République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Dr. YAHIA Fares de Médéa

Faculté des Sciences et de la Technologie

Département de Génie Electrique et de l'Informatique

Projet de fin d'étude

Pour l'obtention du diplôme de Master

En Systèmes des télécommunications

Thème :

Etude et simulation de la voix sur IP en utilisant l'OPNET



Proposé et dirigé par :

- **Dr. OULD ZMIRLI Mohamed**

Réalisé par :

- **MAMI Ihsene**
- **TCHOKETCH KEBIR Hadjer**

Année universitaire:
2012-2013

Remerciement

Au terme de ce mémoire, nous tenons tout d'abord à remercier par nos profondes gratitudes à ALLAH qui nous a donné la force, la patience et le courage nécessaires pour accomplir ce modeste travail.

Nous remercions également nos chers parents qui nous ont toujours soutenu et encouragé.

Nous tenons à remercier notre promoteur : Dr. OULD ZMIRLI Mohamed pour l'aide que nous a apporté, sa disponibilité et ses précieux conseils durant le déroulement de ce travail afin de le bien mener.

Nos vifs et sincères remerciements vont également à tous les enseignants de département de Génie Electrique et Informatique de l'université Dr. YAHYA Fares de Médéa .

Ainsi, nos remerciements s'adressent aux membres de jury pour leur participation dans l'évaluation de ce travail.



Dédicaces

''Le plus court chemin entre deux points forme une ligne directe ''

Je suis très reconnaissant à mes chers parents pour leur Inspiration qui m'a guidé à mes directs buts durant le chemin de ma vie .pour leur encouragement et Leur coopération qui m'a renforcé pour accomplir mes études. Que dieu les garde.

Je dédie ce modeste travail à mon petit frère Youcef.

A mes frères et mes belles-sœurs : Nasreddine et Yasmine et mes neveux Abd El-Rahmane et Ahmad ; Ayoub et Amina et ma nièce Halla.

A mes sœurs et mes beaux-frères : Sara et Farid et ses enfants Anes, Radjaa et Bachir ; Hassiba et Abdallah et mes neveux Abd Alkarim, Abd Elmalak, Abd Elhadi, Abd Eldjalil et Loaye ; Soumia et Mohamed et leur petite fille Rihab et mes neveux Fatahe et Chouaib.

A les familles TCHOKETCH KEBIR et HADRI en générale.

A mes proches amies, en premier lieu mon binôme MAMI Ihsene, a ALI KHOUDJA Imane, BOUMENIR Karima, MOULAI MUSTAFA Touba, OMARI Amina, OULD BABA ALI Leila et TEBIB Meriem.

A tous qui me connait sans exception.



Hadjer

Dédicaces

Je dédié ce travail à :

- ✓ *Mes chères mama et papa qu'ALLAH les garde et à qui je dis merci beaucoup pour votre soutien moral et financier, pour vos encouragements et que c'est grâce à vous que j'ai pu atteindre ce niveau et terminer mes études.*

- ✓ *Mes grands-parents : passido, omi et mani en leur espérant une longue vie avec une bonne santé et que DIEU les protège.*

- ✓ *Celui qui crée le bonheur et la joie dans ma vie, mon petit frère : Ayoub.*

- ✓ *Mes frères : Mohamed, Amine et Yacine.*

- ✓ *Toute l'équipe : Meriem, Karima, Leila, Iman, Amina, Touba et surtout mon binôme Hadjer.*

- ✓ *Toutes les familles : MAMI et SAFAR BATI sans exception.*



Ihsene

ملخص

الصوت عبر بروتوكول الإنترنت هو تكنولوجيا تسمح بنقل المكالمات عن طريق شبكة الإنترنت و هي مرشحة بأن تكون الأكثر شعبية بفضل تكاليفها المنخفضة. في هذا العمل, درسنا هذه التقنية وأيضا تصميمها و بروتوكولاتها. من جهة أخرى درسنا الخصائص التي تتلف جودة الصوت, و هذا استعانة بمحاكات عدة شبكات مثل الإترنت, الويفي و الويماكس باستعمال برنامج OPNET بغية دراسة تأثير المسافة ,عدد الأجهز و نوع المشفر على جودة الخدمة.

مفاتيح : VoIP , شبكة الكمبيوتر , نوعية الخدمة ,WiFi, Ethernet, WiMAX , OPNET

Résumé

La voix sur IP est une technologie qui permet la communication des appels sur un réseau d'Internet et elle est supposée d'être devenue la plus populaire grâce à ces bas coûts. Dans ce travail, nous avons étudié la VoIP ainsi que son architecture et ses protocoles. D'autre part, nous avons étudiés les paramètres qui peuvent détériorer la qualité de la VoIP et cela à l'aide de simulations sur différents types de réseaux : Ethernet, WiFi et WiMAX en utilisant le logiciel OPNET Modeler afin d'évaluer l'influence de la distance, le nombre de postes et le type du codec sur la qualité de service.

Mots clés : VoIP, voix sur IP, qualité de service, réseau, OPNET, Ethernet, WiFi,

Abstract

VoIP is a technology that allows communication calls to be made over the internet and it is expected to become the popular for communication due to its low cost. In this project, we studied the VoIP, its architecture and its protocols. In addition, we studied the parameters which can deteriorate the quality of VoIP using simulations on various kinds of computer networks: Ethernet, WiFI and WiMAX by using OPNET Modeler in order to evaluate the influence of the distance, the number of stations and the type of codec on the quality of service

Keywords: VoIP, quality of service, computer network, OPNET, Ethernet, WiFi, WiMAX.

Table des matières

Introduction générale *1*

Chapitre I : Etude générale de la voix sur IP

I. Introduction **2**

II. Présentation de la voix sur IP **2**

II.1 Définition de la VoIP **2**

II.2 Architecture de la VoIP **2**

II.3 Fonctionnement de la VoIP **3**

II.3.1 Acquisition du signal **4**

II.3.2 Numérisation **4**

II.3.3 Compression **5**

II.3.4 Habillage des en-têtes **6**

II.3.5 Emission et transport **7**

II.3.6 Réception **7**

II.3.7 Conversion numérique analogique **7**

II.3.8 Restitution **7**

III. Protocoles de la voix sur IP **7**

III.1 Protocoles de transport **8**

III.1.1 Protocole RTP **8**

III.1.1.1 Fonctions de RTP **8**

III.1.1.2 En-tête RTP **9**

III.1.1.3 Avantages et inconvénients de RTP **10**

III.1.2 Protocole RTCP **10**

III.1.1.1 Fonctions de RTCP **10**

III.1.1.2 En-tête RTCP **11**

III.1.1.3 Avantages et inconvénients de RTCP **12**

III.2 Protocoles de Signalisation **12**

III.2.1 La norme H.323 de l'UIT **12**

III.2.1.1 Architecture H.323 ..... **12**

III.2.1.2 Pile protocolaire H.323 ..... **13**

III.2.1.3 Avantages et inconvénients **16**

III.2.2 Protocole SIP de l'IETF 18
III.2.2.1 Clients et serveurs SIP 18
III.2.2.2 Messages SIP 19
III.2.2.3 Exemple de communication SIP 20
III.2.2.4 Avantages et inconvénients de SIP 21
III.2.3 Le protocole MGCP 22
III.2.3.1 Architecture MGCP 22
III.2.3.2 Avantages et inconvénients 23
VI. Avantages et inconvénients de la VoIP 24
VI.1 Avantages 24
VI.2 Inconvénients 24
V. Conclusion 25
Chapitre II : Description des différents modèles de simulations réalisées
I. Introduction 26
I.1 Facteurs de dégradation de la qualité de service QoS VoIP 27
a. Latence (Délai de bout en bout) 27
b. Gigue 28
c. Perte de paquets 28
I.2 Note d'opinion moyenne(MOS) 28
II. Présentation de simulateur réseau OPNET Modeler 14.5 29
II.1 Interface d'OPNET 30
II.1.1 Project editor (éditeur de projet) 30
II.1.2 Network model editor (éditeur de modèle de réseau) 32
II.1.3 Node model editor (éditeur de modèle de nœud) 32
II.1.4 Process model editor (éditeur de modèle de processus) 32
II.1.5 Antenna pattern 32
II.1.6 Modulation curve (courbe de modulation) 32
II.1.7 Simulation Sequence (ordre de simulation) 32
II.1.8 Analysis Configuration (Configuration d'analyse) 32
II.2 Cycle traditionnel d'un projet OPNET 33
III. Description des projets de simulations réalisés 33
III.1 Création d'un projet dans l'OPNET 33
III.2 Configuration d'application VoIP et de profil 35

III.2.1 Configuration d'application VoIP 35
III.2.2 Configuration de profil 37
III.3 Topologies des différents cas de simulations (scénarios) 39
III.3.1 Vue générale sur les projets réalisées 39
III.3.1.1 Projet 1 : réseau *Ethernet* 39
III.3.1.2 Projet 2 : réseau *WiFi* 40
III.3.1.3 Projet 3 : *Wimax* 42
III.3.2 Vue générale sur les scénarios 45
III.4 Choix des statistiques à collecter 51
VI. Conclusion 51
Chapitre III : Résultats de simulations et discussions
I. Introduction 53
II. Résultats de simulations et discussions 53
Projet 1 : réseau *Ethernet* 53
1. **Modification de distance 53**
2. **Modification de nombre de poste 55**
3. **Modification de type de codec 59**

Projet 2 : réseau *WiFi* 62
1. **Modification de distance 62**
2. **Modification de nombre de poste 65**
3. **Modification de type de codec 68**

Projet 1 : réseau *Wimax* 71
1. **Modification de distance 71**
2. **Modification de nombre d'utilisateurs 74**
3. **Modification de type codec 77**

III. Conclusion 80
Conclusion générale 81

Liste des figures

Figure I.1 : Architecture de la VoIP **2**

Figure I.2 : Les huit étapes de fonctionnement de la VoIP **4**

Figure I.3 : Echelle MOS des différents codecs **6**

Figure I.4 : En-tête RTP **9**

Figure I.5 : En-tête RTCP **11**

Figure I.6 : Architecture matérielle d'une zone H.323 ..... **12**

Figure I.7 : La pile protocolaire H.323 ..... **14**

Figure I.8 : Scénario complet d'une communication H.323 ..... **15**

Figure I.9 : Architecture protocolaire SIP **18**

Figure I.10 : Ouverture d'une communication en mode proxy **21**

Figure II.1 : Projets de simulation **27**

Figure II.2 : OPNET Modeler 14.5 ..... **29**

Figure II.3 : Palette d'objets **30**

Figure II.4 : Environnement géographique de l'OPNET **31**

Figure II.5 : Création d'un nouveau projet **33**

Figure II.6 : Nommage de projet et de scénario **34**

Figure II.7 : Création d'un scénario vide **34**

Figure II.8 : Choix de la taille du réseau **34**

Figure II.9 : Résumé des choix **35**

Figure II.10 : Application Definition **35**

Figure II.11 : Configuration d'application **36**

Figure II.12 : Application VoIP....**36**

Figure II.13 : Profile Definition....**37**

Figure II.14: Configuration de profil **37**

Figure II.15: Paramètres d'application....**38**

Figure II.16: Attributs de poste de travail **38**

Figure II.17: Supported profile....**39**

Figure II.18: Supported services....**39**

Figure II.19: Configuration de poste de travail **41**

Figure II.20: Configuration de routeur (point d'accès)....**42**

Figure II.21: Configuration de Wimax....**43**

Figure II.22: Configuration de station de base **44**

Figure II.23: Configuration de poste de travail **45**

Figure II.24: Topologie de réseau Ethernet longue distance....**48**

Figure II.25: Topologie de sous réseau d'une compagnie **48**

Figure II.26: Ethernet avec 20 utilisateurs **49**

Figure II.27: Configuration de LAN....**49**

Figure II.28: Choix des paramètres à poursuivre....**51**

Figure III.1: Gigue dans les scénarios courte et longue distance dans le réseau Ethernet....**53**

Figure III.2: Valeur MOS dans les scénarios courte et longue distance dans le réseau Ethernet **54**

Figure III.3: Délai de bout en bout dans les scénarios courte et longue distance dans le réseau Ethernet **54**

Figure III.4: Perte de paquets dans les scénarios courte et longue distance dans le réseau Ethernet **55**

Figure III.5: Gigue dans les scénarios utilisant 2, 10, 20 et 100 postes dans un réseau Ethernet **56**

Figure III.6: Valeur MOS dans les scénarios utilisant 2, 10, 20 et 100 postes dans un réseau Ethernet **56**

Figure III.7: Délai de bout en bout dans les scénarios utilisant 2, 10, 20 et 100 postes dans un réseau Ethernet..... **57**

Figure III.8: Perte de paquet dans les scénarios utilisant 2, 10, 20 et 100 postes dans un réseau Ethernet..... **58**

Figure III.9: Gigue dans les applications VoIP avec différents types de codec dans le réseau Ethernet **59**

Figure III.10: Valeur MOS dans les applications VoIP avec différents types de codec dans le réseau Ethernet..... **60**

Figure III.11: Délai dans les applications VoIP avec différents types de codec dans le réseau Ethernet **60**

Figure III.12: perte de paquet dans les applications VoIP avec différents types de codec dans le réseau Ethernet..... **61**

Figure III.13: Gigue dans les scénarios courte et longue distance dans le réseau WiFi..... **63**

Figure III.14: Valeur MOS dans les scénarios courte et longue distance dans le réseau WiFi **63**

Figure III.15: Délai de bout en bout dans les scénarios courte et longue distance dans le réseau WiFi..... **64**

Figure III.16: Perte de paquets dans les scénarios courte et longue distance dans le réseau WiFi **64**

Figure III.17: Gigue dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiFi . **65**

Figure III.18: Valeur MOS dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiFi **65**

Figure III.19: Délai dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiFi .. **66**

Figure III.20: Perte de paquet dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiFi **67**

Figure III.21: Gigue dans les applications VoIP avec différents types de codec dans le réseau WiFi **68**

Figure III.22: Valeur MOS dans les applications VoIP avec différents types de codec dans le réseau WiFi..... **69**

Figure III.23: Délai dans les applications VoIP avec différents types de codec dans le réseau WiFi **69**

Figure III.24: Perte de paquet dans les applications VoIP avec différents types de codec dans le réseau WiFi **70**

Figure III.25: Gigue dans les scénarios courte et longue distance dans le réseau Wimax **72**

Figure III.26: Valeur MOS dans les scénarios courte et longue distance dans le réseau Wimax **72**

Figure III.27: Délai de bout en bout dans les scénarios courte et longue distance dans le réseau Wimax **73**

Figure III.28 : Perte de paquets dans les scénarios courte et longue distance dans le réseau Wimax **73**

Figure III.29: Gigue dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau Wimax **74**

Figure III.30: Valeur MOS dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau Wimax..... **75**

Figure III.31: Délai dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau Wimax **75**

Figure III.32: Perte de paquet dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau Wimax..... **76**

Figure III.33: Gigue dans les applications VoIP avec différents types de codec dans le réseau Wimax **77**

Figure III.34: Valeur MOS dans les applications VoIP avec différents types de codec dans le réseau Wimax **78**

Figure III.35: Délai dans les applications VoIP avec différents types de codec dans le réseau Wimax **78**

Figure III.36: Perte de paquet dans les applications VoIP avec différents types de codec dans le réseau Wimax **79**

Liste des tableaux

Tableau I.1: Codecs d'état des messages de réponse SIP **20**

Tableau II.1: Exemple de simulateurs réseaux..... **26**

Tableau II.2: Comparaison des satisfactions des utilisateurs en fonction de MOS..... **29**

Tableau II.3: Les fonctions principales de l'éditeur objet **31**

Tableau II.4: Composants Ethernet **40**

Tableau II.5: Composants WiFi **41**

Tableau II.6: Composants Wimax **43**

Tableau II.7: Les topologies des scénarios de courte distance pour les trois réseaux **46**

Tableau II.8: Les topologies des scénarios de longue distance pour les réseaux WiFi et Wimax..... **47**

Tableau II.9: Topologies des réseaux WiFi et Wimax avec différents nombre d'ordinateurs. **50**

Tableau III.1: Gigue, MOS, délai de bout en bout et perte de paquets dans les différents cas de scénario de projet Ethernet **62**

Tableau III.2: Gigue, MOS, délai de bout en bout et perte de paquets dans les différents cas de scénario de projet WiFi **71**

Tableau III.3: Gigue, MOS, délai de bout en bout et perte de paquets dans les différents cas de scénario de projet Wimax..... **80**

Liste des abréviations

ATM: Asynchronous **T**ransfer **M**ode (Mode de transfert asynchrone).

BER: Bit **E**rror **R**ate (Taux d'erreur binaire).

CSRC: Contributing **S**ource (Identificateur de source de contribution).

DNS : Domain **N**ame **S**erver (système de noms de domaine).

DSP: Digital **S**ignal **P**rocessor (Traitement numérique de signal).

DTMF: Dual **T**one **M**ulti **F**requency (Double tonalité multifréquence).

IETF: Internet **E**ngineering **T**ask **F**orce (Détachement d'ingénierie d'Internet).

IP: Internet **P**rotocol (Protocole d'internet).

LDAP: Lightweight **D**irectory **A**ccess **P**rotocol (Protocole d'accès de répertoire léger).

MCU: Multipoint **C**ontrol **U**nit (Unité de contrôle multipoints).

MG: Media **G**ateway (Passerelle de média).

MGC: Media **G**ateway **C**ontroller (Contrôleur de passerelle de média).

MGCP: Media **G**ateway **C**ontroller Protocol (Protocole contrôleur de passerelle de média).

MMUSIC: Multiparty **M**ultimedia **S**ess**I**on **C**ontrol (Contrôle de session multimedia multipartie).

MOS: Mean **O**pinion **S**core (Note d'opinion moyenne).

MPPP: Multilink **P**oint to **P**oint **P**rotocol (Protocole de point à point multiliaisons).

OPNET: Operation **NET**work (Opération de réseau).

PABX: Private **A**utomatic **B**ranch e**X**change. (Autocommutateur de téléphonie privée).

QoS: Qualite **o**f **S**ervice (Qualité de service).

RAS: Remote **A**ccess **S**erver (Serveur d'accès distant).

RNIS: Réseau **N**umérique à **I**ntégration de **S**ervices

RR : Receiver **R**eport (Rapport du récepteur).

RSVP: Resource re**S**er**V**ation setup **P**rotocol (Protocole de réservation des ressources).

RTC : Réseau **T**éléphonique **C**ommuté

RTCP: Real-time **T**ransport **C**ontrol **P**rotocol (Protocole de contrôle de transport temps réel).

RTP: Real-time **T**ransport **P**rotocol (Protocole de transport temps réel).

SAP: Session **A**nnouncement **P**rotocol (Protocole d'annonce de session).

SB-MICDA: Modulation et Codage Différentiel Adaptatif à Sous-Bandes

SDES: Source **Des**cription (Description de la source).

SDP: Session **D**escription **P**rotocole (Protocole de description de session).

SG: Signaling **G**ateway (Passerelle de signalisation).

SIGTRAN: SIGnaling **TRAN**smission (Transmission de signalization).

SIP: Session **I**nitiation **P**rotocol (Protocole d'initiation de session).

SR: Sender **R**eport (Rapport d'émetteur).

SSRC: Synchronization **S**ource (Identificateur de source de synchronisation)

TCP: Transmission **C**ontrol **P**rotocol (Protocole de contrôle de transmission).

TTY: Text **T**elet**Y**pe (Téléscripteur).

UAC: User **A**gent **C**lient (Client agent utilisateur).

UAS : User **A**gent **S**erver (Client agent serveur).

UDP: User **D**atagram **P**rotocol (Protocole de datagramme d'utilisateur).

UIT: Union **I**nternationale des **T**élécommunications.

VoIP: Voice **o**ver **IP** (Voix sur IP).

WiFi: Wireless **Fi**delity (Fédilité sans fil).

Wimax: Worldwide **i**nteroperability for **m**icrowave access. (L'interopérabilité mondiale pour l'accès micro-ondes)



Introduction générale



Introduction générale

Depuis quelques années, la technologie VoIP (voix sur IP) commence à intéresser les entreprises, surtout celles de service comme les centres d'appels. La migration des entreprises vers ce genre de technologie n'est pas pour rien, le but est principalement de minimiser le coût des communications, de configuration et d'assistance.

C'est une sous-estimation pour dire que la VoIP est populaire puisqu'elle a une dominance commandante dans l'industrie des télécommunications. La grande transitoire dans la popularité est due à sa rentabilité et flexibilité sur les marchés des consommateurs d'entreprise. VoIP exige seulement un raccordement à large bande pour une communication locale ou longue distance sur les réseaux IP, elle supporte également des dispositifs de la téléphonie traditionnelle avec un coût moins cher aux consommateurs.

Aujourd'hui, la VoIP est devenue une des technologies les plus employées dans un aspect globale, comme elle présente un développement extraordinaire de son utilisation dans les maisons et les organisations. Jusqu'ici, une série de logiciels de communications VoIP ont déjà en service dans le marché, tel que Skype, AIM, Windows live Messenger, Yahoo Messenger, Jabber et Google Talk.

La voix sur IP est la transmission d'une conversation vocale sur un réseau IP c'est-à-dire sur un réseau de données par opposition à une transmission sur les réseaux téléphoniques classiques ou commutés. Ce travail a pour but d'étudier cette technologie d'une façon générale et d'évaluer les paramètres de sa qualité de service à travers une simulation à l'aide du simulateur réseau : OPNET Modeler 14.5.

Ce mémoire est divisé en trois chapitres, le premier chapitre sera consacré à une étude générale de la voix sur IP, il présente la partie théorique.

Le deuxième chapitre aura le but de présenter le simulateur OPNET en détaillant le fonctionnement de ces interfaces, ainsi que la description des différents scénarios de simulations avec l'explication de la méthode de travail suivie.

Le dernier chapitre présente les résultats obtenus à partir des simulations de plusieurs scénarios décrites dans le deuxième chapitre.



Chapitre 1 :

Etude générale de la voix sur IP



I. Introduction :

VoIP est un terme qui regroupe l'ensemble des protocoles internet destinés à la transmission des signaux sonores à travers un réseau basé sur des adresses IP. De plus, il permet l'extension de l'internet au réseau servant aux communications téléphoniques traditionnelles.

Le but de ce chapitre est d'étudier cette technologie en détaillant son architecture, son fonctionnement, ses protocoles de synchronisation et de transport ainsi que ses avantages et ses inconvénients.

II. Présentation de la voix sur IP :

II.1. Définition de la VoIP:

La voix sur IP (VoIP ou *Voice over Internet Protocol*) consiste à transmettre une conversation vocale sur un réseau au protocole IP (*Internet Protocol*) c'est à dire sur un réseau de données par opposition à une transmission sur le réseau téléphonique classique ou réseau téléphonique commuté (RTC).

IP présente la caractéristique de transporter des données sous forme de paquets. La voix est donc digitalisée, compressée, envoyée par paquets de données sur le réseau conformément au protocole IP. Les données reçues sont décompressées et converties en voix audible.

Tous types de réseau IP peuvent donc être utilisés, réseaux privés ou réseau internet public, ainsi que tous types d'accès au réseau, Frame Relay, ATM, sans fil, fibre… [2]

II.2. Architecture de la VoIP :

L'architecture générale de la voix sur IP en entreprise est présentée dans la figure I.1.

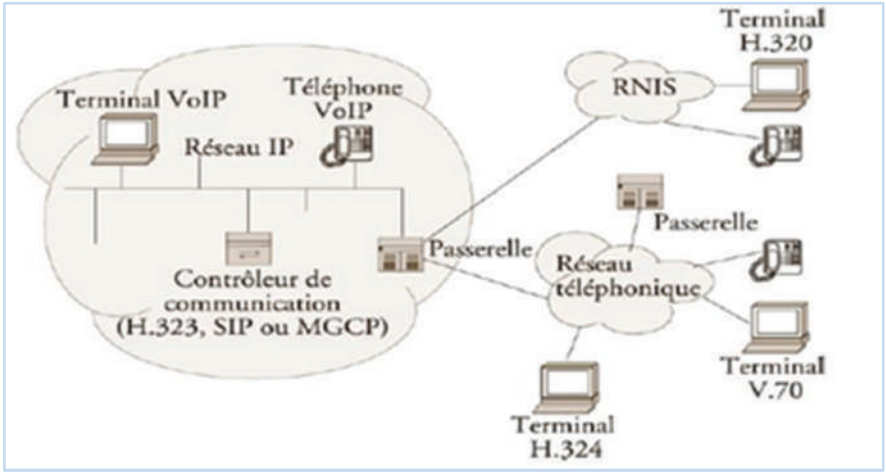


Figure I.1 : Architecture de la VoIP

Le schéma illustré dans la figure I.1, décrit de façon générale la topologie d'un réseau de voix sur IP. Elle comprend des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour garantir une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur le Gatekeeper (contrôleur de communication). On retrouve les éléments communs suivants :

Le routeur : Il permet d'aiguiller les données et le routage des paquets entre deux réseaux. Certains routeurs, comme les Cisco 2600, permettent de simuler un gatekeeper grâce à l'ajout de cartes spécialisées supportant les protocoles VoIP.

Le PABX : C'est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur et le réseau RTC. Une mise à jour du PABX est aussi nécessaire. Si tout le réseau devient IP, il n'y a plus besoin de ce matériel [3].

Terminaux : Ce sont les équipements de traitement destinés aux utilisateurs, leur permettant d'émettre et de recevoir des appels. Deux terminaux doivent au minimum être présents pour qu'une communication ait lieu.

Gatekeeper, ou garde-barrière : C'est l'équipement permettant la localisation des utilisateurs. Ces derniers peuvent s'identifier entre eux par des noms, auxquels il faut attribuer l'adresse IP correspondante dans le réseau ou, si l'appelé n'est pas situé dans un réseau IP, la localisation de l'entité intermédiaire à joindre pour l'appel. Outre cette fonction primordiale, un gatekeeper remplit tout un ensemble de fonctions complémentaires de gestion et de contrôle des communications, certaines étant indispensables et d'autres facultatives.

Gateway, ou passerelle : C'est l'équipement permettant à des utilisateurs du réseau IP de joindre les utilisateurs qui sont actifs sur d'autres types de réseaux téléphoniques, RTC, RNIS ou ATM. On peut avoir autant de passerelles différentes que nécessaire, suivant la nature des réseaux non-IP à interconnecter [4].

II.3. Fonctionnement de la VoIP :

Le principe de la voix sur IP est la numérisation de la voix, c'est-à-dire le passage d'un signal analogique à un signal numérique. Celui-ci est compressé en fonction des codecs choisis, cette compression a comme but de réduire la quantité d'information qui est transmise

sur le réseau. Le signal obtenu est découpé en paquets, à chaque paquet on ajoute les en-têtes propres au réseau (IP, UDP, RTP....) et pour finir, il est envoyé sur le réseau.

A l'arrivée, les paquets transmis sont réassemblés en supprimant d'abord les en-têtes. La donnée ainsi obtenue est décompressée puis convertie en signal analogique afin que l'utilisateur puisse écouter le message d'origine.

La technologie de la voix sur IP nous présente une architecture découpée en 8 grandes étapes comme le montre la figure I.2.

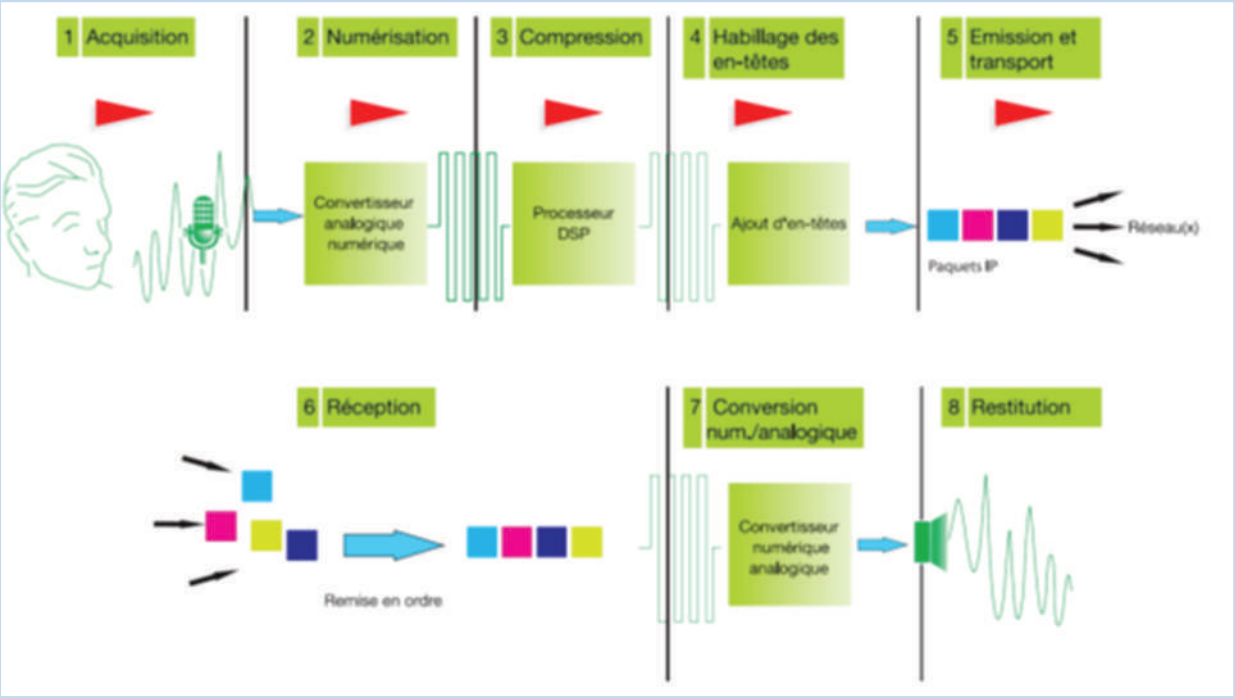


Figure I.2 : Les huit étapes de fonctionnement de la VoIP

II.3.1. Acquisition du signal :

La première étape consiste naturellement à capter la voix à l'aide d'un micro, qu'il s'agisse de celui d'un téléphone ou d'un micro-casque. Ce signal est de type continu ou analogique.

II.3.2. Numérisation :

La voix passe alors dans un convertisseur analogique numérique qui réalise deux tâches distinctes :

- l'échantillonnage du signal sonore, c'est-à-dire un prélèvement périodique de ce signal ;

- la quantification, qui consiste à affecter une valeur numérique (en binaire) à chaque échantillon. Plus les échantillons sont codés sur un nombre de bits important, meilleure sera la qualité (on parle de "résolution") de la conversion.
  Généralement, la voix est échantillonnée à 8 kHz et chaque échantillon est codé sur 8 bits, ce qui donne un débit de 64 kbit/s (norme G711).

II.3.3. Compression :

Le signal une fois numérisé peut être traité par un DSP (*Digital Signal Processor*) qui va le compresser, c'est-à-dire réduire la quantité d'informations (bits) nécessaire pour l'exprimer. Plusieurs normes de COmpression / DECompression (Codecs) sont utilisées pour la voix.

L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal. Mais ce gain peut se faire au détriment de la qualité sonore.

Celle-ci peut être mesurée sur une échelle allant de 1 à 5, appelée échelle MOS (*Mean Opinion Score*). Un score MOS est une mesure subjective réalisée grâce à une étude auprès d'un panel d'individus. L'échelle varie de 1 à 5 où 5 (score théorique) désigne une qualité parfaite.

Parmi les principaux codecs décrits par l'UIT (*Union Internationale des Télécommunications*), on peut citer :

- G711 : compresse le signal à un débit de 64 kbit/s. Cette norme, largement supplantée par les suivantes, continue néanmoins à servir de référence en termes de fidélité au signal. (score MOS de 4,2)
- G722 : Cette norme, connue également sous l'appellation SB-MICDA (*Modulation et Codage Différentiel Adaptatif à Sous-Bandes*), propose trois niveaux de débits : 64, 56, ou 48 kbit/s. Ses principaux avantages sont de coder le spectre sonore jusqu'à 7000 Hz et d'être très rapide (délai algorithmique de 1,5 ms). Son score en 64 kbit/s est de 4.
- G723.1 : Il s'agit d'une norme particulièrement adaptée aux transmissions bas débits puisqu'elle fonctionne à 6,4 kbit/s ou 5,3 kbit/s. La contrepartie est une moindre qualité (scores MOS respectivement de 3,9 et 3,7).
- G729 : Avec les normes de la famille G723, G729 est le codec le plus utilisé pour la VoIP. Il fonctionne à un débit de 8 kbit/s et obtient un score MOS de 4.0, ce qui

correspond à la qualité téléphonique. Comme G723.1, il ne permet pas la transmission des signaux fax ou fréquences vocales (DTMF, *Dual Tone Multi Frequency*).

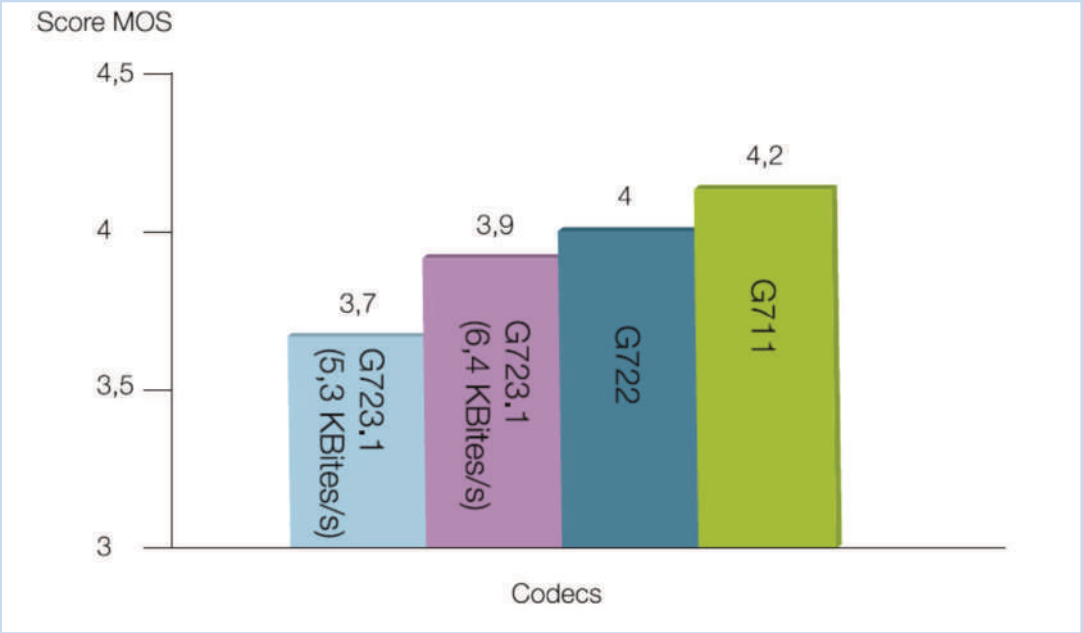


Figure I.3 : Echelle MOS des différents codecs

II.3.4. Habillage des en-têtes :

Les données "brutes" qui sortent du DSP doivent encore être enrichies en informations avant d'être converties en paquets de données à expédier sur le réseau. Trois "couches" superposées sont utilisées pour cet habillage :

- **IP :** La couche IP correspond à l'assemblage des données en paquets. Chaque paquet commence par un en-tête indiquant le type de trafic concerné, ici du trafic UDP.
- **UDP** : La deuxième couche, UDP, consiste à formater très simplement les paquets. Si l'on restait à ce stade, leur transmission serait non fiable : UDP ne garantit ni le bon acheminement des paquets, ni leur ordre d'arrivée.
- **RTP** (*Real Time Protocol*) / **RTCP** (*Real Time Control Protocol*): Pour pallier l'absence de fiabilité d'UDP, un formatage RTP est appliqué de surcroît aux paquets. Il consiste à ajouter des en-têtes d'horodatage et de synchronisation pour s'assurer du réassemblage des paquets dans le bon ordre à la réception. RTP est souvent renforcé par RTCP qui comporte, en plus, des informations sur la qualité de la transmission et l'identité des participants à la conversation.

II.3.5. Emission et transport :

Les paquets sont acheminés depuis le point d'émission pour atteindre le point de réception sans qu'un chemin précis soit réservé pour leur transport. Ils vont transiter sur le réseau (réseau local, réseau étendu voire Internet) en fonction des ressources disponibles et arriver à destination dans un ordre indéterminé.

II.3.6. Réception :

Lorsque les paquets arrivent à destination, il est essentiel de les replacer dans le bon ordre et assez rapidement. Faute de quoi une dégradation de la voix se fera sentir.

II.3.7. Conversion numérique analogique :

La conversion numérique analogique est l'étape réciproque de l'étape 2, qui permet de transformer les données reçues sous forme de série discrète en un signal électrique "continu".

II.3.8. Restitution :

Dès lors, la voix peut être retranscrite par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur [5].

III. Protocoles de la voix sur IP :

La voix sur IP nécessite l'utilisation des protocoles pour la signalisation et le transport des données y compris H.323, SIP, MGCP, RTP et RTCP qu'on va les détailler dans cette partie, ainsi que des protocoles complémentaires comme :

- RSVP (*Resource reSerVation Protocol*) qui autorise pour les flux multimédia, une réservation de ressources réseau de bout en bout. Ce protocole permet la cohabitation des flux multimédia et des flux sporadiques non prioritaires ;
- MPPP (*Multilink Point to Point Protocol*) qui assure la segmentation des paquets longs en petits paquets et autorise le multiplexage de ces paquets avec des paquets temps réel [6].

III.1. Protocoles de transport:

Nous décrivons deux protocoles de transport utilisés dans la voix sur IP à savoir l'RTP et le RTCP.

III.1.1. Protocole RTP :

III.1.1.1. Fonctions de RTP :

RTP est un protocole qui a été développé par l'IETF afin de faciliter le transport temps réel de bout en bout des flux de données, audio et vidéo sur les réseaux IP, c'est à dire sur les réseaux de paquets. RTP est un protocole qui se situe au niveau de l'application et qui utilise les protocoles sous-jacents de transport TCP ou UDP. Mais l'utilisation de RTP se fait généralement au-dessus d'UDP ce qui permet d'atteindre plus facilement le temps réel. Les applications temps réels comme la parole numérique ou la visioconférence constitue un véritable problème pour l'internet. Qui dit application temps réel, dit présence d'une certaine qualité de service (QoS) que RTP ne garantit pas du fait qu'il fonctionne au niveau Applicatif. De plus, RTP est un protocole qui se trouve dans un environnement multipoint, donc on peut dire que RTP possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoint.

RTP est un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de :

- Reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur) ;
- Mettre en place un séquencement des paquets par une numérotation afin de permettre la détection des paquets perdus. Ceci est un point primordial dans la reconstitution des données. Mais il faut savoir quand même que la perte d'un paquet n'est pas un gros problème si les paquets ne sont pas perdus en trop grand nombre. Cependant il est très important de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte. Et ce par le remplacement par un paquet qui se compose d'une synthèse des paquets précédant et suivant ;
- Identifier le contenu des données pour leurs associer un transport sécurisé ;
- L'identification de la source c'est à dire l'identification de l'expéditeur du paquet. Dans un multicast, l'identité de la source doit être connue et déterminée ;
- Transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation). Ces trames sont incluses

dans des paquets afin d'être transportées et doivent de ce fait être récupérées facilement au moment de la phase de dépaquétisation afin que l'application soit décodée correctement.

III.1.1.2. En-tête RTP :

L'en-tête d'un paquet RTP est obligatoirement constitué de 16 octets. Cet en-tête précède le "Payload" qui représente les données utiles.

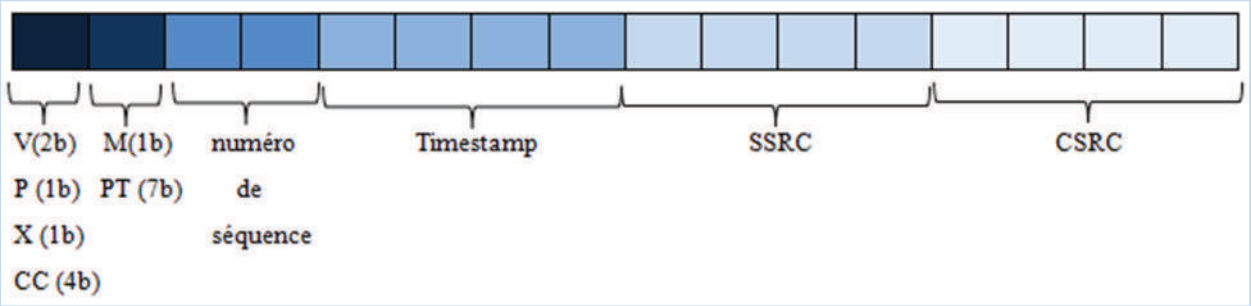


Figure I.4 : En-tête RTP

V : Ce champ permet d'indiquer la version de RTP.

P : Ce bit indique s'il est à 1 que les données possèdent une partie de bourrage.

X : Ce bit spécifie, s'il est à 1, que l'en-tête est suivi d'un en-tête supplémentaire.

CC : Ce champ représente le nombre de CSRC qui suit l'en-tête.

M : Ce bit définit que l'interprétation de la Marque est par un profil d'application.

PT : Ce champ identifie le type du payload (audio, vidéo, image, texte, html, etc.).

Numéro de séquence : Ce champ représente le numéro d'ordre d'émission des paquets. Sa valeur initiale est aléatoire et il s'incrémente de 1 à chaque paquet envoyé, il peut servir à détecter des paquets perdus.

Timestamp : Ce champ horodatage représente l'horloge système ou l'horloge d'échantillonnage de l'émetteur. Elle doit être monotone et linéaire pour assurer la synchronisation des flux.

SSRC : ce champ identifie de manière unique la source de synchronisation, sa valeur est choisie de manière aléatoire par l'application.

CSRC : Ce champ identifie les sources de contribution. La liste des participants ayant leur contribution (audio, vidéo) aux donnée du paquet [3].

III.1.1.3. Avantage et inconvénient de RTP :

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.); de détecter les pertes de paquets; et d'identifier le contenu des paquets pour leur transmission sécurisée.

Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi il ne garantit pas le délai de livraison.

III.1.2. Protocole RTCP :

III.1.2.1. Fonctions de RTCP :

Le protocole RTCP est fondé sur la transmission périodique des paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP.

Le protocole RTP utilise le protocole RTCP, *Real-time Transport Control Protocol,* qui transporte les informations supplémentaires pour la gestion de la session. Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS.

Ces rapports comprennent le nombre de paquets perdus, le paramètre indiquant la variance d'une distribution (plus communément appelé la gigue : c'est à dire les paquets qui arrivent régulièrement ou irrégulièrement) et le délai aller-retour. Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS.

Les principales fonctions qu'offre le protocole RTCP sont les suivants :

- **Une synchronisation supplémentaire entre les médias :** Les applications multimédia sont souvent transportées par des flots distincts. Par exemple, la voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérés et suivre des différents chemins.
- **L'identification des participants à une session :** En effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- **Le contrôle de la session :** En effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus. La périodicité est calculée en fonction du nombre de

participants de l'application. On peut dire que les paquets RTP ne transportent que les données des utilisateurs. Tandis que les paquets RTCP ne transportent en temps réel, que de la supervision.

On peut détailler les paquets de supervision en 5 types:

- **SR (*Sender Report*) :** Ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé de paquets perdus, variation de délai (gigue), etc.). Ces rapports sont issus d'émetteurs actifs d'une session.
- **RR (*Receiver Report)* :** Ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.
- **SDES (*Source Description*) :** Carte de visite de la source (nom, e-mail, localisation).
- **BYE :** Message de fin de participation à une session.
- **APP :** Fonctions spécifiques à une application [8].

III.1.2.2. En-tête RTCP :

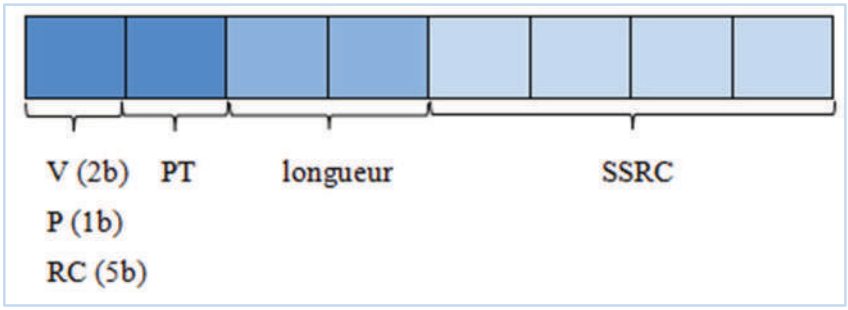


Figure I.5 : en-tête RTCP

V : Ce champ, codé sur 2 bits, permet d'indiquer la version de RTP, qui est la même que dans les paquets RTCP. Actuellement, V=2.

P : Ce bit indique, S'il est à 1, que les données possèdent une partie de bourrage.

RC : Ce champ, basé sur 5 bits, indique le nombre de blocs de rapport de réception contenus en ce paquet. Une valeur de zéro est valide.

PT : Ce champ est fixé à 200 pour identifier ce datagramme RTCP comme SR.

Longueur : Ce champ de 2 octets, représente la longueur de ce paquet RTCP incluant l'en-tête et le bourrage.

SSRC: Ce champ, représente l'identification de la source pour le créateur de ce paquet SR [3].

III.1.2.3. Avantage et inconvénient de RTCP :

Le protocole RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanant sur une session et ces participants. Par contre il fonctionne en stratégie bout à bout. Et il ne peut pas contrôler l'élément principal de la communication « le réseau » [8].

III.2. Protocoles de signalisation:

Il existe plusieurs protocoles qui peuvent supporter la voix sur IP tel que le H.323, SIP et MGCP. Les deux protocoles les plus utilisés actuellement dans les solutions VoIP présentes sur le marché sont le H.323 et le SIP.

III.2.1. La norme H.323 de l'UIT :

III.2.1.1. Architecture H.323 :

La recommandation H.323 définit un modèle architectural pour assurer le transport de la voix sur un réseau en mode paquets de type IP, c'est-à-dire sans qualité de service. L'architecture H.323 comprend diverses fonctionnalités (ou éléments) représentées dans la figure I.6.

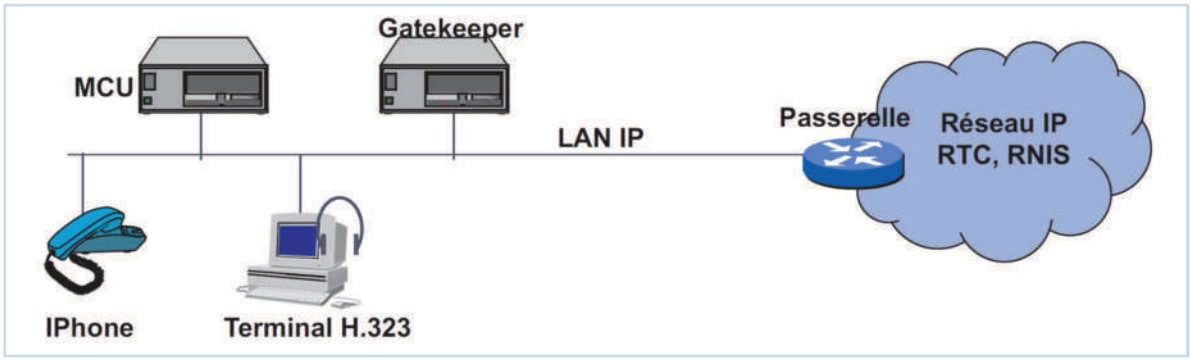


Figure I.6 : Architecture matérielle d'une zone H.323

Les terminaux H.323 sont raccordés directement au LAN IP. Ils ont la capacité d'établir des communications voix, vidéo et/ou données en temps réel avec tout terminal de la zone H.323 ou non en mode point à point, multipoint ou diffusion. L'appel est réalisé selon le protocole Q.931 (protocole D du RNIS). Les protocoles mis en œuvre par un terminal H.323 sont :

- H.225 ou RAS (*Registration Admission Status*), ce protocole gère l'enregistrement auprès d'une passerelle (Registration), réalise une demande de ressource auprès du

Gatekeeper (Admission et Status). Il est également chargé de la signalisation et de l'établissement d'un appel (sous-ensemble du protocole Q.931 du RNIS) ;

- H.245, ce protocole permet aux terminaux d'échanger leurs capacités audio/vidéo (codecs supportés, nombre de canaux possibles, modes de conférence acceptés...) et de négocier les canaux logiques de dialogue ;
- T.120, protocole optionnel qui gère l'échange de données entre terminaux H.323.

La passerelle H.323 ou Gateway assure l'interface avec une entité H.323 et une entité non H.323 comme les réseaux RNIS (H.320) ou ATM (H.321), la conversion de signalisation H.225/Q.931, l'adaptation des supports et des débits. Chaque passerelle H.323 connaît les numéros E.164 (numéros de téléphone) qui lui sont rattachés, elle dispose en mémoire d'une table de correspondance qui associe à un numéro E.164 une adresse IP, un email ou un alias. Si le réseau est important, la maintenance des tables peut devenir vite impossible. Ce problème trouve sa solution par l'emploi d'un Gatekeeper (garde barrière) qui va centraliser les tables de conversion d'adresses. Chaque Gateway vient s'enregistrer sur son Gatekeeper et lui déclare toutes ses adresses E.164. Lorsqu'une passerelle doit établir un appel, elle s'adresse au Gatekeeper qui lui fournit l'adresse IP de la passerelle destination.

Le garde barrière H.323 ou Gatekepeer, système optionnel de gestion des communications établies par les entités H.323 fournit les services :

- Translation d'adresses (alias, email, E.164...) ;
- Contrôle des droits des utilisateurs (rejet éventuel d'appel) ;
- Gestion de la bande passante ;
- Gestion de la passerelle H.323 (management de la zone) ;
- Journalisation des appels.

Enfin, le MCU (*Multipoint Control Unit*) aussi optionnel gère l'établissement, le mixage et la diffusion des conférences (contrôle des liaisons multipoints en multicast).

III.2.1.2. Pile protocolaire H.323 :

La figure I.7 décrit la pile protocolaire H.323. La voix est transportée en mode datagramme sur UDP tandis que la signalisation est transportée en mode connecté sur TCP. Les spécifications H.323 correspondent aux niveaux session et supérieurs du modèle de

référence, cette approche assure l'interopérabilité des systèmes quel que soit le réseau de transport utilisé [6].

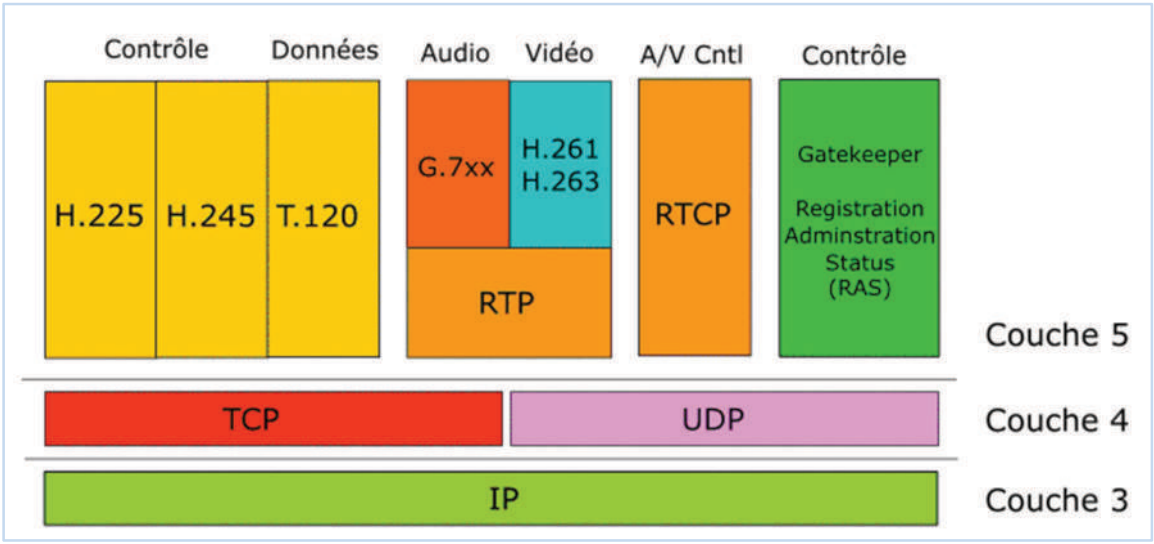


Figure I.7 : La pile protocolaire H.323

Exemple de scénario d'une communication complète :

Une communication complète inclut l'ensemble des messages envoyés pour initier, établir et terminer une communication entre deux correspondants.

On considère une zone H.323 (il y a donc présence d'un gatekeeper pour le contrôle d'admission des terminaux). On suppose que la signalisation se fait en mode direct (seuls les messages de signalisation RAS sont routés vers le gatekeeper). On suppose également que ces terminaux se sont préalablement enregistrés auprès du gatekeeper et qu'ils dépendent tous deux d'un même gatekeeper (la localisation n'est donc pas à entreprendre).

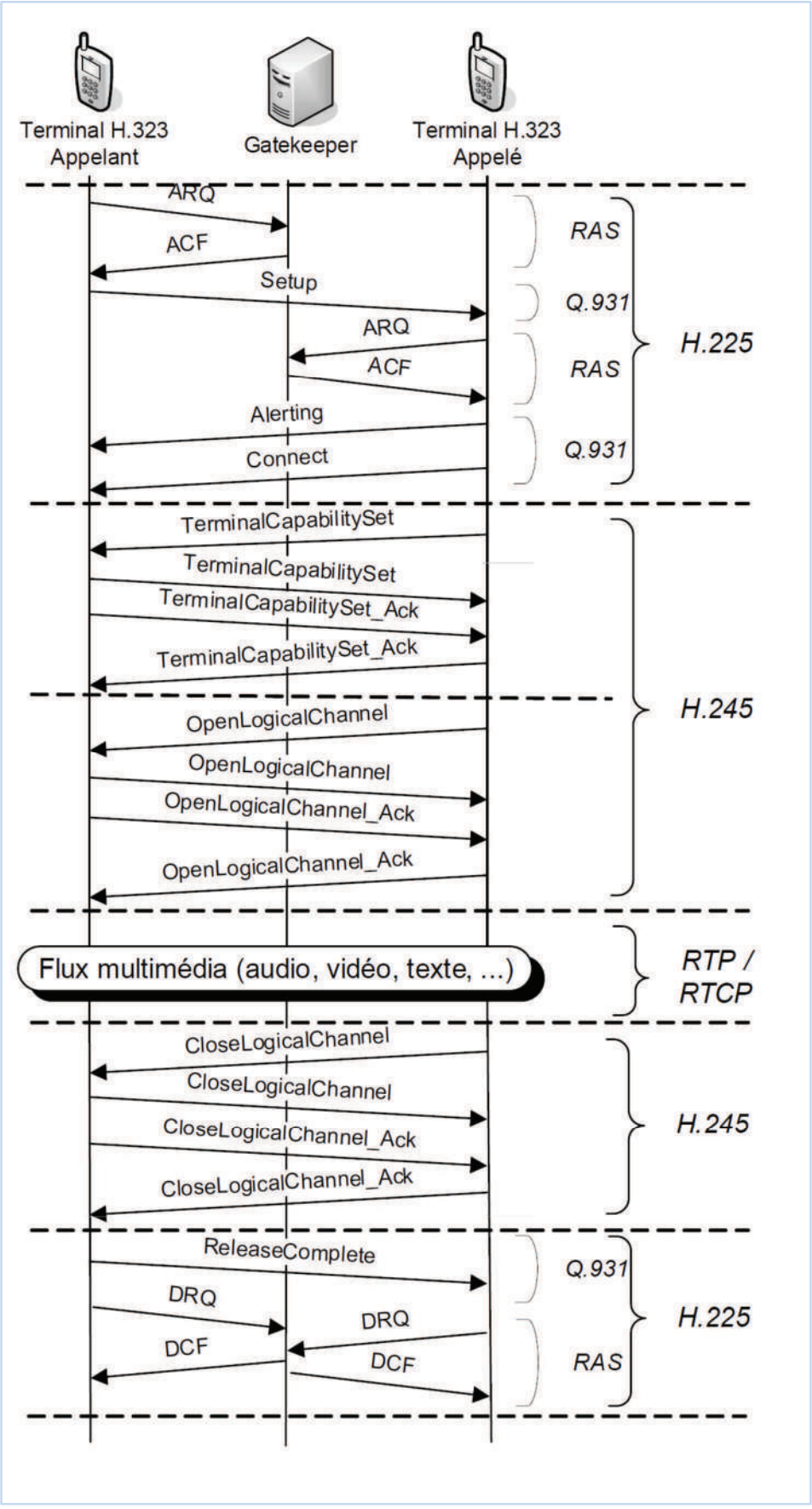


Figure I.8 : Scénario complet d'une communication H.323

La figure I.8 illustre un exemple de communication complète entre deux terminaux H.323. Les étapes successives qui caractérisent cet échange sont les suivantes :

1. Connexion (protocole H.225.0). Avant de contacter son correspondant, l'appelant s'assure d'être autorisé à émettre cet appel auprès du gatekeeper (RAS), puis envoie sa requête au terminal appelé (Q.931). Celui-ci s'assure à son tour auprès du gatekeeper d'avoir le droit d'effectuer cette communication (RAS). Pour les deux correspondants, on considère le cas où l'appel est autorisé pour pouvoir poursuivre. Dès que le terminal appelé reçoit la permission, il envoie des messages alertant l'appelant de sa disponibilité (Q.931) et lui confirmant que la connexion peut être débuté (Q.931).
2. Négociation des paramètres et ouverture du canal de contrôle (protocole H.245.0). Commence un échange réciproque de messages pour déterminer les paramètres à mettre en place lors de la communication (H.245). À ce stade, il serait possible de négocier, par exemple, le choix des flux désirés (voix, vidéo ou les deux), le choix des codecs ainsi que les débits souhaités. Le canal de signalisation de contrôle est ainsi ouvert.
3. Début de la communication (RTP/RTCP). La communication audio et vidéo peut commencer en laissant transiter les médias.
4. Fermeture des canaux de signalisation. Lorsqu'un correspondant met fin à l'appel (en raccrochant son combiné, par exemple), la communication est clôturée par un message de signalisation fermant le canal Q.931. Ensuite, chacun des intervenants indique au gatekeeper la terminaison de l'appel, ce qui permet à ce dernier de déterminer la durée de l'appel à des fins de statistiques, journalisation ou facturation ou d'allouer la bande passante libérée à d'autres appels [4].

III.2.1.3. Avantages et inconvénients :

Les principaux bénéfices qu'apporte la norme H.323 sont les suivants :

- ✓ **Codec standard :** H.323 établit des standards pour la compression et la décompression des flux audio et vidéo. Ceci assure que des équipements provenant de fabricants différents ont une base commune de dialogue.
- ✓ **Interopérabilité :** Les utilisateurs veulent pouvoir dialoguer sans avoir à se soucier de la compatibilité du terminal destinataire. En plus d'assurer que le destinataire est en mesure de décompresser l'information, H.323 établit des méthodes communes d'établissement et de contrôle d'appel.
- ✓ **Indépendance vis à vis du réseau :** H.323 est conçu pour fonctionner sur tout type d'architecture réseau. Comme les technologies évoluent et les techniques de gestion de

la bande passante s'améliorent, les solutions basées sur H.323 seront capables de bénéficier de ces améliorations futures.

- ✓ **Indépendance vis à vis des plates-formes et des applications :** H.323 n'est lié à aucun équipement ou système d'exploitation.
- ✓ **Support multipoint :** H.323 supporte des conférences entre trois points terminaux ou plus sans nécessiter de la présence d'une unité de contrôle spécialisée.
- ✓ **Gestion de la bande passante :** Le trafic audio et vidéo est un grand consommateur de ressources réseau. Afin d'éviter que ces flux ne congestionnent le réseau, H.323 permet une gestion de la bande passante à disposition. En particulier, le gestionnaire du réseau peut limiter le nombre simultané de connexions H.323 sur son réseau ou limiter la largeur de bande à disposition de chaque connexion. De telles limites permettent de garantir que le trafic important ne soit pas interrompu.
- ✓ **Support multicast :** H.323 supporte le multicast dans les conférences multipoints. Multicast envoie chaque paquet vers un sous-ensemble des destinataires sans réplication, permettant une utilisation optimale du réseau.

A l'heure actuelle, le standard de fait pour les systèmes de téléphonie sur IP est la norme H.323 de l'UIT. Indispensable pour permettre un minimum l'interopérabilité entre équipements de fournisseurs différents, ce standard présente toutefois les inconvénients suivants :

- ✓ Protocole complexe, créé initialement pour les conférences multimédia et qui incorpore des mécanismes superflus dans un contexte purement téléphonique. Ceci a notamment des incidences au niveau des terminaux H.323 (téléphones IP, par exemple) qui nécessitent de ce fait une capacité mémoire et un traitement sans incidence au niveau de leur coût.
- ✓ Comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité ou de plus petit dénominateur commun (dans le choix du codec, par exemple). D'autre part, comme le seul codec obligatoire est le codec G.711 (64 Kbits/s) et que le support des autres codecs plus efficaces est optionnel, l'interopérabilité entre produits provenant de constructeurs différents ne signifie pas qu'ils feront un usage optimal de la bande passante. En effet, dans le cas où les codecs à bas débits sont différents, le transport de la voix se fera à 64 Kbits/s, ce qui, en terme de bande passante, ne présente guère d'avantages par rapport à un système téléphonique classique [3].

III.2.2. Le protocole SIP de l'IETF :

Actuellement la plupart des solutions développées utilisent la signalisation H.323 d'origine UIT-T. Développé au sein du groupe de travail MMUSIC (*Multiparty Multimedia SessIon Control*) de l'IETF, le protocole SIP (*Session Initiation Protocol*) beaucoup simple que H.323 pourrait, à terme, remplacer H.323. Les messages SIP sont au format texte, ce qui confère au protocole une grande évolutivité. La figure I.9 illustre l'architecture SIP.

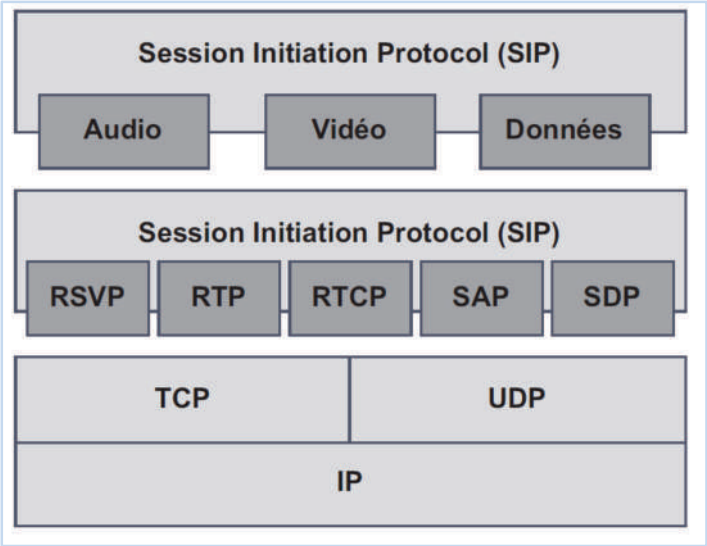


Figure I.9: Architecture protocolaire SIP.

RSVP : Réservation des ressources réseaux sur IP avec une excellente qualité de service.
RTP : Transport des informations en temps réel avec une excellente QoS.
RTCP : Assure le contrôle de flux des données multimédia.
SDP (*Session Description Protocol*) : Décrit les sessions multimédia [8].

À l'instar d'H.323, SIP s'appuie sur les protocoles temps réel (RTP et RTCP), il peut éventuellement utiliser RSVP pour obtenir une certaine qualité de service sur le réseau. Le protocole SAP (*Session Announcement Protocol*) informe de l'ouverture d'une session multimédia en mode multicast ou non et le protocole SDP (*Session Description Protocol*) fournit la description des sessions multimédia.

III.2.2.1. Clients et serveurs SIP :

Basé sur le modèle client-serveur, SIP distingue 2 types d'agent : les clients et les serveurs.

Les clients ou UAC (*User Agent Client*) sont les équipements à l'origine des appels SIP (téléphone IP) ou des passerelles voix. Les passerelles voix SIP ont les mêmes fonctionnalités que les passerelles H323.

Les agents serveurs (UAS, *User Agent Server*) sont des équipements classiques (Serveur NT...) qui regroupent les services offerts par SIP. Ce sont :

- les serveurs d'enregistrement utilisés pour la localisation des utilisateurs (Registar). Les serveurs d'enregistrement contiennent toutes les caractéristiques des agents SIP autres que les passerelles ;
- les serveurs de délégation (Proxy Server) qui gèrent les clients SIP, reçoivent et transmettent les requêtes au serveur suivant (next-hop server). Le SIP Proxy a un rôle similaire au Gatekeeper d'H.323. Un SIP Proxy peut interroger un SIP Registar ou un DNS pour acquérir les informations d'acheminement, de la signalisation et des communications ;
- les serveurs de redirection (Redirect Server) qui sur requête transmettent l'adresse du « nexthop server » à l'agent client.

III.2.2.2. Messages SIP :

Les messages SIP sont de deux types, les requêtes et les réponses. Les primitives de requêtes sont :

- ✓ REGISTER, ce message est émis par un agent pour informer un serveur SIP Registar sur sa localisation. Le client fournit une adresse du type Nom@Domaine ;
- ✓ INVITE, message d'ouverture de session, émis par un UAC. Ce message peut être transmis directement à l'agent appelé ou à un serveur Proxy pour l'acheminement ;
- ✓ BYE, émis par tout agent client pour mettre fin à une session en cours ;
- ✓ CANCEL annule une session, ne peut être utilisé que pendant la phase d'ouverture ;
- ✓ ACK acquitte un message INVITE et établit la session d'échange ;
- ✓ OPTIONS, message d'obtention des capacités (caractéristiques) d'un terminal, similaire à H.245.

Les messages de réponse sont aussi au nombre de 6, ce sont :

- ✓ INFORMATIONAL, simple message de service ;
- ✓ SUCCESSFULL, message indiquant que l'action a été menée à bien (succès)...
- ✓ REDIRECTION, une autre action doit être conduite pour valider la requête ;
- ✓ CLIENT FAILURE, message signalant une erreur de syntaxe, la requête ne peut être traitée ;
- ✓ SERVER FAILURE, message signalant une erreur sur un agent serveur,

✓ GLOBAL FAILURE, erreur générale, la requête ne peut être traitée par aucun serveur.

Les messages de réponse comportent un code d'état, dont les principaux sont listés dans le tableau I.1.

Type de message	code d'état	appellation	commentaires éventuels
INFORMATIONAL	100 180 188	Trying Ringing Queued	Appel pris en compte Retour de sonnerie Mise en attente
SUCCESSFUL	200	OK	Signale que l'appelé a décroché
REDIRECTION	301 305	Moved permanently Use proxy server	Rediriger l'appel vers cette nouvelle position Transiter par ce proxy
CLIENT FAILURE	400 401 420 483 485	Bad request Unauthorised Bad extension Loop Detected Address incomplete	Emis quand un serveur reçoit une requête pour lui-même
SERVER FAILURE	500 504	Interna Server Error Gateway timeout	
GLOBAL FAILURE	600 603	Busy Decline	Emis quand l'appelé ne désire pas établir de communication

Tableau I.1 : Codes d'état des messages de réponse SIP

III.2.2.3. Exemple de communication SIP :

La figure I.10 illustre un appel SIP vers un utilisateur qui s'est déplacé. Le client appelant envoie une requête INVITE au serveur proxy auquel il est relié. Ce message contient l'adresse connue du destinataire. Le Proxy Server interroge le Location Server (DNS, LDAP ou autre) qui lui fournit la nouvelle adresse, le Proxy redirige la requête vers la nouvelle adresse de l'appelé (INVITE). Le poste appelé sonne et le poste appelant reçoit un message de retour de sonnerie (SIP 180). L'appelé décroche signifiant ainsi son acceptation de la communication, le système émet alors un message SIP 200 (OK). L'appelant acquitte le message d'acceptation.

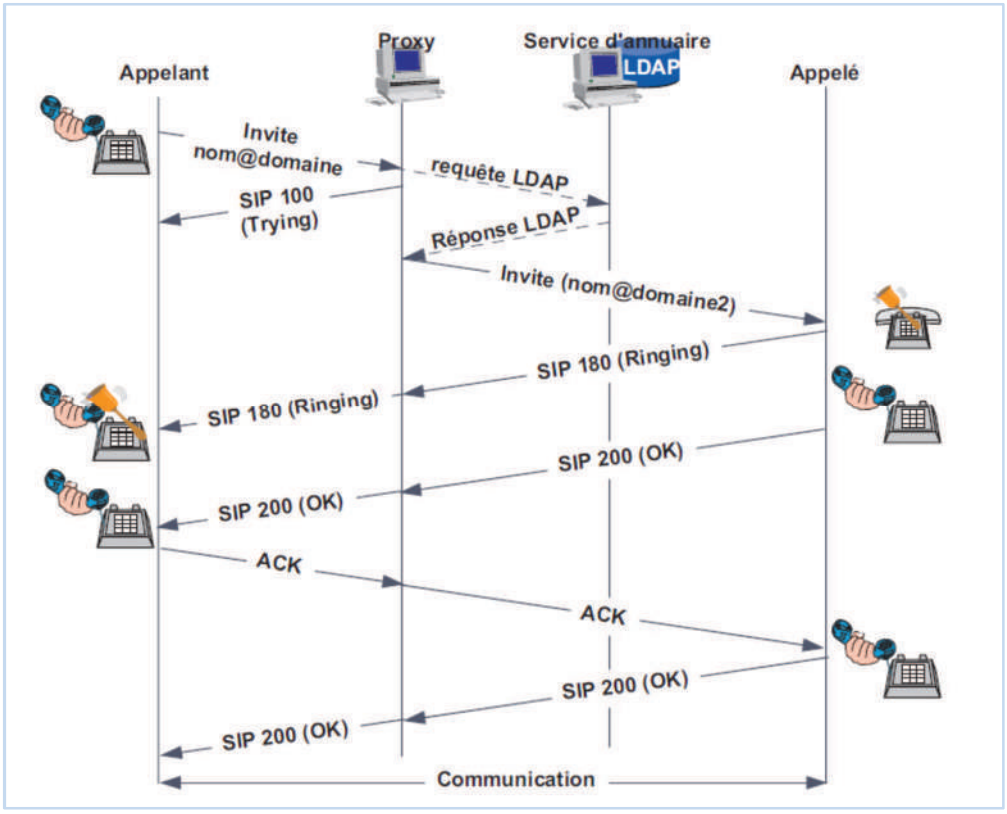


Figure I.10 : Ouverture d'une communication en mode proxy

Sans Server Proxy, l'appelant se serait adressé à un Redirect Server, celui-ci consulte le Location Server et envoie à l'appelant la nouvelle adresse dans un message SIP 302 (*moved temporarily*) ou SIP 301 (*moved permanently*). L'appelant émet alors une requête INVITE directement à l'appelé [6].

III.2.2.4. Avantages et inconvénients de SIP :

Ouvert, standard, simple et flexible sont les principales atouts du protocole SIP, voilà en détails ces différents avantages :

- **Ouvert :** les protocoles et les documents officiels sont détaillés et accessibles à tous en téléchargement.
- **Standard :** l'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP.
- **Simple :** SIP est simple et très similaire à http.
- **Flexible :** SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.).

Par contre une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic

superflu sur le réseau. Un autre inconvénient est le faible nombre d'utilisateurs : SIP est encore peu connu et utilisé par le grand public, n'ayant pas atteint une masse critique, il ne bénéficie pas de l'effet réseau.

III.2.3. Le protocole MGCP:

Un autre protocole entre en compétition, le MGCP (*Media Gateway Control Protocol*) encore plus simple, il centralise « l'intelligence » et peut donc être intégré à des terminaux peu intelligents (clients légers).

MGCP définit plusieurs entités. La passerelle de signalisation (SG, *Signalling Gateway*) assure la mise en relation de la signalisation du réseau téléphonique traditionnel, généralement SS7, avec la signalisation utilisée dans le réseau en mode paquet. La passerelle média (MG, *Media Gateway*) réalise la paquétisation des signaux voix. Enfin, le contrôleur de passerelle média (MGC, *Media Gateway Controller*), cœur du système, pilote les différentes passerelles [6].

III.2.3.1. Architecture de MGCP :

MGCP est un système centralisé composé :

- d'un contrôleur, qui rappelle par sa fonction un ancien standard téléphonique, appelé Media Gateway Controller, MGC ou plus familièrement soft-switch ;
- d'au moins une passerelle multimédia (MG, Media Gateway), qui se charge de convertir les échantillons de voix et vidéo entre circuits téléphoniques et paquets réseau ;
- d'au moins une passerelle de signalisation (Signaling gateway, SG).

Le contrôleur (MGC) utilise MGCP pour dire à la passerelle multimédia (MG) :

- ✓ Quels évènements doivent remonter au contrôleur ;
- ✓ Comment les terminaux (les téléphones) doivent être mis en relation ;
- ✓ Quels signaux doivent être joués sur les terminaux.

MGCP permet également au standard d'interroger l'état actuel des terminaux sur la passerelle multimédia. La passerelle multimédia utilise MGCP pour signaler des évènements comme le raccrochage ou les numéros composés au standard. La passerelle de signalisation se trouve souvent sur le même équipement physique que la passerelle multimédia, mais ce n'est pas une obligation. Le contrôleur n'utilise pas MGCP pour contrôler la passerelle de signalisation ; on utilise plutôt les protocoles SIGTRAN pour transporter la signalisation entre la passerelle de signalisation et le contrôleur.

III.2.3.2. Avantages et inconvénients :

Avantages :

Les avantages du protocole MGCP sont : le réseau peut être configuré de manière centralisée, et les passerelles multimédias sont des éléments simples.

Le Call Agent a un rôle central de gestion des passerelles multimédias. Il offre ainsi le moyen de mettre à jour des fonctionnalités sur les passerelles, sans avoir besoin d'intervenir sur chacune d'elles. Le réseau devient ainsi facilement administrable à distance.

La création de nouveaux services est simplifiée, puisque leur implémentation et leur gestion sont automatiquement propagées. À l'inverse, le Call Agent peut imposer un traitement personnalisé selon des configurations paramétrables qui supportent le nomadisme des utilisateurs. Par exemple, un utilisateur peut avoir la possibilité de personnaliser sa sonnerie d'appel dans une base de données cliente, à laquelle accède le Call Agent. Lorsque l'utilisateur se déplace et se connecte sur un autre réseau, le Call Agent peut détecter les préférences de l'utilisateur dans la base de données, de façon à lui conserver la sonnerie qu'il avait configurée.

Dans la mesure où elles n'assument pas la logique de contrôle des appels, mais seulement les traitements de bas niveau, les passerelles sont des entités relativement simples et peu coûteuses. Si l'une d'elles tombe en panne, il est facile de la remplacer car il n'est pas nécessaire de reprogrammer toutes les configurations de la passerelle décrivant son état avant la panne : c'est le Call Agent qui se charge de configurer dynamiquement la passerelle.

Inconvénients :

MGCP propose une architecture centralisée chargée du contrôle dans le réseau. Par conséquent, le réseau est dépendant de cette entité centrale, qui constitue un point de vulnérabilité.

En cas de dysfonctionnement de ce serveur, le réseau tout entier devient défaillant puisque aucun contrôle ne peut plus y être effectué. Néanmoins, le protocole MGCP a prévu des procédures pour que, en cas de panne, une passerelle puisse basculer d'un contrôleur vers un autre. Un autre inconvénient de MGCP est qu'il impose globalement une plus grande quantité de messages de signalisation. Les terminaux qui l'implémentent ne se connectent jamais directement entre eux, mais doivent impérativement au préalable en demander l'autorisation au centre de contrôle.

Ce mode de fonctionnement se distingue nettement de ceux des protocoles H.323 et SIP, qui permettent aux terminaux de communiquer entre eux sans faire intervenir d'entité

tierce. Globalement, les protocoles H.323 et SIP assurent le contrôle des appels eux-mêmes, tandis que le protocole MGCP assure le contrôle des entités du réseau [4].

IV. Avantages et inconvénients de la VoIP :

IV.1 Avantages :

La VoIP offre de nombreuses nouvelles possibilités aux opérateurs et utilisateurs qui bénéficient d'un réseau basé sur IP. Les avantages les plus marqués sont les suivants :

- **Réduction de coût :**

La VoIP permet la réduction de nombreux coûts tels que les coûts de communication, de câblage, de maintenance, de supervision de système…

- **Flexibilité :**

La VoIP peut selon ses besoins du moment augmenter ou réduire le nombre des postes en services, ajouter ou supprimer des fonctionnalités.

- **Evolutivité :**

La technologie de VoIP trouve ses racines dans deux évolutions structurelles : l'une portant sur les moyens de transport de la voix, l'autre sur le standard lui-même.

- **Standard ouvert :**

La VoIP n'est plus uniquement H323, mais un usage multi-protocoles selon les besoins de services nécessaires. Par exemple, H323 fonctionne en mode égale à égale alors que MGCP fonctionne en mode centralisé. Ces différences de conception offrent immédiatement une différence dans l'exploitation des terminaisons considérées.

IV.2 Inconvénients :

Les points faibles de la voix sur IP sont :

- **Fiabilité et qualité sonore :**

Un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale. En effet, des désagréments tels la qualité de la reproduction de la voix du correspondant ainsi que le délai entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être extrêmement problématiques. De plus, il se peut que des morceaux de la conversation manquent (des paquets perdus pendant le transfert) sans être en mesure de savoir si des paquets ont été perdus et à quel moment.

- **Dépendance de l'infrastructure technologique et support administratif exigent :**

Les centres de relations IP peuvent être particulièrement vulnérables en cas d'improductivité de l'infrastructure. Par exemple, si la base de données n'est pas disponible, les centres ne peuvent tout simplement pas recevoir d'appels. La convergence de la voix et des données dans un seul système signifie que la stabilité du système devient plus importante que jamais et l'organisation doit être préparée à travailler avec efficience ou à encourir les conséquences.

- **Vol :**

Les attaquants qui parviennent à accéder à un serveur VoIP peuvent également accéder aux messages vocaux stockés et au même au service téléphonique pour écouter des conversations ou effectuer des appels gratuits aux noms d'autres comptes.

- **Attaque de virus :**

Si un serveur VoIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au réseau téléphonique. Le virus peut également infecter d'autres ordinateurs connectés au système.

V. Conclusion :

La voix sur IP est une technologie qui utilise les réseaux informatique comme support de communication, elle est basée sur des standards ouverts, chaque standard possède ses propres caractéristiques pour garantir une bonne qualité de service en tenant compte des contraintes temporelles, le facteur le plus important lors de transport de la voix.

La VoIP est une bonne solution en matière de flexibilité, évolutivité et de réduction de coût, alors comme on a pu le voir la voix sur IP est la technologie la plus rentable pour effectuer des conversations. Actuellement, il est évident que la VoIP va continuer à évoluer.



Chapitre 2 :

Description des différents modèles de simulations réalisées



I. Introduction :

Une simulation consiste à simuler par un programme informatique un réseau, et un scénario d'utilisation de ce réseau afin de recueillir des statistiques permettant d'évaluer le fonctionnement d'un mécanisme donné. L'exécution du programme de simulation est donc enregistrée dans une trace, qui peut être analysée (soit en cours de simulation, soit à posteriori).

La simulation est l'un des outils classiquement mis en œuvre lorsque l'on veut analyser les performances quantitatives d'un système. Cet outil complète celui de la modélisation (qui ne permet pas en général de bien représenter les détails de fonctionnement d'un système complexe) et celui du test pratique (qui demande une mise en œuvre lourde, et nécessite la réalisation effective des éléments du système).

La simulation quantitative permet de représenter un niveau de détails variable, et d'évaluer les performances d'un système ou d'un protocole avant que ce dernier ne soit réellement construit ou effectivement déployé dans un réseau. Par contre, comme le problème réel est «modélisé» par un programme, il est souvent nécessaire d'effectuer des simplifications du comportement réel qui peuvent rendre les résultats concernant le système simulé obtenus non représentatifs du comportement du système réel. Tout l'art du simulateur consiste à modéliser de façon simple mais représentative un système complexe. [12]

Il existe plusieurs logiciels de simulation des réseaux, le tableau II.1 présente quelques simulateurs.

NS3	GNS3	Boson Netsim	Packet Tracer	Opnet Modeler
				

Tableau II.1 : Exemple de simulateurs réseau

L'OPNET est le simulateur choisi dans notre projet pour modéliser des réseaux de type Ethernet, Wi-Fi et WiMAX et pour évaluer la transmission de la voix sur IP dans ces réseau en étudiant l'influence de la distance séparant deux utilisateurs, le nombre de postes

communicants et le type de codec utilisé sur la qualité de service QoS de la VoIP, en considérant quelques paramètres y compris la gigue, la valeur MOS , le délai de bout en bout, et la perte des paquets.

Cette étude est de réaliser trois projets basés sur des différents types de réseaux (Ethernet, Wi-Fi et WiMAX), et chaque projet contient plusieurs scénarios permettant de suivre la qualité de service en fonction des changements de plusieurs facteurs.

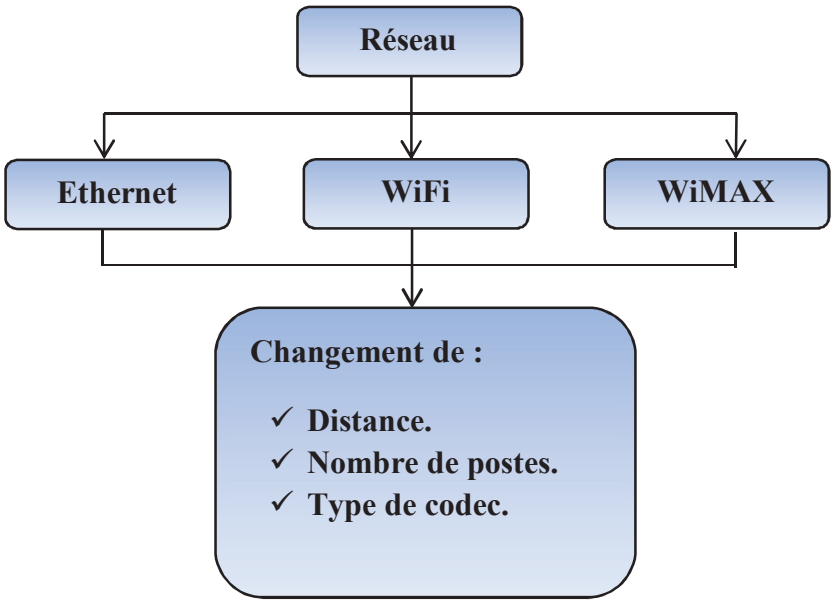


Figure II.1 : Projets de simulation

I.1. Facteurs de dégradation de la qualité de service (QoS) de la VoIP :

Les réseaux de nouvelle génération doivent être capables de prendre en charge la qualité de service de chaque application transitant sur le même réseau. Il est indispensable d'assurer une bonne qualité de service pour fournir aux utilisateurs la même fiabilité et qualité que le réseau à commutation de circuit RTC. La qualité de la VoIP est principalement affectée par : la latence, la gigue et la perte de paquets.

a. Latence (délai de bout en bout) :

La latence désigne le délai de transmission du signal de bout en bout. Le délai est l'intervalle de temps dans lequel se déplacent des paquets d'un nœud à un autre nœud. Il est provoqué par le temps d'extrémité pour créer des paquets, par le temps nécessaire pour

remplir les données en paquets, ou le temps d'organiser des données numériques sur une liaison physique. VoIP est très sensible au retard; par conséquent, elle doit être contrôlée et gérée. Il est inefficace d'attendre que tous les paquets arrivent dans un ordre organisé, par conséquent, certains paquets peuvent être supprimés s'ils ne sont pas arrivés à temps et cela peut provoquer de courtes périodes de silence dans le flux audio et provoquant une mauvaise qualité de la VoIP. Idéalement, la contrainte de délai pour paquets VoIP n'est pas supérieure à 80 ms [9].

b. Gigue :

La gigue est un paramètre également très important de la parole téléphonique. Prenons un exemple. Si les délais de transit de tous les paquets transportant une conversation téléphonique sont égaux à 100 ms, la moyenne est également de 100 ms. Si maintenant le délai de transit d'un paquet sur deux est de 120 ms et d'un paquet sur deux de 80 ms, la moyenne est toujours de 100 ms mais la gigue a augmenté, elle est passée de 0 à 20 ms. Tant que la gigue reste acceptable, il est possible de resynchroniser les paquets. Mais lorsque la gigue augmente trop et dépasse le temps maximal de latence, l'application commence à se dégrader [10].

c. Perte de paquets :

La perte de paquets présente les paquets supprimés afin de gérer le trafic réseau. Il est inévitable dans les réseaux IP et se produit pour diverses raisons. Par exemple, elle se produit lorsque les routeurs ou commutateurs fonctionnent au-delà de la capacité ou de la file d'attente des tampons sur les flux. Les paquets perdus en VoIP sont traités comme du bruit. Bien que certaines applications peuvent tolérer la perte de paquets car elles peuvent attendre que les paquets sont retransmis, certaines applications sensibles au temps ne sont pas tolérantes à la perte de paquets, tels que les applications téléphones à texte (TTY). La perte de paquets en VoIP doit être gérée ou contrôlée car elle effectue la distorsion du signal vocal [9].

I.2. Note d'opinion moyenne (MOS):

Dans la communication vocale, la qualité de service est mesurée sur la base de MOS qui fournit des statistiques de qualité de la voix. Pour déterminer la MOS, la qualité de voix est testée et évaluée après avoir traversée le codec et le nombre spécifique des taux d'auditeurs de

qualité de voix. La gamme de MOS est de 1 (non recommandée) à 5 (très satisfaite) et 4 est considéré comme une valeur convenable. [11]

valeur MOS	satisfaction des utilisateurs
1 - 2.6	non recommandée
2.6 – 3.1	presque tous les utilisateurs insatisfaits
3.1- 3.6	beaucoup d'utilisateurs insatisfaits
3.6 – 4.0	certains utilisateurs insatisfaits
4.0 – 4.3	Satisfaite
4.3 – 5	très satisfaite

Tableau II.2 : Comparaison des satisfactions des utilisateurs en fonction de MOS

II. Présentation du simulateur réseau OPNET Modeler 14.5 :

Commercialisé en 1986 par Alain Cohen (franco-Américain), OPNET est une offre de logiciels de modélisation et de simulation de réseaux s'adressant à différents publics :

- OPNET Modeler qui s'est imposé dans le monde de la recherche et du développement,
- SP Guru pour les opérateurs,
- IT Guru pour les entreprises.

Son approche orientée objet et son éditeur graphique correspondent bien à la structure des réseaux actuels et de ses composants, ce qui permet de modéliser relativement et intuitivement un système. De nombreux réseaux et technologies sont intégrés, permettant ainsi une modélisation précise des systèmes communicants. [12]

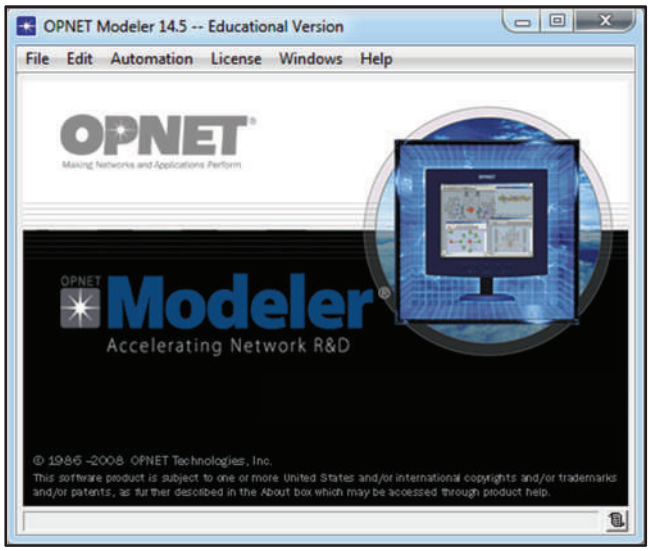


Figure II.2 : OPNET modeler 14.5

OPNET modeler est réputé dans l'industrie pour la modélisation et la simulation des réseaux. Modeler permet de dessiner et d'étudier des réseaux de communications, des équipements, des protocoles et des applications avec facilité et évolutivité. Modeler est utilisé par les entreprises technologiques les plus performantes pour accélérer leurs procédés de recherches et de développements.

L'approche orientée objet associée à des éditeurs graphiques intégrés de Modeler simplifie la composition des réseaux et des équipements. Ceci permet de réaliser facilement une correspondance entre votre système d'informations et votre modèle.

Modeler est basé sur une série d'éditeurs hiérarchisés qui parallélisent la structure du réseau réel, des équipements est des protocoles. [13]

II.1. Interfaces d'OPNET :

Parmi les nombreuses interfaces que propose OPNET au démarrage, nous trouvons :

I.1.1. Project editor (éditeur de projet) :

L'éditeur de projets représente un graphique de la topologie des communications du réseau. Ce dernier est constitué d'objets équipements et liens configurables via des boites de dialogues.

Les méthodes de copier-coller des équipements et des liens à partir des palettes d'objets de l'éditeur permettent de réaliser le réseau. Il est également possible d'utiliser la fonction d'importation rapide de l'ensemble de la configuration. Il est possible d'utiliser la librairie OPNET ou de réaliser une propre palette intégrant des équipements et liens.

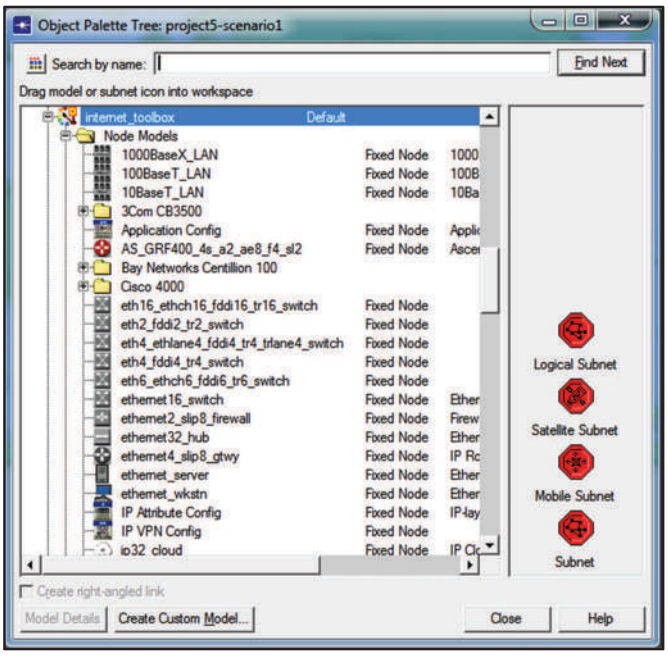


Figure II.3 : Palette d'objet

L'éditeur de projet intègre également un environnement géographique avec des caractéristiques dimensionnelles reprenant les composants utiles pour la modélisation de réseaux câblés ou sans fils.

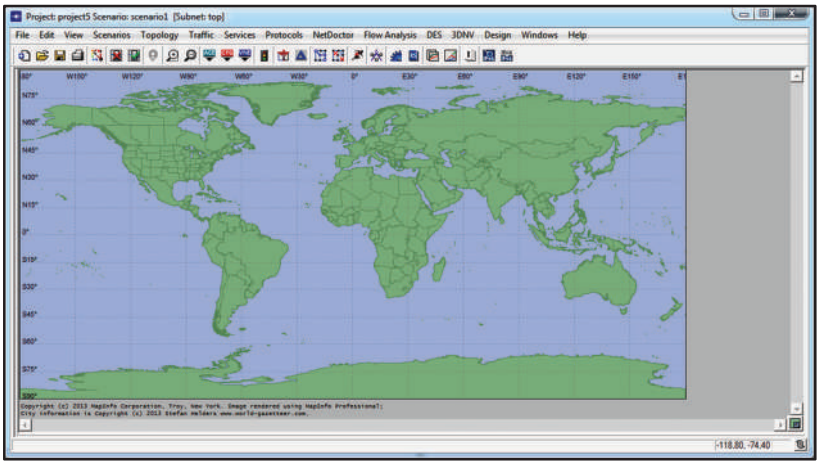


Figure II.4 : Environnement géographique de l'OPNET

L'utilisation du menu Protocoles permet de configurer rapidement les protocoles et d'activer des paramètres particuliers.

Alors Project editor est l'interface principale du logiciel qu'elle permet :

- ✓ d'implanter des modèles issus des bibliothèques OPNET ainsi que des modèles crées par l'utilisateur ;
- ✓ de configurer puis lancer des simulations ;
- ✓ de visualiser les résultats des simulations.

Les principales fonctions de cette interface sont disponibles sous formes d'icônes. Le tableau II.3 montre les plus importantes fonctions.

	ouvrir la palette d'objet
	mise en panne des objets sélectionnés
	remise en marche des objets sélectionnés
	retour au réseau supérieur
	ouvrir le centre de trafic
	lancer la simulation
	visualiser les résultats

Tableau II.3 : les fonctions principales de l'éditeur objet

II.1.2. Network model editor (éditeur de modèle de réseau):

Permet de représenter la topologie d'un réseau de communication constitué de nœuds et de liens par l'intermédiaire de boîtes de dialogues (palettes et glisser/poser). Cette interface tient compte du contexte géographique.

II.1.3. Node model editor (éditeur de modèle de nœud) :

Affiche une représentation modulaire d'un élément de la bibliothèque ou d'un élément créé par l'utilisateur. Chaque module envoie et reçoit des paquets vers d'autres modules. Les modules représentent des applications, des couches protocolaires ou des ressources physiques (buffer, port, …).

II.1.4. Process Model editor (éditeur de modèle de processus):

Offre une représentation d'un module par des machines à états finis ; chaque état est lié à un autre état par des transitions conditionnelles ou non conditionnelles.

II.1.5 . Antenna pattern (modèle d'antenne) :

Cette interface permet de modéliser une antenne pour radiocommunication par son diagramme de rayonnement 3D et ses coordonnées polaires.

II.1.6. Modulation curve (courbe de modulation) :

Donne une visualisation du taux d'erreur binaire BER en fonction du rapport signal sur bruit pour différents types de modulations.

II.1.7. Simulation Sequence (ordre de simulation):

Permet de paramétrer les simulations OPNET en temps et attributs des modèles (types de liens, d'antenne, de services …).

II.1.8. Analysis configuration (configuration d'analyse) :

Configuration du stockage des résultats issus des simulations, sous différentes formes [12].

II.2. Cycle traditionnel d'un projet OPNET :

1. Création d'un projet.
2. Création d'un scénario.
3. Installation des objets dans la zone de travail.
4. Configuration des attributs des objets.
5. Choix de statistiques à collecter.
6. Lancement de la simulation.
7. Visualisation des résultats.

III. Description des projets de simulations réalisés :

Le but général de nos simulations est de suivre la qualité de service de la VoIP dans trois réseaux différents en utilisant l'OPNET. Chaque réseau est modélisé dans un projet contenant 9 scénarios :

- Deux (02) scénarios concernant la distance séparant deux clients VoIP (longue distance et courte distance) ;
- Quatre (04) scénarios concernant le nombre de postes communicants (2, 10, 50, 100) pour le réseau Ethernet et (2, 6, 10,14) pour les deux réseaux sans fil Wi-Fi et WiMAX ;
- Trois (03) scénarios concernant le type de codec utilisé (G.711, G.723 et G729.A).

III.1. Création d'un projet dans l'OPNET :

Pour créer un nouveau projet, on choisit File → New. La fenêtre suivante s'affiche.

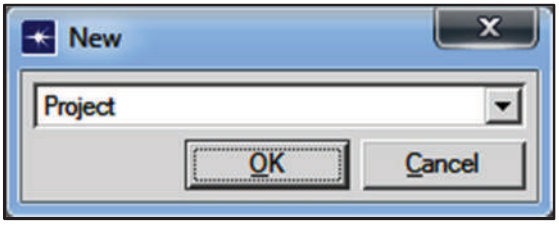


Figure II.5 : Création d'un nouveau projet

On sélectionne « Project » puis on donne un nom au projet et au scénario associé, exemple :

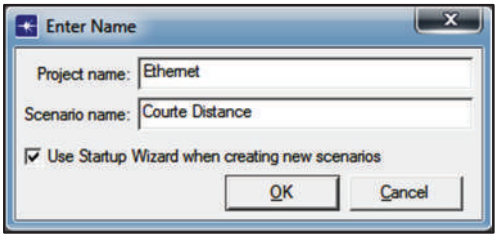


Figure II.6 : Nommage de projet et de scénario

Une fenêtre de topologie initiale s'ouvre, on choisit « *Create empty scenario* » pour créer un nouveau scénario vide.

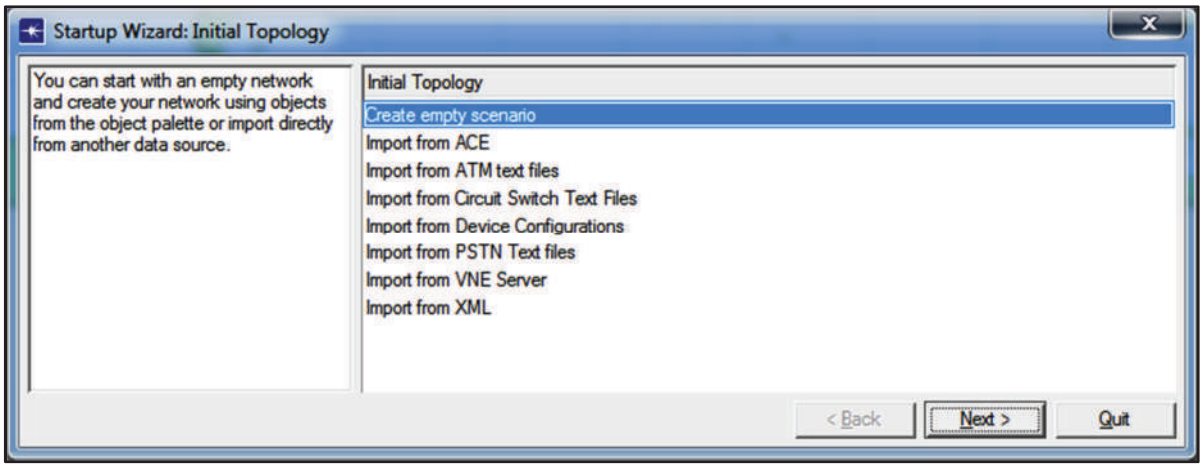


Figure II.7 : Création d'un scénario vide.

On choisit ensuite la taille du réseau : s'il est de l'ordre mondial ou bien s'il s'agit d'un réseau d'entreprise, d'un campus ou tout simplement d'un bureau.

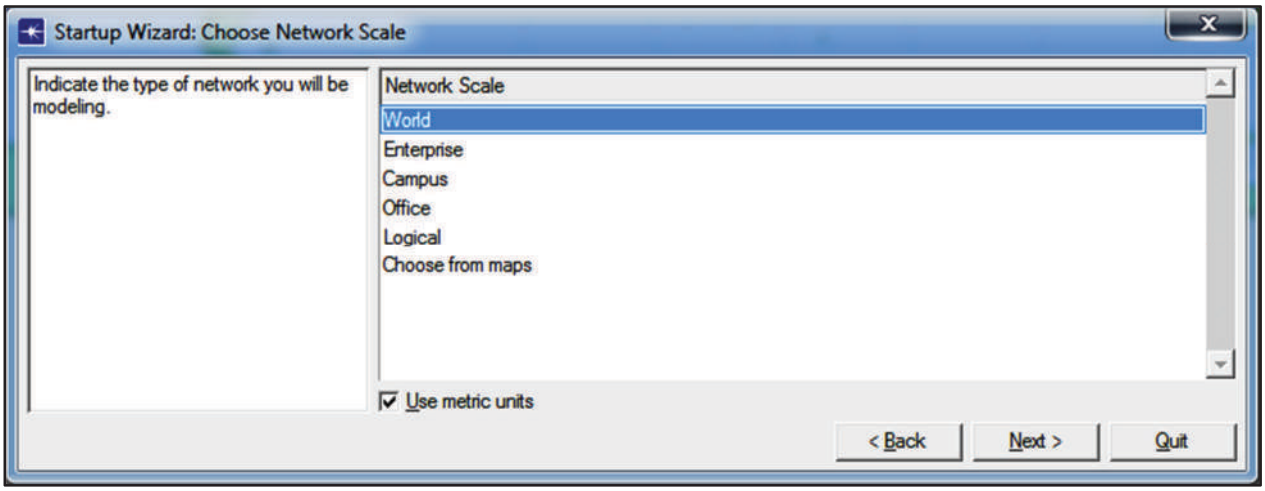


Figure II.8 : Choix de la taille du réseau

Ensuite, une fenêtre pour spécifier la taille s'ouvre, on termine par le choix de la technologie à utiliser. Une dernière fenêtre d'assistant s'ouvre résumant nos choix, on clique alors sur « Finish ». Un espace de travail s'affiche en fonction des paramètres choisis et une fenêtre de palette d'objet s'ouvre.

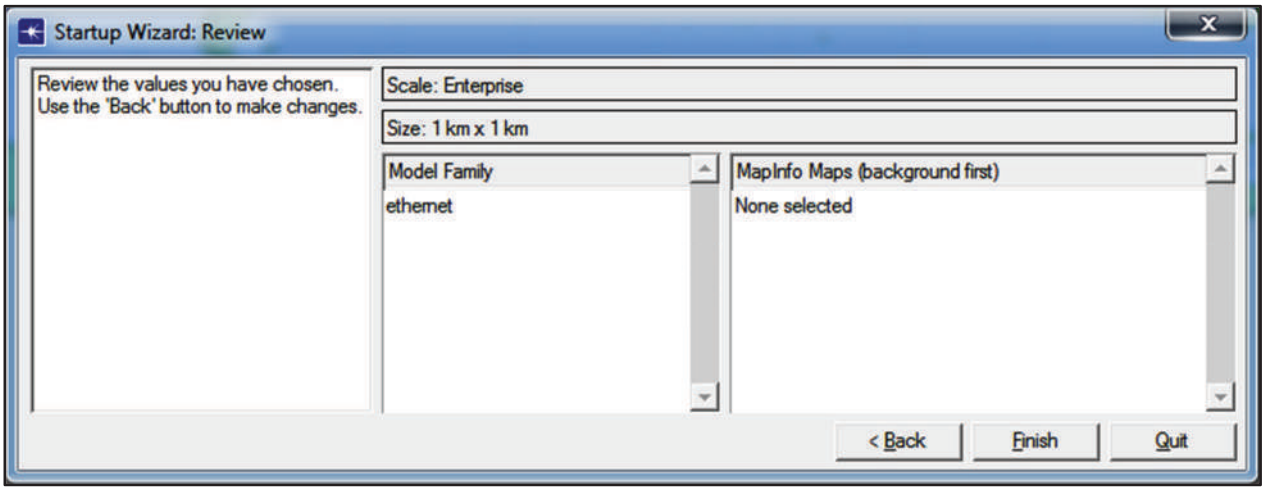


Figure II.9 : Résumé des choix

III.2. Configuration de l'application VoIP et du profil:

Pour une simulation réussite de la voix sur IP dans l'OPNET, les postes de travail doivent être configurés pour supporter les applications VoIP. Alors, il est nécessaire de définir leur comportement dans un profil construit par ces applications.

III.2.1 Configuration de l'application VoIP:

Le composant correspondant à la configuration des applications est tiré de la palette des objets, il permet de définir les applications qu'elles vont être utilisées dans le réseau.



Figure II.10 : Application Definition

Un clic droit sur ce composant puis le choix de « *Edit Attributes* » nous permettent de sélectionner et de modifier les paramètres des applications souhaitées.

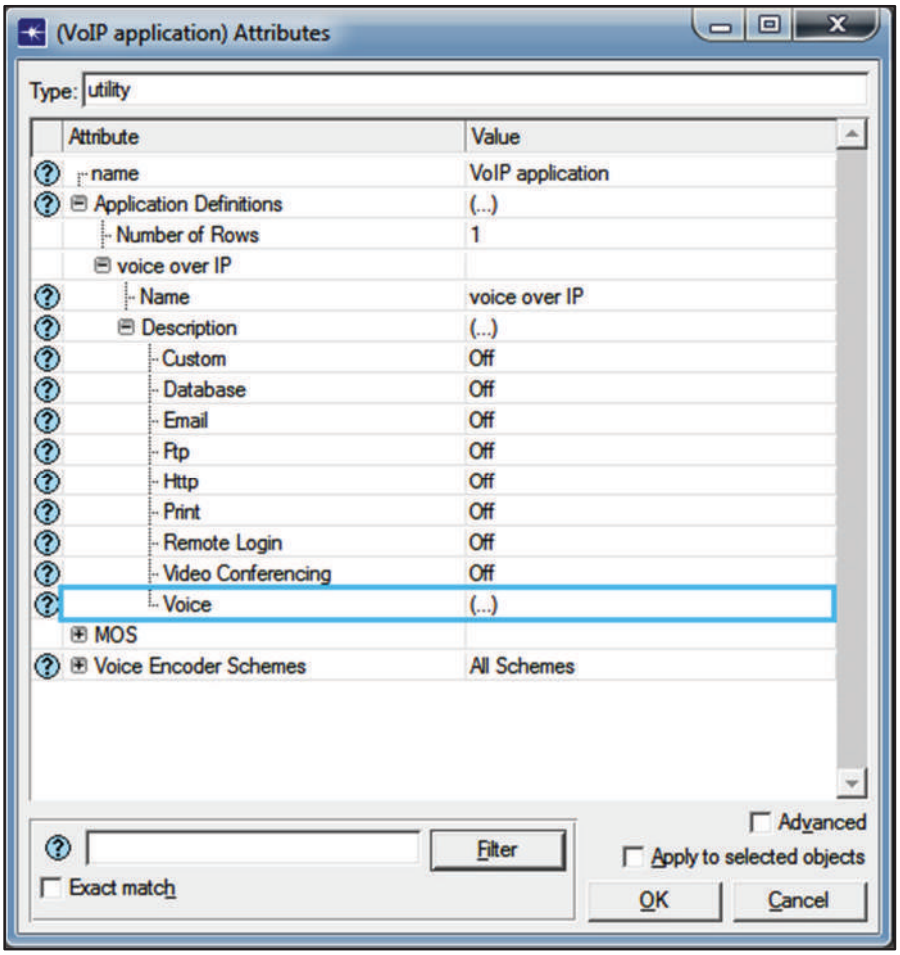


Figure II.11 : Configuration de l'application

Tous les nœuds du réseau sont configurés pour supporter l'application : voix sur IP, les paramètres de cette application sont modifiés par un double clic sur « *voice* ».

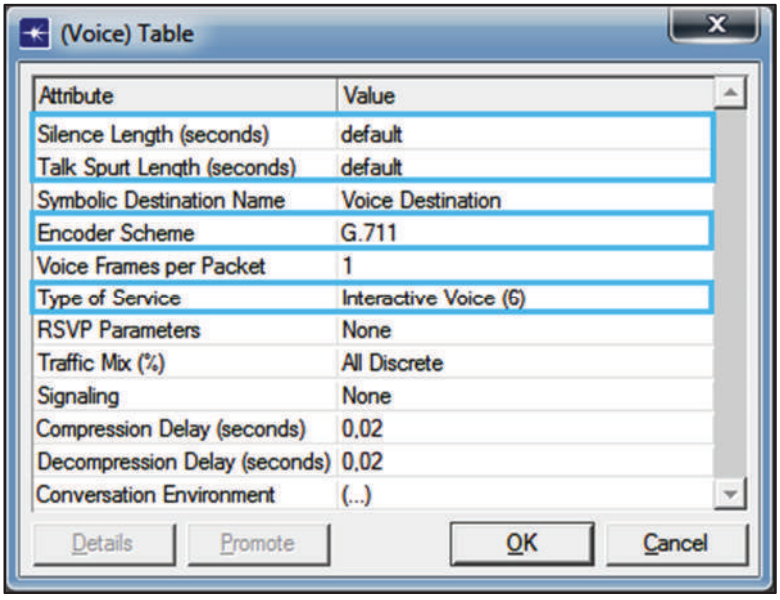


Figure II.12 : Application VoIP

Dans notre cas des applications VoIP, les durés de silence « *Silence Length*» et de conversation « *Talk Spurt Length* » utilisées dans un seul appel ont été laissées avec la distribution exponentielle « par défaut », le type de codec utilisé est G.711 et avec un serveur vocal interactif « *Interactive Voice (6)* » permettant à l'appelant d'être toujours disponible.

Une fois l'application est définie, la définition du profil peut être utilisée pour appliquer le service avec dispositifs de réseau.

III.2.2 Configuration du profil :

La définition du profil est utilisée pour spécifier comment les applications sont utilisées par les utilisateurs, le composant correspondant à sa configuration est le suivant :



Figure II.13 : Profile Definition

Les attributs de ce profil sont modifiés suivant les figure II.14 et II.15.

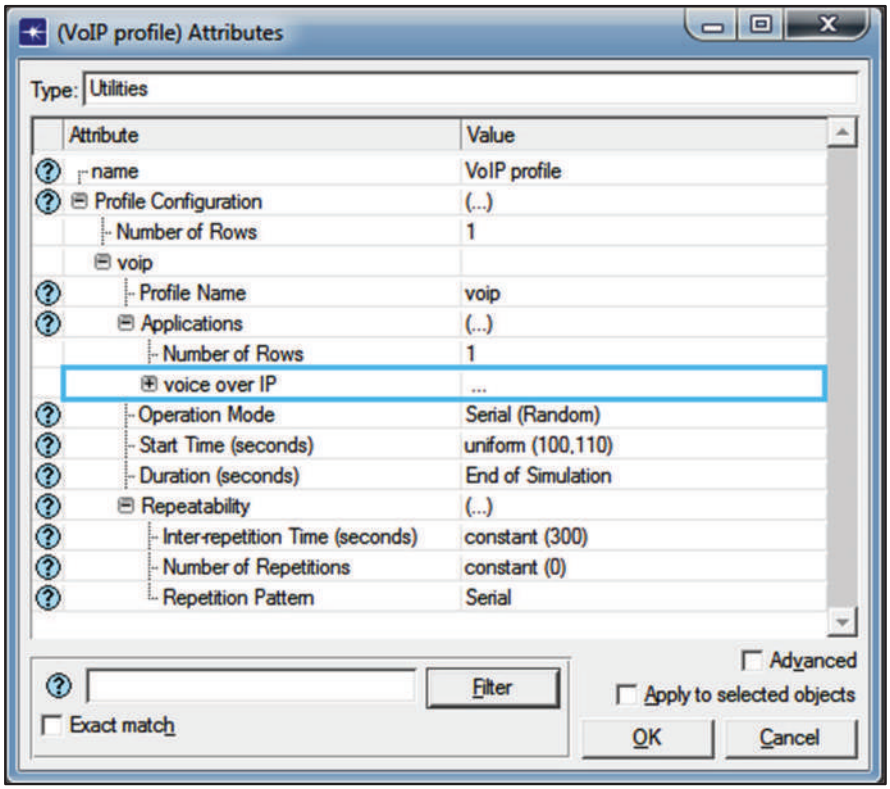


Figure II.14 : Configuration du profil

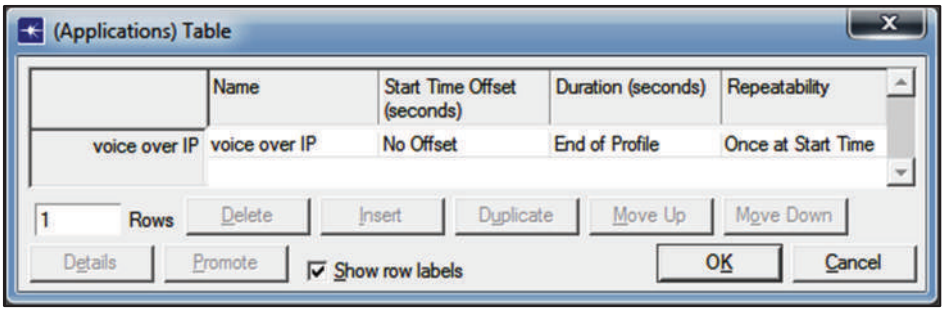


Figure II.15 : Paramètres d'application

- « Start Time Offset » est la durée entre le temps de début de profil et le temps de début de l'application. Pour que le démarrage de l'application soit en même temps que le profil, on règle cette valeur à « *No Offset* ».
- « *Duration* » précise la durée de l'application en quelques secondes, on a met « *End of profile* » pour que l'application puisse prendre fin en même temps que le profil se termine.
- « *Repeatability* » précise le nombre de session d'application dans le profil.

Pour que les postes de travail puissent avoir ce profil, leurs attributs doivent être configurés comme le montre la figure II.16.

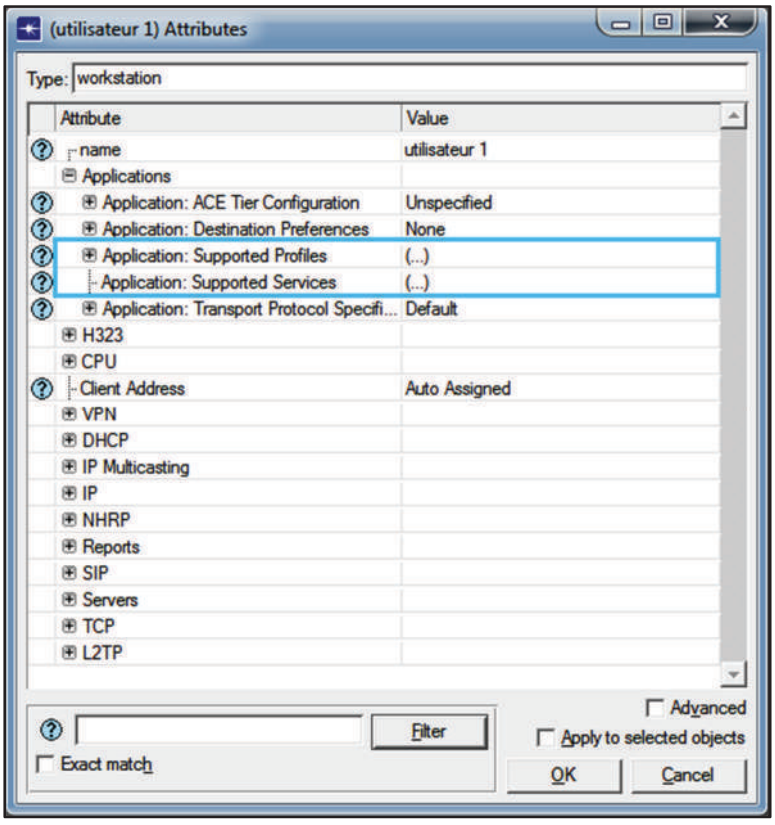


Figure II.16 : Attributs de poste de travail

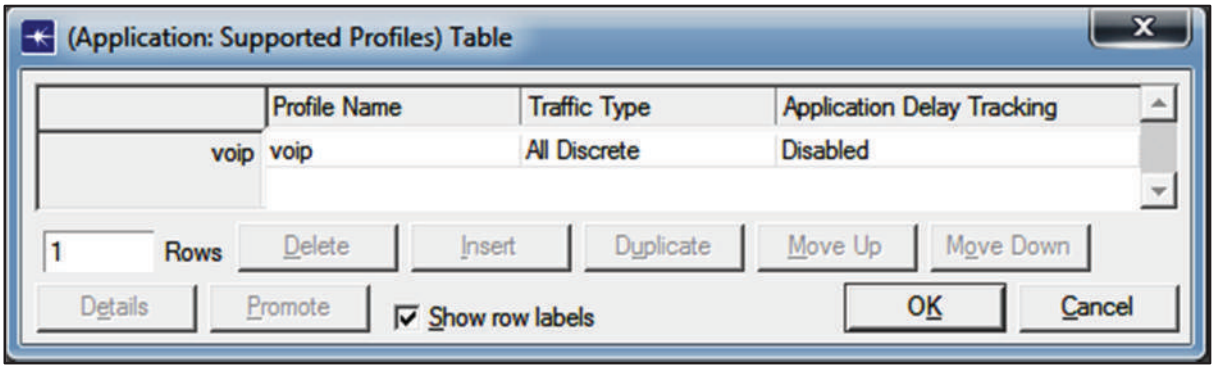


Figure II.17 : Supported Profile

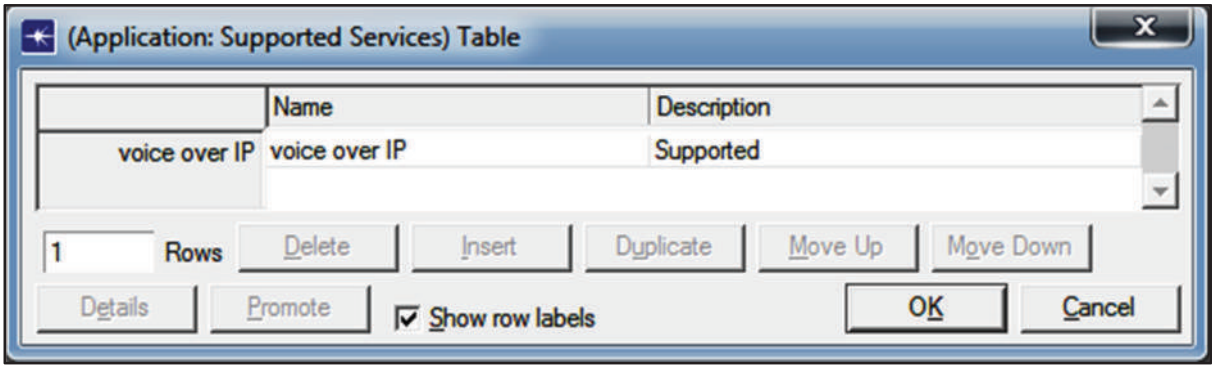


Figure II.18 : Supported Services

III.3. Topologies des différents cas de simulations (scénarios) :

III.3.1. Vue générale sur les projets réalisés:

III.3.1.1. Projet 1 : Réseau *Ethernet :*

Le réseau *Ethernet* est le plus répandu des réseaux locaux sur lequel tous les utilisateurs peuvent communiquer en même temps, son grand avantage est la simplicité. Nous avons utilisé les composants représentés dans le tableau II.4 dans les topologies Ethernet réalisées.

Objet	Description
 ethernet_wkstn	Ce poste de travail supporte la VoIP et il peut être soit émetteur ou récepteur de paquets VoIP.
 10 Base T	Tous les éléments à l'intérieur du réseau local sont connectés en utilisant des liaisons 10 Base T duplex de 10 Mbits/s.
 10 Base T_LAN	Ce composant représente un LAN Ethernet dans une topologie commutée contenant un nombre de clients et un serveur. Le trafic de client peut être dirigé vers le serveur interne aussi bien que les serveurs externes.
 ehernet 16_switch	Cet objet est utilisé comme un commutateur principal, il s'agit de connecter les ordinateurs ou les LANs de même type.
 ethernet4_slip8_gtwy	Les paquets IP arrivant sur n'importe quelle interface sont routés à l'interface appropriée de rendement basée sur leur adresse IP de destination. Ce composant est le responsable de cette opération.
 PPP_DS1	C'est une liaison duplex de point à point connectant deux nœuds de fonctionnement IP à longue distance avec un débit de 1.544 Mbits/s.

Tableau II.4 : Composants Ethernet

II.3.1.2. Projet 2 : Réseau *Wi-Fi* :

La technologie de base utilisée pour construire des réseaux sans fil peu coûteux est la famille des protocoles 802.11, aussi connue sous le nom de *WiFi* (*Wireless Fidelity*). Elle a connu une incroyable popularité ces dernières années.

Les composants utilisés dans ce projet sont décrits dans le tableau II.5.

Objet	Description
 wlan_wkstn	Poste de travail spécifique pour les réseaux locaux sans fil supportant les applications VoIP .
 wlan_ethernet_router	Il s'agit d'un routeur sans fil basé sur LAN avec une interface Ethernet.

Tableau II.5 : Composants WiFi

Les configurations du poste de travail et du routeur permettant aux réseaux de transmettre la voix sur IP sont indiquées dans les figures II.18 et II.19.

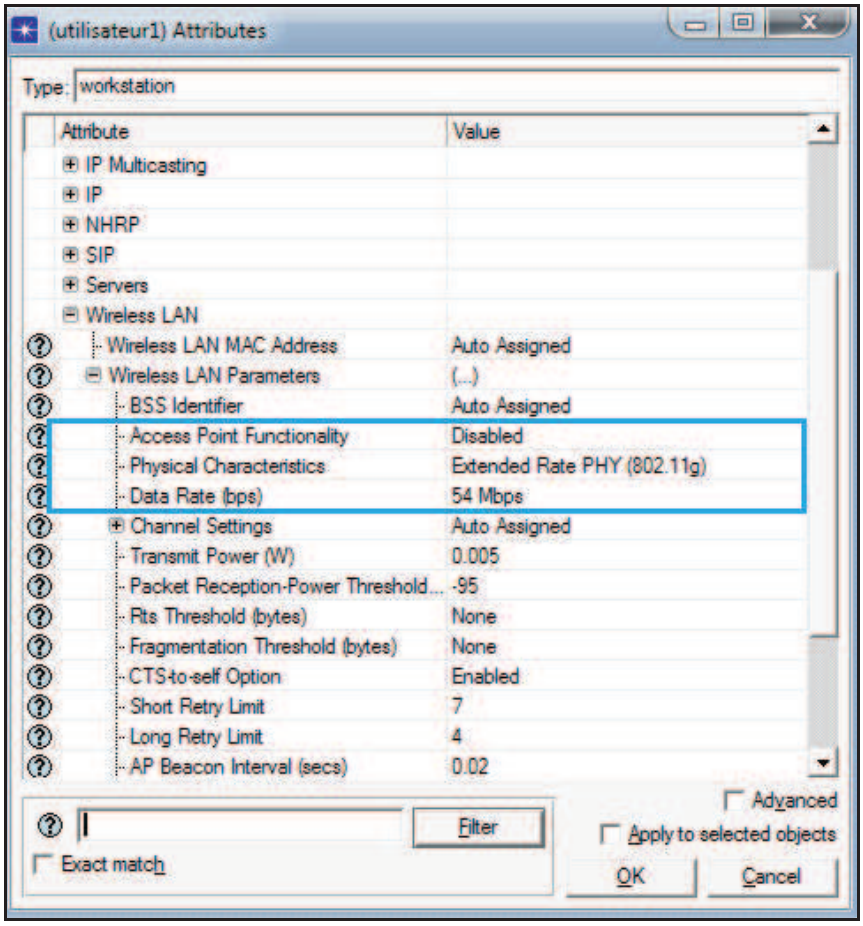


Figure II.19 : Configuration du poste de travail

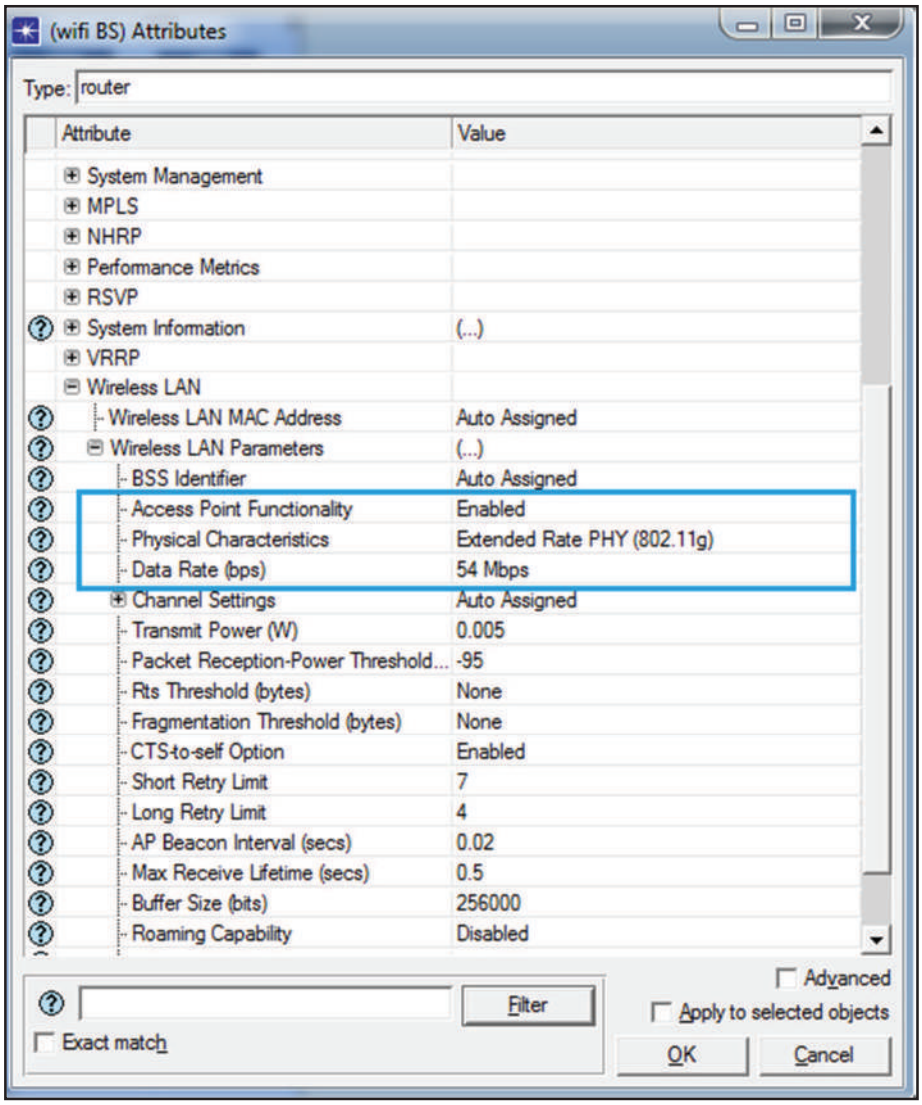


Figure II.20 : Configuration du routeur (Point d'accès).

- *Access Point Functionality (*Fonctionnalité du point d'accès*) :* Il permet de déterminer le point d'accès au réseau WiFi, activé (*enabled*) pour le routeur et (*disabled*) pour les ordinateurs.
- *Physical Characteristics (Caractéristiques physiques) :* Cet attribut détermine la technologie de la couche physique en cours d'utilisation. On a choisi *Extended Rate Phy (802.11g)* avec un débit de *54Mbits/s* qui est très largement répandue actuellement.

II.3.1.3. Projet 3 : *WiMAX* :

Le *WiMAX* (*Worldwide Interoperability for Microwave Access*) s'agit d'un ensemble de normes techniques basées sur le standard de transmission radio 802.16 permettant la

transmission des données IP haut débit par voie hertzienne. Le débit théorique maximum supporté par le WiMAX est de 70 Mbits/s sur une distance théorique de plusieurs dizaines de kilomètres.

Les composants utilisés pour réaliser le réseau WiMAX dans l'OPNET sont mentionnés dans le tableau II.6.

Objet	Description
 wimax_ss_wkstn	Poste de travail spécifique pour les réseaux WiMAX supportant les applications VoIP.
 wimax_bs_ethernet4_slip4_router	Routeur sans fil présentant une station de base WiMAX.
 WiMAX_Config	Ce nœud est employé pour stocker des profils physiques et de services qu'ils peuvent être mis en référence par tous les nœuds WiMAX dans le réseau.

Tableau II.6 : Composants WiMAX

La configuration de ce dernier composant est représentée sur la figure II.21.

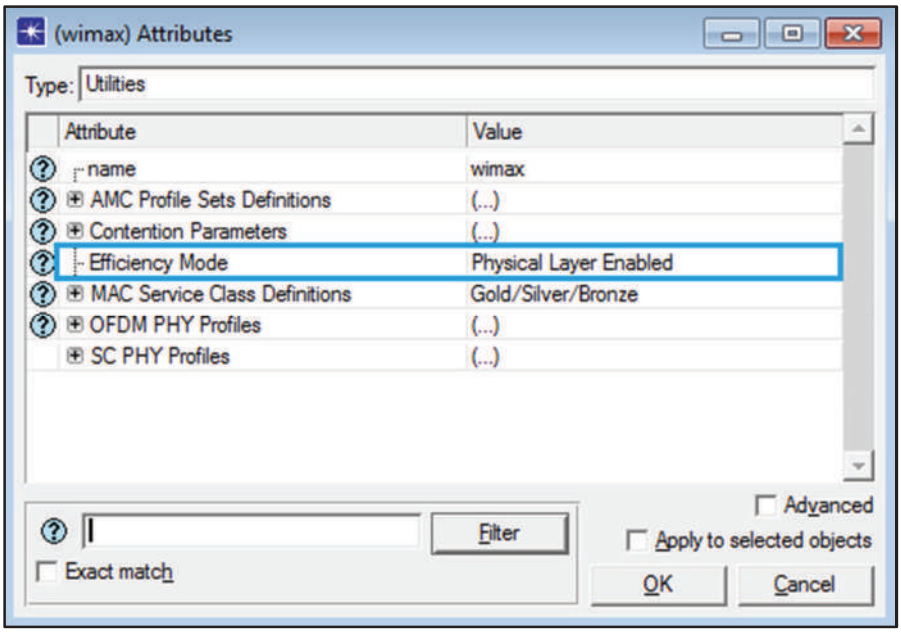


Figure II.21 : Configuration de WiMAX

Les modèles WiMAX dans l'OPNET nécessitent un nœud de configuration additionnel pour spécifier les paramètres de WiMAX. Le paramètre principal est le mode d'efficacité *(Efficiency Mode*) qu'il doit être réglé à *Physical Layer Enabled* (Couche physique activée) afin d'observer les effets de la distance.

La puissance de transmission, le gain d'antenne, sont les paramètres principaux qui ont été manuellement changés pour la station de base et les postes de travail. Les valeurs typiques pour la puissance de transmission sont 10W pour la station de base et 0.5W pour les utilisateurs. Les gains d'antenne de la station de base et des postes de travail sont placés à 15dBi et 14dBi, respectivement [15]. Les figures III.21 et III.22 montrent la configuration WiMAX pour la station de base et les postes de travail.

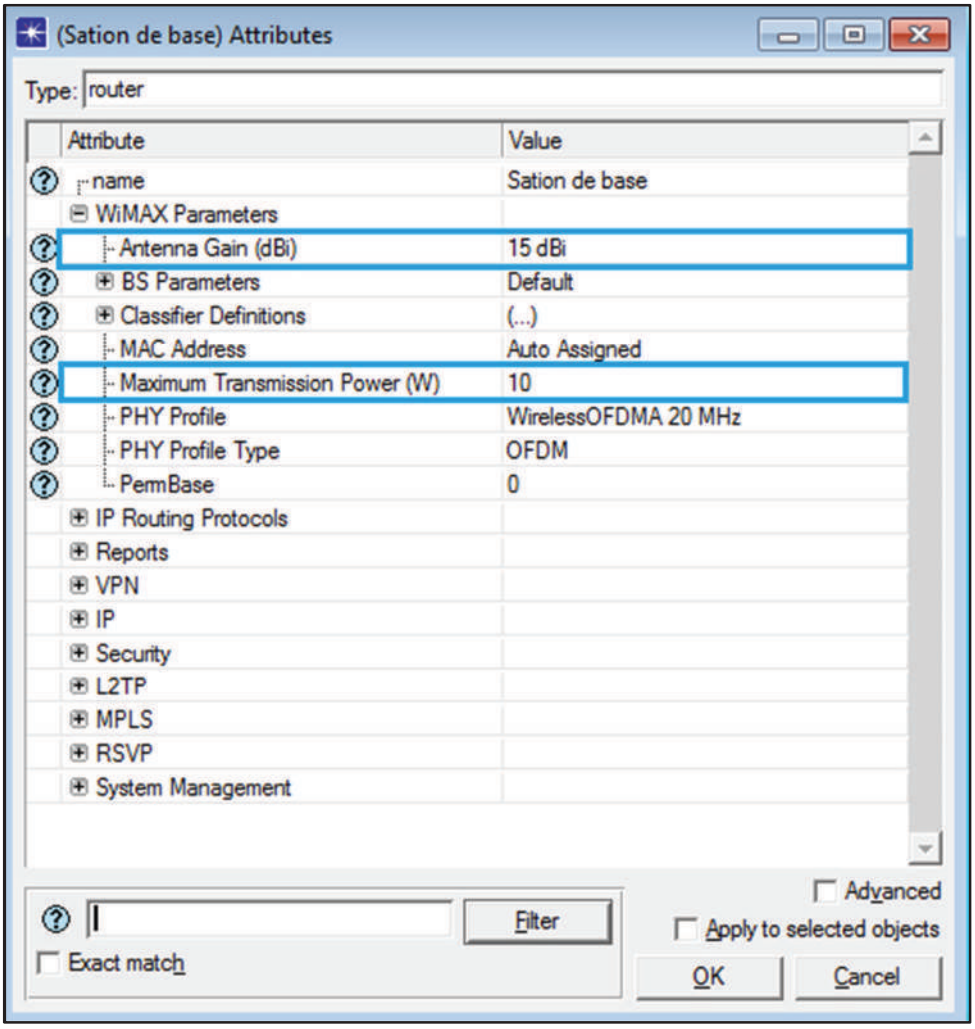


Figure II.22 : Configuration de la station de base

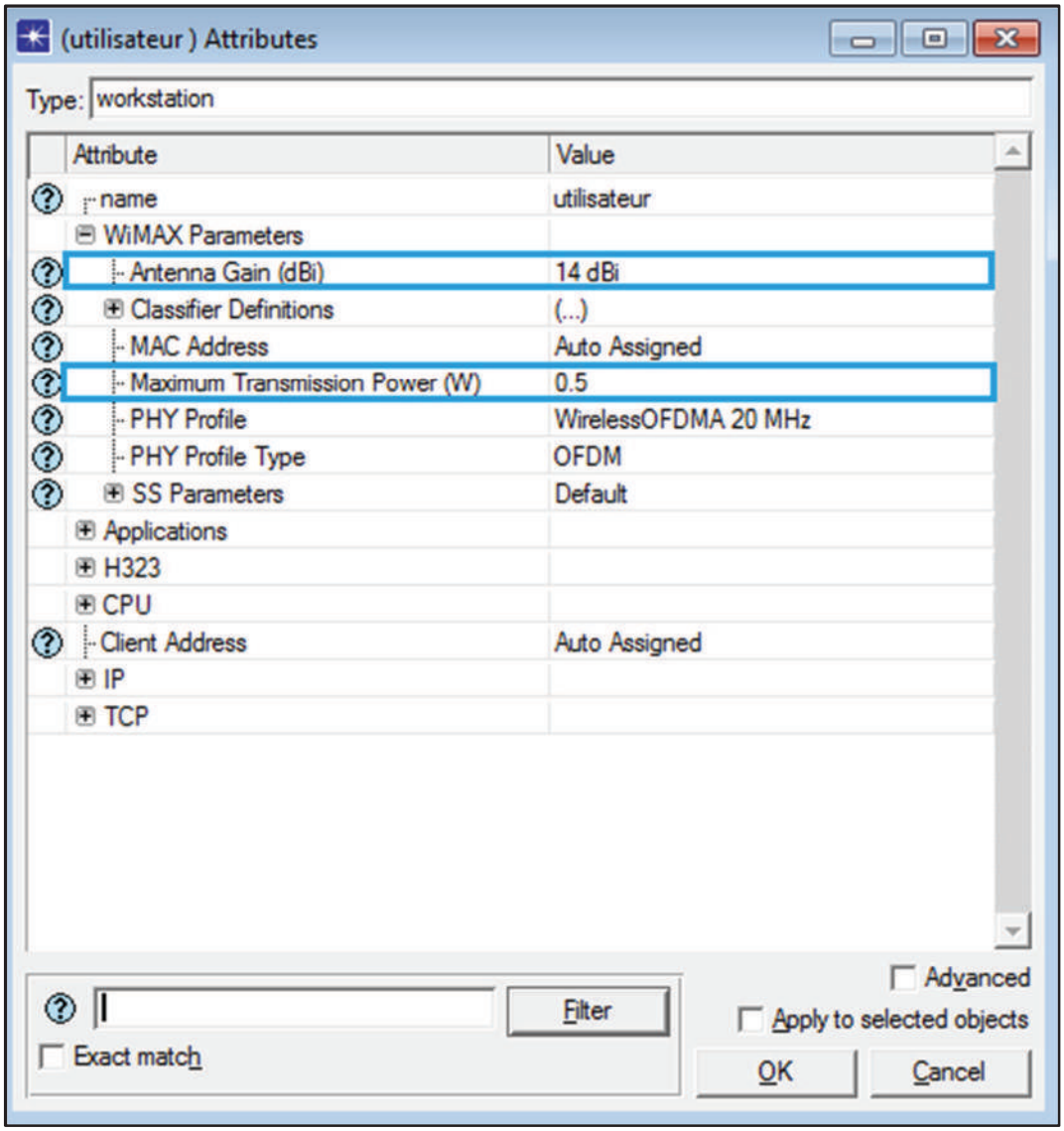


Figure II.23 : Configuration des postes de travail

III.3.2. Vue générale sur les scénarios :

Chaque projet est testé en neuf scénarios de la façon suivante :

Scénario 1 : *Courte distance*

On simule la voix sur IP dans un simple réseau dont la distance entre l'utilisateur et le commutateur est de 400m pour l'Ethernet, 200m pour le WiFi et 12,5km pour le WiMAX.

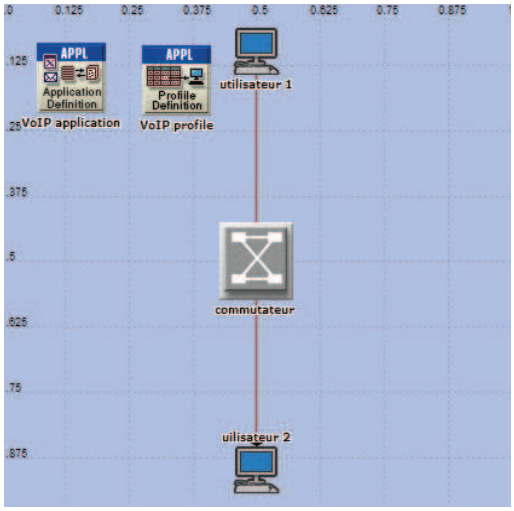
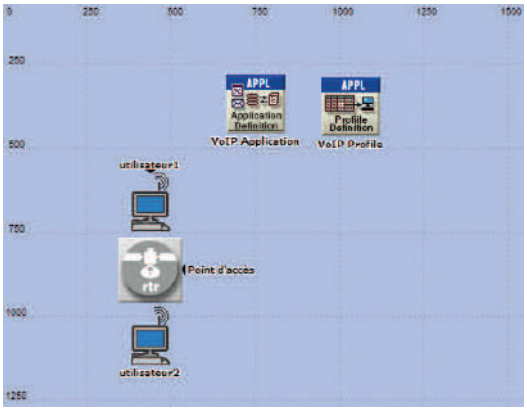
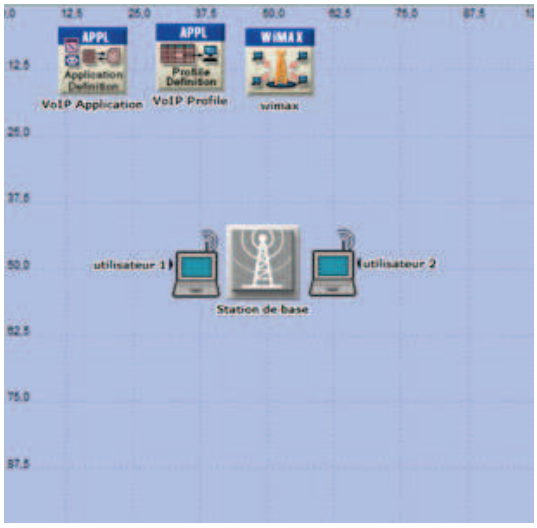
Ethernet (400m)	
WiFi (200m)	
WiMAX (12,5km)	

Tableau II.7 : Les Topologies des scénarios de courte distance pour les trois réseaux

Scénario 2 : *Longue distance*

Dans ce scénario, on sépare les postes de travail et le routeur par une distance de 370m dans le réseau WiFi et d'environ 37km dans celui de WiMAX.

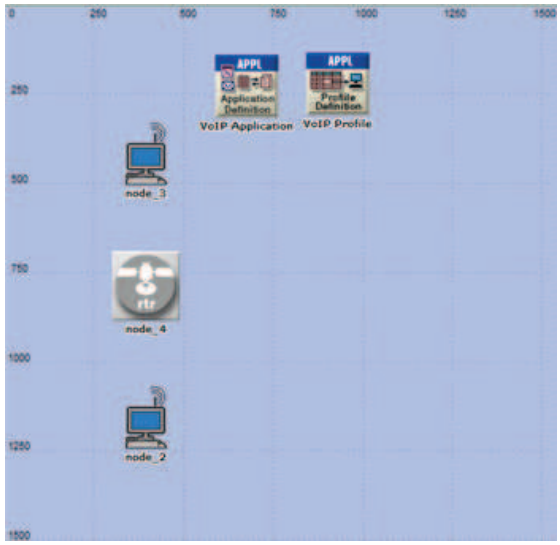
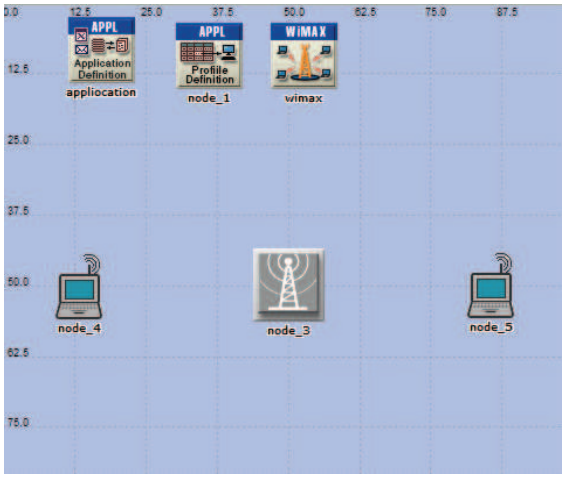
WiFi (370m)	
WiMAX (37km)	

Tableau II.8 : Les Topologies de scénarios de longue distance pour les réseaux WiFi et WiMAX

En cas du réseau Ethernet, deux sous-réseaux situés à Oran et à Constantine respectivement sont installés pour démontrer les performances des appels VoIP longue

distance en utilisant les connexions Ethernet. Une liaison point à point duplex PPP DS1 est utilisée pour connecter les routeurs des deux sous-réseaux.

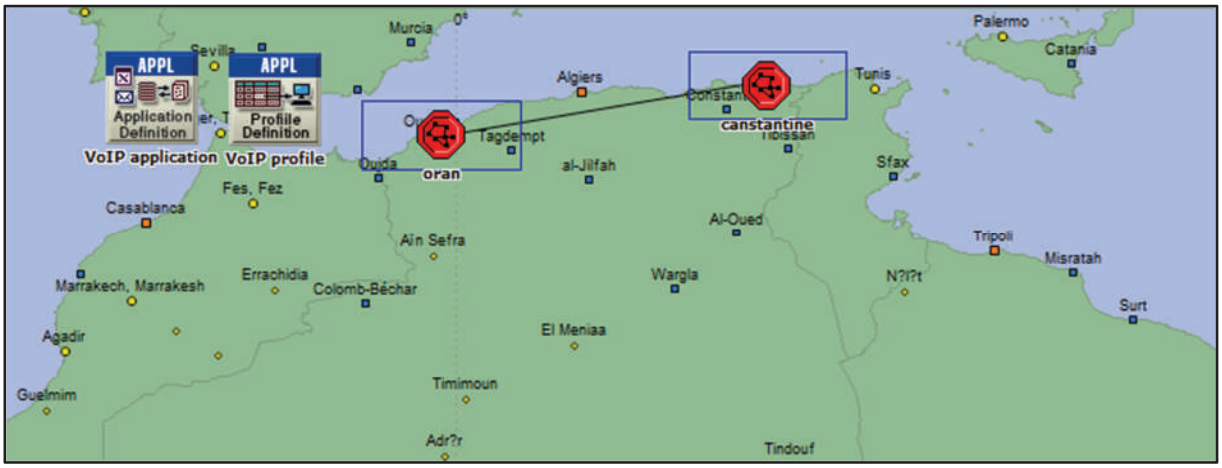


Figure II.24 : Topologie du réseau Ethernet longue distance

Les topologies des deux compagnies sont identiques pour l'uniformité.

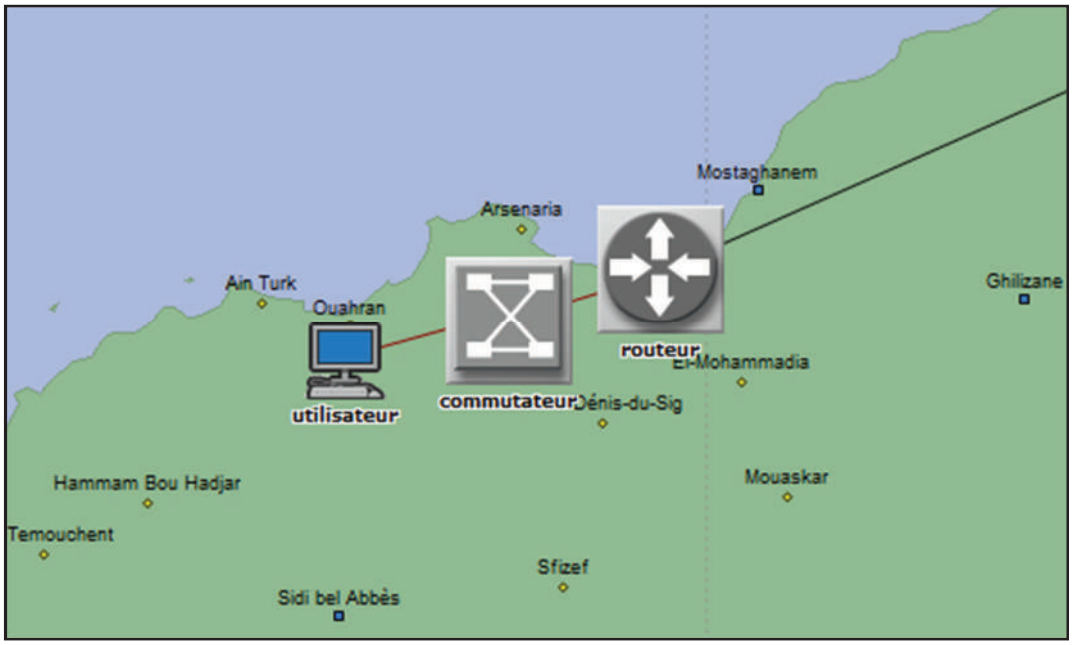


Figure II.25 : Topologie du sous réseau d'une compagnie

Scénarios 3, 4, 5 et 6 : *Changement de nombre de postes*

Pour étudier l'influence du nombre de postes de travail sur la qualité de la VoIP dans un réseau Ethernet, on essaye avec 2, 10 , 20 et 100 abonnés. Pour faciliter la conception de ces

réseaux, on s'appuie sur l'utilisation des réseaux locaux LAN qu'on peut contrôler le nombre de leurs nœuds.

Exemple :

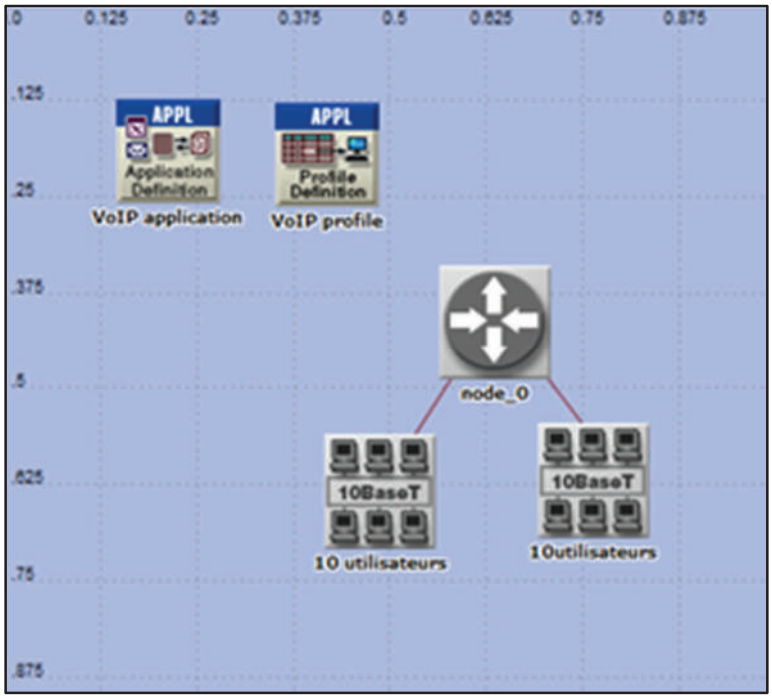


Figure II.26 : Ethernet avec 20 utilisateurs

⊟ LAN	
⊞ LAN Background Utilization	None
LAN Server Name	Auto Assigned
LAN Type	Ethernet
Number of Workstations	10
Switching Speed	500,000
⊞ NHRP	
⊞ SIP	
⊞ TCP	

Figure II.27 : Configuration de LAN.

Et pour les réseaux WiFi et WiMAX, on change le nombre d'utilisateurs de 2, 6, 10 et 14.

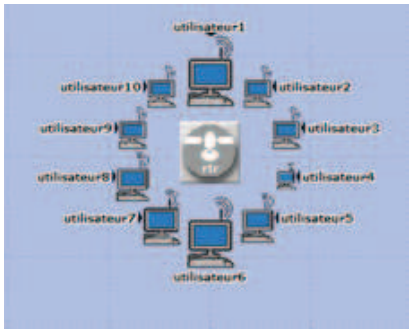
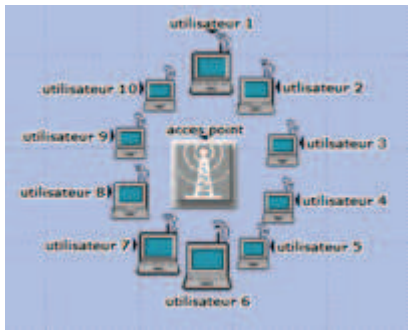
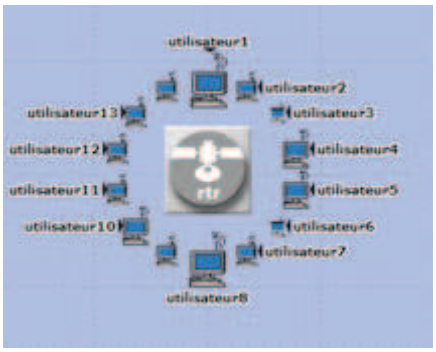
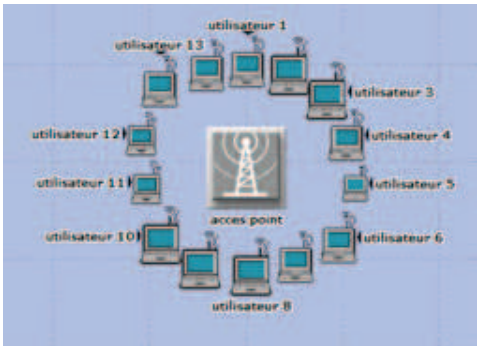
	WiFi	WiMAX
6 postes		
10 poses		
14 postes		

Tableau II.9 : Topologies des réseaux WiFi et WiMAX avec différents nombre d'ordinateurs

Scénario 7, 8 et 9 : *Changement de type de codec*

Les types de codec à étudier sont G.711, G723.1 5.3k et G729.A qu'on peut les modifier à partir de la définition d'application :

« Application Definition » → voice → G.711, G723.1 5.3k ou G729.A

III.4. Choix des statistiques à collecter :

Avant de lancer la simulation, l'OPNET exige l'indication des paramètres qu'on veut les étudier pour pouvoir afficher leurs résultats après la simulation.

Dans notre projet, on va suivre les variations de la gigue, la valeur MOS, le délai de bout en bout (latence) et la perte de paquets.

La sélection de ces paramètres s'effectue par les étapes suivantes :

1. On fait un clic droit sur l'espace de travail et on choisit « *Choose Individual Satistics* » dans le menu déroulant.
2. Une boite de dialogue s'affichant classe hiérarchiquement les statistiques globales, de chaque nœud ou des liaisons.
3. On sélectionne « *Global Statisics* » puis « *voice* ».
4. On coche les cases des paramètres que nous concerne dans notre simulation :
   - ✓ Jitter (sec).
   - ✓ MOS Value.
   - ✓ Packet End to End Delay (sec).
   - ✓ Traffic Received (packet/sec).
   - ✓ Traffic Sent (packet/sec).

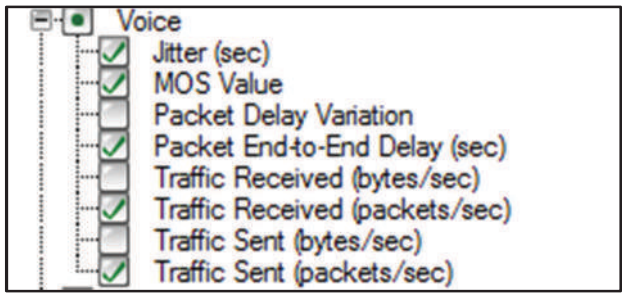


Figure II.28: Choix des paramètres à poursuivre

VI. Conclusion :

OPNET est un logiciel puissant, qui permet de nombreuses modélisations de réseaux grâce à ses nombreuses bibliothèques. De ce fait, le logiciel nécessite une bonne connaissance et appréhension du domaine des réseaux pour maîtriser les tenants et aboutissants du logiciel.

Par ailleurs, il nous semble qu'OPNET par sa complexité et ses nombreuses possibilités de paramétrages nécessite une véritable formation pour être totalement maîtrisé.

Cependant, ce logiciel propose un mode scénario et des fonctionnalités (modélisation, simulation, …) qu'il serait intéressant d'utiliser dans le cadre de sujets pratiques.[14]

Dans notre simulation avec l'OPNET, nous avons décidé d'examiner les performances de la VoIP dans les réseaux Ethernet, WiFi et WiMAX pour une longue et une courte distance, avec différents nombre d'utilisateurs, nous avons également examiné ces performances avec différents types de codecs en détaillant la méthode de simulation en utilisant l'OPNET.



Chapitre 3 :

Résultats de simulations et discussions



I. Introduction :

Dans le chapitre précédant, nous avons réalisé les topologies de nos réseaux et nous avons configuré les objets qu'ils les composent ainsi que nous avons spécifié les statistiques à collecter. Donc nous sommes maintenant prêts à les simuler.

Le lancement de simulation se réalise par le bouton  dans la barre des outils, on simule les scénarios pendant une durée de 10mn.

II. Résultats et discussions des simulations :

II.1. Projet 1 : Réseau *Ethernet*

II.1.1. Modification de la distance :

Les figures III.1, III.2, III.3, et III.4 présentent la gigue, la valeur MOS, le délai de bout en bout et la perte de paquets dans les scénarios courte et longue distance dans le réseau Ethernet.

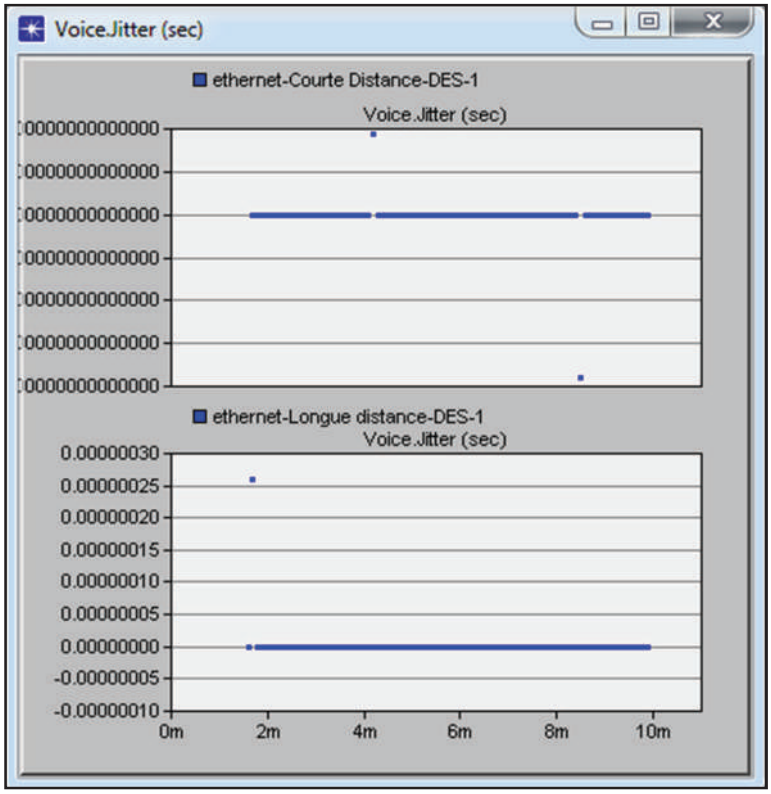


Figure III.1 : Gigue dans les scénarios courte et longue distance dans le réseau Ethernet

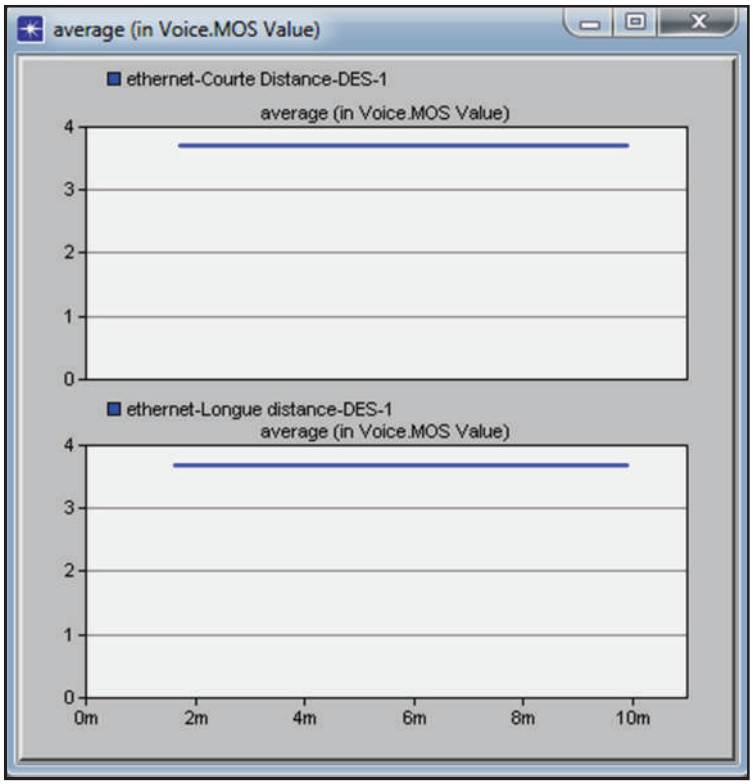


Figure III.2 : Valeur MOS dans les scénarios courte et longue distance dans le réseau Ethernet

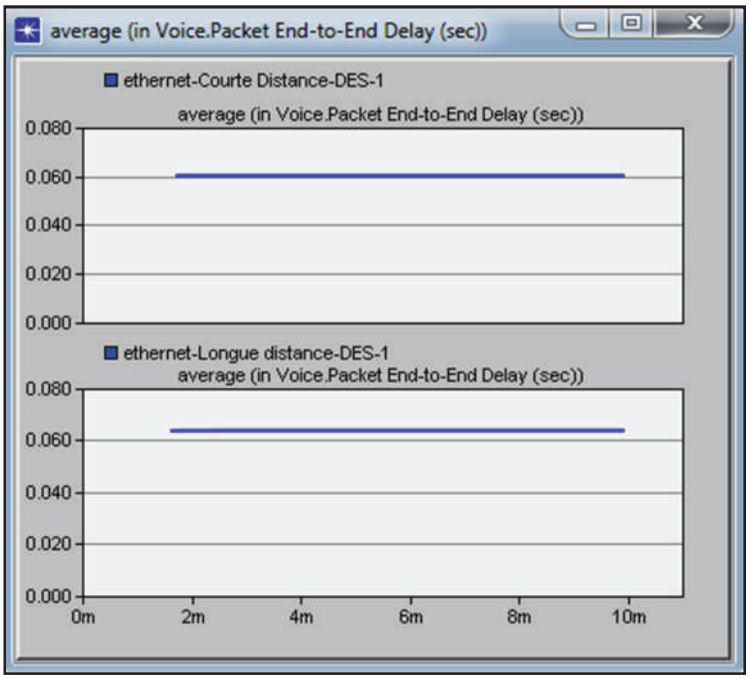


Figure III.3 : Délai de bout en bout dans les scénarios courte et longue distance dans le réseau Ethernet

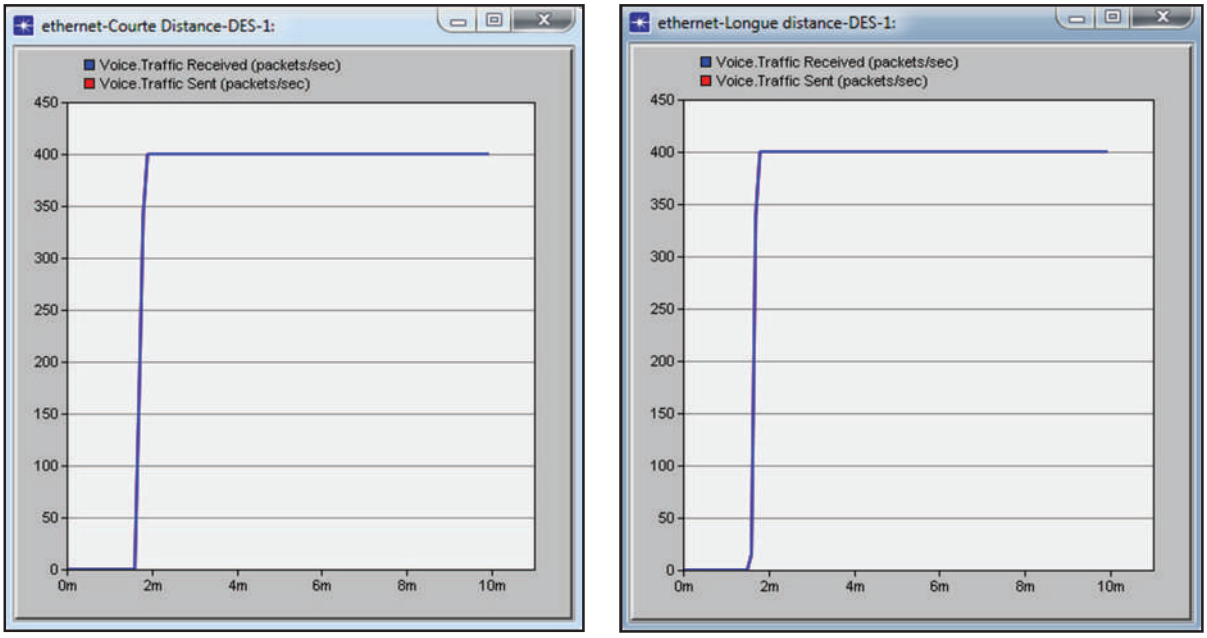


Figure III.4 : Pertes de paquets dans les scénarios courte et longue distance dans le réseau Ethernet

Comme il est évident dans la figure III.1, la gigue est nulle quand la distance entre les utilisateurs et le commutateur est courte et dans le cas d'une longue distance elle augmente de 25µs. D'autre part, la figure III.3 montre l'augmentation du délai de bout en bout avec l'augmentation de la distance, ce qui implique la dégradation de la valeur MOS. En outre, la figure III.4 indique qu'il n y a aucune perte de paquets qu'elle que soit la distance.

II.1.2. Modification du nombre de postes :

Les figures III.5, III.6, III.7 et III.8 nous montrent l'influence du nombre de postes sur la gigue, la valeur MOS, le délai de bout en bout et la perte de paquets.

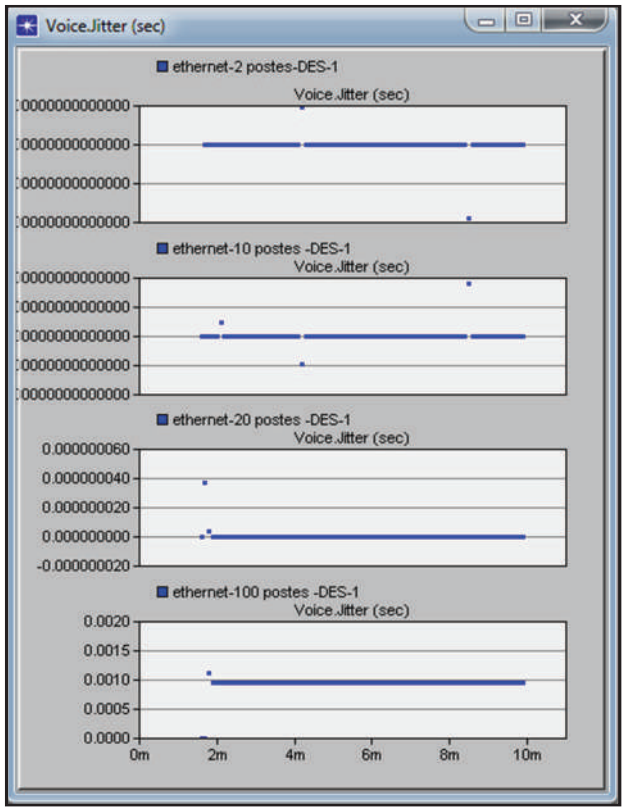


Figure III.5 : Gigue dans les scénarios utilisant 2, 10, 20 et 100 postes dans un réseau Ethernet

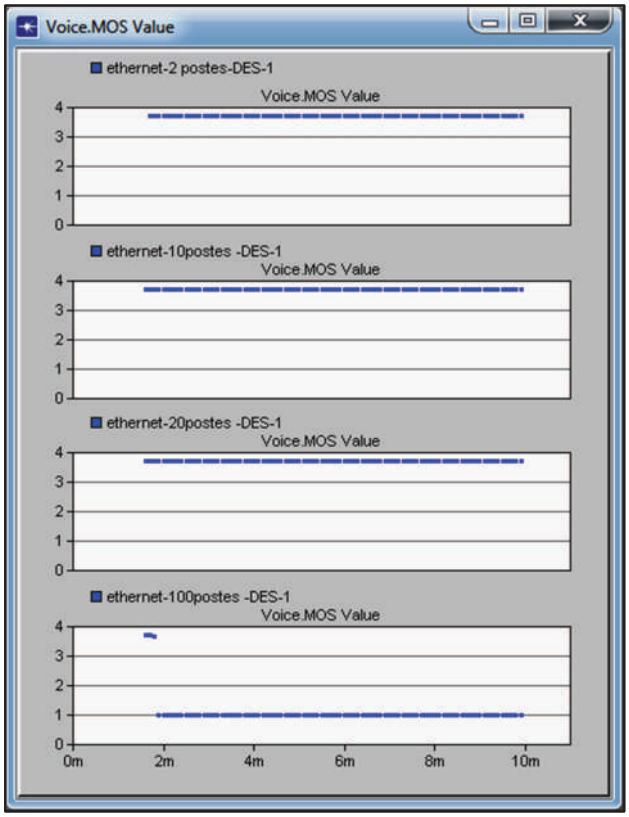


Figure III.6 : Valeur MOS dans les scénarios utilisant 2, 10, 20 et 100 postes dans un réseau Ethernet

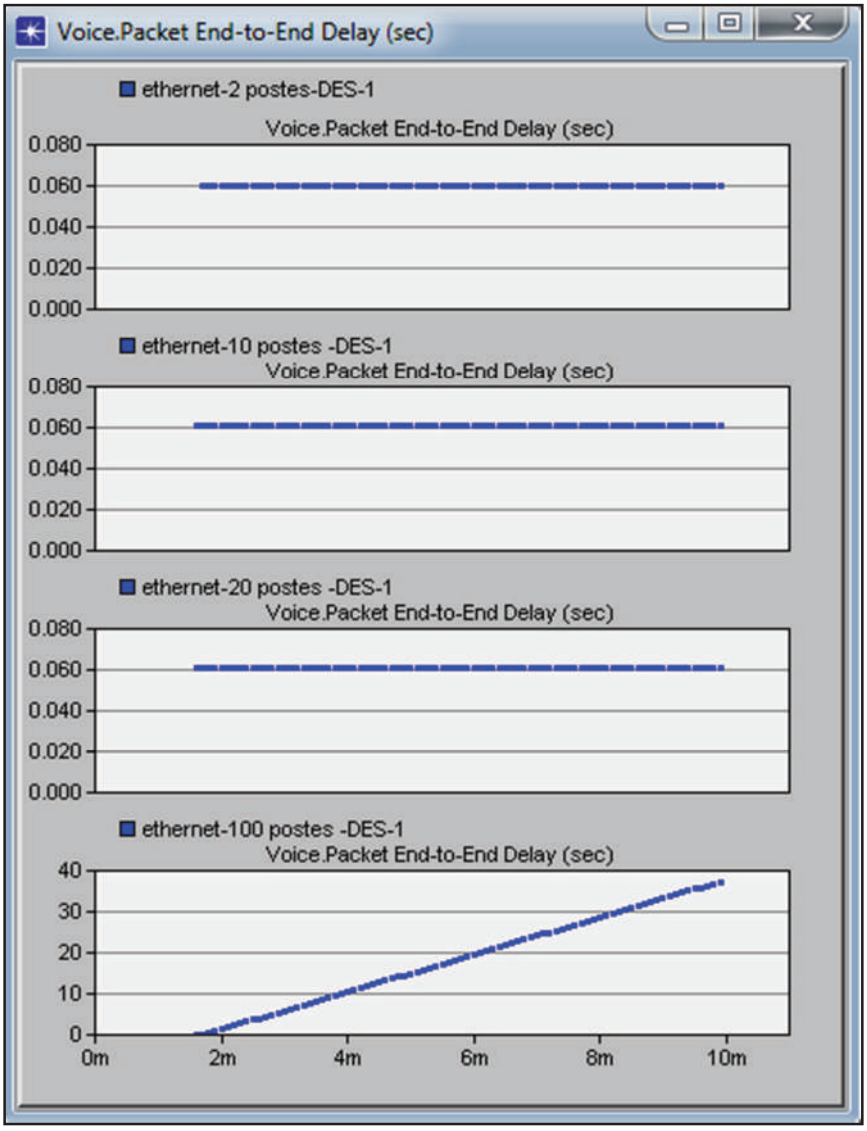


Figure III.7 : Délai dans les scénarios utilisant 2,10, 20 et 100 postes dans un réseau Ethernet

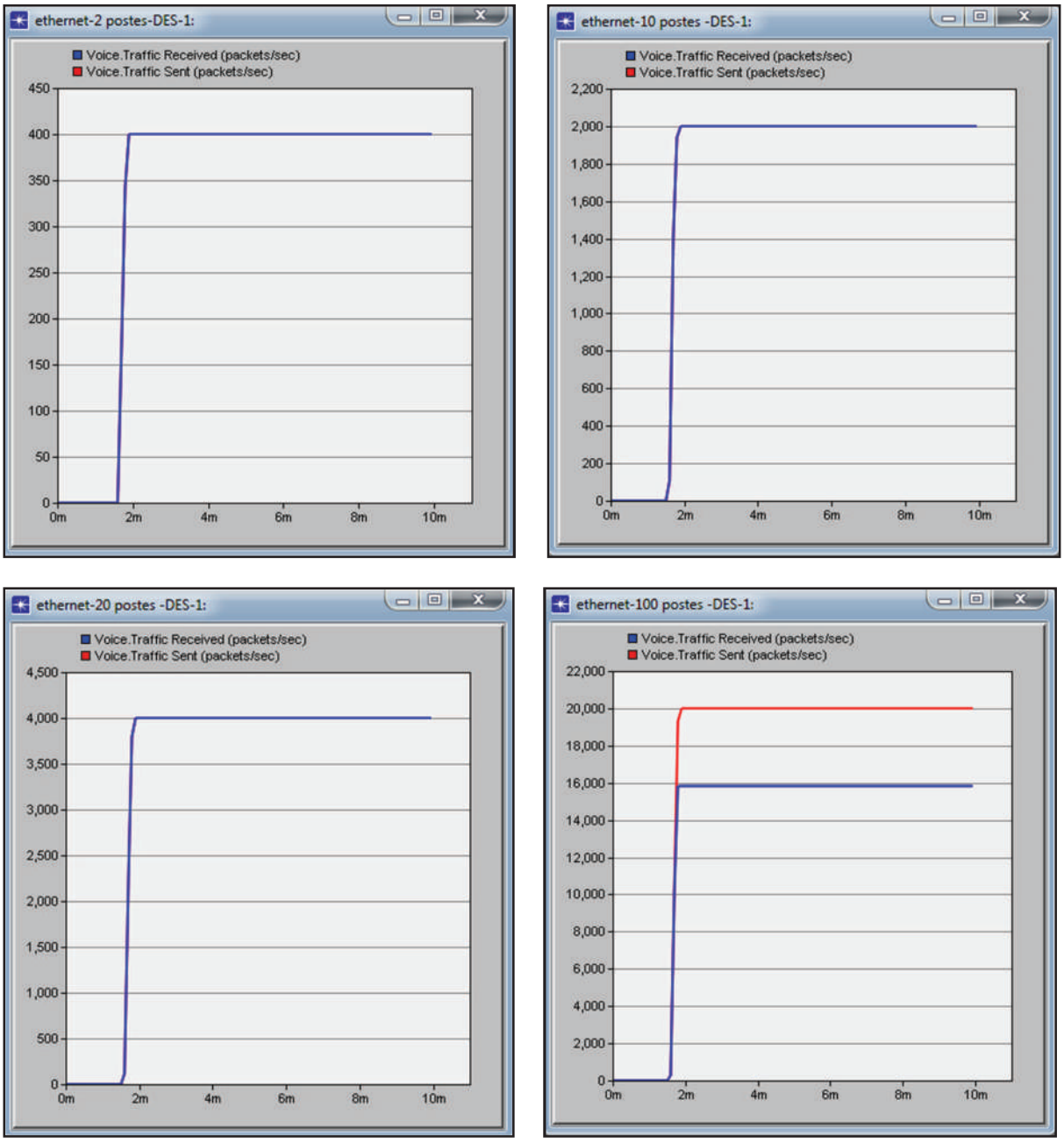


Figure III.8 : Perte de paquets dans les scénarios utilisant 2,10, 20 et 100 postes dans un réseau Ethernet

De toute évidence, quand le nombre de clients VoIP augmente, le délai de bout en bout augmente car plus de paquets sont émis en même temps. La gigue augmente aussi parce que beaucoup de paquets doivent attendre pour être transmis. Ainsi comme on peut le voir dans la figure III.8, le trafic envoyé est 20000 paquets par seconde tandis que 16000 paquets /s sont reçus alors 4000 paquets sont perdus par seconde dans le cas de 100 utilisateurs. Tous ces

facteurs vont abaisser la qualité de service VoIP ce qui est montré par la valeur MOS dans la figure III.6, cette valeur peut tomber jusqu'à ce qu'elle soit égale à 1(non recommandé).

II.1.3. Modification du type de codec :

La gigue, la valeur MOS, le délai de bout en bout, la perte de paquets sont présentés dans les figures III.9, III.10, III.11 et III.12 respectivement.

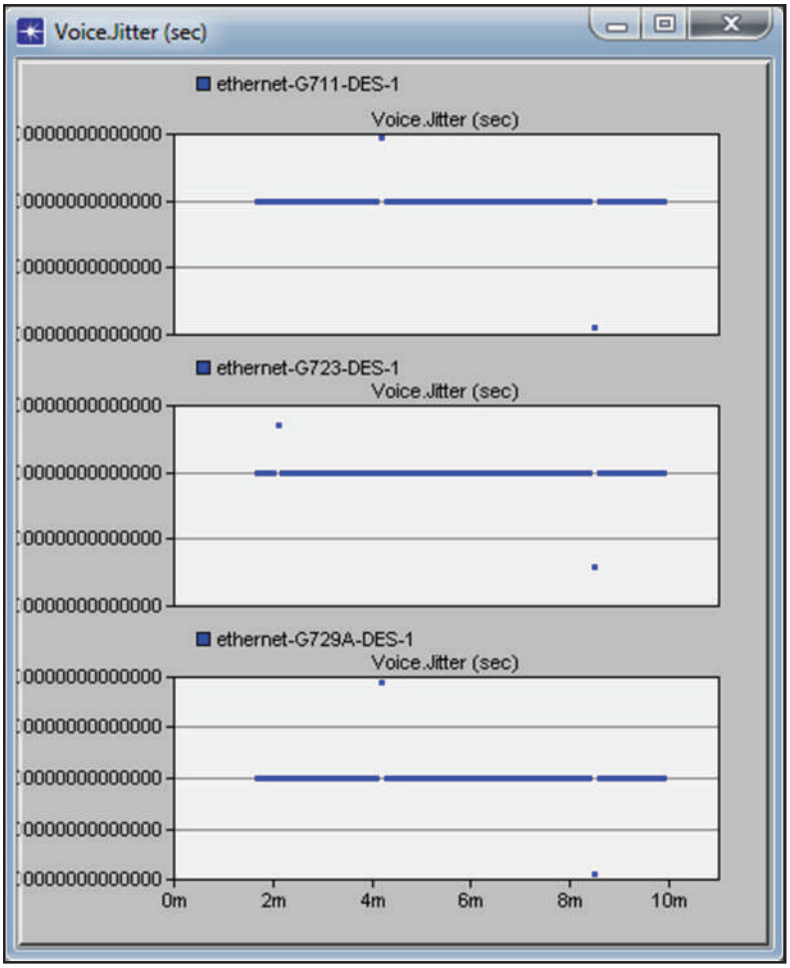


Figure III.9 : Gigue dans les applications VoIP avec différents types de codec dans le réseau Ethernet

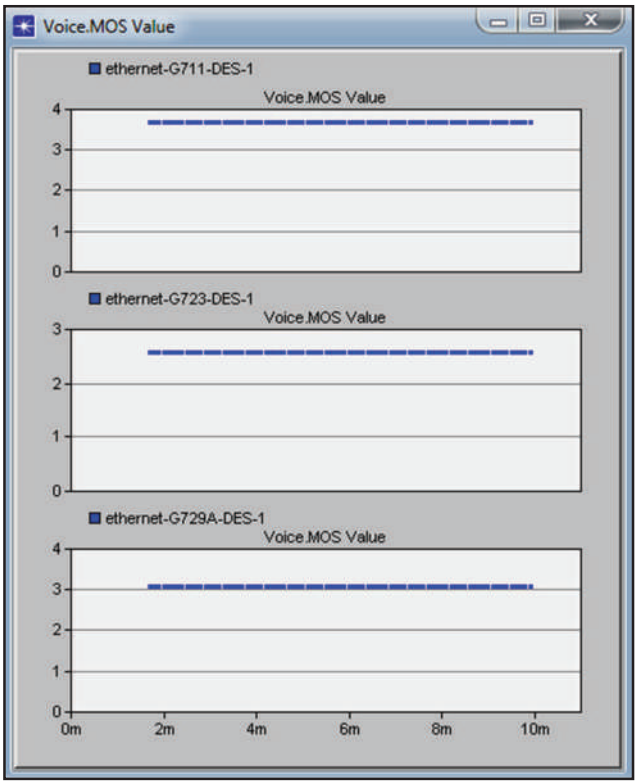


Figure III.10 : Valeur MOS dans les applications VoIP avec différents type de codec dans le réseau d'Ethernet

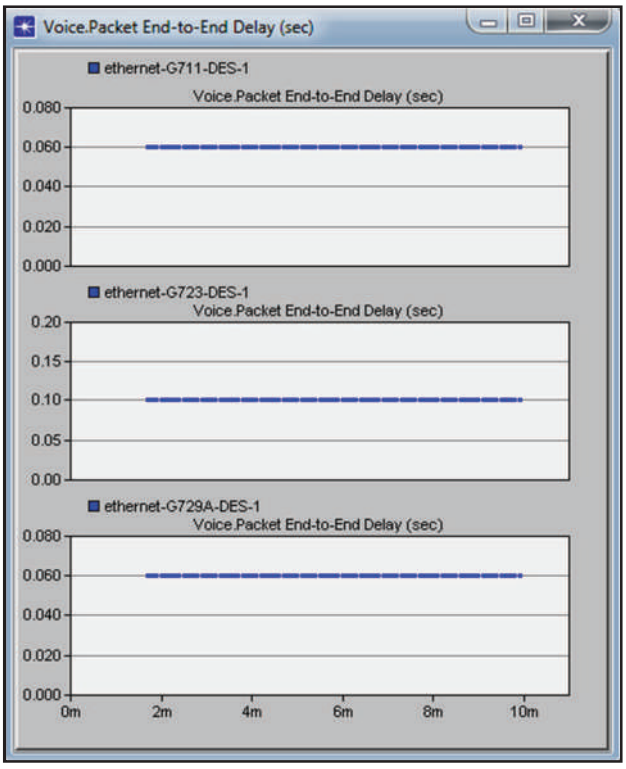


Figure III.11 : Délai dans les applications VoIP avec différents type de codec dans le réseau d'Ethernet

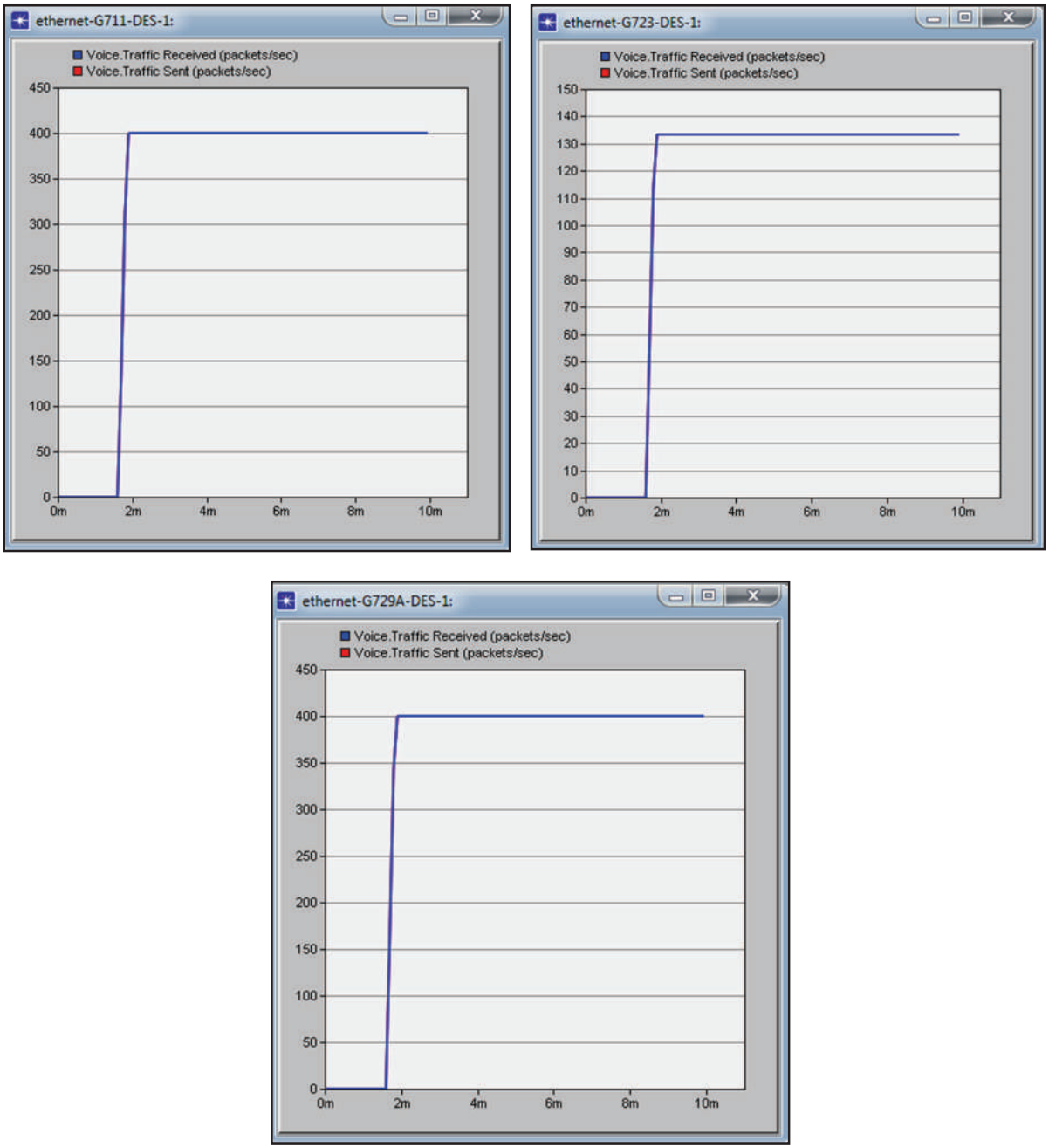


Figure III.12 : Pertes de paquet dans les applications VoIP avec différents type de codec dans le réseau d'Ethernet

A partir des figures ci-dessus, on peut remarquer que le type de codec n'influe pas sur la gigue qu'elle est dans les trois cas nulle, ni sur la transmission de paquet c'est-à-dire pas de perte de paquets mais ce facteur influe d'une façon claire sur la valeur MOS qu'elle est faible dans le cas de l'utilisation du codec G.723. Ce dernier donne un délai très élevé par rapport au codecs G.711 et G.729.

Le tableau III.1 donne une comparaison générale entre les résultats des différents scénarios du projet d'un réseau de type Ethernet.

	Gigue	MOS	Délai	perte de paquets
Courte distance, 2 postes, G.711	0	3.67	60.24ms	pas de perte
Longue distance	25µs	3.69	63ms	pas de perte
10 Postes	0	3.69	60.52ms	pas de perte
20 Postes	0.37µs	3.69	60.52ms	pas de perte
100 Postes	1.12µs	1	très élevé	perte de 20%
G.723	0	2.57	100.14ms	pas de perte
G.729	0	3.08	60.13ms	pas de perte

Tableau III.1 : Gigue, MOS, délai de bout en bout et perte de paquets dans les différents cas de scénarios pour un réseau Ethernet

La gigue est négligeable dans les scénarios de réseau Ethernet. La valeur MOS est satisfaite dans les scénarios de courte et longue distance et lorsqu'on utilise 2, 10 et 20 postes mais elle est insuffisante quand la vois est compressée et décompressée par G.723 et G729.A et dans le cas de 100 clients elle est de 1 montrant une pire qualité de service. Dans ce même réseau, il y a une perte de 20% de paquet ainsi un délai très élevé donc le réseau Ethernet avec 100 postes a un mal fonctionnement. Dans les autres cas le délai est acceptable et il y a aucune perte de paquets.

II.2. Projet 2 : Réseau *WiFi*

II.2.1. Modification de la distance :

Dans les figures III.13, III.14, III.15 et III.16, on observe les variations de la gigue, la valeur MOS, la latence et la perte de paquets en fonction de la distance séparent les utilisateurs et les commutateurs.

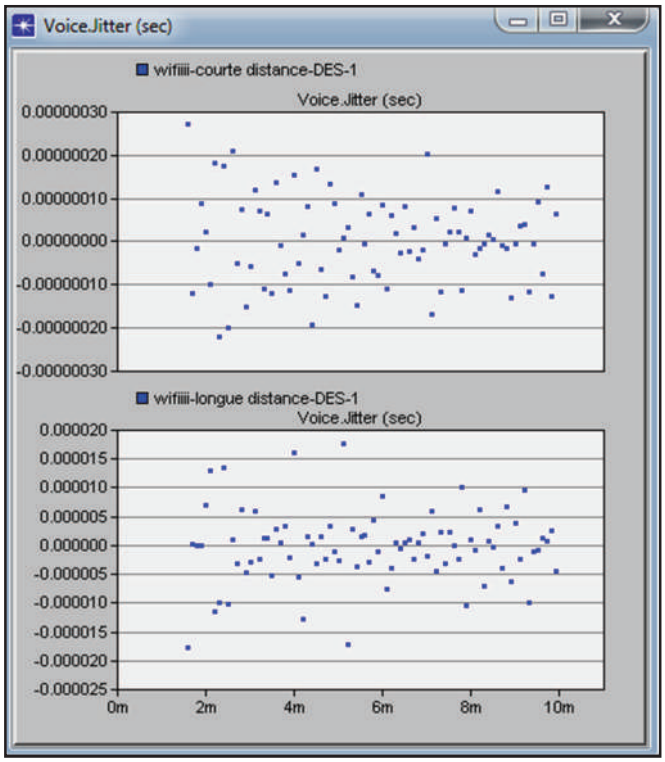


Figure III.13 : Gigue dans les scénarios courte et longue distance dans le réseau WiFi

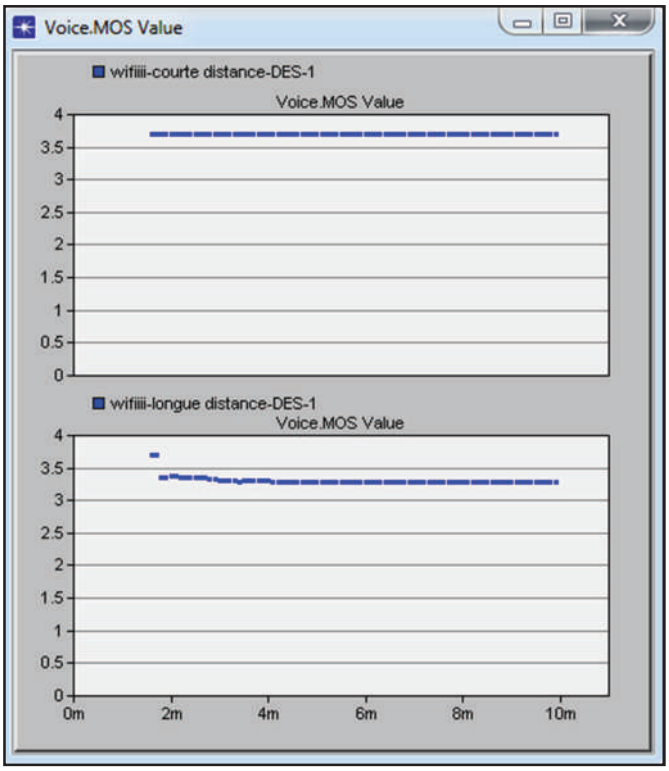


Figure III.14 : Valeur MOS dans les scénarios courte et longue distance dans le réseau WiFi

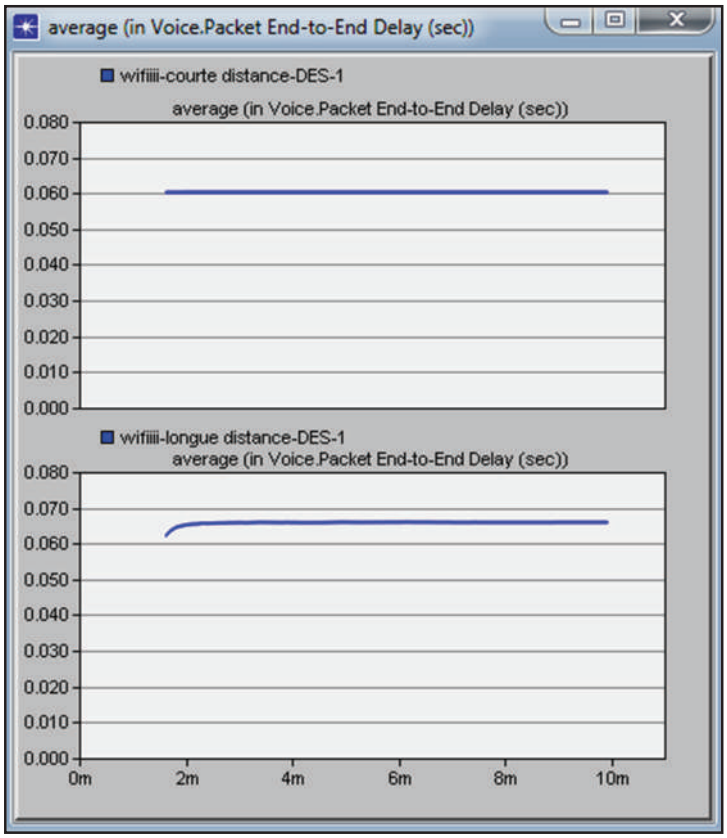


Figure III.15 : Délai de bout en bout dans les scénarios courte et longue distance dans le réseau WiFi

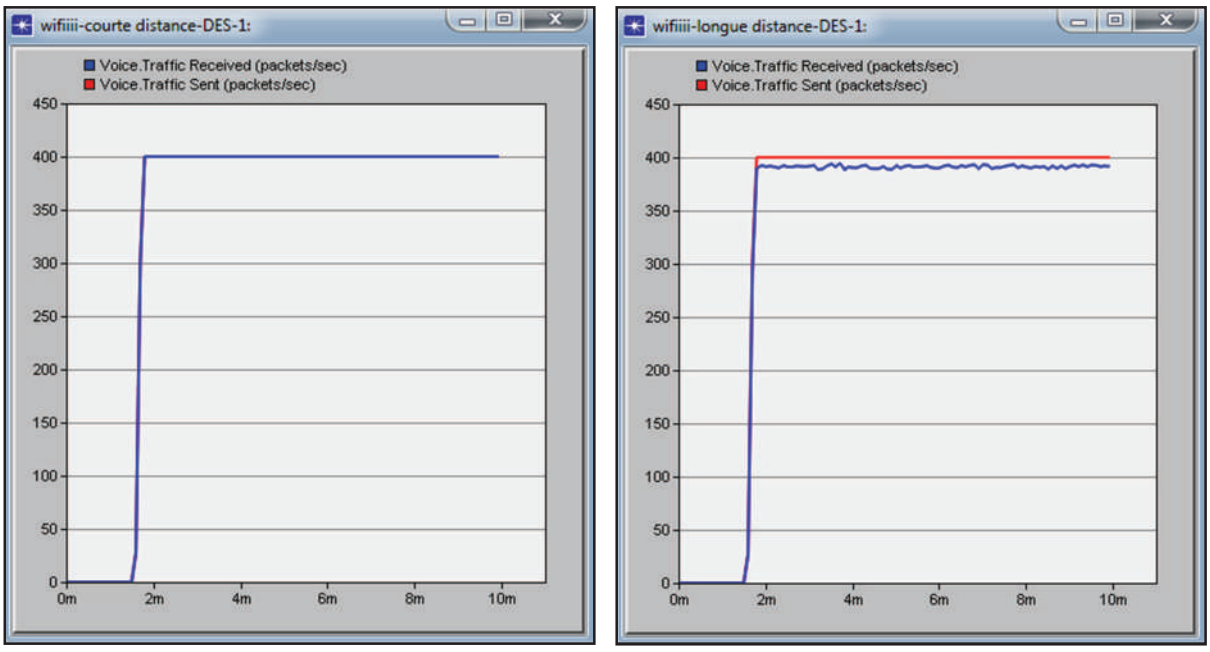


Figure III.16 : Perte de paquets dans les scénarios courte et longue distance dans le réseau WiFi

D'après ce qu'on a vu, il est clair que la gigue et le délai de bout en bout augmentent dans les longues distances mais ils restent acceptables en plus de l'apparition d'une perte de paquets. Ainsi, la valeur MOS diminue indiquant la diminution de la qualité de la voix.

II.2.2. Modification du nombre de postes :

Les figures III.17, III.18, III.19 et III.20 montrent l'influence du nombre d'utilisateurs sur la qualité de la VoIP dans le cas d'un réseau WiFi.

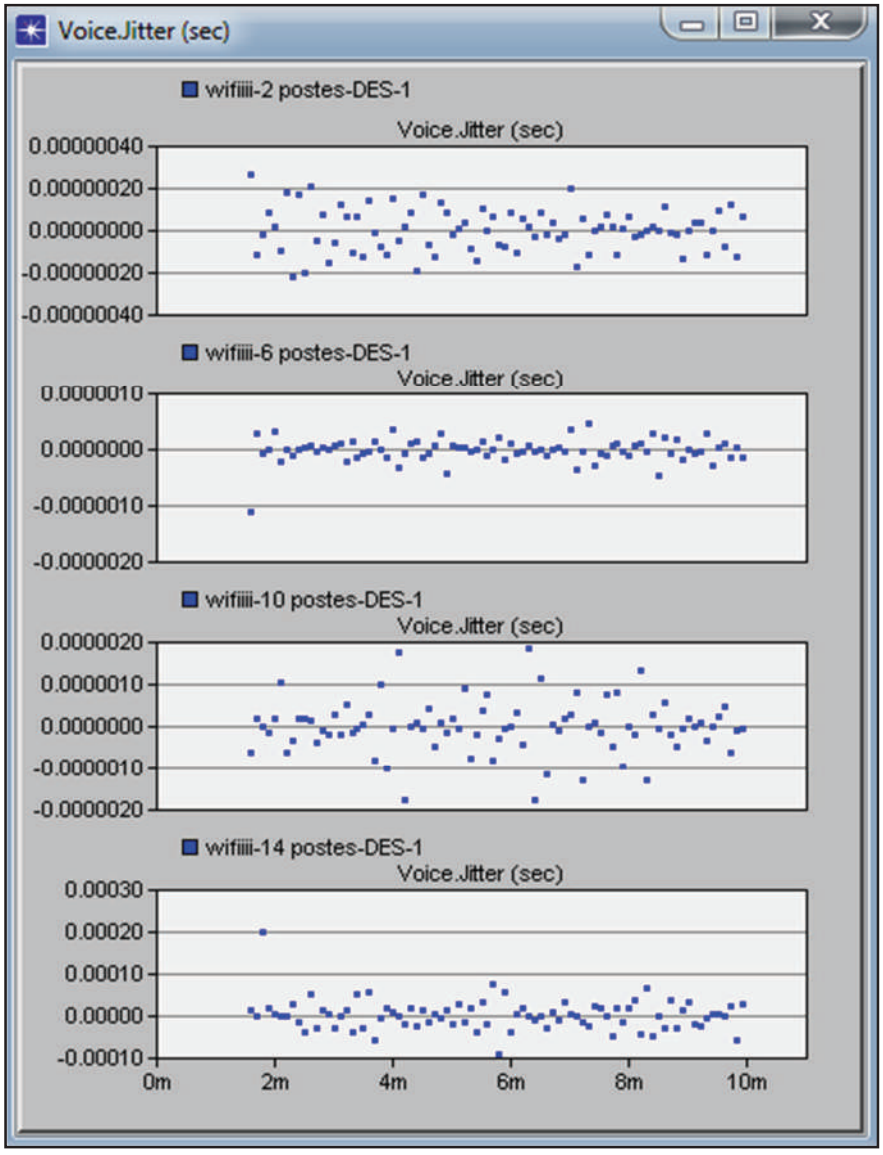


Figure III.17 : Gigue dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiFi

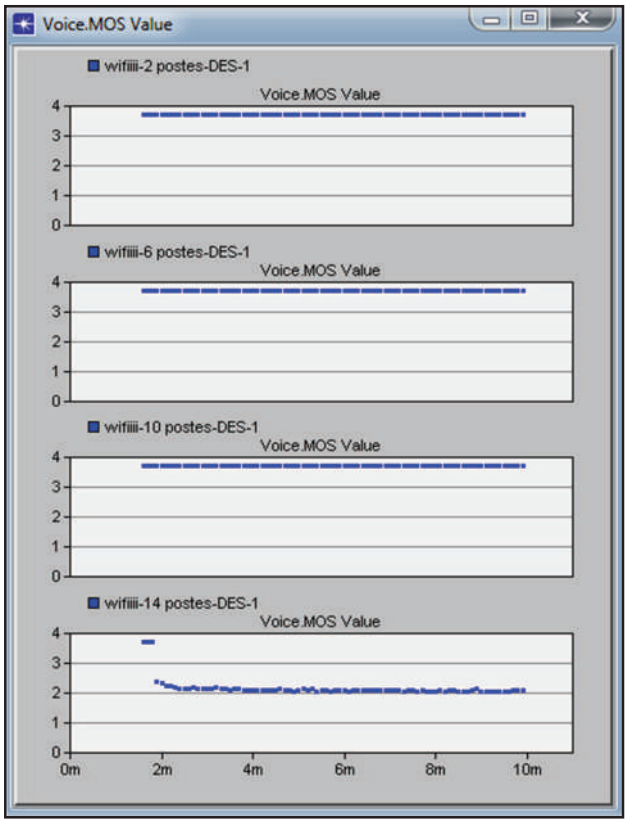


Figure III.18 : Valeur MOS dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiFi

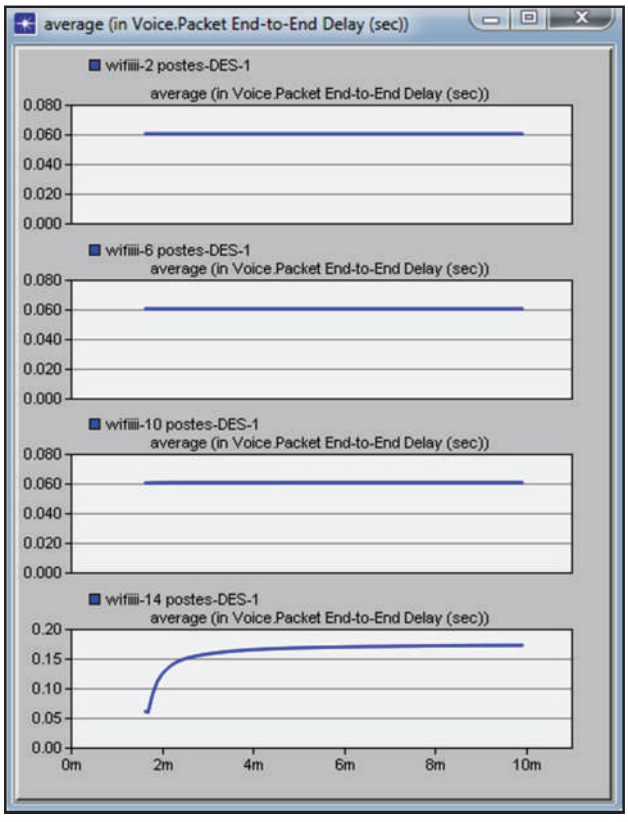


Figure III.19 : Délai dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiFi

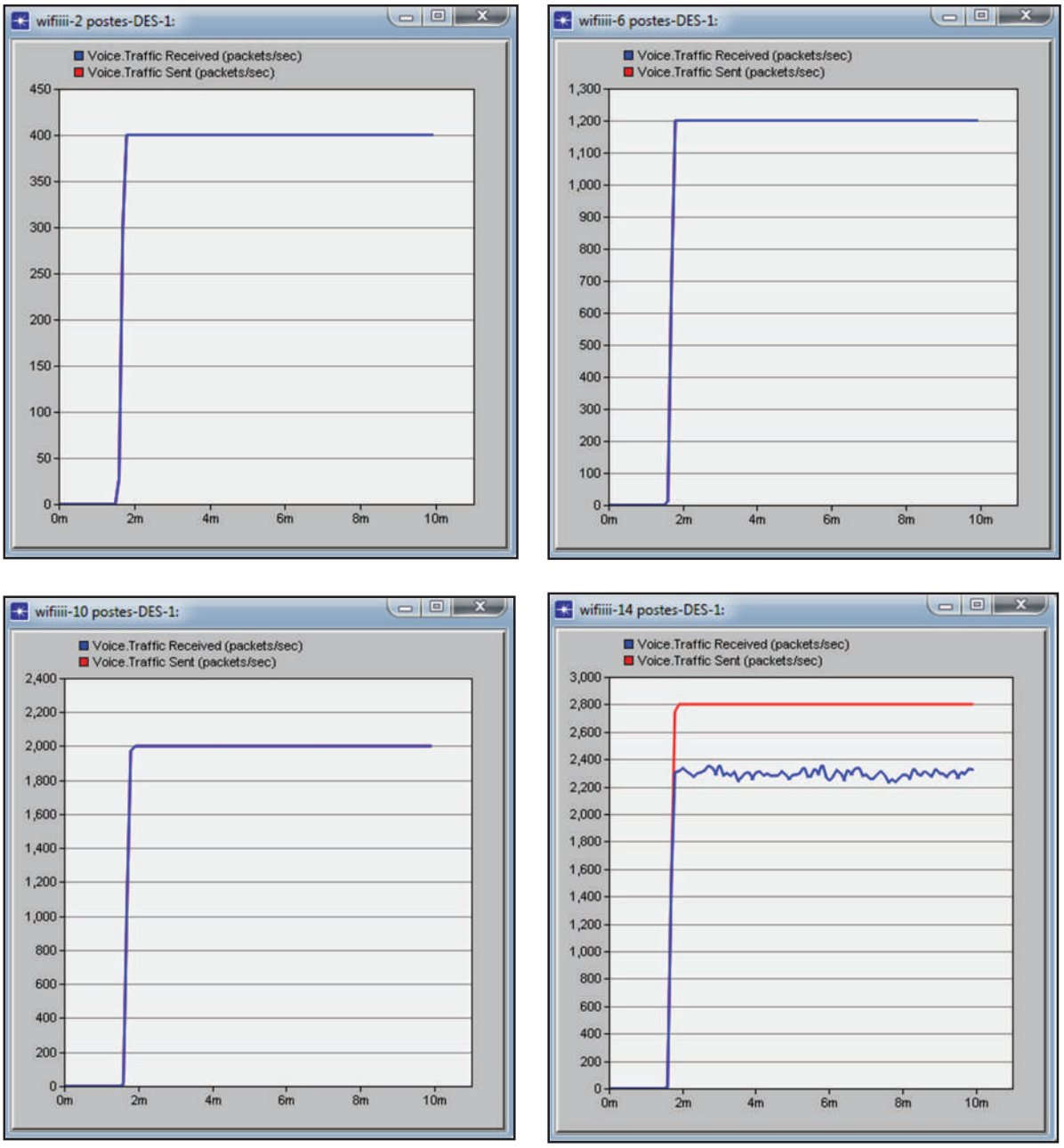


Figure III.20 : Perte de paquets dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiFi

Comme il est apparu dans les figures précédentes, lorsque le nombre de postes augmente, la gigue aussi augmente. Pour le délai de bout en bout il est constant dans les trois premiers cas ce qui donne une valeur constante de MOS et aucun paquet est perdu et il augmente rapidement si on ajoute 4 autres postes alors le MOS diminue et environ 19% de paquets sont perdus par seconde.

II.2.3. Modification du type de codec :

L'influence des codecs G.711, G.723 et G.729 est apparue dans les figures III.21, III.22, III.23 et III.24.

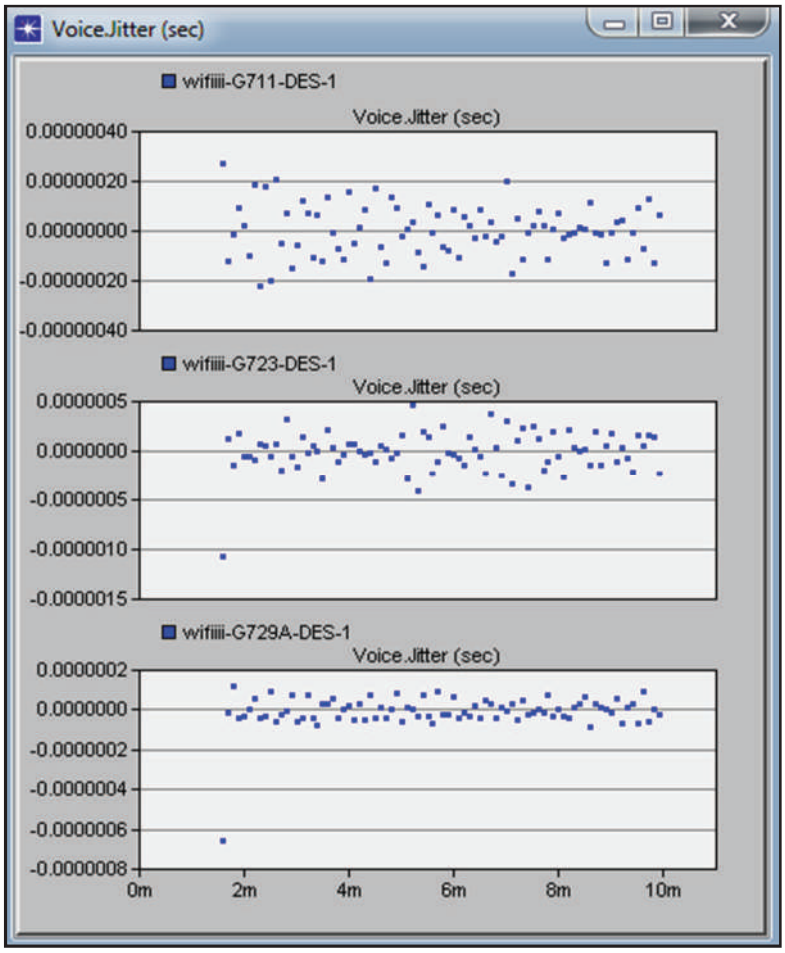


Figure III.21 : Gigue dans les applications VoIP avec différents types de codec dans le réseau WiFi

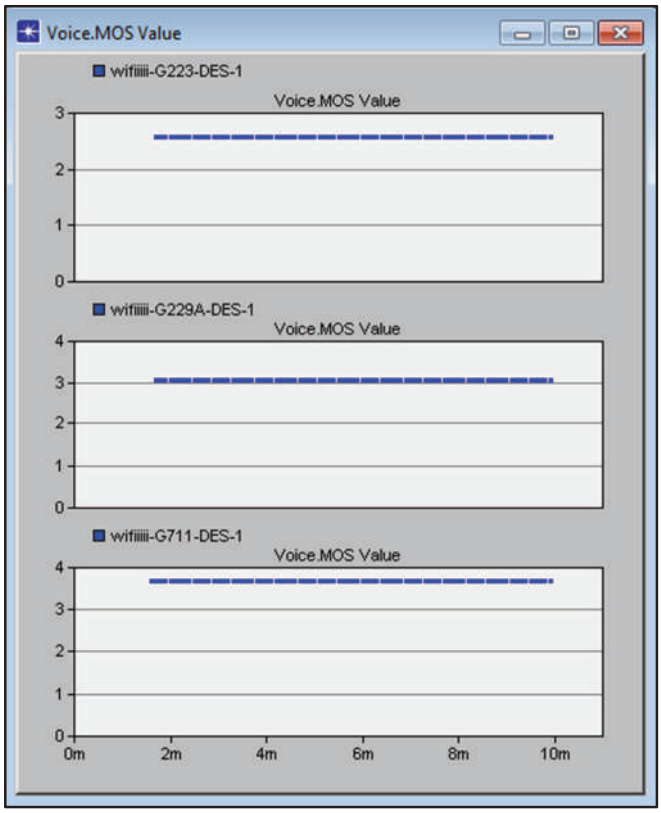


Figure III.22 : Valeur MOS dans les applications VoIP avec différents types de codec dans le réseau WiFi

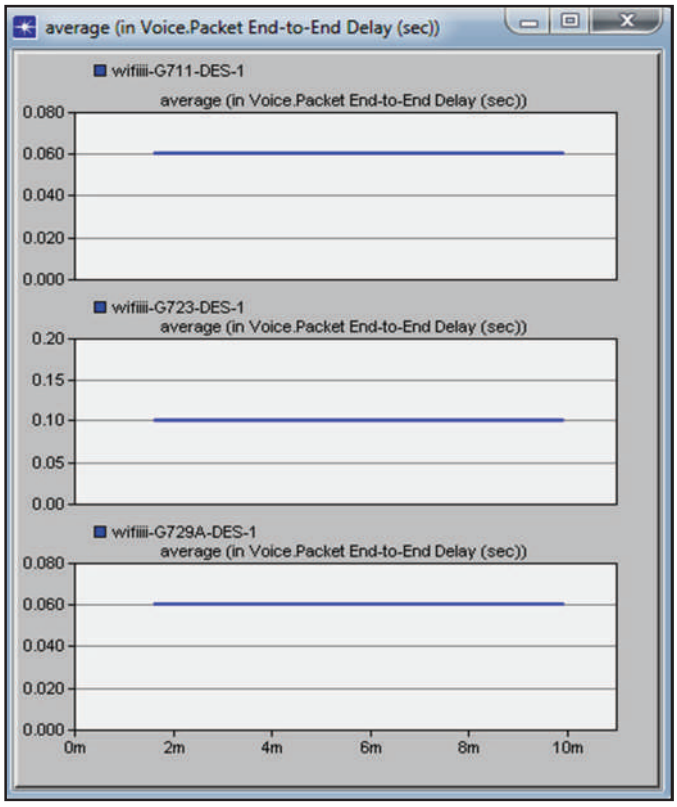


Figure III.23 : Délai dans les applications VoIP avec différents types de codec dans le réseau WiFi

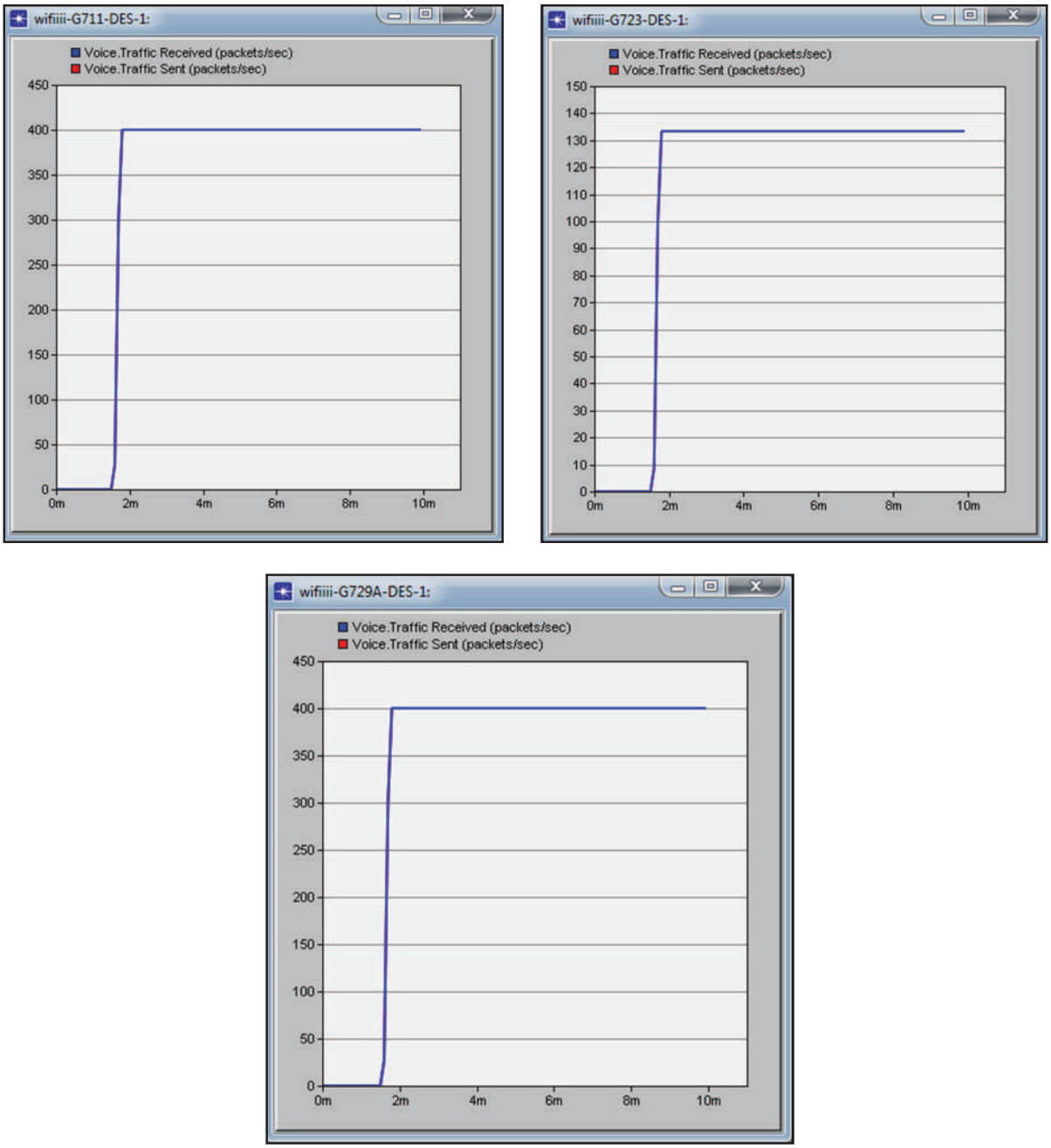


Figure III.24 : Perte de paquets dans les applications VoIP avec différents types de codec dans le réseau WiFi

Vu les résultats représentés dans les figures précédentes, on peut voir que le type de codec utilisé n'influe pas sur la perte de paquets mais quand on parle de la gigue, le délai de bout en bout et la valeur MOS dans le cas de G.711 et G.729 A, ces valeurs sont acceptables par rapport à celles de codec G.723.

Le tableau III.2 nous donne une comparaison globale entre les résultats des différents scénarios dans le cas d'un réseau WiFi.

	Gigue	MOS	Délai	perte de paquets
Courte distance, 2 postes, G.711	0.27µs	3.69	60ms	pas de perte
Longue distance	17.6µs	3.69	66ms	perte de 2.75%
6 Postes	0.45µs	3.69	60ms	pas de perte
10 Postes	1.86µs	3.69	60 ms	pas de perte
14 Postes	0.2ms	2.09	90ms	perte de 19%
G.723	0.47µs	2.57	100 ms	pas de perte
G.729	0.12µs	3.08	60 ms	pas de perte

Tableau III.2 : Gigue, MOS, délai de bout en bout et perte de paquets dans les différents cas de scénarios pour un réseau WiFi

La gigue dans tous les cas reste acceptable alors la resynchronisation des paquets est possible. La valeur MOS reste constante de 3,69 indiquant la qualité moyenne du service VoIP dans les réseaux WiFi de courte distance utilisant le codec G.711 avec 2,6 et 10 clients, et elle est de valeur inférieure à 3,6 dans le cas des codecs G.723 et G729.A et de 14 utilisateurs ce qui implique la dégradation de la qualité de la voix. Le délai de bout en bout de tous les scénarios est acceptable seulement dans les deux scénarios de codec G.723 et de 14 postes où il est un peu élevé. De même, il y a une suppression de paquets dans le cas d'une longue distance et avec 14 postes qu'elle est inacceptable.

II.3. Projet 3 : Réseau *WiMAX*

II.3.1. Modification de la distance :

Les figures III.25, III.26, III.27 et III.28 nous donnent une vue générale sur l'effet de la distance sur la transmission des paquets VoIP dans un réseau WiMAX.

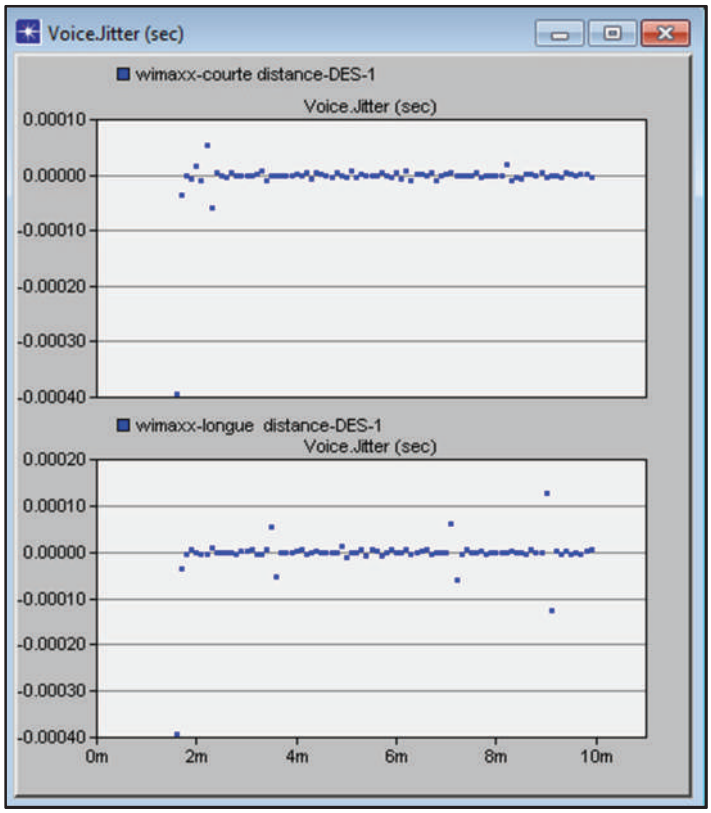


Figure III.25 : Gigue dans les scénarios courte et longue distance dans le réseau WiMAX

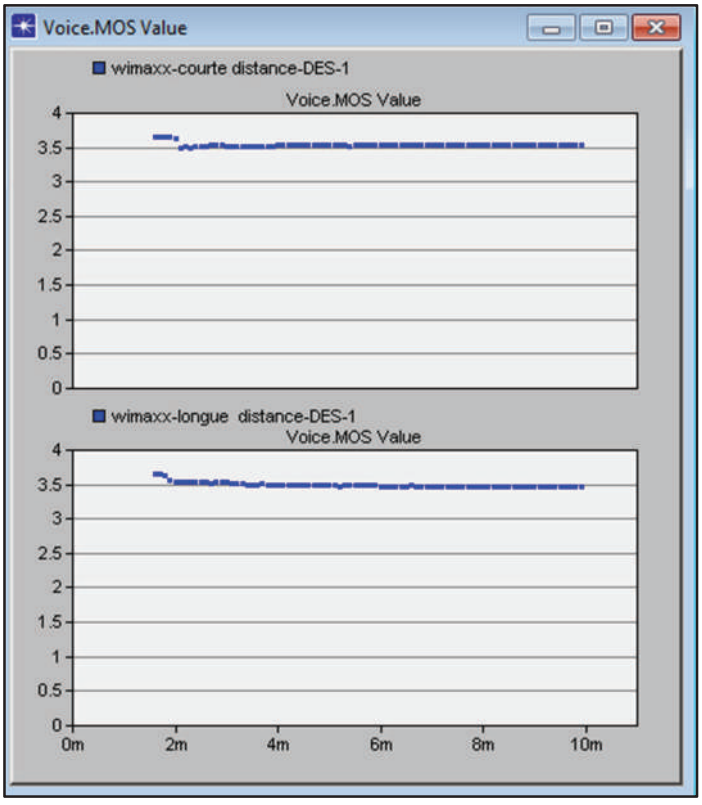


Figure III.26 : MOS dans les scénarios courte et longue distance dans le réseau WiMAX

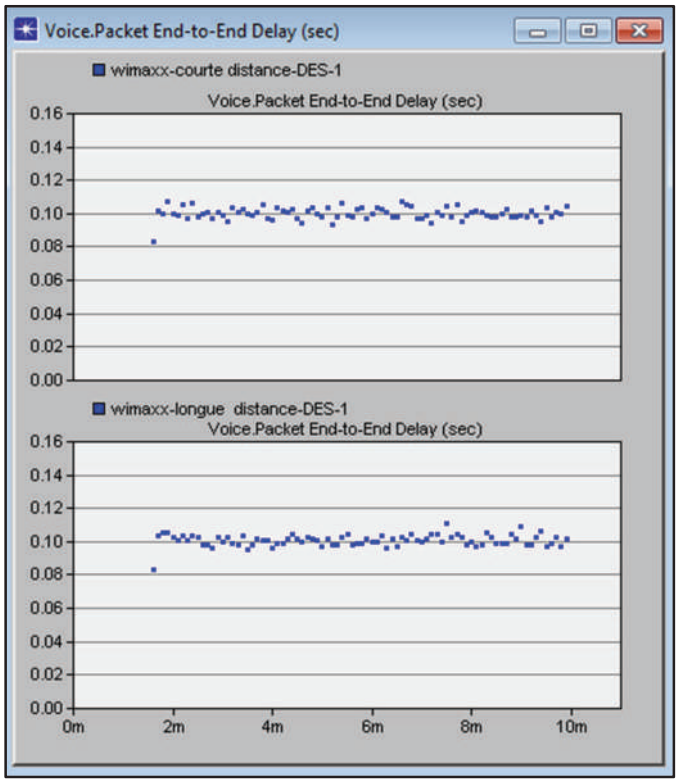


Figure III.27 : Délai de bout en bout dans les scénarios courte et longue distance dans le réseau WiMAX

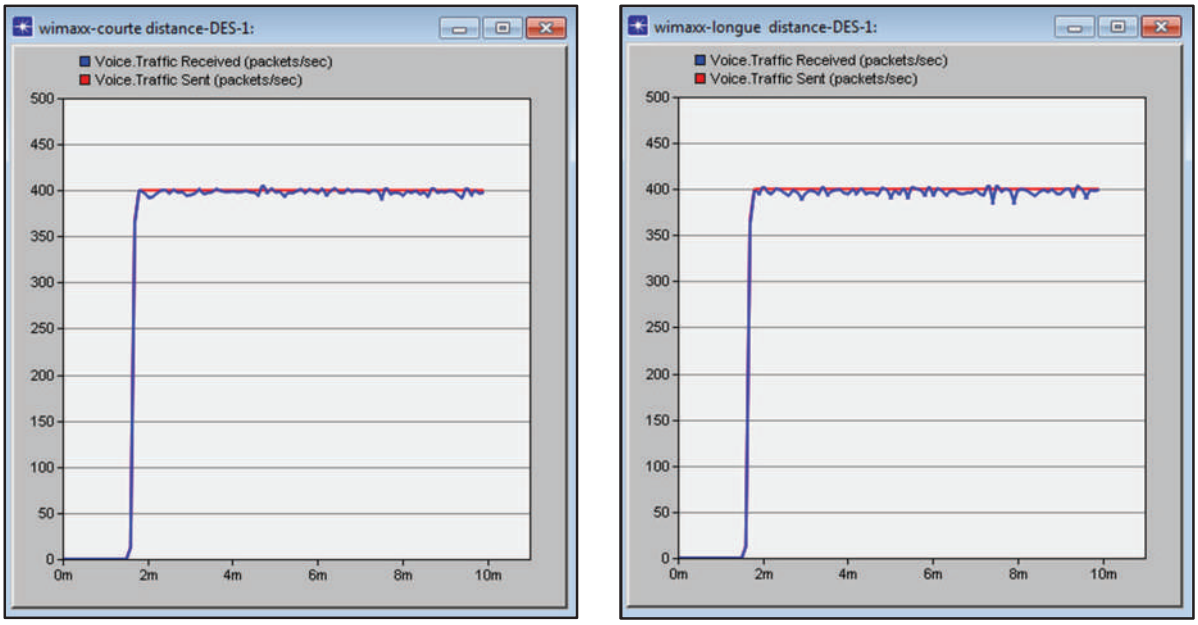


Figure III.28 : Perte de paquets dans les scénarios courte et longue distance dans le réseau WiMAX

La valeur MOS, le délai de bout en bout et la perte de paquets sont inchangeables en fonction de la distance dans nos réseaux WiMAX tandis que la gigue augmente mais elle reste négligeable et acceptable.

II.3.2. Modification du nombre d'utilisateurs :

Les figures III.29, III.30, III.31 et III.32 présentent l'impact du nombre de clients sur la qualité de service VoIP dans un réseau WiMAX.

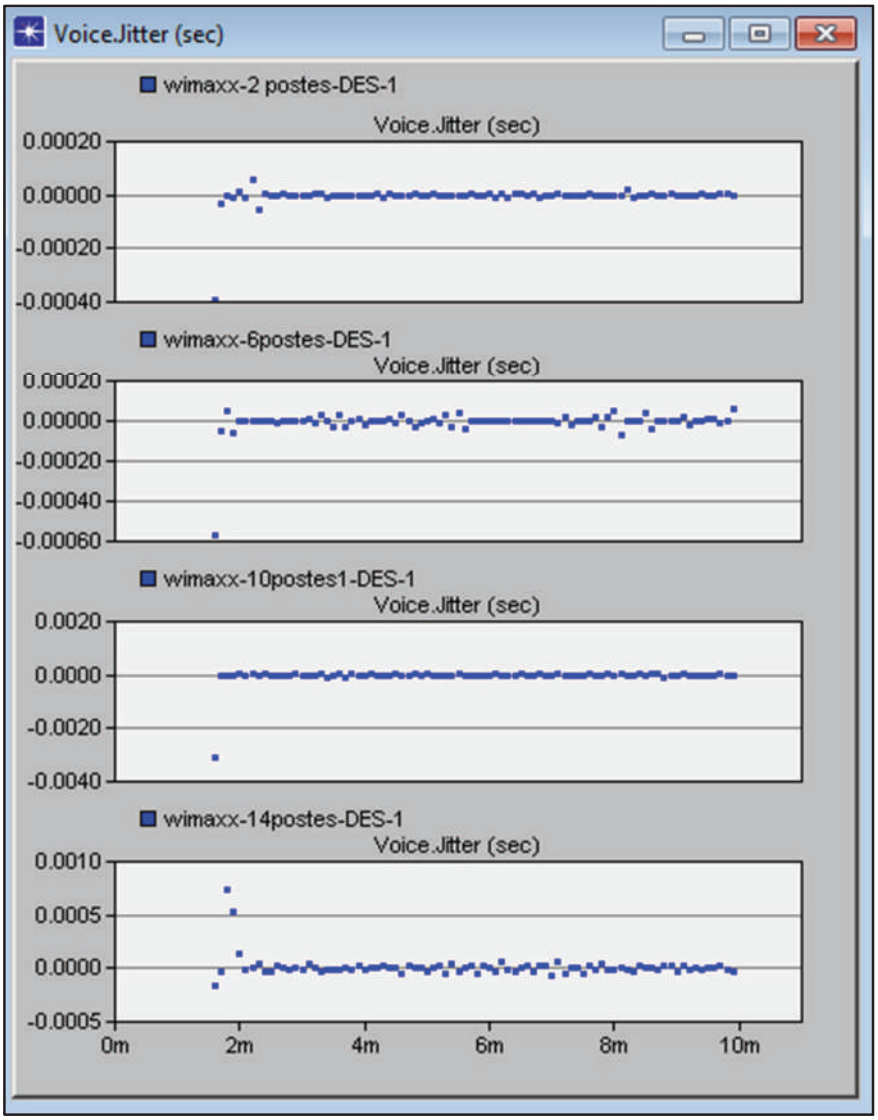


Figure III.29 : Gigue dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiMAX

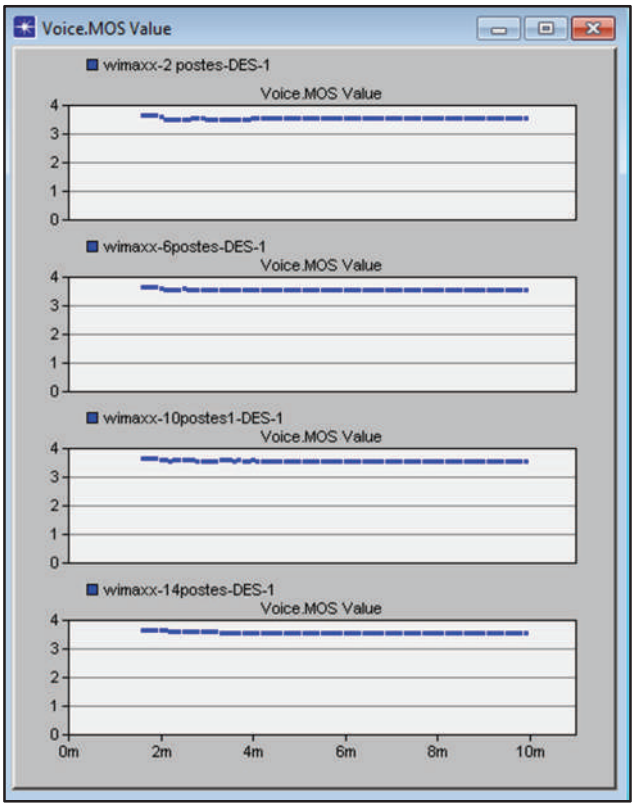


Figure III.30 : Valeur MOS dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiMAX

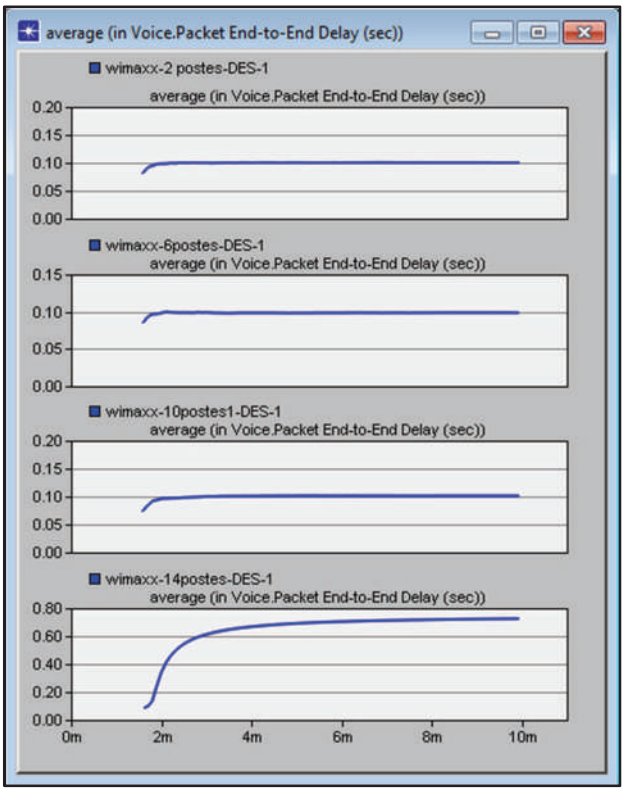


Figure III.31 : Délai de bout en bout dans les scénarios utilisant 2, 6, 10 et 14 postes dans un réseau WiMAX

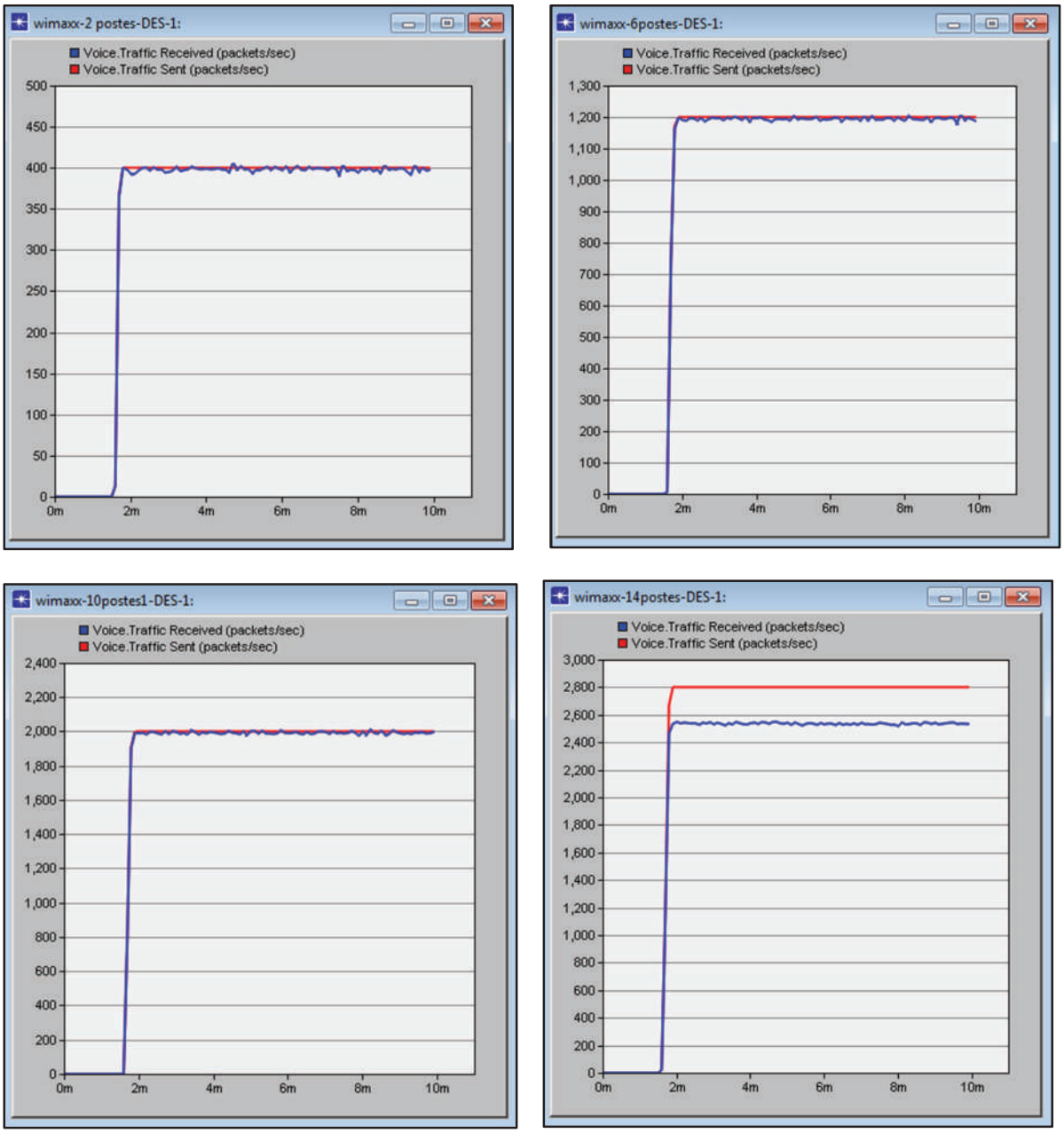


Figure III.32 : Perte de paquets dans les scénarios utilisant 2, 6 et 10, 14 postes dans un réseau WiMAX

Dans le cas de modification du nombre de clients VoIP, on voit d'après les figures ci-dessus que la valeur MOS ne dépend pas du nombre d'utilisateurs dans le réseau WiMAX. Cependant, la gigue, le délai de bout en bout et le taux de paquets perdus augmente avec le nombre de postes, le délai dans ce cas est très élevé et inacceptable.

II.3.3. Modification du type de codec :

Les figures III.33, III.34, III.35 et III.36 nous montrent l'influence du type de codec sur la qualité de la VoIP dans un réseau WiMAX.

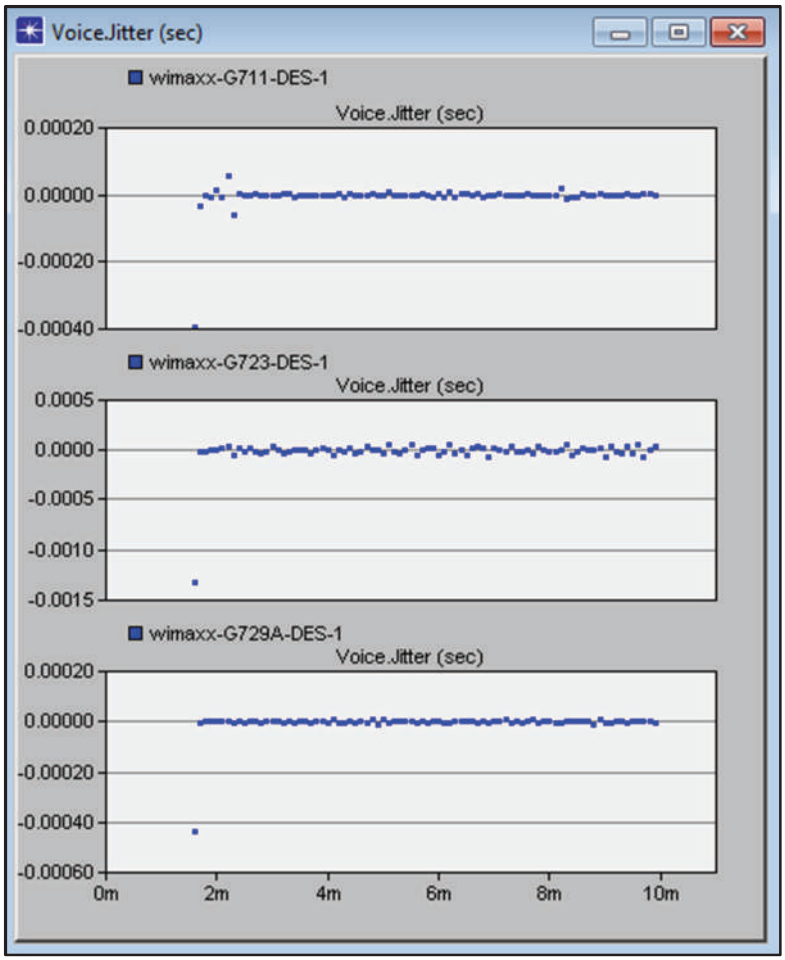


Figure III.33 : Gigue dans les applications VoIP avec différents types de codec dans le réseau WiMAX

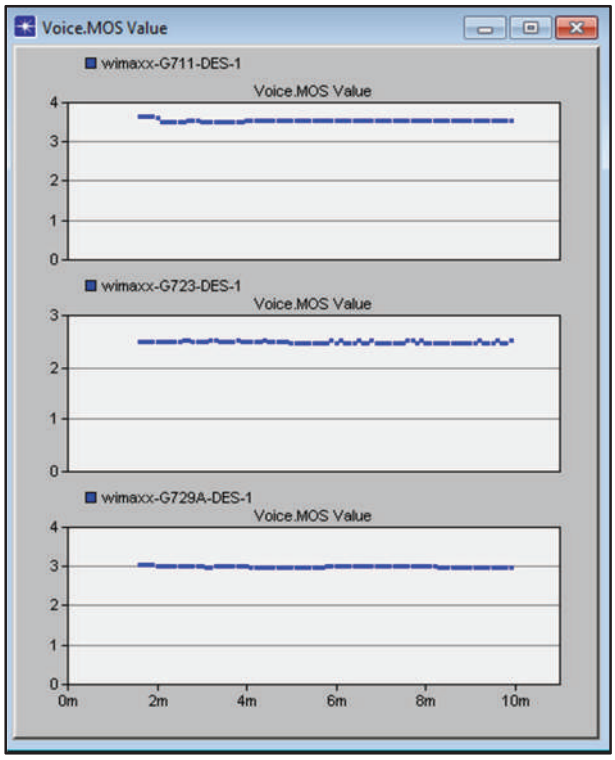


Figure III.34 : Valeur MOS dans les applications VoIP avec différents type de codec dans le réseau WiMAX

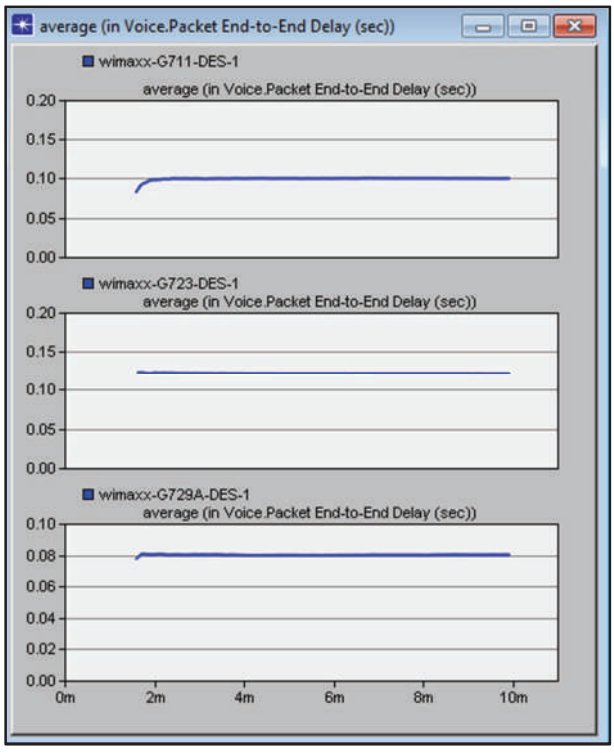


Figure III.35 : Délai de bout en bout dans les applications VoIP avec différents type de codec dans le réseau WiMAX

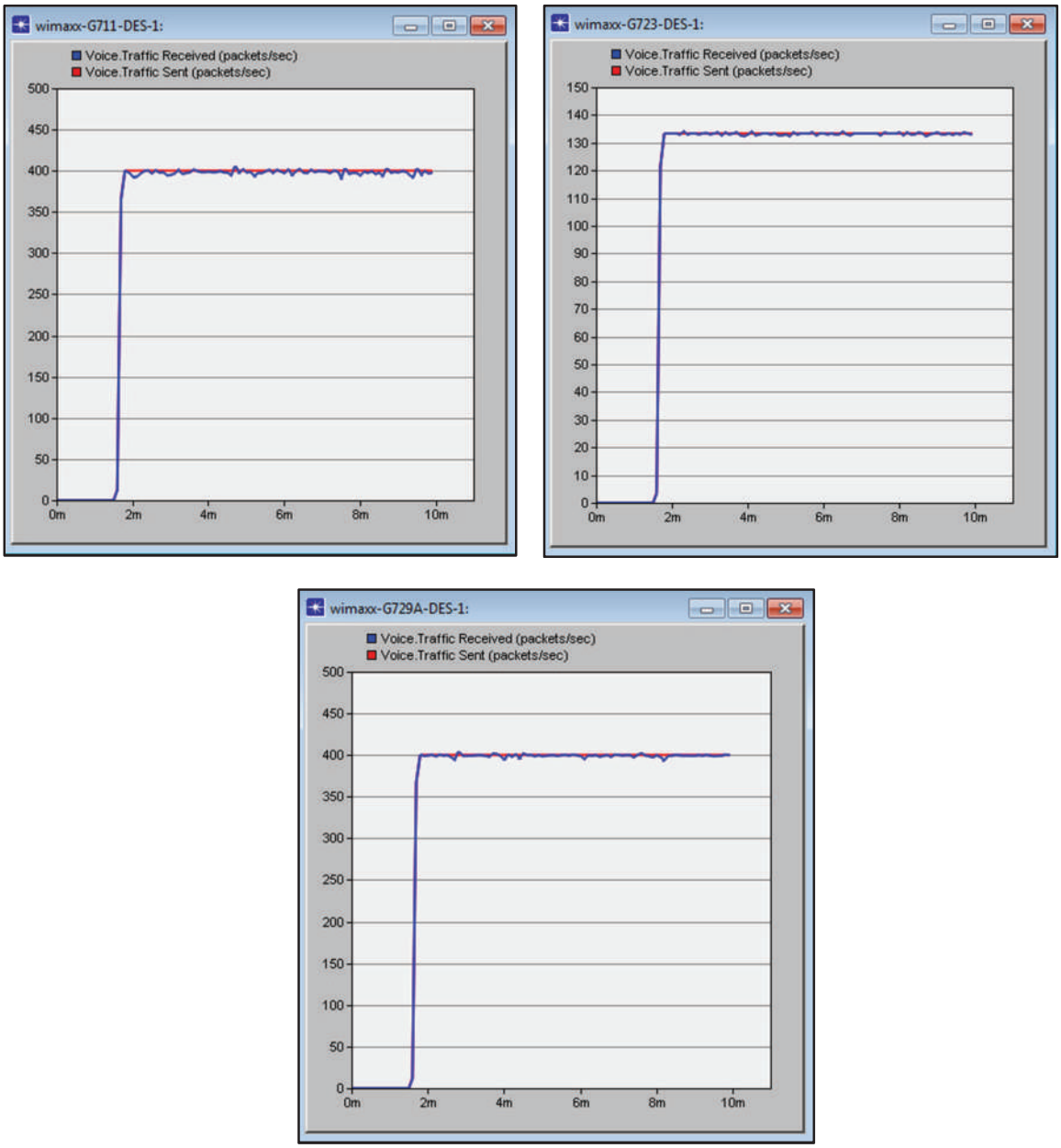


Figure III.36 : Perte de paquets dans les applications VoIP avec différents type de codec dans le réseau de WiMAX

Le codec G.729A est un bon type de codec permettant de donner des valeurs basses et acceptables de la gigue, délai et de perte de paquets alors que le codec G.723 est un mauvais type parce qu'il fournit une valeur MOS de 2,5 (insatisfaite et non recommandée) et un délai plus élevé que celui des codecs G.711 et G729.A.

	Gigue	MOS	Délai	perte de paquets
Courte distance, 2 postes, G.711	55µs	3.55	100ms	faible
Longue distance	127µs	3.55	100ms	faible
6 Postes	60µs	3.55	100ms	faible
10 Postes	86µs	3.55	100ms	faible
14 Postes	741µs	3.55	700ms	environ 9%
G.723	62µS	2.5	120ms	faible
G.729	8µS	3	80ms	faible

Tableau III.3 : Gigue, MOS, délai de bout en bout et perte de paquet dans les différents cas de scénarios pour un réseau WiMAX

En général, dans le WiMAX on a trouvé que la valeur MOS est constante dans tous les réseaux utilisant le codec G.711, si le type de codec est changé la qualité sera diminuée. Lorsqu'on parle de délai, il est le même sauf dans le cas de 14 postes de travail (inacceptable) et dans le cas de codec G.723. La gigue augmente quand la distance et le nombre de clients augmentent et dans tous les cas la perte de paquets est faible.

III. Conclusion :

Dans ce chapitre, nous avons fait des comparaisons entre plusieurs cas y compris longue et coure distance séparant les utilisateurs et le commutateur, avec différents nombres de postes de travail et entre quelques types de codec dans trois réseaux : Ethernet, WiFi et WiMAX.

Les résultats des simulations nous ont indiqués que le codec G.711 est le meilleur parmi les codecs utilisés dans la VoIP pour atteindre une bonne qualité de service.

Les paramètres que nous avons évalués comme la gigue, la note d'opinion moyenne MOS, le délai de bout en bout et la perte de paquets nous aident pour distinguer les avantages et les inconvénients de chaque réseau. Par exemple si on veut communiquer sans fil dans un espace de dimensions limitées, le WiFi est le meilleur choix pour la transmission de la voix sur IP, si on a besoin de transmettre la voix sans fil dans un étendu géographique de quelques kilomètres, la bonne solution est le WiMAX mais il est claire que l'Ethernet reste le plus puissant réseau pour les longues distances et il supporte un grand nombre d'utilisateurs par rapport aux autres réseaux.



Conclusion générale



Conclusion générale

La voix sur IP continuera à être employée et déployée couramment dans les jours qui viennent puisqu'elle a beaucoup d'avantages. Dans ce projet, après avoir établi des études sur la VoIP et ses différents protocoles et standards comme première étape, nous avons réalisé plusieurs simulations en utilisant le fameux logiciel OPNET Modeler.

Nous avons testé plusieurs scénarios avec trois types de réseaux : l'Ethernet, le WiFi et le WiMAX suivi d'une évaluation comparative des facteurs de détérioration de la qualité de service de la VoIP tels que la gigue, le délai de bout en bout, la valeur MOS ainsi que la perte de paquets.

D'après les simulations, nous avons trouvé que la qualité de la voix sur IP dépend de la distance entre les nœuds de communication, le nombre de clients et le type du codec.

Les communications VoIP de longue distance introduisent un délai de bout en bout plus élevé, plus de fluctuation de la gigue, plus de perte de paquets et moins de valeur MOS que les communications de courte distance.

L'augmentation des utilisateurs cause la dégradation dans la qualité de service. De plus, on a trouvé que le codec G711 est le meilleur type de codec à utiliser pour une communication VoIP de haute qualité.

A travers ce travail nous avons appris l'utilisation du logiciel de simulation des réseaux OPNET en choisissant les bonnes configurations pour obtenir les meilleures performances des applications VoIP sur différents types de réseaux d'entreprises.

Et comme perspectives, nous proposons l'évaluation de cette nouvelle technologie de communication, en mode conférence où plusieurs communicants dialogues en même temps. En plus, nous suggérons d'élargir l'application de cette technique sur les communications vidéo et multimédias, où on utilise la compression vidéo (par exemple H.264) au lieu de la compression audio (G 711)

Bibliographie

[1] Khaled Salah, « Deploying VoIP in existing IP Networks », Département de l'information et de l'informatique, université Roi Fahd de Pétrole et minerais.

[2] « VoIP Téléphonie sur IP », cahier de charge, copyright 2008. (En ligne).Disponible : http://www.guidescomparatifs.com/descriptif_voip.asp [Dernier accès : 10 Juin 2013].

[3] SebF, « Tout sur la VoIP ». (En ligne). Disponible : http://www.frameip.com/voip/ [Dernier accès : 10 Juin 2013].

[4] Laurent Ouakil & Guy Pujolle, « Téléphonie sur IP », EYROLLES 2007.

[5] Yannick YANI KALOMBA, «Etude et mise au point d'un système de communication VOIP : application sur un PABX-IP open source "cas de l'agence en douane Getrak" », Université protestante de Lubumbashi - Ingénieur en réseaux et télécoms 2009.

[6] Claude Servin, « Réseau et télécoms », DUNOD 2003.

[7] Jeffrey Tam, Luke Dang & Jason Tsai, « Exploration of VoIP using Ethernet and Wi-Fi networks under different scenarios », université de Simon Fraser, Canada.
Disponible: http://www.sfu.ca/~kta2

[8] Rebha Bouziada, « étude et mise en place d'une solution VOIP sécurisée », mémoire de projet de fin d'étude pour l'obtention du master professionnel en nouvelles technologies des télécommunications et réseaux, 2010-2011

[9] Benson Lam, Winfield Zhao & Mincong Luo, « Communication networks analysis on VoIP using opnet », projet final 2009, université de Simon Fraser.
Disponible: http://www.sfu.ca/~btl2/web.html

[10] Guy Pujolle, « Les Réseaux », 5ème edition, EYEROLLS

[11] Shahid Ali & Bilal Zahid Rana, « OPNET Analysis of VoIP over MPLS VPN with IP QoS », thèse de master 2009, école de l'informatique Blekinge. Disponible : www.bth.se

[12] « Simulation des réseaux », TP OPNET, module TC6, Master 1 Informatique, université de TOULOUSE III.

[13] « OPNET», chapitre 4 (En ligne). Disponible : http://malm.tuxfamily.org/doc/qr_chap4_opnet.htm . Dernier accès : 10 Juin 2013

[14] Deroussen Nadège & Laplagne Hervé, « projet OPNET », cours de Télécom 2 ème année, institut des sciences de l'ingénieur de Toulon.

[15] Jeremy Yoo, « Performance evaluation of voice over IP on Wimax and WiFi based networks », projet final 2009, université de Simon Fraser. Disponible: http://www.sfu.ca/~jty/ensc427/ . Dernier accès : 10 Juin 2013