République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine: **Sciences et Technologies**
Filière: **Génie électrique**
Spécialité: **Télécommunication et réseaux**

Thème

Etude et implémentation de la qualité de service sur VoIP

Mémoire soutenu publiquement le 20/07/2016 devant le jury composé de :

Mr Attaf Youcef
Président, UMMTO

Mme Lahdir Leila
Promoteur, UMMTO

Mr Tahanout mohand
Examinateur, UMMTO

Mr Allouache Djamel
Examinateur, UMMTO

Présenté par **:**
Ouadouri Kamilia

Promotion 2015/2016

DÉDICACES

Je dédie ce travail

A la source qui m'a noyé avec ses sentiments et le cœur qui m'a réchauffé avec son amour, La personne la plus chère au monde : à toi ma ***Mère****.*

A celui qui a combattu toute sa vie pour me procurer tout ce d'ont j'avais besoin, celui qui M'a soutenu tout au long de mon parcours et qui était toujours un très bon exemple pour moi, la personne la plus chère au monde :

à toi mon ***Père****.*

A mes frères

A mes sœurs fetta et ourida et leurs familles

A ma sœur nassima

A mes belles sœurs malika et zahia

A mon cousin mohand.

A toutes mes amies Lilia Aldjama, Cylia Djouadi, Zaoui Tassadit, Nait malek Linda,Tibani Tinhinane, Oukherfella Kenza, Frahi Lila, Ibaghouchene Farida, Yousfene Ghania, et Bougdour Fatma. A ma copine Dalila Boudjemai et Mon ami Youcef Laguel.

A toutes les personnes qui, de près ou de loins, m'ont aidé à la réalisation de ce travail.
A tous mes enseignants de l'université Mouloud Mammeri de Tizi-Ouzou.

Kamilia Ouadouri

REMERCIEMENTS

Je remercie Dieu tout puissant, pour m'avoir donné le courage et la force pour terminer ce travail.

Au terme de ce projet de fin d'études, j'adresse mes sincères remerciements à Monsieur Abdelhalim Fares le directeur technique à l'entreprise ICOSNET, pour m'avoir accepté au sein de l'entreprise et m'avoir proposé ce projet, et pour les moyens qu'il a mis à ma disposition afin d'élaborer ce travail.

Mes remerciements s'adressent également à tous les éléments du Département VoIP.

Un grand remerciement à ma promotrice Madame Lahdir leila, pour son suivi et ses conseils.

Je tiens aussi à présenter mes remerciements et ma gratitude à tous nos enseignants de l'Université Mouloud Mammeri de Tizi-Ouzou, qui nous ont toujours enrichis de leurs savoirs.

Je souhaite exprimer enfin ma gratitude et mes vifs remerciements à ma famille et mes amis pour leur soutien.

SOMMAIRE

SOMMAIRE

Chapitre II : Qualité de service sur les réseaux IP

Chapitre III : Mesure de la qualité de service sur les applications VoIP

Chapitre IV : Solution de monitoring et supervision réseau

GLOSSAIRE

Qos : Qualité of service

RNIS : Réseau Numérique à Intégration de service

RTC: Réseau télécom commuté

ITU-T: International telecommunication Union

TCP/IP : Transmissio Control Protocol/ Internet protocol

UDP : User Datagra Protocol

PPP: Point to point protocol

PSTN: **Public switched telephone network**

PABX : Private automatic Branch Exchange

IPBX : autocommutateur téléphonique utilise le protocole Internet (IP)

SIP: Session Initiation Protocol

RAS: Registration Admission Protocol

MGCP: Media Gateway Control Protocol

ToIP: Telephony over IP

VoIP: Voice over IP

RTP: Real Time Protocol

RTCP: Real Time Control Protocol

IAX : Inter-Asterisk Exchange

SCCP: Signaling Connection and Control Part

CDP: Cisco Discovery Protocol

LLDP: Link Layer Discovery Protocol

IntServ: Integrated Service

RSVP: Protocole de réservation de ressource

DiffServ: Differenciated Service (service différencié)

DSCP: Differenciated Code Point

CU: Currently Unused

TOS: Type Of Service (type de service)

PHB: Per Hop Behavior

IPv4: Internet Protocol version 4

SLA: Service Level Agreement

MPLS: Multi Protocol Label Switching

LSR: label Switch Router

LER: Label Edge Router

AF: Assured Forwarding

EF: Expidited Forwarding

LSP: Label Switching Path

GSM: Global System For Mobile

NAT: Network Address Transmission

CPU: Central Processing Unit

MRTG: Multi Router Traffic Grapher

SNMP: Simple Network Management Protocol

NRPE: Nagios Remote Plugin Executor

NAT: Network Address Transmission

SSh: Protocol Secure Shell

IETF: Internet Engineering task Force

DNS: Domain Name System

FTP: File Transfer Protocol

INTRODUCTION GÉNÉRALE

Introduction Générale

Depuis son invention par Graham Bell à la fin du 19ème siècle, la téléphonie classique, basée sur le principe du réseau commuté (une communication implique une continuité électrique de bout en bout), n'avait évolué que grâce aux avancées de l'électronique.

Mais c'est surtout la formidable évolution technologique qui s'est opérée ces deux dernières décennies qui, en consacrant l'utilisation des protocoles de communication par paquets (en fait ceux de l'Internet) comme support des services de téléphonie, a complètement bouleversé le paysage du marché téléphonique. En effet, la commutation de paquets revient aujourd'hui beaucoup moins chère que la commutation de circuits : la compétition engendrée par la multiplication des équipementiers ont fait baisser les coûts des infrastructures de réseaux des opérateurs télécom.

Ainsi beaucoup d'acteurs en téléphonie sous IP ont vu le jour et proposent des offres très intéressantes en termes de prix par rapport à la téléphonie traditionnelle fixe ou GSM. En revanche la qualité de la voix fait défaut dans la plupart des cas, et ne suit pas le bon indicateur du prix contrairement à la téléphonie traditionnelle, qui certes demande beaucoup d'investissement pour la mise en place du support mais une fois fait, elle est très robuste et présente une forte disponibilité.

Cela est dû principalement à la complexité des réseaux informatiques supportant cette technologie et au travail nécessaire pour imposer des normes sur les équipements et supports utilisés. Le défi aujourd'hui est donc de travailler les mécanismes de QOS afin d'améliorer la qualité de la voix sur les solutions reposant sur la technologie VoIP.

Notre travail s'inscrit justement dans cette optique où nous nous concentrons sur la qualité de service dans les environnements de téléphonie sur IP.

Le mémoire est organisé en quatre chapitres et une conclusion Générale. Après la présentation de l'organisme d'accueil et le projet dans sa vue globale, on va consacrer le premier chapitre aux principes de la VoIP. Nous présenterons les protocoles de signalisation et de transport, un bref comparatif entre les protocoles les plus utilisés et une description plus approfondie du protocole SIP sur lequel reposent la plupart des solutions de téléphonie sur IP de dernière génération.

Le stage que nous avons effectué à ICOSNET, un opérateur téléphonique VoIP, nous a mis tous les moyens nous permettant d'étudier la qualité de la voix sur le réseau des ses clients et nous a permis d'assimiler beaucoup de notions pour les consacrer entièrement au deuxième chapitre. Dans cette partie nous détaillerons les mécanismes de la qualité de service et leur mode d'utilisation et d'implémentation dans diverses architectures réseaux existantes afin d'améliorer la qualité de la voix.

Au troisième chapitre nous présentons les étapes d'installation de notre IPBX office de plate-forme utilisée pour tester notre étude stratégique permettant de conclure sur l'amélioration de la qualité de service en appliquant les mécanismes et normes recommandés.

Comme la qualité de service n'est pas un programme à paramétrer une seule fois dans l'environnement de la plateforme et aux sites clients de l'entreprise, nous avions dédié un quatrième chapitre à la mis en place d'une solution de monitoring permettant de superviser les équipements réseau, s'assurer de leur disponibilité et surtout leur consommation en bande passante qui joue un rôle très important dans le maintien d'un bon niveau de qualité de service.

Enfin, une conclusion Générale, un glossaire et un ensemble de références bibliographiques qui complète ce mémoire

PRESENTATION DU PROJET ET DE L'ORGANISME D'ACCEUIL

I. Introduction

Afin de mettre en pratique les notions acquises durant notre formation de télécommunications et réseaux, nous avions choisi d'étudier la qualité de service et tenter de l'appliquer sur l'environnement d'une entreprise activant dans le domaine des télécommunications. Pour cela nous avions eu l'accord de la société ICOSNET, opérateur téléphonique VoIP, pour la réalisation d'un stage pratique d'une durée de 5 mois dont le but principal est d'étudier le thème de la qualité de service sur la VoIP.

II L'organisme d'accueil [4]

II.1. Présentation : ICOSNET a été créée en 1999, elle se positionne comme un opérateur d'accès internet et de solutions de télécommunication. Avec son équipe pluridisciplinaire, ICOSNET a su capitaliser une importante expérience et nouer un relationnel conséquent avec les différents acteurs du secteur des Télécommunications en Algérie et à l'étranger. ICOSNET se différencie par son approche technique et qualitative. La société a ainsi montré son savoir-faire et sa maîtrise, notamment auprès des entreprises multi-sites.

Sur le marché algérien, ICOSNET est un opérateur à part entière (autorisations ISP, VoIP et Wimax). Ce positionnement permet à ICOSNET de s'adresser à une clientèle large, de convaincre des clients de taille significative et de pouvoir proposer des solutions de connexion et de communication économiquement plus avantageuses et plus abouties.

Les raisons de ces succès sont multiples ; elles sont tout d'abord humaines, combinant l'expérience et l'implication des collaborateurs et la forte expertise des partenaires, elles sont aussi stratégiques, car à partir de 2009 toute la connectivité internet est acheminée depuis Londres, ce qui a largement contribué à la fiabilité du réseau ICOSNET

Aujourd'hui plusieurs entreprises algériennes et grands groupes internationaux implantés en Algérie font confiance à ICOSNET. Cette dernière ambitionne d'étendre son implantation sur le territoire national. Au-delà de ses nouvelles ambitions de croissance, ICOSNET ne perd pas de vue ses valeurs : qualité de service, satisfaction client, anticipation, la veille technologique et innovation sont autant d'objectifs qui restent et resteront prioritaires.

II.2. Couverture géographique : Même si son réseau et en extension continuelle, La société ICOSNET couvre aujourd'hui les plupart des régions du pays.

II.3 Les services proposés par ICOSNET : ICOSNET est un fournisseur d'accès internet et opérateur de solutions télécoms destinées aux PME/PMI et grands comptes, il propose plusieurs services comme :

II.3.1 L'accès Internet : ICOSNET propose deux solutions pour l'accès à l'internet sont :

a. Internet Asymétrique (Wimax) : Solution d'accès Internet sans fil indépendante des aléas des connexions filaires. Icosnet propose son offre Internet asymétrique avec une large gamme de formules pour s'adapter aux besoins de ses clients en utilisant sa technologie radio sécurisée ; elle les connecte directement à son réseau international.

b. Internet Garanti *(Les lignes spécialisées):* est une solution d'accès à haut débit garanti et symétrique pour répondre aux exigences de toutes sortes d'organismes.

c. WDSL : est une offre complète en termes de communications professionnelles. Elle est destinée aux PME/PMI et constitue un pack de services utilisant la technologie sans fil.

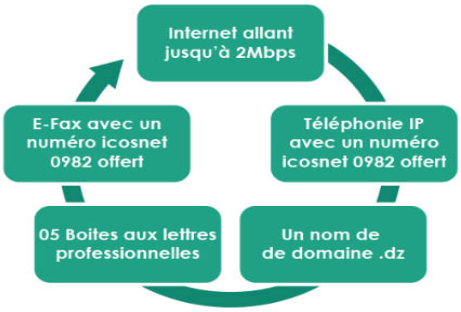


***Figure I.* la solution WDSL**

II.4 La téléphonie [4]

II.4.1 La téléphonie IP : La solution Téléphonie IP permet d'émettre et de recevoir des appels via un numéro national en 09 82 4xx xxx vers toutes les destinations. Ce service est utilisable sur différents supports tel que IP phone, Soft Phone (sur lap top ou smart phone), ou depuis un IPBX… Les lignes téléphonie IP permettent aux standards téléphoniques d'accueillir plusieurs appels simultanément. C'est aussi la solution idéale pour réduire le budget d'appels à l'international.

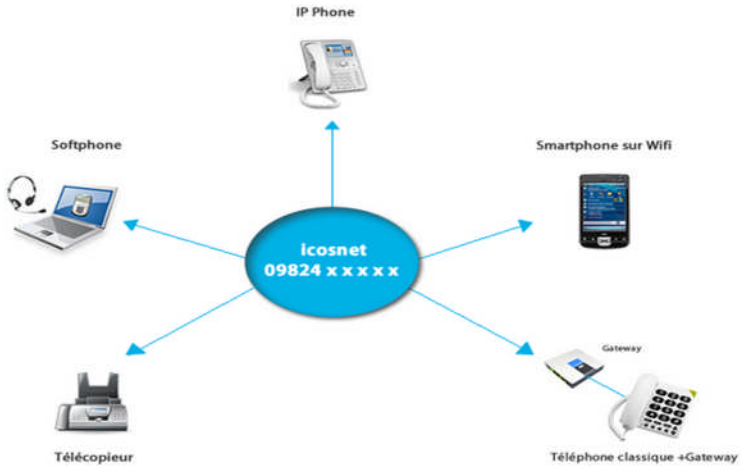


Figure 2. **La téléphonie IP**

II.4.2 Le Centrex : Le centrex d'Icosnet est une solution Cloud (standard virtuel qui permet d'accéder aux fonctionnalités avancées d'un standard téléphonique moderne sans investissement dans un équipement couteux).

Le standard téléphonique est désormais centralisé au sein du réseau sécurisé d'ICOSNET.

Figure 3. **La solution d'ICOSNET Centrex**

II.4.3 L'IPBX : L'IPBX est un standard téléphonique IP tout en un qui permet d'optimiser le budget télécom des entreprises. La solution IPBX d'icosnet fournit un standard téléphonique IP simple et sécurisé, cette solution permet de gérer en toute simplicité le trafic téléphonique.

Figure 4. **La solution ICOSNET IPBX**

II.4.4 ICOSNET call conférence : La solution call conférence d'icosnet permet de réunir plusieurs utilisateurs et d'organiser des conférences téléphoniques en simultané quelques soit leur localisation géographique ou leur type de ligne. La solution est accessible depuis n'importe quel réseau (Fixe ou mobile) national ou international.

Figure 5. **La solution ICOSNET call conférence**

II.4.5 ICOSNET E-Fax :

Le service E-fax d'icosnet représente un outil de communication pour les transactions professionnelles. Il permet d'envoyer et recevoir en toute liberté et sécurité des fax sur notre propre boite email, via notre interface web depuis n'importe quel appareil : Lap top, tablette, et même un Smartphone.

Figure 6. ***La solution ICOSNET E-Fax***

II.4.6 ICOSNET Bulk SMS : C'est une solution qui permet d'envoyer massivement des messages SMS à un groupe de destinataires. BULK SMS est un outil qui propose plusieurs interfaces pour s'adapter aux différents besoins.

Différents modes d'envoi :

- **Single SMS :** une interface web sécurisée pour envoyer un message SMS jusqu'à 100 utilisateurs
- **BULK SMS :** vous permet d'envoyer des messages à partir d'un fichier
- **Groupe SMS:** permet d'implémenter des listes de diffusion pour transmettre rapidement des messages SMS d'alerte

Figure 7. **La solution ICOSNET Bulk SMS**

II.4.7 Vazii : Vazii est une Application de communication unifiée et de messagerie instantanée, elle permet de faire des appels voix et vidéo, envoyer des messages et tout type de pièces-jointes gratuitement avec les autres utilisateurs de Vazii. Elle permet aussi de passer des appels vers des numéros mobiles ou fixes vers tous les réseaux en national et international à des tarifs très bas.

II.5 Les solutions Cloud :[4]

II.5.1 Solutions d'hébergement Web :

Solutions d'hébergement Web : est une gamme de solutions complète pour répondre à vos différents niveaux d'exigence en termes web

Toute entreprise moderne, quelle que soit sa taille, a désormais l'obligation d'avoir une présence web pour communiquer avec son environnement : institutionnels, partenaires, fournisseurs et, bien entendu, clients. Icosnet propose une gamme de quatre offres construites sur la base de ses propres datacenters et en conformité avec la législation algérienne.

Autre nom de domaine :

Icosnet vous propose de réserver et de gérer des noms de domaine et met à votre disposition une large plage d'extension telle que .COM, .ORG, .NET, .TV, .BIZ… .

II.5.2 La solution centre de contact

ICCS est une solution logicielle destinée aux centres de contacts pour la gestion de l'expérience client. Elle s'adapte à tout type d'entreprise, de la PME aux multinationales implantées sur un ou plusieurs sites. Intégrée à vos applications métiers, cette solution améliore votre relation client et développe votre business. Car, ICCS :

III. Présentation du projet

Notre travail consiste à réaliser une étude de Qualité de Service dans un environnement VoiP.

L'environnement d'accueil répond parfaitement aux attentes attendues en termes de moyens nécessaires et applications VoiP à étudier. Nous avons donc une plateforme centrale de téléphonie sur IP sur laquelle nous nous concentrons pour comprendre son fonctionnement, son état actuel et la qualité de la voix sur le réseau de l'opérateur.

Une fois les spécificités de leur produit sont bien assimilées, nous tenterons de comprendre les manquements constatés sur la qualité de la voix sur les réseaux de leurs clients. Nous avons mis en place un environnement de test sur lequel nous avions reproduit les différentes parties constituant la solution de téléphonie de l'opérateur.

Plusieurs tests ont été observés et ont révélé la nécessité de mise en place de mécanismes de qualité de service qui permettront d'améliorer la qualité de la voix.

Pour avoir l'équivalent de la plateforme téléphonique centrale, nous avions installé la solution Open source Asterisk sous linux CentOS. L'ensemble est configuré pour reproduire une grande partie des fonctionnalités de la plateforme de l'organisme d'accueil. Une fois cet environnement mis en place, on fait une étude sur les équipements réseaux utilisés et les préparer pour l'implémentation des mécanismes de qualité de service. Ainsi nous avons travaillé sur des Switch, Routeurs et Gateway de différentes marques.

Au passage nous sommes passés sur quelques clients de l'entreprise pour mesurer la qualité de service qui leur a été offerte par notre société d'accueil. Dès que tous les éléments nécessaires sont prêts sur notre environnement, notre IPBX reçoit et émit bien les appels, nous passons des tests avec et sans l'implémentation des mécanismes de la qualité de service sur différents niveaux de la solution VoIP.

Un constat est fait sur les résultats des deux tests et une conclusion tirée sur la nécessité absolue de mise en place des normes et mécanismes de QoS sur tous les réseaux utilisant notre solution de Téléphonie sur IP.

Pour assurer un service VoIP de qualité et respecter les engagements envers les clients, il est demandé une attention particulière sur les capacités réseau de notre entreprise, leurs disponibilités mais aussi la garantie de la bande passante allouée aux clients. Pour cela, et dans le but de simplifier le travail des administrateurs réseau, nous avions mis en place une solution de monitoring et supervision réseau permettant de surveiller principalement l'état des routeurs et switch mais surtout l'usage de la qualité de service sur ces derniers. Car ce paramètre affecte directement la qualité de service sur notre solution VoIP.

III.1 La problématique :

La téléphonie sur les réseaux VoiP vient concurrencer la téléphonie traditionnelle et GSM sur le prix et la

qualité de la voix. Si le premier paramètre est atteint dès l'avènement de la VoIP, le second est loin d'être satisfait sur la plupart des solutions VoIP existantes.
C'est le défi de recherche d'une bonne stratégie pour l'amélioration de la qualité de la voix qui nous a emmenés à choisir ce sujet.

III.2 Le But du Projet:

Nous nous sommes investis dans les solutions de téléphonie sur IP pour étudier la qualité de service au niveau de notre société d'accueil et tenter de proposer une stratégie pour l'amélioration de la qualité du produit de la voix commercialisé par notre société.

III.3 Le Plan du Projet:

Premièrement nous avions fait une étude approfondie des solutions voix sur IP et nous avions mis en claire leurs manquements et soucis majeurs relatif à la qualité de la voix proposée sur les différentes plateformes. Ensuite nous avions mis en place un environnement de test constitué d'une solution à part entière de téléphonie sur IP sous Asterisk et installée sous un système d'exploitation Linux.

Afin de bien assimiler le fonctionnement de la voix sur IP, nous avions fait une étude sur le traitement et transmission de la voix sur IP et ses protocoles standards à l'instar de H323 et SIP. Ce dernier est utilisé dans tout notre projet mais nous avions aussi présenté H323 et le MGCP.
Nous nous sommes ensuite intéressés aux tests de la qualité de la voix sur notre plateforme Asterisk. Et pour cela des tests ont été faits à partir du site de l'un des clients de l'entreprise d'accueil ICOSNET et cela suivant l'application ou pas des normes de la qualité de service.

Nous avions ensuite installé une solution de supervision réseau permettant de surveiller nos applications VOIP mais aussi les équipements réseaux utilisés par notre plateforme.

Conclusion

Aux termes de notre stage dans la société ICOSNET nous avions pu découvrir la plupart des solutions proposées par cette société et parmi elles la solution de téléphonie over IP. Sur cette dernière que nous avions concentré notre étude sur la qualité de la voix proposée sur cette plateforme et nous avions assimilé son utilisation mais aussi ses manquements en termes de qualités dans certains environnements. Ainsi notre projet portera sur la qualité de service et son implémentation sur la VOIP.

CHAPITRE N°1 :

LA VOIX SUR IP

I. Introduction :

La voix sur IP (Voice over IP) est une technologie de communication vocale en pleine émergence. Elle fait partie d'un tournant dans le monde de la communication. En effet, la convergence du triple play (voix, données et vidéo) fait partie des principaux enjeux des acteurs de la télécommunication aujourd'hui. Plus récemment, l'Internet s'est étendu partiellement dans l'Intranet de chaque organisation, voyant le trafic total basé sur un transport réseau de paquets IP surpasser le trafic traditionnel (réseau à commutation de circuits). Il devenait clair que dans le sillage de cette avancée technologique, les opérateurs, entreprises ou organisations et fournisseurs devaient, pour bénéficier de l'avantage du transport unique IP, introduire de nouveaux services voix et vidéo. Ce fût en 1996 la naissance de la première version voix sur IP appelée H323. Issu de l'organisation de standardisation européenne ITU-T sur la base de la signalisation voix RNIS (Q931), ce standard a maintenant donné suite à de nombreuses évolutions, quelques nouveaux standards prenant d'autres orientations technologiques.

Plus précisément, le signal numérique obtenu par numérisation de la voix est découpé en paquets qui sont transmis sur un réseau IP vers une application qui se chargera de la transformation inverse (des paquets vers la voix). Comme toute innovation technologique qui se respecte, la VoIP doit non seulement simplifier le travail mais aussi faire économiser de l'argent. Les entreprises dépensent énormément en communications téléphoniques, or le prix des communications de la Téléphonie sur IP est dérisoire en comparaison. De plus, la téléphonie sur IP utilise jusqu'à dix fois moins de bande passante que la téléphonie traditionnelle.

Les premières technologies de VoIP imaginées étaient propriétaires (chacune possède un fonctionnement propre à elle) et donc très différentes les unes des autres. Pourtant, un système qui est censé mettre des gens et des systèmes en relation exige une certaine dose de standardisation. C'est pourquoi sont apparus des protocoles standards, comme le H323 ou le SIP.

Ce chapitre nous allons nous étaler sur cette technologie VoIP en expliquant plus en détail son fonctionnement, les différentes architectures, les codecs utilisées, les supports et protocoles de transport ainsi que les avantages et inconvénient qu'offre cette technologie.

II. Généralité sur la VoIP :

II.1 Définition [1]:

La VOIP est une Technique qui permet de communiquer vocalement via le réseau Internet. Contrairement aux téléphones analogiques filaires liés à un réseau téléphonique Commuté (RTC) et à des centraux téléphoniques dédiés, la Voix sur IP permet le Transport de conversations téléphoniques sur tout le réseau, numérique ou Analogique, acceptant le protocole TCP/IP (Ethernet, RNIS, PPP, etc.).

La VoIP (Voice Over IP) est une technologie qui permet d'acheminer, grâce au protocole IP, des paquets de données correspondant à des échantillons de voix numérisée. Cette technologie convertit les signaux vocaux en signaux digitaux qui voyagent par Internet. Par la suite, ces paquets doivent être acheminés dans le bon ordre et dans un délai raisonnable pour que la voix soit correctement reproduite.

II.2 Fonctionnement de la VoIP :

Les signaux vocaux sont découpés en petites unités appelées "paquets" et sont envoyés vers le destinataire à travers le réseau 'maillé ' quel que soit le chemin. Pour arriver à destination, chaque paquet est numéroté et reçoit l'adresse du destinataire. On dit que les paquets sont encapsulés, un peu comme une mise sous enveloppe. Les paquets suivent alors leur propre chemin en fonction de l'encombrement du réseau Internet. Dans le cas ou une ligne ou un circuit tombe, les paquets déjà émis changent automatiquement de route pour arriver à leur point de destination. Une fois arrivés, les paquets sont remis dans leur ordre initial d'émission. Rien n'est perceptible car tout ceci se passe à la vitesse de la lumière. Toutefois, si une multiplicité de paquets met du temps à parvenir, c'est tous les paquets précédents qui mettent du temps d'attente à parvenir en attendant le paquet manquant, ce qui parfois se traduit chez l'usager par un délai à la réception de la voix. On parle de délai de latence ou temps de latence.

Sur les réseaux Internet les signaux vocaux transmis par paquet ne sont plus : "spécifiques – voix", mais sont considérés comme des données particulières à transmettre (communication de point à point) au même titre que la vidéo (ou l'on parle de streaming) ou tout autre fichier.

Ces paquets à transmettre portent les adresses réseau de l'expéditeur et du destinataire, ils seront acheminés par des routeurs et des serveurs avec des chemins différents afin d'atteindre une destination finale, à l'arrivée des paquets, ces derniers doivent être ordonnés par ordre de la transmission d'origine pour avoir une bonne lecture de la voix.

Chaque paquet envoyé dans le réseau se compose de :

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

II.3 Architecture de la VoIP [1] : La communication dans le monde de la téléphonie sur IP s'établit en trois modes à savoir : PC vers PC, PC vers Téléphone/Téléphone vers PC, Téléphone vers un autre

Téléphone. On distingue trois architectures de la téléphonie sur IP permettant de faire la conversation vocale sur un réseau IP.

La première architecture est la mise en place d'un autocommutateur PABX avec l'ajout d'une carte IP. un PABX est un autocommutateur privé qui s'appuie sur le protocole h.323 et permet de faire la téléphonie classique, et comme pas tous les PABX qui supportent la VoIP, il faudrait rajouter une carte IP qui accepte les appels sur IP et une Gateway IP qui va faire une conversation des signaux analogiques qui arrivent d'un téléphone analogique vers les signaux numériques, on appelle cette architecture une architecture hybride.

Le PABX permet de :

- Gérer les appels en interne et vers l'extérieur et distribuer les appels entrants.
- Gérer une boîte vocale (si correspondant absent).
- Gérer les terminaux téléphoniques (postes analogiques ou numériques).

Deuxième architecture est l'architecture Full IP qui est mise en place en remplaçant le PABX par l'IPBX et les téléphones analogiques par des téléphones IP pour faire une communication locale ou étendue d'une entreprise en utilisant les protocoles IP. L'IPBX s'appuie sur le protocole SIP et peut joindre les téléphones IP sur un réseau de l'entreprise ainsi les logiciels équipés de la VoIP de type soft phone (X Lite, PortGo…etc), tous ces équipements sont interconnectés par un IPBX qui est connecté au réseau d'entreprise via des protocoles IP. Aussi, on peut faire des communications au réseau téléphonique commuté(RTC) avec l'ajout d'une Gateway IP.

Les appels venant de l'extérieur de l'entreprise vont passer par un trunk SIP, ce dernier est un service de connectivité pour transporter, en IP, les communications vocales mais également les échanges de signalisation entre le réseau voix de l'opérateur et l'infrastructure ToIP de l'entreprise.

Il permet aux entreprises qui ont un standard IP (IPBX) d'utiliser la VoIP à fin de faire transiter leurs appels entrants et sortants à partir d'une connexion sur le réseau internet via le protocole SIP.

Le trunk SIP permet de faire passer les appels sur internet d'une entreprise sur les réseaux téléphoniques traditionnels (Public switched telephone network PSTN).

Comme le montre la figure ci-après :

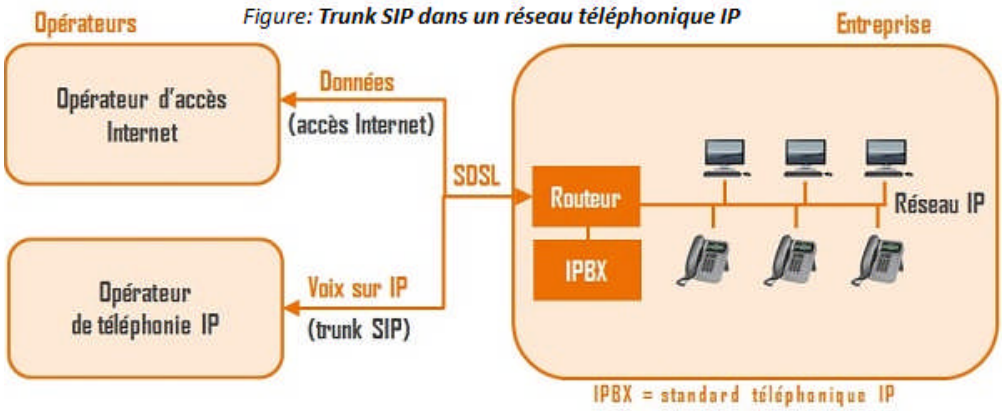


Figure I.1 **Trunk SIP dans un réseau téléphonique IP**

La troisième architecture appelée architecture Centrex IP basée sur l'IPBX virtuel. Il s'agit d'un **IPBX hébergé** et géré par une tierce partie, généralement un opérateur de téléphonie fixe. Les téléphones des utilisateurs s'authentifient au Centrex à travers le réseau Internet. Les appels entrants et sortants transitent sur IP. Cette solution permet de supprimer le standard téléphonique et de réduire considérablement le coût des appels téléphoniques. L'ensemble du service est alors géré par un prestataire et facturé sous forme d'abonnement périodique tout compris, ne nécessitant pas d'investissement pour l'entreprise.

II.4 Processus de traitement de la voix :

II.4.1 Codage et transmission de la VoIP :

Le transport de la voix sur IP est assez complexe et se fait en plusieurs étapes. La première concerne la numérisation du signal aussi appelée « le codage ». Dans la seconde étape, les informations sont divisées en trames pour pouvoir circuler sur un réseau informatique. Sans la voix, nous ne pouvons communiquer ou échanger des informations. Lorsque nous parlons, c'est tout un procédé complexe qui se met en marche. Nous produisons un ensemble de sons possédant des niveaux de fréquences différents (grave, médium, aigüe, etc.). Un son pur possède une fréquence stable et est représenté par le biais d'une sinusoïde. Quant à la voix, cette dernière produit une multitude de fréquences à des vitesses très diverses. La voix provoque donc une superposition de signaux sinusoïdaux, c'est-à-dire analogiques. Pour l'envoyer sur un réseau TCP/IP (donc numérique), il faut convertir ce signal analogique en un signal numérique. Une fois convertie, la voix, numérisée, doit être compressée grâce à un codec (compresseur/décompresseur) pour l'insérer dans un paquet IP. Le codage doit fournir la meilleur qualité de voix possible pour un débit et un délai de compression les plus courts possible. La voix est un signal possédant une bande de fréquence entre 300 et 3400 Hz.

En premier lieu ce signal doit être converti en numérique suivant le format PCM (Pulse code modulation) ou avec le codec G711 à 64Kbit/s. Selon le théorème de Shannon, le signal échantillonné à 8KHz, on a un échantillon chaque 125 µs, ensuite chaque échantillon sera codé sur 8bits ce qui donne un débit binaire de 8*8000=64Kbit /s. ce débit binaire correspond à une voix numérique non compressé.

La compression numérique : On a plusieurs algorithmes permettant de réduire la bande passante à des débits inférieurs, jusqu'à 4Kbit/s et d'augmenter l'efficacité de transport de la voix sur les réseaux informatiques orientés paquets. Il ya plusieurs codecs qui se chargent de cette fonction par exemple : G.726, G.729, G.723, G.728.

Ce signal numérisé, compressé et après suppression du silence, l'ajout des entêtes va être acheminé aux destinataires dans des paquets IP

II.4.2 Les protocoles de transport de la VoIP :

La VoIP, comme chaque domaine en réseau, comporte son lot de protocoles. Certains servent à la signalisation, certains au transport et contrôle de la voix, certains à la configuration des postes, etc… A titre d'exemple Le **protocole** RTCP qui est utilisé pour contrôler le **transport** des paquets RTP, le protocole SIP, H323 ou MGCP utilisés pour l'établissement de connexions en voix sur IP

A cela vient s'ajouter les codecs qui permettent de transformer la voix en donnée informatiques pour permettre le transport ou le stockage. (entre autres G.726, G.729, G.723, G.728)

Passant donc en revue les principaux protocoles et codecs existant.

A. SIP – Session Initiation Protocol [1]

Le protocole **SIP – Session Initiation Protocol** est un protocole de gestion de session de communication en multimédia. Il est ouvert, standard et c'est le protocole principal utilisé pour la signalisation en VoIP.

Il est aussi utilisé en visiophonie, en messagerie instantanée, etc…

En VoIP c'est donc ce protocole qui permet la gestion des appels. Par exemple, c'est grâce à SIP que le poste peut s'enregistrer auprès de l'IPBX.

C'est aussi grâce à SIP que le poste peut indiquer à l'IPBX quand l'utilisateur appui sur les touches du clavier. Il permet aussi à l'IPBX de faire sonner un poste, de mettre en relation deux téléphones, et ainsi de suite.

C'est donc lui qui est au cœur de nos infrastructures de VoIP. Si on doit retenir un bon protocole pour les applications et systèmes VoIP, c'est bien celui-ci. C'est d'ailleurs le protocole utilisé dans la solution de téléphonie de notre organisme d'acceuil.

Il est à noter que ce n'est pas SIP qui permet le transport de la voix. Il ne sert qu'à la signalisation. SIP se situe à la **couche 7 du modèle OSI** et utilise le port **5060 en UDP.**

Il est indépendant des autres protocoles des couches inférieures.

SIP fonctionne de manière similaire à http. Il réutilise de nombreux headers ainsi que des règles d'encodage et des codes de statut de http.

Voici une liste des principaux codes de statut :

1xx : Information (180 : Sonnerie, 100 : Essaie, 181 : Transfert)

2xx : Success (200 : OK, 202 : Accepté)

3xx : Redirection

4xx : Erreur Client (404 : non-trouvé, 401 : Non-autorisé, 408 : Timeout)

5xx : Erreur serveur (500 : Erreur interne au serveur, 503 : service indisponible)

6xx : Panne générale (600 : occupé)

Et voici une liste des requêtes de base :

INVITE : Permet au client de demander une nouvelle session

ACK : Permet l'acknowledgement

CANCEL : Permet l'annulation d'un INVITE en cours

BYE : Permet de terminer une session

REGISTER : Permet de s'enregistrer auprès de l'IPBX

Sur le réseau, chaque ressource SIP est identifiée par une URI de ce type : « sip:Username@Host:Port»

Par défaut le port est le 5060.

Exemple d'URI : sip:1516@sip-server.lan

B. H.323 : [1]

H.323 est un regroupement de protocoles pour la communication de l'audio, de la vidéo et des données.

Il est dérivé du protocole H.320 utilisé sur les réseaux numériques.

Aujourd'hui H.323 est remplacé par SIP sur la plupart des solutions de téléphonie modernes.

On peut découper H.323 en 3 catégories de protocoles :

- Signalisation
- Négociation de Codec
- Transport d'information

B.1a Signalisation:

Le but de la signalisation est le même qu'en SIP (voir précédemment).

Le protocole **RAS – Registration Admission Status** est utilisé pour l'enregistrement et l'authentification (par exemple, l'enregistrement des postes sur l'IPBX).

Le protocole **Q.932** est utilisé pour l'initialisation et le contrôle des appels (appui de touche, lancement d'un appel, faire sonner un poste, etc…).

B.2 Négociation:

Le but de la négociation de Codec est de choisir le Codec adéquat pour l'encodage de la voix ou de la vidéo. Nous verrons plus tard qu'il existe une série de codecs ayant chacun leurs propriétés. Le protocole utilisé pour la négociation est **H.245**.

B.3 Transport:

Enfin, le transport de l'information permet notamment de transporter la voix numérisée grâce aux codecs, sur le réseau.C'est le protocole **RTP** qui est utilisé ici.

Le protocole **RTCP** peut aussi être utilisé pour contrôler la qualité et demander de renégocier les codecs si la bande passante disponible change. H.323 a évolué au cours du temps à travers de nombreuses versions. Aussi, en H.323 les messages sont encodés en format binaire, là où SIP utilise un codage en ASCII. Grâce à la grande flexibilité de SIP, ce dernier tend à remplacer H.323.

C. MGCP :[1]

Le protocole MGCP(Media Gateway Control Protocol) définit par IETF et standardisé par le groupe MeGaCo, est un protocole permettant de contrôler les passerelles multimédia qui assurent la conversion de la voix et la vidéo dans les réseaux IP et les réseaux téléphoniques commuté(RTC).

L'élément le plus intelligent du protocole MGCP est le CALL Agent, il contrôle les passerelles et assure le fonctionnement du Media Gateway,

D. RTP – Real-time Transport Protocol [1]

RTP est un protocole se plaçant au-dessus d'UDP, permettant le transport de données ayant des contraintes de temps réelles.Il est principalement utilisé pour les flux audio et vidéo.

En VoIP nous l'utilisons donc avec SIP ou H.323 pour le transport de la voix. RTP ajoute un entête spécifique à UDP pour plusieurs raisons. Premièrement, il numérote les paquets, pour gérer les pertes et le dé-séquencement (c'est-à-dire les paquets qui arrivent dans le mauvais ordre).

Ensuite, il ajoute une information d'horloge pour gérer la gigue (c'est-à-dire la variation de latence entre plusieurs paquets). Il permet aussi de spécifier le type de données transportées (audio, vidéo, image, texte, etc…). Il y a encore d'autres informations complémentaires dans l'en-tête.

E. RTCP – Real-time Transport Control Protocol [1]

En complément de RTP, nous pouvons utiliser **RTCP** pour contrôler la qualité de la transmission.
Il fonctionne aussi en **UDP**.
RTCP ne transporte pas l'information finale. Il est simplement utilisé en contrôle.
A l'aide de statistiques sur la transmission (paquet perdu, gigue, délai, etc…), il est possible d'estimer la qualité de service. C'est grâce à RTCP que l'on peut renégocier le codec pour s'adapter à la bande passante nécessaire. Les paquets de contrôle sont envoyés à tous les participants de la session.

F. IAX – Inter-Asterisk eXchange [1]

IAX est un protocole qui s'intègre dans le projet Asterisk.
Asterisk est un IPBX open source basé sur Linux. Il permet la mise en place d'un system de téléphonie simple mais gratuit. Il n'offre pas autant de possibilités qu'une solution Cisco, mais il a l'avantage du prix. IAX est un protocole qui permet la communication entre un client et un serveur, ou entre deux serveurs Asterisk.
Il est principalement utilisé pour lier deux serveurs Asterisk (par exemple sur deux sites distants).
Nous appelons cela un Trunk. Dans ce Trunk pourront circuler plusieurs communications en simultané, et cela à travers une seule session IAX. Il propose le transport de la signalisation et des données. Il fonctionne en UDP sur le port 4569.
Nous utilisons actuellement la version 2 d'IAX.

G. SCCP – Skinny Call Control Protocol [1]

SCCP est un protocole de signalisation créé par Cisco. Il a été créé au départ pour palier la trop grande rigidité de H.323. En effet, H.323 posait problème pour la mise en place de certaines fonctionnalités.
SCCP étant propriétaire Cisco, nous le retrouvons sur beaucoup d'équipements Cisco. Certains postes Cisco fonctionnent en SIP, certains en SCCP et certains proposent les deux. Les postes récents tendent à délaisser SCCP au profit de SIP.
En général, si nous avons le choix entre SIP et SCCP, nous prenons SCCP pour des questions de compatibilité et de fonctionnalité.

SCCP a aussi l'avantage de n'utiliser que peu de bande passante. SCCP fonctionne en **TCP** sur le port 2000. Pour le transport des données, c'est RTP qui est utilisé.

H. CDP – Cisco Discovery Protocol et LLDP – Link Layer Discovery Protocol [1]

CDP permet aux équipements Cisco de découvrir les équipements voisins prenant en charge CDP.
En VoIP, il permet au switch d'indiquer aux postes IP le Vlan réservé à la voix à utiliser.
CDP est propriétaire Cisco.

LLDP est un protocole standard visant à remplacer les protocoles tels que CDP.
Il permet aussi au switch d'indiquer le Voice Vlan.

I. UA – Universal Alcatel [1]

Le protocole **UA** est utilisé par les IPBX Alcatel pour la signalisation.

UNISTIM – Unified Networks IP Stimulus

Le protocole **UNISTIM** est utilisé par les IPBX Nortel pour la signalisation.

II.5 Avantages et inconvénients de la téléphonie IP :

II.5.1 Avantages :

- La diminution non seulement des coûts de communication mais également des coûts opérationnels (un seul réseau à gérer).
- La téléphonie IP rassemble tous les appareils de l'entreprise (téléphones, visioconférence, télécopieur, ordinateurs, etc.) sur un même réseau et donc sur un même protocole.
- Une plus grande flexibilité par l'utilisation de l'IP phone même en déplacement ou par l'intégration du poste téléphonique dans le PC.
- L'infrastructure réseau est mieux utilisée (par exemple : Amortissement de la ligne louée pour être utilisée et pour l'internet et pour la téléphonie).

II.5.2 Inconvénients :

- le niveau de qualité des liaisons téléphoniques sur un réseau IP est de faible qualité par rapport à un système de téléphonie classique
- Les téléphones IP sont sensibles aux attaques virales qui peuvent affaiblir leurs capacités.
- le téléphone IP étant directement lié au terminal de réception, il dépend ainsi non seulement du bon fonctionnement du réseau mais également de l'alimentation en électricité de votre domicile : en cas de coupure d'électricité, vous n'aurez pas de téléphone.

Conclusion

Avoir une solution de téléphonie à moindre coûts telle que celle de la VoIP est sans doute un grand avantage mais l'avoir en bonne qualité demande un investissement supplémentaire et minutieux pour garantir la continuité de service et de haute qualité.

Suivant l'environnement du site à équiper de la VoIP, il faudrait combiner les différents mécanismes et protocoles adéquats pour mettre en place une stratégie assurant la capacité à fournir un service conforme à des exigences en matière de temps de réponse et de bande passante.

Le prochain chapitre nous permettra de passer en revue la Qualité de Service, son mode de fonctionnement et son application sur une solution de Téléphonie sur IP (VoIP).

CHAPITRE N°2 : LA QUALITÉ DE SERVICE SUR LES RÉSEAUX IP

I. Introduction

La qualité de service est la capacité de transmission dans de bonnes conditions un certains types de données entre les utilisateurs sur le réseau, comme elle peut donner une classe d'adresse pour certain paquets afin de prioriser la charge utile de données.

La qualité de service est gérée par le gestionnaire réseau qui vérifie les ressources réseau, les utilisateurs et les serveurs. Le gestionnaire réseau a donc la mission de contrôler toutes les affectations des ressources.

L'exploitant du réseau a un objectif qui ressort la qualité de service, cet objectif est de surveiller à ce que les ressources dont dispose les infrastructures (routeurs, commutateurs, liaisons) soient constamment utilisés aux mieux. 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.

Techniquement, ça revient à faire la séparation de flux, en priorisant les flux RTP (dans notre cas relatifs à la voix) en plus d'apporter de la sécurité pour assurer la QOS.

II. Paramètres de la qualité de service [2]:

Au sein d'un réseau donné, la qualité de service est évaluée en fonction des différents équipements qui composent ce réseau, ainsi que du trafic qui y circule, etc.

Des applications multimédia telles que la voix-IP ou la vidéo à la demande, en plus des applications classiques, seront de plus en plus utilisées dans ce type de réseaux. Ces applications multimédia nécessitent un niveau minimal de qualité de service en termes de bande passante, de délai de transit (latence), de gigue ou de taux de pertes de paquets.

- **Le débit :** Il définit le volume maximal pouvant être atteint pour la transmission de l'information (bits) par unité de temps (s) dans une communication entre un émetteur et un récepteur.
- **le délai de transit :** c'est le temps écoulé entre l'émission et la réception de paquets, il compose de :
  - **Délai de traitement** : c'est le temps qui prend le routeur pour déplacer le paquet de l'interface d'entrée, l'examiné et le mettre dans la file d'attente de l'interface de sortie.

- **Délai de mise en file d'attente:** C'est le temps que le paquet passe dans la file d'attente de sortie du routeur. Il dépend du nombre et de la taille des paquets déjà dans la file et de la bande passante de l'interface, ainsi du mécanisme de file d'attente adopté.
- **Délai de sérialisation :** c'est le temps écoulé pour mettre la trame sur le support de transmission.
- **Délai de propagation :** c'est le temps qui prend la transmission d'un bit via un le média de transmission.

- **La gigue :** C'est la variation temporelle de bout en bout du délai de transit (latence).
- **Le taux de perte de paquets :** Ce paramètre représente le pourcentage des unités de données qui ne peuvent pas atteindre leur destination dans un intervalle de temps spécifique. Cette perte de paquets à lieu lorsque le routeur manque d'espace dans le buffer d'une interface, ainsi lorsque la file d'attente de sortie d'une interface particulière est saturée, les nouveaux paquets qui seront dirigés vers cette interface vont être rejetés.

III. Les mécanismes de garantie de la qualité de service [2]

La transmission de la voix à travers les réseaux IP connait généralement des perturbations causées par des retards et des coupures de trames.

L'évolution de diverses applications et ses exigences dans les réseaux convergent à entrainer le développement de trois services principaux pour l'implémentation de la qualité de service, à savoir : le best effort, IntServ, et le DiffServ.

III.1. Le 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 comme le IntServ et DiffServ.

III.2. Réseau Integrated service (IntServ)

IntServ c'est la première architecture capable de prendre en charge la qualité de service(QOS), a été faite par l'IETF, ce mécanisme détermine si un routeur ou un hôte, est capable de répondre à une nouvelle

demande de QoS, sans gêner les demandes qui ont été déjà accordées, le IntServ repose sur deux principes fondamentaux tels que le contrôle d'admission et le mécanisme de réservation de ressources.

Le contrôle d'admission prend en compte la caractérisation en flux long et flux court ainsi les contraintes QoS propres à chaque types de flux afin de prendre la décision d'accepter ou de refuser une demande de service temps réel le long du chemin entre les utilisateurs. Afin de pouvoir garantir que la QoS demandée est bien présente,

Le deuxième mécanisme c'est la réservation de ressources par un protocole de signalisation établissant cette réservation (RSVP). Ce dernier est utilisé pour transporter les messages de réservation de ressources. Ces messages sont ceux qui indiquent aux différents nœuds, la quantité de bande passante qu'une communication souhaite disposer.

Chaque routeur IntServ repose sur :

- **Classificateur:** afin de pouvoir effectuer un contrôle du trafic, il s'agit de pouvoir identifier chaque paquet entrant à l'aide de champ descripteur de flux et donc pouvoir l'associer à une certaine classe; sachant que tous les paquets figurants dans une classe sont soumis au même traitement. Le classificateur se basant sur le contenu de l'en-tête du paquet détermine à quelle classe appartient le paquet. Une classe correspond à une catégorie de flux, par exemple le flux audio, ou encore le flux vidéo. Cela permet d'attribuer des caractéristiques distinctes à chaque flux.

- **Ordonnanceur de paquet (scheduler packet) :** il contrôle l'acheminement des paquets vers la prochaine destination, son but est 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 .

- **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 (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").

III.2.1 Le protocole de réservation de ressources (RSVP) [2]:

RSVP (Resource Reservation Protocol) fait partie de la couche 7 du modèle OSI, est un protocole de contrôle du réseau qui gère les niveaux de priorité en fonction des applications émettrices des flux de données. Ce même protocole sera utilisé par les routeurs du réseau entre eux pour établir et maintenir les tables d'états liées au flux. 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.

Fonctionnement de RSVP :

De manière à pouvoir satisfaire un grand nombre de récepteurs, RSVP rend responsable le récepteur de demander une configuration spécifique de QoS. A partir de là, une demande de QoS est acheminée au « processus » local de RSVP. Une fois la demande de QoS connue, le protocole RSVP achemine cette demande vers tous les nœuds (routeurs et hôtes), en empruntant le chemin inverse jusqu'à la source. Pendant la phase de réservation et de configuration, la demande de QoS passe au travers de deux modules différents, que sont "l'admission control" et "le policy control".

- L'admission control garantit que le nœud a suffisamment de ressources disponibles pour répondre à la demande de QoS.
- Le Policy control détermine si l'utilisateur a les droits pour faire une réservation.

Du fait que la disposition des topologies d'acheminement est sensible de changer au cours du temps, RSVP envoie périodiquement des messages de rafraîchissement, afin de continuer à maintenir les différentes réservations le long du chemin. En absence de ces messages de rafraîchissement, l'état est automatiquement effacé et les ressources libérées.

Sept Types de Messages RSVP ont été prévus:

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

RSVP travaille notamment avec les messages PATH et RESV. Le message PATH part de la source vers la destination et RESV emprunte le chemin inverse. PATH indique les caractéristiques du trafic, et RESV opère la réservation.

III.2.2 Limitation du service 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 réseau étendu, 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 flux. On peut dire que ce service est difficile à déployer à grande échelle et son utilité reste donc restreinte à des niveaux de réseaux locaux de faible étendue.

III.3. Differenciated Service DiffServ [15]:

La difficulté de déployer IntServ sur Internet tient dans sa considération de la qualité de service au niveau du micro-flux. La gestion de la réservation de ressources à ce niveau demande une immense capacité de traitement. Pour cela, le groupe l'IETF est orienté vers un autre modèle d'implémentation de qualité de service, que l'on peut utiliser pour des réseaux importants en envergure, on parle alors du modèle différenciation de services (DiffServ). L'intérêt de ce modèle est de pouvoir s'occuper du problème d'approvisionnement en qualité de service à travers une allocation de services basée sur un contrat établi entre un fournisseur de services et un client.

A l'entrée d'un réseau, le flux du paquet IP perd son identité et circule sur internet en tant qu'un membre d'une classe de flux, le mécanisme DiffServ permet donc à des fournisseurs d'offrir différents niveaux de services à certaines classes de flots de trafic rassemblés. Ainsi, il devient question de supporter un schéma de classification en attribuant des priorités à des agrégats de trafic. De ce fait, les paquets sont classés grâce à un mécanisme de marquage du champs TOS (type of service) qui fixe les priorité.

La zone TOS décompose en premier champ de trois bits « IP précédence » qui précise le niveau de priorité appliqué aux paquets, deuxième champ de quatre bits, dont la valeur détermine le critère de routage, le dernier bit reste inutilisé.

L'architecture de DiffServ définit le champ du DiffServ (DS) qui remplace le champ ToS dans l'IPv4 pour prendre des décisions relative au comportement par saut(PHB) au sujet de la classification de paquets et de fonctions de conditionnement de trafic,

Les six bits de poids fort du champ DiffServ s'appellent comme le DSCP. Les deux derniers bits actuellement inutilisés (CU) dans le champ DiffServ n'ont pas été définis dans l'architecture de champ DiffServ,

Les figures suivantes représentent l'architecture du chomp TOS et le champ DSCP dans l'en-tete IPv4.

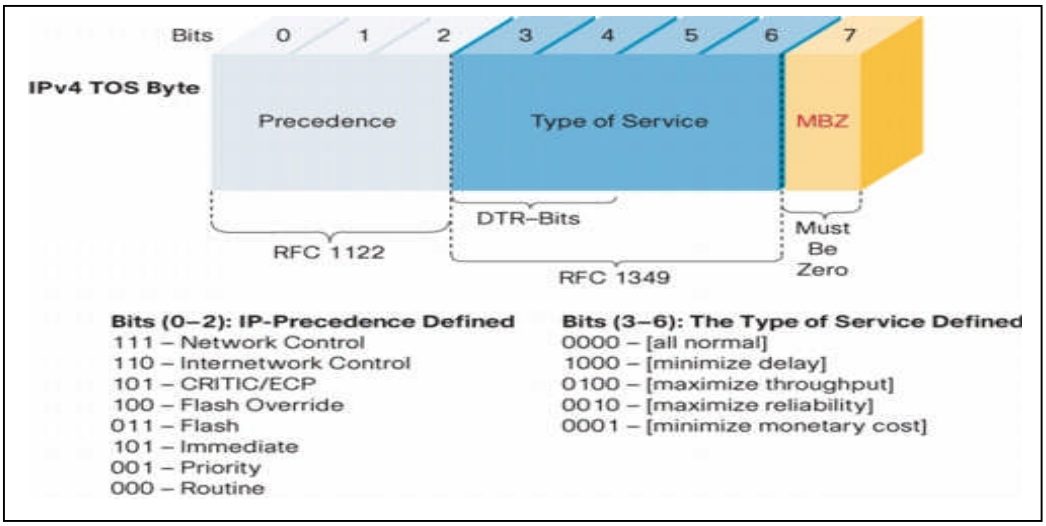


Figure II.1 : champ TOS dans l'en-tête IPv4

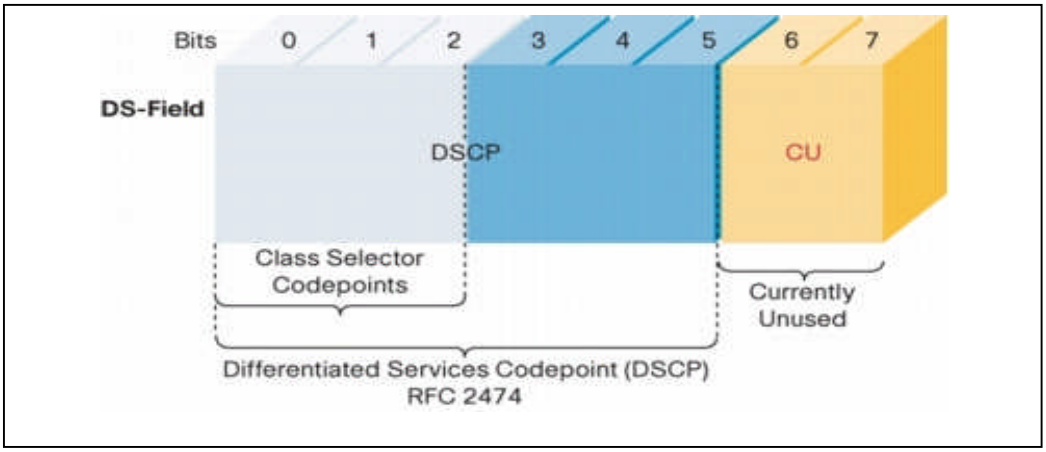


Figure II.2 : champ DSCP dans l'en-tête IPv4

Per hop behaviour (PHB) [15]:

Chaque routeur dans DiffServ gère les paquets d'une manière différente, le per hop behavior (PHB) permet de faire la transmission d'un flux ou un groupe de flux sur un nœud de DiffServ, les paquets sont donc marqués par le code DSCP où chaque paquet a un code DSCP spécifique à lui comme on peut trouver deux paquets avec un même DSCP s'ils ont des mêmes exigences QOS, dans ce cas, ces paquets sont soumis au même traitement particulier.

Les politiques de service des paquets ont une priorité de passage ou de rejet en cas de congestion, pour cela plusieurs PHB standard ont été définis.

III.3.1 Classes de service du DiffServ [15]:

III.3.1.1 le PHB par defaut :

Les paquets marqués par la valeur 000000 de DSCP utilisent le service best effort dans les nœuds DiffServ, si un paquet arrive dans le nœud DiffServ et son code DSCP ne correspond à aucun PHB donc ce paquet recevra le PHB par defaut.

III.3.1.2 Assured Forwarding [15]:

Assured forwarding permet d'offrir les différents niveaux de garantie de transport pour les paquets IP reçus à partir du domaine DS à la clientèle, il garantit une certaine quantité de bande passante aux paquets de la classe AF et donne l'accès à cette bande passante. Il est défini en quatre classes de service dans chaque classe on a trois priorités (faible, moyenne, et haute). Assured Forwarding classifie les paquets selon les quatre classes AF1, AF2, Af3, AF4 qui sont donc choisies par l'utilisateur et restent les mêmes tout au long du trajet dans le réseau.

A l'intérieur de chaque classe, un algorithme de rejet sélectif différencie entre 3 niveaux de priorité. En cas de congestion dans une des classes AF, les paquets de basse priorité sont rejetés en premier.

Les classes Assured Forwarding sont alors identifies par un code DSCP specifique comme il montre la figure suivante.

Baisse	Classe 1	Classe 2	Classe 3	Classe 4
Bas	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Support	001100 AF12 DSCP 12	010100 DSCP 20 AF 22	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Haute	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Tableau II.3 : codage de DSCP correspond à la classe AF

III.3.1.3. Expidited forwarding :

Le service Expedited Forwarding (EF) conçu pour servir des applications demandant de faibles pertes, un délai et une gigue très faibles et une garantie de bande-passante.

Le DSCP correspond à EF est 101110 qui donne une valeur 46 en décimal, tout trafic contenant le code 101110 est un trafic prioritaire par rapport au trafic AF quelque soit leur dégrée de priorité.

Nous résumons dans le tableau ci-dessous les différents services selon leur priorité

Service	Priorité
Best Effort	Faible
Assured Forwarding	Moyenne
Expedited Forwarding	Forte

Tableau II.4 : Récapitulatif des priorités de services DiffServ

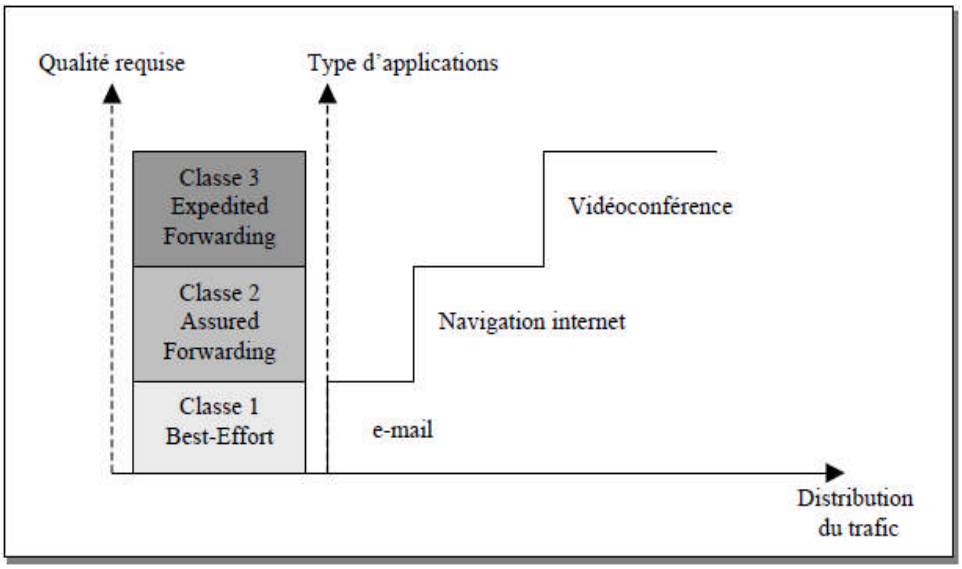


Figure II.5 : Qualités requises pour des applications sous DiffServ

III.4. Architecture DiffServ :

Contrairement à l'architecture IntServ, où les routeurs interagissent au moyen de réservations de ressources afin d'assurer des garanties de bout en bout, un réseau DiffServ est vu comme une interconnexion de routeurs obéissant chacun à une politique déterminée dans l'ordonnancement des paquets, mais agissant indépendamment les uns des autres. De ce fait, l'architecture adoptée par DiffServ est fondée sur deux principales catégories de routeurs : les routeurs de bordure (edge routers) et les routeurs de cœur (ou internes) (core routers),

A. Les routeurs de bordure (edge routers) : Les routeurs « edge » sont responsables de la classification des paquets et du conditionnement du trafic. L'opération de

classification est opérée à l'entrée du réseau, zone où la différenciation de service est mise en oeuvre, Après classification, les paquets subissent une opération de vérification qui consiste à déterminer le niveau de conformité des paquets, s'ils sont conformes ou non avec le contrat etablit. Dans le cas où les paquets sont conformes ils sont envoyés pour être étiquetés, dans le cas contraire ils sont traités selon ces trois principes, la mise en forme (shape), marquage (mark), ou élimination (drop).

B. Le routeur de cœur (core router) : Les routeurs internes se chargent de la gestion des états par classe et traitent les paquets en fonction de la classe codée dans l'en-tête, en les traitant en accord avec le comportement local correspondant : le Per-Hop-Behavior (PHB). Les PHB se basent uniquement sur le marquage de paquet, pour permettre aux routeurs d'identifier la classe de trafic à laquelle le paquet appartient.

L'architecture du modèle DiffServ et présenté dans la figure c'est après :

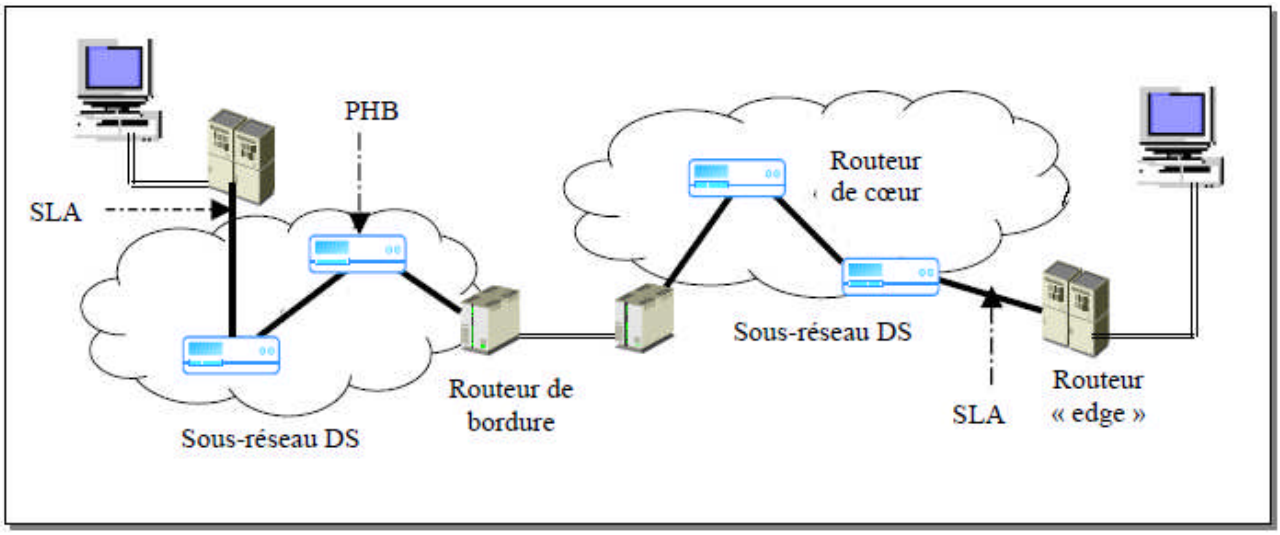


Figure II.6 : Architecture DiffServ

Cette figure présente l'architecture d'un réseau à différenciation de services, et montre les différents types de routeurs utilisés pour bénéficier le type de services.

Nous distinguons deux sous-réseaux DS reliés entre eux par des routeurs de bordure, utilisant chacun les principes de DiffServ.

Les hôtes sont directement rattachés aux routeurs « edge ». Entre ces derniers et les domaines DS, des contrats de service appelé SLA (Service-Level Agreement) sont mis en oeuvre pour spécifier les classes de service supportées et la quantité de trafic autorisée pour chaque classe.

IV. La notion SLA : Service Level Agrement :

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.

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.

V. Gestion de QOS :

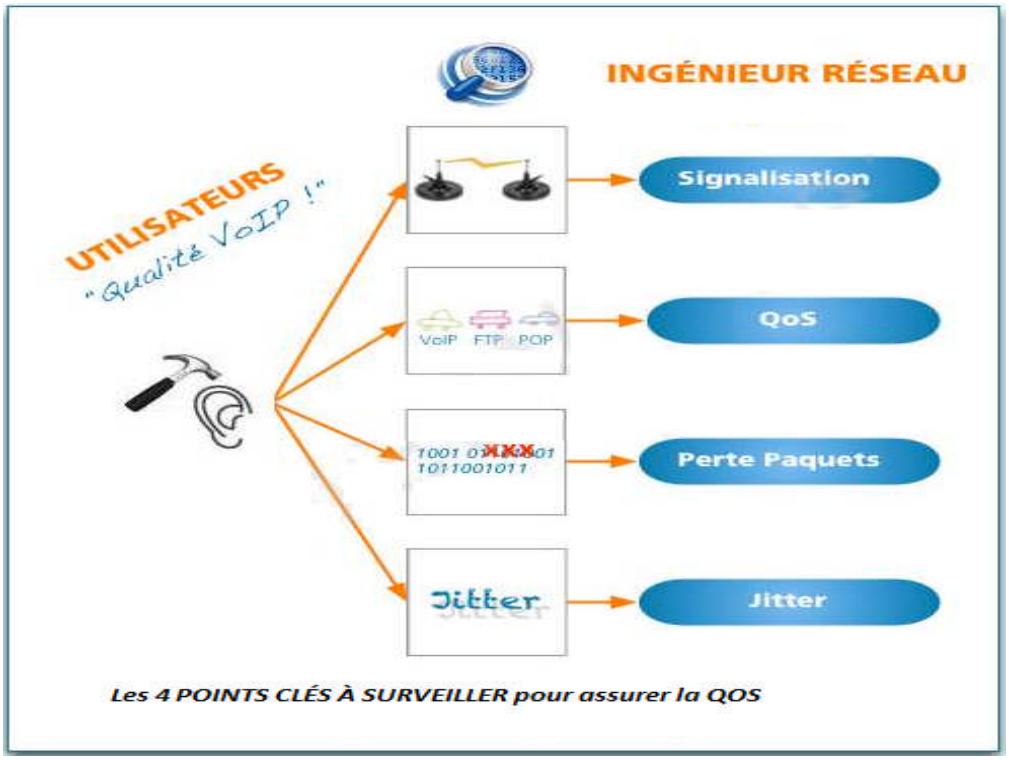


Figure II.7 Les Quatres Points à surveiller pour assurer la Qos

Comme la montre la figure ci-dessus, **la première cause** qui affecte la VoIP est liée aux problèmes de signalisation. Par exemple un signal SIP de type "Busy Call"(Occupé).

La seconde cause est à chercher du coté de la QoS (Qualite Of Service). Du fait de la convergence Voix Data, les données sont amenées à se côtoyer sur les différents segments du réseau. Une mauvaise mise au point de la QoS affectera grandement la qualité sonore des conversations pour les utilisateurs. **La troisième cause** est la perte de paquets entre l'émetteur et le destinataire. A la différence d'autres protocoles moins sensibles, la perte d'un paquet dans les flux VoIP affecte immédiatement la qualité audio de la conversation.

Enfin la quatrième, est due à la variation du temps de transfert des paquets d'un poste téléphonique à l'autre qui doit impérativement être réduite au minimum. Une bonne utilisation des Jitter buffer est essentielle.

Ces 4 indicateurs essentiels permettent une gestion sereine de la qualité sonore de la VoIP dans l'entreprise.

Un système veillant au respect et au contrôle des quatre points cités repose sur :

- **classification:** la classification effectuée à l'arrivée des paquets sur un routeur permet de détecter les classes de service et identifier les paquets reçus sur les nœuds et les associer au micro flux. La classification se base sur les caractéristiques suivantes (adresse source, adresse destination, ports source, port destination, et le type de protocole (UDP ou TCP)).
- **meter (mesure):** consiste à vérifier si les classes des flux entrants ne dépassent pas le contrat (SLA) défini dans le routeur, ensuite il va la transmettre au module marquage et shaping dropping.
- **Marquage(marker):** Les informations sont fournies par le meter, c'est dans cette étape que sera affecté le champ DSCP et faire le choix sur la priorité appliquer à chaque flux, dans le cas d'un flux dépassant un contrat SLA, alors ces flux excédentaires sont marqués avec une priorité moindre .
- **Lissage et rejet des paquets (shapper/drapper) :**

Le lissage s'effectuer lorsque les flux de classe sont permis par le contrat SLA. Les paquets sont rejetés quand leurs flux dépassent le contrat de SLA.

VI. Optimisation de trafic : MPLS(Multi protocol Label swintching) :

VI.1. Définition de MPLS:

Il s'agit d'un nouveau standard de l'IETF permettant de simplifier l'administration d'un tel cœur de réseau en ajoutant de nouvelles fonctionnalités particulièrement intéressantes pour la gestion de la qualité de service. Dans le même esprit que l'architecture DiffServ, Le protocole MPLS ou "Multi Protocol Label Switching", est un protocole qui utilise un mécanisme de routage qui lui est propre, basé sur l'attribution des « labels » ou les «étiquettes » qui sont insérées à l'entrée de chaque paquet et retirés à la sortie. Cela lui permet de router les paquets en optimisant les passages de la couche 2 à la couche 3 du modèle OSI et

d'être indépendant du codage de celles-ci suivant les différentes technologies (ATM, Frame Relay, Ethernet etc).

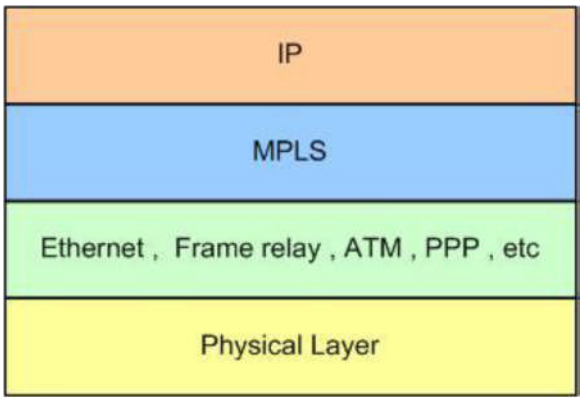


Figure II.8: la couche MPLS

VI.2. Architecture de MPLS :

L'architecture MPLS utilise les LSR(Label Switch Router) et LER(Label Edge Router)

- **LSR (Label Switch Router) :** fonctionne au cœur du réseau, il est responsable des commutations des paquets en fonction des labels, les LSR se basent uniquement sur la lecture des labels et pas des adresses IP.
- **LER (Label Edge Router) :** ce sont des routeurs situés à la frontière du réseau ils sont responsables d'insérer les paquets à l'entrée et de les récupérer à la sortie.

VI.3. Fonctionnement de MPLS :

Le principe de MPLS est d'attribuer un label (une étiquette) à chaque paquet lorsqu'il rentre dans le réseau.

Les réseaux IP/MPLS se basent sur l'établissement de chemin entre deux machines (Les Label Switched Path ou LSP). La commutation des paquets circulant sur ce chemin est faite en analysant un label contenu dans l'entête MPLS qui est ajoutée entre la couche 2 (souvent Ethernet) et la couche IP. Voici un schéma résumant le principe de la commutation de label tout au long d'un chemin ou Label Switched Path :

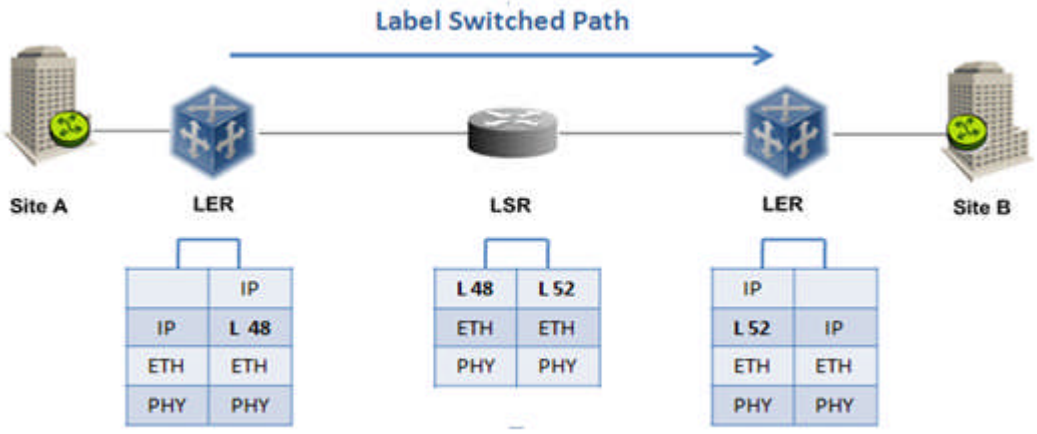


Figure II.9 : principe de commutation de LSP

A l'entrée du réseau MPLS, les paquets IP se voient insérer un label par le "Ingress Label Edge Routeur" ou "Ingress LER". Les LER sont les routeurs MPLS se situant à la périphérie du réseau de l'opérateur. Les paquets labélisés sont ensuite commutés vers le cœur du réseau selon leur numéro de label. Les routeurs MPLS du cœur de réseau, les Label Switching Router, commutent ensuite les labels jusqu'au LER de sortie (Egress LER) Le chemin qui a été pris par le paquet, et préalablement établi, au travers du réseau s'appelle un Label Switched Path (LSP).

Le schéma nous montre le détail de la pile de protocole mise en œuvre durant cette transmission, on remarque la présence du label MPLS entre la couche Ethernet et la couche IP. Nous allons maintenant analyser le format de l'entête MPLS :

Label	CoS	S	TTL
20 bits	3 bits	1 bit	8 bits

L'entête MPLS a une taille de 4 octets et est composé par les champs suivants :

- Le numéro de label
- **CoS** : Chaque paquet labélisé peut se voir attribuer une Class of service, afin de permettre différentes « discard politics » ou « scheduling politics » pour des paquets ayant le même numéro de label. Cependant la RFC précise que c'est un champ encore expérimental.
- **S** : bottom of stack. Le bit "S" est à 1 quand le dernier label de la pile est atteint. On verra par la suite que l'on peut empiler les labels (par exemple pour créer des Tunnels).

- **TTL** : Ce champ a le même rôle que le TTL de l'entête IP. Etant donné que l'entête IP n'est pas analysé par les LSR, la valeur du TTL est recopiée dans l'entête MPLS à l'entrée du réseau par le Ingress LER. Ensuite, à chaque commutation par un LSR, le TTL est modifié. La valeur TTL de l'entête MPLS est ensuite recopiée dans l'entête IP à la sortie du réseau MPLS par le Egress LER.

Conclusion:

Dans ce chapitre nous avons étudié les différents mécanismes de qualité de service existants et nous avons expliqué leur mode d'utilisation et les paramètres recommandés à utiliser pour garantir une meilleure qualité.

Parmi les modèles présentés, on a vu **Integrated Service** et **Differentieted Service**. Nous allons utiliser ce dernier dans nos réseaux et faire les tests sur la qualité de la VoiP dans notre système de téléphonie sur IP. Le prochain chapitre sera consacré aux mesures de la qualité de la voix entre un site client et notre plateforme Asterisk.

CHAPITRE 3 :

MESURE LA QUALITÉ DE SERVICE SUR LES APPLICATIONS VOIP

I. Introduction

La téléphonie sur IP a rendu le monde très petit, grâce à son développement et ses avantages les entreprises peuvent communiquer entre elles avec des billets de transmission moins chère et moins couteux. Ces solutions reposent sur des équipements qui prennent en charge la téléphonie sur IP et rendent la communication facile et simple. Parmi un nombre important de ce type de solutions de téléphonie sur IP, on recense Asterisk qui est approuvé par plusieurs entreprises grâce à sa puissance et sa souplesse. Il fait ainsi office d'un PABX permettant de gérer la téléphonie analogique et la téléphonie sur IP (VoIP).
Notre travail repose justement sur ce deuxième type de téléphonie à savoir la VoIP.

Dans ce chapitre, premièrement nous nous intéressons à expliquer les différentes étapes d'installations du PABX Asterisk, sa configuration et son utilisation. Ensuite nous allons utiliser cette plateforme pour effectuer des appels et réaliser des tests sur la qualité de la voix suivant deux scénarios :

- En premier lieu, nous allons faire des appels entre le site client et notre plateforme Asterisk sans l'application des mécanismes de qualité de service et on prendra les mesures relatives à la qualité de la voix.

- En second, on refait d'autres mesures sur les mêmes sites mais après avoir implémentés les mécanismes de qualité de service sur les deux sous-réseaux.

Enfin on ressort un comparatif des deux résultats et conclure sur la stratégie nécessaire pour l'amélioration de la qualité de la voix.

II. Asterisk: [5]

Asterisk est un autocommutateur téléphonique privé (PABX) open source, crée en 1999 par Mark Spenser. Il est destiné au fonctionnent sous des systèmes linux et publié sous licence GPL. Il permet, entre autres, la messagerie vocale, les files d'attente, les agents d'appels, les musiques d'attente et les mises en garde d'appels ainsi que la distribution des appels. Asterisk implémente les protocoles H.320, H.323 et SIP ainsi qu'un protocole spécifique nommé IAX (Inter-Asterisk eXchange). Ce protocole IAX permet la communication entre deux serveurs Asterisk ainsi qu'entre client et serveur Asterisk. Il peut aussi jouer un rôle d'une passerelle avec les réseaux publics (RTC, GSM, etc.)

Comme annoncé précédemment, nous allons installer Asterisk pour faire un environnement d'exécution similaire à la plateforme propriétaire de notre organisme d'accueil.

II.1 Etapes d'installation:[23]

Pour la mis en place d'un serveur Asterisk, il convient de le télécharger sur le site www.Asterisk.org. Etant une solution open source, le téléchargement de ses paquets d'installation est complètement gratuit.

Pour des fins de tests locaux, nous avions installé un environnement constitué de machines virtuelles nous permettant de simuler les tests entre le client et notre plateforme.

Pour cela, nous avons utilisé VirtualBox pour installer deux systèmes d'exploitation linux (Fedora et CentOS) ainsi qu'un système d'exploitation Windows.

Tel que, Virtual box est un programme qui permettra à l'utilisateur d'installer sur sa machine plusieurs systèmes d'exploitation différents. Il pourra profiter des logiciels spécifiques à chaque plateforme. **Virtual box** peut procéder à la création d'un ordinateur virtuel sur un PC réel en installant un autre système d'exploitation. On pourra par exemple profiter de Windows XP et Linux.

Pour le serveur Astérisk, nous avons choisi de l'implémenter sous le systèmes d'exploitation linux CentOS. Les autres systèmes d'exploitation installés sur les machines virtuelles nous serviront de test.

La plateforme Linux CentOS :

Au moment où nous rédigeons ce travail, la communauté CentOs annonce déjà la version 8 de son système. Mais pour s'assurer de la stabilité du système utilisé, nous préférons mettre en place notre solution sous la version 5.11 de linux CentOS. Cette dernière se repose sur le noyau Red Hat **2.6.**

De même pour Astérisk, il sera également installé sous une version bien testée et confirmée. Pour cela, on télécharge alors la version 1.6.2, réputée très stable, sous format compressé sur le site précédemment cité. Une fois téléchargé, il faudrait le décompresser avec la commande suivante :

```
# tar zxvf asterisk-1.6.2.tar.gz
```

Puis on lance la compilation et l'installation des paquets de la façon suivante :

```
# cd asterisk-1.6.2
# ./ configure
# make
```

Une fois les parquets construits, nous aurons la confirmation suivante :

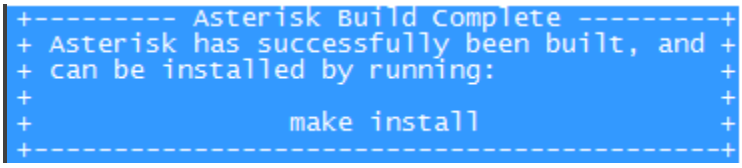


Figure III.1 Fin de la compilation des paquets Asterisk

Nous exécutons ensuite la commande make install pour installer les paquets compilés.

 # make install

A la fin de l'installation nous aurons la confirmation sur tous les paquets installés.

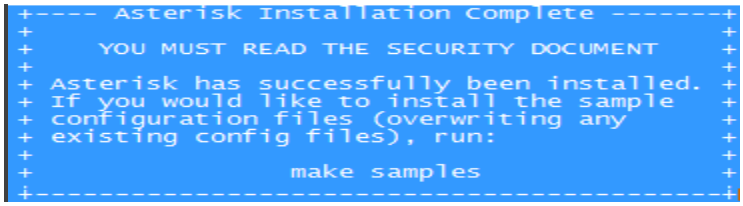


Figure III.2 Confirmation de fin d'installation de Asterisk

L'installation est ainsi bien faite, nous pourrons maintenant lancer l'Asterisk en utilisant la commande suivante :

 # /etc/init.d/asterisk start

En plus de la machine CentOS, nous avions aussi installé Linux Fedora en sa version 23. Les deux machines créées sous VMwere VirtualBox. Cette dernière est installée sur une machine physique dotée de windows Server 2012 R2 pour nous servir de plateforme de test.

II.2 Fonctionnement de Asterisk :[5]

Au bon fonctionnement de la solution Astérisk, il convient de créer un compte SIP pour chaque utilisateur. Cela nous demandera d'ajouter les coordonnées téléphoniques de chaque Softphone à utiliser.

Cette configuration repose sur deux fichiers principaux, à savoir SIP.conf et Extensions.conf (que nous retrouverons un peu plus loin dans ce chapitre).

Pour établir des communications avec le serveur Astérisk, il nous faudra des Soft phones ou IP phones.

Un soft phone est un type de logiciel utilisé pour faire de la téléphonie sur internet depuis un ordinateur plutôt qu'un téléphone. Il existe des milliers de soft phones plus ou moins performants. Nous avions décidé d'utiliser X-Lite (logiciel propriétaire) et PortGo (logiciel libre).

Le but est donc de faire communiquer deux clients entre eux, et pour se faire il nous est indispensable de choisir un client supportant l'utilisation SIP (X-Lite et PortGo).

Dans notre test on utilise deux soft phones X-Lite et PortGo , les figures suivantes montrent l'interface d'appel de chaque soft phone :

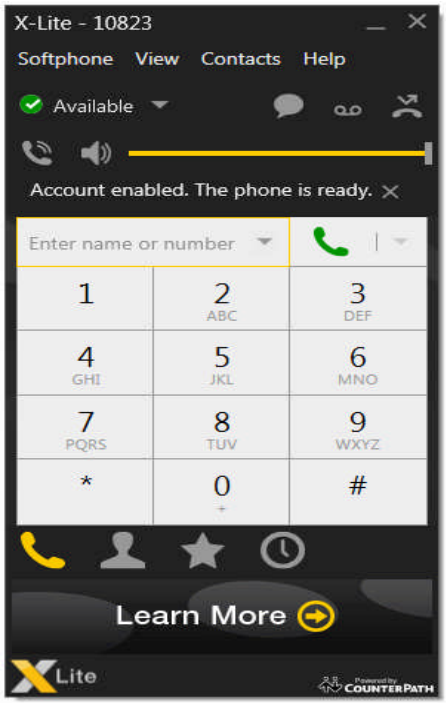


Figure III.3: interface d'appel X-Lite

OPTIONS PORT-GO

1- Menu principal-Stand by-Fermé
2- Statut
3- Webcam
4- Ajout contacts
5- Mode téléphone
6- Liste contacts
7- Historique d'appels
8- Enregistrement audio ou vidéo
9- Transfert appel
10- Appel en attente
11- Répondeur automatique
12- Mode silence
13- Conférence

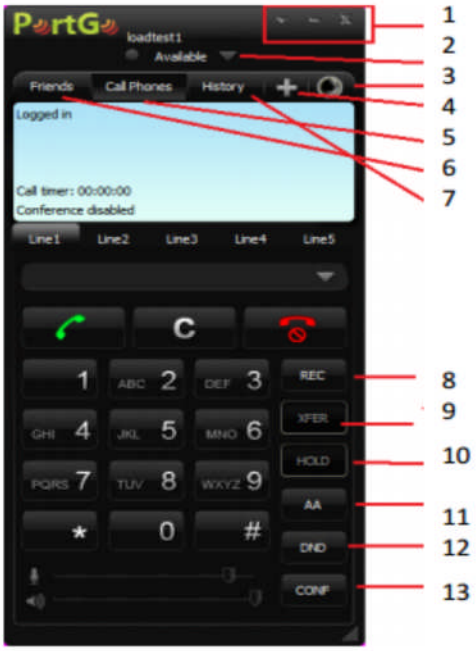


Figure III.4 : interface d'appel de PortGo

Le principe de fonctionnement d'Asterisk consiste en routage des appels vers les différents utilisateurs du réseau après avoir crées les comptes et les extensions de chaque utilisateur.

Chaque extension est alors manipulée depuis sa source (téléphone analogique, téléphones IP ou un soft phone), vers une destination via des règles de routage qui s'enchainent.

La figure suivante montre les différentes étapes pour établir un appel avec le serveur Asterisk.

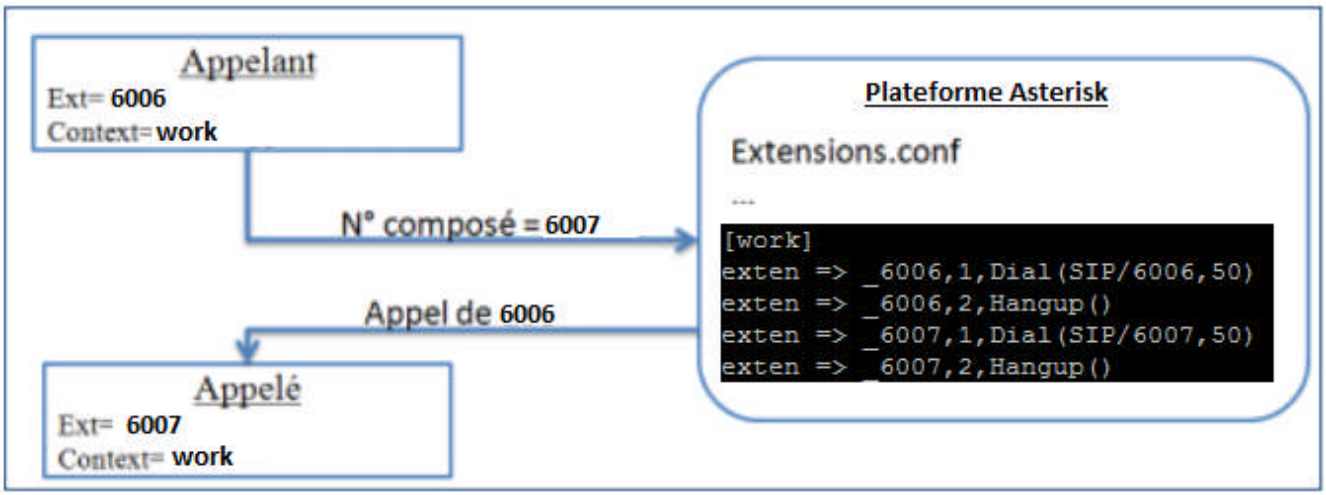


Figure III.5 : principe de routage d'appels avec le serveur asterisk

La communication établie par un appel d'un client (6006) en composant le numéro de l'extension de l'appelé (6007), ce client ensuite va se connecter directement vers le serveur Asterisk, ce dérnier confirme si le numéro de l'appelant est disponible depuis ses extensions, si c'est le cas, il va lui permettre de passer l'appel.

II.3 Les fichiers de configurations de Asterisk: [5]

1) SIP.conf :

Sip.conf est utilisé pour configurer les logins et les mots de passe de tous les périphériques qui peuvent être des soft phones, des passerelles ou d'autres serveurs. Le fichier SIP.conf est organisé selon plusieurs zones appelées « context » définies comme suit :

a) Context générale

[general]

Context = local ; context par défaut pour les utilisateurs

Bindport = 5060 ; port UDP du protocole SIP

Bindaddr = 0.0.0.0 ; adresse IP de l'interface sur lequel le serveur va écouter le trafic 0.0.0.0 pour toutes les interfaces

Language = fr ; messages vocaux en français

b) Context utilisateurs Ce context permet de créer les comptes utilisateurs, par exemple, le X-Lite et le PortGo dans notre cas, et pour que ces deux soft phones arrivent à communiquer entre eux il faut ajouter les paramètres des comptes comme le montre l'exemple suivant :

[john] ; obligatoire ; login SIP

Secret =Yemsal ; obligatoire ; mot de passe SIP

callerid = "John" <200> ; facultatif ; nom affiche et numéro affiche sur le téléphone de l'appeler

context = local ; obligatoire ; les appels que fait l'utilisateur ; seront gérés dans le context "local" du fichier ; extension.conf

mailbox = 200@default ; facultatif ; compte de messagerie vocal, voir ; voicemail.conf

type = friend ; obligatoire ; autorise les appels entrant et sortant

host = dynamic ; obligatoire ; adresse IP du client

nat = yes ; facultatif ; résoudre le problème de l'enregistrement SIP quand le téléphone est derrière un NAT

canreinvite = yes ; facultatif ; résoudre le problème du flux RTP quand le téléphone est derrière un NAT.

c) Contexte passerelles

Dans le cas où le serveur Asterisk joue le rôle d'une passerelle vers les autres réseaux comme GSM et RTC, les passerelles doivent être configurées comme des comptes dans le SIP.conf de la même façon que le contexte utilisateur. Comme dans l'exemple suivant :

[SPA-3102-PSTN]

Secret =Assalas

context=local

type=friend

host=dynamic

En éditant le fichier sip.conf, nous découvrons le détail concernant les utilisateurs enregistrés.

```
; SIP Configuration example for Asterisk

[general]
context=default
port=5060
bindaddr=0.0.0.0
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=fr

[6006]
type=friend
host=dynamic
;host=192.168.43.35
dtmfmode=rfc2833
disallow=all
allow=ulaw
fullname=6006
username=6006
secret=Assalas
context=work
```

Figure III.6 : Configuration des comptes SIP sous Asterisk

2) Extensions.conf

Le fichier extension.conf est utilisé pour router les appels vers un utilisateur ou vers sa messagerie. Par exemple, les appels provenant de comptes SIP dont le context est « local » seront traités dans l'extension « local » du fichier extension.conf.

Sa configuration sur Asterisk est comme suit :

[local]

exten => 6006, 1, Dial (SIP/6006, 10)

exten => 6006, 2, Hangup ()

exten => 6007, 1, Dial (SIP/6007, 10)

exten => 6007, 2, Hangup()

La commande SIP SHOW PEERS exécutée sous CLI> nous affiche la liste de tous les utilisateurs dans notre solution, comme suite :

```
localhost*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
6006/6006                  192.168.43.35    D   N      54717    Unmonitored
6007/6007                  192.168.43.197   D   N      53723    Unmonitored
6008/6008                  (Unspecified)    D   N      0        Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 2 online, 1 offline]
localhost*CLI>
```

Figure III.7 : Liste des utilisateurs connectés sur l'IPBX Asterisk

II.4 Configuration des soft phones pour Asterisk :

Configuration de X-Lite et PortGO:

La mise en place de X-Lite avec le serveur Asterisk, se fait en éditant le menu account Setting et en passant sur propriétés, on renseigne les champs « Display name », « user name », « mot de passe » qui permet au clients de s'identifier dans le serveur, « Authorization user name » définit sur le serveur Asterisk , « domain » c'est l'adresse IP de l'IPBX.

La configuration de ce soft phone est simple, et se fait de la même manière que X-Lite, en remplissant les mêmes paramètres SIP.

Les figures suivantes montrent un aperçu des deux interfaces de configuration

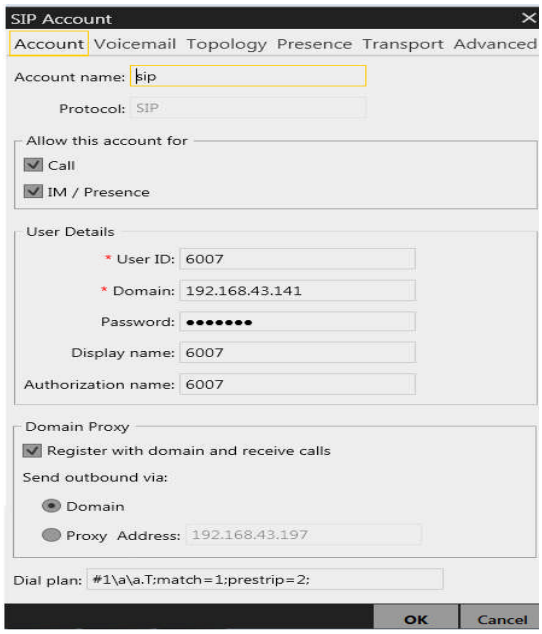
Interface X-Lite	Interface PortGO
	

Figure III.8 : Interfaces X-Lite et PortGo

Maintenant que notre IPBX et les softphones à utiliser sont prêts, nous passons aux outils de mesure nous permettant de connaitre la qualité de nos appels sous IP.

III. iperf [22]

Iperf est un logiciel pour mesurer la bande passante et la qualité d'un lien IP qui est déterminé principalement par la latence, la gigue et le taux de perte de paquets. *Iperf* est délimité par deux machines ; l'une se comporte comme un serveur et l'autre fait office d'un client.

La bande passante est mesurée avec des tests TCP, par default le client *Iperf* se connecte au serveur *Iperf* sur le port 5001 et la bande affichée par *Iperf* est celle du client/serveur.

Pour la mesure de la gigue et le taux de perte on utilise les tests UDP avec l'option « –u ».

On considère la qualité d'un réseau est bonne quand on obtient les valeurs de cette façon pour chaque facteur dans les différents réseaux suivants :

- Sur un réseau LOCAL : perte <0.5%, délais <10ms, gigue <5ms.
- Sur le réseau WAN : perte < 1%, délais < 40ms, gigue <10ms.

- Sur internet ou VPN sur internet : perte < 2%, délais <100ms, gigue <30 ms.

L'installation de *Iperf* est très simple, il s'installe sur la plupart des systèmes d'exploitation, entre autres UNIX/LINUX et Windows. Un hôte est configuré comme étant un serveur et l'autre comme client.

Sous linux, on a téléchargé la version 2.8 de Iperf sous format compressé .tar.gz.

Enregistré dans le répertoire temporaire puis décompressé et installé avec les commandes suivantes :

```
# tar vxfz iperf.2.8.tar.gz
# cd iperf.2.8
# ./configure
# make
# make install
```

Sous Windows on télécharge Iperf sous format compressé ensuite, on l'enregistre dans un répertoire puis on lance son installation.

Nous avons maintenant *Iperf* sur les deux systèmes (windows et linux). Nous avons fait en sorte d'utiliser la même version pour éviter les soucis d'incompatibilités ou de non interprétation des requêtes par le client ou le serveur *Iperf.*

Pour effectuer nos tests, nous avions placé deux combinés d'appel sur les extrémités de l'étendu réseau à tester.

Nous nous sommes déplacés au site A du client (à Birkhadem) et nous avons configuré l'un de ses Ip Phones de sorte qu'il puisse se connecter et pointer ses appels vers notre serveur Asterisk placé au niveau du Site B (à Chéraga). Comme la montre la figure ci-après :

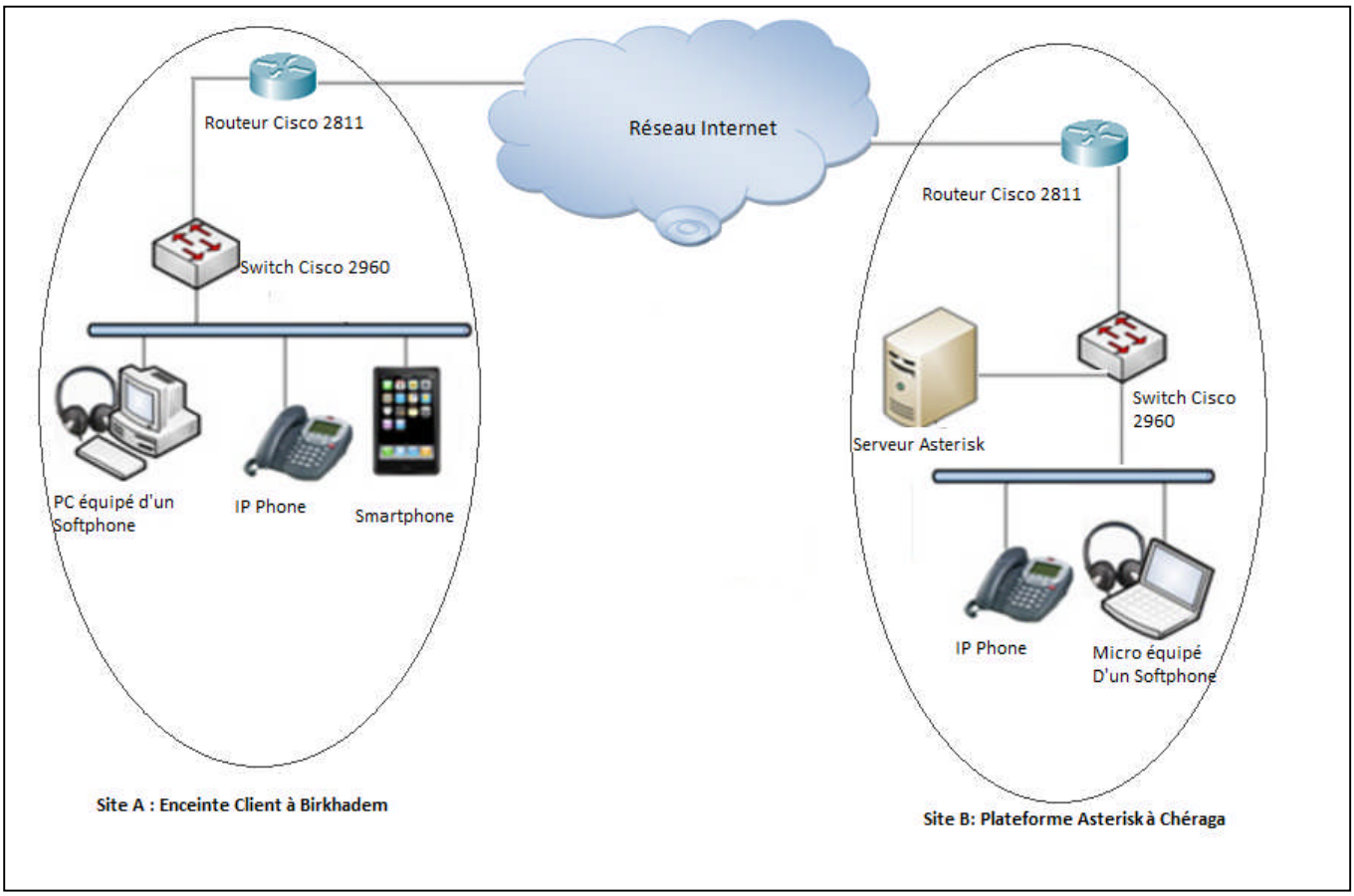


Figure III.9:Interconnexion du site Client Birkhadem à celui de Chéraga

Sur notre serveur Asterisk à Chéraga, nous avions créé deux comptes SIP; l'un correspondant à l'IP Phone du site A et l'autre à la configuration du Soft Phone X-Lite installé sur PC au niveau du Site B. Les deux sites sont distants de 20 Km environs. Les deux moyens d'appel (IP PHONE d'un coté et X-Lite de l'autre) sont logués sur le serveur Asterisk et ainsi prêts à émettre et recevoir des appels.

La stratégie choisie pour nos tests consiste à émettre des appels entre les deux sites et prendre les mesures relatives à la qualité de la voix avec ou sans l'implémentation des mécanismes de QoS sur les équipements réseaux des deux sites. Nous allons donc nous servir de *Iperf* pour effectuer les mesures et tenter de comprendre les résultats obtenus.

Avant de lancer des appels entre les deux sites, nous devons mettre *Iperf* à l'écoute afin d'intercepter les différents flux transitant sur le réseau et ressortir des indicateurs sur la bande passante, la gigue, le nombre de paquets transférés ainsi que le pourcentage des paquets perdus. *Iperf* nous propose plusieurs options nous permettant de ressortir les paramètres recherchés.

Voici entre autres, les possibilités décrites dans le manuel d'aide de la version installée sur nos machines**:[7]**

```
-f, --format [bkmaBKMA] : une lettre spécifie le format de la bande passante à afficher
    'b' = bits/sec                      'B' = Bytes/sec
    'k' = Kbits/sec                 'K' = KBytes/sec
    'm' = Mbits/sec                 'M' = MBytes/sec
    'g' = Gbits/sec                 'G' = GBytes/sec
    'a' = adaptive bits/sec         'A' = adaptive Bytes/sec

-i, --interval      : Temps en secondes entre chaque affichage
-m, --print_mss     : Affichage de la taille MSS (MSS= MTU -40 bytes)
-p, --port          : Port du serveur
-u, --udp           : Utiliser UDP plutôt que TCP (voir aussi l'option -b)
-w, --window        : Pour TCP = Fenêtre TCP et pour UDP = taille du tampon recevant les datagrammes
-M, --mss           : Taille du Maximum Segment size (MTU - 40 bytes)
-o                  : Ecriture du résultat dans un fichier (uniquement pour Window)
-c, --client        : fonction client
-l, --len           : The length of buffers to read or write (Default is 8 KB for TCP, 1470 bytes for UDP.)
```

Figure III.10: Manuel d'aide de Iperf

IV. Mesure de la Qualité de service:[7]

1ère partie des tests: Mesurer la qualité des appels entre nos deux sites **sans** application des paramètres de Qualité de service sur les différents niveaux.

Coté serveur:

Nous commençons donc par lancer *Iperf* coté serveur. Pour cela, on se connecte en ssh sur le serveur Asterisk et on tape la commande suivante :

#iperf –s –u

```
[root@localhost ~]# iperf -s -u
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  108 KByte (default)
------------------------------------------------------------
```

Figure III.11 : Mise à l'écoute de Iperf sur la machine serveur

Par défaut *Iperf* écoute sur le port tcp 5001, mais pour notre cas nous allons utiliser le port UDP pour ressortir le maximum d'indicateurs.

Maintenant que notre serveur *Iperf* est à l'écoute, nous lancer des communications vocales entre nos deux sites.

Nous nous connectons sur la console de Asterisk pour suivre les étapes de déroulement de notre appel.

La capture suivante illustre les étapes de notre appel :

```
localhost*CLI>
  == Using SIP RTP CoS mark 5
    -- Executing [6007@work:1] Dial("SIP/6008-00000000", "SIP/6007,50") in new stack
  == Using SIP RTP CoS mark 5
    -- Called 6007
    -- SIP/6007-00000001 is ringing
[Jul  9 03:59:14] NOTICE[6674]: rtp.c:1809 ast_rtp_read: Unknown RTP codec 126 received from '192.168.43.197'
    -- SIP/6007-00000001 answered SIP/6008-00000000
    -- Packet2Packet bridging SIP/6008-00000000 and SIP/6007-00000001
localhost*CLI>
```

Figure III.12 : étapes de déroulement d'un appel sous Asterisk

L'un des IP Phone placés au niveau du site client à Birkhadem lance une communication avec un interlocuteur se trouvant au niveau du site de Chéraga.

Coté client: [7]

Au moment où l'appel se déroule entre deux combinés se trouvant aux extrémités des deux réseaux, on lance la commande *Iperf* coté client avec la commande :

Iperf – c 192.168.43.141 –u

Tel que l'argument –c spécifie le client et suivi de l'adresse IP du serveur et de l'argument – u pour dire qu'on s'intéresse au flux UDP.

Le résultat de la commande nous donne ce qui suit :

```
C:\Users\JET>iperf3 -c 192.168.43.141 -u
Connecting to host 192.168.43.141, port 5201
[  4] local 192.168.185.19 port 64954 connected to 192.168.43.141 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.00   sec   208 KBytes  1.70 Mbits/sec  26
[  4]   1.00-2.00   sec   160 KBytes  1.31 Mbits/sec  20
[  4]   2.00-3.00   sec   160 KBytes  1.31 Mbits/sec  20
[  4]   3.00-4.00   sec   160 KBytes  1.31 Mbits/sec  20
[  4]   4.00-5.00   sec   160 KBytes  1.31 Mbits/sec  20
[  4]   5.00-6.00   sec   160 KBytes  1.31 Mbits/sec  20
[  4]   6.00-7.00   sec   160 KBytes  1.31 Mbits/sec  20
[  4]   7.00-8.00   sec   160 KBytes  1.31 Mbits/sec  20
[  4]   8.00-9.00   sec   160 KBytes  1.31 Mbits/sec  20
[  4]   9.00-10.00  sec   160 KBytes  1.31 Mbits/sec  20
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datag
rams
[  4]   0.00-10.00  sec  1.61 MBytes  1.35 Mbits/sec  128.423 ms  110/205 (54%)

[  4] Sent 205 datagrams

iperf Done.
```

Figure III.13 : Résultats Iperf du Premier test

IV.1 Interprétation des résultats sans Qos:

Au bout de 10 secondes, Iperf nous livre dans son résultat résumé dans la dernière ligne qui renseigne :

- 1.61 MBytes de trafic UDP transféré
- Une bande passante de 1.35 Mbits/sec
- Une gigue de 128.423 ms
- Un taux de perte qui s'élève à 110 paquets perdus sur 205 paquets envoyées soit un taux de 54%

En termes de qualité de l'appel, nous avons entendu beaucoup de bruit et c'est comme c'est notre interlocuteur était très loin de son combiné. D'ailleurs ce dernier paramètre confirme cette détérioration de qualité de voix en précisant la perte de plus de la moitié de paquets émis et une gigue de 128,423 ms qui sort complètement des valeurs acceptables. Cette valeur représente plus exactement la variation de la latence.

2ème Partie des tests : Ici nous allons procéder à l'implémentation des mécanismes de qualité de service sur les deux sites, relancer des communications vocales puis reprendre les mesures avec notre outil *Iperf*.

Au niveau de chaque site, on se connecte en ssh sur l'interface des équipements réseau et on fait le paramétrage nécessaire pour l'activation de la Qualité de service.

Le site de notre client à Birkhadem est connecté en liaison VPN au réseau de l'opérateur Icosnet, ce qui fait que les deux sites A et B se communiquent en passant sur le réseau Internet mais le trafic est crypté dans un canal VPN pour sécuriser les appels des clients.

Nous nous positionnons dans le site A de Birkhadem et nous allons donc nous servir du VPN existant pour lui appliquer une qualité de service sur le trafic Voix transitant dessus.

Comme le montre le schéma global présenté précédemment, nous retrouvons un routeur Cisco 2811 et un switch Cisco 2960 où sont reliés les IP Phone et les PC ou équipés de soft phone.

IV.2. Implémentation du mécanisme de la qualité de service [14]:

Commençons par le routeur 2811 :[19]

Avant de commencer, nous tenons à préciser que les adresses utilisées dans ce rapport sont modifiées ou masquées pour répondre à l'obligation de confidentialité exigée par l'organisme d'accueil.

Comme première étape, on se connecte par ssh à l'interface du routeur cisco 2811.

Une fois logué, nous passons en mode configuration terminal.

Avant de passer le paramétrage proprement dit de la QoS, nous activons la priorité de file d'attente et nous limitons à 2 méga le seuil des paquets qui transitent le routeur sans rester dans la file d'attente.

Ainsi une fois la bande passante de 2 méga est saturée, les nouveaux paquets qui arrivent seront mis en file d'attente jusqu'à la libération de la bande.
Ci-dessous une capture écran des commandes tapées sur le routeur de Birkhadem :

```
RWBirkhadem(config)# priority-queue outside
RWBirkhadem(config-priority-queue)# queue-limit 2048
RWBirkhadem(config-priority-queue)# tx-ring-limit 256
RWBirkhadem(config-priority-queue)# exit
```

Figure III.13 : Activation de la priorité et la taille de la queue sur l'interface du routeur

Notre stratégie consiste à appliquer la norme DiffServ pour définir un traitement préférentiel des paquets de la voix.

La classification de paquets implique d'employer un descripteur de trafic pour classer un paquet dans un groupe spécifique et de rendre le paquet accessible pour un traitement QoS dans le réseau. Pour cela nous allons utiliser le mécanisme Per Hop Behaviors (PHB) doté du service Expedited forwarding (EF).

PHB **Expedited forwarding** (EF) **[15]** garantit que les paquets dotés du point de code recommandé 46, EF (101110), bénéficient du meilleur traitement disponible sur le réseau. Le service Expedited forwarding est souvent comparé à une ligne spécialisée. Les routeurs Diffserv garantissent un traitement préférentiel aux paquets accompagnés du point de code 46 (101110) pour l'acheminement vers leur destination. Il assure ainsi une basse perte de paquets, une faible latence, une gigue faible, une bande passante assurée et un service de bout en bout par des domaines DS (Diffserv).

Comme le paramètre temps est très important dans la transmission des paquets VOIP, nous allons choisir le PHB EF qui réserve un traitement accéléré au niveau de chaque routeur traversé.

Son application sur les équipements de notre architecture doit pouvoir ainsi prioriser les flux de données souhaités. Nous allons donc l'utiliser pour imposer un traitement prioritaire pour les paquets voip entre nos deux réseaux.

Le paramétrage de la QoS sur le routeur passe par trois étapes essentielles, à savoir :

1. Création de la class-map (indiquant quels sont les critères permettant d'identifier le trafic concerné par les règles de la policy map)
2. Création de la policy-map (indique quelles sont les actions à appliquer pour le trafic intéressant)
3. Application de la policy-map à l'interface concernée.

On passe donc à la création de notre class- map, appelée « client_birkhadem ». Pour laquelle nous appliquons un **DSCP** de priorité **ef**.

```
RWBirkhadem(config)#class-map voice client_birkhadem
RWBirkhadem(config-cmap)# match dscp ef
RWBirkhadem(config-cmap)# match tunnel-group a.b.c.d
RWBirkhadem(config-cmap)# match flow ip destination-address
```

Figure III.14 : Création de la class-map

Où **a.b.c.d** correspond à l'adresse public de notre site de Chéraga.

Notre class-map est ainsi créée, nous paramétrons maintenant la policy-map. On va l'appeler voice_client_birkhadem.

```
RWBirkhadem(config)# policy-map voice_client_birkhadem
RWBirkhadem(config-pmap)# class voice_client_birkhadem
```

Figure III.15 : Création de la policy-map

Suivi des commandes ci-après pour appliquer la priorité à la class-map de cette policy et configurer la priority-queue sur l'interface Outside.

```
RWBirkhadem(config-cmap)# class voice_client_birkhadem
RWBirkhadem(config-pmap-c)# priority
RWBirkhadem(config-cmap)# end
RWBirkhadem# conf term
RWBirkhadem(config)# priority-queue outside
RWBirkhadem(config)# service-policy voice_policy_birkhadem  interface outside
```

Figure III.16 : Application de la Priorité sur la class-map

En fin nous appliquons le service policy de notre policy-map, en l'occurrence voice_policy_birkhadem » sur l'interface Outside du routeur.

Nous avons à présent configuré notre routeur pour utiliser la priorité EF de DSCP comme mécanisme de qualité de service sur le trafic VoiP.

Passons à la configuration de la QoS sur le Switch Cisco 2960 : [20]

Pour cet équipement nous allons configurer tous les ports sur lesquels transite le trafic Voix.

L'application de la QoS diffère d'un port relié à un IP Phone ou SoftPhone d'un port qui est relié à l'interface du routeur. Notre switch possède 24 Ports Ethernet.

La commande à utiliser pour paramétrer automatiquement la qualité de service sur les ports où sont branchés les IP Phone et Soft phones est la suivante :

```
Switch2960(config)# interface Ethernet 0/1
Switch2960(config-if)# auto qos voip cisco-phone
```

Figure III.17 : Activation de la Qos sur l'interface de IP Phone

Il faudrait donc passer en mode configuration et sélectionner l'interface voulue avant de lui paramétrer la QoS.

Pour passer à une autre interface, on sort d'abord par exit et on tape de nouveau Interface suivi du nom de la prochaine interface à configurer avant de lui taper la commande auto qos

Ainsi on répète les même opérations jusqu'au paramétrage de tous les ports utilisés pour les communications VoiP.

Nous passons ensuite à la configuration de l'interface reliée au routeur cisco 2811.

```
Switch2960(config)# interface Ethernet 0/0
Switch2960(config-if)#
Switch2960(config-if)# auto qos voip trust
Switch2960# copy running-config startup-config
```

Figure III.18 : Activation de la Qos sur l'interface reliée au routeur

Pour cette interface on choisit plutôt **trust** à la place de IP Phone.

Une fois la configuration acceptée, on enregistre avec la commande copy running-config startup-config.

De cette façon, nos équipements sont paramétrés pour distinguer le trafic voix transitant sur leurs ports et ainsi pouvoir lui appliquer la haute priorité et ainsi accélérer son traitement.

Il convient d'appliquer les mêmes configurations sur les équipements du site Chéraga où notre solution de téléphonie Asterisk est installée.

Donc au final, nous aurons les deux sous-réseaux configurés pour appliquer la qualité de service sur le trafic voix échangé entre eux.

Nous relançons maintenant nos appels entre le site du client à Birkhadem et la plateforme Asterisk basée à Chéraga et reprendre les mesures avec *Iperf*.

Coté serveur:

Iperf sera donc relancé avec l'argument –s qui signifie serveur suivi de –u pour préciser que les mesures seront prises sur le trafic UDP.

```
[root@localhost ~]# iperf -s -u
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  108 KByte (default)
------------------------------------------------------------
```

Figure III.19 Mise a l'écoute du serveur Iperf

Coté client:

Pendant la tenue des appels entre les deux sites nous lançons la commande *Iperf* coté client avec la commande :

iperf -c 192.168.43.197 -u -i 1

Au bout de 10 secondes, le résultat de cette commande affiche :

```
[root@localhost /]# iperf -c 192.168.43.197 -u -i 1
------------------------------------------------------------
Client connecting to 192.168.43.197, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  108 KByte (default)
------------------------------------------------------------
[  3] local 192.168.43.141 port 40947 connected with 192.168.43.197 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  1.0- 2.0 sec   129 KBytes  1.06 Mbits/sec
[  3]  2.0- 3.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  3.0- 4.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  5.0- 6.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  6.0- 7.0 sec   129 KBytes  1.06 Mbits/sec
[  3]  7.0- 8.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  8.0- 9.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  9.0-10.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0- 9.8 sec   963 KBytes   808 Kbits/sec  11.768 ms  222/  893 (25%)
[root@localhost /]#
```

Figure III.20 Résultat Iperf sur le client après activation Qos

Et sur le serveur nous récupérons le résultat suivant

```
C:\Users\JET>iperf -s -u -i 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.43.197 port 5001 connected with 192.168.43.141 port 40947
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams

[  3]  0.0- 1.0 sec  17.2 KBytes   141 Kbits/sec  22.021 ms    0/   12 (0%)
[  3]  1.0- 2.0 sec  43.1 KBytes   353 Kbits/sec  25.815 ms   34/   64 (53%)
[  3]  2.0- 3.0 sec  54.6 KBytes   447 Kbits/sec  25.929 ms   27/   65 (42%)
[  3]  3.0- 4.0 sec   102 KBytes   835 Kbits/sec  20.835 ms    7/   78 (9%)
[  3]  4.0- 5.0 sec   142 KBytes  1.16 Mbits/sec   2.215 ms  152/  251 (61%)
[  3]  5.0- 6.0 sec   126 KBytes  1.03 Mbits/sec   7.741 ms    0/   88 (0%)
[  3]  6.0- 7.0 sec   126 KBytes  1.03 Mbits/sec  10.487 ms    0/   88 (0%)
[  3]  7.0- 8.0 sec   122 KBytes  1000 Kbits/sec  12.974 ms    0/   85 (0%)
[  3]  8.0- 9.0 sec   134 KBytes  1.09 Mbits/sec  11.965 ms    0/   93 (0%)
[  3]  0.0- 9.8 sec   963 KBytes   808 Kbits/sec  11.769 ms  222/  893 (25%)

C:\Users\JET>
```

Figure III.21 Résultat Iperf sur le serveur après activation Qos

Comme nous le constatons sur la capture ci-dessus, le test a ressorti les paramètres suivants :

- Un transfert de 963 Bytes de données
- Dans une bande passante de 808 Kbits/sec
- Une gigue de 11.768 ms
- Un taux de perte de 25% de paquets

IV.3 Interprétation des résultats avec application QoS :

Ces résultats montrent que la qualité de la voix est significativement améliorée même si sur le plan de la qualité de l'appel nous n'avons pas ressenti la meilleure qualité attendue au moment de l'appel et cela malgré l'application de la configuration QoS. Surtout le taux de perte de paquets de 25% qui reste comme même élevé.

Après analyse de nos résultats, on retient que cela pourrait être du à plusieurs raisons, entre autres :

- Le support des communications : L'appel transite par un VPN donc par Internet du site client à Birkhadem au centre de notre plateforme Asterisk à Chéraga. Ce qui fait que nous ignorons le chemin exact emprunté par nos paquets pour atteindre leur destination et surtout les paquets n'empruntent pas forcement le même chemin, d'où une variation du délai de transit. Une autre cause de la variation du délai de transit dépend du nombre de routeurs traversés et de la charge de chaque routeur traversé.
- Sur Internet, les routeurs et serveurs sur lesquels transitent nos appels, nous ne savons pas leur nombre ni s'ils supportent ou pas les mécanismes de qualité de service.
- Ajouté à cela, le fait que la moitié du chemin traversé par nos paquets était un réseau WIMAX de l'opérateur ICOSNET. Et la technologie WIMAX est connue par sa lenteur en termes des temps de réponse.

Synthèse : La qualité de la voix après application des mécanismes de qualité de service s'est nettement améliorée par rapport aux tests où les deux sites ne sont pas configurés pour supporter la qualité de service. Nos tests comparatifs montrent donc bien l'apport positif de l'application des mécanismes de Qualité de service sur l'amélioration de la qualité des appels vocaux en utilisant notre plateforme VoiP même si pour avoir une qualité garantie il faudrait toucher à tous les niveaux traversés par nos données.

Conclusion :

Nous avons consacré ce chapitre pour la réalisation d'une stratégie de qualité de service et son application sur nos deux sites de test. Nous avons réussi à installer et faire fonctionne notre IPBX et effectuer des appels vers différents types de terminaux et au final nous avions réalisé nos tests à base de ces appels effectués entre les deux sites suivant deux scénarios, avec et son application de la QoS.

Un comparatif des résultats obtenus est alors élaboré et précise bien le rôle très significatif de la QoS sur l'amélioration de la qualité de la voix de nos appels. Or une telle stratégie n'est pas suffisante pour garantir une offre de qualité intéressante. A cette dernière doit s'ajouter l'utilisation de liaisons spécialisées comme support de communication entre les sites de nos clients et celui de notre plateforme centrale de téléphonie. Aussi, l'allocation d'une bande passante suffisante, continue et la maintenance et supervision des différents équipements participant au transport des appels entre l'émetteur et son récepteur demeurent une nécessité absolue.

Le prochain chapitre présentera justement une solution permettant de superviser les équipements réseaux et leur utilisation en termes de bande passante.

CHAPITRE 4 :

SOLUTION DE MONITORING ET SUPERVISION RÉSEAU

I. Introduction [16] [17]:

La mise en place de mécanismes de qualité de service dans un environnement VoIP ne soit efficace qu'avec un suivi régulier et attentif des administrateurs sur les équipements constituant le réseau et en surveillant continuellement la consommation de bande passante sur différents niveaux. Une telle tâche dans un grand parc Informatique ne serait pas du tout simple sans l'automatisation de quelques tâches et la mise en place de système d'alertes nous informant ou nous avertissant d'un souci technique.

Cela nous a emmené à étudier les solutions de supervision open sources existantes et finir par choisir l'application Nagios qui répond mieux à nos attentes.

Ce chapitre serait donc dédié à la présentation de cette solution, son installation sous la distribution linux CentOS et sa configuration pour la supervision de notre solution Asterisk ainsi que les routeurs et switch de notre réseau.

II. Généralités : En informatique, le monitoring est fait par un système capable de surveiller des équipements dans un parc informatique, tel que les Serveurs, Routeurs, Switchs …etc. On obtient rapidement et précisément des événements inattendus (principalement les anomalies).

Dans ce monitoring, on retrouve trois grands niveaux du monitoring :

a) Le monitoring système : il est basé sur la surveillance du cœur du système, il donne les informations sur l'utilisation du CPU, la mémoire, espace de disque dur…etc
b) Le monitoring réseau : ce type de surveillance permet de diagnostiquer la présence d'un équipement physique connecté à un réseau. Il permet aussi de vérifier que la connectique marche et les internautes peuvent consulter leurs serveurs externes (exemple serveur Web).
c) Le monitoring applicatif : en outre de la surveillance de la présence des équipements physique de réseau, il fait aussi la supervision des applications qui s'exécutent et les informations retournées.

III. Définitions et utilités [14]: Le monitoring informatique est un outil de sécurité et de supervision indispensable dans un parc informatique. Il permet de diagnostiquer les anomalies détectées à l'aide des alertes, des emails, des SMS …etc .

Pour les utilités de cet outil on note :

a) La fiabilité : l'utilisation du monitoring informatique a le but de surveillance des équipements en permanence afin de détecter les anomalies.

b) La performance : le but de monitoring de la performance est de retourner les informations sur la disponibilité des équipements comme par exemple le temps de la résolution de DNS , et le temps de connexion et , le temps de récupération de la page web et l'ensembles des éléments (image, scripts…), grâce à cette analyse il permet de diagnostiquer la bande passante.

c) Le contenu : dans ce cas les informations retournées sont analysées ; par exemple détection de la suppression d'un fichier sur un serveur FTP, la modification d'une page web, et la disparition d'un mot clef.

IV. Fonctionnement Principal [17] :

Nagios récupère les informations fournies par les services de surveillance et les analyse, si l'un des résultats de cette analyse fait remonter ou prévenir un problème. les services de surveillance peuvent envoyer des avertissements (alertes) à l'administrateur du réseau de différentes manières: courriers électroniques, messages instantanés, SMS,… etc Les différents états possibles d'un hôte sont :

Up : en marche
Down : éteint
Unreachable : inaccessible
Pending : indéterminé

Nagios repose sur 3 parties :

- Nagios software,
- Configuration files,
- Plugins

Tel que Nagios software consiste au programme obtenu après installation de l'exécutable téléchargé, y compris son interface web.

Configuration files représentent les fichiers de configuration à paramétrer pour que Nagios pusse superviser nos machines.

Le fonctionnement proprement dit de cet outil Nagios repose sur des plugins collectant des informations récupérées auprès des agents installés sur les serveurs linux ou windows et celle

provenant des équipements télécom (switchs, parefeu et routeurs …etc).

Les plugins sont des programmes informatiques développés généralement par la communauté open sources. Ils peuvent être utilisés tels qu'ils sont ou réadaptés à un besoin spécifique. A leurs exécutions, ils interrogent les agents installés sur les machines à surveiller pour leur solliciter des informations concernant cette machine.

Ceci demande donc d'installer l'agent NSClient sur tous les serveurs équipés de systèmes d'exploitation Windows et installer NRPE sur les serveurs dotés de systèmes Linux. Tandis qu'il faudrait configurer des communautés sur les équipements réseaux tels que les switchs, parefeu et routeurs afin de communiquer leurs états au serveur Nagios va le protocole SNMP.

V. installation de Nagios sous Linux CentOS :

Comme tous les produits open sources, Nagios est disponible gratuitement au téléchargement sur leur site principal www.nagios.org

Une fois le fichier compressé en .tar.gz est téléchargé, nous le sauvegardons dans le répertoire **/tmp**

avec la commande suivante on va dézipper le fichier :

tar zxvf nagios-3.2.0.tar.gz

En se positionnant à l'intérieur de son répertoire, on lance l'installation en suivant les étapes suivantes :

./configure –with-command-group=nagcmd

make all

make install

make install-init

make install- config

make install-commandmode

Pour la configuration de son interface web on fait :

make install-webconf

Ensuite, on crée l'utilisateur de Nagios et son mot de passe :

htpasswd –c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Pour prendre en considération ces changement, nous devons redémarrer le le serveur apache :

service httpd restart

Pour vérifier que l'installation est bien fait, lancer cette commande :

/usr/local/nagios/bin/nagios/ -v /usr/local/nagios/etc/nagios.cfg

Le démarrage de Nagios se fait avec la commande suivante :

/etc/init.d/service nagios start

IV.1 -Installation des Plugins Nagios :

Comme évoqué plus haut, nagios repose sur des plugins pour assurer le suivi du parc supervisé. Les Plugins sont des programmes informatiques compilés en Perl , C…etc. Sans ces plugins Nagios ne fonctionne pas, il est incapable de superviser quoi que ce soit. Ces plugins, une fois bien installés et configurés utilisent des codes pour interpréter les anomalies.

Ces codes sont :

OK **:** si tout marche bien.
WARNING **:** alerte simple.
CRITICAL **:** alerte critique.
UNKNOWN **:** problème au moment d'utilisation des plugins.

Les principaux plugins utilisés par nagios sont :

- check_disk : Vérifie l'espace occupé d'un disque dur
- check_http : Vérifie le service "http" d'un hôte
- check_ftp : Vérifie le service "ftp" d'un hôte
- check_mysql : Vérifie l'état d'une base de données MYSQL
- check_nt : Vérifie différentes informations sur un système d'exploitation Windows
- check_nrpe : Permet de récupérer différentes informations sur les hôtes
- check_ping : Vérifie la présence d'un équipement, ainsi que sa durée de réponse
- check_pop : Vérifie l'état d'un service POP (serveur mail)
- check_snmp : Récupère divers informations sur un équipement grâce au protocole SNMP (Simple Network Management Protocol)

Pour son installation on télécharge les plugins à partir du site officiel de nagios sous forme d'un fichier zippé. Après avoir décompressé le fichier avec la commande :

tar zxvf nagios-plugins-1.4.14

On se positionne dans son répertoire et on lance l'installation :

./configure --with-nagios-user=nagios with-nagios-group=nagios

make

make install

VI. Configuration de Nagios [17]:

VI.1 Configuration pour surveiller la machine Windows [17]:

Une fois le client et le serveur installés, il faut configurer Nagios de la manière suivantes :

Ajouter la machine à surveiller dans le fichier **windows.cfg** :

On note qu'il ya pas uniquement une seule manière d'ajouter une machine à la supervision ; on peut par exemple définir toutes les machines Windows dans un seul fichier qu'on nomme windows.cfg et en suite on fait un seul appel à ce fichier dans le fichier de configuration principal de nagios (nagios.cfg). Ou bien on peut aussi créer un fichier de configuration propre à chaque machine, mais avec ça on fait dans nagios.cfg autant d'appels que de host définis.

```
define host{
        use             windows-server
        host_name       machine_test
        alias           My Windows Server
        address         192.168.43.35
        }
```

Puis ajouter les services de la machine qu'on souhaite surveiller (Exemple : Utilisation d'espace disk, utilisation de la mémoire, charge de CPU… etc), il convient de se rendre dans le fichier **nagios.cfg**, ajouter cette ligne pour faire appel au fichier de configuration concernant cette machine (machine_test.cfg).

cfg_file =/usr/local/nagios/etc/objects/machine_test

Et dans le fichier de définition des commandes, on doit déclarer les commandes à utiliser (**commands.cfg**) :

```
# 'check_nt' command definition
        define command{
              command_name      check_nt
              command_line      $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s
              PASSWORD -v $ARG1$ $ARG2$
              }
```

Pour le password mis dans la command_line, ça doit être le même avec celui défini dans nsc.ini de la machine cliente à surveiller.

Il faudrait tout enregistrer et redémarrer le service nagios pour que les modifications soient prises en charge par le serveur.

VI.2 Configuration de Nagios pour surveiller les machines Linux[17] :

Dans les fichiers de configuration du serveur Nagios, il faut configurer les fichiers suivants : linux_test.cfg, nrpe.cfg, nagios.cfg et commands.cfg. Tel que :

* **linux_test.cfg** : Doit contenir les coordonnées de la machine linux à surveiller
* **nrpe.cfg** : Dans ce fichier il faudrait ajouter l'adresse de machine à superviser. En ajoutant cette ligne **allowed_hosts=127.0.0.1,192.168.43.200**

Ces deux adresses représentent l'adresse de la machine locale et celle de la machine à surveiller.
Puis déclarer ces services à surveiller avec cette commande :
command[check_load]=/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20
* **nagios.cfg**: Dans ce fichier, on définit la machine à superviser avec la ligne suivante:
cfg_file=/usr/local/nagios/etc/objects/linux_test.cfg
* **commands.cfg** :Ajouter dans ce le plugin check_nrpe celui qui communique avec l'agent nrpe qu'est installé sur la machine à superviser (linux_test).

```
# 'check_nrpe' command definition

 define command{
        command_name      check_nrpe
        command_line      $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
        }
```

Il convient maintenant de tout enregistrer et redémarrer le service nagios pour les prendre en charge et entamer leur supervision.

VI.3 Configuration de Nagios pour surveiller les Routeurs, Switchs et Parefeu :

Pour superviser ce genre d'équipements, il faut créer une communauté SNMP sur chaque routeur, switch ou parefeu concerné par la supervision.

VI.3.1 Configuration d'une communauté SNMP :

Sur chaque équipement à superviser, il faut se connecter en mode configuration et activer la communauté de cette façon :

```
Enable                                        (pour passe au mode privilégié)
conf terminal                               (pour passer au mode configuration)
snmp-server community MA_Commaute ro 1          (ro veut dire  Read Only)
snmp-server host 192.168.43.200 MA_Commaute      (tel que l'adresse
               192.168.43.200 est l'adresse de serveur de supervision).
```

Sur le serveur de supervision, il faudrait installer un outil (à l'instar de MRTG) capable de récupérer régulièrement les informations sur l'état des équipements télécom et les enregistre dans son fichier log.

Pour notre cas, nous utilisons justement MRTG. Une fois téléchargé, on l'installe sur notre serveur de supervision.

Après vérification de son fonctionnement, il convient et voir également qu'il génère bien le fichier log où seront stockées les informations collectées. On retient ainsi le chemin vers son fichier log pour l'utiliser dans les déclarations à faire sur Nagios.

Exemple pour le Switch Cisco 2960 :

```
define service {
    use                 generic-service
    host_name           Switch-Cisco-2960
    service_description Uptime
    check_command       check_snmp!-C public -o sysUpTime.0
}
```

Dans le paramètre **check_command** de la définition de service ci-dessus, le -C public indique au plugin que le nom de communauté SNMP à utiliser est **public** et que -o sysUpTime.0 indique que l' OID doit être contrôlé. (OID pour Object Identifier).

Si on souhaite s'assurer qu'un port/interface particulier du switch est dans un état up, on peut ajouter la définition de service comme celle-ci:

```
define service {
    use                 generic-service ;
    host_name           Switch-Cisco-2960
    service_description Port 1 Link Status
    check_command       check_snmp!-C public -o ifOperStatus.1 -r 1 -m RFC1213-
MIB
}
```

VI.3.2 Supervision de la bande passante/trafic :

L'une des plus importantes options offertes par Nagios pour la supervision des équipements télécom est sans doute sa capacité à surveiller la consommation de la bande passante.

Comme nous nous intéressons de près à l'usage de la bande passante sur nos switchs et routeurs, qui joue un rôle primordial dans le maintient de la qualité de service sur notre solution VoIP, il nous faudra des outils permettant de collecter cette information à temps et principalement quand le seuil défini est atteint pour agir vite et résoudre la saturation.

En utilisant MRTG sur notre serveur de supervision, nous permettra de s'occuper de cette tâche et récupérer régulièrement ces indicateurs (exemple chaque 5 minutes) et les inscrire dans son fichier log.

Nous allons ensuite paramétrer Nagios afin de consulter ce fichier Log et interpréter les valeurs écrites. Avec son plugin spécifiquement développé pour ça, **check_mrtgtraf** il nous alerte en cas de dépassement des seuils.

Pour pouvoir le faire, nous aurons besoin que le plugin **check_mrtgtraf** connaisse l'emplacement du fichier où MRTG stocke ses données, ainsi que les seuils qu'on lui définit.

Pour notre cas, on supervise l'un des ports d'un switch cisco. Le fichier de log de MRTG est stocké dans **/var/lib/mrtg/192.168.43.200_1.log**.

Voici la définition de service qu'on utilise pour superviser les données de bande passante stockées dans ce fichier…

```
define service {
    use                 generic-service ; Inherit values from a template
    host_name           Switch-Cisco-2960
    service_description Port 1 Bandwidth Usage
    check_command
check_local_mrtgtraf!/var/lib/mrtg/192.168.43.200_1.log!AVG!1000000,2000000!500
0000,5000000!20
}
```

Dans l'exemple ci-dessus, l'option **/var/lib/mrtg/192.168.43.200_1.log** passée à la commande *check_local_mrtgtraf* indique au plugin dans quel fichier de log MRTG il doit aller lire.

L'option AVG indique qu'il doit utiliser des statistiques basées sur la moyenne de la bande passante. Les arguments 1000000,2000000 sont les seuils de warning (en bytes) pour le taux de trafic entrant. Les arguments 5000000,5000000 sont des seuils critiques (en bytes) pour le taux de trafic sortant. L' 20 option indique au plugin de renvoyer un état CRITICAL si le fichier de log MRTG est plus vieux que 20 minutes (il devrait être mis à jour toutes les 10 minutes).

Ci-dessous l'interface de Nagios montrant les status OK du serveur de supervision et du Switch Cisco 2960.

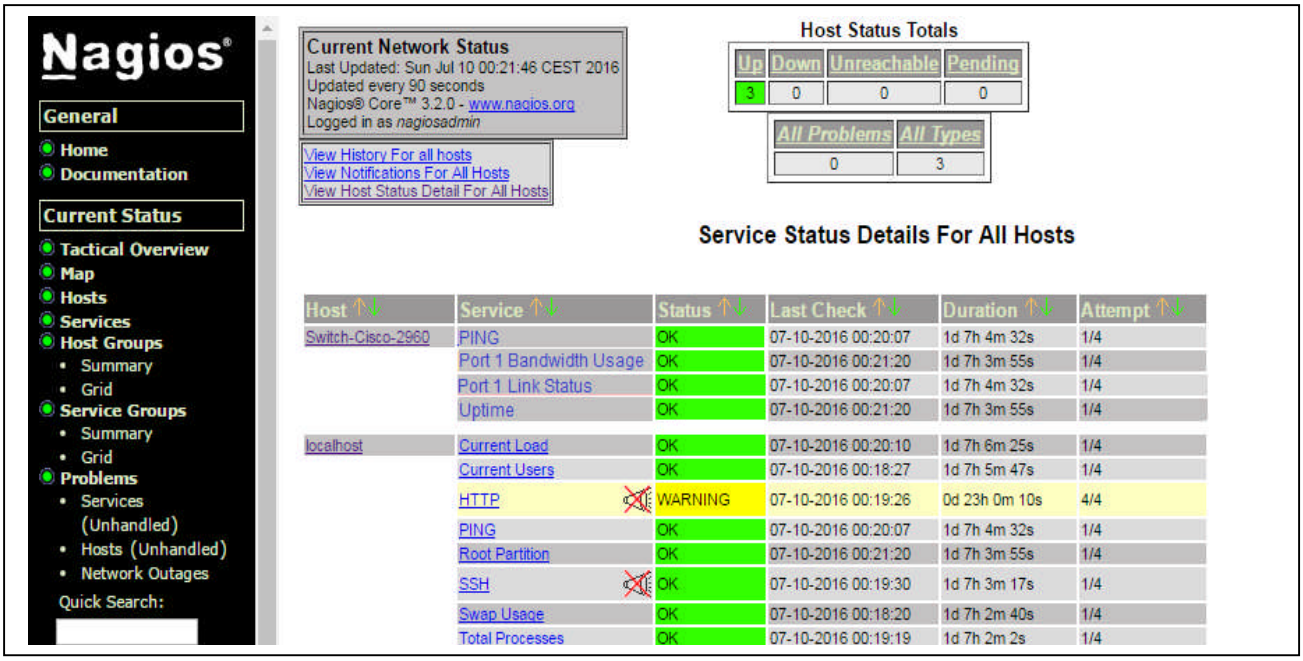


Figure IV.1 Interface de suivi de Nagios

Au niveau des services, nous présentons ci-dessous la capture de l'interface au moment de changement sur le status CRITICAL de l'utilisation de la bande passante sur le Switch Cisco 2960 et au status WARNING sur le port 1 supervisé par notre outl Nagios.

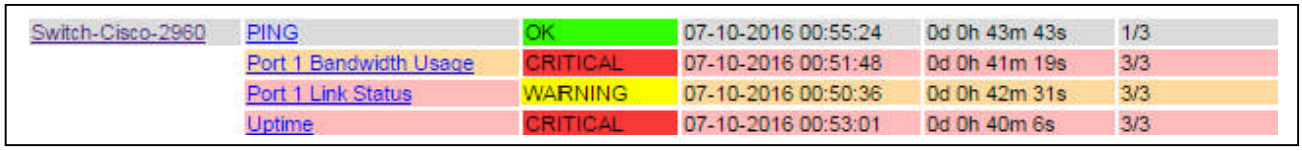


Figure IV.2 Status des services du Switch 2960 supervisé par Nagios

Dans ces conditions, Nagios, en plus de l'affichage sur cette Interface, envoi une alerte sur l'adresse mail configurée pour informer l'administrateur réseau de ces deux cas CRITCAL et

WARNING). Ce dernier pourra donc intervenir rapidement pour voir les causes de la saturation de la bande passante et vérifiera l'avertissement envoyé sur l'état du port 1 du Switch Cisco 2960. Ainsi si le switch en question appartient à un client, l'administrateur de notre entreprise pourra intervenir avant même que le client se rend compte du disfonctionnement survenu.

Conclusion :

L'outil de monitoring présenté dans ce chapitre complètera en grande partie notre solution de Qualité de Service proposée pour maintenir une meilleure qualité pour notre solution de Téléphonie sur IP et assurer sa disponibilité. La multiplicité des équipements informatiques et le fonctionnement en haute disponibilité impose aujourd'hui de faire recours aux solutions automatisées afin de pouvoir assurer une bonne gestion des nos infrastructures réseaux et par conséquent assurer une bonne qualité de service.

CONCLUSION GÉNÉRALE

Conclusion Générale :

Dans ce projet de fin d'études, nous avons fait une étude de la qualité de service dans les environnements VoiP et nous avions détaillé les différents mécanismes permettant d'atteindre une bonne qualité de service. Notre premier objectif était d'arriver à réaliser une solution de téléphonie sur IP, la faire fonctionner et la mettre en production pour tester la qualité de la voix sur ses appels. Une fois mise en place, nous sommes appelés à mettre en place des mécanismes de qualité de service sur lesquels nous devrons ressortir une stratégie de qualité de service permettant à notre entreprise de bien améliorer la qualité de son produit principal qui consiste en la Voix sur IP.

Nous étions bien motivés par le fait d'avoir l'opportunité d'étudier et de réaliser une solution pratique qui nous a permis de toucher et découvrir beaucoup de technologies et principalement le travail sous l'environnement Linux et Cisco.

Au bout de notre travail, nous avons conclu que l'application des mécanismes de qualité de service est plus que nécessaire pour l'amélioration de la qualité voix sur la solution de téléphonie sur VoiP. Mais cela n'est pas suffisant pour la garantir sur les grands réseaux Intranet et encore moins sur les réseaux étendus comme Internet. Afin d'honorer ses engagements SLA avec ses clients, un opérateur VoIP doit bien mettre en avant la nécessité pour ses clients de s'adhérer à l'utilisation des équipements supportant la QOS, les meilleurs codecs ainsi que l'utilisation des supports de meilleurs temps de transport à l'instar des liaisons spécialisées et fibre optique.

Dans ces conditions, la « Telephony Over IP » serait une solution irréprochable en termes de prix et de qualité de la voix.

Au terme de ce travail, nous estimons que nos efforts ont été récompensés par des résultats assez intéressants qui nous ont permis de nous imprégner de connaissances techniques nouvelles sur la technologie des réseaux de communication en général contribuant ainsi à notre formation. Il nous a été une expérience fructueuse et nous a permis de mieux s'approcher du milieu professionnel. Cette expérience nous a permis également de savoir comment gérer et optimiser le temps dans le but d'en profiter au maximum.

Nous considérons également que notre travail pourrait être un bon repère et référentiel pour servir tout autre projet visant à approfondir et déployer d'autres outils destinés à l'environnement VoIP.

BIBLIOGRAPHIE

Références Bibliographiques

[1] La VOIX surIP de Olivier Hersent, David Gurle et Jean-Pierre Petit, de l'édition Dunod imprimé en 2004.

[2] http://www.frameip.com/voip/

[3] http://docplayer.fr/785466-Formation-cisco-ccvp-quality-of-service-v-2-1.html

[4] http://www.icosnet.com

[5] http://www.asterisk-france.net/

[6] http://www.loria.fr/~ichris/Teaching/ESIAL/ESIAL3/TPESR/Diffserv.pdf

[7] http://www.catapulse.org/articles/view/56

[8] http://www.cisco.com/cisco/web/support/CA/fr/109/1096/1096814_qos-voip-vpn.html#tab3

[9] https://www.etsmtl.ca/ETS/media/ImagesETS/Labo/LIVIA/memoires/Memoire_Mourad.pdf

[10] http://blog.nicolargo.com/2009/03/outil-pour-la-mesure-de-la-qos-sur-les-reseaux-ip.html

[11] http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html

[12] http://blog.nicolargo.com/2007/06/utilisation-avancee-de-iperf.html

[13] http://quick-tutoriel.com/395-comment-activer-le-protocole-netflow-sur-un-routeur-cisco/

[14] http://www.cisco.com/cisco/web/support/CA/fr/109/1092/1092197_dscpvalues.html

[15] https://docs.oracle.com/cd/E19957-01/820-2982/ipqos-intro-10/index.html

[16] http://www.monitoring-fr.org/solutions/nagios/

[17] https://www.nagios.org/

[18] http://blog.nicolargo.com/nagios-tutoriels-et-documentations

[19] http://www.cisco.com/cisco/web/support/CA/fr/110/1109/1109083_voice-vlan-00.pdf

[20] http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/qos/configuration_guide/b_qos_152ex_2960-x_cg/b_qos_152ex_2960-x_cg_chapter_011.html

[21] https://www.google.dz/les fichiers log de iperf

[22] http://igm.univ-mlv.fr/~rachedi/docs/resacc/TP_Perf.pdf

[23]https://aful.org/ressources/formations/formation-introduction-linux/downloadFile/file/IntroductionLinux.pdf