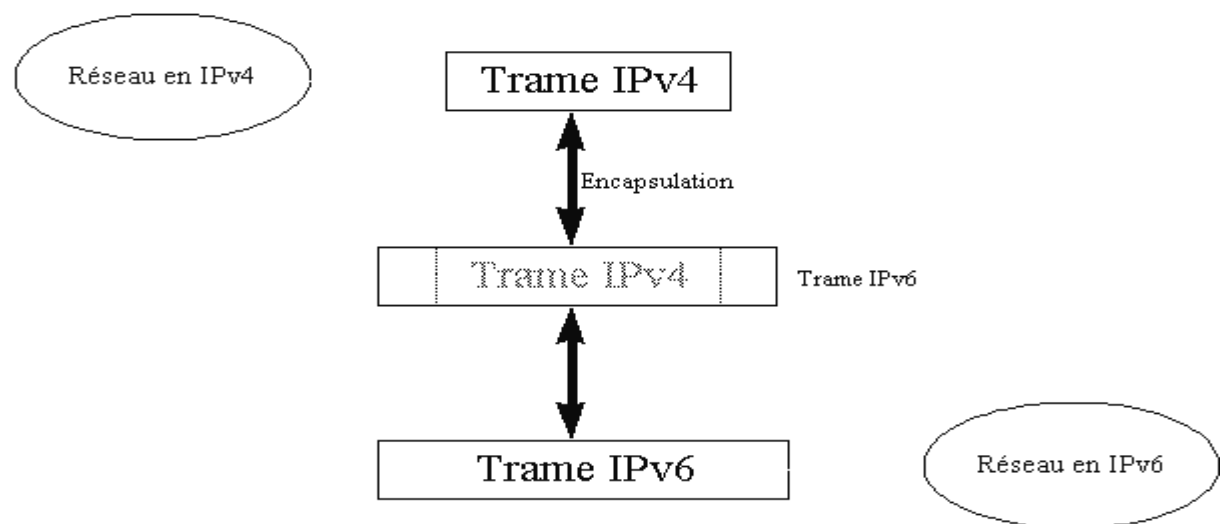


Figure 3.11: Encapsulation de trames IPv4 dans des trames IPv6.

3.3.1 Techniques Dual-stack (Double Pile) :

Elles fournissent un support complet pour IPv4 et IPv6. Les nœuds qui fournissent une implémentation complète d'IPv4 en plus de leur implémentation d'IPv6 sont appelés nœuds IPv6/IPv4.

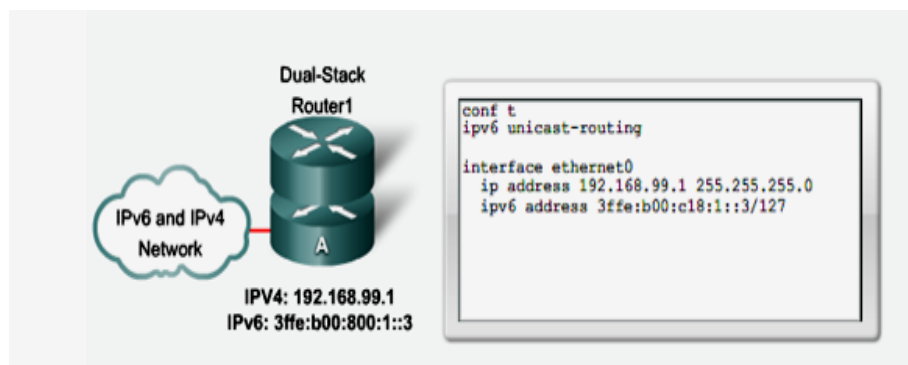


Figure 3.12 : Configuration Dual-Stack sur un routeur Cisco

3.3.2 Tunnels IPv6 sur IPv4 (Tunneling) :

Les tunnels sont généralement classés suivant la façon dont l'adresse du nœud à la fin du tunnel est déterminée.

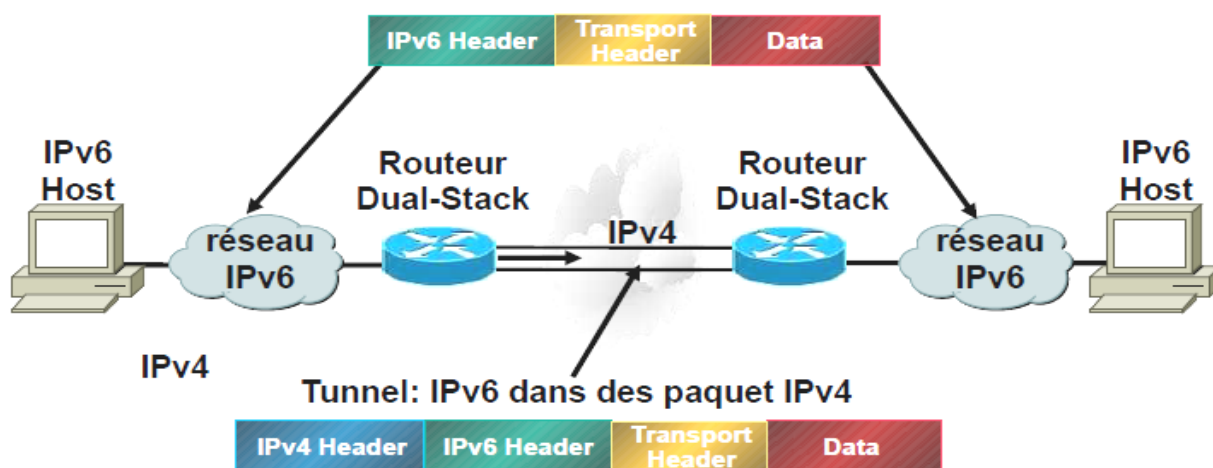


Figure 3.13: Tunnels IPv6 sur IPv4

- Si le nœud à la fin du tunnel n'est pas le nœud destination du paquet, son adresse doit être déterminée par l'information de configuration du nœud encapsulant. C'est un tunnel configuré.
- Si le nœud à la fin du tunnel est le nœud destination du paquet, et si l'adresse de ce nœud est IPv4-compatible, alors l'adresse IPv4 du nœud destination peut être dérivée de son adresse IPv6. C'est un tunnel automatique.

En plus d'ajouter un en-tête IPv4, le nœud encapsulant doit gérer les problèmes de fragmentation et les messages d'erreur ICMP se produisant dans le tunnel.

3.4 Apport du protocole IPv6 à la QoS :

3.4.1 Les apports d'IPv6 pour la Qualité de service :

En plus d'agrandir la plage d'adresses, IPv6 permet de gérer de la QoS. Voici quelques spécificités d'IPv6 répondant à des critères de QoS :



Figure 3.14 : L'en-tête IPv6 standard

- Simplification du format de l'en-tête :

Certains champs de l'en-tête IPv4 ont été enlevés ou rendus optionnels. L'en-tête est passé de 15 à 8 champs. Ceci réduit donc les coûts de gestion des paquets dans les situations classiques et limite le besoin en bande passante pour cet en-tête.

- Un processus de routage accéléré :
Permet d'imposer une route différente de celle offerte Routage libéral (Loose source routing): on indique une liste de routeurs à traverser, les tables de routage peuvent être utilisées pour aller de routeur en routeur .

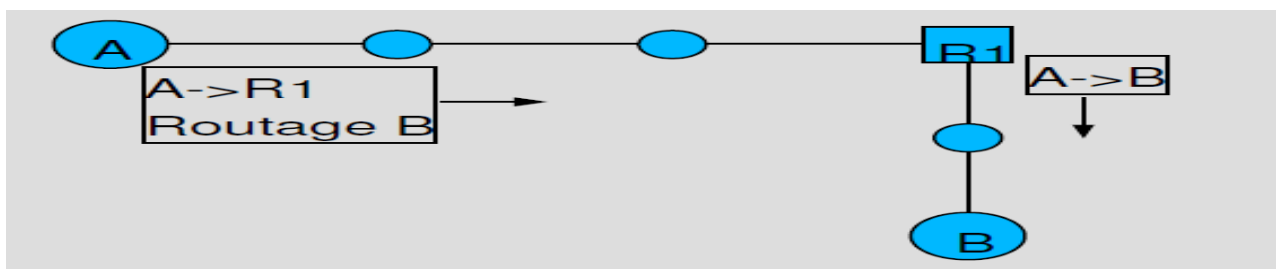


Figure3.15 : Routage IPv6

- Fragmentation :

IPv6 exige que chaque lien inter-réseaux ait une MTU (Maximum Transfert Unit) supérieure ou égale à 1280 octets. Pour tout lien n'ayant pas la capacité requise, les services de fragmentation et de réassemblage doivent être fournis par la couche inférieure à Ipv6.

- Labels relatifs aux flux d'informations (Identificateur de flux) :

Le champ label du flux peut être utilisé par une source pour nommer les séquences de paquets (unicast ou multicast) pour lesquels un traitement spécial est demandé (c'est ce qu'on appelle un flux) : QoS différente de celle prévue par défaut ou service temps réel. Ceci permet d'assurer, par exemple, des qualités de service très fiables ou des services "temps réel" vidéo ou audio.

- IPv6 et VoIP (utilisation des labels de flux) :

Outre le fait que les communications IP sont possibles en mode end-to-end, grâce à l'abondance des adresses IP, Ipv6 permet d'améliorer la performance de la VoIP , Le mode end-to-end permet de communiquer entre deux terminaux IP, directement reliés au réseau IP sans passer par le réseau commuté pour aboutir sur un téléphone standard, ni sans transiter par un ordinateur qui transformera les paquets IP en voix : les terminaux sont des " Téléphones IP " et transforment la voix en paquets de données et inversement, et sont directement connectés comme des nœuds de réseau.

- Classes de trafic :

Le champ Classe de trafic a été créé pour être utilisé par des nœuds d'origines et ou des routeurs transmetteurs pour identifier et distinguer différentes classes ou priorités de paquets IPv6. Cette gestion est effectuée par le protocole Diffserv (RFC 2474) qui permet d'exploiter ce champ "classe de trafic". L'émetteur de flux spécialisé (multimédia, temps réel, etc.) spécifie une classe de service à travers le champ classe de trafic. Les routeurs, équipés d'algorithmes (Packet Classifier), interprètent ce champ et mettent en oeuvre un traitement différencié (adaptation

file d'attente, etc.) à l'aide du répartiteur de paquet (packet scheduler). Ce champ comporte deux parties :

- DSCP: DiffServ Code Point : sur 6 bits qui contient les valeurs des différents comportements.
- CU : sur 2 bits, non utilisé.

Aujourd'hui, seuls deux types de comportement sont standardisés par l'IETF :

- Assured Forwarding (AF) : il définit 4 classes de service et trois priorités. Les classes sont choisies par l'utilisateur et restent les mêmes jusqu'au destinataire. La priorité peut être modifiée par les routeurs.
- Explicit Forwarding : comportement équivalent à une liaison louée à débit constant.

- Durée de vie maximale du paquet :

Les nœuds IPv6 ne sont pas obligés d'imposer un temps de vie maximum au paquet. Il y a donc une réduction des pertes d'information du fait d'une absence de paquets rejetés à la fin de cette durée.

3.4.2 La Qualité de service (QoS) :

Pour supporter la qualité de service, il faut pouvoir différencier et garantir certains flux. Les champs supportant la QoS sont "Flow label" et "Traffic Class" dans l'en-tête. Ces champs serviront comme indicateur à l'hôte pour identifier les paquets nécessitant un traitement spécial des routeurs compatible IPv6. Les routeurs pourront ainsi procéder à un service en temps réel ou de qualité soutenue.

Définition expérimentale du champ Traffic Class (1 octet) :

- Bit D (1bit) privilégie le délai par rapport au débit
- Prio (3bits) définition de la priorité pour la remise des paquets
- Réserve (4bits)

3.4.3 Evolution vers DiffServ :

L'IETF travaille sur un mécanisme, Diffserv, transformant l'Internet en réseau de services différenciés. Il offrira à chaque application le niveau de performance requis. Le champ (TOS) sous IPv4 ou champ en-tête sous IPv6 sert à classifier les paquets. Désormais appelé DS (Diffserv) ce champ de 8 bits est composé de deux parties :

- DSCP : Diffserv code point 6bits (64 combinaisons possibles)
- CU : 2 bits (4 combinaisons possibles) actuellement inutilisé

Trois classes ont été pour l'instant définies par l'IETF:

- EF : Expedited Forwarding
- AF : Assured Forwarding
- DE : Default

La classe EF permet de garantir une certaine bande passante à chaque nœud, elle serait un peu l'équivalent d'une liaison louée. La classe AF permet de définir quatre priorités de trafic ayant différents niveaux de bande passante (Or, Argent, Bronze, Best Effort). Enfin pour les clients ne désirant pas de services différenciés, la classe DE, correspond à l'actuel service de base de l'Internet.

3.4.4 La Mobilité :

Basée sur MobileIPv4, mais tire partie des mécanismes d'IPv6 (configuration automatique, extensions destination, etc.) :

- Plusieurs adresses IPv6 pour le mobile
- Nœud « agent mère » dans chaque réseau qui relaie les données au mobile
- Mécanisme de table des associations pour permettre communication directe

3.4.5 La Sécurité :

IPsec: mécanismes de sécurité pour IP (v4 ou v6) optionnel pour IPv4, obligatoire pour IPv6

L'extension d'authentification (AH : Authentication Header):

- S'assurer que l'émetteur du msg est bien celui qu'il prétend être
- Contrôle d'intégrité pour garantir au récepteur que personne n'a modifié le contenu d'un message lors de son transfert sur le réseau
- L'extension ESP (Encapsulating Security Payload): permet de chiffrer l'ensemble des paquets ou leur partie transport et de garantir l'authentification et l'intégrité de ces paquets, Détecter les rejeux Garantir(de façon limitée) la confidentialité du flux.

3.5 Stratégie D'implémentation de la QoS pour IPv6 :

Les paquets IPv6, sont transmis par des chemins qui sont différents de ceux pour IPv4. Les fonctions prises en charge pour les environnements IPv6, comprennent la classification des paquets, la mise en attente, la régulation de trafic, la détection précoce aléatoire pondérée (WRED), basée sur des paquets classe marquage, et la police des paquets IPv6. Toutes les fonctionnalités de qualité de service disponible pour les environnements IPv6 sont gérés à partir de la QoS modulaire de l'interface de ligne de commande (CLI). La conception modulaire de la CLI nous permet de définir des classes de trafic, de créer et de configurer des règles de la circulation, puis attacher les règles de trafic à des interfaces.

Chapitre 4

Déploiement de VoIP avec le protocole IPv4 et IPv6

Introduction

L'objectif de notre travail consiste à déployer la solution Call Manager Express de Cisco, que nous avons choisi comme solution VoIP. Ainsi, nous allons diviser cette partie en trois en commençant par déployer une infrastructure réseau avec une topologie comprenant deux réseaux distants et par la suite nous allons lancer la solution. Nous terminerons par des tests d'appels entre des utilisateurs qui se trouvent dans les deux réseaux distants que nous appellerons Local User et Remote User. Nous avons opté pour un scénario de base calqué sur une l'architecture globale d'un réseau d'entreprises.

4.1 Architecture du réseau :

4.1.1 Composantes de l'architecture réseaux :

Pour notre architecture du réseau distant, nous avons choisi une topologie, dans laquelle deux sites distants (LANs) que nous appellerons Local et Remote d'une entreprise sont reliés à travers une liaison WAN (Wide Area Network), à travers un routeur qu'on appellera ISP (Internet Service Providers) en référence au fournisseur d'accès internet .

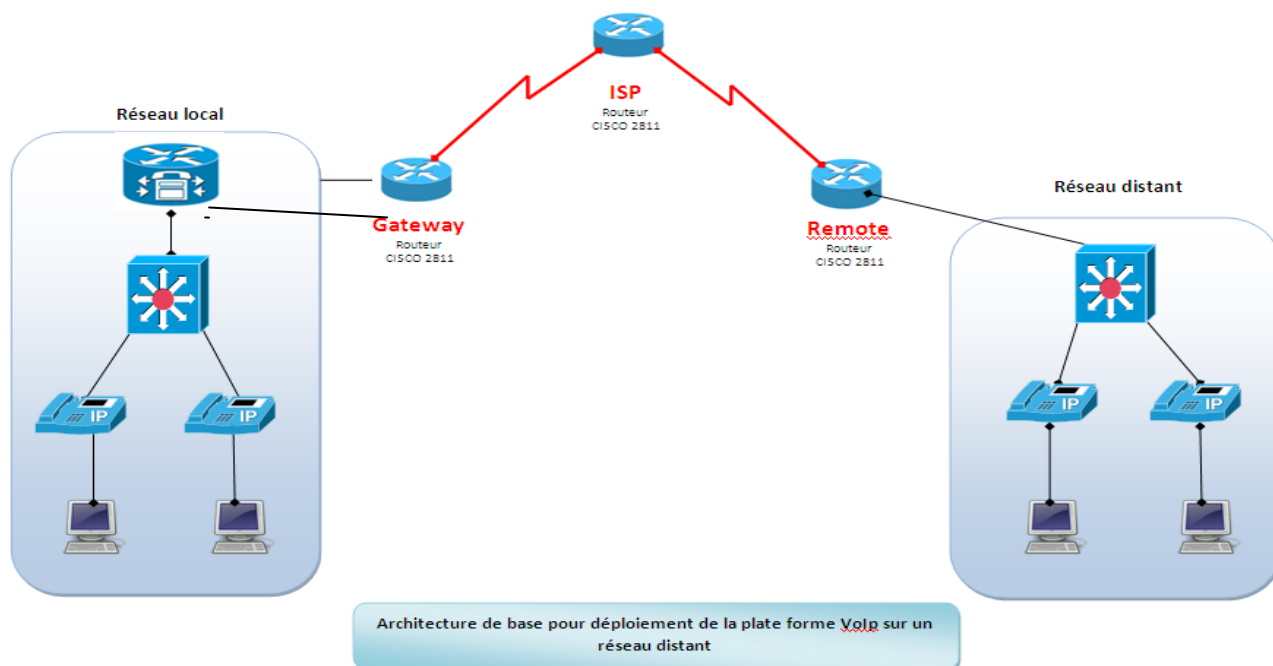


Figure 4.1 : L'architecture réseau du déploiement de la plate forme VoIP

4.1.2 Caractéristiques des équipements utilisés :

L'architecture globale de notre réseau présente plusieurs équipements, dont chacun a un rôle bien déterminé et avec les caractéristiques telles que le montre le tableau ci-dessous :

Tableau 4.1 Equipements utilisé dans l'architecture réseau

Equipement	Description	Type	Configuration et version
Routeur avec CME	CME	2811	Version 12.4(15)T
Routeur	Gateway	2811	Version 12.4(15)T
Routeur	ISP	2811	Version 12.4(15)T
Routeur	Remote	2811	Version 12.4(15)T
Switch	PoE	3560	Version IP-base
Câble	Câble null Modem	DTE-DCE	

4.1.3 Conception LAN pour la VoIP :

Dans les réseaux IP, une communication entre deux utilisateurs est initiée au niveau local, dans un réseau LAN Ethernet, et est transmise sur des réseaux longs distants WAN pour s'acheminer sur un réseau LAN Ethernet. La conception des infrastructures LAN est extrêmement importante, pour le fonctionnement correct de la VoIP sur un réseau convergent. En outre, une bonne conception de l'infrastructure LAN exige le déploiement de bout en bout de la qualité de service sur le réseau, ainsi qu'une disponibilité du réseau assurée avec des équipements redondants avec équilibrage de charge.

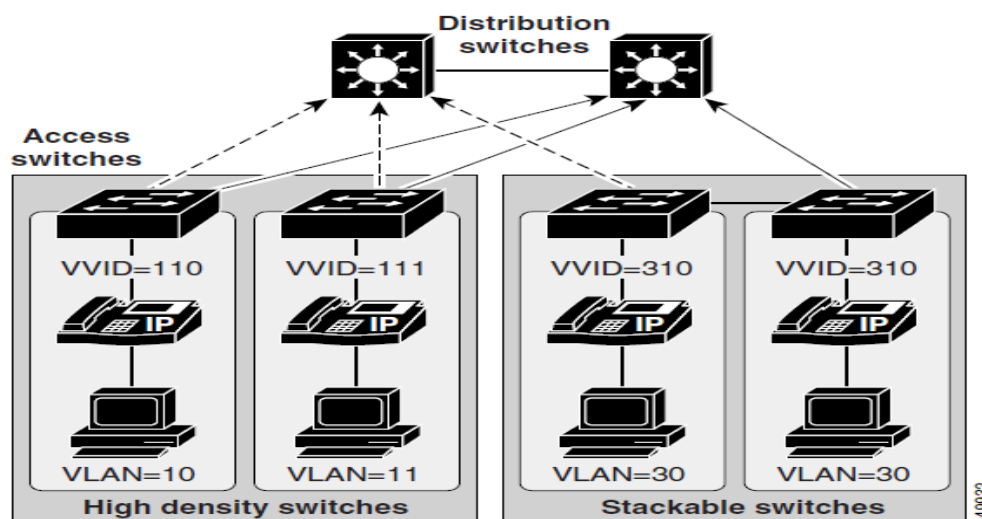


Figure 4.2 Exemple du déploiement avec haute disponibilité.

4.1.4 Intérêt du VLAN Voice :

Lors du déploiement du système voix dans un réseau LAN, on doit configurer un VLAN (Virtual local area network) pour le trafic voix, que nous appellerons VLAN Voice. Cela permet la séparation des paquets IP Voice et les paquets IP Data au niveau du réseau, et de fournir une qualité de service au niveau des passerelles.

4.1.5 Commutateurs avec Power over Ethernet (PoE) :

Les Commutateurs (Switch) sur lesquelles nous avons branché nos téléphones IP possèdent des ports de type Power over Ethernet PoE (alimentation par câble). Ils sont de 48 Volt DC d'alimentation fournis sur Ethernet standard, câbles non blindé à paire torsadée (UTP) définis dans la norme norme IEEE 802.3af PoE standard. La gamme Cisco Catalyst 6500, Cisco Catalyst 4500 et Cisco Catalyst 3750 sont capables de supporter la norme 802.3af.

4.1.6 La liaison WAN :

Une bonne conception de l'infrastructure WAN est importante pour le fonctionnement correct de la VoIP . Si les appels VoIP sont échangés entre les sites, les considérations WAN sont importantes. Elle doit être aussi hautement disponible que possible et qui offre un débit garanti. En outre, une bonne conception de l'infrastructure WAN exige le déploiement de bout

en bout de la qualité de service sur toutes les liaisons WAN. Pour cette raison, il est important de choisir une topologie WAN et le type de lien qui peut fournir une bande passante dédiée garantie. Les technologies suivantes liaison WAN peuvent fournir une bande passante dédiée garantie: Lignes louées, Frame Relay, Mode de transfert asynchrone (ATM), Service de relais ATM-à-Frame Interfonctionnement, Multiprotocol Label Switching (MPLS), Voix et vidéo Cisco IP Enabled sécurité VPN (IP Sec V3PN) .

Dans notre cas, nous allons simuler cette liaison avec le câble null modem X21 avec un côté DCE pour synchroniser l'autre côté DTE et avec un débit max de 2 Mbps.

4.2 Déploiement de la solution VoIP avec le Protocol IPv4 :

4.2.1 Modèle de conception :

Afin de réaliser notre objectif, qui est l'évaluation des performances de la voix sur IP dans un réseau long distant WAN, qui est formé de deux sites (Local , Remote) avec le protocole IPv4 puis avec le protocole IPv6, nous avons choisi une architecture centralisée. Dans chacun des sites, nous simulons la présence de deux utilisateurs et auxquelles nous attribuons un téléphone IP du type Cisco IP phone7965, en lui affectant une ligne représentée par un numéro qu'on va choisir dans une plage d'adresses 1XX.

4.2.2 Choix de la topologie Réseau Distant :

Le choix de la topologie réseaux a été dicté par le fait que dans les réseaux informatiques, ou une communication est initiée dans un réseau LAN et traverse des réseaux WAN pour s'acheminer dans un réseau LAN.

4.2.3 Présentation de la solution CME (Call Manager Express) :

Cisco Unified Communications Express est une solution de communication IP qui est fournie avec la gamme Cisco Integrated Services router. La nouvelle appellation officielle est Cisco Unified Communication Manager Express (CUCME), mais elle est toujours désignée par son ancien nom, qui est CCME (Cisco Call Manager Express), destinée aux entreprises de petite taille souhaitant développer une infrastructure de téléphonie IP.

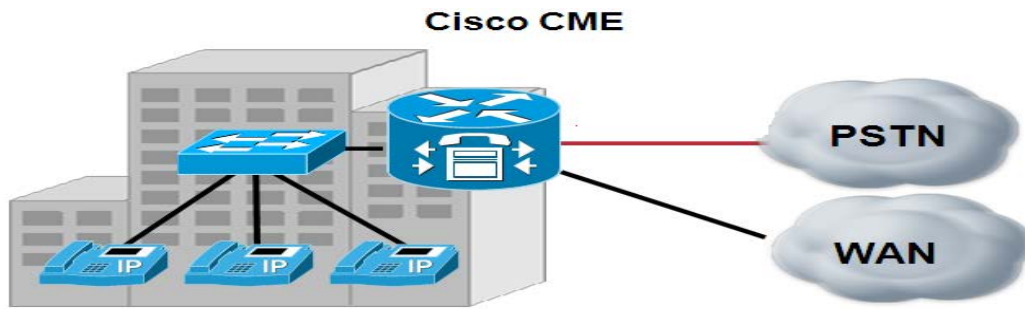


Figure 4.3 Déploiement de Cisco Call Manager Express

a. Les caractéristiques de la solution :

- Fonctionne sur les routeurs Cisco .
- Capable de gérer de 24 à 450 Phones en fonction du modèle de routeur.
- Solution basée sur l'IOS des routeurs Cisco.
- Une solution intégrée de VoIP .

b. Les protocoles VoIP supportés par CME :

1. SIP :

Session Initiation Protocol (SIP) est un protocole standard ouvert de gestion de sessions souvent utilisé dans les télécommunications multimédias (son, image, etc.) Il est depuis 2007 le plus courant pour la VoIP. SIP n'est pas seulement destiné à la VoIP mais aussi à de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo en ligne.

2. H323 :

H.323 regroupe un ensemble de protocole de communication de la voix, de l'image et de données sur IP. C'est un protocole développé par l'UIT-T qui le définit comme : « Systèmes de communication multimédia en mode paquet ». Il est dérivé du protocole H . 320 , utilisé sur RNIS .

3. Skinny Client Control Protocol (SCCP) :

Le Skinny Call Control Protocol (*SCCP*) est un protocole de communication, faisant partie de la couche application du modèle OSI. Le H.323 étant trop rigoureux pour certaines utilités de la téléphonie IP (comme le renvoi d'appel, le transfert, la mise en attente), Cisco a mis en place ce protocole beaucoup plus léger qu'est le SCCP (il utilise le port 2000). L'avantage de Skinny est qu'il utilise des messages prenant très peu de bande passante, c'est pourquoi il est utilisé pour les communications entre les téléphones IP et le Call Manager, ainsi que pour contrôler une conférence.

b. Les Codecs supportés par CME :

CME supporte le G711 , G729 , on peut visualiser ceci sur le routeur CME comme suit :

CME(config-ephone)#codec ?

g711ulaw Use G.711 u Law 64000 bps voice codec (default)

g729r8 Use G.729 8000 bps voice codec to save network bandwidth



Figure 4.4 : Plate forme matérielle utilisée pour le déploiement et les tests de la solution VoIP avec IPv4 et IPv6 basée sur CME.

c. Plates formes supportées :

CME supporte toutes les IOS jusqu'à la version 12.4. A partir de la version 12.5, Cisco a introduit le concept d'un «IOS universelle» qui offre tous les services (1 à 8), mais sont activés avec la licence appropriée. Avec l' IOS 15, il est nécessaire d'avoir une UC (Unified Communications) licence activée afin de pouvoir utiliser et configurer Cisco CallManager Express ou services vocaux. La dernière version disponible est la version 8.1 qui est présente dans la version IOS 15.1 (2) T

d. Exigences pour la configuration matérielle :

Elle dépend de la version du produit et de la plate-forme sur laquelle il sera installé. Par exemple, dans la version v8.1 les exigences d'un routeur Cisco 2811 sont de 256 Mo de DRAM et au moins 128 Mo de mémoire Flash. Cela fournira un soutien pour un maximum de 35 téléphones IP. Un routeur Cisco 2851 prend en charge jusqu'à 100 téléphones IP, cependant, il faudra une DRAM 384 MB accompagnées d'au moins 128 Mo de mémoire Flash.

En général, si on souhaite utiliser Cisco CallManager Express, la version 7.1 (version IOS 12.4 (24). T) est un excellent point de départ, car elle contient de nombreuses corrections de bugs et améliorations. Pour notre cas nous utiliserons un routeur ISR 2811.

e. Les modèles de déploiement de la solution CME :

On peut déployer les capacités de traitement d'appels de la solution CME de Cisco selon l'un des modèles suivants, en fonction de la taille, la répartition géographique et les besoins fonctionnels de L'entreprise:

4. Site unique :

Dans le modèle à un seul site, chaque site possède sa propre CME. Aucun trafic voix ne se déplace sur le réseau WAN IP, au contraire, les appels externes ou des appels vers des sites distants utilisent le réseau téléphonique public commuté (RTPC). Seuls les codecs G.711 sont utilisés pour tous les appels téléphoniques IP.

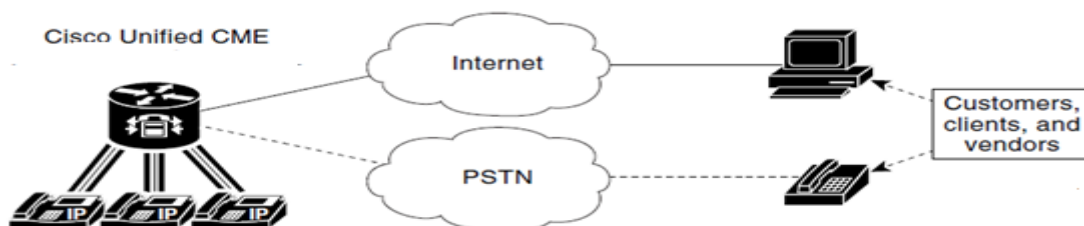


Figure 4.5: Mode site unique

5. La mise en œuvre multi site avec traitement des appels Distribué :

Dans le modèle multi-WAN avec le traitement d'appel distribué, chaque site possède sa propre CME. Communication entre les sites se fait normalement sur l'IP WAN, avec le RTPC servant de trajet de conversation de sauvegarde. Avec ce modèle, vous pouvez connecter n'importe quel nombre de sites à travers le WAN IP. Le modèle multi-WAN avec le traitement des appels distribuée se compose de plusieurs sites indépendants, chacun avec son propre agent de traitement d'appels relié à un réseau RTPC ou IP WAN (ou une combinaison des deux) qui transporte le trafic voix entre les sites distribués.

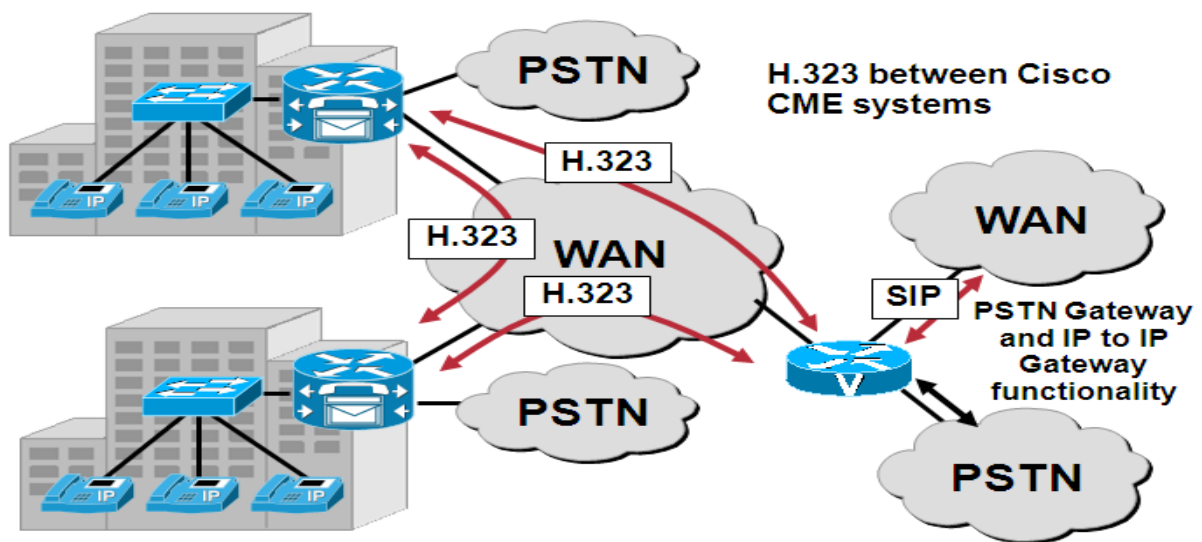


Figure 4.6 illustre un déploiement distribué typique de traitement des appels, avec une interconnexion IP WAN et une connexion de secours RTC

4.2.4 Architecture centralisée (dans notre cas) :

Dans notre conception topologique, on a choisi une architecture centralisée donc la solution VoIP utilisée est implémentée sur un seul site qui est le site local qui va gérer les utilisateurs (téléphone IP) de tous les autres sites de notre réseau d'entreprises. Le choix de cette topologie est dicté par des raisons de coût d'investissement et de contrôle du trafic

4.3 Etape de configuration de la solution Cisco Call Manager Express :

La plate forme VoIP est montée sur un routeur CISCO 2811, sur lequel nous activons les fonctionnalités nécessaires au bon fonctionnement de l'application :

4.3.1 Configuration des VLAN Data et Voice sur les commutateurs :

Tous les utilisateurs de la VoIP seront mis dans un VLAN Voice et ceci dans le but de différencier entre les trames de données Data et les trames Voice au niveau des passerelles (Routeurs) et pour nous permettre de gérer la QoS. Il est nécessaire de séparer le trafic voix du trafic données. Nous nommerons le Commutateur dans le réseau local « Local » et le commutateur sur le réseau distant « Remote »:

1. Sur le Switch Local :

```
Local # configure terminal
```

```
Local (config)# vlan 10
```

```
Local (config-vlan)# name VOICE
```

```
Local (config-vlan)# exit
```

```
Local (config)# vlan 50
```

```
Local (config-vlan)# name DATA
```

```
LocalSwitch (config)# interface FastEthernet0/1
```

```
LocalSwitch (config-if)# switchport trunk encapsulation dot1q
```

```
LocalSwitch (config-if)# switchport mode trunk
```

```
LocalSwitch (config)# interface FastEthernet0/2
```

```
LocalSwitch (config-if)# switchport access vlan 200
```

```
LocalSwitch (config-if)# switchport mode access
```

```
LocalSwitch (config-if)# switchport voice vlan 100
```

```
LocalSwitch (config)# interface FastEthernet0/3
```

```
LocalSwitch (config-if)# switchport access vlan 200
```

```
LocalSwitch (config-if)# switchport mode access
```

```
LocalSwitch (config-if)# switchport voice vlan 100
```

2. Sur le Switch Remote :

```
RemoteSwitch # configure terminal
```

```
RemoteSwitch (config)# vlan 100
```

```
RemoteSwitch (config)# name VOICE
```

```
RemoteSwitch (config)# vlan 200
```

```
RemoteSwitch (config)# name DATA
```

```
RemoteSwitch (config)# interface FastEthernet0/1
```

```
RemoteSwitch (config-if)# switchport trunk encapsulation dot1q
```

```
RemoteSwitch (config-if)# switchport mode trunk
```

```
RemoteSwitch (config)# interface FastEthernet0/2
```

```
RemoteSwitch (config-if)# switchport access vlan 200
```

```
RemoteSwitch (config-if)# switchport mode access
```

```
RemoteSwitch (config-if)# switchport voice vlan 100
```

```
RemoteSwitch (config)# interface FastEthernet0/3
```

```
RemoteSwitch (config-if)# switchport access vlan 200
```

```
RemoteSwitch (config-if)# switchport mode access
```

```
RemoteSwitch (config-if)# switchport voice vlan 100
```

4.3.2 Configuration du routage Inter-VLAN sur le Routeurs CME et Routeur Remote :

1. Sur le Routeur CME :

```
CME (config)# interface FastEthernet0/0
```

```
CME (config-if)# no shutdown
```

```
CME (config)#interface FastEthernet0/0.10
```

```
CME (config-subif)#encapsulation dot1Q 10
```

```
CME (config-subif)# ip address 192.168.10.1 255.255.255.0
```

```
CME (config-subif)#interface FastEthernet0/0.50
```

```
CME (config-subif)#encapsulation dot1Q 50
```

```
CME (config-subif)#ip address 192.168.50.1 255.255.255.0
```

```
CME (config)#interface FastEthernet0/0.99
CME (config-subif)#encapsulation dot1Q 99 native
CME (config-subif)#ip address 192.168.99.1 255.255.255.0
```

1. Sur le Routeur Remote :

```
Remote (config)# interface FastEthernet0/0
Remote (config-if)# no shutdown

Remote (config)#interface FastEthernet0/0.100
Remote (config-subif)#encapsulation dot1Q 100
Remote (config-subif)#ip address 192.168.100.1 255.255.255.0
Remote(config-subif)# ip helper-address 172.16.2.2

Remote (config)#interface FastEthernet0/0.200
Remote (config-subif)#encapsulation dot1Q 200
Remote (config-subif)#ip address 192.168.200.1 255.255.255.0
Remote(config-subif)# ip helper-address 172.16.2.2
```

4.3.3 Activation du service Serveur DHCP sur le routeur CME :

L'activation du service serveur DHCP permet au routeur d'attribuer les paramètres IP ainsi que les firmware (Soft) au telephone IP :

```
CME# configure terminal
CME(config)# ip dhcp excluded-address 192.168.100.1 192.168.100.10
CME(config)# ip dhcp excluded-address 192.168.200.1 192.168.200.10
CME(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
CME(config)# ip dhcp excluded-address 192.168.50.1 192.168.50.10
```

4.3.4 Création du pool Voice pour l'attribution automatique des adresses IP au téléphone IP :

```
CME(config)# ip dhcp pool voice
CME (dhcp-config)#network 192.168.10.0 255.255.255.0
CME (dhcp-config)#default-router 192.168.10.1
CME (dhcp-config)#dns-server 2.2.2.2
CME (dhcp-config)#option 150 ip 192.168.10.1
```

4.3.5 Création du pool Data pour l'attribution automatiques des adresses IP au PC et autres téléphones IP :

```
CME(config)# ip dhcp pool data
CME (dhcp-config)#network 192.168.50.0 255.255.255.0
CME (dhcp-config)#default-router 192.168.50.1
CME (dhcp-config)#option 150 ip 192.168.50.1
```

```
CME(config)# ip dhcp pool Remotevoice
CME (dhcp-config)#network 192.168.100.0 255.255.255.0
CME (dhcp-config)#default-router 192.168.100.1
CME (dhcp-config)#dns-server 2.2.2.2
CME (dhcp-config)#option 150 ip 192.168.1.2
```

```
CME(config)# ip dhcp pool Remotedata
CME (dhcp-config)#network 192.168.200.0 255.255.255.0
CME (dhcp-config)#default-router 192.168.200.1
CME (dhcp-config)#dns-server 2.2.2.2
CME (dhcp-config)#option 150 ip 192.168.1.2
```

Remarque :

6. Option 150 indique au téléphone IP le serveur TFTP
7. Le serveur TFTP (Dans notre cas le routeur CME) contient les fichiers de configuration et le firmware pour les téléphones IP

4.3.6 Activation du service téléphoné sur IP :

Nous allons définir le nombre maximum des ephones qui peuvent être définis dans le système (par défaut: 0) et le nombre maximum de ephone-dn qui peuvent être définis dans le système (par défaut: 0) :

```
CME(config)# telephony-service
CME(config-telephony)# max-ephones 20
CME(config-telephony)# max-dn 40
```

Cette commande identifie l'adresse et le port par lequel les téléphones IP communiqueront avec Cisco CME :

```
CME(config)# ip source-address 192.168.10.1 port 2000
```

4.3.7 Création des lignes et affectation au téléphone IP avec ephone-dn et ephone:

Nous allons affecter le numero 101 pour un utilisateur qui est sur le réseau Local :

- CME(Config)#ephone-dn 1
- CME(Config-ephone-dn)#number 101
- CME(config)#ephone 1
- CME(config-ephone)# mac-address 0025.4595.91F6
- CME(config-ephone)# type 7965
- CME(config-ephone)# button 1:1

- L'utilisateur **102** SUR le reseau Local :
- CME(Config)#ephone-dn 2
- CME(Config-ephone-dn)#number 102
- CME(config)#ephone 2
- CME(config-ephone)# mac-address 0025.4595.936F
- CME(config-ephone)# type 7965
- CME(config-ephone)# button 1:2

- | |
|---|
| <ul style="list-style-type: none"> • L'utilisateur 103 sur le réseau Remote : • CME(Config)#ephone-dn 3 • CME(Config-ephone-dn)#number 103 • CME(config)#ephone 3 • CME(config-ephone)# mac-address 0025.4595.94C9 • CME(config-ephone)# type 7965 • CME(config-ephone)# button 1:3 |
| <ul style="list-style-type: none"> • L'utilisateur 104 sur le réseau Remote : • CME(Config)#ephone-dn 4 • CME(Config-ephone-dn)#number 104 • CME(config)#ephone 4 • CME(config-ephone)# mac-address • CME(config-ephone)# type 7965 • CME(config-ephone)# button 1:4 |

4.4 Déploiement de la solution et tests :

Tout d'abord, nous allons tester le fonctionnement du réseau de bout en bout, à l'aide de la commande Ping entre deux utilisateurs situés sur les deux réseaux distants.

4.4.1 Lancement de la solution VoIP et enregistrement des téléphones IP :

Nous allons lancer la commande Show ephone pour voir que l'enregistrement des différents utilisateurs a été effectué et que la session VoIP initié utilise le protocole SCCP de Cisco comme protocole de signalisation.

```
CME # show ephone
```

```
ephone-1 Mac:0025.4595.91F6 TCP socket:[2] activeLine:0 REGISTERED in SCCP ver 1
```

```

2 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:9
IP:192.168.10.12 52296 7965  keepalive 23 max_line 6
button 1: dn 1  number 101 CH1  IDLE      CH2  IDLE
ephone-3 Mac:0025.4595.94C9 TCP socket:[3] activeLine:0 REGISTERED in SCCP ver 1
2 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:9
IP:192.168.100.11 49176 7965  keepalive 22 max_line 6
button 1: dn 3  number 103 CH1  IDLE      CH2  IDLE

```

```

ephone-3 Mac:0025.4595.94C9 TCP socket:[3] activeLine:0 REGISTERED in SCCP ver 1
2 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:9
IP:192.168.100.11 49176 7965  keepalive 22 max_line 6
button 1: dn 3  number 103 CH1  IDLE      CH2  IDLE

```

Dans cette section, et après avoir exécuté les étapes suivantes:

- La mise en place de la topologie réseau et test de fonctionnement.
- Le déploiement de la solution VoIP .
- Création des utilisateurs en leur affectant des numéros d'appel.

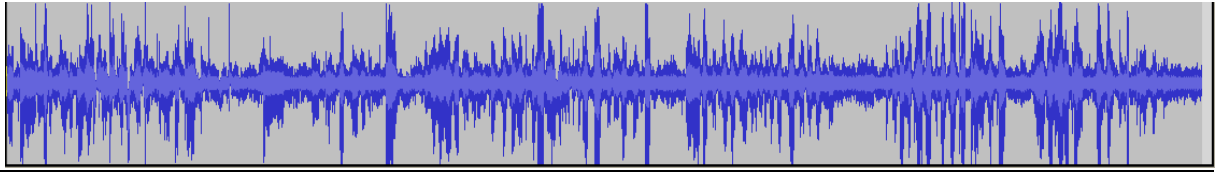
Nous allons commencer l'étape des tests avec initiation d'appel entre utilisateurs :

4.4.2 Lancer une session VoIP et enregistrement des fichiers .WAV :

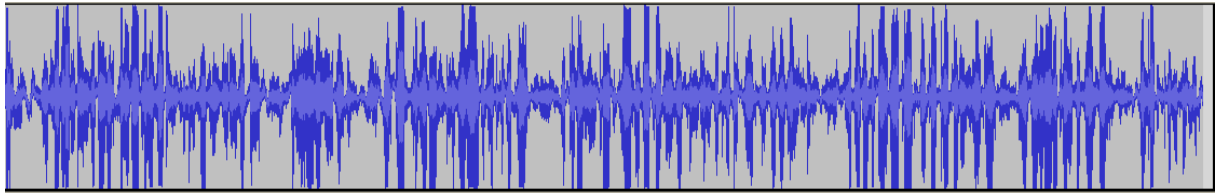
Dans cette partie nous allons lancer des appels entre deux utilisateurs, l'un sur le réseau local avec son numéro d'appel 101 et l'utilisateur distant sur le réseau Remote avec son numéro d'appel 103. Nous allons enregistrer le signal vocal en mode WAV avec un microphone au niveau de l'utilisateur 101 et sa sortie au niveau de l'utilisateur 103 et ceci pour les différents tests que nous allons réaliser en variant la valeur de la bande passante sur le lien WAN.

Représentation des fichiers .wav avec le logiciel Audacity et ceci au niveau de l'utilisateur distant :

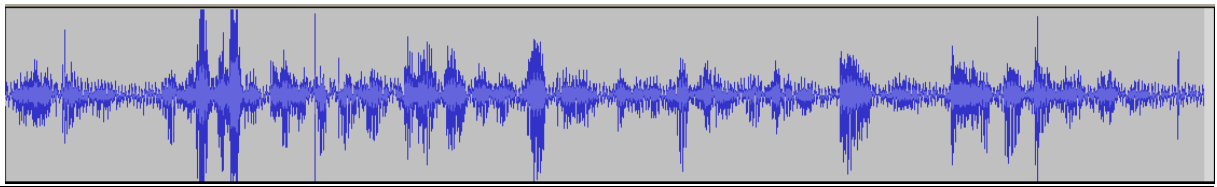
- Avec une Bande Passante de 128 kb/s :



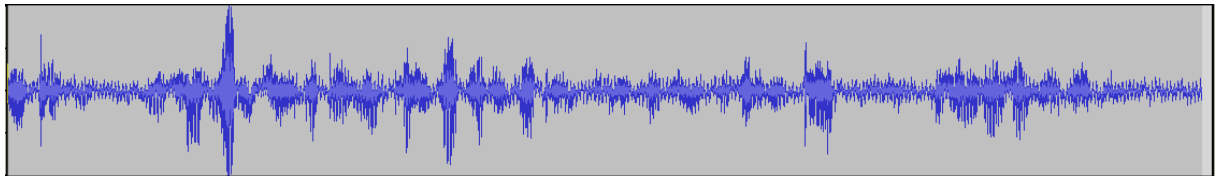
- Avec une Bande Passante de 256 kb/s :



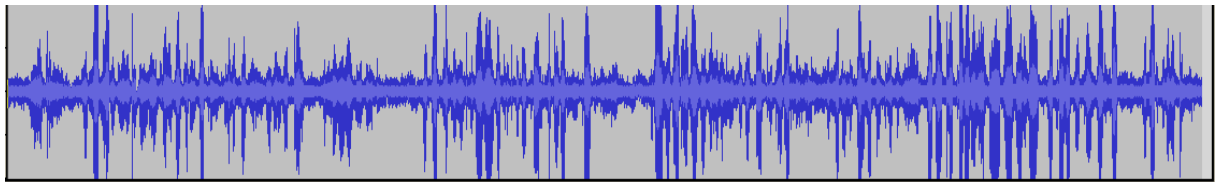
- Avec une Bande Passante de 512 kb/s :



- Avec une Bande Passante de 1 Mb/s :



- Avec une Bande Passante de 2Mb/s :



4.5 Déploiement de VoIP sur IPv6 :

Dans cette partie, nous allons configurer le protocole IPv6 sur la liaison WAN en mode tunnel et en mode Dual Stack, comme mode de transition entre le réseau IPv4 (le LAN) et le réseau WAN IPv6 :

4.5.1 Configuration des routeurs d'extrémité Gateway et Remote en mode tunnel :

- Sur le routeur Gateway :

Gateway (config) # ipv6 unicast-routing
Gateway (config) # interface Tunnel0
Gateway (config) # ip address 172.16.1.1 255.255.255.0
Gateway (config) # tunnel source Serial0/0/0
Gateway (config) # tunnel destination 2001:11::1
Gateway (config) # tunnel mode ipv6
Gateway (config) # interface FastEthernet0/1
Gateway (config) # ip address 172.16.2.1 255.255.255.0
Gateway (config) # interface Serial0/0/0
Gateway (config) # no ip address
Gateway (config) # ipv6 address 2001:10::1/64
Gateway (config) # ipv6 enable
Gateway (config) # ip route 172.16.3.0 255.255.255.0 172.16.1.2
Gateway (config) # ip route 192.168.1.0 255.255.255.0 172.16.2.2
Gateway (config) # ip route 192.168.10.0 255.255.255.0 172.16.2.2
Gateway (config) # ip route 192.168.50.0 255.255.255.0 172.16.2.2
Gateway (config) # ip route 192.168.100.0 255.255.255.0 172.16.1.2
Gateway (config) # ip route 192.168.200.0 255.255.255.0 172.16.1.2
Gateway (config) # ipv6 route 2001:11::/64 Serial0/0/0 2001:10::2

- Sur le routeur Remote :

Remote (config) # ipv6 unicast-routing
Remote (config) # interface Tunnel0
Remote (config) # ip address 172.16.3.1 255.255.255.0
Remote (config) # tunnel source Serial0/2/0
Remote (config) # tunnel destination 2001:10::1
Remote (config) # tunnel mode ipv6
Remote (config) #interface FastEthernet0/0
Remote (config-if) #no shutdown
Remote (config) #interface FastEthernet0/0.100
Remote (config-if) #encapsulation dot1Q 100
Remote (config-if) #ip address 192.168.100.1 255.255.255.0
i Remote (config-if) #p helper-address 172.16.2.2
Remote (config-if) #interface FastEthernet0/0.200
Remote (config-if) #encapsulation dot1Q 200
Remote (config-if) #ip address 192.168.200.1 255.255.255.0
Remote (config-if) #ip helper-address 172.16.2.2
Remote (config) #interface Serial0/2/0
Remote (config-if) #ipv6 address 2001:11::1/64
Remote (config) # interface Serial0/2/1
Remote (config) # ip route 172.16.1.0 255.255.255.0 172.16.3.2
Remote (config) # ip route 172.16.2.0 255.255.255.0 172.16.3.2
Remote (config) # ip route 192.168.1.0 255.255.255.0 172.16.3.2
Remote (config) # ip route 192.168.10.0 255.255.255.0 172.16.3.2
Remote (config) # ip route 192.168.50.0 255.255.255.0 172.16.3.2
Remote (config) # ip route 192.168.99.0 255.255.255.0 172.16.3.2
Remote (config) # ipv6 route 2001:10::/64 Serial0/2/0 2001:11::2

Visualisation de la configuration sur le routeur ISP :

ISP#show running-configuration :

```
interface Serial0/2/0
```

```
ip address 172.16.1.2 255.255.255.0
```

```
ipv6 address 2001:10::2/64
```

```
no fair-queue
```

```
interface Serial0/2/1
```

```
ip address 172.16.3.2 255.255.255.0
```

```
ipv6 address 2001:11::2/64
```

4.5.2 Configuration des routeurs d'extrémité Gateway et Remote en mode Dual Stack ainsi que le router ISP :

- Sur le routeur Remote :

```
Remote (config) # ipv6 unicast-routing
```

```
Remote (config) # interface Serial0/2/0
```

```
Remote (config) # ip address 172.16.3.1 255.255.255.0
```

```
Remote (config) # ipv6 address 2001:11::1/64
```

```
Remote (config) # ip route 172.16.1.0 255.255.255.0 172.16.3.2
```

```
Remote (config) # ip route 172.16.2.0 255.255.255.0 172.16.3.2
```

```
Remote (config) # ip route 192.168.1.0 255.255.255.0 172.16.3.2
```

```
Remote (config) # ip route 192.168.10.0 255.255.255.0 172.16.3.2
```

```
Remote (config) # ip route 192.168.50.0 255.255.255.0 172.16.3.2
```

```
Remote (config) # ip route 192.168.99.0 255.255.255.0 172.16.3.2!
```

```
Remote (config) # ipv6 route 2001:10::/64 Serial0/2/0
```

- Pour le routeur Gateway :

```
Gateway (config) # ipv6 unicast-routing
```

```
Gateway (config) # interface Serial0/0/0
```

```
Gateway (config) # ip address 172.16.1.1 255.255.255.0
```

```
Gateway (config) # ipv6 address 2001:10::1/64
```

```
Gateway (config) # ip route 172.16.3.0 255.255.255.0 172.16.1.2
```

```
Gateway (config) # ip route 192.168.1.0 255.255.255.0 172.16.2.2
```

```
Gateway (config) # ip route 192.168.10.0 255.255.255.0 172.16.2.2
```

```
Gateway (config) # ip route 192.168.50.0 255.255.255.0 172.16.2.2
```

```
Gateway (config) # ip route 192.168.100.0 255.255.255.0 172.16.1.2
```

```
Gateway (config) # ip route 192.168.200.0 255.255.255.0 172.16.1.2
```

```
Gateway (config) # ipv6 route 2001:11::/64 Serial0/0/0
```

- **Test de fonctionnement du réseau avec le Ping :**

```
Remote #ping 2001:10::1
```

```
!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

```
Gateway# ping 2001:11::1
```

```
!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms
```

- **Lancer une session VoIP et Enregistrement des fichiers .wav :**



Conclusion :

Dans cette phase de notre travail, nous avons finalisé la préparation de notre plate-forme de travail réseau, nous avons ensuite lancé des tests d'appels entre des utilisateurs distants et nous avons fait des captures du signal vocal. La prochaine étape de notre travail va porter sur l'évaluation et test de la solution VoIP basée sur l'IPv6.

Chapitre 5

***Evaluation et test de la solution VoIP sous IPv6
proposée***

Introduction :

Dans cette section, nous allons utiliser des outils d'évaluation de la qualité de la parole, pour tester la solution VoIP sous IPv6 proposée dans ce travail. Différentes méthodes de traitement seront appliquées en comparant un signal d'entrée de parole qui est une phrase lue par l'initiateur de la communication (Local User) et le signal de sortie de parole à l'autre bout du réseau WAN. La première fois en utilisant le protocole IPv4, ensuite avec le protocole avec IPv6. une étude comparative sera effectuée pour valider l'approche proposée.

5.1 Les différentes méthodes de mesures :**5.1.1 L'échelle MOS :**

La première approche, pour mesurer la qualité d'une restitution sonore est de faire appel à un panel d'observateurs qui vont l'évaluer. C'est le principe qui sous-entend la méthode MOS (Mean Opinion Score) [ITU-T recommandation P.800].. Cette technique est issue de la téléphonie analogique. C'est une mesure subjective.

5.1.2 Le E-Model :

L'E-Model consiste à effectuer des mesures réseau sur les qualités objectives directement à partir des trames réseau (délais, gigue,etc.). Il a été standardisé par l'UIT. On complète ces données avec des informations issues d'une table d'évaluation des codecs. On obtient ainsi une note R comprise entre 0 et 100. Une table de correspondance permet d'établir un lien calculé entre l'échelle R et l'échelle MOS comprise entre 1 et 5. On obtient des résultats très proches de ceux obtenus dans les mêmes conditions par le modèle MOS d'origine. Cette mesure est entièrement automatisable et peut aussi servir à effectuer de la surveillance.

5.1.3 PESQ (Perceptual Evaluation of Speech Quality) :

L'ETSI, en collaboration avec certains laboratoires, a recommandé un autre outil de mesure de la qualité d'une transmission VoIP, le PESQ (Perceptual Evaluation Speech Quality). Le but était de proposer un modèle objectif, basé sur le modèle psycho-acoustique humain. Il effectue une mesure comparative entre deux informations, celle injectée à une extrémité et la

même information recueillie à l'autre extrémité après avoir traversé le système étudié. Après traitement, le PESQ restitue ses résultats sur une échelle MOS.

5.2 Evaluation objective et subjective de la qualité de la parole :

Les recherches en psycho-acoustique sur la qualité de la parole ont, entre autres, comme but de créer des outils d'évaluation objectifs. Ceux-ci donnent une valeur de la qualité globale de La parole perçue à travers un système de communications.

Mais vu que la perception auditive est interne à l'auditeur, la qualité d'un système de téléphonie ne peut pas être mesurée, de manière absolue, par une méthode objective. Les tests de jugement de la qualité par des auditeurs sont les seules évaluations valables et sûres d'un système de parole. Cependant, ces tests sont assez difficiles à mettre en place et assez coûteux.

Des méthodes instrumentales de jugement de la qualité ont donc été développées, essayant de prévoir la qualité de la parole en se basant sur la mesure de signaux caractéristiques. On peut ensuite les classer suivant trois types de modèle.

- Modèles basés sur des mesures comparatives à base de signaux (Ex : PESQ).
- Modèles de planification de réseaux.
- Modèles de surveillance de réseau.

5.3 Evaluation objective de la qualité de la parole :

5.3.1 Speech Quality Testing – PESQ :

Un exemple de modèle basé sur des mesures du signal est le modèle “Perceptual Évaluation of Speech Quality “ (PESQ) [ITU-T Rec. P.862, 2001]. À la base, ce modèle était destiné à prévoir la qualité d'un seul composant d'un système de télécommunications complet. Mais il peut juger certains autres problèmes, comme certains types de pertes de paquets. Ce modèle fonctionne par comparaison entre un signal non traité et un signal qui est passé à travers un système. Il utilise une représentation du signal sous forme psycho acoustique. L'évaluation perceptuelle de la qualité de la parole (PESQ) est une méthode reconnue de précision et du test du niveau de qualité qui sera perçue par l'utilisateur d'un réseau VoIP.

5.3.2 La méthode de mesure :

La mesure se fera en comparant un fichier WAV, qui n'est autre qu'une phrase lue à partir d'un téléphone IP dans le réseau local, avec le fichier reçu à l'autre extrémité du réseau WAN qu'on a appelé Remote, afin de déterminer toute perte de qualité en cours de route. Le PESQ fournit une note dans la gamme de 1 à 5, où 1 est inacceptable et 5 est une excellente. Théoriquement une plage typique pour la VoIP est de 3,5 à 4,2. La phrase utilisée est la suivante :

/ Bonjour tout le monde ,voici un échantillon de parole que je vais utiliser pour une communication VoIP et sur un réseau distant, le test se fera en premier lieu avec le protocole IPv4 puis avec le nouveau protocole IPv6 ce qui va ne permettre d'évaluer la qualité de service de cette communication /

5.3.3 Résultats des mesures avec le PESQ :

Nous allons prendre tous les fichiers WAV que nous avons récupérés à l'entrée de réseau local et leur sortie sur le réseau Remote, afin de tester la qualité de la parole avec le PESQ, Les mesures ont été faites avec une variation de la bande passante sur le lien WAN et ceci avec le protocole IPv4 en premier lieu :

a. Solution VoIP basée sur le protocole IPv4 et influence de la bande passante :

- Bande Passante à 128 kb/s :

```

Perceptual Evaluation of Speech Quality <PESQ>
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 100.WAV
donner le Nom du fichier de sortie : signal de parole synthetique = 1.WAV
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 100.WAV...done.
Reading degraded file 1.WAV...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 2.208

```

Figure 5.1 : Test N°1

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 200.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 2.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 200.WAU...done.
Reading degraded file 2.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.660

```

Figure 5 .2 : Test N°2

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 300.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 3.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 300.WAU...done.
Reading degraded file 3.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 4.035

```

Figure 5 .3 : Test N°3

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 400.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 4.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 400.WAU...done.
Reading degraded file 4.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.453

```

Figure 5 .4 : Test N°4

- Bande Passante à 256 kb/s :

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 1.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 1B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 1.WAU...done.
Reading degraded file 1B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.934

```

Figure 5 .5 : Test N°1

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 2.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 2B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 2.WAU...done.
Reading degraded file 2B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.797

```

Figure 5 .6 : Test N°2

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 3.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 3B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 3.WAU...done.
Reading degraded file 3B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.641

```

Figure 5 .7 : Test N°3

```

Perceptual Evaluation of Speech Quality <PESQ>
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 4.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 4B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 4.WAU...done.
Reading degraded file 4B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 1.946

```

Figure 5 .8 : Test N°4

```

Perceptual Evaluation of Speech Quality <PESQ>
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 2.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 2B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 2.WAU...done.
Reading degraded file 2B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.351

```

- Bande Passante à 512 kb/s :

Figure 5 .9 : Test N°1

```

Perceptual Evaluation of Speech Quality <PESQ>
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 3.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 3B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 3.WAU...done.
Reading degraded file 3B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.579

```

Figure 5.10 : Test N°2

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 4.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 4 B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 4.WAU...done.
Reading degraded file 4 B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.986

```

Figure 5.11 : Test N°3

- Bande Passante à 1Mb/s :

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 1.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 1B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 1.WAU...done.
Reading degraded file 1B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.712

```

Figure 5.12 : Test N°1

```

Perceptual Evaluation of Speech Quality <PESQ>
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 2.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 2B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 2.WAU...done.
Reading degraded file 2B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 1.754

```

Figure 5.13 :Test N°2

```

Perceptual Evaluation of Speech Quality <PESQ>
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 3.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 3B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 3.WAU...done.
Reading degraded file 3B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 4.108

```

Figure 5.14 :Test N°3

```

Perceptual Evaluation of Speech Quality <PESQ>
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 4.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 4B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 4.WAU...done.
Reading degraded file 4B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 4.105

```

Figure 5.15 :Test N°4

- Bande Passante 2Mb/s :

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 1.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 1B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 1.WAU...done.
Reading degraded file 1B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 2.059

```

Figure 5.15 : Test N°1

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 2.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = 2B.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 2.WAU...done.
Reading degraded file 2B.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 4.294

```

Figure 5.16 : Test N°2

```
Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 3.WAV
donner le Nom du fichier de sortie : signal de parole synthetique = 3B.WAV
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 3.WAV...done.
Reading degraded file 3B.WAV...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.818
```

Figure 5.17 : Test N° 3

```
Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = 4.WAV
donner le Nom du fichier de sortie : signal de parole synthetique = 4B.WAV
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file 4.WAV...done.
Reading degraded file 4B.WAV...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.545
```

Figure 5.18 : Test N°4

Avec la fonction du NAT (Network Adresse Translation) : le test a été fait avec une bande passante de 2Mb /s : Les réseaux natés introduisent une certaine latence en regard du changement d'en-têtes IP sur les adresses. Ce paramètre de la QoS peut être approché par une étude comparative entre réseaux natés et réseaux non natés. Pour cela nous avons effectué des mesures avec un réseau naté avec une bande passante de 2 Mb/s

```

Perceptual Evaluation of Speech Quality (PESQ)
ITU-T Recommendation P.862.
Version 1.2 - 2 August 2002.

donner le Nom du fichier d'entree : signal de parole originale = NATA101 1.WAU
donner le Nom du fichier de sortie : signal de parole synthetique = NATB103 1.WAU
donner la frequence d'echantillonnage +8000/+16000= : +8000

*****
Reading reference file NATA101 1.WAU...done.
Reading degraded file NATB103 1.WAU...done.
Level normalization...
IRS filtering...
Variable delay compensation...
Acoustic model processing...
Prediction : PESQ_MOS = 3.510

```

Figure 5.19

- Les mesures avec le PESQ effectuées avec l'IPv4 ont été regroupées dans le tableau 5.1 :

Tableau 5.1 Tableaux récapitulatif des résultats (PESQ) obtenus avec IPv4

Avec IPv4	128kb/s	256kb/s	512kb/s	1Mb/s	2Mb/s
Test N° 1	2,20	3,93	2,98	3,71	2,10
Test N° 2	3,66	3,78	3,35	1,75	4,29
Test N° 3	4,00	3,64	3,60	4,10	3,82
Test N° 4	3,45	2,00	4,00	4,10	3,55

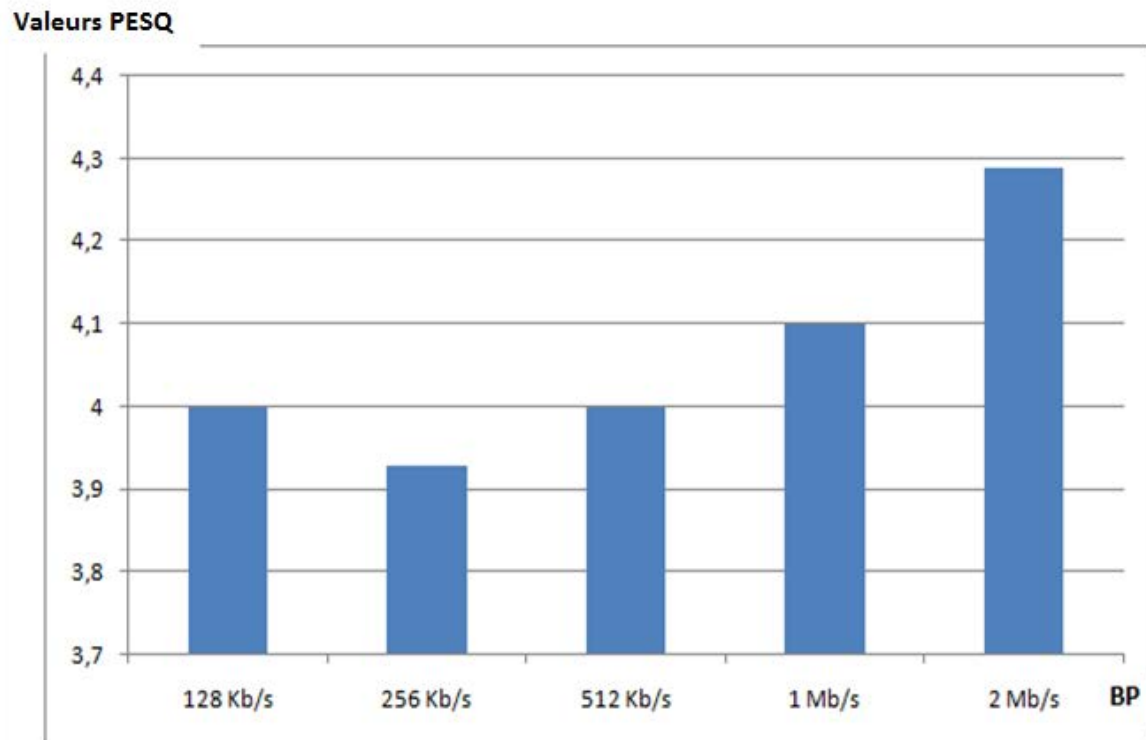


Figure 5.20 Representation des meilleurs valeurs obtenue dans le tableau 5.1

- Avec le NAT (Network adresse translation) et pour une bande passante de 2Mb/s :
PESQ = 3,52

b. Solution VoIP basée sur le protocole IPv6 et influence de la bande passante : Les résultats obtenus avec IPv6 en utilisant les deux méthodes qui sont le dual stack et le mode tunnel.

Tableau 5.2 Tableaux récapitulatif des résultats (PESQ) obtenus avec IPv6

Avec IPv6	Résultat du PESK Dual Stack	Résultat du PESK Mode Tunnel
Test N° 1	3,10	3,74
Test N° 2	3,20	3,17
Test N° 3	3,00	3, 6
Test N° 4	2,30	3 ,65

MOS

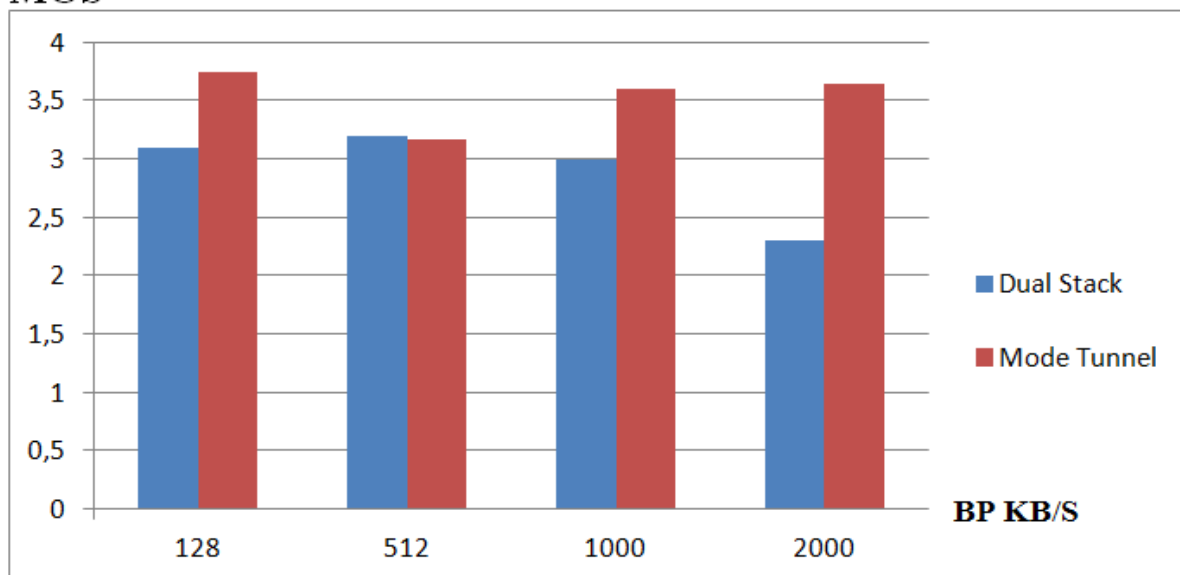


Figure 5.21 Representation des valeurs du tableau 5.2

5.4 Evaluation subjective de la qualité de la parole

5.4.1 MOS (Mean Opinion Score) :

La clarté d'une conversation téléphonique est essentiellement subjective. Une des méthodes les plus efficaces pour mesurer la qualité de la voix transportée par un réseau est d'utiliser relativement une grande quantité d' « auditeurs » humains dans une procédure de test bien définie. Une note d'évaluation moyenne peut ainsi être attribuée au réseau : cette méthode simple, mais coûteuse, a été utilisée pendant de nombreuses années et clairement définie par la spécification ITU P800 (MOS Mean Opinion Score - note moyenne d'appréciation). Les essais d'opinion d'écoute débouchant sur une notation subjective : le MOS (Mean Opinion Score) .

5.4.2 Méthodologie :

Le principe de calcul du MOS, est basé sur un sondage d'un échantillon supposé représentatif de la population des utilisateurs. Les personnes constituant l'échantillon sont invitées à écouter un signal d'entrée (dans notre cas un signal voix), puis son équivalent à la sortie à l'autre bout du réseau. Après chaque écoute, l'auditeur donne une note sanctionnant la qualité qu'il a perçue. La moyenne des notes fournies par la population constitue le MOS. Les essais (dans notre cas 10) sont réalisés dans des conditions bien définies (Salle d'essai, bruits, établissement de la connexion et surveillance) et selon un processus déterminé. La procédure de mesure est également spécifiée : choix des sujets, échelle d'appréciation subjective (opinion : de 1 mauvais à 5 excellent - difficulté : oui/non) ainsi que le recueil et le traitement des résultats et parce que le MOS est classé par l'homme le score est subjectif.

Tableau 5.3 : Valeur du MOS :

Excellent	Bon	Correct	Faible	Maivais
5	4	3	2	1

5.4.3 Procédure de mesure:

- **Choix des auditeurs :**

Ils sont choisis au hasard parmi des étudiants. Les conditions étant, qu'ils n'aient pas participé à des travaux en cours et qu'ils n'aient pas participé à des essais subjectifs au cours des 6 mois précédents.

- **Echelles d'appréciation subjective :**

L'étudiant va donner une note selon son opinion en utilisation la notation MOS. C'est une échelle d'appréciation subjective de conversation.

- **Recueil des données :**

L'expérimentateur recueille deux réponses subjectives par test et par sujet. Les données essentielles se composent des notes d'opinion sur la conversation et de la décision concernant les difficultés.

Traitement des résultats :

On calcule une moyenne des notes d'appréciations pour chaque condition d'essai. Dans notre cas les évaluations ont été obtenues par l'utilisation du codec G711 et pour les différentes valeurs de la bande passante.

- **Les Evaluations avec IPv4 :**

Tableau 5.4 Tableaux récapitulatif de meilleures valeurs obtenues avec IPv4

Locuteurs	Valeurs MOS (128B/S)	Valeurs MOS (512B/S)	Valeurs MOS (1MB/S)	Valeurs MOS (2MB/S)
1	3,2	3.7	3.7	3.9
2	3.4	3.6	3.8	3.9
3	3.5	3.7	3.9	4.0
4	3.4	3.8	3.8	4.1
5	3.6	3.7	3.9	4.2
6	3.6	3.8	3.9	4.2
7	3.5	3.7	3.8	4.2
8	3.5	3.7	3.9	4.2
9	3.7	3.8	3.8	4.2
10	3.8	3.9	4.0	4.0

- **Les Evaluations avec IPv6 :**

Tableau 5.5 Tableaux récapitulatif des résultats (MOS) obtenus avec IPv6

Locuteurs	Valeurs MOS En mode Dual Stack IPv6	Valeurs MOS En mode Tunnel IPv6
1	4.0	3.8
2	4.2	3.8
3	4.2	3.8
4	4.0	3.9
5	4.0	4.2
6	3.9	4.0
7	4.0	4.3
8	4.0	4.2
9	3.9	4.2
10	3.8	4.1

- Le Résultat des tests avec les tableaux suivants :

Tableau 5.6 Récapitulatif de la valeur moyenne MOS obtenus avec IPv4

Condition sur La Bande Passante Avec IPv4	La Moyenne des résultats des locuteurs Score MOS
128 Kb/S	3 ,52
512 Kb/S	3 ,74
1 MB/S	3,85
2 MB /S	4 ,09

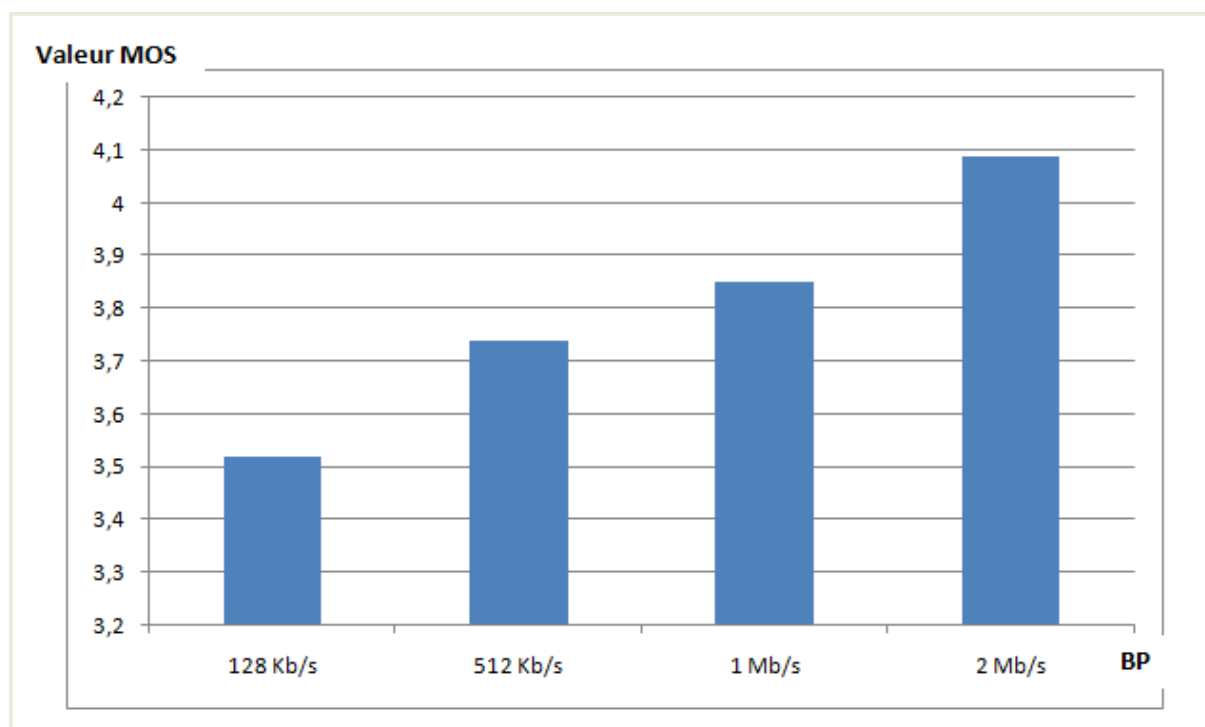


Figure 5.22 representation des valeurs obtenue dans le tableau 5.6

Tableau 5.7 Tableaux récapitulatif de la valeur moyenne MOS obtenus avec IPv6

Mode IPv6	La Moyenne des résultats des locuteurs Score MOS
Dual Stack	4,01
Tunnel IPv6	4,02

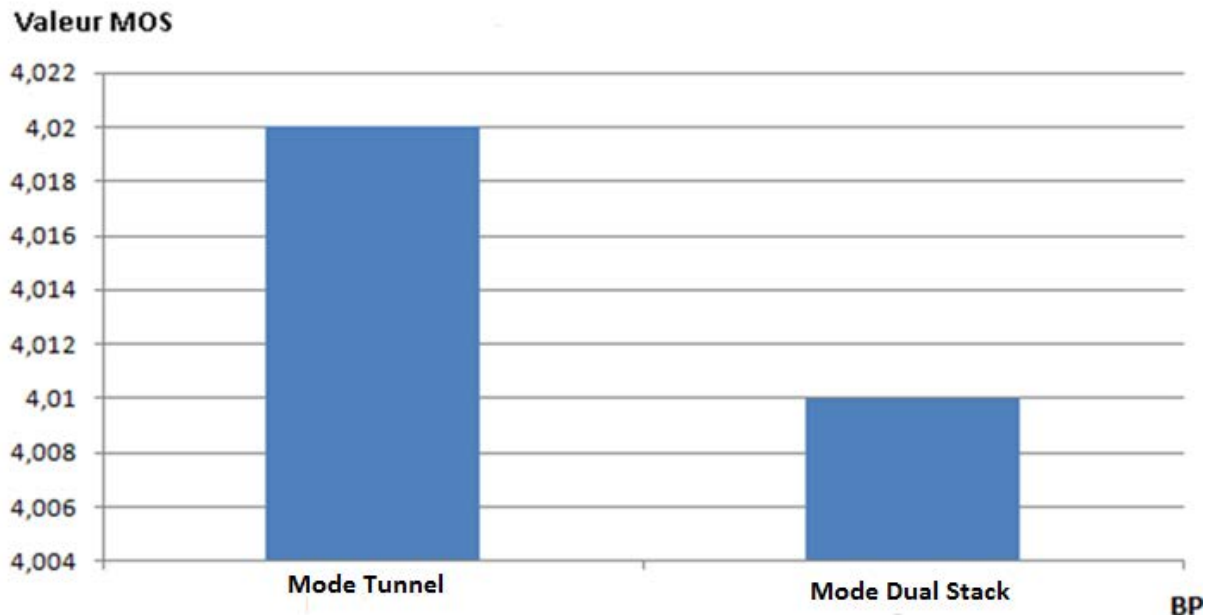


Figure 5.6 Representation des valeurs obtenue dans le tableau 5.7

Conclusion :

Dans ce chapitre, nous avons évalué la solution proposée à travers une étude comparative basée sur les protocoles IPv4 et IPv6, en utilisant les méthodes objectives et subjectives . Si le PESQ n'a pas été en mesure de différencier entre les 2 protocoles, avec la méthode subjective, nous avons obtenu une amélioration de la qualité de la communication à chaque fois que la valeur de bande passante augmente. Pour autant, les résultats ont montré aussi qu'avec le protocole IPv6, le mode Tunnel donne une nette amélioration de la communication VoIP par rapport au mode Dual Stack .

Conclusion Générale :

Dans ce travail, nous avons proposé le déploiement d'une solution VoIP basée sur l'IPv6 et une investigation dans ce domaine à travers l'étude d'un paramètre de QoS qui est la bande passante.

Nous avons d'abord fait une étude sur le fonctionnement d'une communication VoIP, en particulier les étapes de transmission d'un appel VoIP, en déterminant les différentes étapes d'encapsulation sur le réseau IP, avec la nécessité d'introduire de nouveaux protocoles pour une transmission fiable d'un paquet VoIP. Ensuite, nous nous sommes intéressés aux contraintes de la VoIP et leur influence sur la bonne réception d'un appel VoIP et sa clarté, notamment les paramètres de Gigue, délai, perte, Codec.

Pour le développement de la solution de VoIP proposée dans ce travail, nous avons choisi une solution matériel réelle qui est le CME (Call manager Express) de Cisco, et ceci pour des raisons de stabilité et pour garantir des résultats fiables. Par ailleurs, pour le déploiement de la solution VoIP, on a simulé deux réseaux distants (WAN) avec deux routeurs Cisco 2811 et deux commutateurs Catalyst 3560 et quatre téléphones IP du type Cisco 7965, en utilisant différents types de câbles réseau, pour le lien WAN et pour les liens LAN .

L'étape suivante était de lancer des appels VoIP entre deux utilisateurs distants, et de capturer la communication à l'entrée et à la sortie du réseau sous format de fichiers audio .WAV pour d'éventuels tests.

Les différents tests d'évaluation avec la méthode objective (PESQ), n'ont pas donné des résultats concluants quand à l'influence de la bande passante sur la qualité objective de la parole.

Enfin, avec la méthode subjective les résultats des sujets montrent une différence suivant le locuteur. En effet, nous avons obtenu une amélioration de la qualité de la communication à chaque fois que la valeur de bande passante augmente.

Pour autant, les résultats de l'étude comparative effectuée dans ce mémoire montrent que le passage au protocole IPv6 améliore nettement la qualité d'une conversation VoIP et ceci par Les différents mécanismes introduits dans cette versions .

En effet, nous avons observé qu'il existe une différence de qualité de la voix transmise par un système de communication avec le protocole IPv4 et le protocole IPv6, et qu'une

communication VoIP est plus nette et plus audible lorsque la bande passante dans le réseau augmente, ce qui permet d'améliorer la qualité de la parole perçue par l'auditeur. Dans cette ordre d'idée , les résultats expérimentaux montrent une supériorité du mode Tunnel sur le mode Dual Stack pour la solution IPv6 .

En perspective, pour la suite de nos travaux, il sera nécessaire de procéder à de nouveaux tests où le choix du matériel ou de la solution permettra de faire varier d'autres paramètres et notamment l'utilisation de différents Codecs.

L'extension de cette étude aux autres paramètres de la QoS, notamment la perte de paquets serait intéressante et pourrait compléter le déploiement de la solution VoIP basée sur l'IPv6 proposée dans ce travail.

Références Bibliographie :

1. J. Delacroix, "Comment trouver sa voix sur IP ?", Publication coordonnée par la direction de la communication de Completel et l'EBG, Janvier 2006.
2. J.L. Mélin, "Qualité de service sur IP", Edition Eyrolle, 2000.
3. Accellent, "La qualité de service en voix sur IP (Principes et assurance)", document PDF du site : <http://www.accellent.com>, 2009.
4. H. Sathu and M. A. Shah. "Performance Comparison of VoIP Codecs on Multiple Operating Systems using IPv4 and IPv6". *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol. 2, No. 2, April 2012
5. L. Ouakil , et G. Pujolle. "Téléphonie sur IP", Eyrolles. 2007
6. M. Schaffer, "Introduction à la téléphonie IP Asterisk sous GNU/Linux", schaefer@alphanet.ch .C+RInformatique libre 2008
7. Cisco System. "Cisco IOS IPv6 Configuration Guide".Cisco.com 2008
8. Cisco System. "Implementing VoIP for IPv6First Published": October 10, 2008Last Updated,Cisco.com, July 22, 2011
9. R. Yasinovskyy, A. L. Wijesinha, and R. Karne. " Impact of IPsec and 6to4 on VoIP Quality over IPv6". Towson University, Maryland, USA ryasin1@students.towson.edu, awijesinha@towson.edu, rkarne@towson.edu 2009
10. R.Yasinovskyy, A.L. Wijesinha, R.K. Karne, and G. Khaksari, " A Comparison of VoIP Performance on IPv6 and IPv4 Networks". Towson University, 2007
11. M. Chutet . "Téléphonie sur IP – TOIP" ,2008
12. R. Merahi "Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc ".Thèse de Doctorat, Ecole nationale supérieure des télécommunications Paris, 2009
13. J.M. Lozano-Gendreau, A.Z. Halabi, M. Choueiri and V. Besong. " VoWF (Vo-IP over Wi-Fi). Electronics, Communications and Computers, 2006. CONIELECOMP 2006. 16th International Conference on, vol, no, pp. 2- 2, 27-01 Feb. 2006.
14. Cisco System . "Tunneling IPv6 through an IPv4 Network (Configuration Example) ".Cisco .com
15. J. Liu, Z. Niu. "An adaptive receiver buffer adjust algorithm for VoIP applications considering voice characters. Proc. 10th Asia-Pacific Conf. on Comm. " Vol.2, pp.597-601, Beijing, China, August 2004
16. M. A. Tamon , M. Gokool, D. Afahounko . "Manuel de laboratoire IPv6", AfriNIC Ltd
17. R. Beuran, " Mesure de la qualité dans les réseaux informatiques", Thèse pour obtenir le grade de Docteur de l'Université « POLITEHNICA » Bucureti et de l'Université « Jean Monnet » St. Etienne 2004
18. J. Cloara , M. J. Cavanaugh , K. A. Krake. " CCNA Voice" .Ciscopress .com 2011

1. E. Gressier-Soudan, Introduction à la problématique des Réseaux avec QoS, 2002.
2. Par le groupe d'experts sur la téléphonie sur IP : UIT .Le Rapport essentiel sur la téléphonie IP. Union Internationale des Télécommunications.2003
3. Amehraye, Débruitage perceptuel de la parole, Thèse pour obtenir le grade de : Docteur de Télécom Bretagne. Ecole Nationale Supérieure des Télécommunications de Bretagne. 2009