الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
المركز الجامعي لعين تموشنت
Centre Universitaire Belhadj Bouchaib d'Ain-Temouchent
Institut de Technologie
Département de Génie Electrique

Mémoire de Fin d'Etudes

En vue de l'obtention du diplôme de Master Académique

Domaine : SCIENCES ET TECHNOLOGIES

Filière : TELECOMMUNICATION

Spécialité : Réseaux et Télécommunications

Thème :

Mise en œuvre d'une solution de gestion de la qualité de service Voix sur IP (VoIP)

Présenté Par :

- ALKADER Habib
- OGOUBI Komivi Shine

Soutenu en Septembre 2020 devant le Jury :

MOULESSEHOUL Wassila	M.C.B	C.U.B.B (Ain Temouchent)	Présidente
BENGANA Abddelfatih	M.C.B	C.U.B.B (Ain Temouchent)	Examinateur
SLIMANE Zohra	M.C.A	C.U.B.B (Ain Temouchent)	Encadrante
DEBBAL Mohammed	M.C.A	C.U.B.B (Ain Temouchent)	Co-Encadrant

Année universitaire 2019/2020

Dédicace

Au nom d'Allah, le Tout Miséricordieux, le Très Miséricordieux, Je dédie ce modeste travail :

Aux deux personnes qui me sont les plus chères au monde, mes chers parents, auxquels je tiens à exprimer ma profonde gratitude de leur soutien incessant, de leur patience incommensurable, de leurs sacrifices inestimables, et surtout de leur encouragement.

A mon frère Alkader Souleymane et ma sœur Alkader Mounia.

A mon binôme Ogoubi Komivi Shine et toute sa famille.

Alkader Habib

La vie n'est qu'un éclair,
Et un jour de réussite est un jour très cher.

A mon cher père,
et ma chère mère.

Pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance.
Et pour leurs patiences et leurs sacrifices. Je remercie le bon et miséricordieux Dieu de nous avoir permis de réaliser ce travail.

A mon cher frère Ogoubi Enyo Light ;

A mon binôme Alkader Kabib et toute sa famille ;

A nos encadreurs et tous les professeurs de la c.u.a.t ;

A tous ceux qui m'aiment et que j'aime ;

A tous mes ami(e)s.

Je dédie ce mémoire.

Ogoubi Komivi Shine

Résumé

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

Dans ce mémoire de Master, nous déployons une plateforme VoIP utilisant le protocole IPV4. A cette plateforme, nous y ajoutons un serveur FTP ainsi qu'un client FTP afin de pouvoir accéder aux fichiers à distance et être capable de les modifier.

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

Nous utilisons les applications de simulateur de réseau GNS3 et Vmware qui est une machine virtuelle

Mais tout d'abord avant de passer à l'étape de simulation nous vous expliquons en détails la signification de la VoIP, de ses avantages et inconvénients, des protocoles utilisés dans ce dernier ainsi que des différentes particularités.

Nous vous expliquons aussi la signification de la qualité de service (QoS), A quoi sert-t-il ? et comment l'implémenter dans un réseau grâce à des commandes spécifiques.

Mots clés :

Internet protocol, VoIP, FTP, CME, protocole IPV4, simulateur de réseau, GNS3, Vmaware, machine virtuelle.

Abstract

The convergence of communications networks based on IP (Internet Protocol) has been fostered by the advent of the packetization of voice and image. In this context, VoIP (Voice over Internet Protocol) is becoming more and more preponderant and has become nowadays an interesting challenge for the development of communication networks.

In this paper by Masters, we deploy a VoIP platform using the IPV4 protocol. To this platform, we add an FTP server as well as an FTP client in order to be able to access files remotely and be able to modify them.

After implementing the hardware platform, the deployed solution is based on the Call Manager Express (CME) of the manufacturer Cisco, a choice dictated by the availability of hardware offering the possibility of experimental implementation in concrete situations.

We use the GNS3 network simulator applications and Vmware which is a virtual machine.

But first of all, before moving on to the simulation stage, we explain in detail the meaning of VoIP, its advantages and disadvantages, the protocols used in it and the various particularities.

We also explain the meaning of Quality of Service (QoS), what is it used for, and how to implement it in a network using specific commands.

Keywords:

Internet protocol, VoIP, FTP, CME, IPV4 protocol, network simulator, GNS3, Vmware, virtual machine.

Remerciements

Au terme de ce projet de fin d'études, on adresse nos sincères remerciements à Monsieur DEBBAL Mohammed et Madame SLIMANE Zohra, nos encadreurs de la CUAT, pour nous avoir proposé ce projet et pour leur encadrement.

Mes remerciements s'adressent également à l'administration et aux professeurs de la CUAT pour les moyens qu'ils ont mis à notre disposition afin d'élaborer ce travail.

On souhaite exprimer enfin notre gratitude et nos vifs remerciements à nos familles et nos amis pour leurs soutiens.

Pour finir, on remercie les membres du jury qui ont accepté d'évaluer notre projet. Nous leurs présentons toutes nos gratitudes et nos profonds respects.

TABLE DE MATIÈRES

Chapitre 2 : Eléments de base de l'implémentation de la Qualité de Service

Liste des figures

Acronymes

A

ACL	Acces Control List
ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding
ARQ	Admission ReQuest
ATM	Asynchronous Time Switching (commutation temporelle asynchrone)

B

BE	Best Effort

C

CAA	Commutateurs à Autonomie d'Acheminement
CAN	Convertisseur Analogique Numérique
CAR	Committed Access Rate
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CFI	Canonical Format Indicator
CL	Commutateurs Locaux
CME	Cisco callManager Express
CNA	Convertisseur Numérique Analogique
CoS	Class of Service
CRC	Contrôle de Redondance Cyclique
CTP	Commutateur de Transit Principal
CTS	Commutateurs de Transit Secondaires

D

DHCP	Dynamic Hot Configuration Protocol
DiffServ	Differentiated Services
DS	DiffServ
DSCP	Differentiated Services Code Point

E

ECN	Explicit Congestion Notification
EF	Expedited Forwarding

F

FAI	Fournisseur d'Accès Internet
FRF	Frame Relay Fragmentation
FTP	File Transfert Protocol

G

GPS	Global Positioning System
GRQ	Gatekeeper ReQuest
GS	Guaranteed Service
GSM	Global System for Mobile

H

HTTP HyperText Transfert Protocol

I

IAX Internet Asterisk eXchange
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IIS Internet Integrated Services
IOS Iphone OS
IP Internet Protocol
IPBX Internet Protocol Branch eXchange
IPV4 Internet Protocol Version 4
IPV6 Internet Protocol Version 6
IPX Internetwork Packet eXchange
ISDM Informed Shared Decision Making
ISDN Integrated Service Digital Network
ISP Internet Service Provider
ITU International Telecommunication Union

L

LAN Local Area Network
LRQ Location ReQuest

M

MC Multipoint Controller
MCU Multipoint Control Unit
MIC Modulation par Impulsion et Codage
MG Media Gateway
MGC Media Gateway Controller
MGCP Media Gateway Control Protocol
MLP MultiLink point-to-point Protocol
MP Multipoint Processor
MPLS MultiProtocol Label Switching
MQC Modular Quality of sevice Command-line interface

N

NAT Network Address Translation
NBAR Network-Based Application Recognition
NGN (New Generation Network

P

P2P Peer 2 Peer
PABX Private Automatic Branch eXchange
PBR Policy-Based Routing
PBX-IP Protocol Branch eXchange-Internet Protocol
PC Portable Computer
PCP Priority Code Point
PME Petite et Moyenne Entreprise
PHB Per-Hop Behaviour
PPP Point-to-Point Protocol
PSTN Public Switched Telephone Network

Q

QoS Quality of Service

R

RAS	Registration Admission Status
RJ45	Registered Jack 45
RNIS	Réseau Numérique à Intégration de Service
RRQ	Registratio ReQuest
RSVP	Ressource reSerVation Protocol
RTC	Reseau Téléphonique Commuté
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol

S

SCTP	Stream Control Transmission Protocol
SDH	Synchronous Numerical Hierarchy
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLS	Service Level Specification
STUN	Simple Traversal of Udp through Nats

T

TCI	Tag Control Identifier
TCP	Transmission Control Protocol
TFTP	Trivial File Transfert Protocol
ToIP	Telephony over Internet Protocol
ToS	Type of Service
TPE	Très Petite Entreprise
TPID	Tag Protocol IDentifier

U

UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
USA	United States of America

V

VID	Vlan IDentifier
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol

W

WAN	Wide Area Network
WRED	Weighted Random Early Detection

Z

ZAA	Zone à Autonomie d'Acheminement
ZTP	Zone de Transit Principal
ZTS	Zone de Transit Secondaire

Introduction générale

L'histoire de la communication est aussi vielle que l'histoire de l'humanité. Depuis l'antiquité, l'homme a eu besoin de communiquer. C'est-à-dire de transmettre une information à travers divers procédés afin de faire parvenir le message au destinataire. Ainsi, au fil du temps, l'homme à travers les efforts intellectuels aussi bien que physiques à découvert et simplifier les méthodes de communication afin de réduire les distances entre les interlocuteurs et de permettre la rapidité de l'acheminement de l'information.

Au début du 20ème siècle, l'arrivée de l'électronique a créé une véritable révolution pour les télécommunications. Cette époque est marquée par l'innovation de l'électricité, des composants, circuits électroniques de base ayant des bonnes performances qui constituent un progrès des télécommunications causée par la convergence de l'informatique et des technologies des télécommunications. Ces progrès sont à l'origine de la naissance d'autres technologiques de communications à savoir la radiomessagerie, la téléphonie mobile, les réseaux de fibre optique, Internet et enfin la téléphonie sur IP (VoIP).

Avènement de la voix sur IP (VoIP) a marqué une véritable révolution dans le monde de la communication. En effet, la voix sur IP est une technologie plus performante qui se base sur le transport de la voix en mode paquet via protocole IP sur réseau privé ou Internet ce qui la distingue des réseaux téléphoniques traditionnels pour l'acheminement des appels téléphonique.

Etant un protocole de niveau 3 du modèle ISO, L'IP est un protocole appartenant à la couche Réseau responsable de segmenter les données numérisées et les acheminer vers le réseau d'où le principe de fond qui est la commutation de paquets. De même, il assure un meilleur acheminement des datagrammes, ce qui permet un bon niveau de qualité de transport de la voix.

Par conséquent, la Téléphonie sur IP est considérée aujourd'hui comme une des plus importantes révolutions dans le domaine des Télécommunications, Au-delà de la nouveauté technique, il s'adapte parfaitement à tous types de structures grâce à sa grande flexibilité, sa possibilité de fusion des réseaux IP et téléphonique conduisant réduction des matériaux nécessaires pour la gestion de deux réseaux, Ainsi qu'une baisse importante des coûts de communication avec la possibilité d'implémenter de nouveaux services utilisant la voix et les données.

Avec les progrès de la technologie des télécommunications, la voix sur IP qui est une technologie permet au gens de se parler à travers Internet ainsi que par Intranet (réseau local). Elle nécessite beaucoup de critères et caractéristiques dont un faible coût de communication. Avec le temps, grâce à l'extension des PABXs software a permis de bénéficier d'une grande flexibilité, d'une bonne intégration du monde des données de la voix. On remarque diverses solutions libres comme Asterisk basées sur les protocoles libres (SIP, H323, …), en outre, aucun protocole ne s'est imposé comme standard de la VoIP, même si le protocole SIP, est le plus d'actualité.

Dans ce travail nous nous intéressons à la téléphonie sur IP, l'étude des différents protocoles de VoIP, les architectures et la mise en place d'une solution de la voix sur IP basée sur des outils open source, précisément le serveur Asterisk, GNS3.

CHAPITRE 1

ETUDE THEORIQUE DE LA VOIX SUR IP

1. Introduction à la téléphonie :

❖ La téléphonie :

La téléphonie est un ensemble de techniques et opérations concernant la transmission de son, la voix humaine tout en respectant sa qualité et son timbre à une distance entre deux points. Elle utilise comme support des lignes électriques à travers lesquelles un courant analogue aux signaux sonores. Afin d'acheminer le signal vocal (parole issue d'une onde acoustique) entre deux ou plusieurs utilisateurs. Le signal sonore (signal analogique) doit subir diverses transformations afin de donner un signal électrique pour être acheminé chez le destinataire avec une restitution du signal électrique en signal sonore (signal analogique). Nous verrons plus amplement ce que sont le téléphone, microphone et l'écouteur qui exécutent cette opération.

❖ Le téléphone :

Le téléphone est un dispositif de communication, de base conçue pour transmettre la voix humaine et permettre une conversation à distance. Afin que cela puisse marcher, le téléphone doit indispensablement avoir une infrastructure qu'elle soit terrestre ou spatiale : le réseau téléphonique.

Les composants internes du téléphone permettant une conversation du poste téléphonique assurant l'échange de parole entre les deux terminaux sont :

❖ Le microphone :

Est un transducteur électroacoustique, c'est-à-dire un dispositif capable de convertir l'énergie (signal acoustique en signal électrique). Une membrane électronique étant sensible vibre sous l'effet des ondes sonores ou acoustiques qui produisent un signal électrique variant au rythme de voix ou du signal acoustique perçu. Ces oscillations sont transformées en signal électrique qui provoque le déplacement de la membrane qui agit sur une bobine produisant ainsi une tension induite. Sa fonction principale est la transformation d'ondes acoustique en variation de tension induite.

Son rôle capital est le changement du signal acoustique en le convertissant en signal électrique qui est une variation de tension.

❖ L'écouteur :

Les écouteurs fonctionnent sur le même principe qu'un haut-parleur, il restitue le signal reçu en signal acoustique en la transformant en énergie mécanique imposant un mouvement vibratoire à l'air ambiant. Le signal électrique reçu passe par une bobine qui se trouve dans un champ magnétique et de ce fait, la membrane réagit et les ondes acoustiques deviennent audibles.

Son rôle capital est le changement du signal électrique en le convertissant en vibrations sonores audibles à l'oreille.

Historique de la téléphonie :

Du premier télégraphe de Chappe en 1790 au RTC actuel, dès la fin du XVIII siècle l'histoire des communications a connu un grand essor et une propulsion dans le monde de la technologie et électroniques. Nous noterons quelques grandes dates qui auront marqué l'histoire telles que :

- 1794 : L'ingénieur Français Claud Chappe crée le premier télégraphe.4
- 1837 : Premier télégraphe électrique inventé par Samuel Morse.
- 1876 : Le téléphone est inventé par Graham Bell.
- 1889 Almon B. Strowger (USA) invente le premier « sélecteur » automatique et donne
- Ainsi naissance à la commutation téléphonique automatique
- 1892 : Apparition du téléphone Mildé, durant la même année Almon B. Strowger invente le premier « sélecteur » automatique et donne ainsi naissance à la commutation téléphonique automatique.
- 1910 : Le téléphone Marty fait son apparition : le récepteur et le microphone sont liées sur le combiné.
- 1920 : Naissance du téléphone à cadran : les chiffres de 0 à 9 permettent de composer directement le numéro du correspondant, sans avoir à passer par un intermédiaire.
- 1930 : Création du combiné en Bakélite par le Suédois Ericsson.
- 1938 Alec Reeves (Français) dépose le brevet des futurs systèmes à modulation par Impulsion et codage (MIC) : quantification et échantillonnage du signal à intervalles Réguliers, puis codage sous forme binaire.
- 1938 : Dépôt du brevet des systèmes à modulation par impulsion et codage (MIC) par le Français Alec Reeves.
- 1962 : Lancement des premiers systèmes de transmission multiplex de types MIC aux Etats-Unis qui permettent une liaison à 24 voies entre centraux téléphoniques, en même temps en France on installe des MIC à 32 voies.
- 1970 : La mise en œuvre des centraux téléphoniques publics en commutation électronique temporelle.
- 1979 Lancement du minitel en France.
- 1987 Le RNIS est mis en service en France.
- 1990 : Apparition de nouveaux concepts tels que la commutation temporelle asynchrone (ATM) et la hiérarchie numérique synchrone (SDH).
- 1993 : Apparition du téléphone cellulaire 2G.
- 2010 : Avènement des smartphones et des nouveaux concepts intégrés dont le GPS, la GSM ainsi que les systèmes d'exploitation (IOS et Android).
- 2010 à nos jours : Régressions progressive des téléphones fixes faisant place aux smartphones.

1.1. La téléphonie et la voix sur IP : [1]

Introduction :

L'Internet a révolutionné le monde des réseaux de communication comme rien d'autre auparavant. Elle donne naissance à la synthèse de communication et Informatique qui donne le réseau informatique qui se trouve être la source de l'émergence de la ToIP (Telephony over Internet Protocol ou Téléphonie sur IP). Cette dernière a pour objectif d'assurer le transport de la voix sur un réseau IP (Internet Protocol) en l'encapsulant dans des paquets IP, par le biais de la technique de VoIP (Voice over IP) qui offre des divers avantages telles que : le coût et la flexibilité du réseau.

Nous allons établir son importance pour les entreprises, de faire converger le réseau de données IP et le réseau téléphonie, avec une optique sur le principe de fonctionnement de ces deux technologies, les différences qui existent entre elles, ainsi que les protocoles associés à la VoIP permettent la signalisation et le transport de données.[1, 2]

1.1.1. Définition :

Etymologiquement, il convient de préciser que le terme téléphonie sur internet ou téléphonie IP étant corrélatif à la téléphonie utilisant la communication par paquets et les technologies liées à l'internet (IP pour Internet Protocol).

La VoIP (Voice over IP) est la technique qui permet de numériser la voix puis d'acheminer sous forme de paquets sur des réseaux compatibles IP (réseau privé ou Internet). Pour établir une communication entre des individus afin d'avoir un réseau pour la voix et les données, il impératif de relier des terminaux (Phone), ainsi que des logiciels sur PC connecté sur le même réseau IP appelé (SOFTPHONE).[1, 3]

1.1.2. Principe de fonctionnement de la VoIP :

Depuis de nombreuses années, il est possible de transmettre un signal à une destination éloignée sous forme de données numériques. Avant la transmission, il faut numériser le signal à l'aide d'un CAN (Convertisseur Analogique-Numérique). Le signal est ensuite transmis, pour être utilisé, il doit être transformé de nouveau en un signal analogique, à l'aide d'un CNA (Convertisseur Numérique-Analogique).

La VoIP fonctionne par numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Le signal numérique est plus tolérant au bruit que l'analogique.

Les réseaux TCP/IP sont des supports de circulation de paquets IP contenant un en-tête (pour contrôler la communication) et une charge utile pour transporter les données.

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

1.1.3. Principe de fonctionnement de la ToIP : [1, 4]

La mise en place d'une communication ToIP (téléphonique sur IP) se déroulent en cinq grandes étapes suivantes :

- **Mise en place de la communication :**

Une signalisation démarre la session. Le premier élément à prendre en compte est la localisation du récepteur (User Location). Ce procédé se fait par une conversion de l'adresse du destinataire (adresse IP ou adresse téléphonique classique) en une adresse IP ou machine qui puisse joindre le destinataire (qui peut être aussi destinataire). Le récepteur peut être un combiné téléphonique classique sur un réseau d'opérateur télécoms ou une station de travail (lorsque la communication s'effectue d'un combiné téléphonique vers un PC). Le protocole DHCP (Dynamic Hot Configuration Protocol) et les passerelles spécialisées (Gatekeeper) sont employés à cette fin.

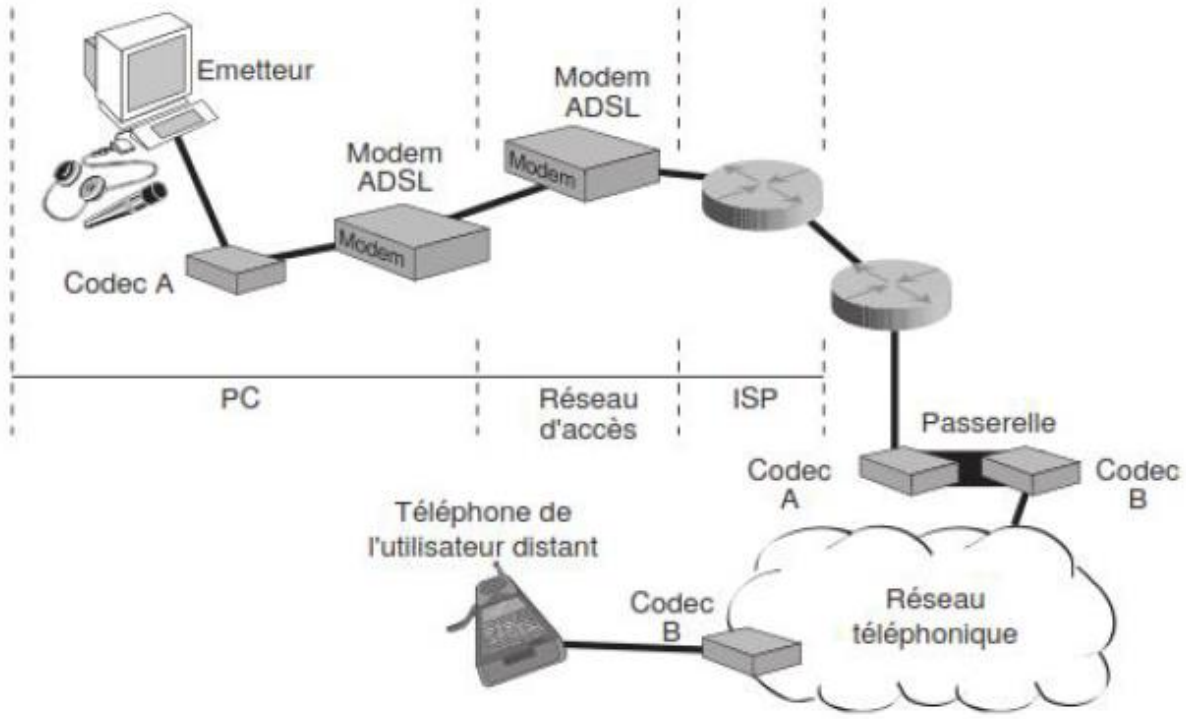


Figure 1 : *les équipements à traverser par une communication téléphonique sur IP.[4]*

- **Etablissement de la communication :**

Cette étape se déroule par le consentement du terminal destinataire, que ce dernier soit un téléphone, une boîte vocale ou un serveur web. Plusieurs protocoles de signalisation peuvent être utilisés pour cette étape, mais le protocole SIP (Session Initiation Protocol) de l'IETF (Internet Engineering Task Force). Le SIP étant un protocole d'initiation de session. Une requête SIP contient un ensemble d'en-têtes, qui décrivent l'appel, suivis du corps du message, qui contient la description de la demande de session. SIP est un protocole client-serveur, qui utilise la syntaxe et la sémantique de HTTP. Le serveur gère la demande et fournit une réponse au client. Trois types de serveurs gèrent différents éléments : un serveur d'enregistrement (Registration Server), un serveur relais (Proxy Server) et un serveur de redirection (Redirect Server). Ces serveurs travaillent à trouver la route : le serveur proxy détermine le prochain serveur (Next- Hop Server), qui, à son tour, trouve le suivant, et ainsi de suite. Des champs supplémentaires de l'en-tête gèrent des options, comme le transfert d'appel ou la gestion des conférences téléphoniques.

- **Transport de l'information téléphonique :**

Cette étape se déroule grâce au protocole RTP (Real-time Transport Protocol) qui se charge du transport de l'information téléphonique proprement dit. Sa fonction principale est d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie de façon à restituer l'information avec ces caractéristiques initiales (vérification du synchronisme, des pertes, etc.) il permet de corriger les défaillances du réseau, c'est un protocole de niveau transport.

- **Changement de réseau :**

Cette étape, est caractériser par un lieu de transit important de la ToIP qui est constitué par les passerelles, qui permettent de passer d'un réseau à transfert de paquets à un réseau à commutation de circuits, en gérant les difficultés d'adressage, de signalisation et de transcodage que cela pose. Ces passerelles ne cessent de se multiplier entre FAI (Fournisseur d'Accès Internet) et opérateurs télécoms.

- **Arrivée au destinataire :**

Le protocole SIP se charge encore une fois d'envoie une requête à la passerelle pour déterminer s'il y'a possibilité d'effectué une liaison circuit de façon à atteindre le destinataire. Théoriquement, toutes les passerelles sont aptes à appeler n'importe quel numéro de téléphone. Toutefois, afin de minimiser les coûts, il serait judicieux de choisir une passerelle locale, qui assure la partie du transport sur le réseau téléphonique classique et le moins coûteux possible.

1.1.4. Architecture de la ToIP/VoIP :

Depuis plusieurs années, les éditeurs de logiciels cherchent à utiliser le réseau informatique pour pouvoir transmettre la voix. Grâce à l'apparition de protocoles comme le H323 ou SIP, les autocommutateurs se sont vus adopté la notion IP à leurs solutions dans une optique de convergence voix-données. Au départ, cette convergence a pris la forme de carte optionnelle s à intégrer dans les commutateurs privée (PABX) existants, pour être proposée aujourd'hui de façon native. C'est ce qu'on appelle la téléphonie sur IP (ToIP).

En offrant la possibilité de faire transiter les communications de voix sur des réseaux de donnée, la ToIP marque la fin d'une cohabitation entre deux réseaux distincts, très différents, du point de vue de la gestion et la technologie. Ce transfert de la totalité des flux sur une infrastructure unique marque les prémices d'une convergence des réseaux multiservices existants (voix, données, vidéo).

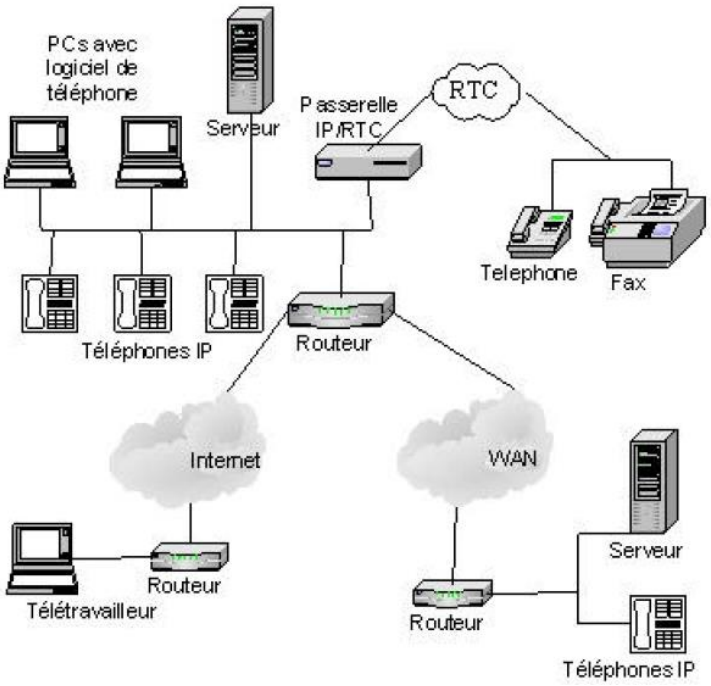


Figure 2 : *Convergence des réseaux voix-données.[5]*

Le schéma ci-dessus décrit de façon générale la topologie d'un réseau téléphonie IP. Elle est constituée toujours des terminaux, un serveur de communication et une passerelle menant à d'autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour assurer une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/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.
- **La passerelle :** il s'agit d'une interface entre le réseau commuté et le réseau IP.
- **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.
- **Les terminaux :** Des PC ou des téléphones VoIP.
- **L'IPBX ou PABX7-IP :** C'est un autocommutateur compatible avec la téléphonie sur IP. Il permet comme un commutateur téléphonie standards, d'établir une communication téléphonique entre deux abonnés distants.

1.1.5. Les enjeux de la téléphonie sur IP :

Les offre de téléphonie IP pour PME (petite et moyenne entreprise) et TPE (très petite entreprise) se multiplie : réduction des coûts, convergence des réseaux et simplification de gestion, d'où le besoin de distinguer entre les prestataires. La téléphonie n'a jamais été une application simple. Les contraintes temps réel et de synchronisation demeure un problème sur sa mise en application, et la téléphonie par paquet ne fait que compliquer le transport. En outre, divers raisons démontre le succès de la téléphonie sur IP.

Tout d'abord nous illustrerons ces avantages et inconvénients les plus marquantes :

1.1.5.1. Avantages de la ToIP :

❖ **Convergence :**

Traditionnellement, les réseaux téléphoniques et les données étaient séparé ce qui conduit à un grand logistique matériel et administrateur. Ce pendant depuis l'arrivée de la ToIP, Plusieurs flux information sont véhiculées un seul réseau : le flux de voix, de vidéos, texte. Les plus communications devient plus facile et assez nette. Les utilisateurs pourront faire plusieurs taches en même temps telles que : envoyer des fichiers texte étant en communication quel soit vidéo ou audio. Elle représente un très grand apport pour les entreprises, la productivité est améliorée. Avantageuse pour les administrateurs, un seul réseau est à administré pour une bonne gestion du trafic.

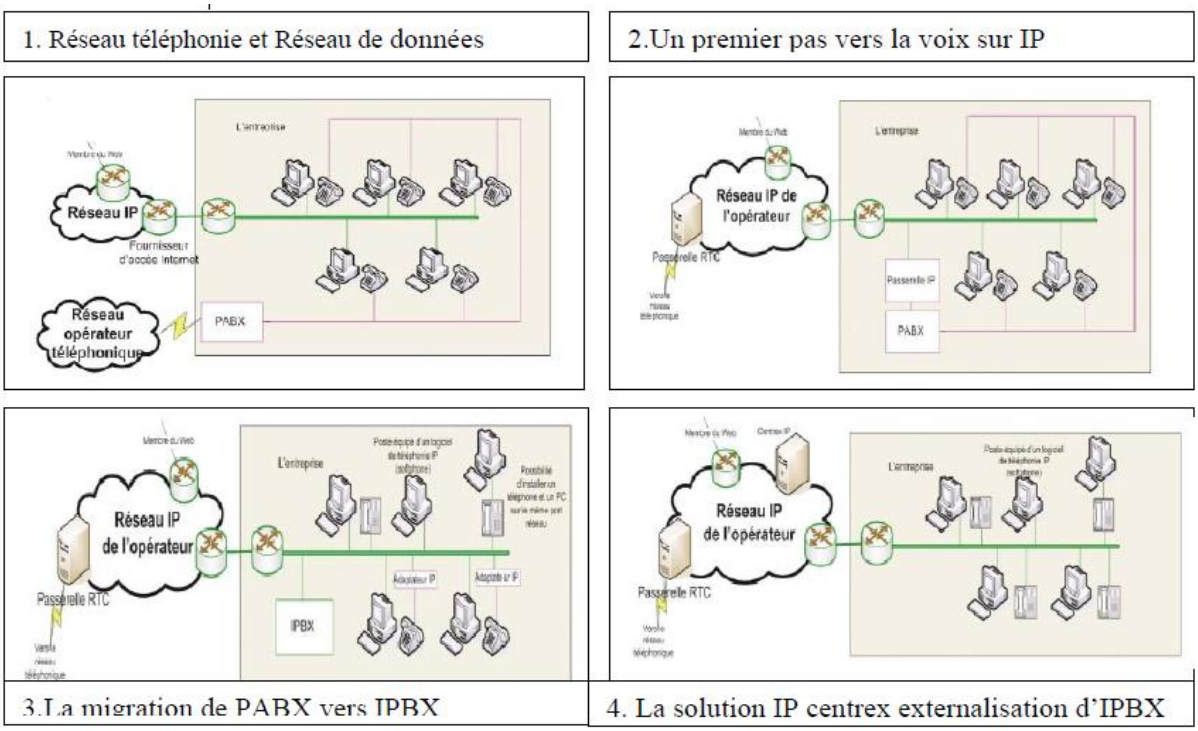


Figure 3 : *les étapes de développement des réseaux d'entreprises.*

❖ **Optimisation des ressources et suppression de silence :**

La téléphonie sur IP qui est basé sur le transfert de paquets, montre une faible utilisation des ressources par rapport à la communication de circuits. Le réseau RTC, qui est à communication de circuits, dédiant des ressources pour toute la durée de la communication qu'elle utilisées ou non. Ceci dit, la communication de circuits gaspille trop de ressources parce que : même le silence d'une conversation téléphonique cause une énorme consommation de bande passante contrairement au réseau IP, l'utilisation de deux canaux l'un pour l'émission et l'autre pour la réception pour une communication simultané (full-duplex) entre deux individués. C'est pourquoi en matière de cout le réseau IP est nettement mieux.

❖ **Réduction du coût :**

La téléphonie sur IP exploite un réseau de données IP pour offrir des communications vocales sur un réseau unique de voix et de données. Cette convergence s'accompagne de multiples avantages, dont le coût d'investissement devient quasiment nul en infrastructure, une forte réduction de la facture téléphonique. Les réseaux des opérateurs se chargent d'effectuer le transport de toutes les données. Auparavant, les opérateurs allouaient au moins deux réseaux, celui de la téléphonie et celui de donnée, tandis qu'à présent ils maintiennent qu'un seul. Le prix des équipements de réseau : serveurs, concentrateurs, switches ou routeurs, sont inférieur à celui des autocommutateurs télécoms.

❖ **Services et disparition des commutateurs locaux :**

Le réseau IP dispose de divers services. Notamment, le service de présence, qui a pour objectif de détecter si un utilisateur occupe la ligne réseau ou non, ne nécessite pas d'allouer des ressources dans un réseau IP, à la différence du réseau RTC. Cela a conduit à la possibilité de gérer les téléphones depuis le réseau de l'opérateur. Des solutions médiatrices, comme le PBX-IP, permettant de basculer lentement des circuits numériques aux liaisons paquet IP.

1.1.5.2. Inconvénients de la ToIP :

Comme toute technologie la téléphonie sur IP rencontre aussi ces difficultés tel que la qualité de service, actuellement inférieure tout au moins sur Internet ou en extranet, à celle constater sur les réseaux traditionnels de télécommunications et l'interopérabilité et qualité sonore des différentes solutions IP. En effet, lorsqu'on parle de téléphonie IP, quelques problèmes restent à régler. Les principaux inconvénients de la téléphonie IP sont les suivants :

- **Sécurité :**

Dans la téléphonie classique, la sécurité est fortement garantie par un réseau spécifique, lequel ne peut être attaqué par l'émission de paquets car le réseau n'est pas à transfert de paquets. Tandis que dans la ToIP, la confidentialité est assez simple à garantir. Reste le problème de l'authentification de l'utilisateur, qui mérite réflexion.

- **Qualité sonore :**

Une des contraintes majeures de la ToIP est la qualité de la retransmission qui n'est pas encore optimale. Cependant, des inconvénients tels la qualité de la restitution 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 (latence) peuvent être une contrainte capitale dans le milieu professionnel. En outre, il se peut quelque morceau de l'information manquent (des paquets perdus pendant la transmission) sans pouvoir savoir si les paquets ont été perdus et à quel moment.

- **Technologie émergente et constante évolution des normes :**

La technologie IP n'a pas encore atteint l'apogée de ces limites : des nouveaux standards de téléphonie IP sont annoncés presque chaque période. Ceci dit, même si des progrès ont été faits et qu'elle est à présent utilisable. La téléphonie IP reste une technologie ayant un essor évolutif, qui risque d'avoir des impacts à chaque fois sur le CRC (contrôle de redondance cyclique) qui est un contrôleur d'erreur.

- **Dépendance de l'infrastructure technique et support administratif exigeant :**

Les centres de relations IP, peuvent être vraiment vulnérables si l'infrastructure n'est pas adéquate aux normes de la demande. Notamment, si la base de données n'est pas disponible, les centres ne peuvent tout simplement pas recevoir d'appels.

Etant donné que la voix et les données sont transmises dans un seul système, cela signifie que la stabilité du système devient importante et ainsi qu'une bonne administration. Ceci dit il est important de considérer certains éléments tels que : la qualité sonore sera différente et que cette technologie dépend d'Internet (légers, délai à prévoir, pannes, etc.).

2. Les Réseaux Téléphoniques :

Réseaux publics :

On distingue deux types de réseaux publics selon le protocole de signalisation utilisée au niveau des transmissions :

- **Réseaux téléphoniques analogiques :**

Les anciens systèmes et réseaux téléphoniques étaient analogiques (certains le sont encore), avec les systèmes analogiques, la voix est représentée par un signal électrique continu. Les réseaux RTC Publics (PSTN, en anglais) acheminent des signaux analogiques.

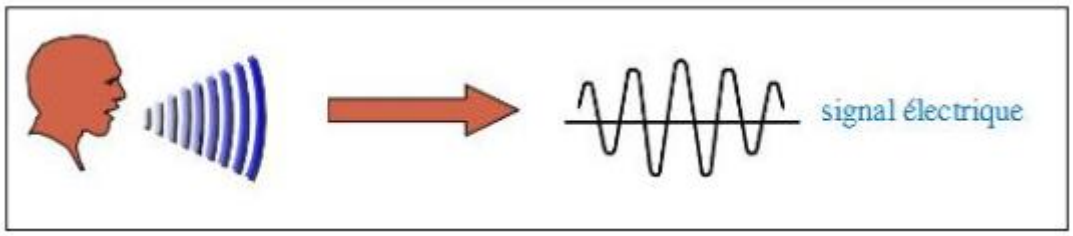


Figure 4 : *La transmission analogique.[6]*

- **Réseaux numériques :**

Les équipements modernes numériques utilisent des nombres binaires (0 et 1) également appelés bits, avec les systèmes téléphoniques numériques, la voix est convertie en
système binaire. Les réseaux RNIS transportent les bits.

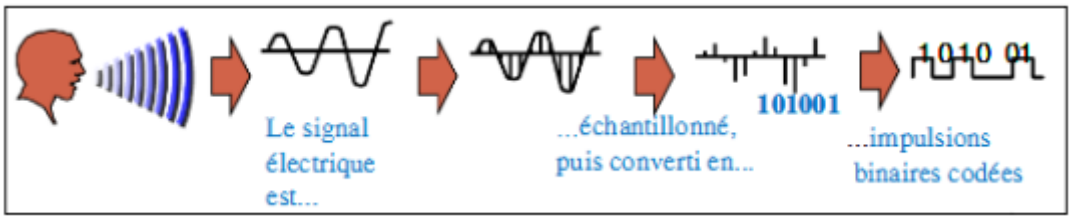


Figure 5 : *La transmission numérique.[6]*

2.1. Le Réseau Téléphonique Commuté (RTC) :

2.1.1. Définition :

Le Réseau Téléphonique Commuté **(RTC)**, en anglais Public Switched Telephone Network **(PSTN)** est un réseau fixe et mobile dans lequel un poste d'abonné est relié à un central téléphonique par une paire de fils alimentée en boucle locale.[6]

2.1.2. Principe de fonctionnement :

Utilisant le principe de la commutation de circuits, un canal de communication est ouvert entre deux abonnés et l'intégralité de cette bande passante est réservée à ces deux interlocuteurs. Même s'ils ne parlent pas, la bande passante est utilisée et perdue.

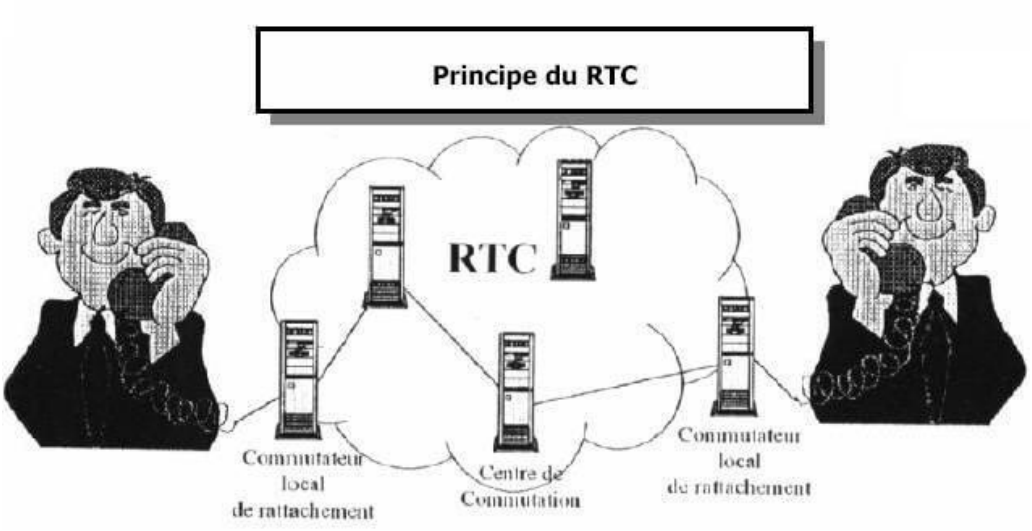


Figure 6 : *Principe du RTC.[7]*

2.1.3. Architecture du RTC :

Le réseau RTC est structuré en trois (3) parties :

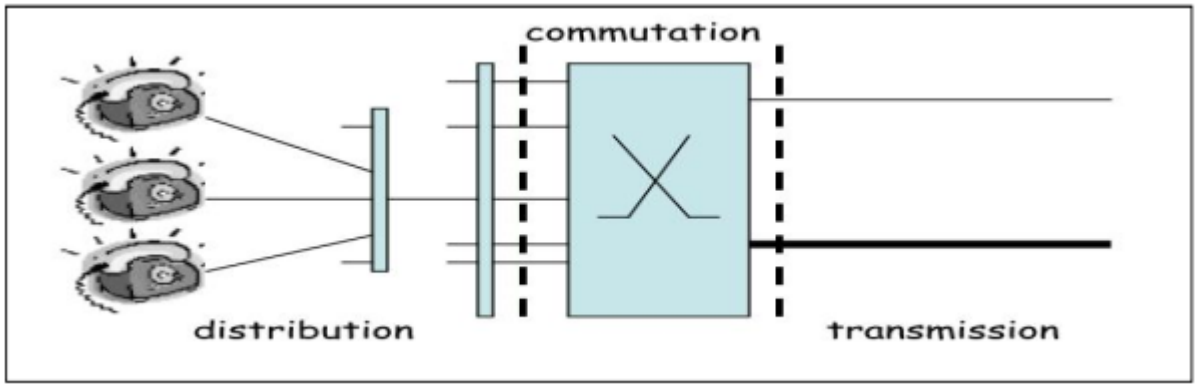


Figure 7 : *Architecture global du RTC.[6]*

Comme le montre la figure ci-dessus, le réseau RTC se divise en 3 grandes parties :

- **La distribution :**

C'est la partie support de télécommunication du réseau, cette fonction est remplie soit par un système filaire cuivre (en voie de disparition), de la fibre optique ou des faisceaux hertziens. Aujourd'hui, le réseau est pratiquement intégralement numérisé, seule la liaison d'abonné reste analogique.

- **La commutation :**

C'est la partie centrale du réseau. Elle permet de mettre en liaison les abonnés. Elle comprend essentiellement la liaison d'abonné ou boucle locale (paire métallique torsadée) qui relie l'installation de l'abonné au centre de transmission de rattachement. Cette ligne assure la transmission de la voix, de la numérotation et de la signalisation générale.

- **La transmission :**

C'est la fonction essentielle du réseau, elle consiste à mettre en relation deux abonnés, maintenir la liaison pendant tout l'échange et libérer les ressources à la fin de celui-ci. C'est le réseau qui détermine les paramètres de taxation et impute le coût de la communication à l'appelant.

2.1.4. La hiérarchie du RTC : [6]

Le réseau téléphonique commuté a une organisation hiérarchique à trois niveaux. Il est structuré en zones correspondant à un niveau de concentration comme suit (voir figure 6) :

- **Zone à Autonomie d'Acheminement (ZAA) :**

C'est la zone la plus basse de la hiérarchie, comporte un ou plusieurs commutateurs à autonomie d'acheminement (CAA) qui eux-mêmes desservent des commutateurs locaux (CL). Les commutateurs locaux ne sont que de simples concentrateurs de lignes auxquels sont raccordés les abonnés finaux. Cette zone est un réseau étoilé, elle constitue le réseau de desserte ;

- **Zone de Transit Secondaire (ZTS) :**

Cette zone comporte des Commutateurs de Transit Secondaires (CTS). Il n'y a pas d'abonnés reliés à ces commutateurs. Ils assurent le brassage des circuits lorsqu'un commutateur à autonomie d'acheminement (CAA) ne peut atteindre le CAA destinataire directement (réseau imparfaitement maillé) ;

- **Zone de Transit Principal (ZTP) :**

Cette zone assure la commutation des liaisons longue distance. Chaque ZTP comprend un commutateur de transit principal (CTP), l'un d'eux relié au commutateur international de transit.

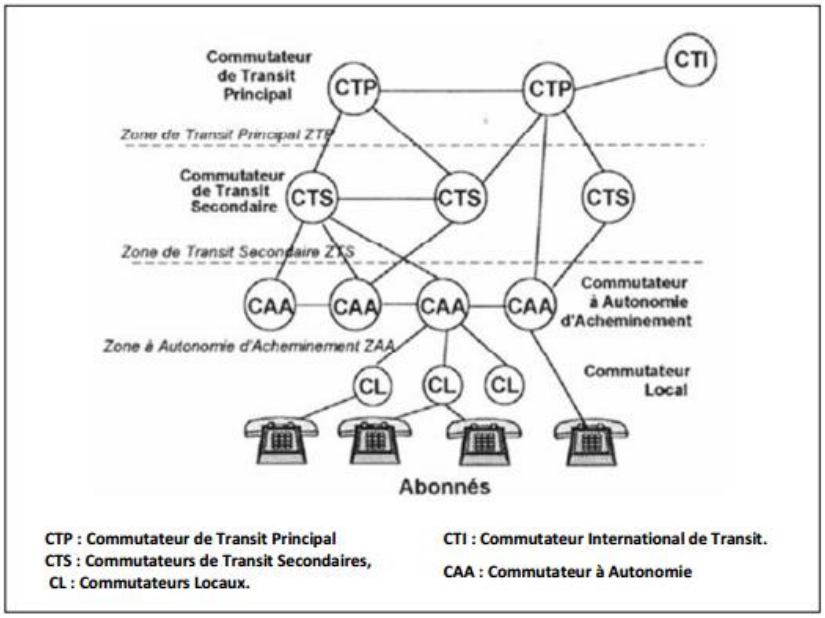


Figure 8 : *Hiérarchie du RTC.[6]*

2.1.5. Avantages :

Le RTC est :

- Très pratique pour la communication vocale grâce à la transmission point à point ;
- Très étendu, il atteint tous les pays du globe ;
- Full duplex, deux utilisateurs peuvent émettre et recevoir en même temps, cette fonctionnalité est utilisée par les modems ;
- Peu coûteux pour les courtes distances ;
- Sécurisable en utilisant le cryptage sur les lignes téléphoniques.

2.1.6. Inconvénients :

- Le RTC est analogique, quelques problèmes sont rencontrés lors de la transmission des données numériques ;
- Les équipements analogiques perturbent le signal transmis, qui entraine l'ajout du bruit sur le signal au cours de sa transmission.

2.2. Le réseau numérique à intégration de services (RNIS ou ISDN) : [1]

2.2.1. Définition :

En anglais ISDN (Integrated Service Digital Network), RNIS est l'abréviation de « Réseau Numérique à Intégration de Service ». Un RNIS est un réseau qui fournit ou contribue à fournir plusieurs services de télécommunications différents en établissement des connexions numériques entre interfaces usager-réseau. Le **C.C.I.T.T.** (Comité Consultatif International Télégraphique et Téléphonique) a donc définit le réseau RNIS ainsi : *"Un Réseau Numérique à Intégration de Services est un réseau développé en général à partir d'un réseau téléphonique numérisé, qui autorise une connectivité numérique de bout en bout assurant une large palette de services, vocaux ou non, auquel les usagers ont accès par un ensemble limité d'interfaces polyvalentes."* [8]

2.2.2. Principe de fonctionnement :

Dans un réseau téléphonique analogique, une boucle sur une paire torsadée de fils de cuivre entre le commutateur central de la compagnie de télécommunication et l'abonné supporte un canal de transmission unique. Ce canal ne traite qu'un seul service simultanément la voix ou les données. Avec un Réseau Numérique à Intégration de Services, la même paire torsadée est divisée en plusieurs canaux logiques.

2.2.2.1. Les canaux logiques RNIS :

Le CCITT a défini la notion de « canal de communication » associé à une interface d'accès usager-réseau. Un canal représente une capacité de transfert d'information à travers l'interface d'accès. Une même ligne de raccordement physique va pouvoir transporter des informations relatives à différentes communications.

Les canaux sont regroupés en différentes classes présentant des caractéristiques communes :

- **Les canaux B**

Le canal B est un canal à 64 Kbps permettant de transmettre, tout type de "train d'information'' comme :

- L'information vocale numérisée à 64 Kbps (ou à des débits inférieurs)
- L'information de données à commutation de circuits ou de paquets à des débits inférieurs ou égaux à 64 Kbps.

Les canaux B sont des canaux à commutation de circuits (ce qui n'interdit pas leur utilisation en mode paquets) par lesquels les abonnés peuvent communiquer.

- **Les canaux D**

Les canaux D peuvent proposer différents débits (16 Kbps en accès de base et 64 Kbps en accès primaire) ; ils sont à l'origine destinés au transfert de la signalisation nécessaire à la gestion des circuits mis en œuvre par la communication sur le RNIS tel que : appels, établissement des connexions, demandes de services, routage des données sur les canaux B et enfin libération des connexions. Il est aussi possible de transmettre des données utilisateur à travers les canaux D, mais comme le débit de ces canaux est limité ce type d'utilisation est rare.

Les canaux D sont des canaux à commutation de messages par lesquels peuvent aussi transiter des informations émises par les applications de l'utilisateur comme des données utilisateurs en commutation de paquets.

- **Les canaux H**

Ces canaux à moyen et haut débit ont des caractéristiques identiques à celles des canaux B ; ils offrent néanmoins un débit de n x 64 Kbps Le CCITT a retenu les structures H0 (384 Kbps), H11 (1536 Kbps) et H12 (1920 Kbps).

2.2.2.2. Les interfaces standards RNIS :

Le CCITT a défini plusieurs types de structures d'interfaces usager-réseau polyvalentes dont en particulier l'interface de base et l'interface à débit primaire.

- **L'interface de base**

Aussi appelée interface S/T, elle est caractérisée par :

- Un débit utile de 144 Kbps réparti sur deux canaux B à 64 Kbps et un canal D à 16 Kbps pour la signalisation (on parle d'interface d'accès 2 B + D) ;
- Une utilisation suivant une topologie point à point ou multipoint ;
- Un connecteur de raccordement normalisé à 8 plots (RJ45).

- **L'interface à débit primaire**

Elle a les caractéristiques suivantes :

- Un débit utile de 1984 Kbps réparti sur 30 canaux B à 64 Kbps et un canal D à 64 Kbps (30 B + D) ;

- Un débit utile de 1536 Kbps réparti sur 23 canaux B à 64 Kbps et un canal D à 64 Kbps (23 B + D).

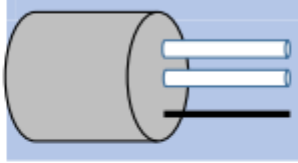
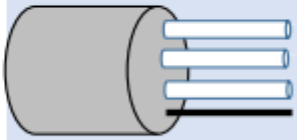
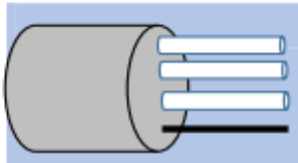
Type	Débit utile		Structure	Débit du canal D	
Interface de base	144 Kbits/s		2 B + D	16 Kbits/s X	64 Kbits/s
Interfaces à débit primaire	1536 Kbits/s		23 B + D		X
	1984 Kbits/s		30 B + D		X

Figure 9 : *Les interfaces standards RNIS.*

2.2.3. Avantages et inconvénients :

- **Avantages**
  - L'utilisation de données numériques sur la boucle locale (liaison numérique de bout en bout) ;
  - Offre de meilleurs débits aux utilisateurs distants ;
  - Une latence moins élevée ;
  - Les réseaux RNIS acheminent différents signaux de trafic (voix, données, vidéo).
- **Inconvénients**
  - L'information passe par le réseau téléphonique commuté, et subit les tarifs du téléphone, ce qui est particulièrement pénalisant pour la longue distance ;
  - Le débit d'information peut s'avérer insuffisant, surtout si l'on transfère des fichiers déjà ripés (CTP) ;
  - Les constructeurs ne sont pas d'accord au niveau des normes d'agrégation des canaux.

3. Protocole de Signalisation VoIP :

Pour le bon déroulement d'une communication sur IP, cette dernière doit respecter un modèle de signalisation. Parmi les plus connus et les plus utilisés on cite le protocole H.323 et le protocole SIP.

3.1. H323 :

3.1.1. Définition : [6]

Le standard H.323 a été conçu par l'ITU-T. Il spécifie les composants, protocoles et procédures permettant la mise en place d'un service multimédia sur un réseau à transmission par paquets (LAN, WAN…). H.323 fait partie d'une série de recommandations qui, toutes décrivent des transmissions multimédia mais sur des réseaux différents. H323 transmet des informations multimédia sur des réseaux à paquets commutés sans garantie de bande passante. Ce standard est valable pour la VoIP car il permet de transmettre uniquement la voix et des données. Il est constitué par un ensemble de protocoles permettant des communications entre plusieurs équipements basés sur le modèle H.323. C'est une famille de protocoles qui sont utilisés pour l'établissement ou la clôture d'un appel, l'enregistrement des postes, l'authentification des utilisateurs, ainsi que bien d'autres services. Ceux-ci sont transportés sur un réseau IP à travers des protocoles TCP ou UDP.

3.1.2. Architecture et rôle des composants H323 :

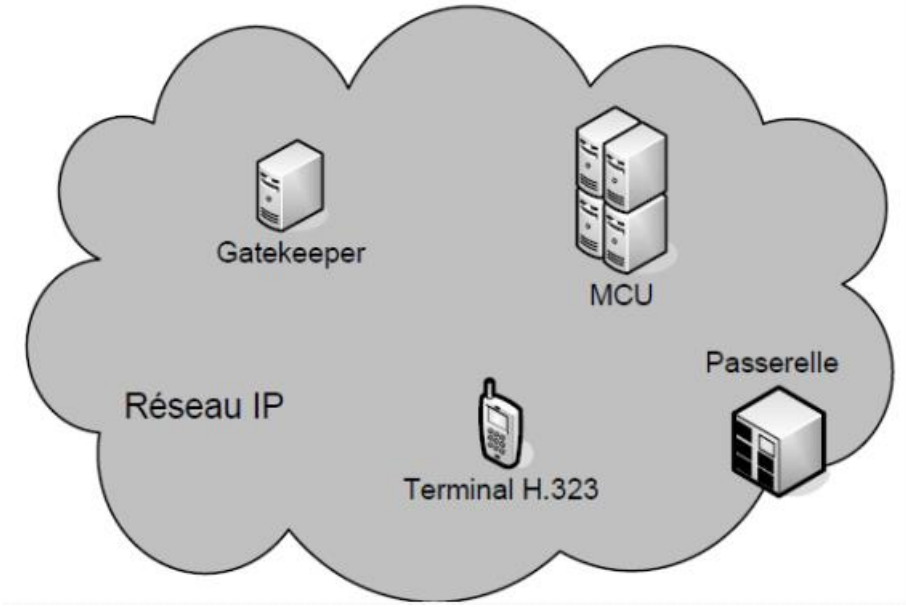


Figure 10 : *Architecture générale du H323.*

Une architecture H.323 est généralement composée des quatre catégories d'entités suivantes.

- **Terminal**

  Est un endpoint permettant des communications temps réels avec d'autres endpoints. Il s'agit d'un équipement utilisateur tel qu'un PC ou un téléphone IP qui supporte au moins un codec audio et éventuellement d'autres codecs audios et vidéo.[9]

- **Passerelle**

  Ou gateway, 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, etc.). On peut avoir autant de passerelles différentes que nécessaire, suivant la nature des réseaux non-IP à interconnecter. [10]

- **Gatekeeper**

  Un Gatekeeper est le composant le plus important d'un réseau H.323. Il agit comme étant le point central pour tous les appels dans sa zone et contrôle les endpoints. Un Gatekeeper H.323 agit comme un commutateur virtuel. Le Gatekeeper exécute deux fonctions importantes. La première est la translation d'adresse d'un alias LAN d'un terminal ou d'une passerelle (Gateway) vers une adresse IP ou IPX. La deuxième fonction est la gestion de bande passante. Le Gatekeeper n'est pas obligatoire dans un réseau H.323 mais lorsqu'il existe, tous les équipements de la zone doivent dialoguer avec lui pour établir des communications. [9]

- **Multipoint Control Unit (MCU)**

  Est un terminal qui supporte des conférences entre 3 (ou plus) terminaux. Il peut s'agir d'un équipement indépendant (PC) ou peut être intégré dans un Gateway, un gatekeeper ou un terminal. Un MCU consiste en deux fonctions, à savoir, contrôleur multipoint (Multipoint Controller, MC) et processeur multipoint (Multipoint Processor, MP) La fonction MC met en œuvre le contrôle et la signalisation pour le support de la conférence alors que la fonction MP reçoit les flux des terminaux, les traites, et les retournes aux terminaux participant à la conférence. [9]

3.1.3. Les étapes d'une communication H323 :

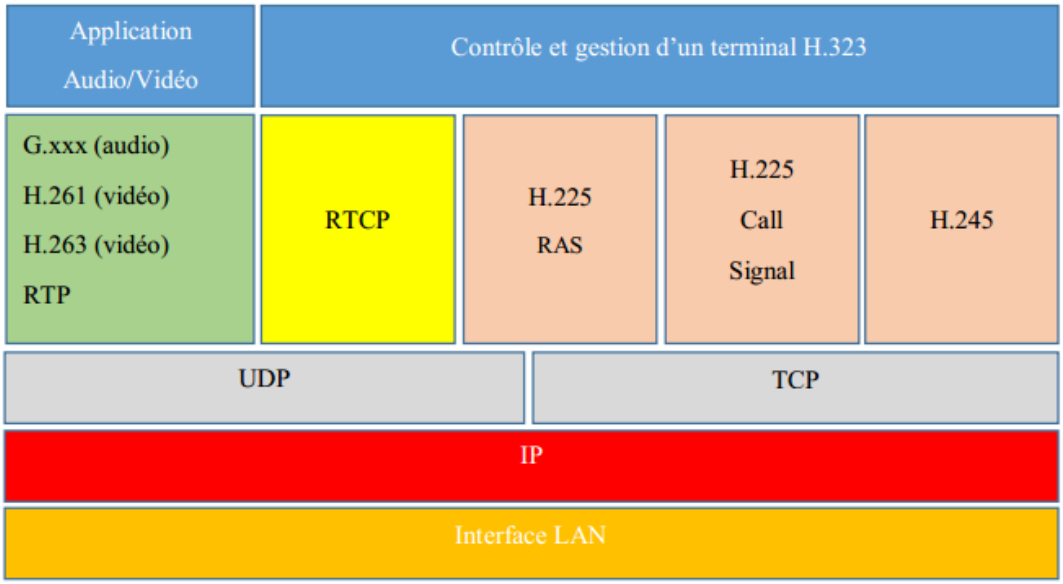


Figure 11 : *Pile protocolaire H323.*

H323 se dessine en 3 grandes parties (Voir figure ci-dessus). En effet, pour établir une communication audio ou vidéo sur IP, le signal doit être encodé en utilisant des codecs normalisés définis dans la norme H323. H323 normalise aussi la signalisation à utiliser pour l'établissement d'une communication. La voix ou la vidéo est transmise en utilisant le protocole

UDP, associé aux protocoles RTP et RTCP pour le transfert des données en temps réel. [1] La signalisation pour l'établissement des appels est mise en œuvre à l'aide de trois protocoles :

- **H.225 Signalisation d'enregistrement RAS (Registration, Admission and Status) :**

La signalisation RAS est utilisée entre les endpoints et le Gatekeeper qui les contrôle. RAS perrmet donc au Gatekeeper de contrôler les endpoints présents dans sa zone.

La signalisation RAS est utilisée entre les terminaux et le Gatekeeper qui les contrôle. Les messages RAS sont de 3 types : (REQUEST), (REJECT) ou (CONFIRM). Voici quelques messages RAS REQUEST:

GRQ (GATEKEEPER REQUEST) : En envoyant ce message, le terminal recherche un gatekeeper susceptible de le prendre en charge. Plusieurs gatekeepers peuvent répondre. L'adresse du gatekeeper peut être renseignée en statique sur le terminal ou être déterminée par une résolution de type DNS.

RRQ (REGISTRATION REQUEST) : Ce message permet au terminal de s'enregistrer auprès du gatekeeper.

ARQ (ADMISSION REQUEST) : Pour initier ou recevoir un appel, un terminal doit être soumis à un contrôle d'admission auprès du gatekeeper.

LRQ (LOCATION REQUEST) : Ce message est envoyé à un gatekeeper soit par un endpoint, soit par un gatekeeper pour demander la localisation d'un utilisateur.

- **H.225 Signalisation d'appel ou Call signaling (Q.931)** :

Cette signalisation permet d'établir et de libérer des connexions entre endpoints H.323. Les messages utilisés sont ceux du protocole de signalisation Q.931 (RNIS) modifiés par la recommandation H.225.

La signalisation d'appel permet l'établissement d'un appel, la libération de la communication et la transmission des messages indiquant l'état d'un appel (occupation d'un poste, redirection, etc.). Les cinq messages fondamentaux suivants doivent obligatoirement être supportés :

- **SETUP :** envoyé pour initier et établir une communication avec un terminal H.323.
- **ALERTING :** indique que le poste appelé est en train de sonner et que l'appelant se met en attente de sa réponse.
- **CONNECT :** indique que la communication peut débuter.
- **RELEASE COMPLETE :** envoyé pour initier la terminaison de l'appel.
- **STATUS FACILITY :** envoyé pour demander des services complémentaires.

➢ **H.245** :

Lorsque l'appelé décroche, le protocole H.245 permet l'établissement de canaux RTP/RTCP permettant le transfert de données multimédia et le contrôle de ce transfert.

Le protocole H.245 permet de créer un canal de contrôle pour la négociation des paramètres de la communication (codeur utilisé, contrôle de flux, etc.), et d'établir un canal de transmission RTP/RTCP.

La signalisation de commande H.245 permet donc :

- L'échange de capacités multimédia (audio, vidéo), afin d'assurer une transmission selon un mode audio, vidéo particulier.
- La détermination du terminal maître et du terminal asservi afin d'éviter tout conflit dans le contrôle d'une conférence.
- L'établissement et la libération de canaux logiques (RTP/TRTCP) permettant le transfert de données multimédia.

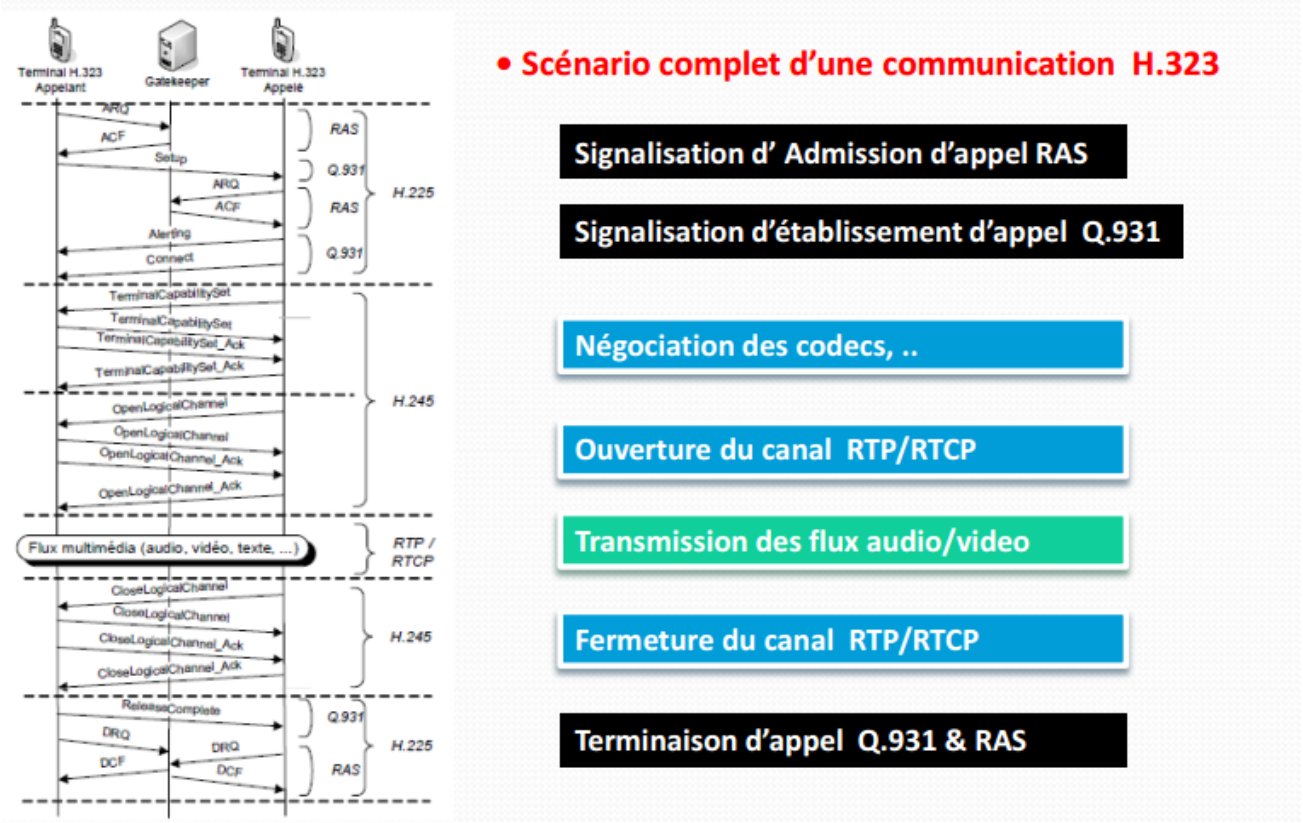


Figure 12 : *Scénario complet d'une communication H323.*

3.1.4. Avantages et Inconvénients :

La technologie H.323 possède des avantages et des inconvénients. Parmi les avantages qui sont les suivants :

- ***La gestion de bande passante*** : le protocole H.323 permet la bonne gestion de la bande passante en posant quelques restrictions au flux audio/vidéo pour permettre le bon fonctionnement des applications critiques sur le réseau LAN. Tout terminal H.323 est capable d'ajuster la bande passante et modifier du débit en fonction du comportement du réseau en temps réel (latence, perte de paquets et gigue).

- ***Support Multipoint*** : H.323 permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.

- ***Support Multicast*** : H.323 permet également de faire des transmissions en multicast.

- ***Interopérabilité :*** H.323 permet aux utilisateurs de ne pas se préoccuper de la manière dont se font les communications, les paramètres (les codecs, le débit…) sont négociés de manière transparente.

- ***Flexibilité :*** une conférence H.323 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones…) qui peuvent partager selon le cas, de la voix de la vidéo et même des données grâce aux spécifications T.120.

Les inconvénients de la technologie H.323 sont :

- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence des services de téléphonie et d'Internet, ainsi qu'un manque de modularité et de souplesse.

- Comprend de nombreuses options susceptibles d'être implémentées de façon différente par les constructeurs et donc de poser des problèmes d'interopérabilité.

3.2. Protocole SIP :

3.2.1. Définition :

Le protocole d'ouverture de session ou « Session Initiation Protocol » en anglais (SIP) est une norme de l'IETF pour la conférence multimédia sur IP. Le SIP, protocole de contrôle de la couche application (signalisation) utilisé pour la création, la modification et la clôture de sessions avec un ou plusieurs participants. Ces sessions peuvent inclure des sessions Internet conférences multimédia, appels téléphoniques sur Internet et de distribution multimédia. Le SIP est un système moins compliqué et il est plus souple que le protocole H.323.[11]

Il se charge également de la négociation sur les types de média utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol). SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP étant indépendant de la transmission des données, tout type de données et de protocoles peut être

utilisé pour cet échange. Cependant le protocole RTP (Real-time Transport Protocol) assure le plus souvent les sessions audios et vidéos. SIP remplace progressivement H323.

SIP est le standard ouvert de VoIP, interopérable, le plus étendu et vise à devenir le standard des télécommunications multimédia (son, image, etc.). Skype par exemple, qui utilise un format propriétaire, ne permet pas l'interopérabilité avec un autre réseau de la voix sur IP et ne fournit que des passerelles payantes vers la téléphonie standard. SIP n'est donc pas seulement destiné à la VoIP mais pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo.

3.2.2. Architecture et rôle des composants SIP :

Contrairement à H.323, largement fondé sur une architecture physique, le protocole SIP s'appuie sur une architecture purement logicielle.

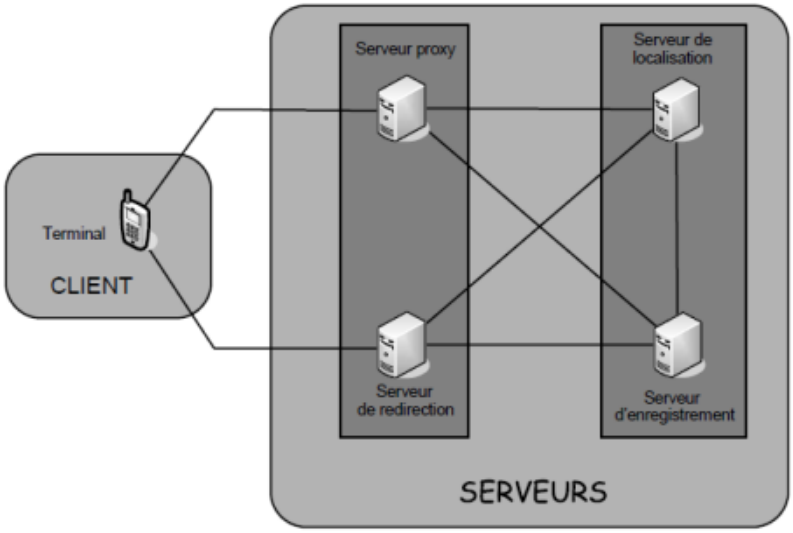


Figure 13 : *Architecture de SIP.*

L'architecture de SIP s'articule principalement autour des cinq entités suivantes :

- **Terminal Utilisateur :**

Le terminal est appelé UA (User Agent). Il s'agit d'une application sur un équipement de l'usager qui émet et reçoit des requêtes SIP. Il se matérialise par un logiciel installé sur un PC, sur un téléphone IP. Il est constitué de deux sous-entités, comme illustré à la figure suivante :

- Une partie cliente, appelée UAC (User Agent Client), chargée d'émettre les requêtes. C'est l'UAC qui initie un appel.
- Une partie serveur, appelée UAS (User Agent Server), qui est en écoute, reçoit et traite les requêtes. C'est l'UAS qui répond à un appel.

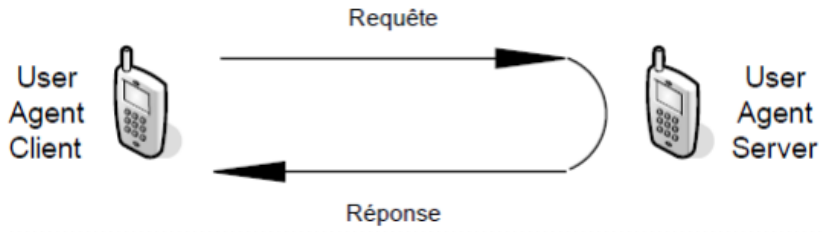


Figure 14 : *Composition d'un terminal utilisateur.*

- **Serveur d'Enregistrement :**

  Est un serveur qui gère les requêtes d'enregistrement (requêtes REGISTER) envoyées par les Users Agents (UA) pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données.

- **Serveur de Localisation :**

  Le serveur de localisation (Location Server) joue un rôle complémentaire par rapport au serveur d'enregistrement en permettant la localisation de l'abonné.

  Ce serveur contient la base de données de l'ensemble des abonnés qu'il gère. Cette base est renseignée par le serveur d'enregistrement. Chaque fois qu'un utilisateur s'enregistre auprès du serveur d'enregistrement, ce dernier en informe le serveur de localisation.

  Presque toujours, le serveur de localisation et le serveur d'enregistrement sont implémentés au sein d'une même entité.

- **Serveur de Redirection**

  Le serveur de redirection (Redirect Server) agit comme un intermédiaire entre le terminal client et le serveur de localisation. Il est sollicité par le terminal client pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur.

  L'appelant envoie une requête de localisation d'un correspondant au serveur de redirection. Celui-ci joint le serveur de localisation afin d'effectuer la requête de localisation du correspondant à joindre. Le serveur de localisation répond au serveur de redirection, lequel informe l'appelant en lui fournissant la localisation trouvée.

- **Serveur Proxy**

  Le serveur proxy permet d'initier une communication à la place de l'appelant. Il joue le rôle d'intermédiaire entre les terminaux et agit pour le compte de ces derniers.

  Le serveur proxy remplit les différentes fonctions suivantes :

  - Localiser un correspondant ;
  - Réaliser éventuellement certains traitements sur les requêtes ;
  - Initier, maintenir et terminer une session vers un correspondant.

3.2.3. Les étapes d'une communication SIP :

Modèle d'échange

Le protocole SIP repose sur un modèle Requête/Réponse. Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. La liste des requêtes échangées est la suivante :

- **Invite :** Cette requête est utilisée afin d'établir une session entre UAs. Elle contient les informations sur l'appelant et l'appelé et sur le type de flux qui seront échangés (voix, vidéo, etc.).
- **Ack :** Cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête **Invite.**
- **Bye :** Cette requête est utilisée par le terminal de l'appelé afin de signaler qu'il souhaite mettre un terme à la session.
- **Register :** Cette requête est utilisée par un UA afin d'indiquer au Serveur d'enregistrement la correspondance entre son adresse SIP et son adresse IP
- **Cancel :** Cette requête est envoyée par un terminal ou un proxy server à fin d'annuler une requête non validée par une réponse finale comme, par exemple, si une machine ayant été invitée à participer à une session, et ayant accepté l'invitation ne reçoit pas de requête Ack, alors elle émet une requête Cancel
- **Option :** Cette requête est utilisée afin d'interroger les capacités et l'état d'un User agent ou d'un serveur. La réponse contient ses capacités ou le fait que l'UA soit indisponible.

Scénario d'une communication SIP

Quatre étapes seulement suffisent à mettre en relation les deux utilisateurs :

Etape 1 : L'appelant (UAC) envoie un message (requête INVITE) proposant à son correspondant (UAS) d'initier une communication. Ce message contient les paramètres désirés pour établir la communication.

Etape 2 : Dès que l'UAS reçoit le message, il en informe l'utilisateur appelé (le téléphone sonne, avec indication de l'appelant et du motif de son appel s'il a renseigné ce champ, ainsi que des services disponibles). Dans le même temps, il indique à l'appelant (par une réponse provisoire 180 RINGING) que l'appelé est en train d'être averti de l'appel.

Etape 3 : Dès que l'appelé accepte l'appel (en décrochant), l'UAS informe l'appelant (par une réponse définitive 200 OK) que l'appel peut débuter. Ce message contient les paramètres que l'UAS supporte pour la session.

Etape 4 : L'UAC retourne à l'UAS un message d'acquittement (requête ACK) lui indiquant qu'il a pris note que l'appel peut débuter. Ce message contient les paramètres fixés pour la session, qui prennent en compte ces possibilités et celles de l'UAS. Les participants sont par la suite mis en liaison et peuvent communiquer.

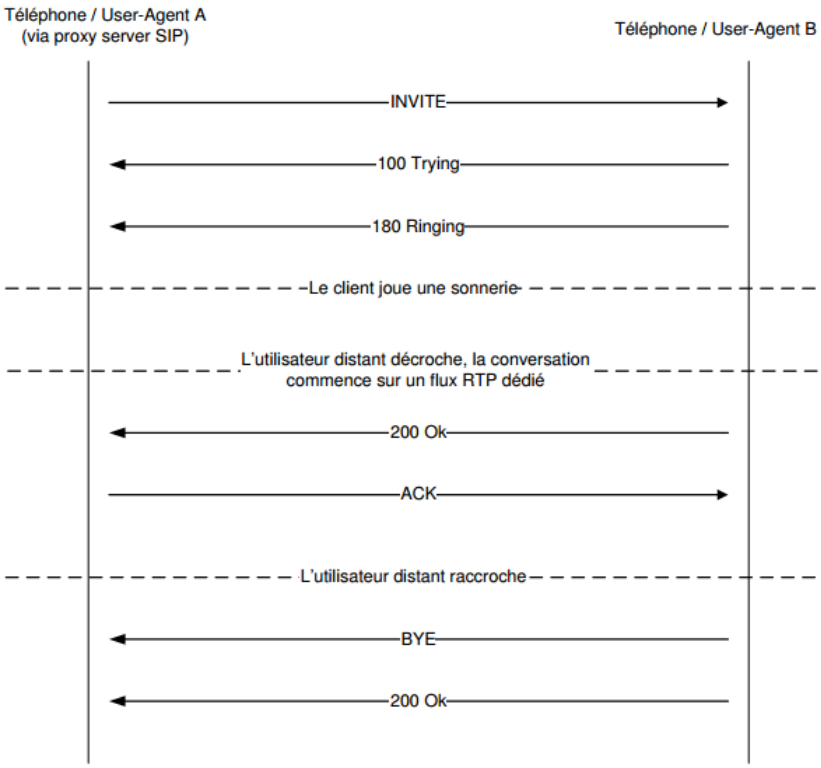


Figure 15 : *Chronologie des messages SIP envoyés d'un user-agent A vers un user-agent B dans le cadre d'un établissement de conversation.[2]*

3.2.4. Avantages et Inconvénients :

3.2.4.1. Avantages :

- ✓ Ouvert : les protocoles et 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.
- ✓ P2P : sur un LAN, SIP fonctionne complètement en P2P (encore plus facilement avec l'intégration de Zeroconf), ce n'est pas le cas pour l'établissement de sessions entre deux pairs séparés par un NAT.
- ✓ Flexible : SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.).

- ✓ Téléphonie sur réseaux publics : il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM, etc.) permettant d'émettre ou de recevoir des appels vocaux.

- ✓ Points communs avec H323 : l'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

3.2.4.2. Inconvénients :

- ✓ Basé sur l'adresse IP : le protocole SIP ne franchit pas les NAT, mais cela peut être résolu en déployant des mécanismes client-serveur supplémentaires comme par exemple STUN ou en couplant SIP avec Jabber.

- ✓ Mauvaise implémentation : 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.

- ✓ Présence et messagerie instantanée : SIP montre un certain nombre de faiblesses dans la gestion de la présence et la messagerie instantanée, mais l'intégration du standard ouvert spécialisé Jabber résout la plupart de ces problèmes.

- ✓ 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.

3.3. Comparaison H323 et SIP :

Le tableau ci-dessous montre une étude comparative entre le protocole SIP et H.323 :

	SIP	**H.323**
Nombre d'échanges pour établir une connexion	1 à 5 allers-retours	6 à 7 allers-retours
Maintenance protocolaire	Simple par sa nature textuelle à l'exemple de http	Complexe et nécessitant un compilateur
Evolution du protocole	Protocole ouvert à de nouvelles fonctions	Ajout d'extension Propriétaire sans concertation entre vendeurs
Fonction de conférence	Distribuée	Centralisée par l'unité MC
Fonction de téléservices	Oui, par défaut	H.323 v2+H.450
Détection d'un appel en boucle	Oui	Inexistante sur la version 1 Un appel routé sur l'appelant provoque une infinité de requêtes
Signalisation multicast	Oui, par défaut	Non

Tableau 1 : *Comparaison SIP et H323*

4. Autres protocoles VoIP :

En outre, il existe divers protocoles en dehors de ceux que l'on a énuméré précédemment qui sont utilisés dans la VoIP tels que : **MGCP, MEGACO, etc.**

4.1. MGCP et MEGACO/H243

Ce sont des protocoles de signalisation asymétriques, qui permettent la mise en communication entre Client-Serveur dont leurs caractéristiques sont les suivants :

4.1.1. Le protocole MGCP : [7]

4.1.1.1. Présentation :

Le protocole MGCP (Media Gateway Control Protocol) est un protocole asymétrique (client-serveur) de la voix IP. Il se distingue des protocoles SIP et H323 qui sont symétriques (client-serveur).

SIP et H323 ont les caractéristiques d'être des protocoles architecturés en mode peer to peer (poste-à-poste), cela veut dire que chaque terminal est indépendant et est donc capable d'établir des communications (appels) et les services associés. Les terminaux SIP/H323 ont la particularité d'être autonome.

En outre, en scrutant les tendances et les attentes des entreprises en matière de télécommunication, on constate que très peu de ces terminaux autonomes ISDM (Informed Shared Decision Making) sont utilisés dans un réseau. La majorité des postes téléphoniques clients sont des postes simples (analogiques) n'assurant que les fonctions d'appels de base et sont eux-mêmes contrôlés par commutateur (PABX) pour la gestion des services spécifiques des appels.

Ainsi, il était nécessaire d'avoir un protocole VoIP apte de fonctionner de la même manière pour pouvoir laisser le contrôle des fonctionnalités à l'opérateur et ne délivrer que les services de base (appel, décroché, raccroché) côté abonné. D'où, la gestion des services d'appels est centralisée et assurée côté serveur, tandis que les terminaux côté clients ne gèrent que les fonctionnalités basiques d'appels et vont recevoir les instructions du serveur. Ce type de procédé est très utile dans un environnement où l'opérateur désire garder le contrôle des services sur l'abonné.

4.1.1.2. Architecture de la MGCP :

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

- **Les terminaux MGCP :** cela se trouve du côté clients qui sont des passerelles chargées de recevoir et de restituer les instructions du contrôleur central (call agent).

- **Le call agent :** il est responsable du réseau MGCP, il s'occupe de commander et fournir des instructions aux passerelles MGCP. Le call agent et les terminaux vont communiquer par des échanges de transactions en utilisant le port UDP 2727(call agent) et 2427(terminaux). Les flux voix sont gérés également par le protocole RTP/RTCP comme en SIP et H323.
  Le protocole MGCP est complémentaire à H323 ou SIP, et traite des problèmes d'interconnexion des terminaux IP et PSTN. MGCP intervenant que sur la bordure du cœur du réseau.

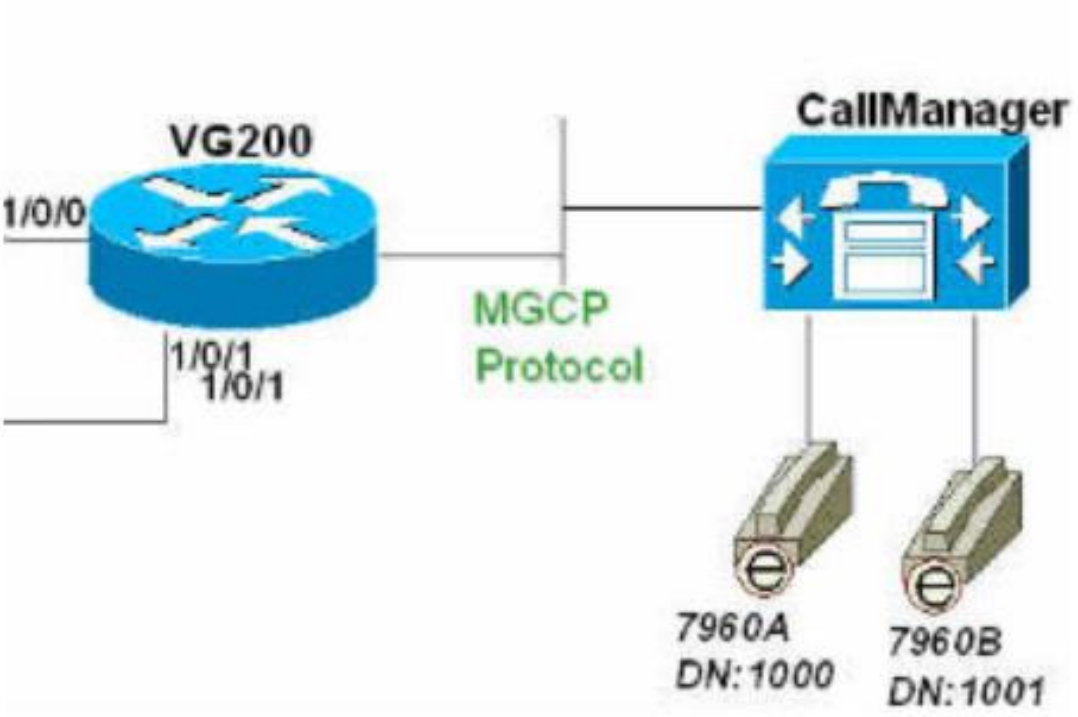


Figure 16 : *Architecture de la MGCP[7]*

4.1.2. MEGACO/H.248 : [12]

4.1.2.1. Présentation :

Le protocole H.248 est nommé MEGACO qui est un accomplissement des efforts d'ITU et d'IETF. Le protocole dérive du MGCP et possède des améliorations par apport à celui-ci :

- Il support des services multimédias et des vidéoconférences.
- Il utilise des codages en modes textes.
- Possibilité d'utilise UDP, TCP et SCTP.

4.1.2.2. Architecture du MEGACO/H248 :

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

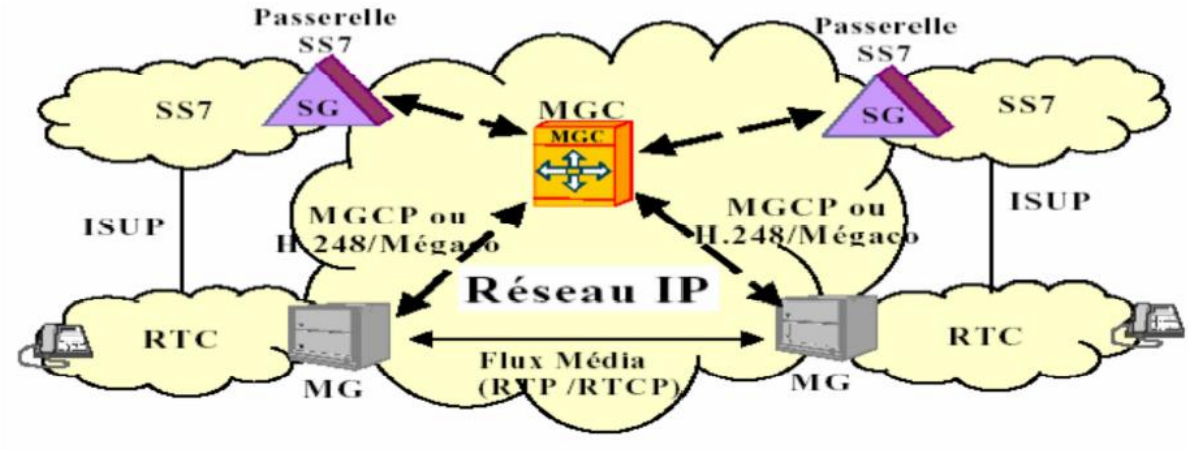


Figure 17 : *Architecture de H.248/MEGACO[12]*

❖ **Les équipements utilisés :**

MG (Media Gateway) : une media Gateway fait la conversion des flux médias entre les différents réseaux.

MGC (Media Gateway Controller) : il contrôle l'état d'appel pour les communications entre le soft switch et une media Gateway.

Terminaison : est une entité logique dans une MG, représentant des ports connectes à celle-ci, capable d'envoyer ou de recevoir un ou plusieurs flux médias. Elle est décrite par un ensemble de caractéristiques qui sont groupes sont groupes dans un ensemble de descripteurs inclus dans des commandes.

Chaque terminaison définit un seul contexte et désigné par un indicateur de terminaison unique (Terminaison ID) choisie par le MG.

4.2. Le protocole IAX, le protocole d'Asterisk pour la NAT : [7]

IAX, est un protocole de signalisation qui peut remplacer le protocole SIP. Il s'agit du protocole sur lequel se base Asterisk bien que ce dernier soit en mesure de supporter les autres principaux protocoles de la VoIP comme le SIP. Il permet d'établir la communication entre client et serveur et entre serveurs. Il est plus puissant que SIP, car il a été conçu spécialement pour le contrôle et la transmission de flux multimédia avec un débit plus faible.

❖ **Fonctionnement :**

IAX2 utilise un port UDP unique qui est le port 4569 (IAX1) utilise le port 5036) et ceci marque l'une des grandes différences avec le protocole SIP. En effet, le protocole SIP, en plus de sa fiabilité, est également célèbre pour sa principale limite qui est la difficulté à l'implémenter derrière un NAT.

5. Conclusion :

Lors de l'élaboration de ce chapitre, nous avons eu à parler de la téléphonie, puis nous avons présenté les deux Réseaux téléphoniques classiques dont le RTC et RNIS tout en énumérant leurs avantages et inconvénients. Ainsi, nous avons abordé les enjeux de la téléphonie sur IP.

La VoIP est une solution plus avantageuse pour effectuer des conversations ; il est évident qu'elle présente un intérêt considérable et une nouvelle étape dans l'évolution des technologies des télécommunications. C'est une technologie qui apporte une solution d'implémentation, fiabilité et coût, sans oublier qu'elle ne possède pas un standard unique et que chaque standard présente des caractéristiques diffèrent pour assurer une bonne qualité de service.

La qualité de service sera l'objet de notre prochain chapitre.

CHAPITRE 2

Eléments de base de l'implémentation
De la Qualité de Service

1. Introduction :[6]

La qualité de service (QOS) est le terme utilisé pour représenter l'ensemble des contraintes imposée par un usager (être humain ou composant logiciel) sur la performance d'une application lors de son exécution. Elle se manifeste par des paramètres pouvant prendre des valeurs qualitatives, c'est-à-dire qui ne peuvent pas être mesurée directement mais perceptibles par l'utilisateur, ou bien se traduit par des valeurs quantitatives qui sont directement observées et mesurées aux points d'accès. Pour pouvoir fournir les services demandés le gestionnaire de réseau gérer en vérifiant les ressources réseau, les utilisateurs, et les serveurs. Le gestionnaire réseau a donc la mission de contrôler toutes les affectations des ressources. Le but de la qualité de service (QOS) est donc d'optimiser les ressources du réseau et de garantir une bonne performance des applications, elle permet d'offrir aux utilisateurs des débits et de temps de réponse différenciés par application suivant les protocoles mis en œuvre au niveau de la couche réseau.

2. Paramètre de QoS :

2.1. Latence :

La latence ou le délai de transmission représente le temps d'acheminement entre le transfert d'un paquet et sa réception par le destinataire. Dans la téléphonie, la maitrise de transmission est l'un objectif primordial parmi tant d'autre afin de bénéficier d'un véritable mode conventionnel et minimiser la perception d'écho qui crée une réverbération. Cette réverbération est causée par les composants électroniques des parties analogiques. Un écho < 50 ms n'est pas perceptible. Au-delà, l'interlocuteur s'entend parler en retard. Ceci dit la transmission est subdivisée en plusieurs délais qui sont :

- **Le délai de transit :** il représente le temps d'acheminement des paquets jusqu'au destinataire, il est composé de :
- **Délai de traitement :** c'est le temps que prend le routeur pour faire parcourir le paquet de l'interface d'entrée, inspecté et le place dans la file d'attente de l'interface sortie.
- **Délai de mise en file d'attente :** c'est le temps que le paquet écoule dans la vie la file d'attente de sortie du routeur. Cela dépend du nombre et la taille des paquets déjà dans la file d'envoie et de la bande passante de l'interface, ainsi du mécanisme de la file d'attente adopté.
- **Délai de sérialisation :** c'est le temps fait pour que la trame soit mise sur le support de transmission.
- **Délai de propagation :** c'est le temps que prend la transmission d'un bit par le biais d'un média de transmission.

2.2. Perte de paquets :

La perte de paquets ou Loss, est le paramètre qui représente le pourcentage des unités de données qui ne peuvent pas arrivée au destinataire dans un intervalle de temps donnée. Cette perte de paquet est causée par la saturation du buffer (mémoire) d'une interface saturée, qui se trouve dans le routeur. Ainsi ils libèrent automatiquement de la bande passante en se débarrassant d'une certaine proportion des paquets entrants, en fonction du seuil fixé.

Si aucun procédé fiable de récupération des paquets perdus n'est mis en place, alors la perte de paquets IP se traduit par des ruptures de la conversation et une impression de coupure de la parole.

2.3. Gigue :

C'est la variation temporelle de bout en bout du délai de transit (latence). En d'autres termes, elle est la conséquence du fait que tous les paquets contenant des échantillons de voix ne vont pas traverser le réseau à la même vitesse. Cela crée une déformation de la voix ou un hachage, pour compresser la gigue on utilise généralement des mémoires tampons.

Elle est indépendante du délai de transit. Le délai peut être court et la gigue importante ou inversement. La gigue est le résultat d'un encombrement passage sur le réseau, ce dernier ne pouvant plus transporter les données de manière constante dans le temps. La valeur de la gigue va de quelques ms à quelques dizaines de ms.

2.4. Bandwidth : [13]

La gestion de la Bandwidth ou bande passante QoS, permet de contrôler les flux de trafic sur un réseau afin que le trafic n'excède pas la capacité du réseau (risque de congestion du réseau) et vous permet également d'allouer de la bande passante pour certains types de trafic, pour les applications et les utilisateurs. La QoS, aide à faire respecter la largeur de bande pour le trafic à une échelle étroite ou large.

3. Classification et Marking :

3.1. Traffic Classification et Traffic Marking : [14]

La classification est un processus qui permet d**'examiner** les champs d'en-têtes **dans le but de prendre une action QoS** sur un paquet.

Le Marking est un processus qui permet **de modifier** les valeurs des champs "ToS" ou "Traffic Class".

3.1.1. Les Méthodes de classification Cisco :

Cette classification peut se réaliser :

- Sur la base des paquets avec des champs disponibles dans les ACLs, dans des class-maps.
- Par interface, automatiquement avec le système "Network-Based Application Recognition" (NBAR).
- Par interface, avec le champ « **Type of Service (ToS)** » d'un paquet IPv4 ou le champ « **Traffic Class** » d'un paquet IPv6 qui sont mise en valeur par une valeur « DSCP » (differentiated service code point), le champ **Class of Service (CoS**) d'un en-tête IEEE 802.1q.
- Par interface, avec les "trust modes".

Remarque : Committed Access Rate (CAR) et Policy-Based Routing (PBR) sont des méthodes obsolètes Cisco IOS de classification.

3.1.2. Les Champs d'en-têtes QoS :

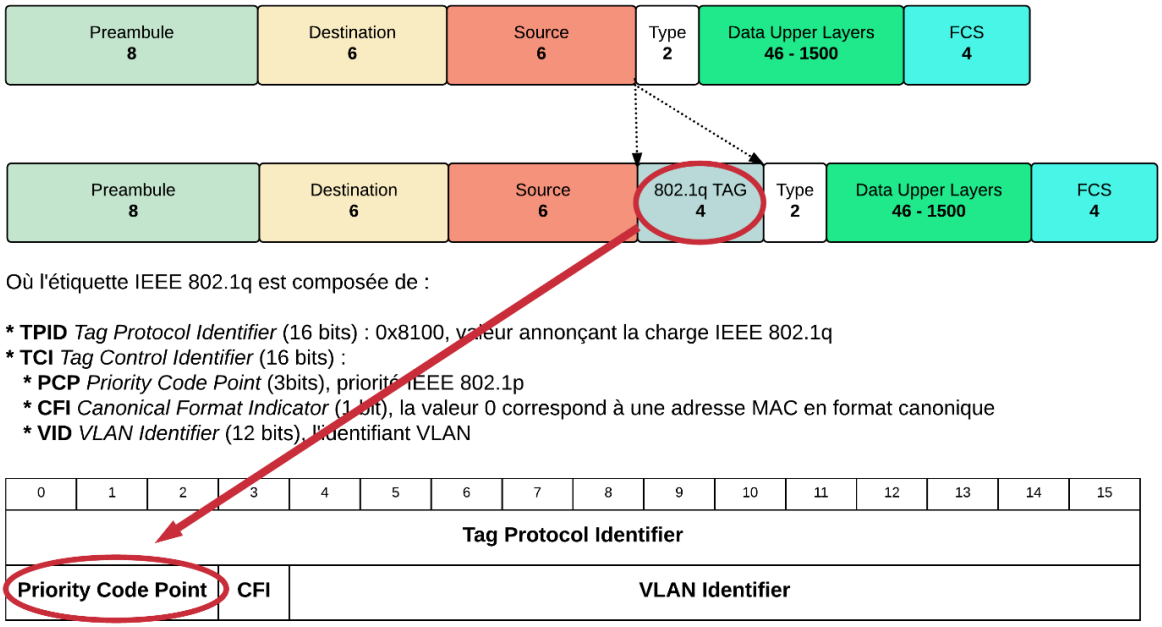


Figure 18 : *Champ "CoS" d'une trame Ethernet[14]*

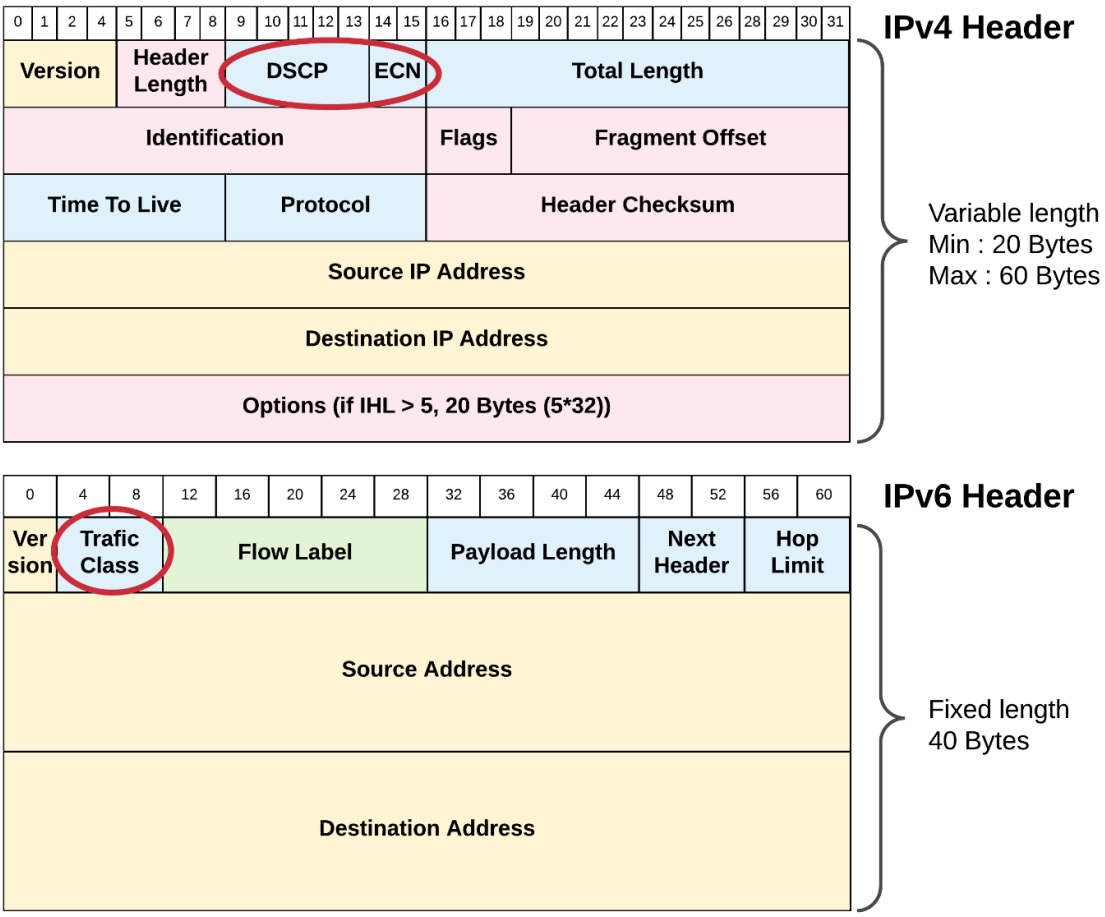


Figure 19 : *Les Champs « DSCP (ToS) » et « Traffic Class » d'un paquet IPv4 et d'un paquet IPv6.[14]*

3.1.3. Correspondance par défaut entre les champs CoS et DSCP :

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

3.1.4. Correspondance par défaut entre les champs IP Precedence et DSCP :

IP Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

3.1.5. Trust Boundaries :

Lorsqu'un commutateur fait confiance à la valeur du champs « CoS » d'un paquet entrant sur un port **QoS trusted**, il fait la correspondre de la valeur entrante avec une valeur "DSCP". Lorsque l'interface est configurée en mode **QoS unstruted**, le commutateur marque tous les paquets entrants avec une valeur « DSCP » interne à 0.

Par exemple, les téléphones IP peuvent marquer avec une valeur "CoS" les trames qu'ils placent sur les commutateurs.

3.1.6. Le Marking :

- Le *« marking »* fait allusion aux modifications apportées aux valeurs "DSCP", "CoS" ou "IP Precedence" des trames et des paquets entrants.
- Il peut se configurer par interface ou avec des **policy maps** (sortes d'ACLs évoluées).
- Il modifie les valeurs "DSCP" des paquets pour la convertir en valeur "DSCP" interne.

3.2. Link efficiency : [15]

Le logiciel Cisco IOS offre un certain nombre de mécanismes ou de caractéristiques d'efficacité de la couche de liaison (énumérés ci-dessous) conçus pour réduire la latence et la gigue du trafic réseau. Ces mécanismes fonctionnent avec la mise en file d'attente et la fragmentation pour améliorer l'efficacité et la prévisibilité des niveaux de service des applications.

Les mécanismes de l'efficacité de la couche de liaison sont les suivantes :

3.2.1. PPP Multilink :

Au niveau supérieur, le PPP Multilink (également connu sous le nom de MLP ou simplement Multilink) fournit l'entrelacement de paquets, la fragmentation, et le re-séquencement des paquets sur de multiples liaisons de données logiques. L'entrelacement des paquets, le paquet.

La fragmentation et le re-séquencement des paquets sont utilisés pour tenir compte des délais de transmission rapides requis pour l'envoi de paquets en temps réel (par exemple, des paquets de voix) sur les liaisons du réseau. Multilink est particulièrement utile sur des liaisons réseau lentes (c'est-à-dire une liaison réseau dont la vitesse est inférieure ou égale à 768 kbps).

3.2.2. Fragmentation des relais de trames :

Cisco a développé les trois méthodes suivantes pour effectuer la fragmentation du Frame Relay:

- Fragmentation de bout en bout FRF.12 (et plus)
- Fragmentation du Frame Relay à l'aide du FRF.11 (et plus)
- Encapsulation propriétaire de Cisco

3.2.3. Compression d'en-tête :

La compression d'en-tête est un mécanisme qui comprime l'en-tête IP dans un paquet avant que celui-ci ne soit transmis. La compression de l'en-tête réduit la surcharge du réseau et accélère la transmission du transport en temps réel. Les paquets de protocole (RTP) et de protocole de contrôle de transmission (TCP). La compression de l'en-tête réduit également la quantité de bande passante consommée lors de la transmission des paquets RTP ou TCP. Cisco fournit deux types de compression d'en-tête de base : la compression d'en-tête RTP (utilisée pour les paquets RTP) et Compression de l'en-tête TCP (utilisée pour les paquets TCP).

3.3. Congestion Management :

La gestion de la congestion fait allusion aux éléments mis en œuvre sur les interfaces qui par défaut mettent les paquets dans des **files d'attente**, sortes de tampons, quand elles rencontrent un problème de ressource pour transférer le trafic (soit de la congestion).

C'est dans le "Queuing" que le marquage et la classification s'avèrent utiles.

3.4. Congestion Avoidance :

Les techniques d'évitement de congestion (*congestion avoidance*) observent la charge du trafic sur les interfaces dans le but d'anticiper et éviter la gestion sur des goulots d'étranglement connus du réseau.

Deux algorithmes d'évitement de congestion sont utilisés sur les commutateurs Cisco :

- **La Chute de la Queue** (Tail Drop) Utilisé par défaut
- **Détection Précoce Aléatoire Pondérée** (Weighted Random Early Detection) ou **WRED**

4. Eléments de base de l'implémentation de la QoS : [16]

L'évolution des diverses applications et ses exigences dans les réseaux convergent a entrainé le développement de trois modèles principaux pour l'implémentation de la qualité de service :

4.1. Le modèle Best Effort :

Dans ce modèle, chaque nœud dans le réseau essayera de livrer chaque paquet de donnée à son destinataire dans un délai de temps raisonnable, mais il ne fait absolument aucune garantie et aucune qualité de service. Des paquets peuvent donc être livrés en retard ou pas du tout.

L'avantage, c'est qu'il est relativement simple à mettre en œuvre. L'architecture best-effort établi par les réseaux IP ne permet pas de garantir aucune qualité de service, donc il a été nécessaire de définir des nouvelles architectures de réseaux pour répondre à ces nouveaux besoins. De cette nécessité sont nées les architectures à intégration de service (modèle IntServ) qui s'appuient sur une réservation préalable des ressources et un multiplexage statistique des trafics, et plus récemment les architectures à différentiation de services (modèle DiffServ) qui effectuent un traitement différencié des trafics, regroupés en quelques classes de services, pour garantir la qualité de service.

4.2. Modèle à intégration de service (IntServ) :

La première proposition d'architecture capable de prendre en charge la Qualité de service (QoS)
a été faite par l'IETF avec le modèle IIS (Internet Integrated Services) ou IntServ. L'idée de base du modèle IntServ est de fournir une QoS individualisée à chaque connexion en utilisant un
mécanisme de contrôle d'admission et de réservation de ressources via le protocole RSVP dans les différents éléments du réseau. Ces ressources permettent d'assurer une certaine qualité de service pour les flots identifiés ayant requis cette qualité de service.

4.2.1. Fonctionnalités :

Le modèle d'implémentation IntServ dans un routeur fait apparaître de nouvelles fonctions pour celui-ci :

- **Reservation Setup Agent :**

Ce processus, exécuté en tache de fond, consiste à recevoir les messages de réservation de ressources, à contrôler la disponibilité des ressources nécessaires (Admission Control), à accepter ou refuser la demande en conséquence et à tenir à jour la table d'états liés aux flots ("Traffic Control Database").

- **Classifier :**

Ce processus, inséré dans le chemin de données après le traitement effectué par le contrôleur d'entrée, consiste à détecter les paquets appartenant à des flots requérant une qualité de service particulière et à classer tous ceux-ci par classe de service.

- **Packet Scheduler :**

Ce processus a pour but de mettre les paquets dans les files d'attente de sortie du routeur en fonction de la classe de service à laquelle ils sont rattachés et de la qualité de service requise.

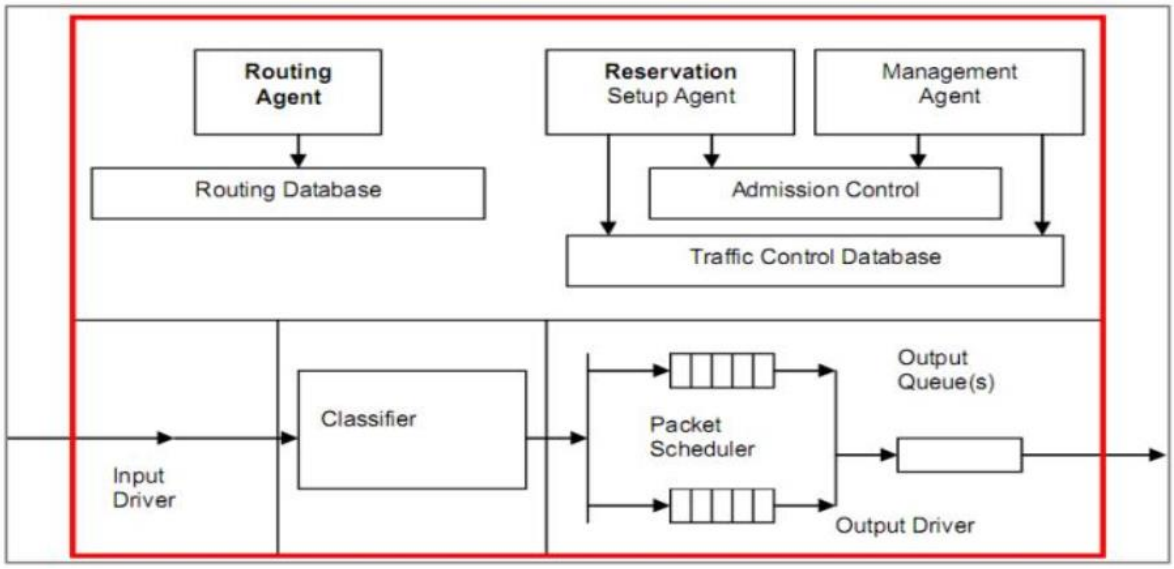


Figure 20 : *Fonctionnalités dans un routeur IntServ[16]*

4.2.2. Les classes de service :

Les classes de service définies dans IntServ sont les suivantes :

- **Guaranteed Service (GS) :**

S'efforce d'assurer le maximum de QoS en garantissant un débit et un temps de transit étroitement définis. Il n'y a cependant pas de garantie sur la gigue. Le service garanti est donc adapté aux applications temps réel non tolérantes (flots les plus exigeants en termes de délai et de débit).

- **Controlled-Load (CL) :**

Est une classe de service intermédiaire qui offre un service équivalent au service best-effort dans un réseau peu chargé. Ce service fournit uniquement des garanties de débit moyen. Il est adapté aux applications temps réel tolérantes qui peuvent tolérer un certain taux de perte ou un certain délai sur les paquets (flux audio, visioconférences).

- **Best-Effort (BE) :**

Le service dit « au-mieux » ou service normal, ne garantit aucune qualité de service, aucun critère de qualité de service n'est considéré pour acheminer les flots de diverses natures. Ce service adapté aux applications élastiques.

4.2.3. Le protocole RSVP (Resource reSerVation Protocol) :

Ce protocole est défini par le RFC 2205, "Resource Reservation Protocol V1", et son mode d'utilisation dans le cadre de IntServ par le RFC 2210, "The Use of RSVP with IETF Integrated Services".

RSVP est utilisé par une application pour demander au réseau d'assurer une certaine qualité de service pour un flot donné. Ce même protocole sera utilisé par les routeurs du réseau entre eux pour établir et maintenir les tables d'états liées au flot. RSVP identifie une session par les

éléments suivants : adresse de destination, le type de protocole utilisé par la couche transport et le numéro de port de la destination.

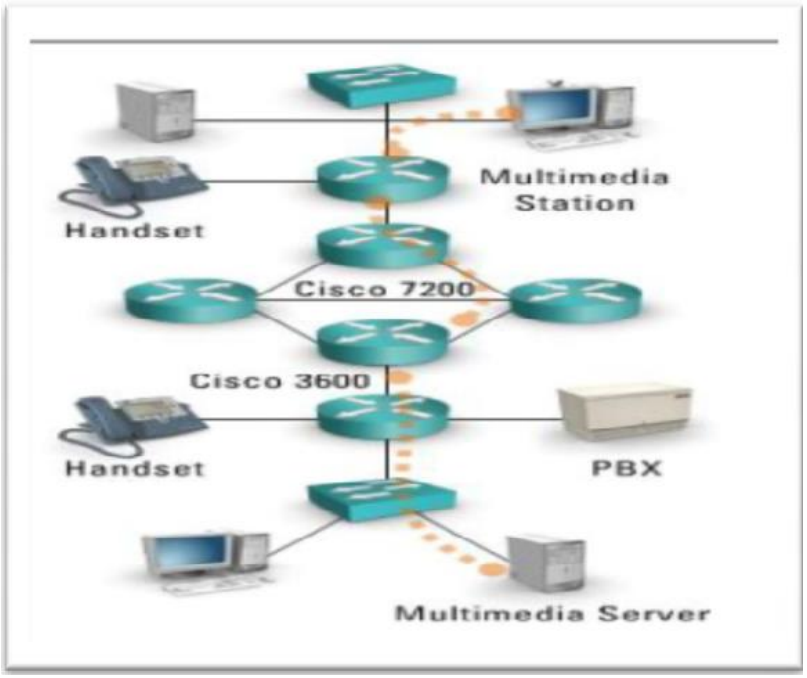


Figure 21 : *Processus RSVP[16]*

RSVP_session = <dest_address, protocol_transport-layer, dest_port_number>

Par ailleurs, le protocole de réservation de ressources est basé sur l'utilisation de deux types de messages unidirectionnels :

- Le message PATH qui permet d'établir un état dans chaque nœud du réseau qu'il traverse et qui trace le chemin à suivre par le second type de message ;
- Le message RESV émis des récepteurs vers les émetteurs et qui consiste à réaliser la réservation proprement dite.

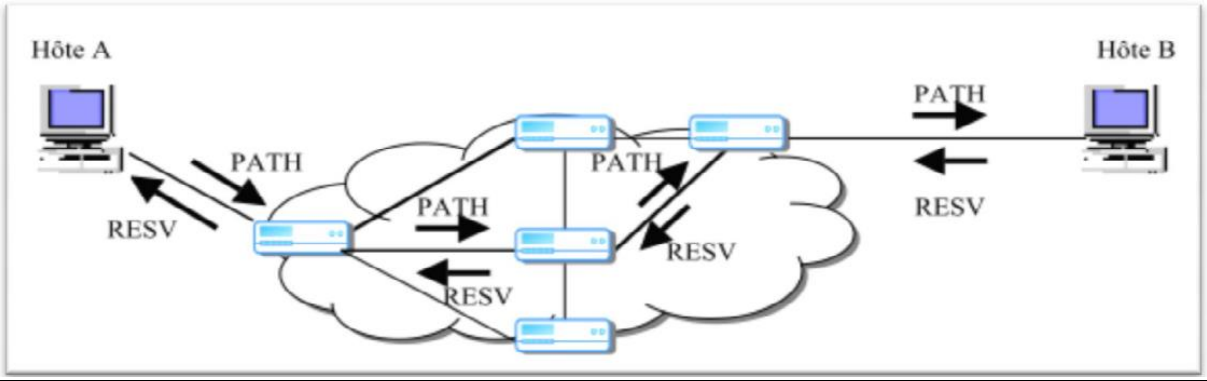


Figure 22 : *Fonctionnement du protocole RSVP.[16]*

L'émetteur du flot envoie régulièrement des messages de contrôle « path » vers le ou les destinataires. Chaque destinataire répond par un message « RESV » dans lequel il indique les critères de la qualité de service qui lui convient. Les ressources nécessaires, si disponibles, sont réservées par les routeurs sur le chemin dentinaire vers l'émetteur. Dans le cas d'un flot

multicast, les différentes réservations concourantes sont agrégées. Dans le cas d'absence de message "path" pendant un certain temps, les ressources réservées sont libérées. Les messages "path" et "resv" sont transmis comme des datagrammes ordinaires en "Best-Effort".

4.2.4. Difficultés et limitation du modèle IntServ :

L'algorithme de RSVP semble être bien complexe puisque chaque routeur doit subir plusieurs opérations ; or les réseaux étant constitués d'un nombre important de nœuds, il est difficile de concevoir l'utilisation de RSVP au sein de réseaux de grande envergure, et à forte charge. La difficulté est notamment due aux communications générées par le protocole entre les équipements, mais aussi au traitement qui est effectué par flots plutôt que par agrégats. Par conséquent, il est incontestable de penser qu'un tel modèle est difficile à déployer à grande échelle et son utilité reste donc restreinte à des niveaux de réseaux locaux de faible étendue.

4.3. Modèle à différenciation de service (DiffServ) :

Devant les limitations du modèle IntServ un second groupe de l'IETF s'est orienté vers un autre modèle d'implémentation de qualité de service, que l'on peut utiliser pour des réseaux importants en envergure, mais aussi en charge : Le modèle à différenciation de services.

Le principe consiste à rejeter dans les routeurs situés aux frontières du réseau toutes les fonctions de classification de paquets et de mise en forme de trafic, tandis que les routeurs du cœur du réseau n'auront qu'à appliquer des comportements prédéfinis (Per-Hop Behaviour) à des agrégats de flots marqués dans ce but par les routeurs de frontière.

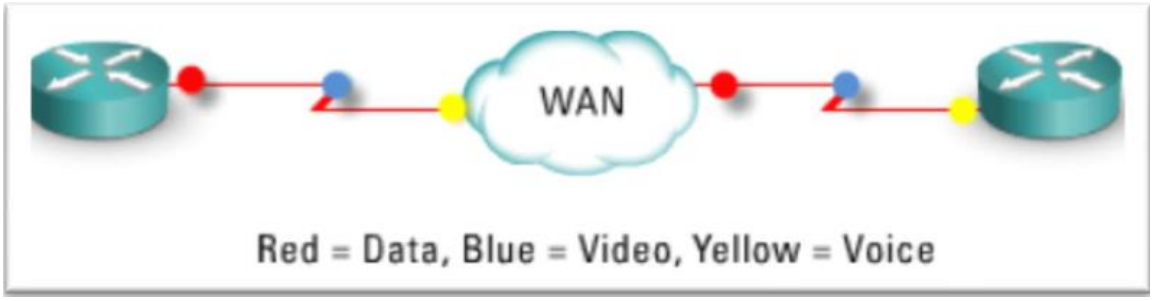


Figure 23 : *Principe DiffServ[16]*

Dans le cœur du réseau, tous les paquets sont marqués, ces marques sont utilisées par des routeurs pour déterminer le comportement qui doit leur être appliqué. Les différents comportements interviennent dans la gestion des files d'attente et dans les algorithmes de sélection de paquets à rejeter en cas de congestion d'une file d'attente. Le choix à faire par le routeur du mode de comportement en fonction de la marque présente dans le paquet est très rapide puisqu'il n'y a plus qu'un seul champ à analyser dans l'en-tête du paquet.

4.3.1. Le champ DS :

Pour l'identification des classes, DiffServ définit un champ de remplacement dans l'entête IP, champ appelé DiffServ (DS) qui remplace les champs déjà existants : Type of Service (TOS) dans l'en-tête IP version 4 ou Traffic Class dans l'en-tête IP version 6. Plus exactement, seulement six bits sur 8 sont utilisés. Les deux autres bits (réservés) sont utilisés pour la notification explicite de la congestion. Les six bits utilisés pour marquer les paquets sont désignés sous le nom DSCP (DiffServ Code Point). Cette valeur DSCP est utilisée par les routeurs cœur pour sélectionner le comportement (PHB) à appliquer au paquet.

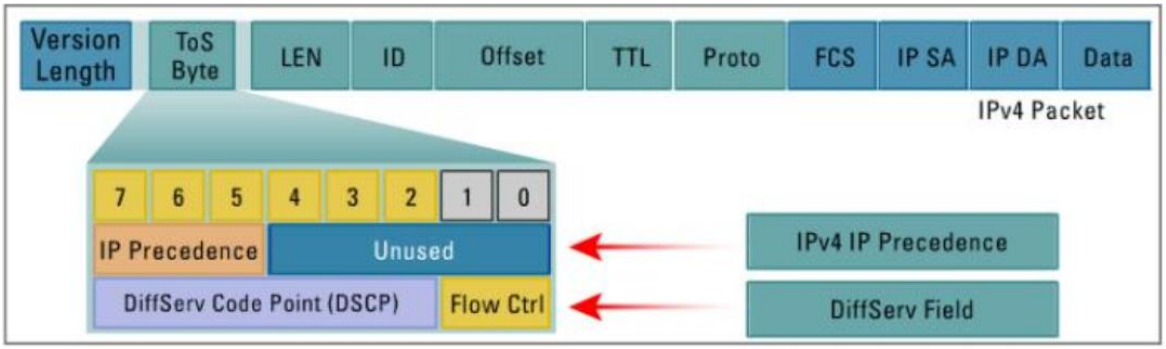


Figure 23 : *Le champ DS dans l'en-tête IPv4[16]*

4.3.2. La notion de comportement (PHB : Per Hop Behavior) :

La RFC 2475 définit le PHB comme le comportement d'acheminement observable de l'extérieur qui s'applique aux données dans un nœud DiffServ. Le système marque les paquets conformément aux codes DSCP et tous les paquets ayant le même code seront agrégés et soumis au même traitement particulier. Un comportement inclut le routage, les politiques de service des paquets (notamment la priorité de passage ou de rejet en cas de congestion) et éventuellement la mise en forme du trafic entrant dans le domaine. Plusieurs PHB standard ont été définis :

- **Le PHB par default** :

Il spécifie que les paquets marqués avec la valeur DSCP «000000 » utilisent le service « traditionnel » Best-Effort dans un nœud DiffServ. De plus, si un paquet arrive dans un nœud et son code DSCP ne correspond à aucun PHB, ce paquet recevra le PHB par default.

- **Assured Forwarding (AF) PHB :**

Ce PHB établit une méthode pour laquelle l'agrégation détermine différents niveaux d'assurances sur l'acheminement des paquets avec une haute probabilité sans tenir compte des délais. Quatre classes AF1, AF2, AF3, et AF4 ont été ainsi définies avec des différents niveaux de traitement (rejet) en cas de congestion du réseau. Dans ce cas-là, les paquets de basse priorité sont rejetés en premier. La priorité peut être modifiée dans le réseau par les opérateurs en fonction du respect ou non des contrats.

- **Expedited Forwarding (EF) PHB** (service premium)

A pour but d'offrir un service robuste avec peu de pertes, avec gigue et délai petits et une bande passante garantie. Pour assurer l'efficacité du système, ce service devrait être réservé pour un certain type d'applications (critiques, multimédia, temps réel). La valeur recommandée pour le code DSCP EF PHB est « 101110 ».

4.3.3. Architecture du modèle DiffServ et terminologie :

L'architecture DiffServ définit les principes suivants :

- Domaine DiffServ (DS domain) :

Un domaine un ensemble de nœuds (hôtes et routeurs) administrés de façon homogène et qui possèdent une même définition de service et de PHB. Dans un domaine, on distingue les nœuds internes et les nœuds frontières : les premiers ce sont des équipements centraux du réseau qui appliquent le comportement approprié (PHB) aux paquets IP et assure le service de transit sur le réseau, alors que, les seconds ce sont des équipements de bordure de domaine DiffServ et qui sont connectés à des nœuds frontières d'autres domaines (Figure 24).

Si on considère le sens de communication de la source vers la destination, les nœuds de frontières peuvent être d'entrée (Ingress) dans le domaine ou de sortie (Egress).

- Région DiffServ (DS région) :

C'est un ensemble contigu de domaines DiffServ, qui peuvent offrir la différenciation des services sur des routes empruntant ces domaines. Chaque domaine ne met pas obligatoirement en ouvre la même politique d'approvisionnement ni les même PHB. L'opérateur doit garantir que l'ensemble des domaines DiffServ assurera une QoS de bout en bout.

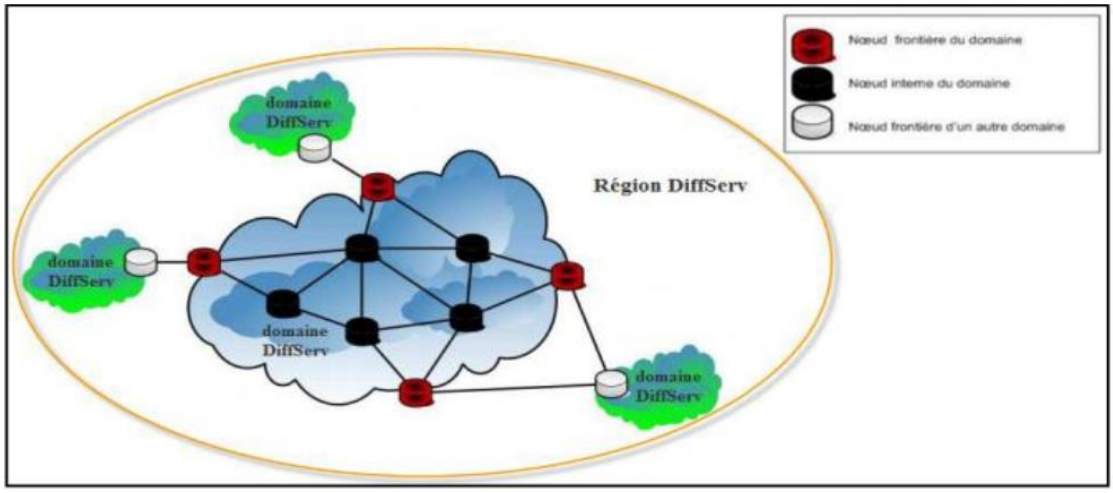


Figure 24 : *Architecture DiffServ[16]*

4.3.4. La notion de SLA (Service Level Agreement) :

L'utilisation des services DiffServ implique pour le client la souscription d'un contrat avec le fournisseur des services : ce contrat s'appelle un Service Level Agreement (SLA). Contrairement à ce qui se passe avec RSVP, ce contrat est signé avant toute connexion au réseau. Les spécifications techniques du SLA sont contenues dans le SLS (Service Level Specification). Le SLA contient les informations suivantes :

- Le trafic que l'utilisateur peut injecter dans le réseau fournisseur (en termes de volume de données, de débit moyen, d'hôtes source ou destination, …) ;
- Les actions entreprises par le réseau en cas de dépassement de trafic (rejet, surtaxe, remise en forme du trafic) ;
- La QoS que le fournisseur s'engage à offrir au trafic généré ou reçu par l'utilisateur (ou les deux). Celle-ci peut s'exprimer notamment en termes de délai, de bande passante, de fiabilité ou de sécurité.

4.3.5. Routeurs de bordure :

Les routeurs de bordure sont les portes d'entrées obligatoires pour un flot pénétrant dans le domaine DiffServ. Ils effectuent des traitements classifier, meter et shapper sur les paquets entrants.

4.3.6. Routeurs de cœur de réseau :

Les routeurs du cœur de réseau réalisent des opérations simples de bufférisassions et de routage des paquets en se basant uniquement sur le marquage effectué par les routeurs situés en bordure de domaine DiffServ. La différenciation de service se fait au niveau des deux mécanismes cruciaux du modèle DiffServ : l'ordonnancement et prévention de congestion.

Chaque sortie du routeur possède un nombre fixe de files logiques où le routeur dépose les paquets arrivant selon leur classe de service. Les files sont servies en accord avec l'algorithme d'ordonnancement. Les trois fonctions principales de routeur de cœur de réseau sont : Routage, prévention de congestion, Ordonnancement Généralement, il n'est pas nécessaire pour DiffServ d'associer un régulateur de type Token Bucket à chaque file des routeurs de cœur de réseau. En effet, tous les trafics entrant dans le cœur de réseau ont déjà subi la fonction de police dans les routeurs de bordure.

5. Conclusion :

Dans ce chapitre, nous avons présenté la qualité de service et ses modèles d'implémentation qui sont basés sur plusieurs mécanismes de gestion de la qualité de service.

La mise en œuvre de l'ensemble des mécanismes décrit dans ce chapitre est une tâche très lourde. Il est difficile, voire impossible, de configurer manuellement l'ensemble des équipements d'un grand réseau. Pour cette raison, on utilise des solutions software basés sur la gestion par politiques permettant de faciliter l'implémentation de ces mécanismes.

CHAPITRE 3

Implémentation de la QoS VoIP

Etude de cas

1. Introduction :

L'objectif de notre travail consiste à déployer la solution Call manager Express de Cisco en configurant l'ordre de priorité dans notre réseau, que nous avons choisi comme solution VoIP. Ainsi, nous allons diviser cette partie en trois dont le déploiement d'une infrastructure réseau avec une topologie comprenant deux réseaux distants ensuite nous allons lancer la solution tout en configurant un FTP-serveur et un FTP-client. Nous achèverons notre travail par des tests d'appels entre deux utilisateurs qui se trouvent dans les deux réseaux distants que nous appellerons Ip-Phone1 (Agence 1) et Ip-Phone2 (Agence 2). Nous avons opté pour un scénario de base conforme à une architecture globale d'un réseau d'entreprises.[17]

2. Présentation du schéma étudié et étape de configuration :

2.1. Présentation du schéma étudié :

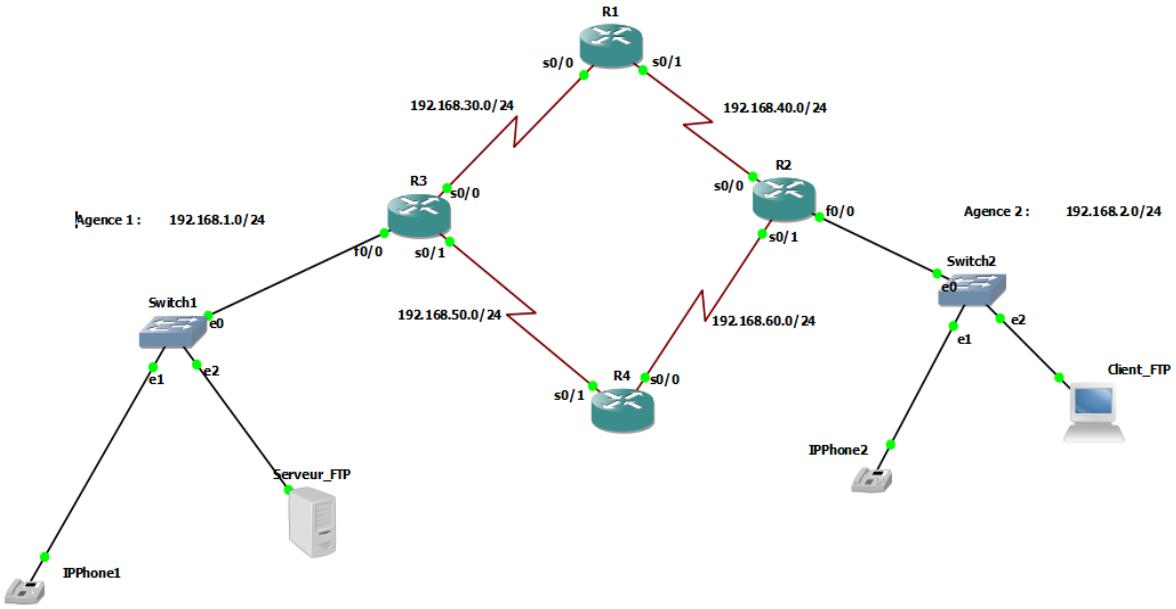


Figure 25 : *Architecture VoIP*

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

- 4 routeurs **(R1, R2, R3 et R4)** ;
- 2 switchs ethernet **(Switch1 et Swich2)** ;
- 2 IP Phones **(IPPhone1 et IPPhone2)** ;
- 1 serveur FTP ;
- 1 client FTP ;

2.2. Etapes de configuration :

La plateforme VoIP est montée sur les routeurs C3725 sur lesquels nous activons les différentes fonctionnalités nécessaires au bon fonctionnement de notre architecture :

- Nous avons mis en marche les interfaces en leur attribuant des adresses IP et régler la fréquence d'horloge à 64000 bits.

R1# R1#Configure terminal R1(config)#interface Serial0/0 R1(config-if)#ip address 192.168.30.2 255.255.255.0 R1(config-if)#clock rate 64000 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#interface Serial0/1 R1(config-if)#ip address 192.168.40.2 255.255.255.0 R1(config-if)#clock rate 64000 R1(config-if)#no shutdown R1(config-if)#exit	R3# R3#Configure terminal R3(config)#interface Serial0/0 R3(config-if)#ip address 192.168.60.2 255.255.255.0 R3(config-if)#clock rate 64000 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#interface Serial0/1 R3(config-if)#ip address 192.168.50.2 255.255.255.0 R3(config-if)#clock rate 64000 R3(config-if)#no shutdown R3(config-if)#exit
R2# R2#Configure terminal R2(config)#interface Serial0/0 R2(config-if)#ip address 192.168.30.1 255.255.255.0 R2(config-if)#clock rate 64000 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#interface Serial0/1 R2(config-if)#ip address 192.168.50.1 255.255.255.0 R2(config-if)#clock rate 64000 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#interface FastEthernet0/0 R2(config-if)#ip address 192.168.1.1 255.255.255.0 R2(config-if)#no shutdown R2(config-if)#exit	R4# R4#Configure terminal R4(config)#interface Serial0/0 R4(config-if)#ip address 192.168.40.2 255.255.255.0 R4(config-if)#clock rate 64000 R4(config-if)#no shutdown R4(config-if)#exit R4(config)#interface Serial0/1 R4(config-if)#ip address 192.168.60.1 255.255.255.0 R4(config-if)#clock rate 64000 R4(config-if)#no shutdown R4(config-if)#exit R4(config)#interface FastEthernet0/0 R4(config-if)#ip address 192.168.2.1 255.255.255.0 R4(config-if)#no shutdown R4(config-if)#exit

- Nous avons utilisé le protocole de routage opsf afin d'établir des liaisons avec ses réseaux voisins :

R1(config)#router ospf 1 R1(config-router)#network 192.168.30.0 0.0.0.255 area 0 R1(config-router)#network 192.168.40.0 0.0.0.255 area 0	R3(config)#router ospf 1 R3(config-router)#network 192.168.50.0 0.0.0.255 area 0 R3(config-router)#network 192.168.60.0 0.0.0.255 area 0
R2(config)#router ospf 1 R2(config-router)#network 192.168.30.0 0.0.0.255 area 0 R2(config-router)#network 192.168.50.0 0.0.0.255 area 0 R2(config-router)#network 192.168.1.0 0.0.0.255 area 0	R4(config)#router ospf 1 R4(config-router)#network 192.168.40.0 0.0.0.255 area 0 R4(config-router)#network 192.168.60.0 0.0.0.255 area 0 R4(config-router)#network 192.168.2.0 0.0.0.255 area 0

- Sur les routeurs R2 et R4 :

Nous avons configuré l'activation du service DHCP qui permet aux routeurs d'attribuer les paramètres IP ainsi que la création des pools voic pour l'attribution automatique des adresses IP aux téléphones IP et PC.

R2(config)#ip dhcp pool VOIC R2(dhcp-config)#network 192.168.1.0 255.255.255.0 R2(dhcp-config)#default-router 192.168.1.1 R2(dhcp-config)#dns-server 4.2.2.2 R2(dhcp-config)#option 150 ip 192.168.1.1	R4(config)#ip dhcp pool VOIC R4(dhcp-config)#network 192.168.2.0 255.255.255.0 R4(dhcp-config)#default-router 192.168.2.1 R4(dhcp-config)#dns-server 4.2.2.2 R4(dhcp-config)#option 150 ip 192.168.2.1

Remarque :

- Option 150 indique au téléphone IP le serveur TFTP.
- Le serveur TFTP (dans notre cas le routeur R2) contient les fichiers de configuration et le firmware pour les téléphones IP.

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

R2(config)#telephony-service R2(config- telephony)#max-ephones 2 R2(config- telephony)#max-dn 4	R4(config)#telephony-service R4(config- telephony)#max-ephones 2 R4(config- telephony)#max-dn 3

Cette commande identifie l'adresse et le port par lequel les téléphones IP communiqueront avec le Router R2 :

R2(config- telephony)#ip source-address 192.168.1.1 port 2000	R4(config- telephony)#ip source-address 192.168.2.1 port 2000

Création des lignes et affectation aux téléphones IP avec ephone-dn et ephone :

R2(config- telephony)#system message Bienvenue_Agence1 R2(config- telephony)#exit R2(config)#ephone-dn 1 dual-line R2(config-ephone-dn)#number 1000 R2(config-ephone-dn)#label Tifon R2(config-ephone-dn)#description Agence_1.Tifon R2(config-ephone-dn)#name Tifon R2(config-ephone-dn)#exit R2(config)#ephone-dn 2 R2(config-ephone-dn)#number 1001 R2(config-ephone-dn)#label personne R2(config-ephone-dn)#name personne R2(config-ephone-dn)#exit R2(config)#ephone 1 R2(config-ephone)#mac-address 000C.29CE.D410 R2(config-ephone)#button 1:1 2:2 R2(config-ephone)#exit	R4(config- telephony)#system message Bienvenue_Agence2 R4(config- telephony)#exit R4(config)#ephone-dn 1 dual-line R4(config-ephone-dn)#number 2000 R4(config-ephone-dn)#label Admin R4(config-ephone-dn)#description Agence2_Administrateur R4(config-ephone-dn)#name Tifon R4(config-ephone-dn)#exit R4(config)#ephone-dn 2 R4(config-ephone-dn)#number 2001 R4(config-ephone-dn)#label personne 2 R4(config-ephone-dn)#name personne 2 R4(config-ephone-dn)#exit R4(config)#ephone 1 R4(config-ephone)#mac-address 000C.29DE.620F R4(config-ephone)#button 1:1 4:2 R4(config-ephone)#exit

3. Descriptions de la solution QoS proposée :

Cisco callManager Express (CME) est une solution de traitement des appels intégrée aux routeurs d'accès Cisco sous la forme d'un ensemble de fonctionnalités du logiciel Cisco IOS.

CME assure la gestion des appels téléphoniques de 1 à 100 téléphones pour les PME (Petites et Moyennes Entreprises). Cette solution offre des services locaux de traitement des appels, de messagerie vocale et d'accueil automatique via une unique plateforme de routage intégrée. Il s'agit donc pour le client d'une solution alliant économie, haute fiabilité et grande richesse fonctionnelle.[18]

4. Présentation de GNS3 :

GNS3 est un émulateur graphique de réseaux capable de charger des vraies images de l'IOS de Cisco permettant ainsi d'émuler entièrement des routeurs ou firewalls Cisco.

GNS3 est un logiciel libre qui fonctionne sur de multiples plateformes incluant Windows, Linux, et MacOS X.

5. Présentation de Vmware :

VMware Workstation est un logiciel permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existante réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte.

6. Configuration GNS3-Vmware :

La configuration GNS3-vmware consiste tout simplement à attribuer les carte réseau virtuel aux appareils disponibles sur GNS3, ainsi la connexion GNS3-vmware est établie.

7. Implémentation de la QoS :

Nous avons envisagé différents types de mécanismes de qualité de service qui pourraient être très utiles pour la mise en œuvre sur un canal de connexion de données encombré et lent afin de réduire la congestion et permettre à certains types de trafic critiques d'être transportés sans retard et sans perte de paquets. Dans ce chapitre, Nous aimerions montrer comment certains mécanismes de qualité de service très simples pourraient, en mis en œuvre sur un réseau d'appareils. Par exemple, nous avons utilisé des appareils Cisco, en tant que produit de mise en réseau. De la même manière, on pourrait configurer des appareils de réseau d'autres marques, mais avec un type de syntaxe différent.

Les informations ci-dessous résument les trois étapes à suivre lors de la configuration de la qualité de service. Chaque étape répond à une question concernant les classes attribuées aux différents flux de trafic :

- **Construisez une class map** :

La première étape du déploiement de la QoS est d'identifier le trafic intéressant. Cette étape définit un groupe de trafic réseau : une class map dans la terminologie MQC avec : divers outils de classification : Listes de contrôle d'accès (ACL), adresses IP, priorité IP, point de code de services différenciés IP (DSCP), IEEE 802.1p, MultiProtocol Label Switching Experimental bit (MPLS EXP), et Reconnaissance des demandes en réseau (Network Based Application Recognition - NBAR). Dans cette étape, nous configurons le trafic en utilisant la commande class-map.

- **Policy map :**

Nous décidons de ce qu'il faut faire avec les classes de trafic de l'étape 1. Cette étape est la construction proprement dite d'une politique de qualité de service. Une Policy-map dans la terminologie MQC : le choix du groupe de trafic (class map) sur lequel est assuré les fonctions de qualité de service. Des exemples de fonctions de qualité de service sont la mise en file d'attente et l'abandon, le maintien de l'ordre, le façonnage et le marquage. Dans cette étape, nous configurons chaque politique de trafic en associant la classe de trafic avec une ou plusieurs caractéristiques de qualité de service à l'aide de la commande "policy map".

- **Service policy :**

Appliquer la carte politique appropriée aux interfaces, sous-interfaces ou autres interfaces souhaitées. Dans cette étape, nous joignons la politique de trafic vers le trafic entrant ou sortant sur des interfaces, des sous-interfaces ou des circuits virtuels en utilisant la commande de "service policy".

Nous avons implémenté la Qos au niveau du routeur R4 grâce aux lignes de commandes suivantes :

```
R4(config)#acces-list 1 permit 192.168.2.4
R4(config)#class-map client
R4(config-cmap)#match access-group 1
R4(config-cmap)#exit

R4(config)#policy-map client
R4(config-pmap)#class client
R4(config-pmap-c)#set precedence 5
R4(config-pmap-c)#exit
R4(config-pmap)#exit

R4(config)#interface FastEthernet 0/0
R4(config-if)#service-policy input client
R4(config-if)#exit
R4(config)#exit
```

- **Explication des commandes :**
  - La commande **acces-list** permet de créer une liste dans laquelle figure les adresses IP autorisés à utiliser la qualité de service proposée.
  - La commande **class-map** permet de créer un trafic dans le réseau.
  - La commande **match** permet associer le trafic créer à un groupe spécifique.
  - La commande **policy-map** permet d'associer la classe de trafic à une ou plusieurs caractéristiques de qualité de service.
  - La commande class permet de choisir parmi les ou la class-map précédemment crée.
  - **Set precedence** consiste à choisir l'ordre de priorité dans notre cas nous avons choisi le 5.
  - La commande **service-policy** permet d'activer les paramétrages de la QoS sur l'interface choisi.

8. Résultat de test :

❖ Etape 1 :

Tout d'abord, nous allons tester le fonctionnement du réseau de bout en bout à l'aide la commande **Ping** entre 2 utilisateurs situés sur les 2 réseaux distants :

```
C:\Users\shine>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time=124ms TTL=125
Reply from 192.168.1.5: bytes=32 time=19ms TTL=125
Reply from 192.168.1.5: bytes=32 time=14ms TTL=125
Reply from 192.168.1.5: bytes=32 time=37ms TTL=125

Ping statistics for 192.168.1.5 :
        Packet: sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 124ms, Average = 45ms
```

```
C:\Users\shine>ping 192.168.2.15

Pinging 192.168.2.15 with 32 bytes of data:
Reply from 192.168.2.15: bytes=32 time=17ms TTL=125
Reply from 192.168.2.15: bytes=32 time=18ms TTL=125
Reply from 192.168.2.15: bytes=32 time=15ms TTL=125
Reply from 192.168.2.15: bytes=32 time=16ms TTL=125

Ping statistics for 192.168.2.15 :
        Packet: sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 18ms, Average = 16ms
```

❖ Etape 2 :

Nous allumons chaque Ip-phone et nous remarquons que chaque Ip-phone a bien était connecté au ligne attribué.

Ip phone 1

Ip phone 2

❖ **Etape 3 :**

Nous lançons l'appel depuis Ip phone 1 (Tifon) vers Ip phone 2 (Admin) et nous remarquons que l'Ip phone 2 sonne

Ip phone 1

Ip phone 2

❖ **Etape 4 :**

La communication est établie aussitôt que Ip phone 2 (Admin) décroche l'appel.

Ip phone 1

Ip phone 2

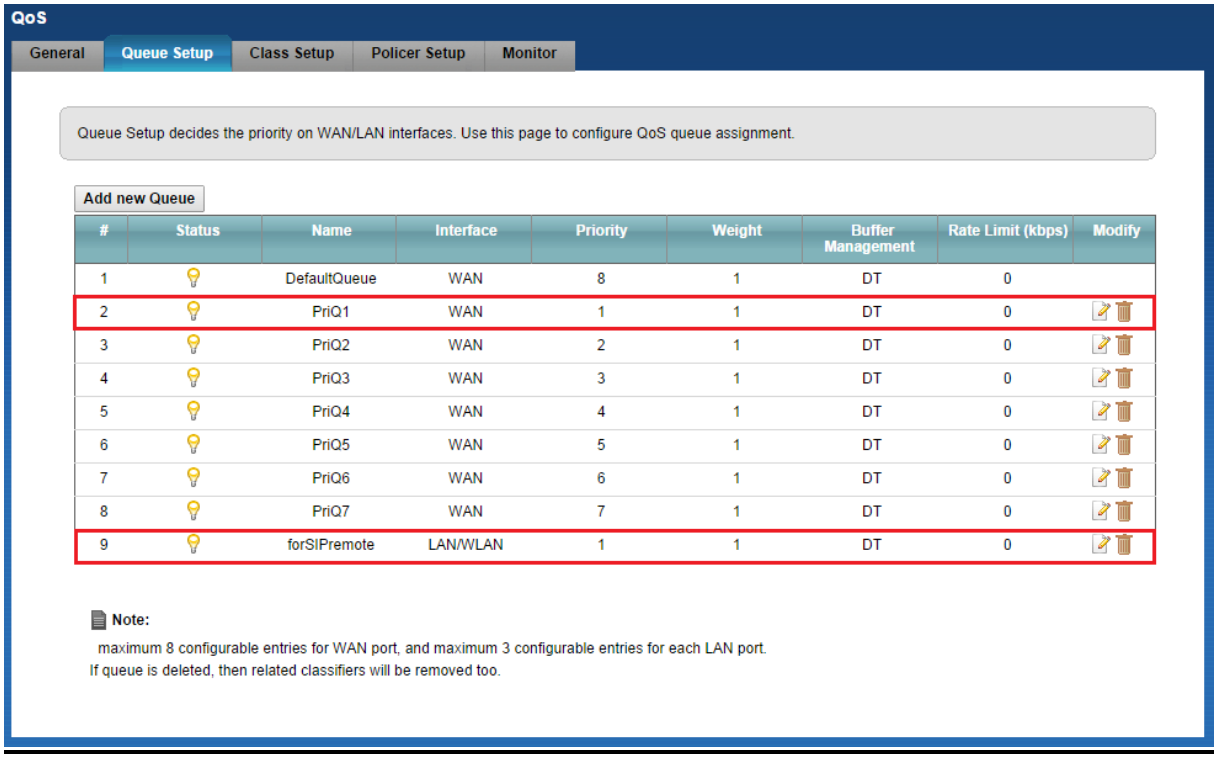


Figure 26 : *Gestion de la QoS au niveau d'un routeur.*

Cette figure ci-dessus représente comment est géré le réseau lors de l'implémentation de la QOS au niveau des interfaces du routeur.

Chaque interface est classée selon un ordre de priorité définie au préalable. Donc lorsqu'il y a un conflit pendant une transmission de données au niveau des interfaces du routeur, le routeur gère les paquets entrant par priorité. Le plus prioritaire est transmis en premier.

9. Conclusion :

Dans ce chapitre au cours de notre travail, nous avons finalisé l'infrastructure de notre réseau ainsi que les diverses configurations implémentées grâce aux divers logiciels dont GNS3 et Vmware afin de permettre l'acheminement du trafic d'information, nous avons par la suite lancé des tests d'appels entre des utilisateurs distants et nous avons fait des captures de nos résultats.

Conclusion générale

Dans ce travail, nous avons eu à parler d'une manière générale sur la téléphonie et des réseaux téléphoniques classiques sans oublier leurs atouts et inconvénients, ainsi que sur la technologie VoIP du point de vu implémentation et ses différents standards. Etant indispensable pour la bonne transmission des paquets VoIP, nous avons parlé d'une manière théorique de la QoS et de son implémentation.

Nous avons proposé le déploiement d'une solution VoIP CME (Call Manager Express) de Cisco pour des raisons de stabilité et pour garantir la fiabilité, et une investigation dans ce domaine à travers l'étude d'un paramètre de QoS qui est celle de priorité d'adresse.

Par conséquent, on a simulé deux réseaux distants avec quatre routeurs Cisco 3725, deux switch Ethernet, deux IP phones, un ftp-server et un pc ftp-client, en utilisant différents types de câbles réseau pour les liens WAN et les liens LAN.

La phase suivante était d'effectuer des appels VoIP entre deux utilisateurs distants, et de capturer la communication à l'entrée et à la sortie pour d'éventuels tests.

Les différents tests recueillis grâce à l'émulation de notre infrastructure ont donné des résultats concluants.

L'utilisation de GNS3, et vmware permet de simuler une situation réelle de déploiement réseau tel est le cas dans notre projet, ce qui est très important dans le monde professionnel.

Tout au long de ce mémoire, nous avons accumulé une masse considérable de connaissances, théoriques et pratiques, dans l'espoir qu'elles nous seront utiles dans le monde professionnel.

Annexes

Installation de GNS3 :

Les étapes qui vont suivre vous montrerons comment télécharger et installer le logiciel GNS3 ainsi que les logiciels prérequis à l'aide d'un environnement Windows.

Pour notre projet nous utilisons la version 2.2.9 de GNS3.

GNS3 prend en charge les systèmes d'exploitation Windows suivants :

- Windows 7 SP1 (64 bits)
- Windows 8 (64 bits)
- Windows 10 (64 bits)
- Windows Server 2012 (64 bits)
- Windows Server 2016 (64 bits)

Dans notre cas nous utilisons Windows 10 (64bits)

❖ Etape 1 :

Vous pouvez télécharger le logiciel GNS3 en allant sur le lien suivant :

https://gns3.com/software

❖ Etape 2 :

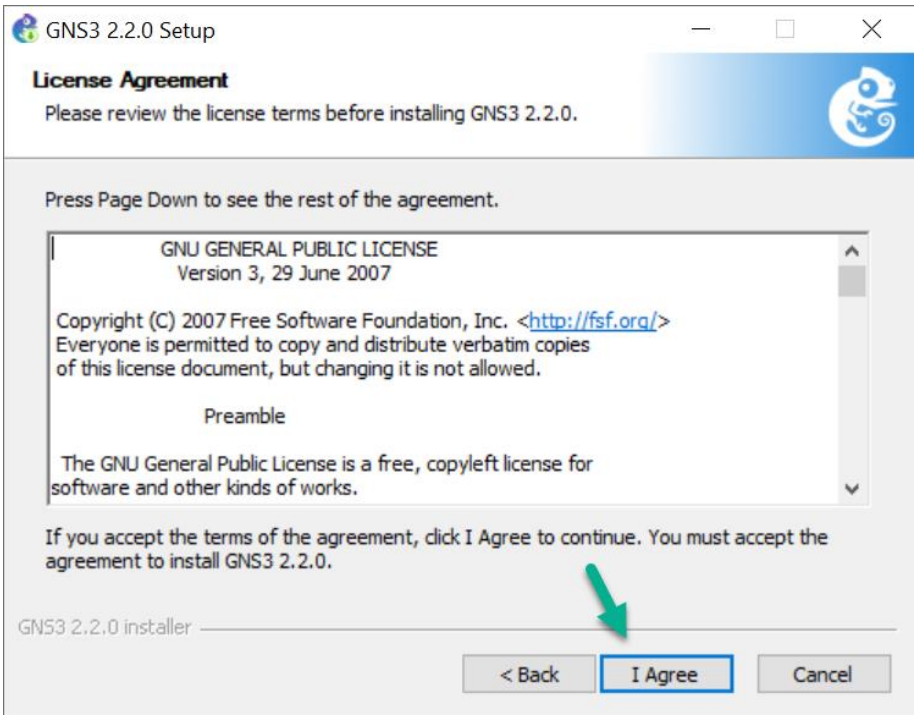
Extraire le fichier téléchargé et lancer le setup GNS3.

❖ Etape 3 :

L'assistant d'installation GNS3 s'affiche. Cliquez sur **Next>** pour démarrer l'installation :

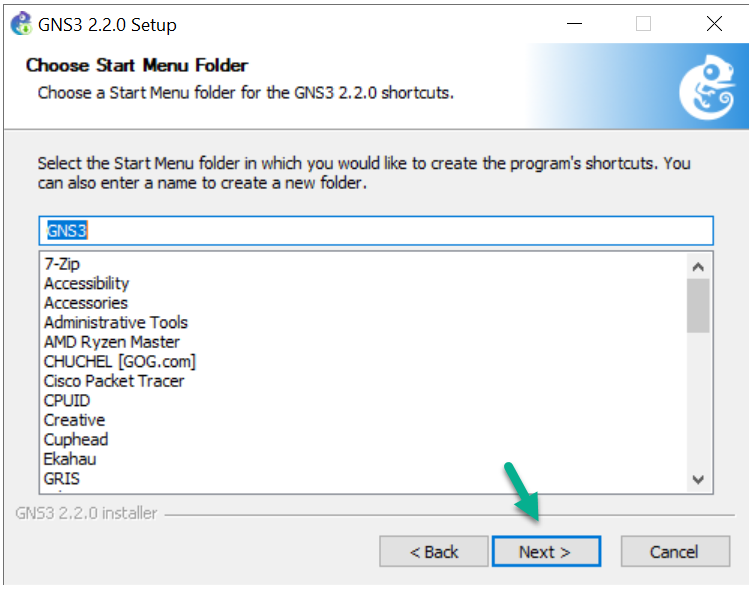
❖ **Etape 4 :**

Lisez le contrat de licence, et si vous êtes d'accord avec le contenu, cliquez sur le bouton **I Agree** pour continuer l'installation :



❖ **Etape 5 :**

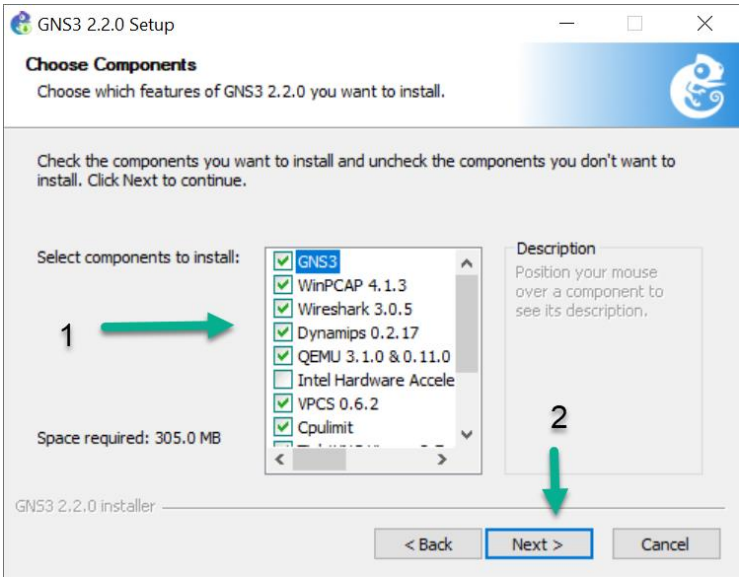
Sélectionnez le dossier du menu Démarrer pour le raccourci GNS3. La valeur par défaut est le dossier GNS3. Cliquez sur **Next>** pour continuer l'installation :



❖ **Etape 6 :**

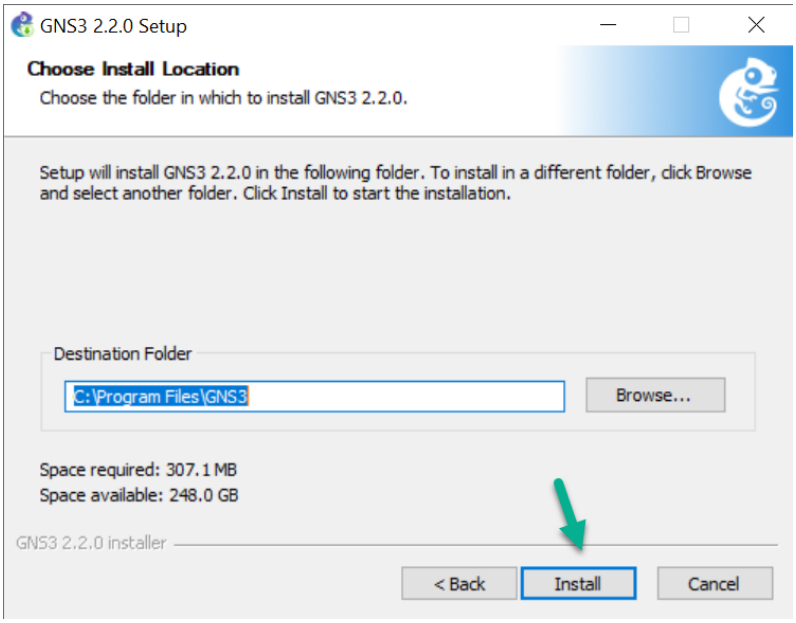
GNS3 est fourni avec divers logiciels prérequis et optionnels. Par défaut, la plupart des logiciels sont sélectionnés pour l'installation, mais vous pouvez décider de n'installer que des logiciels spécifiques.

Si vous n'êtes pas sûr, laissez toutes les sélections de logiciels à leur sélection par défaut et cliquez sur **Next>** pour continuer l'installation :



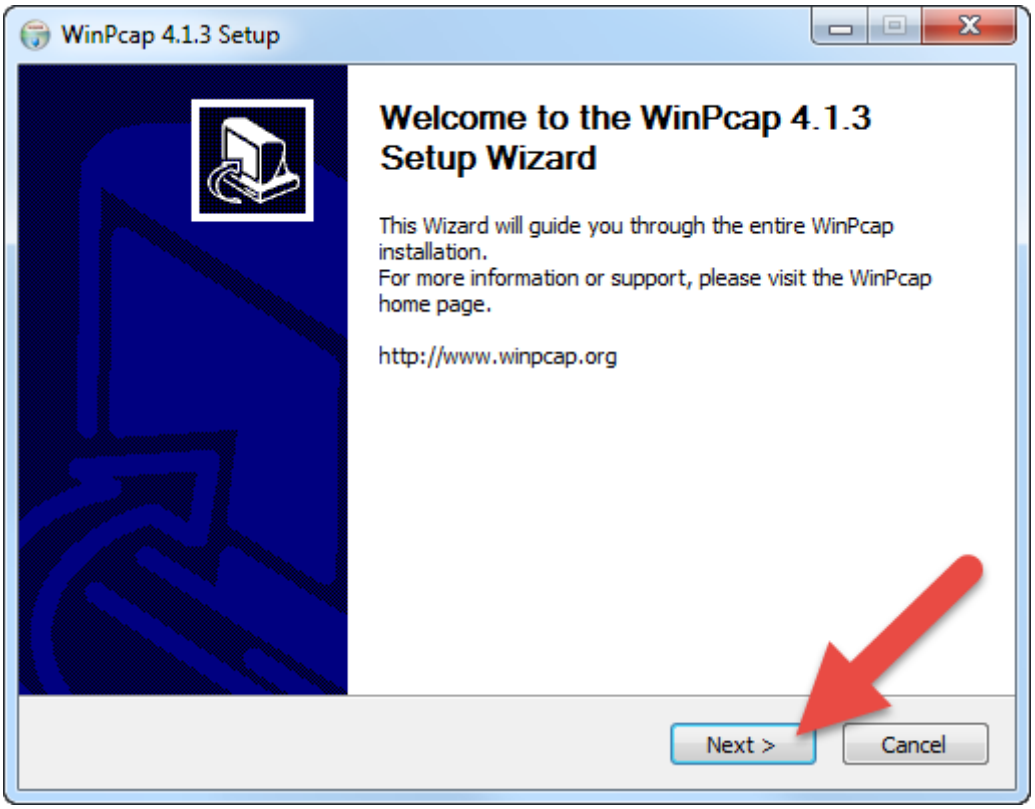
❖ **Etape 7 :**

Choisir un emplacement d'installation. L'emplacement par défaut est **C: \ Program Files \ GNS3** . Cliquez ensuite sur **Install** :



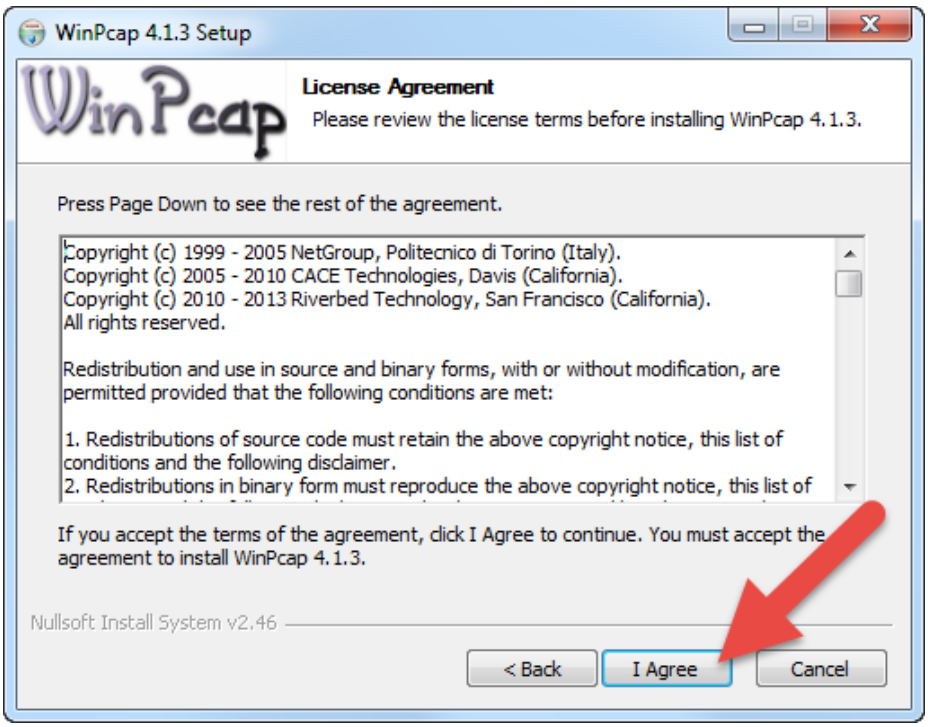
❖ **Etape 8 :**

L'assistant d'installation de WinPcap s'affiche. Cliquez sur **Next>** pour continuer l'installation :



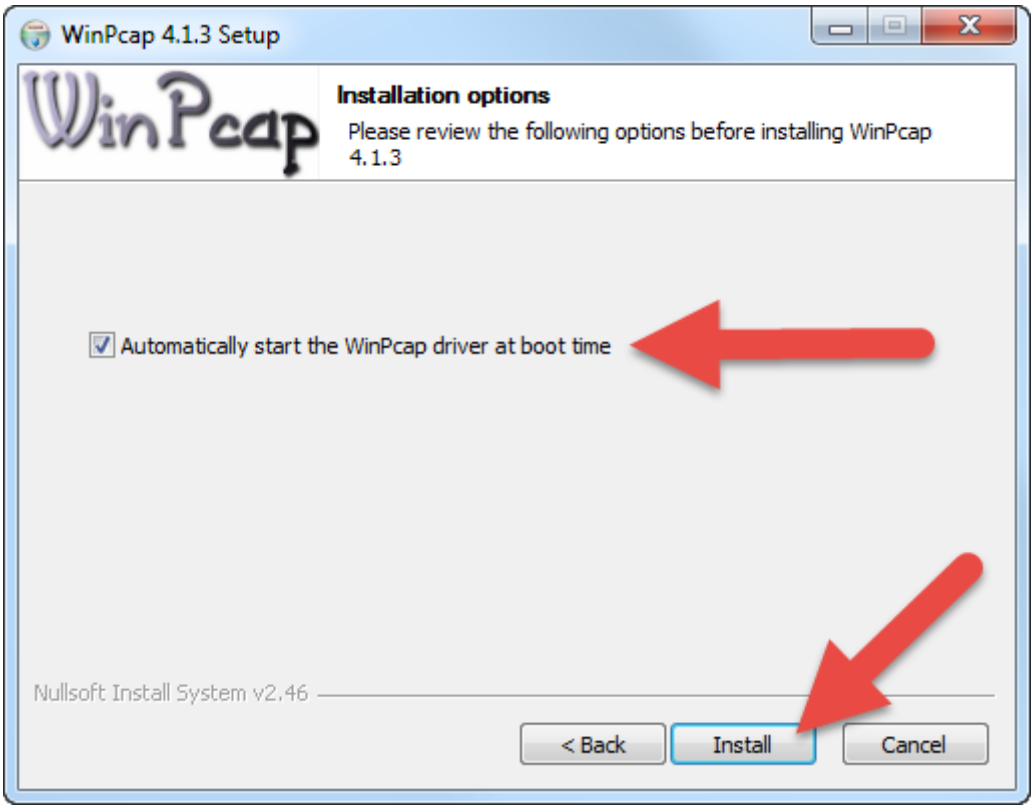
❖ **Etape 9 :**

Le contrat de licence WinPcap s'affiche. Lisez l'accord et si vous êtes d'accord, cliquez sur le bouton **I Agree** pour continuer l'installation :



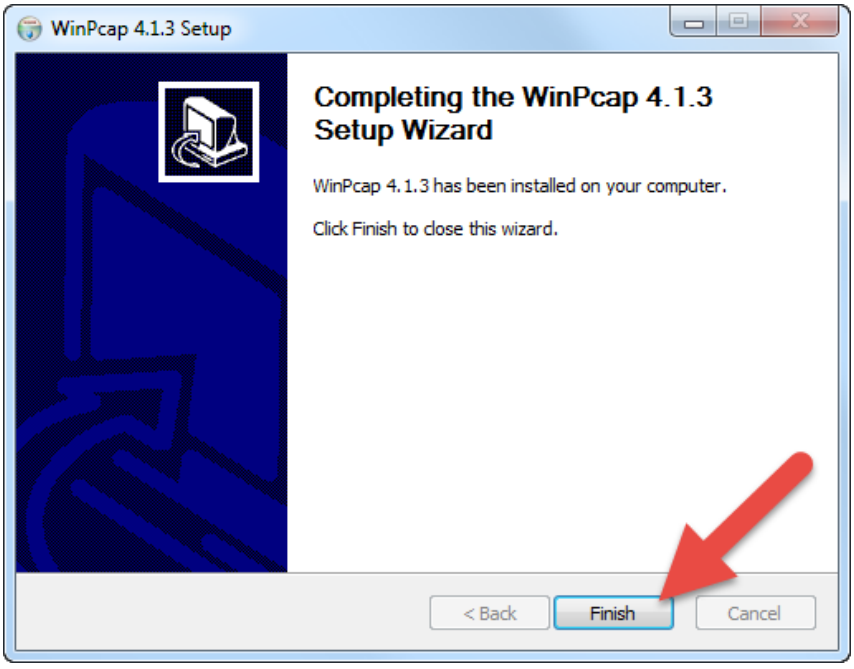
❖ **Etape 10 :**

Laissez la case à cocher **Démarrer automatiquement le pilote WinPcap au démarrage** coché et cliquez sur **Install** :



❖ **Etape 11 :**

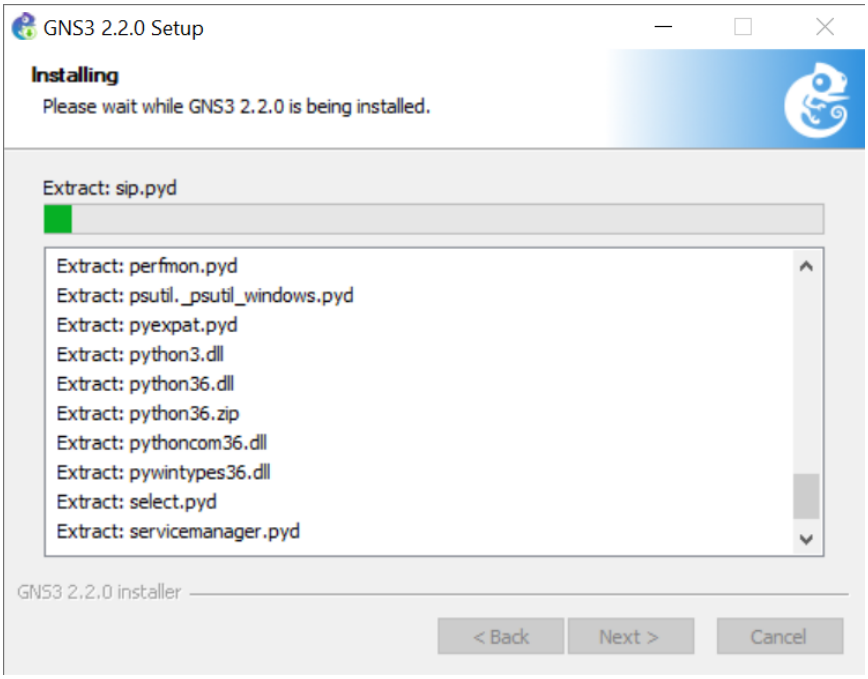
L'installation de WinPcap continue. Cliquez sur **Finish** pour terminer l'installation :



❖ **Etape 12 :**

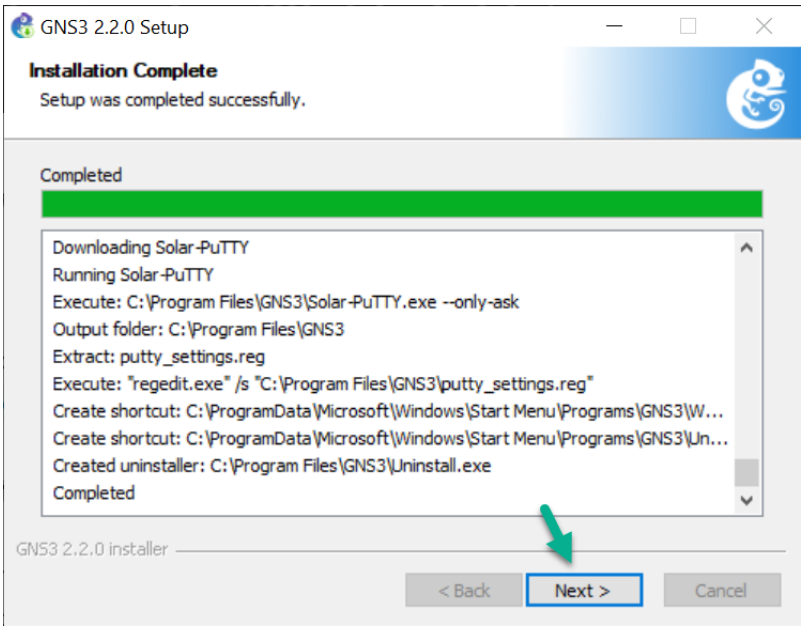
Si vous avez sélectionné l'installation de Wireshark, le logiciel de configuration GNS3 téléchargera les fichiers d'installation de Wireshark. Attendez la fin du processus.

GNS3 effectuera ensuite une installation silencieuse de Wireshark. Attendez la fin du processus.



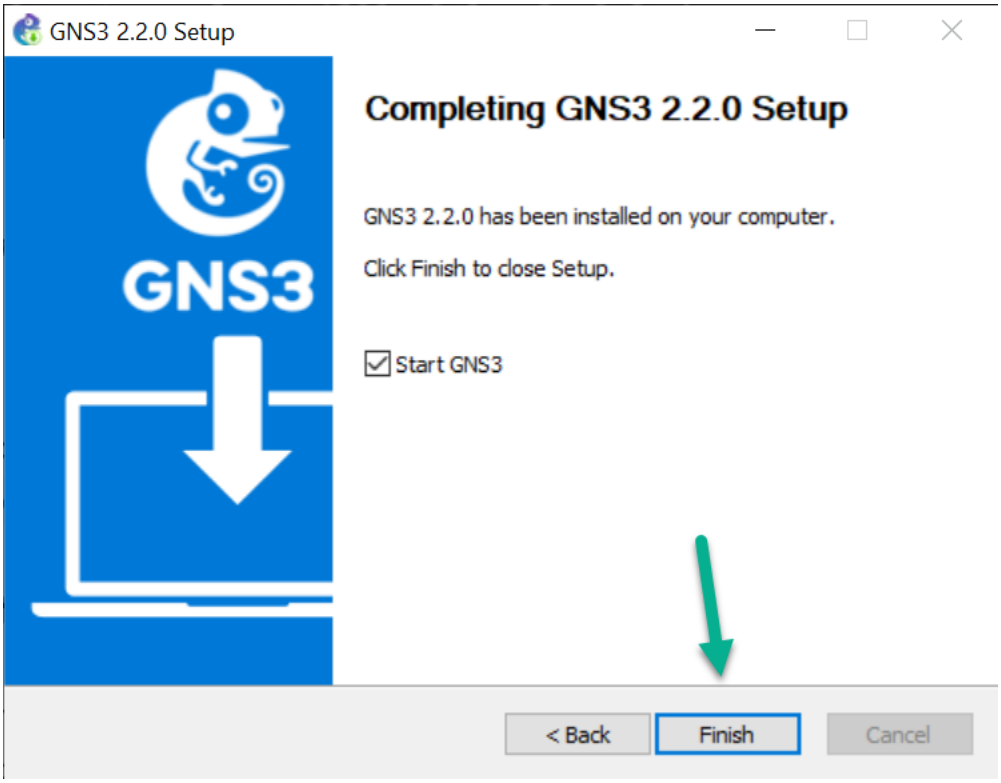
❖ **Etape 18 :**

Une fois le logiciel GNS3 de base (et tous les éléments sélectionnés en option) installés, cliquez sur **Next>**

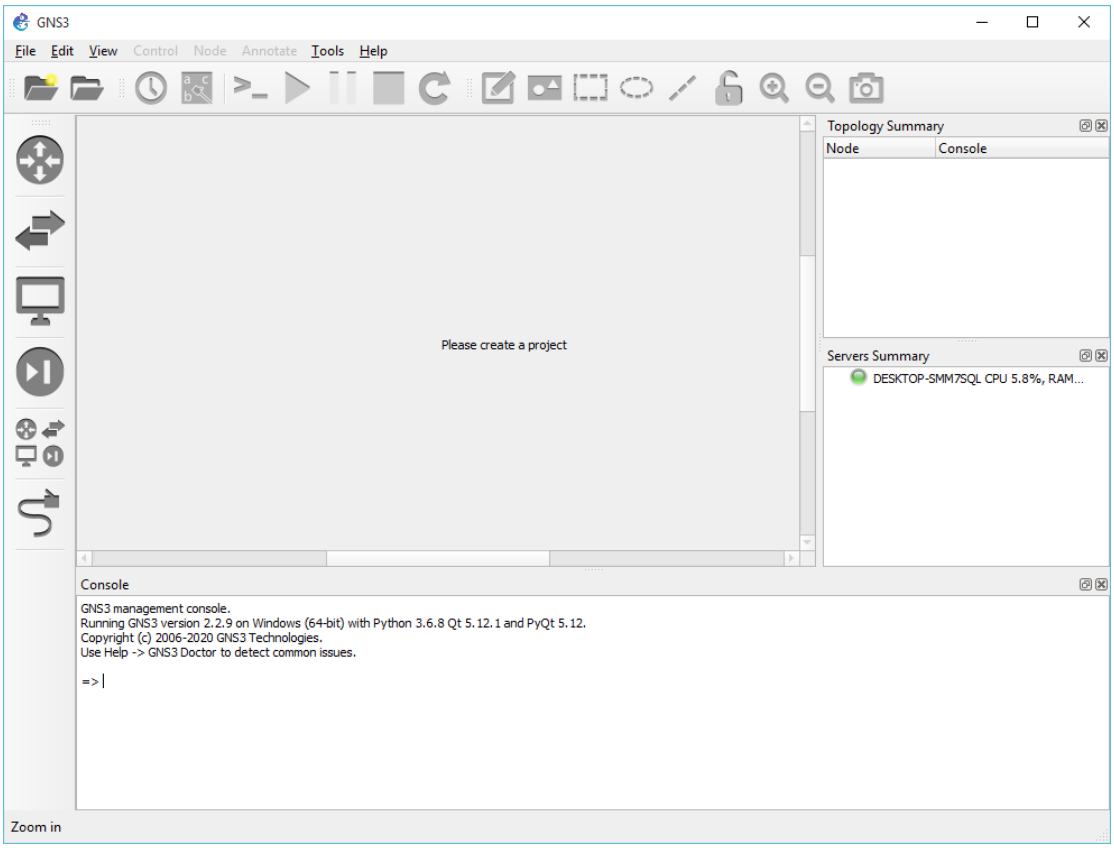


❖ **Etape 19 :**

Cliquez sur **Finish** pour terminer l'installation de GNS3 :



❖ Voici l'interface de GNS3 après son installation.



Installation de Vmware :

Les étapes qui vont suivre vous montrerons comment télécharger et installer le logiciel Vmware à l'aide d'un environnement Windows.

Pour notre projet nous utilisons Vmware Workstation Pro 12.

Etape 1 :

Vous pouvez télécharger le logiciel Vmware grâce à ce lien.

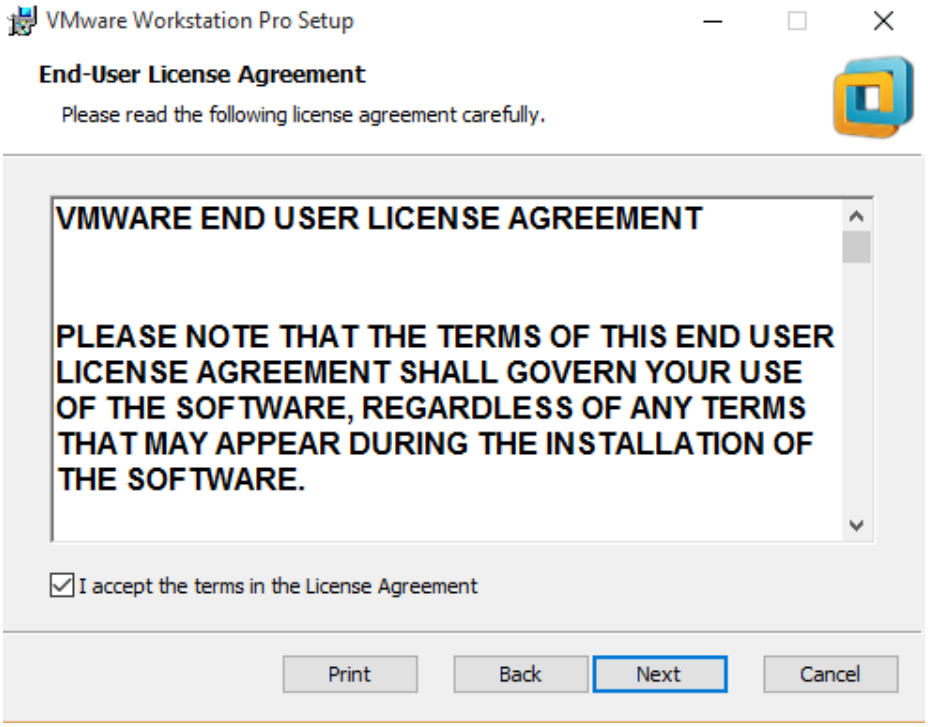
https://my.vmware.com/fr/web/vmware/details?downloadGroup=WKST-1259-WIN&productId=524&rPId=20844

Etape 2 :

Lancez l'application Vmware, l'assistant d'installation s'ouvre ; cliquez ensuite sur **Next** pour continuer.

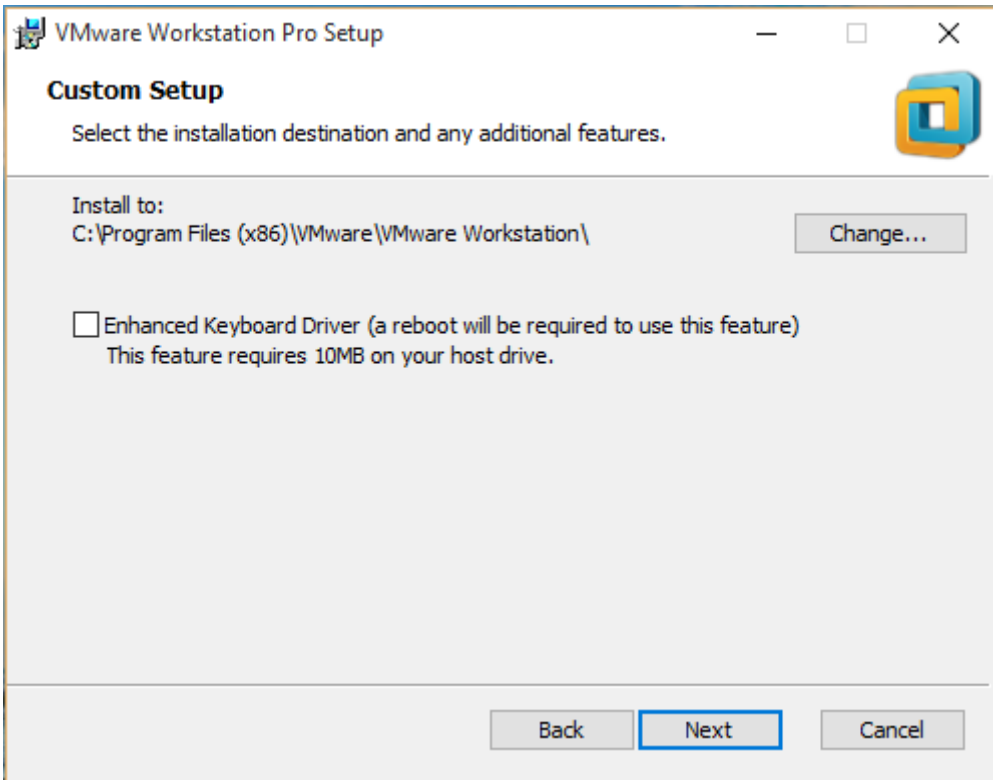
❖ **Etape 3 :**

Le contrat de licence Vmware s'affiche, cochez la case **J'accepte les termes de contrats de licence** puis cliquez ensuite sur le bouton **Next** pour continuer l'installation :



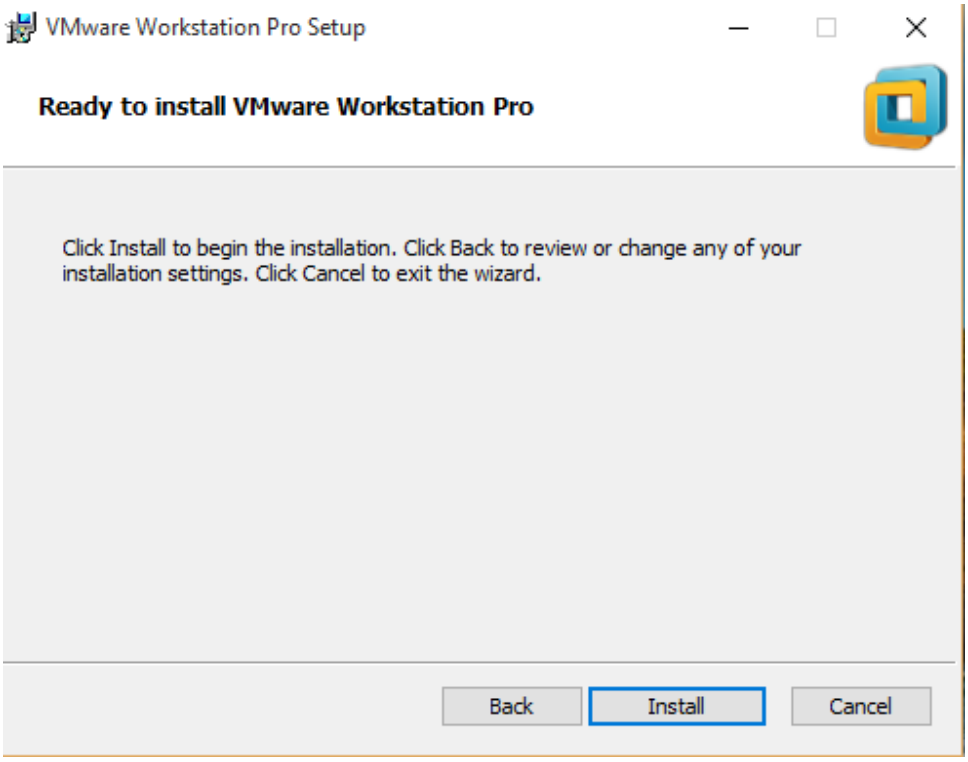
❖ **Etape 4 :**

Choisir un emplacement d'installation. L'emplacement par défaut est **C: \ Program Files (x86) \ Vmware Workstation** . Cliquez ensuite sur **Next** :



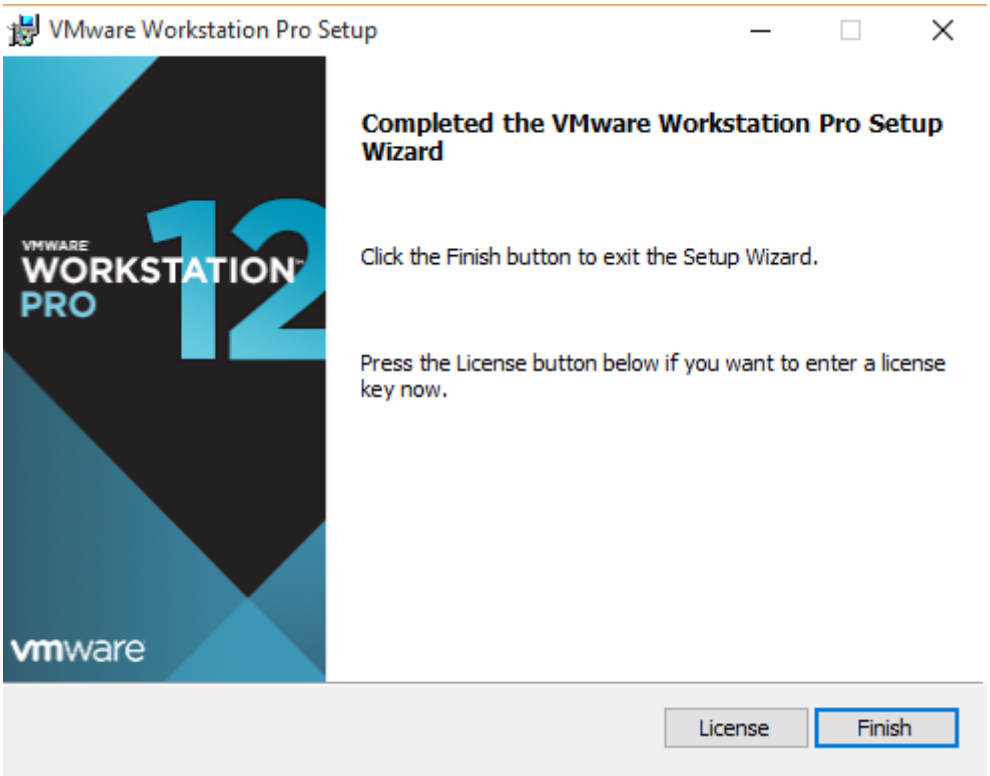
❖ **Etape 5 :**

Cliquez sur **Install** pour procéder à l'installation de vmware.

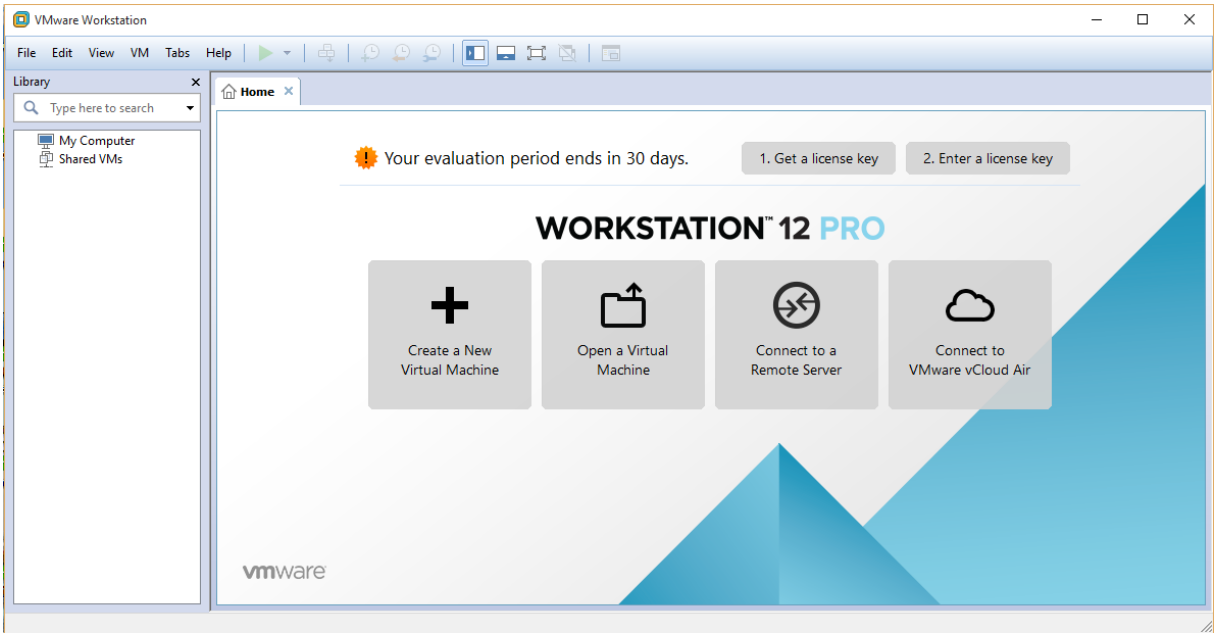


❖ **Etape 5 :**

Cliquez sur **Finish** pour terminer l'installation.



❖ Voici l'interface de vmware après son installation.



[1] R. Bouzid and D. Chabana, "Etude d'un système de communication VoIP," Université Abderrahmane Mira-Bejaia, 2019.
[2] N. Dubée, "La voix sur IP (VoIP): une opportunité pour la sécurité?," in *Proceeding of SSTIC symposium*, 2007.
[3] R. Frédéric and C. TESSEREAU, "Téléphonie sur IP," 2007.
[4] S. BACHIRI and B. BELARBI, "Déploiement d'une application de TOIP," 2015.
[5] C. Bassil, "SVSP (Secure Voice over IP Simple Protocol) une solution pour la sécurisation de la voix sur IP," 2005.
[6] S. Irnatene, D. Cheroufa, and A. Sider, "Service ToIP avec Asterisk pour l'université de Béjaia," Université abderrahmane mira béjaia, 2012.
[7] "Etude et mise ne place d'un centre d'appels via IP," 25 mars 2011.
[8] M. D. e. E. Scace, " CCITT Recommendations on the ISDN: A Review," *CCITT Red Book,* vol. 4, n°3, p. 320, 1986.
[9] "H.323 Architecture et Protocoles," *EFFORT,* 2005.
[10] L. O. a. G. Pujolle, "Téléphonie su IP," *1ère édition, EYROLLES, Paris,* p. 454, 2007.
[11] E. B. Fernandez, J. C. Pelaez, and M. M. Larrondo-Petrie, "Security patterns for voice over ip networks," in *2007 International Multi-Conference on Computing in the Global Information Technology (ICCGI'07)*, 2007, pp. 33-33: IEEE.
[12] A. Zahia and B. Hanane, "Etude et Configuration du protocole (SIPTG) dans la téléphonie IP," Université Mouloud Mammeri, 2015.
[13] *PAN-OS® Administrator's Guide,* vol. 8.1, 01 Mai 2020.
[14] F.-E. Gauffinet, *Guide CCNA 200-301,* 2020.
[15] *QoS: Latency and Jitter Configuration Guide, Cisco IOS Release 15M&T*.
[16] C. Wafa Wafa and B. Yasmina, "Gestion de qualitè de service dans las Rèseacux NGN."
[17] K. Safir, "Déploiement d'une solution VoIP avec IPv6, gestion de la QoS et évaluation en reconnaissance vocale," 2014.
[18] A. Headquarters, "Cisco Unity Express 3.1 Guide to Writing and Editing Scripts," 2007.