République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira de Bejaïa

Faculté des Sciences Exactes

Département d'Informatique

MEMOIRE DE MASTER

En

Informatique

Option

Administration et Sécurité des Réseaux

Thème

Déploiement d'une solution VoIP en utilisant les mesures de la qualité de service

---

Réalisé par :

M. ZENOUCHE Lyes

M. HAMADACHE Amine

Promoteur :

M. MOKTEFI Mohand

Année universitaire 2021/2022

Résumé

Toute nouvelle entreprise a besoin d'un réseau robuste sur lequel s'appuyer pour ses communications internes et externes et la VoIP est l'une des solutions disponibles pour répondre à ces besoins, mais elle peut être considéré comme une solution faible tout seul, elle doit être soutenue par des mesures de qualité de service bien mises en place et également bien sécurisée contre les attaques internes et externes.

Par conséquent, afin de réaliser notre mémoire, nous avons fait une réalisation d'un réseau simulé pour pouvoir créer une solution de VoIP et appliquer sur celle-ci les politiques de sécurité et les mesures de qualité de service nécessaires.

Mots clefs: VoIP, QoS, ToIP, GNS3, Firewall, PfSence, Asterisk, MicroSIP, Sécurité.

Abstract

Any new company needs a robust network to rely on for its internal and external communications and VoIP is one of the solutions available to meet these needs, but it can be considered as a weak solution on its own, it must be supported by well implemented QoS measures and also well secured against internal and external attacks.

Therefore, in order to realize our thesis, we made a realization of a simulated network to be able to create a VoIP solution and apply on it the necessary security policies and quality of service measures.

Key words: VoIP, QoS, ToIP, GNS3, Firewall, PfSence, Asterisk, MicroSIP, Security.

Remerciement

Nous remercions en premier lieu ALLAH le tout puissant et miséricordieux, qui nous a donné la force et la volonté pour accomplir ce modeste travail.

Nous tenons à remercier notre promoteur M. MOKTEFI Mohand pour avoir accepté de diriger ce travail, pour son aide, ses précieux conseils, sa confiance sa patience, tout au long de la réalisation de ce mémoire.

Nous souhaitons formuler notre remerciement les plus affectueux à nos familles et surtout nos très chers parents et frères et sœurs, qui ont toujours été là pour nous.

Nous tenons également à remercier notre maitre de responsable de stage M. AMMARENE Arezki pour avoir fourni les moyens et les ressources nécessaire à la réalisation de ce projet.

Nous remercions également tous nos amis qui ont contribués de près ou de loin à nous encouragé, sans oublier toute personne qui nous a aidés à mener à terme notre projet.

Dédicaces

Je dédie ce travail

A mes très chers parents qui ont été la source de ma réussite grâce à leurs prières et leur encouragement qui m'ont offert leur amour indéfectible et qui n'ont cessé de me donner le nécessaire à ma réussite. Toute ma gratitude pour leur soutient tout au long de mes études, que dieu les protège et les garde pour moi.

A mes très chères sœurs Aicha, Wezna et Maissa qui ont été là pour moi tout au long de mon parcours universitaire.

A mes amis Amar, Yasser, Abdou et Sara qui m'ont aidé dans les moments difficiles pour réaliser ce travail.

A toute personne qui m'ont aidé à achever ce niveau.

Lyes.Z

Dédicaces

Je dédie ce travail

A mes très chers parents qui ont été la source de ma réussite grâce à leurs prières et leur encouragement qui m'ont offert leur amour indéfectible et qui n'ont cessé de me donner le nécessaire à ma réussite. Toute ma gratitude pour leur soutient tout au long de mes études, que dieu les protège et les garde pour moi.

A mes très chères sœurs Hamida, Amina

A mes très chers frères Mohamed et Mourad

A mes très chers cousins Billal et Ayoub

Qui ont été là pour moi tout au long de mon parcours universitaire.

A mes chers amis Amar, Abdelghani, Abdou, Sara et Fatima qui m'ont aidé dans les moments difficiles pour réaliser ce travail.

A toute personne qui m'ont aidé à achever ce niveau.

Amine.H

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

ADSL	**Asymmetric Digital Subscriber Line**
AF	**Assured Forwarding**
APC	**Assemblée Populaire Communal**
ASCII	**American Standard Code for Information Interchange**
CDP	**Cisco Discovery Protocol**
CoS	**Class of Service**
DHCP	**Dynamic Host Configuration Protocol**
DiffServ	**Differentiated Services**
DNS	**Domain Name System**
DSCP	**Differentiated Services Code Point**
EF	**Expedited Forwarding**
ESP	**Encapsulation Security Payload**
FEC	**Forward Error Correction**
FTP	**File Transfer Protocol**
GNS3	**Graphical Network Simulator-3**
HTTP	**Hypertext Transfer Protocol**
HTTPS	**Hypertext Transfer Protocol Secure**
IETF	**Internet Engineering Task Force**
IAX	**Inter-Asterisk Exchange Protocol**
IntServ	**Integrated Services**
IMAP	**Internet Message Access Protocol**
IP	**Internet Protocol**
IP-PBX	**Private Automatic Branch Exchange**
IPsec	**IP Security**
IP TV	**IP Television**
ISAKMP	**Internet Security Association and Key Management Protocol**
LDP	**Label Distribution Protocol**

LER	**Label Edge Router**
LLDP	**Link Layer Discovery Protocol**
LSR	**Label Switch Router**
LSP	**Label Switched Path**
MGCP	**Media Gateway Control Protocol**
MPLS	**Multiprotocol Label Switching**
OSI	**Open Systems Interconnection**
PABX	**IP Private Branch Exchange**
PBX	**Private Branche Exchange**
PC	**Personal Computer**
PHB	**Per-Hop Behavior**
POP3	**Post Office Protocol 3**
PSTN	**Public Switched Telephone Network**
RAS	**Registration Admission Status**
RSVP	**Resource Reservation Protocol**
RSVP-TE	**Resource Reservation Protocol for Traffic Engineering**
RTC	**Réseau Téléphonique Commuté**
RTCP	**Real-time Transport Control Protocol**
RTP	**Real-time Transport Protocol**
RTT	**Round Trip Time**
SCCP	**Skinny Client Control Protocol**
SIP	**Session Initiation Protocol**
SIP-URI	**Session Initiation Protocol- Uniform Resource Identifiers**
SMTP	**Simple Mail Transfer Protocol**
SRTP	**Secure Real-Time Transport Protocol**
TCP	**Transmission Control Protocol**
ToIP	**Telephony over Internet Protocol**
ToS	**Type of Service**
TTL	**Time To Live**
UA	**Universal Alcatel**
UDP	**User Datagram Protocol**
UNISTIM	**Unified Networks IP Stimulus**

VLAN	**Virtual Local Area Network**
VoD	**Video on Demand**
VOIP	**Voice over IP**
VPN	**Virtual private network**

Introduction générale

L'une des choses les plus importantes qui ont contribué à façonner le monde moderne dans lequel nous vivons aujourd'hui est la capacité de communiquer sur de longues distances et nous avons pu le faire à l'aide de l'invention de la téléphonie en utilisant le mécanisme de réseaux commutés (grâce à l'établissement d'une liaison électronique de bout en bout entre l'expéditeur et le récepteur) mais, cette solution est devenue très gourmande en ressources, elle pose d'énormes problèmes de maintenance, ainsi que le cout des appels téléphoniques de distances considérablement longues.

Evidemment à l'aide de l'évolution de la technologie qui nous a donné l'internet, on a obtenu la capacité d'envoyer différents types d'informations en utilisant les protocoles de communication par paquets, et cela nous a permet de rendre les communications plus abordables pour tous utilisateurs à cause de la multiplication des équipementiers d'interconnexions.

De ce fait, de nombreux acteurs de la téléphonie IP ont émergé avec des offres très intéressantes par rapport aux téléphones fixes traditionnels en matière de prix. Mais cette solution présentait l'inconvénient de réduire la qualité de la voix transmise dans la plupart des cas contrairement à La téléphonie traditionnelle, dont la mise en place nécessite de bien entendu des investissements importants pris en charge, mais une fois fait, il est très robuste et hautement disponible.

La raison de cette dégradation de qualité est l'infrastructure compliquée des équipements d'interconnexion de l'internet et les limitations des services dédient à assurer le transfert la voix par paquets « la technologie VOIP », qui fait l'objet de nos travaux.

Nous nous concentrons dans notre projet sur le concept de la qualité de service et son importance, ainsi que sur l'impact de l'utilisation des mécanismes pour mettre en œuvre des règles et des politiques visant à améliorer et à garantir une bonne qualité de voix sur les solutions téléphonie IP.

Et dans ce cadre on a choisi de repartitionner le contenu de notre mémoire en quatre parties pour le mettre en bon structure comme suite :

Présentation de l'organisme d'accueil

On a dédié cette partie pour présenter l'entreprise qui nous a prenez en charge ainsi que pour bien définir les activités qu'on a eu la chance de voir en pratique.

Chapitre 1 : La voix sur IP

Dans ce chapitre nous allons parler de la VoIP, la définition de ses concepts de base, présenter les protocoles utilisés, ainsi qu'une description approfondie du protocole SIP avec lequel nous travaillerons pour réaliser notre solution IPBX.

Chapitre 2 : La qualité de service

Ce chapitre est dédié aux aspects QoS dans les réseaux IP, nous détaillerons ses différents mécanismes et services (IntServ, DiffServ...) ainsi que les moyens de gestion de la QoS.

Chapitre 3 : Mise en place de la solution proposée

Ce chapitre vise à traiter la partie réelle de notre projet, après avoir réalisé une analyse comparatif entre l'utilisation des deux méthodes pour réaliser les solution de communication pour démontrer l'avantage de la VoIP, nous avons parcouru les étapes pour installer notre IPBX (Astérisk) dans un environnement GNS3, afin de pouvoir appliquer les politiques de la QoS sous les appareils interconnectés ainsi que les politiques nécessaires de sécurité plutôt que de faire une comparaison avec un (Wireshark) capturer et tirer des conclusions**.**

Présentation et de l’organisme d’accueil

1. Introduction

Afin de mettre en pratique les différentes connaissances que nous avons acquises durant notre formation en administration et sécurité des réseaux, pour réaliser notre mémoire, nous avons obtenu un accord avec la société d'installation de réseaux téléphoniques ETS AMMARENE pour la réalisation d'un stage pratique d'une durée de 5 mois dont le but principal qui est d'étudier et de mettre en œuvre les notions de la qualité de service sur les solutions VoIP.

2. Présentation de l’entreprise

Crée en 2010. L’entreprise ETS AMMARENE se situe à la commune de M’chedallah wilaya de Bouira. Elle est lancée dans les affaires en premier lieu dans l’installation de petits réseaux informatiques, puis se généralise dans les installations réseaux de télécommunications, et réseaux des infrastructures internes.

Depuis sa création, l’entreprise est en partenariat avec l’ALGERIE TELECOM pour aider à l’installation et la mise en place de plusieurs réseaux téléphoniques ADSL au niveau des espaces géographiques urbains non connectés à l’internet, ainsi que l’installation des modems routeurs chez les utilisateurs, ainsi l’installation des réseaux de communication pour différents types de contrats, que ce soit pour les organisations privées (les hôtels, les concessionnaires automobiles…) ou les contrats étatiques (APC , Daïras et Wilayas).

3. Qualité de service

L’entreprise assure la qualité d'une gamme de produits grâce au travail honorable effectué et de nombreux contrats satisfaits par la qualité du travail d'installation et de maintenance. Par la faveur de leurs services, l'entreprise a établi sa place sur le marché et elle a acquise une certaine confiance par ses clients avec ses hautes expertises dans le domaine conjugués grâce à la qualité du personnel informatique.

4. Services proposés de l’entreprise

Comme l'entreprise est centrée sur le domaine de l’informatique, les services fournis varient entre l'installation, la maintenance, la configuration et la mise en marche des

équipements informatiques et réseaux, elle se poursuit à l'apprentissage aux besoins du marché, parmi les services qu'elle offre :

5. Mise en place des moyens de télésurveillance

L'entreprise compte de nombreux clients qui doivent surveiller leurs places de business, tels que des hôtels, des magasins et des centres commerciaux, elle accomplit cette tâche en :

- Réaliser un plan de travail et des équipements nécessaires.
- Appliquer l'architecture matérielle.
- Installer et configurer les différents types de caméras.
- Sécuriser les accès aux différents équipements de la surveillance.
- Centralisations, configurations et gestions des droits des accès.

Figure i - équipement de réseaux vidéo surveillance [20].

6. Installations des interphones et systèmes d’alarmes

L’entreprise est également spécialisée dans l’installation de différents types d’interphones et de systèmes d’alarmes, avec ou sans fil, afin d’assurer une sécurité totale autour des lieux souhaités.

Dans ces types d’installations, l’entreprise se concentre principalement sur :

- Réaliser un plan du logement pour l’implantation des détecteurs.
- Préparer les éléments de l’alarme pour l’installation.
- Poser les détecteurs, la sirène et le clavier.
- Installer le boîtier central et programmer l’alarme.
- Tester l’installation.

Figure ii - Réseaux de système d'alarme [20].

7. L'installation des réseaux informatique

Ce genre d'installation dépend totalement de client ou l'entreprise qui définira clairement ces besoins. Après cette étape l'entreprise commence à l'exécution du projet avec l'installation des différents équipements et du câblage nécessaire entre eux, ainsi que tout type de configuration des switches et routeurs tout dépend de cahier de charge, aussi que l'établissement des droits des accès et les privilèges de l'administrateur, en mettant des politiques de sécurités.

Souvent l'objectif de ces installations est de trouver des moyens pour établir des solutions aux différents besoins de communications au sein d'une entreprise ou entre les différents établissements d'une même entreprise, et ici les solutions de la VoIP deviennent intéressantes pour satisfaire ses nécessités.

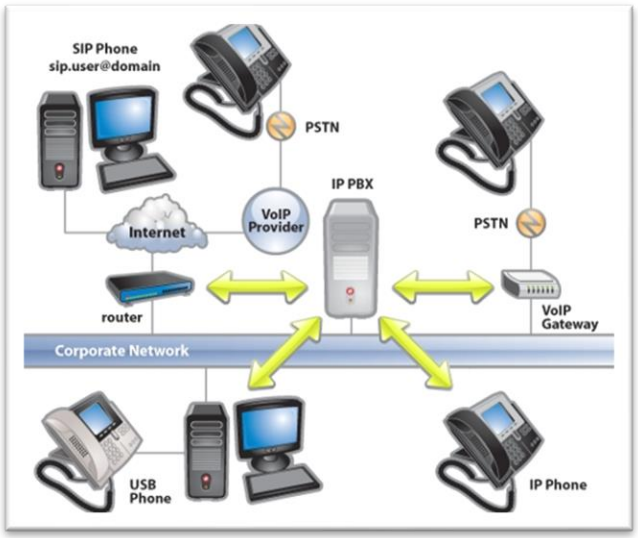

Figure iii - Réseaux IPBX [20].

8. Conclusion

L’ETS AMMARENE est une entreprise spécialisée dans l’installation des réseaux de télécommunications comme l’installation de différents types de câblage (coaxial, fibre optique, etc.), aussi la configuration des différents équipements informatiques. Le stage effectué dans cette entreprise nous a donné un grand avantage pour voir le côté pratique de notre formation ainsi que pour accumuler les informations nécessaires à réaliser notre projet.

Chapitre 1 - Généralités sur la Voix sur IP

Introduction

La VoIP (Voice over Internet Protocol), est un système permettant de transformer des signaux audio analogiques en données numériques pouvant être transmises sur Internet (connexion par paquets). En d'autres termes, il s'agit d'une solution permettant de remplacer les moyens téléphoniques traditionnels en utilisant une connexion Internet à large bande pour passer des appels téléphoniques illimités entre des postes séparés par longue distance tout en conservant l'intégrité de la voix transmis.

La VoIP utilise des protocoles et des mécanismes pour transformer la voix analogique en paquets numériques (numérisation) et vice-versa (de paquets vers la voix). Le signal numérique obtenu par la numérisation de la voix est divisé en paquets qui sont transmis aux destinataires sur un réseau IP. Les solutions VoIP doivent non seulement simplifier le travail mais aussi permettre de réaliser des économies. Les entreprises dépensent beaucoup d'argent en appels téléphoniques, mais le prix des appels de la téléphonie IP est dérisoire en comparaison. En outre, la téléphonie IP utilise considérablement moins de bande passante que la téléphonie traditionnelle.

Dans ce chapitre, nous allons parler de cette technologie, en expliquant plus en détail son fonctionnement, les différentes architectures, les codecs utilisés, les supports et les protocoles de transport, ainsi que les avantages et les inconvénients de cette technologie.

1.2 Définition

La VOIP est une Technique qui permet aux interlocuteurs de communiquer entre eux vocalement en temps réel avec le transport de conversations téléphoniques sur tous les réseaux qui acceptant le protocole TCP/IP. Contrairement aux téléphones analogiques liés à un réseau téléphonique Commuté (RTC) et à des centraux téléphoniques dédiés.

La Voix sur IP (Voice over IP), comme son nom l'indique, permet d'acheminer des paquets de données correspondant à des échantillons de voix numérisée sur un réseau de données à commutation de paquets qui utilise exclusivement le protocole IP (Internet Protocol). Le principe même de l'échantillonnage est de convertir les signaux vocaux en signaux digitaux,

puis les transmettre via le réseau Internet. Ces paquets doivent être acheminés dans le bon ordre et dans un délai raisonnable pour que la voix soit correctement reproduite.

1.3 Fonctionnement de la VoIP

Les signaux vocaux sont découpés en petites unités appelées « paquets » et sont envoyés vers le destinataire à travers le réseau quel que soit le chemin. Pour arriver à la destination, chaque paquet est numéroté et reçoit l'adresse du destinataire. Les paquets suivent alors leur propre chemin en fonction de l'encombrement du réseau Internet. Dans le cas où une ligne ou un circuit tombe en panne, les paquets déjà émis changent automatiquement de route pour arriver à leur point de destination. Une fois les paquets arrivés, ils sont remis dans leur ordre initial d'émission. 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 le réseau Internet les signaux vocaux transmis par paquet ne sont plus : « spécifiques – voix », mais ils 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 IP de l'expéditeur et du destinataire, ils seront acheminés sur le réseau par des routeurs avec des chemins différents afin d'atteindre sa 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.

1.4 Architectures de la VoIP

Il y a trois architectures de la téléphonie sur IP permettant de faire une conversation vocale sur un réseau IP :

1.4.1 Architecture hybride

Cette architecture basée sur l'installation d'un PABX avec une carte IP ajoutée. Un PABX est un PBX (Private Branche eXchange) autocommutateur téléphonique privé basé sur

le protocole H.323 et permet de faire la téléphonie traditionnelle, il faudrait rajouter une carte IP qui accepte les appels sur IP car les PABX ne prennent pas en charge la VoIP, ou d'ajouter une passerelle IP externe qui va faire une conversation des signaux analogiques qui arrivent d'un téléphone analogique vers les signaux numériques (figure 1.1) [3].

Le PABX permet de :

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

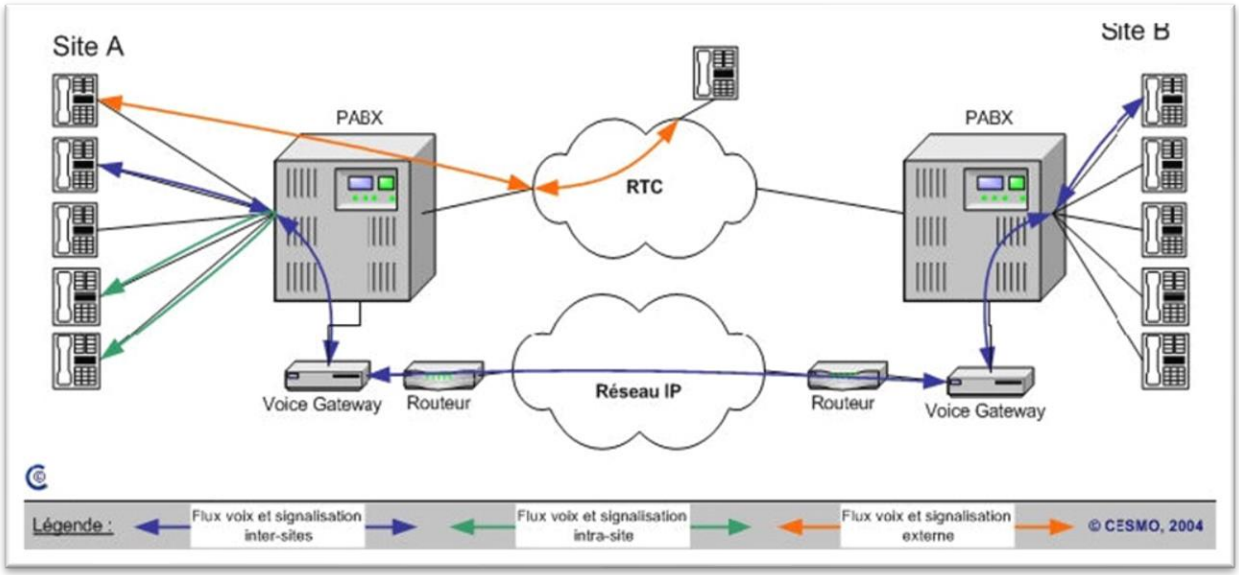

Figure 1.1 - Architecture Hybride [3].

1.4.2 Architecture Full IP

Elle constitue une migration complète de la téléphonie de l'entreprise sur IP et pour avoir ça en remplaçant les PABX et les téléphones analogique par les IPBX et les téléphones IP pour faire une communication locale ou étendue d'une entreprise en utilisant les protocoles IP. L'IPBX basé sur le protocole SIP et peut joindre les téléphones IP en mode téléphone vers téléphone sur un réseau de l'entreprise ainsi les logiciels de types soft phone (X-Lite, MicroSiP…etc.) en mode (pc vers téléphone) et (pc vers pc), tous ces équipements sont interconnectés par un IPBX qui est connecté au réseau d'entreprise. Aussi, on peut faire des communications au réseau téléphonique commuté (RTC) avec l'ajout d'une Gateway IP (figure 1.2) [3].

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 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 afin de faire passer 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) [3].

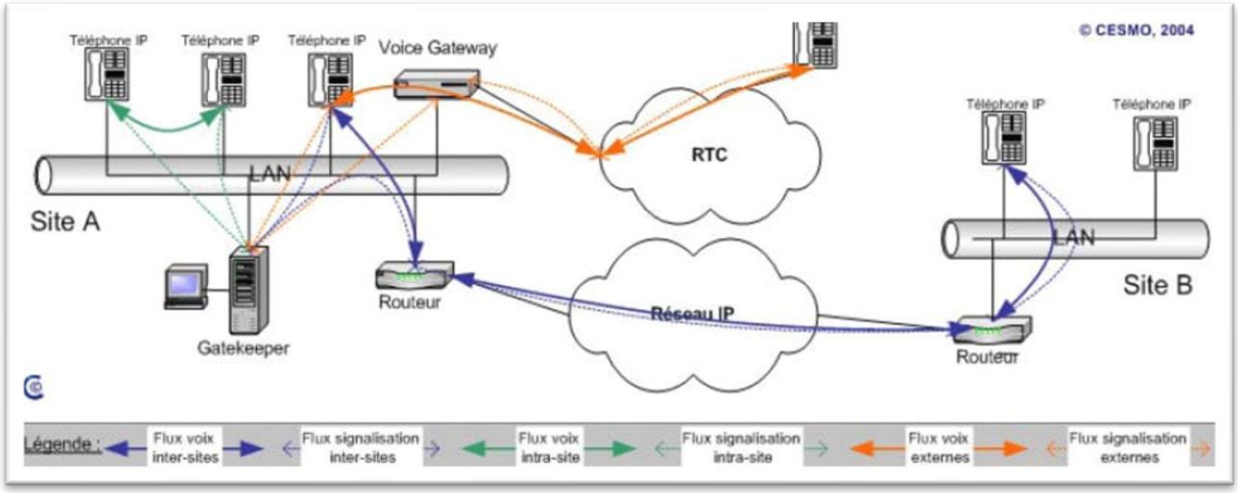

Figure 1.2 - Architecture Full IP [3].

1.4.2 Architecture Centrex IP

Dans la solution Centrex IP, le standard IP (IPBX) est hébergé et gérer par l'opérateur de téléphonie fixe. L'authentification des téléphones des utilisateurs au centrex à travers le réseau internet. Les appels téléphoniques entrants et sortants transitent sur IP (figure 1.3) [3].

La solution Centrex IP permet aux entreprises de :

- Supprimer les Standards IP (IPBX), donc évité le coût de les maintenir.
- La mobilité à la téléphonie fixe.
- Réduire le coût des appels téléphoniques.

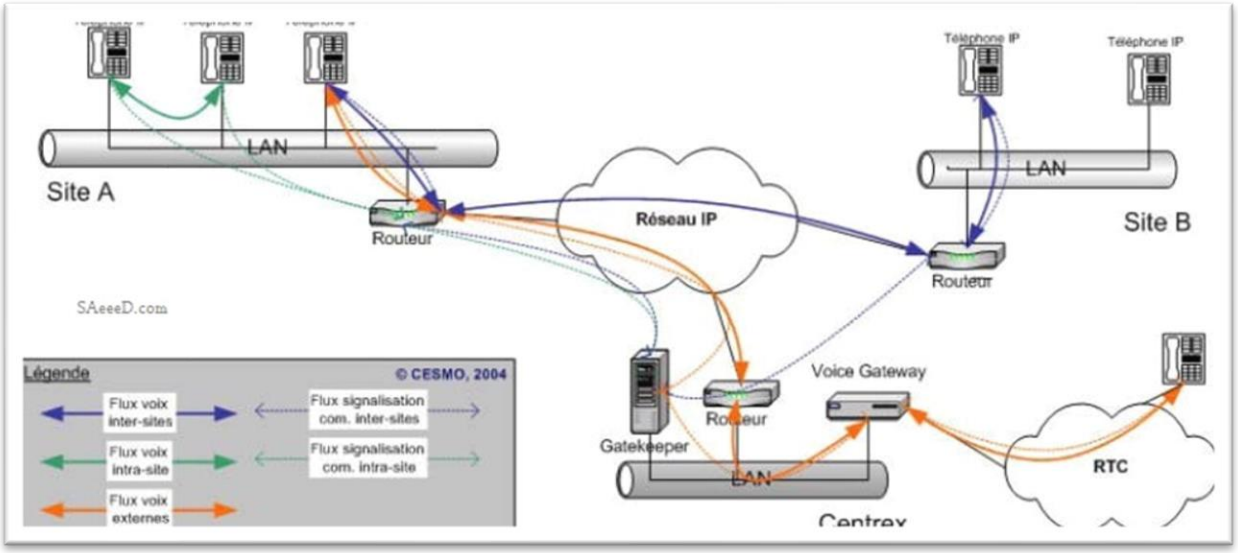

Figure 1.3- Architecture Centrex IP [3].

1.5 Les protocoles utilisé par la VoIP

La VoIP a plusieurs protocoles différents qui garantissent son fonctionnement. Certains de ces protocoles servent à la signalisation par exemple le protocole SIP, H323 ou MGCP utilisés pour l'établissement de connexions en voix sur IP, certains au transport et le contrôle de la voix comme le protocole RTCP qui est utilisé pour contrôler le transport des paquets RTP, certains servent à la configuration des postes…etc. Sans oublier les codecs qui permettent de convertir l'audio et la vidéo en données informatiques pour permettre la transmission.

Voici les principaux codecs de l'audio et la vidéo :

Type	**Codecs**
Audio	G.711, G.722, G.723, G.226
Vidéo	H.245, H.263, H.264

Tableau 1- Principaux Codecs [1].

1.5.1 Le Protocole SIP

Le protocole **SIP (Session Initiation Protocol)** est un protocole qui permet la gestion des communications en multimédia. Est un protocole de signalisation et pas de transport. Son rôle est d'ouvrir, modifier et libérer les sessions entre un ou plusieurs utilisateurs. L'ouverture

de ces sessions permet de réaliser de l'audio ou vidéoconférence, de l'enseignement à distance, les appels téléphoniques sur IP [1].
Donc c'est grâce au protocole SIP que le poste peut s'enregistrer auprès de l'IPBX et de l'indiquer à l'IPBX quand l'utilisateur appui sur les touches du clavier. Il permet aussi à l'IPBX de mettre en relation deux téléphones et de faire sonner un poste. C'est donc lui qui est au cœur de l'infrastructure de la VoIP.

Le protocole SIP se situe à la couche application du modèle OSI et utilise le port 5060 en UDP. Il est indépendant des autres protocoles des couches inférieures. SIP fonctionne de la même manière que HTTP, réutilisant de nombreux en-têtes, règles de d'encodage et codes d'état de HTTP.

La liste des principaux codes d'état :

- **1xx Provisoire** : Information (180 : Sonnerie, 100 : Essaie, 181 : Transfert).
- **2xx Réussite** : Success (200 : OK, 202 : Accepté).
- **3xx** Réorientation : Redirection (Informations sur la nouvelle localisation de l'utilisateur).
- **4xx Défaillance de la demande** : Erreur Client (404 : non-trouvé, 401 : Non-autorisé, 408 : Timeout).
- **5xx Défaillance de Serveur** : Erreur serveur (500 : Erreur interne au serveur, 503 : service indisponible).
- **6xx Échecs** : Une panne générale (600 : occupé).

Voici une liste des requêtes de base :

- **INVITE** : Permet au client de demander une nouvelle session
- **ACK** : Permet de confirme que le client a reçu une réponse définitive à une requête INVITE.
- **CANCEL** : Permet l'annulation d'un INVITE en cours.
- **BYE** : Permet de terminer une session.
- **REGISTER** : Permet de s'enregistrer auprès de l'IPBX.

L'identification de chaque ressource SIP effectué par un système d'adressage SIP qui s'appelle le SIP-URI. Il ressemble à une adresse email contient le numéro de téléphone SIP d'un Utilisateur, le nom de domaine ou l'adresse IP et le numéro du port.

Voici le format de SIP-URI :

SIP URI = sip :x@y:port → **x** = Nom d'utilisateur. **y = hôte** (Domaine ou IP), Port par défaut 5060

Par exemple sip : 1530@sip-server.hm

1.5.2 Le Protocole H.323

H.323 en anglais (Packet-based MultiMedia Communications Systems) ou systèmes de communication multimédia fonctionnant en mode paquet. C'est un regroupement des protocoles pour la communication audio et vidéo [1]. Comme indique son nom il peut être utilisé pour tous les réseaux à commutation de paquets. Aujourd'hui il est remplacé par le protocole SIP sur la plupart des solutions de téléphonie moderne.

Le protocole H.323 est spécifié pour :

1. Le traitement de la signalisation des données multimédias.
2. La négociation de codec.
3. Le transport d'informations.

Signalisation

La signalisation permet d'ouvrir et fermer une session multimédia (voix, vidéo), donc son but est le même qu'en protocole SIP (comme nous l'avons vu précédemment). Elle permet l'enregistrement et l'authentification des postes sur L'IPBX grâce au protocole RAS (Registration Admission Status), aussi l'installation et le contrôle des appels (faire sonner un poste, lancement d'un appel, etc…) grâce au protocole Q.932 [1].

Négociation de codec

La négociation de Codec permet de choisir un Codec commun entre les deux extrémités de la communication. Le codec choisi doit être supporté par tous les participants de la communication. Il existe plusieurs codec, et chacun leurs propriétés mais le protocole le plus utilisé pour la négociation est le H.245 [1].

Transport d'informations

Le transport de l'information permet de transporter la voix numérisée (encodée) par des codecs, sur le réseau IP. Il est pris en charge par le protocole RTP. Aussi en utilisant le protocole RTCP pour contrôler la qualité et demander de renégocier les codecs si la bande passante disponible change. Le protocole H.323 a évolué au cours du temps à travers de nombreuses versions. Aussi, les messages sont encodés en format binaire, donc là où le protocole SIP utilise un codage en ASCII. Grâce à la flexibilité de SIP, ce dernier tend à remplacer H.323 [1].

1.5.3 Le Protocole RTP

Le RTP en anglais (Real Time Protocol) est un protocole se plaçant au-dessus du protocole UDP au niveau de la couche transport du modèle OSI, il permet le transport de données ayant de contraintes de temps réel. Il est utilisé pour le transport des flux multimédia (audio, vidéo). En VoIP on l'utilise donc avec H.323 ou SIP pour le transport de la voix [1].

Le RTP ajoute un entête spécifique à UDP pour plusieurs raisons :

- La numérotation des paquets, pour gérer les pertes et le dé-séquencement (c'est-à-dire les paquets qui arrivent dans le mauvais ordre).
- Il ajoute une information d'horloge pour gérer la gigue (c'est-à-dire la variation de latence entre plusieurs paquets).
- Permet de spécifier le type de données transportées (audio, vidéo, image, texte, etc…). Il y a encore d'autres informations complémentaires dans l'en-tête.

1.5.4 Le Protocole RTCP

En complément du protocole RTP, on peut utiliser le RTCP pour contrôler la qualité de la transmission. Il fonctionne en UDP. Le RTCP ne transporte pas l'information finale. Il est utilisé en contrôle. A l'aide de statistiques sur la transmission (gigue, paquet perdu, délai, etc…), il est possible d'estimer la qualité de service. C'est grâce au protocole 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 communication [1].

1.5.5 Le Protocole MGCP

Le protocole MGCP (Media Gateway Control Protocol) définit par IETF et standardisé par le groupe MeGaCo [16], 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 [16].

1.5.6 Le Protocole IAX

IAX (Inter-Asterisk eXchange) est un protocole de voix sur IP issu du projet Asterisk développé par la société (Digium). L'Asterisk est un IPBX open source basé sur le système d'exploitation (Lunix). Il permet la mise en place d'un système téléphonie sur IP simple et gratuit. L'IAX est un protocole qui permet la communication entre client et serveur Asterisk, ou entre deux serveurs (par exemple lier deux serveurs Asterisk sur deux sites distants). On appelle cela un Trunk. Dans le Trunk pourront circuler plusieurs communications en simultané à travers une seule session IAX. Il n'utilise qu'un seul port UDP le 4569 pour la signalisation et des données [1].

1.6 Les Avantages de la voix sur IP

- La téléphonie sur IP rassemble tous les appareils de l'entreprise (téléphones, visioconférence, ordinateurs, etc.) sur un même réseau et donc sur un même protocole
- La diminution non seulement des coûts de communication mais également des coûts opérationnels (un seul réseau à gérer).

- Une plus grande flexibilité par l'utilisation de l'IP phone même en déplacement, par exemple (les employés peuvent s'y connecter de la maison, de leurs voitures, ou tout autre endroit où il y a un accès au réseau internet (bande passante).
- L'infrastructure réseau est mieux utilisée (par exemple : Amortissement de la ligne louée pour être utilisée et pour l'internet et pour la téléphonie).

1.7 Les inconvénients de la voix sur IP

- La qualité des liaisons téléphoniques sur un réseau IP est faible par rapport à un système de téléphonie traditionnelle (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.

1.8 Conclusion

La VoIP offre des services très intéressant pour réaliser des solutions pour la communication en termes de cout et de simplicité a mise en marche. Les solutions VoIP nécessite que certain matériel qui support la technologie (hardware IP) et des configurations des protocoles, critique pour le fonctionnement correct. Mais souvent ces genres de solution n'est pas le meilleur en termes de qualité de voix, car il y'a toujours un risque de perte des paquets, ainsi que les risques de sécurité. Mais il existe certain techniques et mécanismes pour assurer le meilleur niveau de performance qu'on peut atteindre, et grâce à ces techniques en peut rendre les solutions de la VoIP plus durable et intéressant par rapport aux anciennes moyennes de transmettre la voix

Chapitre 2 - La Qualité de Service

Introduction

Dans les premiers temps de l'internet, son seul but était d'assurer que l'information arrive à la station réceptrice, ce qui signifie que tant que nos paquets IP arrivent à destination sans aucune perte de paquets, malgré le temps élevé qu'il nécessite pour faire, nous sommes satisfaits, mais avec l'évolution, le réseau IP a rencontré d'énormes problèmes autour de l'envoi de paquets multimédias, parce que le cœur de l'architecture IP ne traite pas les paquets différemment, tous les paquets sont envoyés de la même façon et ils peuvent être abandonnés en cas de dépassement de la mémoire tampon sans tenir compte de l'importance du paquet.

Et donc les conséquences en négligeant les paquets critiques du multimédia ont abouti à une transformation multimédia en temps réel non durable pour le réseau IP. Et c'est là que les solutions de la QoS prennent place pour assurer une bonne qualité de service autour de l'envoi de données critiques avec l'optimisation des ressources du réseau pour garantir une bonne performance des applications, ainsi que d'offrir aux utilisateurs des débits et de temps de réponse différenciés par application suivant les protocoles mis en œuvre au niveau de la couche réseau.

2.2 Définition

La QoS (qualité de service) est la description ou la mesure de la performance globale d'un service, tel qu'un réseau téléphonique ou informatique ou un service de (Cloud Computing), en particulier la performance perçue par les utilisateurs du réseau. Pour mesurer quantitativement la qualité de service, plusieurs aspects connexes du service réseau sont souvent pris en compte, tels que la perte de paquets, le débit binaire, le débit, le retard de transmission, la disponibilité, la gigue, etc.

Dans le domaine des réseaux informatiques et d'autres réseaux de télécommunication à commutation de paquets, la qualité de service fait référence aux mécanismes de contrôle de la priorisation du trafic et de la réservation des ressources plutôt qu'à la qualité de service obtenue. La qualité de service est la capacité de fournir différentes priorités à différentes applications,

utilisateurs ou flux de données, ou de garantir un certain niveau de performance à un flux de données.

La qualité de service est particulièrement importante pour le transport du trafic ayant des exigences particulières. En particulier, les développeurs ont introduit la technologie de la voix sur IP pour permettre aux réseaux informatiques de devenir aussi utiles que les réseaux téléphoniques pour les conversations audio, ainsi que pour prendre en charge de nouvelles applications ayant des exigences encore plus strictes en matière de performance de réseau [5].

2.3 Les métriques de la qualité de service QoS

L'explosion de l'utilisation des applications multimédia sur les réseaux étendus en général et dans Internet en particulier ont incité les chercheurs à mener des études plus approfondies sur la QoS.

En effet, augmenter uniquement les ressources telle que la bande passante afin d'éviter la congestion n'assure pas une bonne utilisation des ressources. Cependant, les caractéristiques des flux multimédia sur Internet, présents de plus en plus, ont changé, et requièrent différents prérequis en termes de paramètres de QoS, le réseau Internet est devenu pratiquement omniprésent et utilisé pour toute communication étendues (VPN, Vidéo conférences, payement électronique, ToIP … etc.).

Les applications multimédia ont besoin des services réseaux, au-delà de ce que L'IP peut fournir. La latence ainsi que la synchronisation nécessaire pour la voix, les données et les images sont des préoccupations majeures. En effet, la téléphonie sur IP et d'autres applications multimédias telles que la vidéo conférence, la vidéo à la demande et le streaming de médias exigent des garanties de service ainsi que des exigences de délais strictes. La gestion de la QoS nous permet d'assurer un débit, un délai, une gigue, ainsi qu'un taux de perte de paquets, selon les prérequis des différentes applications.

Alors, voici les métriques de la qualité de service qu'on a :

2.3.1 La disponibilité de bande passante

Elle se rapporte à la capacité inutilisée d'un lien par unité de temps. Elle dépend de la capacité du lien mais aussi de la quantité de données présente dans le lien. Cette métrique est une variable dépendante du temps, sachant que la capacité du lien est la quantité maximale de données pouvant transiter sur ce lien par unité de temps.

2.3.2 La latence

C'est le temps total nécessaire à la transmission d'un paquet de sa source à sa destination. On parle du Round Trip Time (RTT) pour qualifier le temps nécessaire d'un aller-retour. Cette latence est liée à la congestion des liens de transmission, de la capacité de traitement des équipements réseaux ainsi qu'à la distance parcourue par le paquet pour atteindre sa destination.

Les applications sensibles à la latence sont les applications temps réel comme la transmission vidéo, la communication vocale, les applications interactives de type jeux-vidéo, etc. La maîtrise du délai de transmission est un élément essentiel pour bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho dans la téléphonie ou dans la visiophonie.

La latence dépend de nombreux facteurs :

- Le début de transmission sur chaque lien.
- Le nombre d'éléments réseaux traversés.
- Le temps de traversée de chaque élément, qui est lui-même fonction de la puissance et la charge de ce dernier.
- Le délai de propagation de l'information.
- L'influence du codec, et du nombre d'échantillons par paquet.
- L'influence de la politique de gestion de la mémoire tampon de compensation de gigue.
- L'influence du système d'exploitation utilisé, qui est un élément à prendre en compte pour minimiser les délais des applications multimédias.

2.3.3 La gigue

Connue aussi sous le nom de (jitter), elle représente la différence des délais, elle nécessite des capacités de mémoires tampons proportionnelles à son importance, et elle peut par conséquent agir sur la qualité de la voix.

La gigue résulte principalement du fait que les paquets peuvent prendre des chemins différents, de plus, la charge supportée par le réseau est instable. Donc on peut avoir des temps d'attente différents sur la même file et pour le même flux, ce qui provoque une variation dans le délai.

Le récepteur doit être capable de la compenser. Ceci est réalisable grâce à des protocoles qualifiés temps-réel. Il serait peut-être nécessaire de préciser que la gigue serait présente mais

non gênante dans le cas où les codecs n'éliminent pas le silence, sur le plan traitement bien sûr, c'est-à-dire qu'il n'est plus indispensable de mettre en place un marquage temporel.

Il est à noter que les buffers de la gigue causent un délai supplémentaire, car pour restituer le premier paquet à la réception, il nous faut attendre jusqu'à un certain temps appelé temps de libération.

2.3.4 Le taux de perte de paquets

Ce taux correspond au nombre de paquets qui n'arrivent pas correctement jusqu'à leurs destinations dû à la congestion de l'infrastructure réseau (liens de transmission ou équipements réseaux saturés).

Il peut être amélioré en agissant sur plusieurs aspects, tels que le routage intelligent connu sous le nom du TE, cette métrique influence négativement sur la QoS des applications temps réel comme le streaming vidéo ou audio, plus est-elle est élevée, plus la qualité se dégrade.

Les contraintes temps réel de délai de transit évoquées ci-dessus rendent inutile la retransmission des paquets perdus, même retransmis, un datagramme d'une application multimédia arriverait bien trop tard pour être d'une quelconque utilité dans le processus de reconstitution des données perdues. De ce fait et afin de réduire cette métrique, plusieurs modèles d'implémentation de la QoS ont été élaborés par l'IETF tels que le modèle à intégration de service (IntServ), à différentiation de service (DiffServ) et MPLS [6].

2.4 Les classes de service CoS

Tout dépend des besoins des différentes applications et services, ces paramètres sont regroupés entre eux, Ces groupes forment alors des Classes de Services (class of services : CoS).

Les requêtes de QoS des applications ou des services seront toujours affectées à une classe de service donnée. A chaque classe, correspond un ensemble de paramètre de QoS avec des objectifs quantifiés. Plusieurs modèles de CoS ont été standardisés et peuvent être utilisés indifféremment.

- **Voix :** Regroupe toutes l'application du type conversationnel (voix, Visio, conférence, ...etc.) ayant pour contrainte forte des objectifs sur le délai et la gigue. Elles sont également sensibles au taux de perte bien qu'il ne soit pas possible de retransmettre les données et requièrent des débits assez faibles.

- **Vidéo :** Regroupe toutes les applications multimédia (vidéo à la demande-VoD, la télévision sur IP –IP TV...) ayant pour contrainte forte le taux de perte et le débit et dans une moindre mesure le délai et la gigue.
- **Donnée :** Regroupe toutes les applications de transfert de données ayant pour seule contrainte un taux de perte nul et qui s'accommodent d'un délai et d'une gigue quelconque. Un débit garanti caractérise cette classe sans toutefois en faire une contrainte stricte.

- **Défaut :** Désigne toutes les applications n'exigeant aucune garantie de QoS. Bien connu sous l'anglicisme « BEST-EFFORT » c'est le mode de transport du protocole IP [7].

2.5 Les mécanismes de la qualité de service

La transmission des paquets à travers un réseau IP nécessite des performances respectables ainsi qu'une grande stabilité. Une transmission est gravement perturbée par d'éventuels retards ou coupures, il faut donc veiller à ce que le flot soit le plus continu possible et que les variations restent faibles [8].

Dans Un réseau IP Classique le service utilisé est celle de « best effort ». Mais la diversité des services à supporter entraine également une stratégie de gestion de qualité de service différente tout dépend de la situation qu'on veut gérer. IntServ est une technique qui permet un service garanti en traitant les flux des paquets en fonction de la demande de la source juste avant de démarrer l'envoi des paquets utiles et cela par la réservation des ressources. Cependant, ce mécanisme est intéressant comme une solution de privilégier certaine communication par rapport aux autres, mais ce mécanisme se heurte à un autre problème, celui du facteur d'échelle.

Avec L'IntServ chaque routeur dans le réseau doit garder l'état de chaque flux qui y transite jusqu'au moment où la liaison s'achève. Un deuxième service qui est permit sur le réseau IP est le service différencié et cela par le mécanisme DiffServ. Ce dernier permet de différencier les classes au niveau de chaque routeur. Il résout le problème du facteur d'échelle d'IntServ en définissant un nombre limité de comportement au niveau de chaque nœud. Le MPLS est aussi un mécanisme de qualité de service permettant des applications temps réel parce qu'il permet une optimisation de trafic et délai d'acheminement plus court.

2.5.1 Best Effort

Avec ce service, le réseau n'exerce pas de contrôle de flux sur les sources de données en fonction de la capacité des destinations à les accepter. Les paquets d'information sont acheminés de nœud en nœud du réseau avec des files d'attente dans chacun. Ces files ayant une capacité volontairement limitée pour préserver des temps courts de traversée du réseau, les paquets qui devraient être ajoutés à une file qui se trouve saturée sont éliminées. Il en résulte que le réseau ne peut pas garantir par lui-même un taux de transmission de données sans pertes [9].

Le service best-effort offre le transfert de paquets mais sans aucune garantie sur le délai qui dans le pire des cas peut être infini, c'est à dire le paquet peut être perdu. Les applications utilisant ce service sont des applications élastiques, c'est à dire qu'elles peuvent s'adapter aux conditions variables de bande passante disponible et aux variations du délai des paquets. Avec le service best-effort les applications n'ont pas besoin de faire une requête avant de commencer à envoyer leurs paquets et elles peuvent envoyer autant de trafic qu'elles veulent.

Bien Evidemment, il se peut que tout le trafic ne puisse pas être acheminé à cause d'un manque de capacité du réseau. L'idéal est que l'application adapte son trafic en fonction de la capacité disponible à tout moment. Ceci peut être effectué, par exemple, en utilisant TCP. Cependant, avec le service best effort, il existe aussi le risque qu'un ou plusieurs utilisateurs surchargent les routeurs et ne permettent pas que d'autres utilisateurs puissent envoyer leurs paquets. Du coup, un problème majeur dans le service actuel best-effort est le manque d'isolation de flux.

2.5.2 IntServ (Integrated Services)

Pour améliorer la QoS dans l'Internet, le groupe IntServ de l'IETF, crée en 1994, a proposé une architecture à Intégration de Services dans laquelle il est possible de garantir le taux de perte et le délai d’acheminement observés par un flux individuel, tout en contrôlant la distribution de ressources entre les flux.

Le modèle de IntServ, issu des travaux de standardisation, définit deux nouveaux services : Garanti (Guaranteed) et à charge contrôlée (Controlled Load), mieux adaptés aux nouveaux besoins des utilisateurs et des applications.

La philosophie de ce modèle repose sur un contrôle d'admission et sur la réservation de ressources sur tous les nœuds traversés et pour chaque flux. Pour effectuer cette réservation par flux, le protocole de signalisation RSVP (ReSerVation Protocol) a été développé. RSVP établit et maintient un état logiciel entre les nœuds constituants le chemin emprunté par les paquets.

Cet état logiciel est caractérisé par des messages périodiques de rafraîchissement envoyés le long du chemin pour maintenir l'état de réservation.

Au niveau technique, la réservation de ressources par flux présente des difficultés d'implémentation et des limitations de déploiement. Le déploiement à grande échelle de RSVP se heurte à la difficulté de gérer un grand nombre d'utilisateurs (scalability). Plus il y a d'utilisateurs de IntServ/RSVP, plus il y a d'états à créer et maintenir pour des destinations différentes à chaque fois. Le coût introduit par la gestion des états et l'ordonnancement par flux peut entraîner une réduction considérable de leur performance [10].

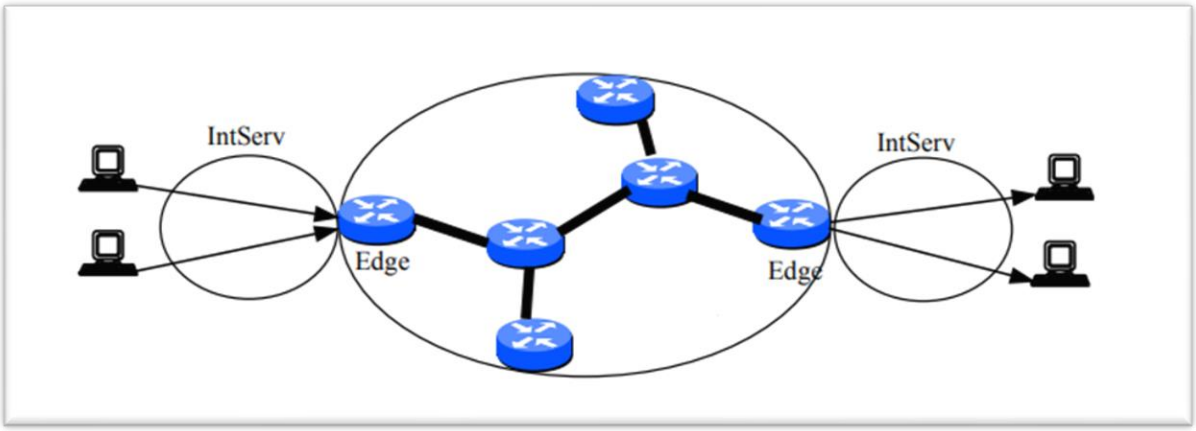

Figure 2.1 - Architecture IntServ [17].

Le modèle IntServ pour l'architecture IP QoS définit trois classes de service basées sur les exigences des applications en matière de délai (de la plus haute performance à la plus basse):

- Classe de service garanti : avec des garanties de bande passante, de délai limité et d'absence de perte.
- Classe de service à charge contrôlée : se rapprochant du service "best-effort" dans un réseau légèrement chargé, qui prévoit une forme d'accord de service de retard statistique (retard nominal) qui ne sera pas violé plus souvent que dans un réseau non chargé.
- Classe de service best-effort : similaire à celle qu'offre actuellement l'Internet, qui se subdivise en trois catégories :
    a. Rafale interactive (par exemple, Web).
    b. Interactif en masse (par exemple, FTP).
    c. Asynchrone (par exemple, le courrier électronique).

Le point principal est que les classes de service garanti et de charge contrôlée sont basées sur des exigences de service quantitatives, et toutes deux nécessitent une signalisation et un contrôle d'admission dans les nœuds du réseau. Ces services peuvent être fournis soit par flux, soit par agrégat de flux, en fonction de la concentration des flux en différents points du réseau. Bien que l'architecture IntServ ne soit pas nécessairement liée à un protocole de signalisation particulier, le protocole de réservation des ressources (RSVP) est souvent considéré comme le protocole de signalisation dans IntServ. Le service Best-effort, quant à lui, ne nécessite pas de signalisation [11].

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.

- **Réservation 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).

Les Avantages d'IntServ

Le principal avantage d'IntServ est qu'il fournit des classes de service qui correspondent étroitement aux différents types d'application décrits précédemment et à leurs exigences. Par exemple, la classe de service garantie est particulièrement bien adaptée au support des applications critiques et intolérantes. D'autre part, les applications critiques, tolérantes et

certaines applications adaptatives peuvent généralement être prises en charge efficacement par les services de charge contrôlée. Les autres applications adaptatives et élastiques sont prises en charge par la classe de service "best-effort".

IntServ fournit un ensemble très intéressant de classes de services qui, même si elles ne sont peut-être pas idéales, représentent une excellente approximation du type de services requis dans une plate-forme de télécommunication mondiale, puisqu'elle ne discrimine aucune application.

Les Inconvénients d'IntServ

Bien que (IntServ) soit un modèle de QoS simple, les garanties de service de bout en bout ne peuvent être supportées que si tous les nœuds le long de la route supportent IntServ. C'est évidemment le cas, car tout nœud de type "best-effort" le long d'une route peut traiter les paquets d'une manière telle que les accords de service de bout en bout sont violés.

Dans le cas de l'implémentation de bout en bout du modèle IntServ QoS, il est reconnu par l'industrie que le support des garanties per-flow dans le cœur de l'Internet posera de sérieux problèmes d'évolutivité.

Par conséquent, l'évolutivité est une préoccupation architecturale clé pour IntServ, puisqu'elle nécessite une signalisation de bout en bout et doit maintenir un état souple par flux à chaque routeur le long du chemin. D'autres préoccupations concernent l'autorisation et la priorisation des demandes de réservation, et ce qui se passe lorsque la signalisation n'est pas déployée de bout en bout. En raison de ces problèmes, il est généralement admis que (IntServ) est un meilleur candidat pour les réseaux d'entreprise (c'est-à-dire pour les réseaux d'accès), où les flux d'utilisateurs peuvent être gérés au niveau de l'utilisateur du bureau, que pour les grandes dorsales des fournisseurs de services.

2.5.3 Le protocole (RSVP)

Le protocole RSVP (Ressource reSerVation Protocol)) est un protocole de contrôle de réseau qui permet au destinataire des données de demander une certaine qualité de service (par exemple le délai ou la bande passante) à travers le réseau. Ce protocole de signalisation permet d'allouer dynamiquement de la bande passante : il est utilisé par les applications "temps réel" afin de réserver les ressources nécessaires au niveau des routeurs pour que la bande passante nécessaire soit disponible lors de la transmission.

Les routeurs communiquent via RSVP pour initialiser et gérer la bande passante réservée aux sessions. Ce protocole est responsable de la négociation des paramètres de connexion avec ces routeurs. Si la réservation est établie, RSVP se charge aussi du maintien de l'état des routeurs et de l'hôte afin de fournir le service demandé.

Dans RSVP, le destinataire est responsable de la réservation de ressources QoS. L'émetteur RSVP envoie ses exigences au destinataire. Après réception, le destinataire RSVP utilise le même chemin pour renvoyer un message spécifiant la QoS souhaitée et fixer la réservation des ressources correspondantes dans chaque nœud. L'émetteur RSVP envoie alors les données.

Ce protocole a pour objectif :

- Etablissement et maintien d'un chemin unique pour la transmission de données.
- Elaboration d'un système d'ordonnancement des paquets.
- Création d'un module de contrôle pour les ressources des différents nœuds du réseau [12].

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.

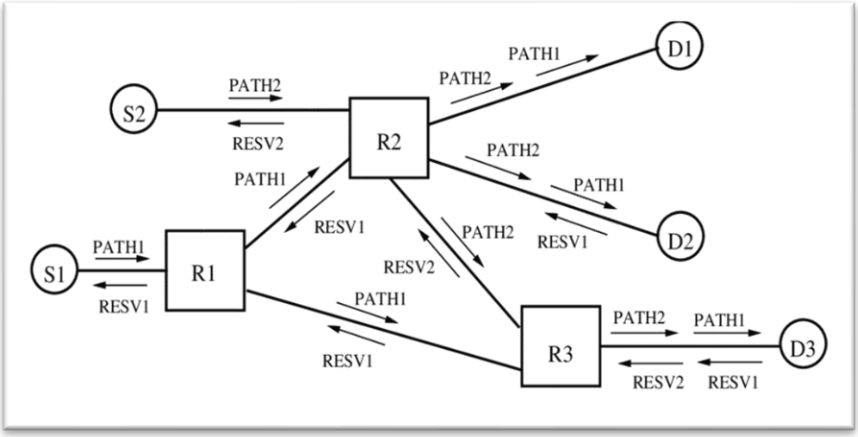

Figure 2.2 - Fonctionnement de protocole RSVP [19].

Cependant, IntServ souffre du problème de passage à l'échelle. Les ressources nécessaires pour exécuter RSVP sur les requêtes augmentent avec le nombre de réservations, résultant ainsi en de mauvaises performances de ceux-ci ; en effet, un routeur doit maintenir l'état de chaque flux (qui nécessite une réservation) qui le traverse.

2.5.4 DiffServ (Differentiated Services)

La différenciation de services consiste dans une situation de congestion à reporter les pertes de paquets sur certaines classes de trafic, pour en protéger d'autres. Il n'y a donc pas de garantie sur les flux car il n'y a pas de contrôle d'admission dynamique permettant d'éviter une congestion. Le contrôle d'admission est fait a priori par la définition d'un contrat pour chaque classe de trafic et par le dimensionnement des ressources pour pouvoir garantir ce contrat.

Les paquets DiffServ sont marqués à l'entrée du réseau et les routeurs décident en fonction de cette étiquette de la file d'attente dans laquelle les paquets vont être placés. Cette architecture convient à des réseaux pour lesquels il n'est pas raisonnable d'envisager une signalisation flux par flux. Elle ne considère donc que des agrégats de flux pour lesquels une signalisation avec réservation de ressources peut être envisagée. En fait un routeur de cœur ne conserve pas d'état pour un flux ou un agrégat donné, mais traite tous les paquets d'une classe donnée de la même manière. Les données sont identifiées grâce à un marquage dans le champ ToS (Type of Service, champ spécifique réservé dans l'en-tête IP de 8 bits), qui fixe les priorités.

La différenciation de services présente les avantages suivants :

- La signalisation est faite dans chaque paquet en attribuant une signification différente aux bits du champ type de service. Il n'est plus besoin de garder dans le routeur un contexte liant le flux de signalisation au flux de données. Cela permet aussi une agrégation naturelle des flux, ainsi pour un opérateur, les paquets qui sont marqués pour une certaine classe peuvent appartenir à plusieurs sources.
- La complexité du traitement est concentrée dans les routeurs aux frontières du réseau. Ils effectuent les opérations « complexes » de contrôle de la validité du contrat pour les différentes classes de trafic. Dans le cœur du réseau, le traitement est plus simple, ce qui autorise un relayage rapide des données [13].

Le groupe DiffServ propose donc d'abandonner le traitement du trafic sous forme de flots pour le caractériser sous forme de classes. Chaque classe est identifiée par une valeur codée dans l'en-tête IP. Cette classification doit se faire sur les routeurs de bordures (Edge router) à l'entrée du réseau.

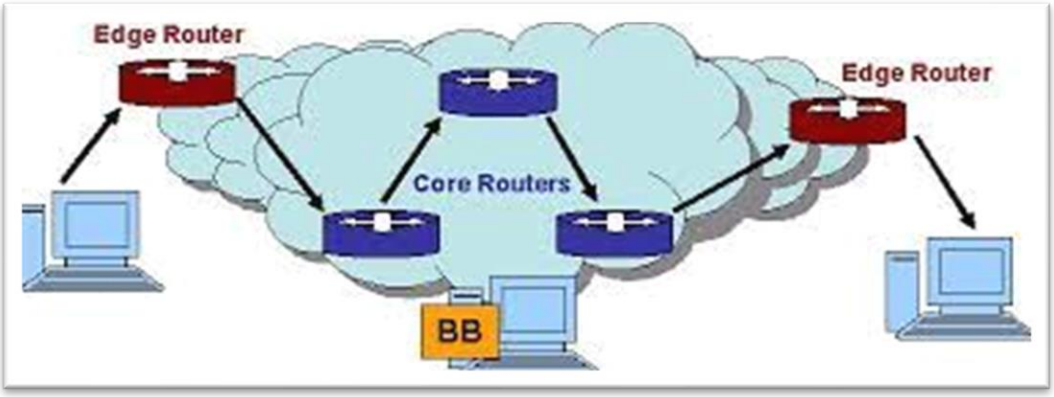

Figure 2.3 - Architecture DiffServ [17].

L'architecture des services différenciés contient 2 types d'éléments fonctionnels :

- **Les éléments de bordures** (Edge functions) : ils sont responsables de la classification des paquets et du conditionnement du trafic. En bordure du réseau, c'est à dire à l'arrivée du premier élément actif capable de traiter le champ DS (*DS-capable*), les paquets arrivants ont dans leur champ TOS (pour IPv4) ou Traffic Class Octet (pour IPv6), une certaine valeur DS. La marque qu'un paquet reçoit identifie la classe de trafic auquel il appartient. Après son marquage, le paquet est envoyé dans le réseau ou jeté.
- **Les éléments du cœur du réseau** (core functions) : ils sont responsables de l'envoi uniquement. Quand un paquet, marqué de son champ DS, arrive sur un routeur *DS-capable*, celui-ci est envoyé au prochain nœud selon ce que l'on appelle son PHB (Per Hop Behaviour) associé à la classe du paquet. Le PHB influence la façon dont les buffers du routeur et le lien sont partagés parmi les différentes classes de trafic. Une chose importante dans l'architecture DS est que les PHB routeurs se basent uniquement sur le marquage de paquet, c'est à dire la classe de trafic auquel le paquet appartient ; en aucun cas ils ne traiteront différemment des paquets de sources différentes.

L'avantage de (Diffserv) est qu'il n'y a plus nécessité de maintenir un état des sources et des destinations dans les (Core Routers), d'où une meilleure évolutivité.

Comportement du routeur :

Expedited Forwarding (EF)

- le routeur assure une émission à bas délai (file prioritaire).
- les flux utilisant ce comportement ne doivent pas expérimenter des pertes.
- un contrôle d'accès est nécessaire pour faire respecter la condition.

Assured Forwarding (AF)

- L'utilisateur choisit une des 4 classes AF pour chaque flux. (tous les paquets d'un même flux appartiennent à la même classe).
- Chaque classe obtient une quantité différente de ressources dans les routeurs du Backbone.
- 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.

Service Premium

- Le routeur d'entrée ne laisse passer que des paquets conformes (shape, discard).
- Basé sur le comportement EF.
- Ne garantir aucune perte demande une coordination entre domaines (Bandwidth Brokers).
- Son utilisation risque de demander une politique de facturation élaborée.

Service Olympique

- L'utilisateur définit pour chaque flux:
  - la classe AF à utiliser (or, argent, bronze).
  - le profil du flow (paramètres token-bucket).
- A l'entrée du réseau, une étiquette est ajoutée à chaque paquet qui reflète:
  - La classe AF pour le flux.
  - une priorité calculée par le routeur d'entrée en fonction du respect du profile accordé.

- La différentiation entre flux est atteinte grâce à une attribution différente des priorités en fonction du profil.

2.5.5 La différence entre IntServ et DiffServ

IntServ et DiffServ sont deux modèles développés pour réaliser des solutions pour implémenter la QoS sur les réseaux. Il y a une grande différence entre les deux modelés. DiffServ est un modèle de fourniture de QoS sur Internet en différenciant le trafic, tandis qu'IntServ est un modèle de fourniture de QoS dans les réseaux en créant un circuit virtuel sur Internet à l'aide de la technique de réservation de données. Le DiffServ n'exige pas que les nœuds du réseau se souviennent des informations d'état sur le flux, contrairement à IntServ, qui mémorise les informations d'état dans les routeurs. De plus, la réservation de chemins et la mémorisation des informations d'état dans un réseau occupé tel que « l'internet » seraient une tâche fastidieuse. Par conséquent, la mise en œuvre d'IntServ serait pratiquement difficile sur Internet. Pour cette raison, IntServ conviendrait aux petits réseaux privés, tandis que DiffServ convient parfaitement aux vastes réseaux comme « Internet ».

2.5.6 Le protocole MPLS

Le Protocole MPLS (Multi Protocol Label Switching) est un protocole conçu pour optimiser et accélérer le trafic réseau. Il a été développé à la fin des années 1990 par un groupe d'ingénieurs de l'entreprise (Ipsilon Networks). Le but de ce protocole est d'éviter aux routeurs de perdre constamment du temps à chercher dans les tables de routage. Le MPLS permet à la plupart des paquets de données d'être acheminés par commutation plutôt que par routage.

Cette technologie en MPLS a permis aux fournisseurs Internet de développer leurs offres sur l'ensemble du territoire, dans un temps assez court. Il est clair que le MPLS a joué un rôle important dans le développement des réseaux de télécommunications. Même si aujourd'hui, on utilise la plupart du temps des routeurs hauts performance, le MPLS est encore utilisé dans différentes situations. En effet, il permet à l'heure actuelle de contrôler les flux de données d'un réseau. De plus, cette technologie est aussi utilisée dans des réseaux privés virtuels (VPN) Dans ce cas précis, le MPLS peut servir dans le cadre de réseaux de communication virtuels qui utilisent Internet comme moyen de transport [15].

D'ailleurs, il faut savoir qu'il existe deux types de réseaux MPLS :

- **VPN** de couche 2 : dans ce premier cas de figure, le réseau virtuel privé peut être utilisé pour des connexions à distance.
- **VPN** de couche 3 : dans le second cas, le réseau virtuel va se baser sur une infrastructure IP unique.

2.5.7 Les principes et concepts de MPLS

Architecture de MPLS

L'architecture du réseau MPLS utilise des LSR (Label Switch Router) et des LER (Label Edge Router):

Label Switch Router LSR

Le LSR est un équipement de type routeur, ou commutateur qui appartient au domaine MPLS dont Les fonctions sont :

- L'échange d'informations de routage.
- L'échange des labels.
- L'acheminement des paquets.

Label Edge Router LER

LER est un LSR qui fait l'interface entre un domaine MPLS et le monde extérieur. En général, une partie de ses interfaces supportent le protocole MPLS et l'autre un protocole de type IP. Les deux types de LER qui existent sont :

- **Ingress LER** est un routeur qui gère le trafic qui entre dans un réseau MPLS.
- **Egress LER** est un routeur qui gère le trafic qui sort d'un réseau MPLS.

La figure ci-dessous représenté l'architecture du réseau MPLS :

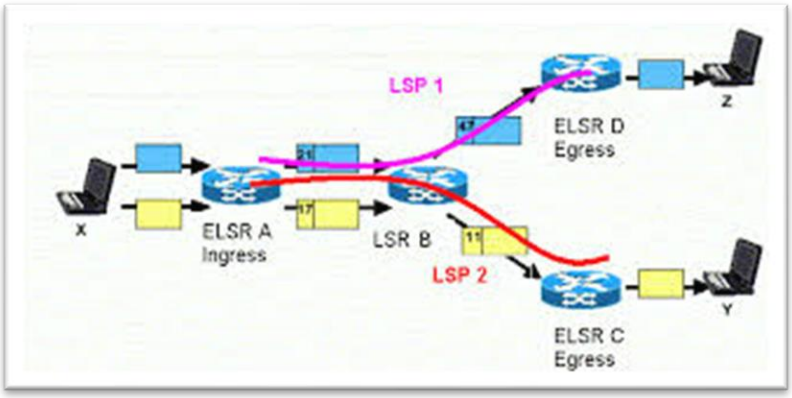

Figure 2.4 - Architecture Réseaux MPLS [14].

L'En-tête MPLS

L'entête MPLS se situe entre les entêtes des couches 2 et 3, où l'entête de la couche 2 est celle du protocole de liaison de données et celle de la couche 3 est l'entête IP. L'entête est composé de quatre champs:

- Le champ Label (20 bits).
- Le champ Exp ou CoS (3 bits) pour la classe de service (Class of Service).
- Le champ BS sur (1 bit) pour supporter un label hiérarchique (empilement de labels).
- champ TTL (Time To Live) pour limiter la durée de vie du paquet (8 bits). Ce champ TTL est le même que pour IP.

La figure suivante montre les champs qui se composent l'en-tête MPLS :

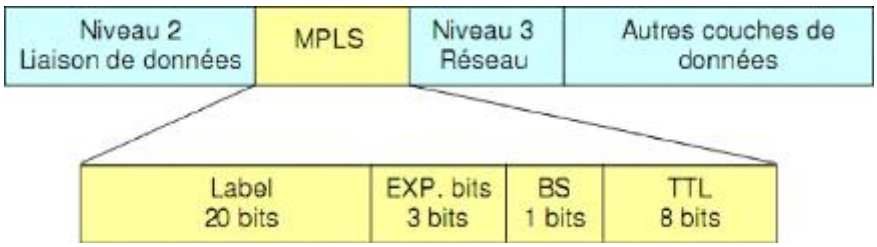

Figure 2.5 - L'en-tête MPLS [14].

Forwarding Equivalence Class (FEC)

Une FEC est la représentation d'un ensemble de paquets qui sont transmis de la même manière, qui suivent le même chemin au sein du réseau et ayant la même priorité. Le MPLS constitue les FEC selon de nombreux critères : adresse destination, adresse source, application, QoS, etc.

Label Switched Path (LSP)

Un LSP est le chemin établi au travers d'un ou plusieurs LSRs pour rejoindre plusieurs LERs au sein d'un réseau MPLS, configuré uniquement via le mécanisme des labels, pour une FEC particulière. Il peut être établi statiquement ou dynamiquement [14].

Penultimate Node

Un Penultimate Node est le routeur immédiat précédent le routeur LER de sortie pour un LSP donné au sein d'un réseau MPLS. C'est l'avant denier saut sur un LSP. Il joue un rôle particulier pour l'optimisation [14].

2.5.8 Fonctionnement de MPLS

Le fonctionnement de MPLS basé sur la détermination de caractéristiques communes à un ensemble de paquets et dont dépendra l'acheminement de ces derniers. Cette notion de caractéristiques communes est appelée le FEC.

Donc quand un paquet IP arrive à un *Ingress LER*, il sera associé à une FEC. Puis, exactement comme dans le cas d'un routage IP classique, un protocole de routage sera mis en œuvre pour découvrir un chemin jusqu'à *l'Egress LER* (Voir Figure **5**). Mais à la différence d'un routage IP classique cette opération ne se réalise qu'une seule fois. Ensuite, tous les paquets appartenant à la même FEC seront acheminés suivant le chemin LSP. Ainsi on a eu la séparation entre fonction de routage et fonction de commutation. Le routage se fait uniquement à la première étape. Ensuite tous les paquets appartenant à la même FEC subiront une commutation simple à travers ce chemin découvert.

Pour que les LSR puissent commuter correctement les paquets, l'Ingress *LER* ajoute un en-tête MPLS qui contient une étiquette appelée *Label* à ces paquets (Label Imposition *ou* Label Pushing). Ainsi, si on prend l'exemple de la figure **5**, Le LSR1 saura en consultant sa table de commutation que tout paquet entrant ayant le label L=18 appartient à la FEC tel et donc doit être commuté sur une sortie tel en lui attribuant un nouveau label L=21 (Label Swapping). Cette opération de commutation sera exécuter par tous les LSR du LSP jusqu'à aboutir à l'Egress LER qui supprimera le label (*Label Imposition* ou *Label Pushing)* et routera le paquet de nouveau dans le monde IP de façon traditionnelle, mais Comme les opérations de routage sont complexes et coûteuses, il est recommandé d'effectuer l'opération de dépilement sur le dernier LSR (Penultimate Node) du LSP (avant-dernier nœud du LSP avant le LER) pour éviter de surcharger le LER inutilement. L'acheminement des paquets dans le domaine MPLS ne se fait donc pas à base d'adresse **IP** mais de label (commutation de label) [14].

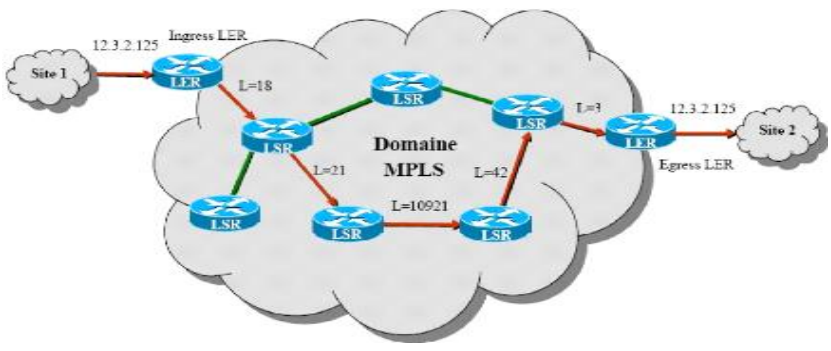

Figure 2.6 - Commutation d'étiquettes dans MPLS [14].

Il est claire qu'après la découverte de chemin (par le protocole de routage), il faut mettre en œuvre un protocole qui permet de distribuer les labels entre les LSR pour que ces derniers puissent constituer leurs tables de commutation et ainsi exécuter la commutation de label adéquate à chaque paquet entrant. Cette tâche est effectuée par *le protocole de distribution de label* " tel que LDP (Label Distribution Protocol**)** ou RSVP-TE (ReSerVation Protocol-Traffic Engineering).

Donc les trois opérations fondamentales sur les labels (Pushing, Swapping et Popping) sont tout ce qui est nécessaire pour MPLS. Le Label (Pushing/Popping) peut être le résultat d'une classification en FEC aussi complexe qu'on veut. Ainsi on aura placé toute la complexité aux extrémités du réseau MPLS alors que le cœur du réseau exécutera seulement la fonction simple de (Label Swapping) en consultant la table de commutation [14].

2.6 Conclusion

La qualité de service est un moyen indispensable pour le fonctionnement fiable des variations des communications multimédia, pour effectuer des transferts de paquets de voix et d'audio avec un délai qui assure la haute performance en temps réel, ainsi que la distribution idéale de la bande passante.

Nous avons vu dans ce chapitre les différentes variations de la qualité de service en relation avec son évolution, IntServ à aider à appliquer les mesures de la QoS mais en termes de petits réseaux. Et à cause de ces limitations, au fil du temps l'IETF s'est adapté à un modèle mieux répondu à ses besoins, l'architecture DiffServ assure une distinction des paquets par classe critique à l'utilisation de la bande passante. Il modifie l'en-tête IP pour définir les informations de QoS, et en passant par les routeurs ils peuvent alors distinguer les paquets qui ont la priorité sur les autres pour assurer les critères nécessaires, tout dépend de leurs configurations. Et lorsque MPLS est arrivé, il a vraiment contribué à généraliser la mise en œuvre de la QoS, car il s'appuie sur les classes DiffServ ainsi que sur sa capacité à fonctionner avec tous les protocoles existants.

Chapitre 3 - Mise en place de la solution proposée

Introduction

Dans ce chapitre, nous allons réaliser une analyse de besoins et faire une comparaison par rapport aux couts entre la méthode traditionnelle de réaliser le réseau pour une entreprise (concessionnaire automobile) et notre solution , nous allons principalement nous concentrer sur l'installation et la configuration de notre IPBX et sur l'application des mesures de QoS nécessaires et on assure qu'il est sécurisé, nous allons le faire en décrivant les étapes de l'installation de nos logiciels et suivre les configurations tout en faisant quelques tests pour s'assurer que nos changements sont appliqués en toute sécurité.

3.2Analyse de besoins

Dans le but d'illustrer l'avantage principal de notre solution proposée (élimination des coûts supplémentaires) pour les entreprises ainsi que la possibilité d'ajouter d'autres succursales si désiré, sans l'obligation de payée les coûts d'installation d'équipements de communication supplémentaires, nous avons fait une analyse de besoins pour l'entreprise (concessionnaire automobile) avec l'installation des différents équipements réseaux en utilisant l'architecture existante et une analyse des besoins pour notre solution proposée sous forme de tableau :

3.2.1Ancienne architecture

L'entreprise héberge son site web sur un serveur interne et protège son réseau avec des routeur-firewalls, on a supposé dans cette analyse que les prix utilisés compris les frais d'installation des différents équipements.

Equipements	Nombre d'unités	Prix unitaire	Prix totale
Ordinateur complet	6	50 000.00 DA	300 000.00 DA
Combines téléphoniques	6	10 000.00 DA	60 000.00 DA
Prises téléphoniques	6	200.00 DA	12 000.00 DA
Câblage téléphonique	Environ 400 mètres	130.00 DA	52 000.00 DA
Standard téléphonique	1	80 000.00 DA	80 000.00 DA
Switch	4	12 000.00 DA	48 000.00 DA
Router-firewall	2	30 000.00 DA	30 000.00 DA

Serveur	1	170 000.00 DA	170 000.00 DA
Câblages réseaux	Environ 400 mètres	200.00 DA	80 000.00 DA
Prises réseaux	6	300.00 DA	1 800.00 DA
		Totale	833 800.00 DA

Tableau 2- analyse de besoins avec l'ancienne installation.

3.2.2Architecture proposée

Dans l'architecture que nous avons proposée, on n'a pas besoin de différents équipements de communication téléphoniques ainsi que le câblage nécessaire pour leur installation, alors tous ces frais supplémentaires sont éliminés dans cette analyse.

Le tableau suivant montre les frais nécessaires pour implémenter la solution proposée :

Equipements	Nombre d'unités	Prix unitaire	Prix totale
Ordinateur complet	6	50 000.00 DA	300 000.00 DA
Switch	4	12 000.00 DA	48 000.00 DA
Router-firewall	2	30 000.00 DA	30 000.00 DA
Serveur	1	170 000.00 DA	170 000.00 DA
Câblages réseaux	Environ 400 mètres	200.00 DA	80 000.00 DA
Prises réseaux	6	300.00 DA	1 800.00 DA
		Totale	629 800.00 DA

Tableau 3- analyse de besoins avec la solution proposée.

3.2.3Comparaison

D'après l'analyse effectué, on trouve que l'entreprise va gagner une somme de 204 000.00 DA par rapport à l'ancienne architecture, et ça c'est intéressant si l'entreprise veut créer des nouvelles succursales, elle peut juste utiliser la méthode proposée pour réaliser la solution de communication avec juste une mise à jour de configuration pour le serveur de l'entreprise ainsi que l'installation des logiciels nécessaires qui cout vraiment moins chère que l'ancienne méthode.

3.3 Présentation de l'environnement de travail

Nous allons décrire notre environnement de travail dans cette section à la fois sur la partie matérielle (où nous avons exécuté notre simulation) et sur la partie logicielle (les logiciels utilisés).

3.4 Environnement matériel

Pour la réalisation de notre simulation, nous avons utilisé un laptop dont les caractéristiques décrites ci-dessous sont résumées dans un tableau :

Processeur	Intel (R) Core (TM) i5-5300u CPU @ 2.30 GHz 2.30 GHz
Mémoire RAM	8 Gb
Système d'exploitation	Windows 10
Type de système	Système d'exploitation 64 bits
Disque dur	HDD 500 Gb

Tableau 4- caractéristique technique.

3.5 Environnement logiciel

Nous avons utilisé beaucoup de logiciels différents dans notre projet, nous allons les décrire ici :

A Gns3 : (Graphical Network Simulator-3) est un émulateur de réseau logiciel, publié pour la première fois en 2008. Il permet la combinaison de dispositifs virtuels et réels, utilisés pour simuler des réseaux complexes. Il utilise le logiciel d'émulation Dynamics pour simuler Cisco IOS [2].

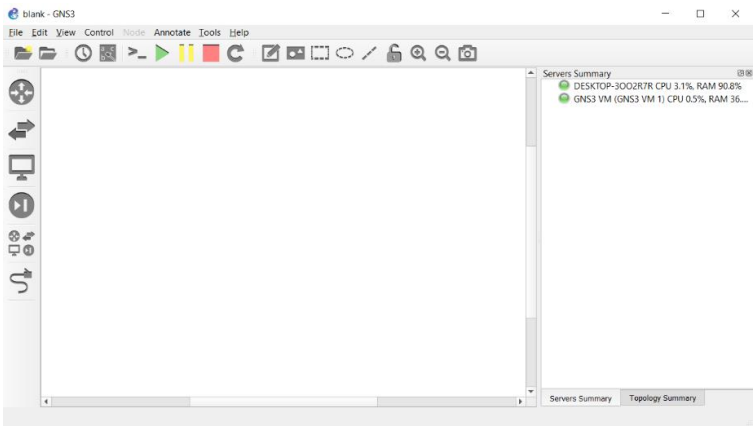

Figure 3.1 - Interface de Gns3.

B Virtuel box : Oracle VM Virtual-Box est un logiciel de virtualisation multiplateforme. Il permet aux utilisateurs d'étendre leur ordinateur existant pour exécuter simultanément plusieurs systèmes d'exploitation, dont Microsoft Windows, Mac OS X, Linux et Oracle Solaris [2].

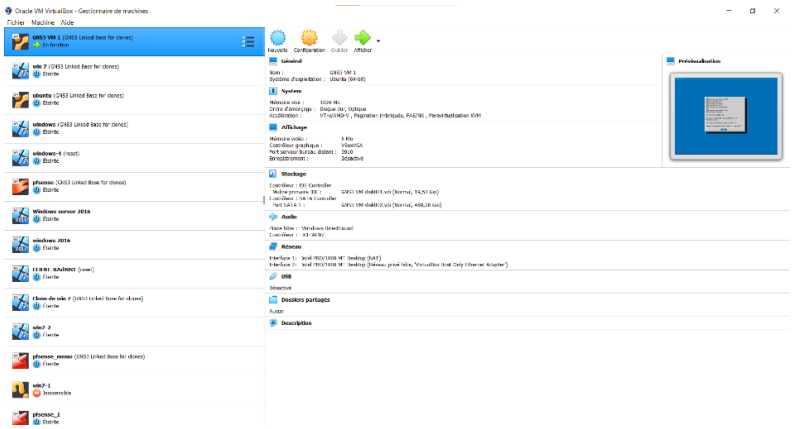

Figure 3.2 - Interface de Virtuel box.

C MicroSIP : MicroSIP est un (softphone) SIP portable basé sur la pile PJSIP disponible pour Microsoft Windows. Il facilite les appels VoIP de haute qualité (p2p ou sur des téléphones ordinaires) basés sur le protocole ouvert SIP [2].

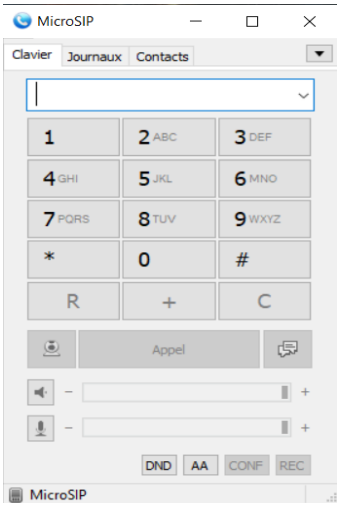

Figure 3.3- Interface de MicroSIP.

D Ubuntu : Ubuntu est une distribution Linux basée sur Debian et composée principalement de logiciels libres et open-source. Ubuntu est officiellement publiée en trois éditions : Desktop, Server, et cœur pour les appareils et robots de l'Internet des objets. Toutes les éditions peuvent fonctionner sur l'ordinateur seul, ou dans une machine virtuelle [2].

E Pfsense : PfSense est une distribution logicielle de pare-feu/routeur basée sur FreeBSD. Les logiciels open source (PfSense Community Edition) et (PfSense) Plus sont installés sur un ordinateur physique ou une machine virtuelle afin de constituer un (pare-feu/routeur) dédié à un réseau [2].

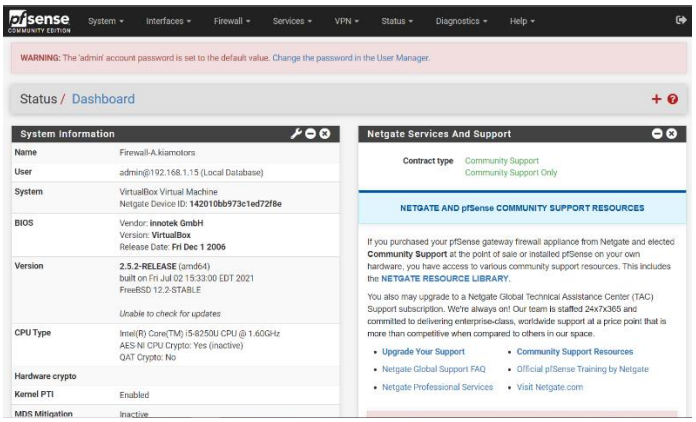

Figure 3.4 - Interface d'accueil Pfsense.

F Asterisk : Asterisk est une implémentation logicielle d'un autocommutateur privé (PBX). Associé à des interfaces matérielles de téléphonie et à des applications réseau appropriées, Asterisk est utilisé pour établir et contrôler des appels téléphoniques entre des terminaux de télécommunication, tels que des postes téléphoniques classiques, des destinations sur le réseau téléphonique public commuté (RTPC) et des dispositifs ou services sur des réseaux de voix sur IP (VoIP). Son nom vient du symbole de Asterisk (*) pour un signal utilisé dans la numérotation multifréquence à double tonalité [2].

3.6 Architecture adoptée

Dans notre stage nous avons eu la chance d'assister à l'installation de réseaux de communication pour plusieurs clients, on a choisi le projet d'installation de réseau de communication pour le concessionnaire automobile situé à BOUIRA qui est réalisé avec un PBX pour tester l'efficacité de notre solution VoIP en appliquant les mesures nécessaires de la qualité de service sur ses zones et différentes sections avec notre simulation.

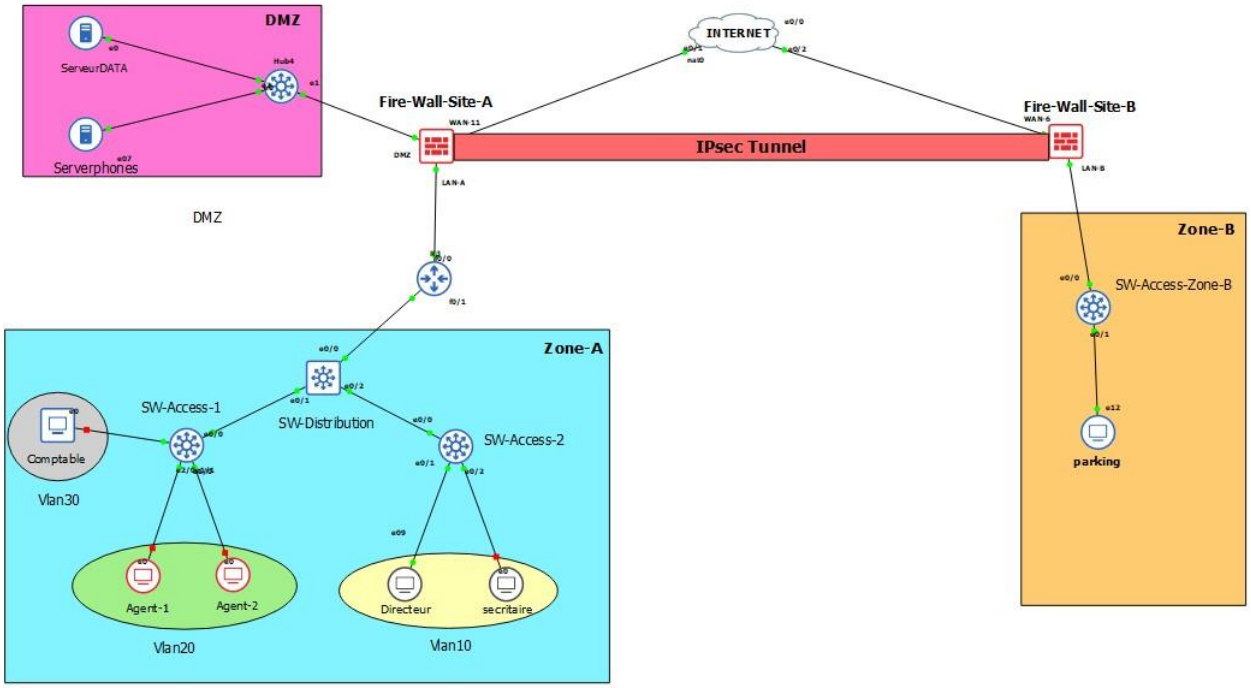

Figure 3.5 - Architecture adoptée.

3.7 Tableau d'adressage

Dans ce tableau, nous avons présenté les tableaux d'adressage des équipements de chaque zone :

	Zones	Interfaces	Adresses
Firewall-A	Wan	em0	1.1.1.2/8
	DMZ	Em1	10.10.10.254/24
	Lan-A	Em2	192.168.1.254/24
Router-A	Lan-A	F0/0	192.168.1.253/24
	Zone-A	F0/1.10	192.168.10.254/24
		F0/1.20	192.168.20.254/24
		F0/1.30	192.168.30.254/24
SW-Access-1	Vlan-10	E0/1	DHCP
	Vlan-20	E1/0	DHCP

	Vlan-30	E2/0	DHCP
SW-Access-2	Vlan-10	E0/2	DHCP
	Vlan-20	E1/1	DHCP
	Vlan-30	E2/1	DHCP
Servers	Server Phone	E07	10.10.10.15
	Server Data	E0	10.10.10.60

Tableau 5- Adressage site A.

	Zones	**Interfaces**	**Adresses**
Firewall-B	Wan	em0	2.2.2.1/8
	Lan-A	Em1	192.168.50.254/24
SW-B	-	E0/1	DHCP
	-	E1/0	DHCP

Tableau 6- Adressage site B.

3.8 Configuration des équipements de l'architecture

Configuration des switches de la zone-A

Dans la zone A, on a 3 commutateurs (Switches) pour lesquels nous avons créé les Vlans nécessaires pour notre entreprise :

- Vlan 10 : pour le secrétaire et le directeur.
- Vlan 20 : pour le service de commerce.
- Vlan 30 : pour le service de finance.

Nous avons également activé le mode (trunk Dot1q) sur les interfaces entre les commutateurs (Switches) pour pouvoir faire passer le trafic de plusieurs vlan sur le même lien,

ainsi que le (DHCP Snooping) qui n'accepte que les adresses distribuées automatiquement et envoyées par l'interface choisie (Trusted Port) ou le port de confiance.

Configuration du router de la zone-A

Après avoir configuré la configuration de base de notre routeur, nous avons choisi d'utiliser le routage par défaut pour accéder aux réseaux externes (internet), et pour activer la communication entre les Vlans, on a configuré le routage inter-vlans ainsi que la distribution automatique d'adresses IP (DHCP).

3.9 Machines virtuelles utilisées

Comme il s'agit d'un lieu de travail simulé que nous avons réalisé avec le logiciel GNS3, nous avons installé différentes machines pour qu'elles représentent le matériel réel, voici donc les machines qu'on a utilisées :

- **Windows 7 :** nous avons installé le système d'exploitation Windows 7 sur certaines de nos machines simulées pour représenter les postes de travailles des différents secteurs de notre entreprise.

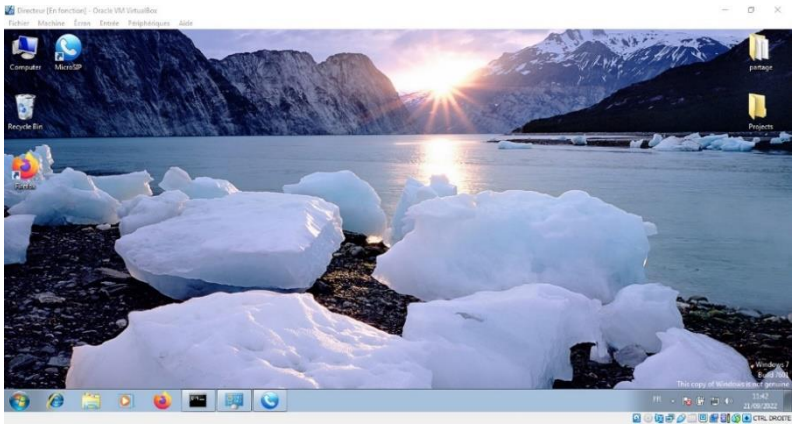

Figure 3.6 - Machine virtuel Windows 7 (Directeur).

- **Ubuntu :** pour représenter le serveur, nous avons choisi de travailler avec le système d'exploitation Ubuntu (distribution Linux) pour ses caractéristiques et fonctionnalités, et sa simplicité pour installer notre application Asterisk pour jouer le rôle de notre PBX de VoIP.

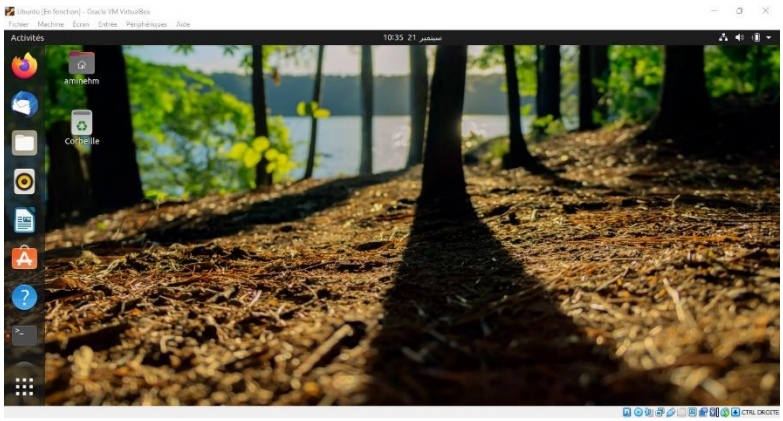

Figure 3.7 - Machine virtuel Ubuntu.

3.10 Configuration Asterisk

La première chose à faire est d'installer l'application Asterisk sur notre machine Ubuntu virtuel en exécutant cette commande :

```
aminehm@aminehm-VirtualBox:~$ sudo apt-get install asterisk
```

Figure 3.8 - Installation Asterisk.

Après avoir terminé l'installation d'Asterisk, pour assurer qu'il est bien installé dans notre unité, nous exécutons la commande qui nous dit quelle version nous avons installée et confirme son installation.

```
aminehm@aminehm-VirtualBox:~$ sudo asterisk -rvvv
Asterisk 16.2.1~dfsg-2ubuntu1, Copyright (C) 1999 - 2018, Digium, Inc. and other
s.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for detail
s.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 16.2.1~dfsg-2ubuntu1 currently running on aminehm-VirtualB
ox (pid = 795)
aminehm-VirtualBox*CLI>
```

Figure 3.9 - Accès au console Asterisk.

Après avoir installé Asterisk, pour pouvoir l'utiliser comme PBX de VoIP, nous devons configurer les bons fichiers qui contiennent les informations critiques pour pouvoir passer des appels entre les pairs configurés, pour ce faire, nous devons configurer les fichiers (extensions.conf) et (sip.conf) en ajoutant nos utilisateurs et les informations des contacts, ces dernières sont situées dans le répertoire (/etc/asterisk/).

Le fichier SIP

Pour configurer notre fichier (sip.conf) nous devons configurer le bloc général avec les configurations illustrées dans la figure 3.10, nous utilisons la ligne (encryption = yes) pour pouvoir utiliser le protocole de cryptage SRTP, afin de maximiser notre sécurité contre les menaces de piratage.

Pour les utilisateurs nous ajoutons des blocs avec (Type= friend), et la partie essentielle de ces configurations est la configuration (Secret) qui est le mot de passe utilisé par le client pour accéder à son compte, et dans la ligne (Callerid) nous trouvons le nom et le numéro dédié pour atteindre notre utilisateur.

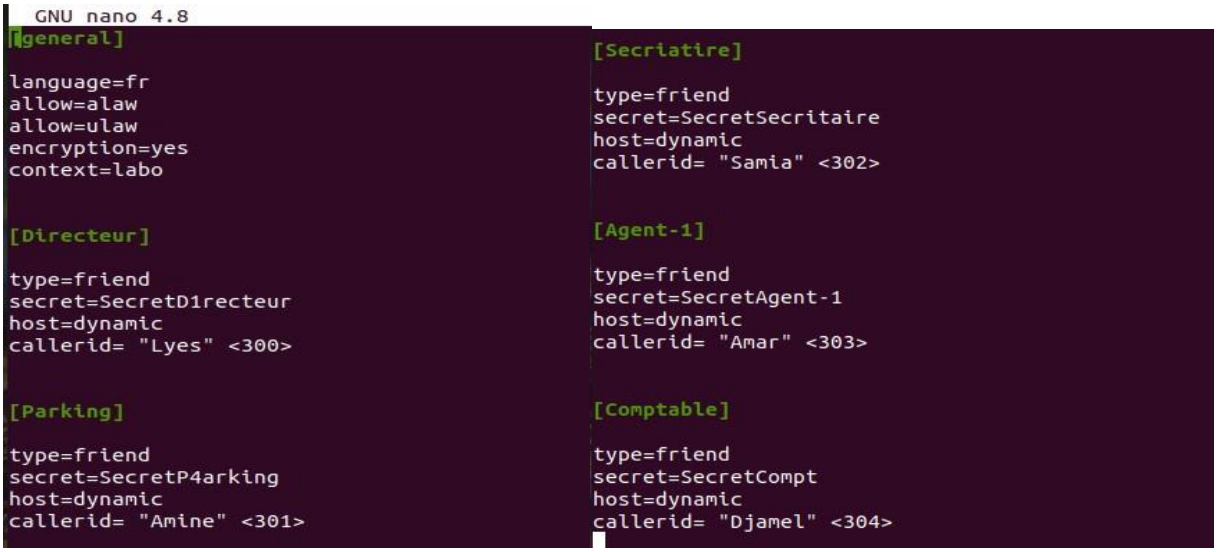

Figure 3.10 - Configuration de fichier Sip.conf.

Le fichier extensions

Le fichier (extensions.conf) est l'un des fichiers de configuration les plus importants du PBX Asterisk, il contient le (Dialplan) qui est Le plan d'appel, ou "le cœur du système Asterisk", définit la façon dont le PBX Asterisk va gérer les appels entrants et sortants, il contient également tous les numéros d'extension. Le plan d'appel est divisé en sections appelées contextes. Chaque contexte est composé de plus d'une extension. L'extension est le numéro de téléphone. Avec l'aide des contextes, nous pouvons organiser notre plan d'appel.

Dans notre configuration, nous nous sommes concentrés sur le fait de pouvoir passer l'appel en toute sécurité et d'en faire une configuration simple, c'est pourquoi, nous avons spécifié trois actions pour chaque utilisateur :

- Dial : pour faire sonner le l'utilisateur destinataire.

- Answer : pour faire l'action de rependre aux appels entrants.
- Hangup : pour faire l'action de couper l'appelle.

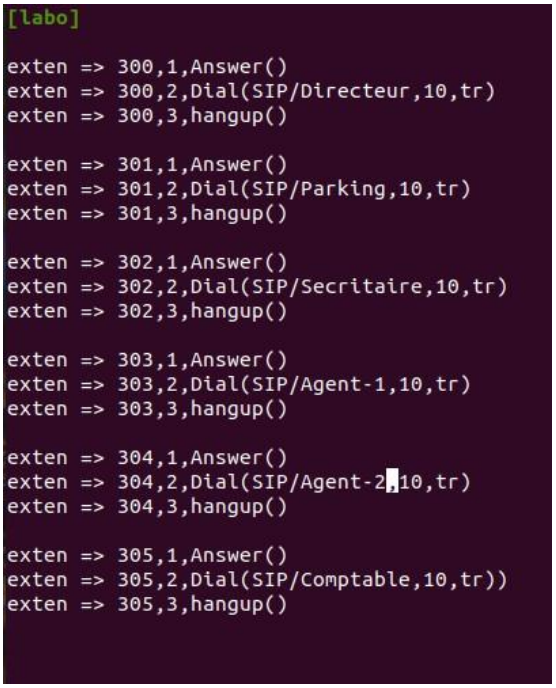

Figure 3.11 - Configuration de fichier extesion.conf.

Après avoir installé l'application asterisk et configuré le nécessaire, nous avons créé des comptes sur notre softphone MicroSIP sur les différentes machines virtuelles Windows 7 en spécifiant l'adresse IP du serveur asterisk (Ubuntu), Et remplir les champs avec les informations du client.

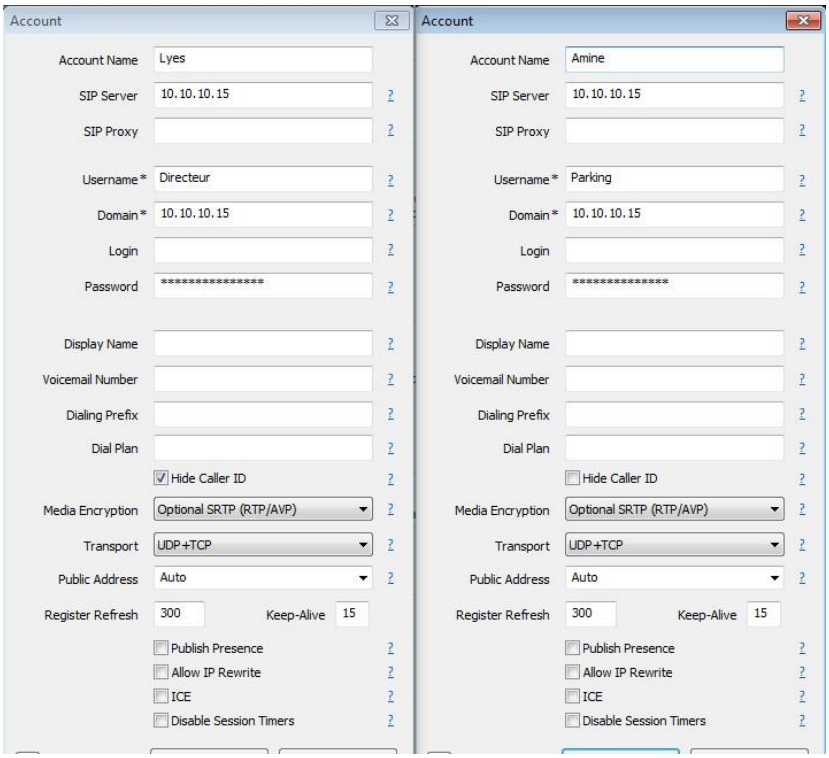

Figure 3.12 - Configuration de fichier extesion.conf.

Lors de la configuration du compte, nous nous sommes assurés de changer le paramètre de cryptage des médias par le protocole SRTP et de saisir le mot de passe correct défini dans le fichier sip.conf afin qu'il puisse se connecter au serveur sans problème.

Après avoir fait toutes ces étapes, nous pouvons voir que les clients des différentes machines virtuelles (Windows 7) sont bien connectés à notre serveur asterisk en exécutant la commande illustrée dans la figure ci-dessous après avoir exécuté la commande pour accéder à l'interface de commande Asterisk.

```
aminehm-VirtualBox*CLI> sip show peers
```

Figure 3.13 - La commande pour voire les utilisateurs connectés.

Après l'exécution de la commande, il apparaît que nos clients sont bien connectés avec leurs propres adresses IP et ports de communication.

Nous avons choisi de lancer les 2 utilisateurs "Directeur" et "Parking" pour tester la connectivité.

```
Directeur/Directeur      192.168.11.10                    D  Auto (Yes) No             49155    Unmonitored
Parking/Parking          192.168.50.12                    D  Auto (No)  No             52113    Unmonitored
```

Figure 3.14 - Les utilisateurs connectés aux serveurs.

Après s'être assuré que tout était connecté, nous avons testé un appel entre les utilisateurs, et bien sûr il a passé après avoir analysé la capture Wireshark nous pouvons voir que tous les paquets échangés entre les clients utilisent bien le cryptage SRTP.

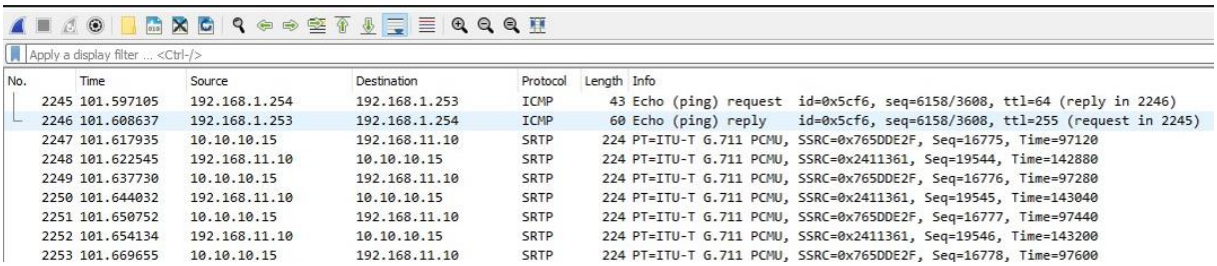

Figure 3.15 - Capture Wireshark de l'appelle réalisée.

3.11 Configuration de Pfsense

IPSec

Pour bien sécuriser les sites séparés de notre entreprise, nous avons dû configurer notre firewall Pfsense pour avoir un tunnel sécurisé entre les deux sites, nous avons donc choisi l'option IPSec pour le faire, et pour créer un tunnel IPSec sur nos deux firewalls Pfsense, nous devons configurer deux phases.

Phase une

Les étapes importantes de la phase 1 ou de la création de notre tunnel IPSec sont de spécifier la version de la clé d'échange, le protocole internet utilisé (ipv4), l'interface de sortie et la passerelle du pare-feu de l'autre site ainsi que l'algorithme de cryptage.

Nous avons fait ces étapes pour nos deux pare-feu :

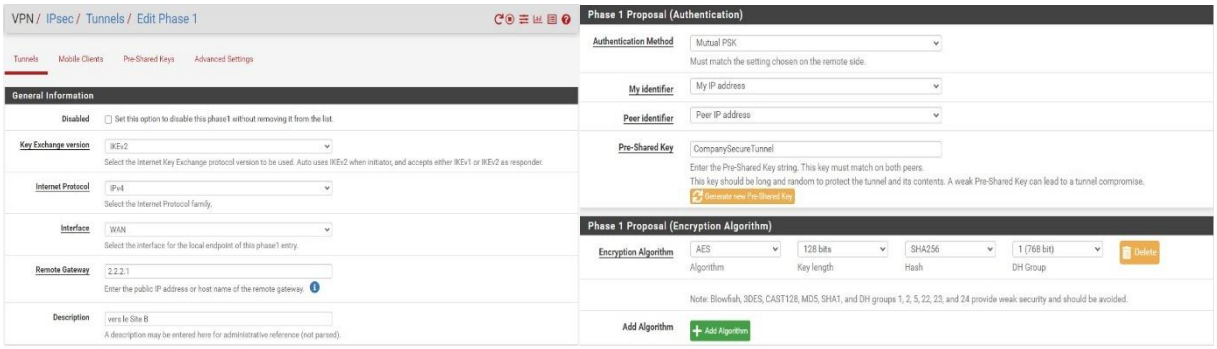

Figure 3.16 - Phase une de crier le tunnel IPSec site A.

Phase deux

Pour compléter la configuration IPSec sur notre firewall, nous devons poursuivre la phase deux de la configuration qui se concentre principalement sur la spécification de l'interface à crypter et l'adresse IP du site distant, ainsi que le protocole utilisé pour effectuer le cryptage et la taille de l'en-tête de cryptage.

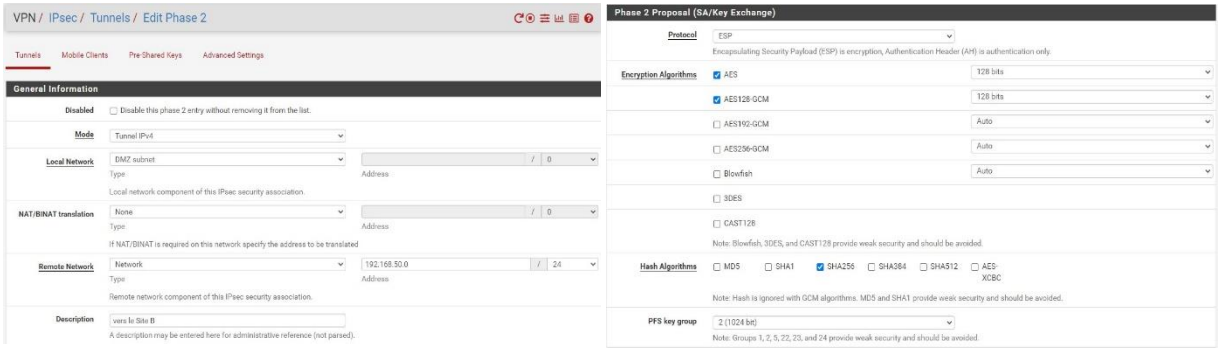

Figure 3.17 - Phase deux de crier le tunnel IPSec site A.

Après la création de notre tunnel IPSec, nous pouvons vérifier sa fonctionnalité en effectuant un appel entre les deux sites et en analyser la capture Wireshark, et nous constatons que toutes nos communications entre les deux sites sont cryptées et que chaque paquet envoyé est de type ESP.

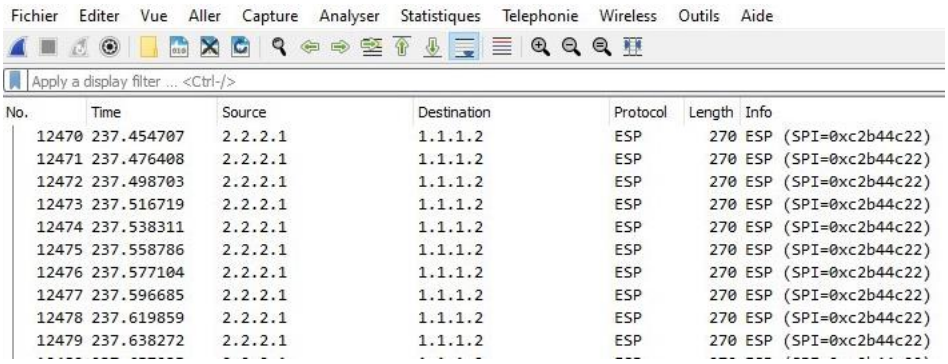

Figure 3.18 - Capture Wireshark après la réalisation de tunnel IPSec.

Configuration des Règles d'accès

Pfsense est un firewall puissant qui nous permet d'appliquer certaines règles sur les interfaces et notre trafic sortant et entrant pour pouvoir le contrôler, et nous avons configuré nos firewalls de manière à n'autoriser que ce dont notre entreprise a besoin pour communiquer et à s'assurer de le protéger contre le piratage en bloquant le trafic non désiré.

Nous l'avons fait de différentes manières selon les interfaces :

- **WAN** : pour l'interface Wan, nous n'avons autorisé que les protocoles nécessaires pour pouvoir se connecter à l'internet tels que (HTTP, HTTPs et DNS), et le protocole ISAKMP, qui est utilisé pour créer notre connexion VPN (IPSec).

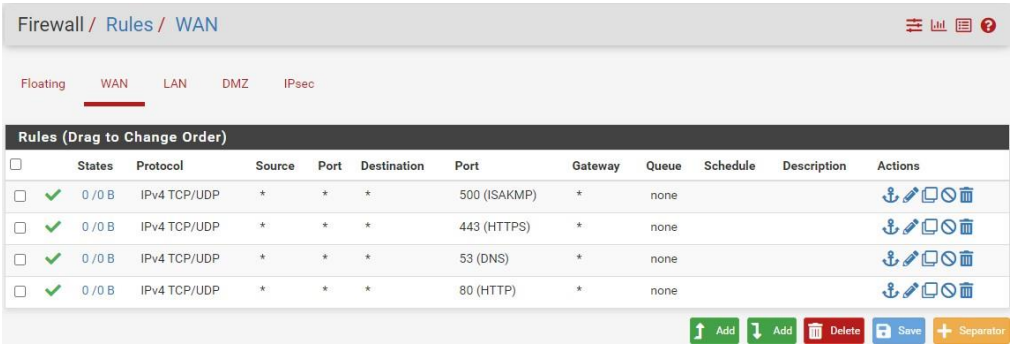

Figure 3.19 - Règles d'accès pour l'interface WAN site-A.

- **IPSec** : Pour l'interface IPSec, nous avons dû définir le protocole utilisé pour notre mécanisme de cryptage, pour lequel nous avons utilisé le protocole ESP.

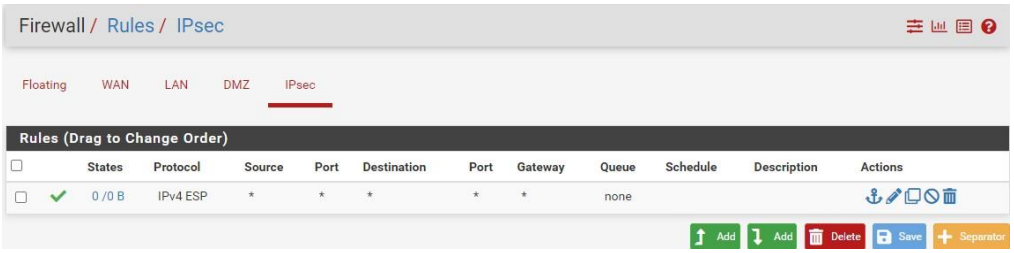

Figure 3.20 - Règles d'accès pour l'interface WAN site-B.

Après avoir configuré le pare-feu du site A, nous avons effectué les mêmes configurations sur l'autre réseau distant (site B).

3.12 Configuration de la QoS

Dans notre architecture, on a activé deux types de configuration pour appliquer les mesures de la qualité de service pour assurer le bon partage par priorité de la bande passante, la première est par rapport à l'application intégrée dans le pare-feu Pfsense (Traffic Shaper), on a appliqué ces configurations sur les deux pare-feu de notre entreprise. Et pour la deuxième c'est au niveau de routeur situé à la zone-A en utilisant des politiques de qualité de service.

Traffic Shaper

Nous avons utilisé l'assistant intégré de Pfsense (Traffic Shaper) pour appliquer les paramètres de qualité de service configurés en fonction de nos besoins en donnant la priorité aux protocoles qui sont importants pour nous et en diminuant la priorité des autres.

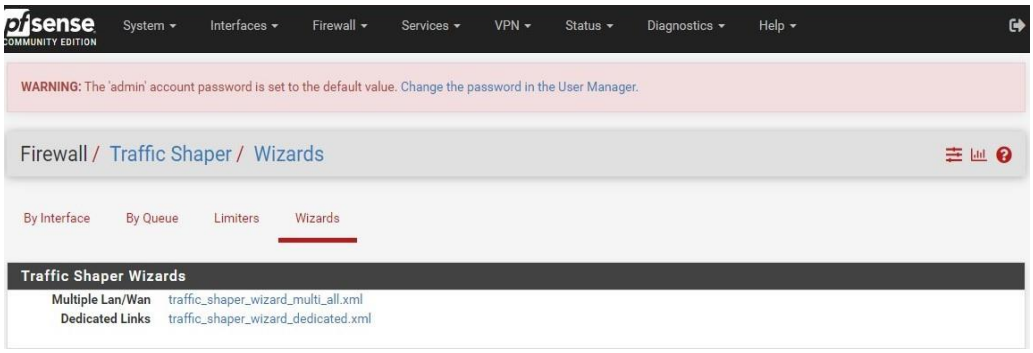

Figure 3.21 - Interface de l'application Traffic Shaper.

Le Traffic (Shaper) a besoin de certaines informations connues pour fonctionner correctement et l'une d'entre elles est la capacité de la bande passante, en faisant un test sur notre internet, nous avons constaté que notre internet a environ 3 Mégabits en (upload) et 5 Mégabits en (download).

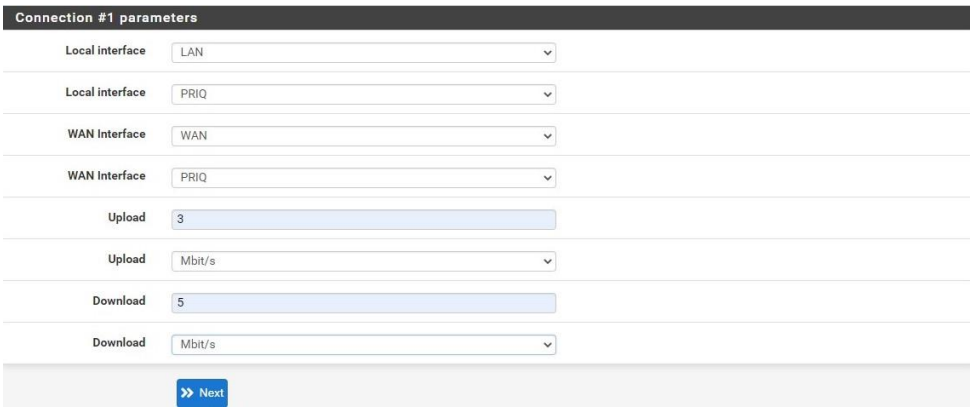

Figure 3.22 - Définition des valeurs d'upload et download.

Nous continuons les configurations en priorisant le trafic de la voix sur IP et en définissant les mêmes paramètres que ci-dessus :

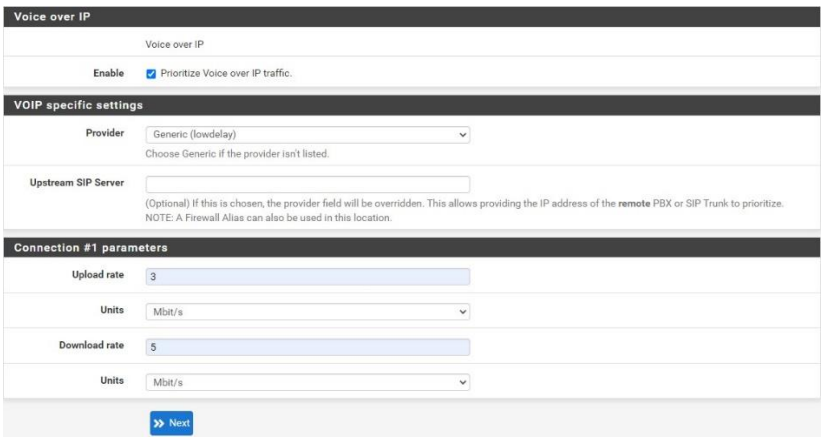

Figure 3.23 - Activation de la priorité pour la VoIP.

L'étape suivante est d'activer la priorité customisée pour d'autres protocoles de réseau, et dans cette étape nous nous assurons de donner la priorité aux protocoles multimédia, et puisque nous utilisons le (VPN IPSec) nous donnons la priorité à ce protocole également, tout en réglant les autres protocoles non importants sur "Basse priorité".

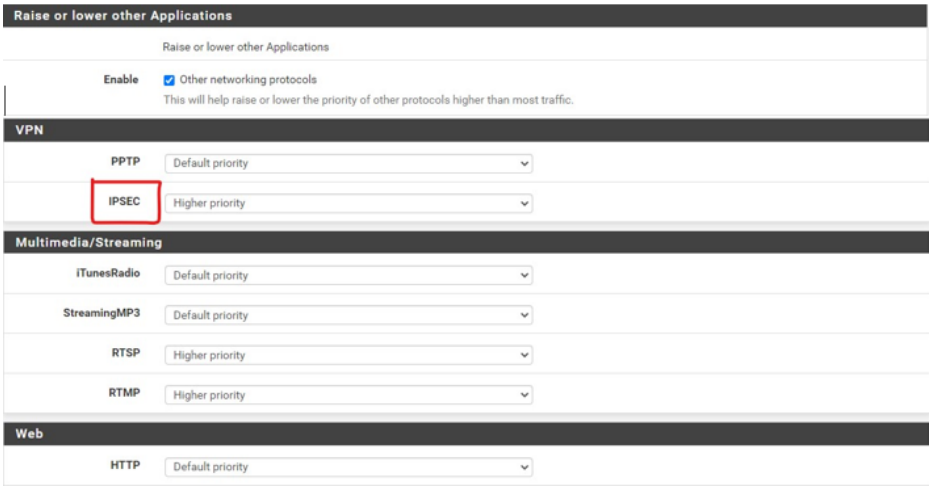

Figure 3.24 - Personnaliser la liste des priorités.

Après avoir configuré notre (Traffic Shaper), en entrant dans son interface, nous pouvons voir que les changements sont appliqués avec succès et aussi avoir une vue de notre file d'attente de trafic en direct (Figure 3.25) :

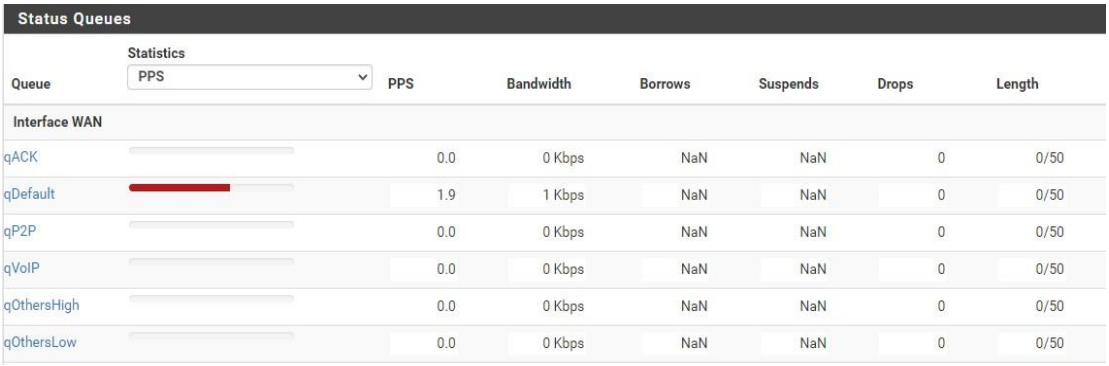

Figure 3.25 - L'état des files d'attentes.

Router-A

Dans les routeurs Cisco, il y a une qualité de service intégrée qui peut être configurée et qui s'appuie sur le modèle DiffServ en appliquant des paramètres configurés sur une interface choisie pour le trafic entrant ou sortant, et il fonctionne en créant des class-maps pour nos groupes de trafic choisis et en leur donnant un certain traitement de QoS.

Une configuration DiffServ commence par la définition des class-map, qui classent le trafic en fonction de leur protocole IP et d'autres critères. Chaque class-map peut ensuite être associée à une policy-map, qui définit comment traiter la classe de trafic. Les classes qui incluent du trafic sensible au temps peuvent être assignées à des policy-map qui donnent la priorité sur le reste du trafic.

Dans cette partie, nous allons parler des étapes pour effectuer les mesures de QoS a appliquée sur le trafic sortant sur l'interface FastEthernet 0/0 de notre routeur :

Création des class-map

Au début, il est nécessaire de créer des class-map distinguant chaque groupe de trafic par son nom afin d'appliquer ultérieurement des règles de QoS différentes.

On a crié trois class-map, la première est dédié pour le trafic de voix (Voice) en spécifiant les protocoles RTP et RTCP.

```
Router-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router-A(config)#class-map match-all Voice
Router-A(config-cmap)#match protocol rtp audio
Router-A(config-cmap)#match protocol rtcp
Router-A(config-cmap)#exit
```

Figure 3.26 - Class-map Voice.

On continue par la deuxième class-map (Email) avec les protocoles utilisé par la communication par Email (POP3, Imap, eXchange et Smtp).

```
Router-A(config)#class-map match-any Email
Router-A(config-cmap)#match protocol pop3
Router-A(config-cmap)#match protocol imap
Router-A(config-cmap)#match protocol exchange
Router-A(config-cmap)#match protocol smtp
Router-A(config-cmap)#exit
```

Figure 3.27 - Class-map Email.

La troisième class-map est réservé pour le trafic web (les protocoles http et https).

```
Router-A(config)#class-map match-all Web
Router-A(config-cmap)#match protocol http
Router-A(config-cmap)#match protocol secure-http
Router-A(config-cmap)#exit
```

Figure 3.28 - Class-map Web.

Création de policy-map

Dans cette étape nous devons configurer la politique de QoS pour chaque classe créée, nous avons choisi d'utiliser les commandes "bandwidth" pour spécifier le pourcentage de bande passante réservé pour chaque classe ainsi que la valeur DSCP qui détermine la priorité de la classe, nous avons choisi cs7 comme valeur pour indiquer la plus haute priorité "présidence 7" pour la classe Voix avec une réservation de bande passante de 50%, et DSCP cs4 avec 30% pour la classe Web.

Nous avons choisi d'activer le « Policing » sur la troisième classe (Email), avec une limitation de la bande passante fixée à 10%, tout paquet dépassant cette limite sera abandonné.

```
Router-A(config)#policy-map QoS-policy
Router-A(config-pmap)#class Voice
Router-A(config-pmap-c)#bandwidth percent 50
Router-A(config-pmap-c)#set dscp cs7
Router-A(config-pmap-c)#exit
Router-A(config-pmap)#class Web
Router-A(config-pmap-c)#Bandwidth percent 30
Router-A(config-pmap-c)#set dscp cs4
Router-A(config-pmap-c)#exit
Router-A(config-pmap)#class Email
Router-A(config-pmap-c)#police rate percent 10
Router-A(config-pmap-c-police)#exit
Router-A(config-pmap-c)#exit
```

Figure 3.29 - Policy-map QoS-policy.

Pour voir la politique créée, nous pouvons utiliser la commande show policy-map.

```
Router-A(config)#do show policy-map
  Policy Map QoS-policy
    Class Voice
      Bandwidth 50 (%) Max Threshold 64 (packets)
      set dscp cs7
    Class Web
      Bandwidth 30 (%) Max Threshold 64 (packets)
      set dscp cs4
    Class Email
     police rate percent 10
       conform-action transmit
       exceed-action drop
```

Figure 3.30 - Show policy-map.

Configuration de Service-policy

Lorsque nous avons terminé les étapes ci-dessus, nous définissons la (policy-map) crée (QoS-policy) comme notre Service-policy (la politique de QoS à utiliser) sur l'interface sortante

de notre routeur "FastEthernet0/0" et spécifions le trafic auquel notre politique sera appliquée (output).

```
Router-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router-A(config)#interface fastEthernet 0/0
Router-A(config-if)#service-policy output QoS-policy
```

Figure 3.31 - Attribution de notre policy-map sur l'interface de routeur.

Une fois que tout est configuré, nous pouvons voir la progression de la qualité de service en utilisant la commande show (policy-map) interface, qui nous permet de voir les statistiques des paquets envoyés et reçus ainsi que les paquets abandonnés en raison de la saturation de la bande passante.

```
Router-A(config-if)#do show policy-map interface  fastethernet 0/0
 FastEthernet0/0

  Service-policy output: QoS-policy

    Class-map: Voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol rtp audio
      Match: protocol rtcp
      Queueing
        Output Queue: Conversation 265
        Bandwidth 50 (%)
        Bandwidth 5000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
      QoS Set
        dscp cs7
          Packets marked 0
    Class-map: Web (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol http
      Match: protocol secure-http
      Queueing
        Output Queue: Conversation 266
        Bandwidth 25 (%)
        Bandwidth 2500 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
      QoS Set
        dscp cs4
          Packets marked 0
```

Figure 3.32 - Les statistiques des classes Web et Voice.

Dans le cas où on a utilisé le (policing) le command donne plus d'information que les classes présidentes, comme le nombre de paquets qui sont supprimé à cause de dépassement de la limite précisée.

```
Class-map: Email (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: protocol pop3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: protocol imap
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: protocol exchange
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: protocol smtp
    0 packets, 0 bytes
    5 minute rate 0 bps
  police:
      rate 10 %
      rate 1000000 bps, burst 31250 bytes
    conformed 0 packets, 0 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
  288 packets, 17872 bytes
```

Figure 3.33 - Les statistiques de la classe Email.

Conclusion

Ce dernier chapitre nous a permis d'effectué les installations et les configurations de tous les équipements permettant un bon fonctionnement de notre solution «VoIP» avec le simulateur GNS3. Nous avons fait les différentes étapes pour crée et configurer notre IPBX « Asterisk » ainsi que d'appliquer les règles de la qualité de service sur les défirent site du réseau de l'entreprise.

Conclusion générale

Dans ce projet de fin d'études, nous avons réalisé une simulation d'un réseau d'entreprise pour créer un système VoIP et renforcer sa fiabilité en mettant en œuvre des mécanismes de qualité de service et en le sécurisant par différentes méthodes, afin de montrer l'utilité de ce système en termes de coût pour les petites entreprises qui n'ont pas besoin d'un grand réseau d'infrastructure basé sur les Standard PBX comme solution couteuse pour réaliser leurs communications internes.

Notre premier objectif dans la réalisation de notre simulation était de construire le système VoIP, de le rendre opérationnel et de le mettre en production pour tester la qualité de la voix sur ses appels. Une fois la solution mise en place, nous avons défini une stratégie de qualité de service pour améliorer la qualité de la voix transmise et l'avons appliquée aux équipements d'interconnexion tout en mettant en place une politique de sécurité pour protéger notre réseau contre les attaques internes et externes.

Au bout de notre travail, nous avons conclu que l'application de mécanismes de QoS est plus que nécessaire pour améliorer la qualité de la voix sur la solution VoIP. Mais elle n'est pas suffisante pour la garantir sur les réseaux étendus comme l'Internet. Nous avons donc constaté que pour obtenir une meilleure qualité de service, il est nécessaire pour tout réseau de disposer d'équipements supportant la QoS ainsi que l'utilisation de supports de transmission avec un meilleur temps de transport comme la fibre optique.

Ce projet nous a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il nous a initiés au monde de la recherche sur les réseaux surtout en ce qui concerne la qualité de service, ainsi que les différents modes de communication, leurs applications, ainsi que les protocoles qui les gèrent. Grâce à notre modeste travail, nous avons eu l’occasion de voir beaucoup de choses de plus près et d’enrichir nos connaissances, nous avons aussi eu la chance de mettre nos capacités en valeur et de faire face aux situations les plus critiques et aux obstacles et apprendre comment procéder pour s’en sortir.

Bibliographie

- [1] https://www.networklab.fr/protocoles-de-voip-et-codecs-audio/, (consulté le 10/05/2022).
- [2] www.wikipedia.org , (consulté le 15/07/2022).
- [3] Mr BASSIROU KASSE, Dr Djiby Sow ; Etude et mise en place d'un système de communication de VoIP appliqué à un PABX IP open source 2006 Université Cheikh Anta Diop de Dakar - Master II professionnel - Système d'informations réparties, (consulté le 18/07/2022).
- https://wikimemoires.net/?post_series=voip , (consulté le 25/07/2022).
- [4] Comprendre la VoIP http://www.testeur-voip.com , (consulté le 25/07/2022).
- [5] https://en.wikipedia.org/wiki/Quality_of_service, (consulté le 25/07/2022).
- [6] Djamel Eddin HENNI, thèse doctorat : Gestion de la qualité de service des flux multimédia dans les réseaux SDN, (consulté le 25/07/2022).
- [7] Architectures des réseaux pour le contrôle de la QoS - 123dok FR https://123dok.net/document/nq7xl0oy-architectures-reseaux-controle-qos.html ,(consulté le 02/08/2022).
- [8] Karim SAFIR Thème Déploiement d'une solution VoIP avec IPv6, Gestion de la QoS Evaluation et Reconnaissance Vocale (consulté le 29/08/2022).
- https://repository.usthb.dz/bitstream/handle/123456789/2513/TH7978.pdf, (consulté les 2/08/2022).
- [9] https://fr.wikipedia.org/wiki/Best_effort_(r%C3%A9seau),(consulté le 3/08/2022).
- [10] Abed Ellatif Samhat, IntServ sur DiffServ : Etude du rapport micro-flux/agrégat https://www.researchgate.net/publication/264843528_IntServ_sur_DiffServ_Etude_du_rapport_micro-fluxagregat, (consulté le 6/09/2022).
- [11]https://tacs.eu/analyses/Internet/ip%20qos%20architectures/int-serv_architecture.htm, (consulté le 06/09/2022).
- [12]http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002/Leroy-Lhote/RSVP.htm#:~:text=Le%20protocole%20RSVP%20(Ressource%20reSerVation,passante)%20%C3%A0%20travers%20le%20r%C3%A9seau,(consulté le 08/06/2022).

- [13]https://123dok.net/article/mod%C3%A8le-diffserv-architecture-routeur-supportant-qos.zx5k61vq ,(consulté le 10/09/2022).
- [14] https://www.memoireonline.com/03/11/4293/m_Mise-en-oeuvre-dun-coeur-de-reseau-IPMPLS7.html ,(consulté le 11/08/2022).
- [15] https://www.futura-sciences.com/tech/definitions/internet-mpls-3901/ ,(consulté le 15/09/2022).
- [16] OUAKIL, Laurent et PUJOLLE, Guy. Téléphonie sur IP: SIP, H. 323, MGCP, QoS et sécurité, Asterisk, VoWiFi, offre multiplay des FAI, Skype et autres softphones, architecture IMS.. Editions Eyrolles, 2011 (consulté le 23/09/2022).
- [17] https://www.researchgate.net/figure/Architecture-IntServ-DiffServ_fig1_264843528 (consulté le 24/09/2022).
- [18]http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2003/Pamphile-Tiesset/diffserv3.htm (consulté le 24/09/2022).
- [19] https://www.semanticscholar.org/paper/Design-and-implementation-of-an-RSVP-based-quality-Barzilai-Kandlur/83e97712507744e8b988cc96c98eeffe00a32b7a (consulté le 24/09/2022).
- [20] www.google.com (consulté le 23/06/2022).