République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Faculté de Technologie

Département Génie Electrique

Mémoire pour l'obtention du diplôme de Master en Télécommunication
Spécialité : Réseaux et Télécommunication

جامعة بجاية
Tasdawit n'Bgayet
Université de Béjaïa

سوناطراك
sonatrach

Thème

Configuration et implémentation de la qualité de service de la voix sur IP (par priorisation de flux)

Cas d'étude : Réseau SONATRACH

Préparé par :

Mlle TACHOUGAFT Kahina

Mlle TAGUELMIMT Loubna

Devant le Jury composé de :

Mr	KHIREDDINE.A.	Pr.	Univ de Bejaia	Président
Mlle	ACHOUR.L.	MAA.	Univ de Bejaia	Examinatrice
Mr	BERRAH.S.	Pr.	Univ de Bejaia	Encadreur
Mr	MADDI.K.	Ingénieur	SONATRACH	Co-encadreur

Année Universitaire 2018/2019

Remerciements

Nous remercions Dieu le tout puissant de nous avoir donné la force, la volonté de donner le meilleur de nous-même et le courage de mener ce travail.

Nous remercions notre encadreur « Mr BERRAH Smail » qui a accepté de nous encadrer, pour le temps qu'il nous a consacré et ses conseils.

Un grand merci à « Mr MESSAOUDI Hicham » pour tous ses conseils ainsi que ses orientations.

Nous adressons aussi un remerciement spécial à « Mr MADDI Kamel » et « Mr HANANE Hamide » les encadreurs de stage pour leurs encouragements, documentations, patience.

Nous exprimons aussi notre gratitude et remerciements aux Président et membres de jury pour l'intérêt qu'ils ont porté à notre travail et pour l'honneur qu'ils nous font de bien vouloir le juger.

Nous avons pu aller au bout de notre recherche grâce au soutien de nos familles respectives.

Nous ne pouvons conclure sans avoir remercié tous ceux qui ont aidé de près ou de loin au succès de notre formation.

Loubna – Kahina

Dédicace

Je dédie cet humble travail

A **mes chers parents** qui ont œuvré pour ma réussite, de par leur charité, leurs soutiens, tous les sacrifices consentis, je leur dois l'expression de mes sentiments et de mon éternelle gratitude

A mes sœurs : Linda, Samia, Karima et Ayda

A **mes frères : Samir, Djillali, Saber et Salem**, ainsi que **mon beau-frère, Saïd et mes belles sœurs,** avec mes souhaits de bonheur de santé et de succès.

A **mes chers neveux : Ilan, Adam, Rayane, Yanni, Aiden et Axel.**

A **ma nièce : Eclair**

A **tous mes amis et amies** exceptionnellement : **Hicham, Loubna, Fifi** et tous ceux qui me connaissent de loin ou de près.

Kahina

Dédicace

Je dédie ce mémoire

Avec un énorme plaisir, un cœur ouvert et une immense joie, à **mes très chers et respectueux parents** qui m'ont soutenus tout en long de ma vie ainsi qu'à **mes sœurs et mes frères** et en particulier

À **ma binôme Kahina** ainsi que sa famille.

A toute **ma familles : grand-mère, oncles, tantes, cousins et cousines.**

A **mes ami(e)s et collègues** de la promo

A toute personne qui m'a aidé et encouragé de prêt ou de loin toute au long de mes études.

Que Dieu vous protège et vous garde en bonne santé.

Loubna

Table des matières

CHAPITRE 3 : ORGANISME D'ACCUEIL

CHAPITRE 4 : CONCEPTION ET CONFIGURATION DU RESEAU SONATRACH

CHAPITRE 5 : IMPLEMENTATION DE LA QUALITE DE SERVICE PAR PRIORISATION DE FLUX

CONCLUSION GENERALE

Liste des figures

Liste des tableaux

Liste des annexes

Liste des acronymes

- **VoIP** : Voice over Internet Protocol.
- **RTC** : Réseau Téléphonique Commuté.
- **RTPC** : Réseau Téléphonique Public Commuté.
- **PABX :** Private Automatic Branch eXchange.
- **L'UIT-T :** Union International Télécommunication.
- **GW** : GateWay.
- **GK** : GateKeeper.
- **BP:** Bande passante.
- **MCU** : Multipoint Control Unit.
- **MC**:Multipoint Controller.
- **MP**:Multipoint Processor.
- **U.A**:User Agent.
- **UAC** : User Agent Client.
- **UAS** : User Agent Server.
- **RNIS** : Integrated Services Digital Network.
- **PSTN**: Public SwitchedTelephone.
- **IETF**: Internet Engineering Task Force.
- **SIP:** Session Initiation Protocol.
- **DoS**: Denis of Service.
- **RTP**: Real-time Tansport Protocol.
- **RTCP**: Real-time Control Protocol.
- **TCP**: Transmission Control Protocol.
- **UDP**: User Datagram Protocol.
- **SCCP**: Skinny Call Control Protocol.
- **ICMP**: Intrenet Control Message Protocol.
- **SNMP**: Simple Network Management Protocol.
- **CNAME**: Canonical name.
- **LAN**: local Area Network.
- **WAN**: Wide Area Network.
- **CISCO**: Computer Information System Company.
- **CLI:** Commande Langage Interface.
- **IP**: Internet Protocol.
- **OSI**: Open System Interconnexion.
- **ISO**: International Standards Organization.
- **DHCP:** Dynamic Host Configuration Protocol.
- **DNS:** Domain Name System.

- **HTTP:** Hypertext Transfer Protocol.
- **WWW**: World Wide Web.
- **VLAN:** Virtual Local Area Network.
- **VTP :**Vlan Trunking Protocol.
- **QoS**: Quality of Service.
- **IntServ:** Integrated Service.
- **DiffServ**: Differentiated Services.
- **RSVP**: Resource reSerVation Protocol.
- **MPLS:** Multiprotocol Label Switching.
- **TOS**: Type of service.
- **DoS:**Denial of Service.
- **PHB**: Per-Hop Behavior.
- **DSCP:** Differentiated Services CodePoint.
- **EF**: Expedited Forwarding.
- **AF**: Assured Forwarding.
- **WRED** : Weighted Random Early Detection.
- **SONATRACH** : Société Nationale pour la Recherche, la Production, le Transport, la Transformation, et la Commercialisation des Hydrocarbures.
- **TRC :** Transport par canalisation.
- **RTI** : Région Transport Ain-Amenas.
- **RTH** : Région Transport Haoud El Hamra.
- **RTC** : Région Transport Centre Béjaia.
- **RTO** : Région Transport Ouest Arzew.
- **DRGB :** La direction régionale de Bejaia.
- **HEH** : Haoud-El-Hamra.
- **MTN :** La maintenance.
- **TMR**: Terminal MaRin de Bejaia.
- **SCADA:** Supervisory Control and Data Acquisition**.**

INTRODUCTION GENERALE

Consiste à présenter l'objet de notre travail, le contexte dans lequel il s'inscrit et son intérêt. Elle définit, également, les objectifs auxquels nous tenterons atteindre, tout en expliquant la démarche suivi.

Introduction générale

Les réseaux IP (Internet Protocol) étaient conçus à l'origine pour échanger des données simples et qui n'exigent aucune garantie de service.

Par la suite, ces réseaux ont rapidement évolué pour transporter des applications multimédia telles que la téléphonie sur IP, la vidéoconférence et d'autres applications plus exigeantes en termes de délai, bande passante et de gigue.

Cependant Les réseaux IP tels qu'ils étaient conçus ne répondaient plus à ces exigences en termes de qualité de service (QoS).

Le problème majeur qu'on rencontre souvent est la congestion du réseau ; Les équipements actifs des réseaux ne donnent aucune priorité aux trafics qui circulent. Ils appliquent le principe du premier arrivé, premier sorti (FIFO) en cas de concurrence d'accès, ainsi un trafic de faible importance peut consommer de la bande passante au détriment de trafic plus important ce qui induit à une anarchie dans le réseau. Ceci, a donc crée un grand besoin de techniques pour assurer la QoS dans les réseaux IP.

De ce qui précède nous avons mené notre réflexion sur la base du questionnement suivant :

- **Peut-on intégrer des techniques permettant d'assurer la qualité de service de la voix sur IP ?**

C'est pourquoi, on a opté pour une technique qui est la mise en œuvre de la QoS par priorisation de flux, et qui va nous permettre de traiter les trafics non pas en fonction de leur ordre d'arrivée, mais en fonction de leur priorité et donc assurer une qualité de service qui répond mieux aux besoins des clients et aux exigences des applications en temps réel.

Ce travail est projeté sur l'état actuel du réseau SONATRACH de Bejaia.

Pour cela, on a divisé notre travail de la manière suivante :

Le premier chapitre titré « étude générale de la voix sur IP » a pour but d'étudier la VoIP (Voice over Internet Protocol ou Voix sur Internet Protocole) et donc voir ses différents aspects ; Nous allons parler de son architecture, ses éléments et son fonctionnement .et par la suite citer les différents protocoles VoIP, leurs principes de fonctionnement ainsi que leurs principaux avantages et inconvénients.

Le deuxième chapitre sera décomposé en deux parties, la première consiste à donner un aperçu sur le modèle de références OSI, les différents serveurs et protocoles d'un réseau ainsi le modèle hiérarchique. Dans la deuxième partie nous allons étudier la qualité de service (QoS) notamment ses contraintes ainsi qu'à ses paramètres et ses modèles de gestion.

Dans le troisième chapitre, nous allons établir une description générale de l'entreprise SONATRACH et précisément du département Telecom où nous avons effectué notre stage.

Le quatrième chapitre sera consacré à la conception et configuration du réseau SONATTRACH.

Le travail sera complété par un chapitre sur l'implémentation de la qualité de service (QoS) en définissant certaines priorités du trafic selon les besoins de l'entreprise. Ceci, en exposant les différentes configurations nécessaires, suivies des tests de validation pour s'assurer du bon fonctionnement du réseau.

CHAPITRE 1 :
ETUDE GENERALE DE LA VOIX SUR IP

Ce chapitre se concentre sur l'étude de la VoIP (Voice over Internet Protocol ou Voix sur Internet Protocole) et de ses différents aspects.

1.1. Introduction

La fusion du réseau téléphonique (RTC) et le réseau IP durant les années 90 a donné naissance à un réseau convergé permettant de transporter à la fois la voix et les données après avoir été séparés.

L'un des services optimisés offerts par le réseau convergé est la voix sur protocole Internet (VoIP), qui est considéré comme étant l'un des plus attrayants et plus important service de nos jours dans les réseaux de communication, Elle fait référence à la transmission de la voix utilisant les technologies IP sur des réseaux à commutation de paquets.

L'objectif de ce chapitre est l'étude de la VoIP (Voice over Internet Protocol ou Voix sur Internet Protocole) et de ses différents aspects. Nous parlerons de son architecture, ses éléments et son fonctionnement .Nous détaillerons par la suite des protocoles VoIP de signalisation et de transport, leurs principes de fonctionnement ainsi que leurs principaux avantages et inconvénients.

1.2. Le Réseau Téléphonique Commuté (RTC) [1]

Le Réseau Téléphonique Public Commuté (RTPC) ou Réseau Téléphonique Commuté dans sa version abrégée (RTC) est le système téléphonique international qui se base sur la commutation de circuit pour acheminer des données vocales analogiques entre des téléphones individuels pour un échange public.

On distingue deux grandes parties dans ce réseau :

- Le réseau capillaire ou de distribution, c'est le raccordement de l'abonné à un point d'entrée du réseau. Cette partie du réseau est analogique.
- Le réseau de transit, effectue pour sa part le transport des communications entre les nœuds de transit (concentrateurs / commutateurs). Cette portion du réseau est actuellement numérique.

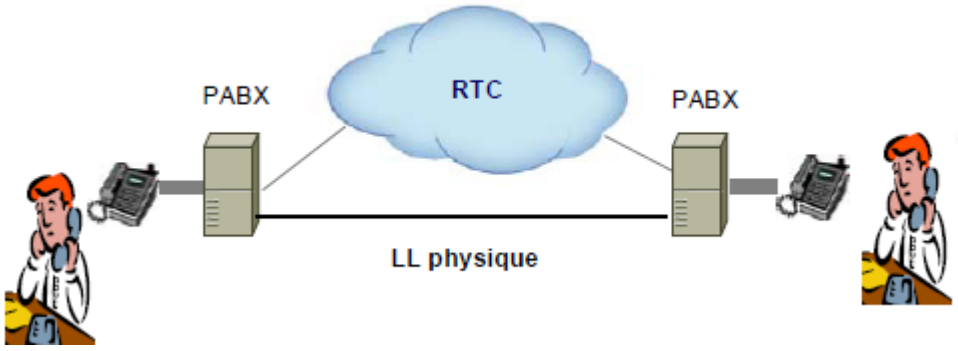

Figure 1.1-Réseau téléphonique commuté RTC. [2]

1.3. Présentation de la voix sur IP

1.3.1. Définition

La téléphonie VoIP (Voice over Internet Protocol) est une technologie basée sur la commutation de paquet, permet la transmission de la voix en utilisant le protocole IP. Elle est ainsi capable de fournir des services de communication flexibles, tout en intégrant les services téléphoniques classiques avec les services et applications informatiques. [3]

Un système VoIP de base se compose de trois éléments principaux : l'expéditeur, le réseau IP et le destinataire.

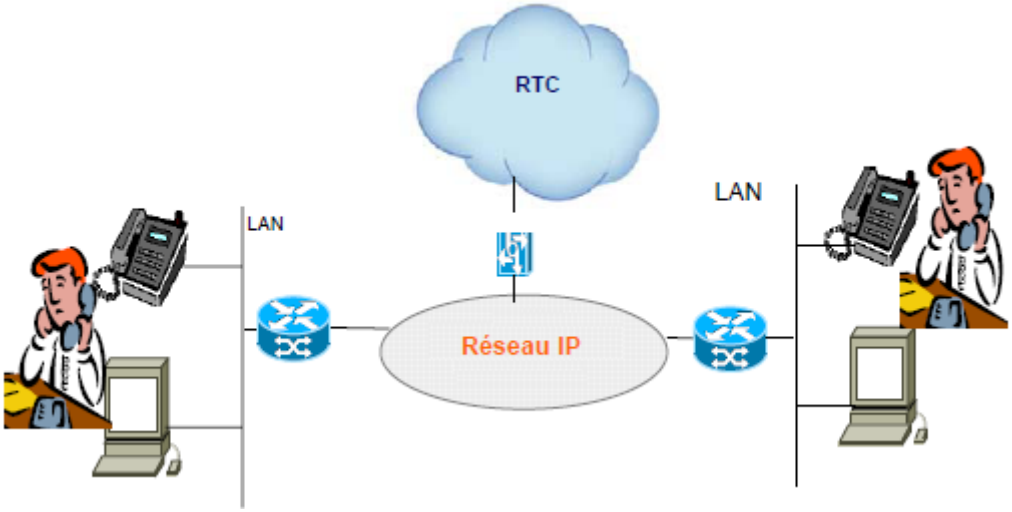

Figure 1.2-Réseau convergé. [2]

1.3.2. Architecture VoIP

La VoIP (voix sur IP) est une nouvelle technologie de communication qui ne détient pas encore de standards unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités. Les principaux protocoles sont H.323 et SIP, ce qui mène à plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP.

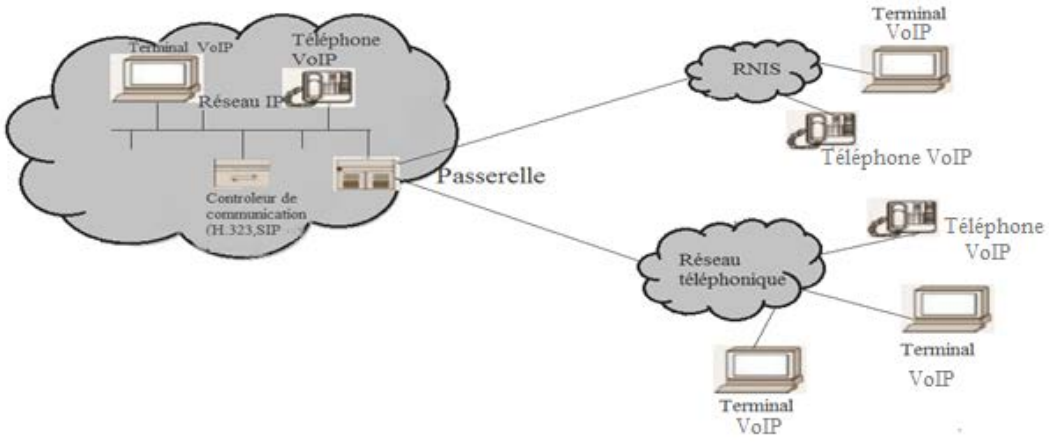

Figure 1.3-Architecture générale de la voix sur IP.[4]

La figure1.3 Représente, la topologie d'un réseau de téléphonie IP. Elle est constituée d'un ensemble d'équipements de base tel que les terminaux, un serveur de communication et une passerelle vers les autres réseaux, permettant l'interconnexion entre les différentes entités du réseau. Chaque norme a ensuite ses propres caractéristiques, pour garantir une certaine qualité de service.

Nous retrouvons ainsi les éléments suivants :

- **Le routeur** : Est un équipement essentiel permettant d'effectuer le transfert de paquets ; lorsqu'il transmet des données entre différents segments du réseau, le routeur examine l'en-tête de chaque paquet pour déterminer le meilleur itinéraire par lequel acheminer le paquet.
- **La passerelle (Gateway)** : Est un système matériel et logiciel qui sert à relier deux réseaux utilisant deux protocoles et/ou architectures différentes ; comme par exemple un réseau local et un réseau IP.
- **Terminaux** : Ils permettent à un utilisateur d'accéder aux ressources du réseau ; comme le pc ou les téléphones IP.
- **Le PABX (Private Automatic Branche Xchange)** : Est un commutateur permettant la liaison entre la passerelle ou le routeur et le réseau téléphonique classique (RTC).si tout le réseau dévient IP, ce matériel devient obsolète ce qui nécessite une mise à jour. [5]

1.3.3. Principe de fonctionnement de la VoIP

Le fonctionnement de la téléphonie sur le réseau IP, consiste en premier lieu à numériser la voix du fait que le format numérique est plus facile à contrôler. Le signal numérique correspondant sera par la suite comprimé et puis découpé en paquets de données.

Ces derniers seront transportés sur les réseaux TCP/IP qui représentent des supports de circulation de paquets IP.

A l'arrivé, le signal de données obtenu après réassemblage de paquets est décomprimé puis converti en signal analogique pour une restitution sonore à l'utilisateur.

1.3.4. Les services VoIP

La téléphonie sur IP englobe la suite complète de services VoIP, parmi lesquels [6] :

- L'interconnexion de téléphones VoIP pour les communications entre différents utilisateurs.
- Des services associés tels que la facturation et les plans de composition sérialisée.
- Des services de communications fiables et hautement sécurisés.
- Des fonctionnalités de base telles que les conférences, le transfert et la mise en garde

1.3.5. Protocoles de la VoIP

Un protocole est un ensemble de règles utilisé par deux entités homologues pour réaliser l'échange d'information entre elles.

En effet, Les protocole VoIP permettent de gérer la transmission de paquets vocaux à l'aide du protocole IP.

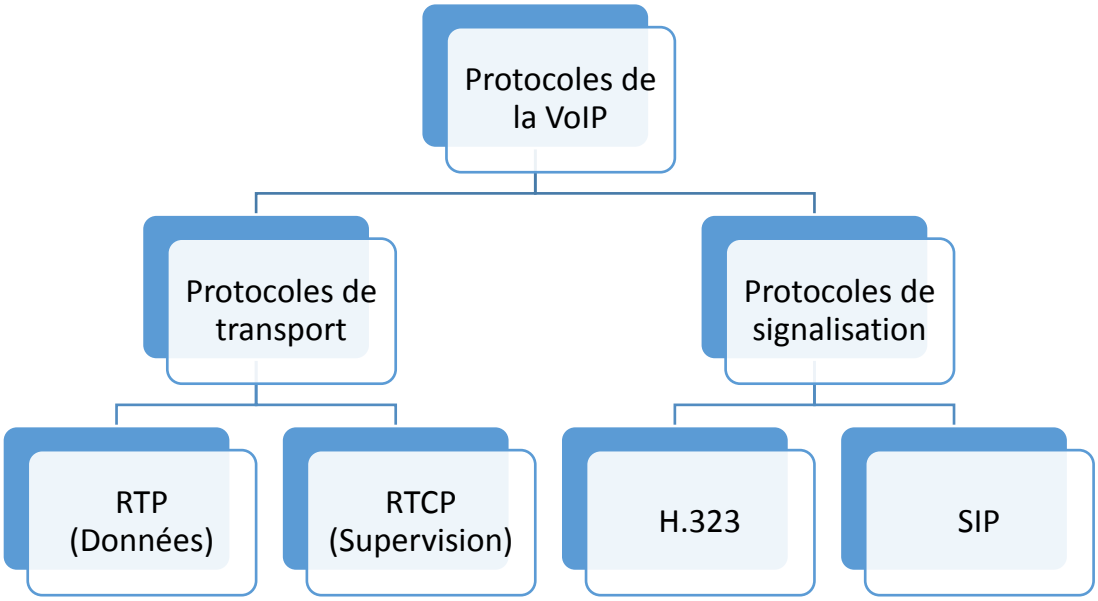

Figure 1.4- Les différents protocoles de la VoIP .

On distingue ainsi deux types de protocoles :

1.3.5.1. Protocoles de Signalisation

La voix sur IP met en œuvre des techniques de télécommunications sur un réseau de paquets. A cet égard, une normalisation de signalisation est donc nécessaire pour garantir l'interopérabilité des équipements.

Il existe deux protocoles de signalisation pour la VoIP :

1. **Protocole H.323**

H.323 défini un ensemble d'entités et de protocoles appartenant à la couche transport du modèle OSI et qui coordonne leurs actions pour qu'une session Multimédia ait lieu. Il a été développé à l'origine comme l'une des nombreuses recommandations de visioconférence, publiées par l'UIT-T (Secteur de la normalisation des télécommunications). La norme H.323 est conçue pour permettre aux clients des réseaux H.323 de communiquer avec des clients d'autres réseaux de vidéoconférence.

Cette recommandation décrit les composants de l'architecture H.323 ; Cela comprend les terminaux, les passerelles (GW), les portiers (GK), les unités de contrôle multipoint (MCU), le contrôleur multipoint (MC) et processeurs multipoints (MP).[7]

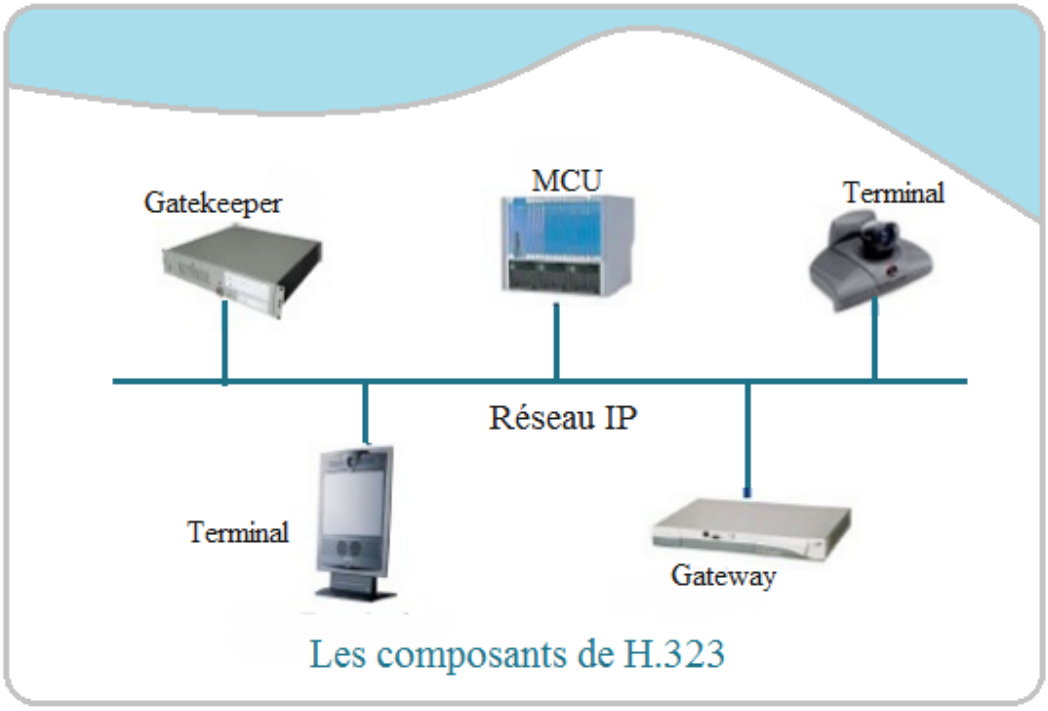

Figure 1.5-Les composants de H.323. [8]

- **Terminal :** C'est l'équipement utilisateur, il peut être physique (hardware) ou logique (software) il fournit des communications bidirectionnelles en temps réel avec un autre terminal H.323, GW ou MCU. Cette communication consiste en un contrôle, des indications, du son, des images vidéo couleur en mouvement et / ou des données entre les deux terminaux.

  Un terminal peut fournir uniquement la parole, la parole et les données, la parole et la vidéo, ou la parole, les données et la vidéo. [9]

- **GateKeeper(Portier) :** Cette entité sert à l'enregistrement des terminaux dans le réseau H.323.Elle assure la traduction des adresses et contrôle l'accès au réseau pour les terminaux H.323, GW et MCU.

  Le GK peut également fournir d'autres services aux terminaux, aux GW et aux MCU, tels que la gestion de la bande passante et la localisation des GW.[9]

- **M.C (Multipoint Controller) :**C'est l'entité destinée à la gestion de session Multimédia dans le cas de conférence (groupe d'utilisateurs s'échangeant des informations en temps réel). Il gère les conférences multipoints entre trois terminaux ou passerelles ou les deux ou plus. Pour établir une telle conférence, il fournit un support qui pourra être partagé entre les entités du réseau et transmet un

ensemble de capacités aux différents participants à la conférence. Un contrôleur de gestion peut résider dans une unité de contrôle multipoint (MCU) distincte ou peut être intégré à la même plate-forme qu'une passerelle, un terminal H.323 ou un portier. [10]

- **La passerelle(Gateway**) : C'est un point d'extrémité H.323 qui fournit des services de traduction entre le réseau H.323 et un autre type de réseau, qui peut être une passerelle RNIS (Integrated Services Digital Network) ou PSTN (Public Switched Telephone).Une passerelle a un double type d'interface ; D'un côté, elle prend en charge la signalisation H.323 et transmet les données conformément au réseau H.323. De l'autre côté, elle transmet les données en s'interfaçant avec un réseau à commutation de circuits. [10]

a. Architecture Protocolaire

L'architecture protocolaire de la norme H.323 se présente comme suit :

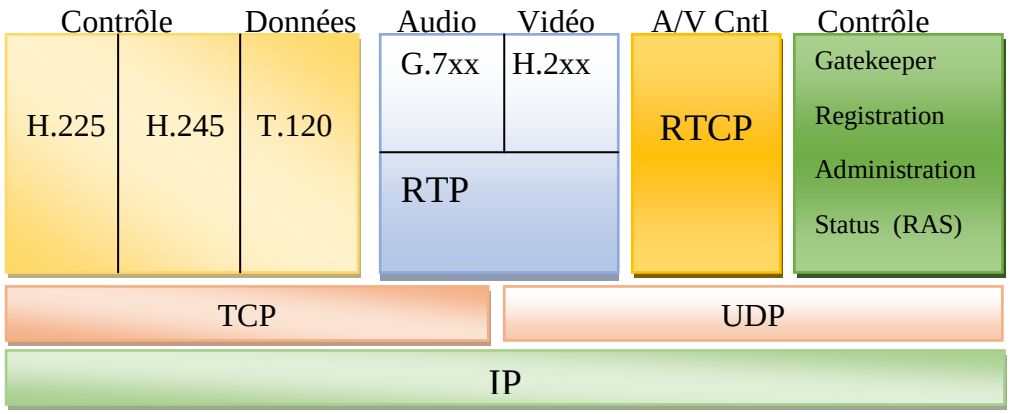

Figure 1.6-Architecture protocolaire de H.323. [11]

En examinant la pile de protocole, nous pouvons noter que H.225, H.245 et T120 sont utilisés conjointement avec TCP pour s'assurer de la fiabilité de l'échange de l'information lors d'initialisation de session.

Go7xx et H.2xx définissent des standards de compression audio et vidéo respectivement .Il emploient RTP sur UDP pour transport de l'information.

Le GateKeeper utilise en vérité H.225 pour maintenir l'information sur l'état (en ligne, hors ligne) des utilisateurs.

- **H.225** : Met en place un canal de signalisation d'appel et d'enregistrement afin d'assurer une mise en relation des interlocuteurs.

- **H.245** : Négocie l'ouverture et l'utilisation des canaux ainsi que les paramètres de la communication.

b. Avantages et inconvénients de H.323 [12]

Les avantages :

- **Codecs standards** : H.323 établit des standards pour la compression et la décompression des flux audio et vidéo.
  Ceci assure que des équipements provenant de fabricants différents ont une base commune de dialogue.
- **Support multipoint** : H.323 supporte des conférences entre trois terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée.
- **Gestion de la bande passante** : Le trafic audio et vidéo est un grand consommateur de ressources réseau. Afin d'éviter que ces flux ne congestionnent le réseau, H.323 permet une gestion de la bande passante à disposition. En particulier, le gestionnaire du réseau peut limiter le nombre simultané de connexions H.323 sur son réseau ou limiter la largeur de bande à disposition de chaque connexion. De telles limites permettent de garantir que le trafic important ne soit pas interrompu.
- **Support multicast** : H.323 supporte le multicast dans les conférences multipoint. Multicast, c'est le fait d'envoyer un paquet vers un sous-ensemble de destinataires sans réplication ; ce qui permet une utilisation optimale du réseau.
  Les inconvénients de la technologie H.323 sont **:**
  - La complexité de mise en œuvre : le protocole H.323 incorpore des mécanismes superflus dans un contexte purement téléphonique. Ceci a notamment des incidences au niveau des terminaux H.323 (téléphones IP, par exemple) qui nécessitent de ce fait une capacité mémoire et de traitement sans incidence au niveau de leur coût.
  - Elle comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité ou de plus petit dénominateur commun.
  - Le protocole H.323 est une des normes envisageables pour la voix sur IP à cause de son développement inspiré de la téléphonie. Cependant, elle est pour l'instant employée par des programmes propriétaires (Microsoft, etc.). La documentation est difficile car l'ITU (Union International Télécommunication) fait payer les droits d'accès aux derniers développements

de cette technologie. Ainsi son adaptation au réseau IP est assez lourde ; C'est pourquoi au fil des recherches est né le SIP.

2. Le protocole SIP

a. Description générale du protocole SIP

Session Initiation Protocol (dont le sigle est SIP)est un protocole de signalisation appartenant à la couche application du modèle OSI , normalisé et standardisé par l'IETF (Internet Engineering Task Force) en1999 .il a été conçu principalement pour établir, modifier et terminer des sessions multimédia(voix, vidéo, données).Le protocole SIP permet de supporter de nombreux services tels que la messagerie instantanée, le transfert d'appel, la conférence et les services complémentaires de téléphonie.[7]

b. Entités du protocole SIP

Le protocole SIP dispose des entités qui interagissent entre elles afin de garantir les services SIP, on retrouve particulièrement des entités utilisateurs et des entités réseaux :

- **Les entités Utilisateurs :** Sont appelées des agents utilisateurs(U.A) dont on peut distinguer les UAC (User Agent Client) etUAS (User Agent Server).Le client envoie les requêtes SIP lorsqu'il initialise un appel, l'UAS est une application qui contacte l'utilisateur si un appel lui est destiné.
- **Les entités réseaux**

Sont constituées de plusieurs serveurs qui sont :

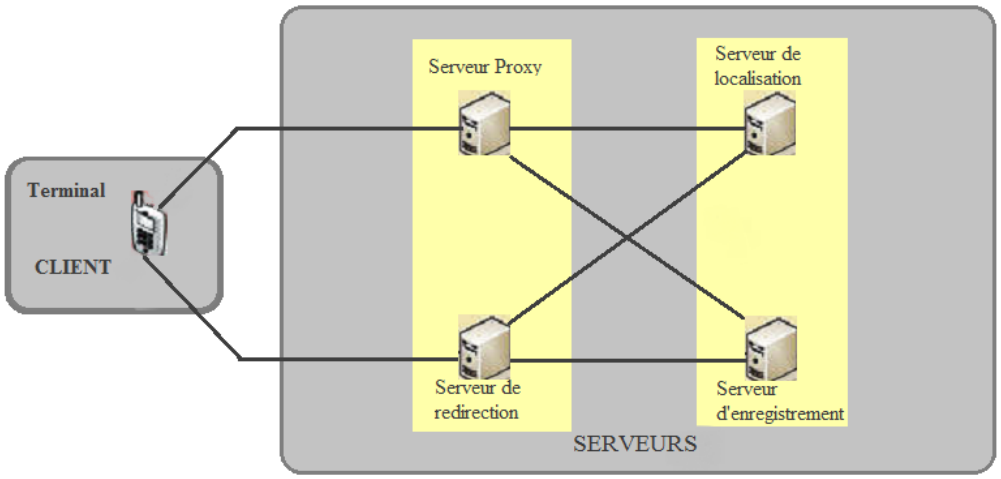

Figure 1.7-Architecture de SIP [13]

- **Serveur proxy** : on retrouve au moins un serveur Proxy dans chaque domaine, celui-ci est le premier interlocuteur d'un client qui souhaite initier une session IP. Le

serveur Proxy agit comme serveur et client à la fois, c'est-à-dire qu'il peut envoyer et recevoir des requêtes.

- **Serveur d'enregistrement :** Chargé d'enregistrer chaque utilisateur qui rentre dans le réseau SIP, en particulier, il se charge de déterminer l'association client/adresse IP de chaque UA (User Agent), et permet de garder des traces de localisations des utilisateurs.
- **Serveur de redirection :** Le rôle de ce serveur est de répondre aux requêtes des UA ou de serveur proxy concernant la localisation de correspondant. Ce serveur se chargera de renvoyer les informations nécessaires au client appelant, pour qu'il puisse établir une connexion directe avec l'interlocuteur désiré.
- **Serveur de localisation** : Les informations recueillies pour le serveur d'enregistrement sont déposées auprès du serveur de localisation. Ce dernier contient donc toute la base de données utilisateurs qui sont enregistrés dans le réseau.

Les UA et le serveur Proxy peuvent être interrogés par le serveur de localisation pour localiser les correspondants.

c. Avantages et inconvénients

Les principaux avantages du protocole SIP sont [14]:

- SIP est un protocole rapide et léger. La séparation entre ses champs d'en-tête et son corps du message facilite le traitement des messages et diminue leur temps de transition dans le réseau.
- Flexible : SIP est également utilisé pour tout type de sessions multimédia (voix,

vidéo, mais aussi musique, réalité virtuelle, etc.).

- Simple par sa nature textuelle à l'exemple de http.

Par contre SIP est très vulnérable face à des attaques de types DoS (Dénis de Service), détournement d'appel, trafic de taxation, etc.de plus Le SIP, devient de plus en plus utilisé pour la mise en place de la téléphonie sur IP ; la compréhension de ce protocole aidera le professionnel à l'épreuve de la sécurité sur le réseau.

1.3.5.2. Protocoles de transport

Le transport de l'information repose sur le protocole RTP (Real-time Tansport Protocol), un protocole de transport qui transporte la voix, la vidéo ou les données numérisées par les codecs. Il est souvent associé aux messages RTCP (Real-time Control

Protocol), un protocole de contrôle des flux RTP, qui permet de véhiculer des informations sur la qualité de service ainsi que sur les participants de la session.

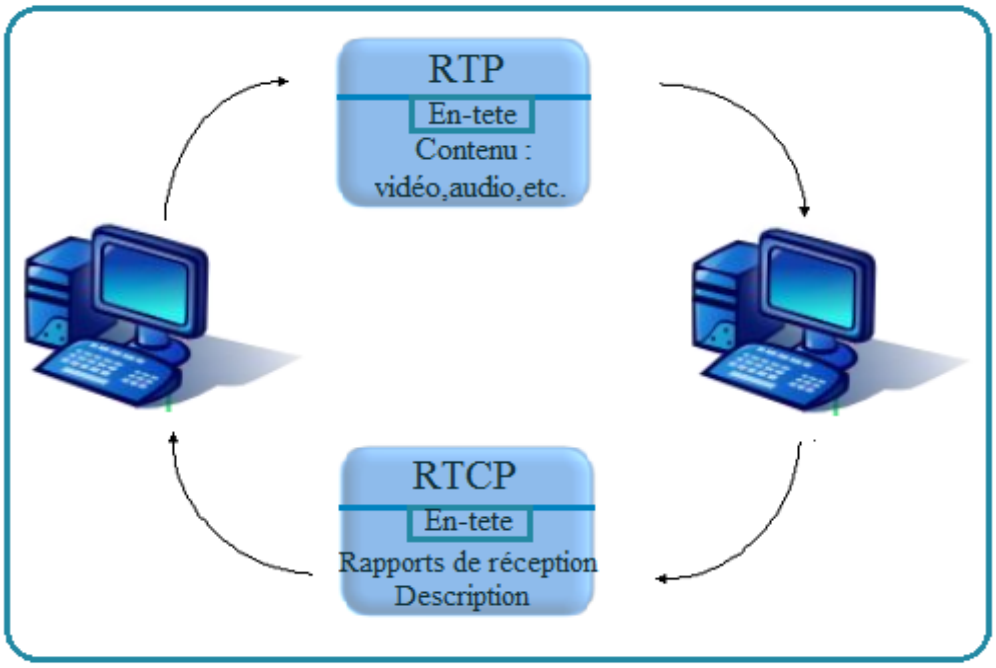

Figure 1.8-Les protocoles RTP/RTCP**. [15]**

1.3.5.3. Le protocole RTP

1. Description de RTP

RTP (Real Time Protocol), standardisé en 1996, est un protocole qui a été développé par l'IETF, pour faciliter transport en temps réel de bout en bout, des flots de données audio et vidéo sur les réaux IP. Il se situe au niveau de la couche d'application et il utilise les protocoles se sous-jacents de transport TCP ou UDP. Mais l'utilisation de RTP se fait généralement au-dessus d'UDP, ce qui permet d'atteindre plus facilement le temps réel.

Les applications en temps réel, comme la parole numérique ou la visioconférence constitue un véritable problème pour internet. Une application en temps réel exige une certaine qualité de service (QOS) que RTP ne garantit pas du fait qu'il fonctionne au niveau applicatif.

De plus RTP est un protocole qui se trouve dans un environnement multipoints, donc on peut dire que RTP possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoints.[16]

2. Les fonctions de RTP

Le protocole RTP a pour but de fournir un moyen uniforme de transmettre des données soumises à des contraintes en temps réel, tout en organisant les paquets à l'entrée du réseau et de les contrôler à la sortie. Il permet ainsi :

- L'identification de ce qui est transporté dans le message pour permettre, par exemple, une compensation en cas de perte.
- L'identification de la source. Dans les applications en multicast, l'identité de la source doit être déterminée.
- Le séquencement des paquets par une numérotation. Cette numérotation permet de détecter les paquets perdus, ce qui est important pour la recomposition de la parole. La perte d'un paquet n'est pas un problème en soi, à condition qu'il n'y ait pas trop de paquets perdus. En revanche, il est impératif de repérer qu'un paquet a été perdu de façon à en tenir compte et à le remplacer éventuellement par une synthèse déterminée en fonction des paquets précédant et suivant.

3. Avantages et inconvénients du protocole RTP

Le protocole RTP permet de reconstituer les messages multimédia (audio, vidéo, etc.) ; de détecter les paquets perdus ; et d'identifier le contenu des paquets pourleurs transmission sécurisée.

En revanche, il n'assure pas le contrôle de la qualité de service (QoS) ; ne prévoit pas la retransmission automatique des paquets manquants ; et n'agit pas au niveau des routeurs.

1.3.5.4. Le protocole RTCP

1. Description de RTCP

RTCP (Real Time Transport Control Protocole ou protocole de transport en temps réel) est basé sur la transmission périodique de paquets de contrôle par tous les participants dans la session. C'est un protocole de contrôle utilisé conjointement avec RTP pour contrôler les flux de données RTP, et qui permet de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service. [17]

2. Les fonctions de RTCP

Le protocole RTCP remplit trois fonctions :

- L'information sur la qualité de service : RTCP fournit, en rétroaction des informations sur la qualité de réception des données transmises dans les paquets RTP.
- L'identification permanente : RTCP transporte une identification de la source RTP c'est-à-dire la provenance du flux, appelée CNAME (Canonical name). Cet identificateur permet une identification permanente de chacun des flux multimédia entrants.
- La connaissance à tout moment du nombre de participants présents dans la session.

3. Avantages et inconvénients du protocole RTCP

RTCP est un protocole adapté pour la transmission de données temps réel. Il permet un contrôle permanant sur une session et ses participants.

Par contre il fonctionne en stratégie bout en bout .Et il ne permet pas le contrôle de l'élément principal de la communication « le réseau ».

1.3.6. Points forts et limites de la voix sur IP

La VoIP offre de nouvelles possibilités aux utilisateurs qui bénéficient d'un réseau basé sur IP, c'est pour cette raison là que les entreprises s'orientes vers la VoIP comme solution pour la téléphonie. Les avantages les plus marqués sont les suivants :

- **Réduction des couts :** En effet le trafic véhiculé à travers le réseau RTC est plus couteux que sur un réseau IP. Réductions importantes pour des communications internationales en utilisant le VoIP, ces réductions deviennent encore plus intéressantes dans la mutualisation voix/données du réseau IP intersites (WAN). Dans ce dernier cas, le gain est directement proportionnel au nombre de sites distants.[16].
- **La mobilité infinie :** Les utilisateurs de la téléphonie VoIP n'ont plus besoin de rester scotché à un téléphone filaire pour recevoir ou passer des appels depuis son numéro de fixe. Désormais, depuis n'importe quel dispositif connecté à internet et surtout, depuis n'importe quel endroit dans le monde, l'utilisateur peut utiliser sa ligne téléphonique VoIP. [18]
- **Un réseau voix, vidéo et données (triple play) :** En positionnant la voix comme une application supplémentaire du réseau IP, l'entreprise ne va pas uniquement substituer un transport opérateur RTC à un transport IP, mais simplifier la gestion des trois réseaux (voix, données et vidéo) par ce seul transport. Une simplification de gestion, mais également une mutualisation des efforts financiers vers un seul outil. [19]

Les points faibles de la voix sur IP :

- **Fiabilité :** La VoIP dépend en grande partie de la connexion internet, ainsi la qualité de service de cette dernière sera affectée par la qualité et la fiabilité de votre service internet. Si le trafic sur le réseau est élevé, la qualité de la voix diminue. Cela se voit généralement dans les appels longue distance ou internationaux où la voix semble déformée, ce qui pose problème, principalement pour les appels professionnels pour lesquels la communication doit être rapide et des mesures doivent être prises en fonctions de la réponse. [20]

- **Qualité de voix de VoIP:** La VoIP a un peu amélioré la qualité de la voix, mais pas dans tous les cas. La qualité de service de la VoIP dépend de plusieurs facteurs : votre raccordement à bande large, votre matériel, le service fourni par votre fournisseur, la destination de votre appel etc. Beaucoupde gens apprécient la qualité des appels téléphoniques utilisant la VoIP, mais d'autres d'utilisateurs se plaignent toujours d'attendre beaucoup avant d'entendre une réponse etc… [20]
- **Sécurité :** Les services Internet ont toujours été confrontés au problème de la sécurité. Même est le cas avec la VoIP aussi. Le piratage téléphonique a été une préoccupation majeure à cet égard. En raison du peu de temps accordé pour l'analyse des paquets de données, les performances des pare-feu peuvent être moins que satisfaisantes. La VOIP est également affectée par les vers et les virus. Tous ces éléments constituent une menace pour la sécurité. [21]

1.4. Conclusion

Dans ce chapitre nous avons présenté la voix sur IP à savoir son architecture, les services qu'elle dispose, les protocoles de signalisation et les protocoles de transport qui assurent son fonctionnement et nous avons clôturé ce chapitre part les points fort et limites de la VoIP.

Dans le chapitre qui suit nous aborderons le concept des VLANs et étudier la qualité de service ainsi ses différentes caractéristiques.

CHAPITRE 2 :
CONCEPT DES VLANs ET ETUDE DE LA QUALITE DE SERVICE

Ce chapitre se concentre sur l'identification des VLANs et l'étude de la qualité de service (QoS).

2.1. Introduction

Alors que les applications utilisateur continuent d'engendrer la croissance et l'évolution du réseau, la demande de prise en charge de différents types de trafic augmente également. Différents types d'applications avec de différentes exigences créent un besoin de stratégies administratives imposant comment les applications doivent être traitées par le réseau.

L'emploi et l'exécution des règles de la qualité de service (QoS) au sein d'un réseau jouent un rôle essentiel qui permet aux administrateurs et aux architectes du réseau de répondre aux demandes des applications en temps réel. La QoS est un élément crucial de toute politique administrative qui définit la gestion du trafic applicatif sur un réseau.

Le réseau doit fournir des services sécurisés, prévisibles, mesurables et parfois garantis. Le réseau d'administrateur et les concepteurs peuvent mieux réaliser cette performance depuis le réseau en gérant les paramètres de retard (gigue), le provisionnement en bande passante et les paramètres de perte de paquet avec des techniques de qualité de service(QoS).

Ce chapitre sera décomposé en deux parties, la première consiste à définir le modèle de références OSI, les différents serveurs et protocoles d'un réseau ainsi le modèle hiérarchique.

Dans la deuxième partie nous aborderons la notion de qualité de service (QoS) ; ses contraintes ainsi qu'à ses paramètres ; ses modèles de gestion.

2.2. Modèle OSI de L'ISO

Le modèle de référence OSI (Open System Interconnexion) a été élaboré par l'ISO en 1983 constitué de 7 couches remplissant chacune une fonctionnalité particulière.

L'illustration ci-après présente la structure de ce modèle.

Donnée	**Application** (Point d'accès aux services réseau) ex: HTTP,HTPS,SNMP,FTP,Telnet,NFS,ect...
Donnée	**Présentation** (Conversion et chifrement des données) ex: ASCII,Unicode,MIME,SMB,AFP,ect...
Donnée	**Session** (Communication interhost) ex: ISO 8327/CCITT X.255,RPC,ASP,ect...
Segment	**Transport** (Connexion de bout en bout et controle de flux "TCP") ex: TCP,UDP,ATP,ect...
Paquet	**Réseau** (Détermine le parcours et l'adressage logique "IP") ex: IP(IPv4 ou IPv6),ICMP,IGMP,ARP, RIP,IPX,DDP,ect...
Trame	**Liaison** (Adressage physique "MAC et LLC") ex: Ethernet,Token Ring,Frame relay,RNIS(ISDN),ATM,Wi-Fi,Bluetooth,ZigBee,ect...
Bit	**Physique**(Transmission binaire numérique ou analogique) ex: technique de codage du signal(électronique,radio,..) pour la transmission desinformations sur les réseaux physiques(réseaux fillaire,optiques,..)

Figure 2.1-Modèle OSI.

2.3. Les serveurs réseau :

Un serveur réseau est un ordinateur puissant, conçu pour fournir des informations et des logiciels à d'autres ordinateurs qui lui sont reliés via un réseau.il est aussi capable d'exercer plusieurs fonctions en même temps.

2.3.1. Serveur DHCP

Un serveur DHCP (Dynamic Host Configuration Protocol) est un serveur qui délivre des adresses IP aux ordinateurs qui se connectent sur le réseau. Son rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque sous réseau.

2.3.2. Serveur DNS

Le système de noms de domaines DNS (Domain Name System) est un système de données distribuées qui fournit la correspondance entre le nom de domaine d'une machine d'un réseau associé et son numéro IP.

2.3.3. Serveur HTTP

Le serveur http (Protocole de Transfert Hypertexte) est un serveur définissant la communication entre un client (navigateur web) et un serveur sur le World Wide Web **(WWW)** basé sur le principe « requête-réponse ».

2.4. Les réseaux locaux virtuels (VLANs) :

Les performances réseau constituent un facteur majeur dans la productivité d'une entreprise. L'une des technologies permettant de les améliorer consiste à diviser de vastes domaines de diffusion en domaines plus petits. Par définition, Un réseau local virtuel (VLAN) est un réseau local (LAN) qui regroupe un ensemble de machines de manière logique et non physique, distribué sur des équipements de niveau 2 du modèle OSI (couche liaison) , il a pour rôle de réduire la taille des domaines de diffusion et permettent à un administrateur de segmenter les réseaux ce qui permettra d'augmenter ou d'améliorer les performances (débit, bande passante, sécurité…).

2.4.1. Les avantages des VLAN :

Les principaux avantages des VLAN sont les suivants :

- **Sécurité :** les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.
- **Réduction des coûts :** des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à une utilisation plus efficace de la bande passante.
- **Meilleures performances** : diviser des réseaux linéaires de couche 2 en plusieurs domaine de diffusion réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- **Réduction des domaines de diffusion :** la division d'un réseau en VLAN réduit le nombre de périphériques dans le domaine de diffusion personnel.

2.4.2. Les méthodes de construction d'un VLAN

- **VLAN de niveau 1(Vlan par port) :** Les VLAN de niveau 1 sont également appelés VLAN par port (port-Based VLAN).chaque port du commutateur est affecté à un VLAN particulier.
- **VLAN de niveau 2 (VLAN MAC) :** Les VLAN de niveau 2 sont également appelés VLAN MAC, VLAN par adresse IEEE ou MAC Address-BasedVLAN.Ils sont constitués en associant les adresses MAC des stations à chaque VLAN.

Le commutateur détermine le VLAN de chaque trame à partir de l'adresse MAC source ou destination.

- **VLAN de niveau 3 (VLAN par sous réseau ou VLAN par protocole) :** Divisé en deux :

- **Le VLAN par sous-réseau (Network Address-Based VLAN) :** il associe des sous réseaux selon l'adresse IP source des datagrammes.

- **Le VLAN par protocole (Protocol-**Based VLAN) : il permet de créer un réseau par type de protocole, regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau virtuel.

2.4.3. Création du Voice VLAN

Le VOICE VLAN est une option que CISCO à créer pour permettre au port des switchs d'avoir une double fonction, c'est de pouvoir brancher un IP Phone et un PC sur le même port et chacun d'eux appartiens à son propre VLAN.

2.4.4. Port Trunk (802.1q)

Le port Trunk est capable de communiquer avec tous les VLAN, il permet d'ajouter à la trame une information indiquant de quel VLAN elle provient. il est utilisé à chaque fois qu'une ressource doit être accessible à partir de tous les VLAN, permettant la propagation de plusieurs VLAN sur un même lien physique (Trunk).

2.5. Les protocoles LAN

Les protocoles de manière générale permettent d'échanger des données de manière structurée au sein d'un réseau, en définissant ainsi les différents protocoles utilisés dans les réseaux LAN (local Area Network).

2.5.1. Le protocole VTP

Le VTP (Vlan Trunking Protocol) ou VLAN Trunking Protocol est un protocole de messagerie utilisant les trames d'agrégation pour gérer l'ajout, la suppression et l'attribution de noms aux VLAN. Il autorise aussi les changements qui sont communiqués aux autres commutateurs du réseau. Les messages VTP sont encapsulés dans des trames IEEE 802.1Q, puis transmis sur des liens multi-VLAN aux autres éléments du réseau.

Les ports des commutateurs sont affectés à un seul VLAN, mais les ports multi-VLAN transportent les trames de tous les VLANs du réseau. Ce port dit "port trunking", dans lequel passeront plusieurs VLANs, est un lien "Trunk".[6]

2.5.2. Protocole SpaningTree

Le SpanningTree Protocol est un protocole de niveau deux (couche liaison de données) qui empêche la création de boucle au sein d'un réseau, il est conçu pour les switch CISCO, Cependant il est nécessaire de rajouter des paramètres par rapport à la configuration qui est en cours sur le réseau sinon il peut s'avérer une contrainte majeur dans la rapidité et la fluidité de circulation de l'information dans le réseau.

De plus, la convergence du réseau dispose d'une redondance ce qui fait le temps va être très long ce qui induit a des coupures de communications ou un transfert de fichier en cours.

2.5.3. Protocole TCP/IP

Segmente l'information à envoyer en petits paquets et la reconstitue à l'arrivée en remettant les paquets dans le bon ordre.

2.6. Le modèle hiérarchique

Le modèle de conception hiérarchique à trois couches a été inventé principalement par Cisco, il consiste à créer un design réseau structuré en trois couches de telle façon à ce que chacune de ces couches ait un rôle précis.

- **La couche cœur** : elle est considérée comme le backbone du réseau, son rôle est de commuter les paquets le plus rapidement possible.
- **Couche distribution** : elle fait le lien entre la couche « cœur de réseau » et la couche accès, elle assure les fonctions du routage et permet la segmentation pour accéder à des départements ou des groupes de travail.
- **Couche accès :** c'est le point d'entrée autorisé dans le réseau, elle permet aux utilisateurs d'accéder aux périphériques du réseau.

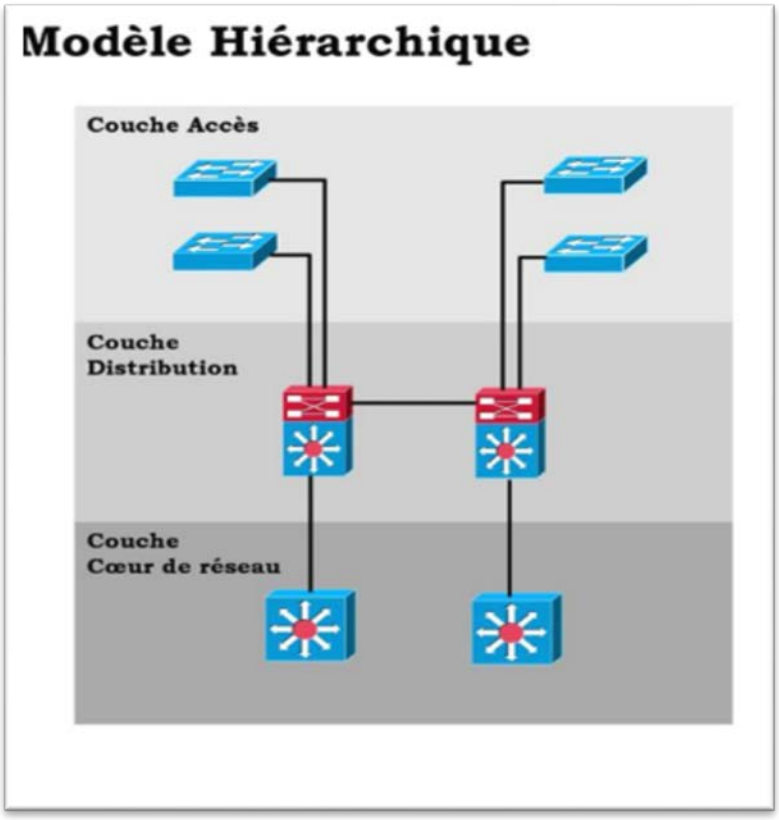

Figure 2.2-Modèle hiérarchique.

2.7. Notion de qualité de service (QoS)

La qualité de service est l'une des préoccupations majeures des communications vocales. Elle désigne la capacité du réseau à offrir un meilleur service aux utilisateurs et aux applications.

L'objectif de qualité de service(QoS) est de fournir un service meilleur et plus prévisible tout en fournissant une bande passante dédiée, la gigue et la latence contrôlée et des caractéristiques améliorées. Ces objectifs sont atteints tout en apportant des outils pour la gestion de la congestion du réseau, mise en forme du trafic réseau, l'utilisation de coûteux liens étendus de manière plus efficace, et en définissant des politiques de la circulation à travers le réseau.

Une fois la QoS est correctement appliquée, elle permet d'offrir des services de réseau qui aident à assurer une performance cohérente et prévisible.[22]

2.7.1. Avantages et contraintes de la QoS

Les quatre grands problèmes de la qualité de service auxquels sont confrontés les réseaux d'entreprise sont les suivantes [22] :

- **La bande passante :**Les fichiers graphiques volumineux, les utilisations multimédias et l'utilisation croissante de la voix et de la vidéo entraînent des problèmes de capacité de bande passante sur les réseaux de données.
- **La latence (délai de bout en bout/delay) :** c'est le temps nécessaire à un paquet pour atteindre le point de réception après avoir été transmis. Cette période de temps est appelée "délai de bout en bout" et se compose de deux composants :
  - **Délai réseau fixe :** la sérialisation et la propagation sont deux types de délais fixes. La sérialisation consiste à placer des bits sur le circuit. Plus la vitesse du circuit est élevée, moins est le temps pour placer les bits sur le circuit. Par conséquent, plus la vitesse du lien est élevée, moins le délai de sérialisation est engagé. Le délai de propagation est le temps nécessaire aux images pour transiter sur le support physique.
  - **Délai réseau variable :** le délai de traitement est un type de délai variable. C'est le temps nécessaire à un périphérique réseau pour rechercher l'itinéraire, modifier l'en-tête et effectuer d'autres tâches de commutation. Dans certains cas, le paquet doit également être manipulé, par exemple lorsque le type d'encapsulation ou le nombre de sauts doit être modifié. Chacune de ces étapes peut contribuer au délai de traitement.
- **La gigue (variation de délai) :** c'est la différence du total des valeurs de délai de bout en bout de deux paquets de voix dans le flux de voix.
- **Perte de paquets** : Elle correspond à la non-délivrance d'un paquet de données qui est généralement due à un encombrement dans le réseau étendu, entraînant des interruptions de la parole ou un effet de bégaiement si le côté lecture tente de s'en accommoder aux paquets précédents.

En général la qualité de service fournit un service réseau meilleur (et plus prévisible) en fournissant les fonctionnalités suivantes :

- Prise en charge de la bande passante dédiée.
- Améliorer les caractéristiques de perte.
- Eviter et gérer la congestion du réseau.

- Façonner le trafic réseau.
- Définition des priorités de trafic sur le réseau.

2.7.2. Les exigences de la QoS

- **Identifier le trafic et ses exigences** : Cette étape consiste à identifier le trafic sur le réseau puis déterminer les exigences de qualité de service pour le trafic ; Celles-ci affectent la voix, la vidéo et les paquets de données.
- **Les classes de qualité de service du trafic :** La répartition de trafic en classes se fait comme suite :
  - **Classe voix** : Priorité absolue pour la voix sur IP (VoIP).
  - **Classe critiques** : Petite série d'applications métier critiques définies localement.
  - **Classe transaction** : Accès base de données, services de transactions.
  - **Classe best-Effort** : Internet, e-mail.
- **Définir des stratégies pour chaque classe de trafic** : Définir une stratégie de qualité de service pour chaque classe de trafic, implique les activités suivantes :
  - Définir une garantie de bande passante minimale
  - Définir une limite de bande passante maximale.
  - Attribuer des priorités à chaque classe.
  - Utiliser les technologies de qualité de service, telles que les files d'attente avancées, pour gérer la congestion.

2.8. Gestion de la qualité de service (QoS)

Afin de répondre aux exigences de ces applications en temps réel , différentes approches de QoS ont été proposées pour la mise en œuvre d'une technologie qui implémente et gère la qualité de service dans les réseaux IP.Les plus connues, et les plus déployées sont : le **modèle IntServ**, le **modèle DiffServ**.[22]

2.8.1. Modèle Best-Effort

Le modèle meilleur effort est un service qui permet de livrer les paquets sans aucune garantie, et dans des conditions d'acheminement non-spécifiées qui dépendent seulement de la charge du réseau et non des besoins requis par les applications.

2.8.1.1. Avantages et Inconvénients du model Best-Effort

Best-Effort présente les avantages significatifs suivants :

- **Evolutivité quasi illimitée** : Le seul moyen d'atteindre les limites d'évolutivité est d'atteindre les limites de bande passante, auquel cas tout le trafic est retardé de manière égale.
- **Aucun mécanisme spécial requis** : il n'est pas nécessaire de recourir à des mécanismes spéciaux de qualité de service pour utiliser le modèle Best-Effort. C'est le modèle le plus facile et le plus rapide à déployer.

Le modèle Best-Effort présente également les inconvénients suivants :

- **Aucune garantie** : Les paquets arriveront chaque fois qu'ils le pourront, dans n'importe quel ordre, s'ils arrivent tous.
- **Pas de différenciation des services** : Les paquets ne font pas l'objet d'un traitement préférentiel

2.8.2. Le modèle IntServ (Integrated Service)

Le modèle de services intégrés (IntServ) est une architecture qui offre une garantie de qualité de service de bout en bout , il fournit un moyen de satisfaire les différentes contraintes de QoS exigées par les applications, et cela à travers la gestion directe des ressources du réseau ce qui permet de fournir la QoS appropriée à des flux de paquets bien spécifiques du trafic.Ce modèle, a été proposé par l'IETF (Internet Engineering Task Force) .

IntServ se base sur deux principaux mécanismes pour établir et maintenir la QOS : la réservation de ressources et le contrôle de flux.

2.8.2.1. Protocole RSVP

RSVP (Resource ReSerVation Protocol) est avant tout un protocole de signalisation qui permet de réserver dynamiquement de la bande passante, et de garantir un délai, ce qui le rend particulièrement efficace pour des applications comme VoIP.

Ce protocole assure la réservation de ressource au niveau de chaque nœud que traverse un flux de trafic. Il existe sept types de message RSVP :

- **Messages PATH** : Un message de chemin RSVP est envoyé par chaque expéditeur au destinataire.
- **Messages (RESV)** : Un message de demande de réservation est envoyé par chaque hôte destinataire aux expéditeurs.
    - **Messages d'erreur et de confirmation** : Les informations contenues dans les messages d'erreur peuvent inclure les éléments suivants :

- Échec d'admission.
- Bande passante indisponible.
- Service non supporté.
- Mauvais débit.

- **PathTear** : Indique aux routeurs les états concernant la route.
- **ResvTear** : Indique aux routeurs les états de réservation (fin de session).
- **ResvConf** : Message de confirmation envoyé par le dernier routeur recevant le message RESV, au récepteur.

2.8.2.2. Le contrôle de flux

Le contrôle de flux englobe quatre principales fonctions qui doivent être implémentées par les différents nœudsdu réseau.

- l'ordonnancement des paquets (scheduling).
- la classification des paquets.
- la suppression des paquets (packet dropping).
- le contrôle d'admission.

2.8.2.3. Avantages et Inconvénients du model IntServ

Les principaux avantages d'IntServ sont les suivants :

- Contrôle d'admission explicite des ressources (de bout en bout).
- Contrôle d'admission de stratégie .
- Signalisation de numéros de ports dynamiques (par exemple, H.323).

Les principaux inconvénients d'IntServ et de RSVP sont les suivants :

- Signalisation continue en raison de l'architecture avec état.
- Approche non évolutive pour les grandes implémentations telles que l'Internet public.

2.8.3. Le modèle DiffServ

Differentiated Services (DiffServ) est un modèle multi-service pour la mise en œuvre de qualité de service (QoS) du réseau, il a été conçu pour surmonter les limites des modèles Best-Effort et IntServ.il peut également fournir une qualité de service «presque garantie». Tout en restant économique.

Avec DiffServ, le trafic réseau est divisé en classes en fonction des besoins de l'entreprise. Chacune des classes peut ensuite se voir attribuer un niveau de service différent.

Lorsque les paquets traversent un réseau, chacun des périphériques du réseau identifie la classe de paquet et traite le paquet en fonction de cette classe.

Le trafic vocal des téléphones IP est généralement traité de manière préférentielle par rapport à tout autre trafic applicatif.

2.8.3.1. Classe de service

Une classe consiste à identifier, fonctionner et distinguer entre les flux de trafic spécifiques tel que la voix, la vidéo, réseau internet……etc

Une fois le trafic réseau est défini et trié (c'est-à-dire classifié), il sera marqué afin que tous l'équipement qu'il va traverser et qui applique la QoS n'est pas à le re-classifier à chaque fois.

L'architecture DiffServ propose d'utiliser le champ ToS (Type Of Service) dans l'en-tête des paquets IP pour identifier et coder les différentes classes de service. Ainsi, les 6 premiers bits de ce champ correspondront au Code de Service Différencié (Differentiated Service CodePoint, DSCP), qui contiendra l'identifiant de la classe à laquelle appartient le paquet.

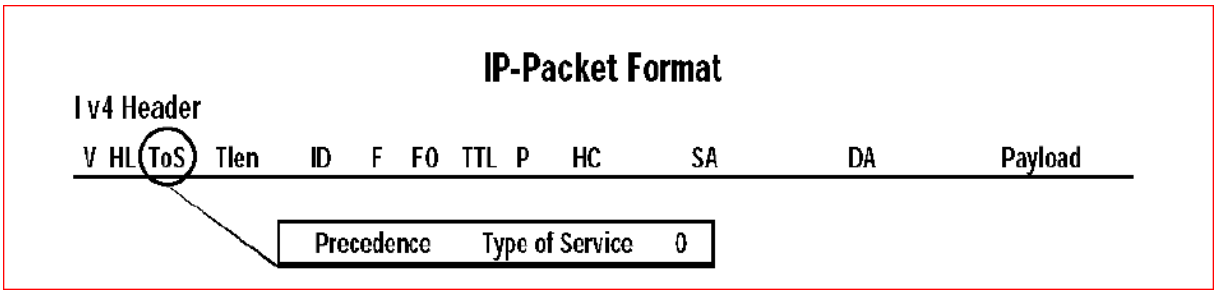

Figure 2.3-Format d'un paquet IP.

2.8.3.2. Avantages et Inconvénients du model DiffServ

DiffServ présente les principaux avantages suivants :

- Un modèle très évolutif.
- Il offre de nombreux niveaux de qualité.

DiffServ a aussi ces inconvénients :

- Aucune garantie absolue de qualité de service ne peut être faite.
- Cela nécessite un ensemble de mécanismes complexes.

2.9. Conclusion

Ce chapitre est constitué de deux parties ; la première partie consiste à définir le modèle OSI en présentant ses différentes couches, définir les protocoles LAN ainsi les serveurs réseau en terminant par le modèle hiérarchique à trois couches. La seconde partie est basé sur l'étude de la qualité de serviceen abordant les différents paramètres liés à la QoS, ses exigences, les différents mécanismes et les modèles déployés pour la mise en œuvre de la QoS ainsi leurs avantages et leurs inconvénients.

CHAPITRE 3 :

ORGANISME D'ACCEUIL

Nous consacrons ce chapitre à la présentation du groupe SONATRACH.

3.1. Introduction

Dans cette partie, nous présentons le groupe SONATRACH et sa structure hiérarchique, nous introduisons après le réseau de télécommunication et nous donnons un aperçu sur les équipements utilisés.

3.2. Historique de l'entreprise

SONATRACH « **S**ociété **N**ationale pour la Recherche, la Production, le **T**ransport, la Transformation, et la **C**ommercialisation des Hydrocarbures S.P.A »est la plus importante compagnie d'hydrocarbures en Algérie et en Afrique. Elle intervient dans l'exploration, la production, le transport par canalisations, la transformation et la commercialisation des hydrocarbures et de leurs dérivés depuis sa création le 31 décembre 1963.

Au fil des années,Sonatrach a adopté une stratégie de diversification en développant des activités de génération électrique, d'énergies nouvelles et renouvelables, de dessalement d'eau de mer, de recherche et d'exploitation minière. Poursuivant sa stratégie d'internationalisation, Sonatrach opère en Algérie et dans plusieurs régions du monde.

En 2008, l'entreprise est classée 1ère en Afrique et 12ème dans le monde, également 4ème exportateur mondial de GNL, 3ème exportateur mondial de GPL, et 5ème exportateur de Gaz Naturel.

Jusqu'à présent, SONATRACH est considérée comme une puissance internationale qui ne cesse d'évoluer.

3.3. Les activités de l'entreprise

Les activités que le groupe SONATRACH développe sur le plan international sont les suivantes :

- Exploration et production.
- Transport par canalisation.
- Liquéfaction et séparation.
- Raffinage et pétrochimie.
- Commercialisation.

Dans ce projet, on va faire le point sur l'activité de Transport par canalisation.

3.4. Transport par canalisation (TRC)

Considéré comme l'une des plus importantes activités de SONATRACH, elle a pour missions de développer le réseau d'infrastructures de transport par canalisations, de stockage, de chargement et déchargement à travers les infrastructures portuaires à quai et en haute mer. Elle assure le transport des hydrocarbures depuis les pôles de production au sud vers les pôles de demande et de transformation au nord (marché national et exportation).

Le premier projet lancé et réalisé par SONATRACH était l'oléoduc OZ1 reliant Haoud-El-Hamra à Arzew, en 1966.

Figure 3.1-Transport par canalisation.

L'activité Transport par Canalisation est regroupée en divisions :

- Division Exploitation.
- Division Maintenance.

Elle est assurée par cinq régions de transport à savoir :

- Région Transport Ain-Amenas RTI.
- Région Transport Haoud El Hamra RTH.
- Région Transport Centre Béjaia RTC.
- Région Transport Ouest Arzew RTO.
- Région de transport Est SKIKDA.

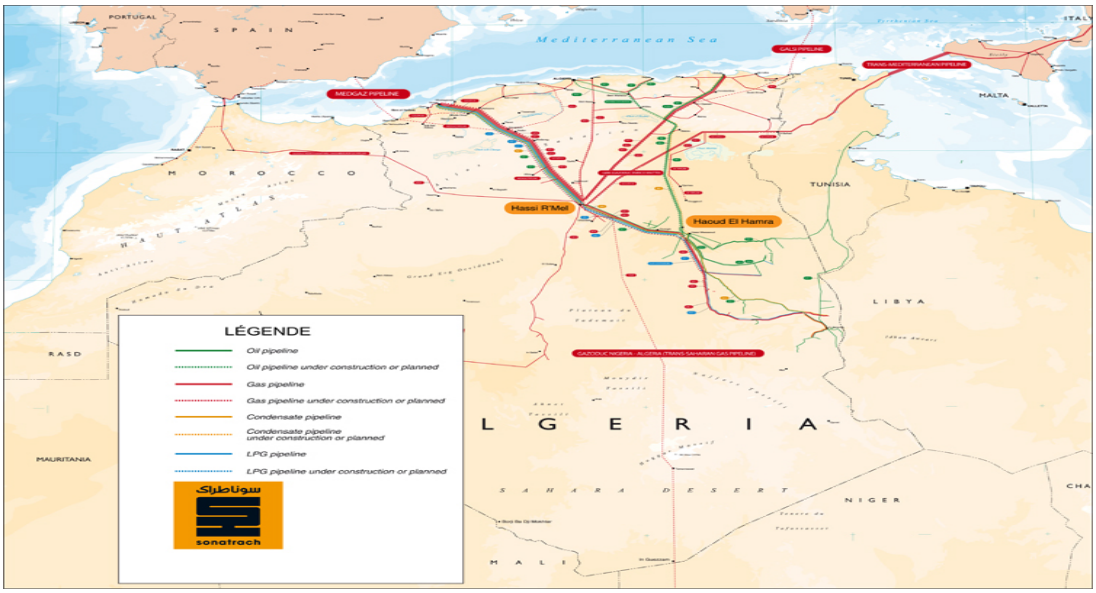

Figure 3.2-Réseau de transport par canalisation.

3.5. La direction régionale de Bejaia DRGB

La DRGB appelée aussi La Région Transport Centre Bejaïa (RTC)est l'une des cinq directions régionales de transport par canalisations des hydrocarbures (TRC).Elle a pour rôle de transporter, stocker et livrer les hydrocarbures liquides et gazeux. Elle est chargée de l'exploitation de deux oléoducs, d'un gazoduc et d'un port pétrolier.

- **Oléoduc Haoud-El-Hamra vers Bejaïa(OB124/22) :**C'est le premier pipe-line à être mis en place en Algérie. Des stations de pompages principales et satellites ont irrigués le long de l'axe :
  - Station de pompage de Haoud-El-Hamra(HEH) SP1.
  - Station de pompage de DJAMAA SP1 BIS.
  - Station de pompage de Biskra SP2.
  - Station de pompage de M'SILA SP3.

- **Oléoduc Beni-Mensour vers Alger (DOG1 20):** Il a une longueur de 130 Km et un diamètre de 16 pouces, prend en charge l'alimentation de la raffinerie d'Alger à partir de la station de pompage de Beni-Mansour.

- **Gazoduc HassiR'Mel vers Bordg-Menail:** Il alimenteen gaz naturel toutes les villes et pôles industriels du centre du pays depuis 1981.

- **Le port pétrolier de Bejaia :** Consacré aux hydrocarbures, il se compose de deux postes de chargement à partir d'un parc de pétrole brut composé de 16 bacs. Au niveau du trafic de pétrole brut et condensat, le port se positionne à la 3ème place en Algérie, après les ports d'Arzew et de Skikda.

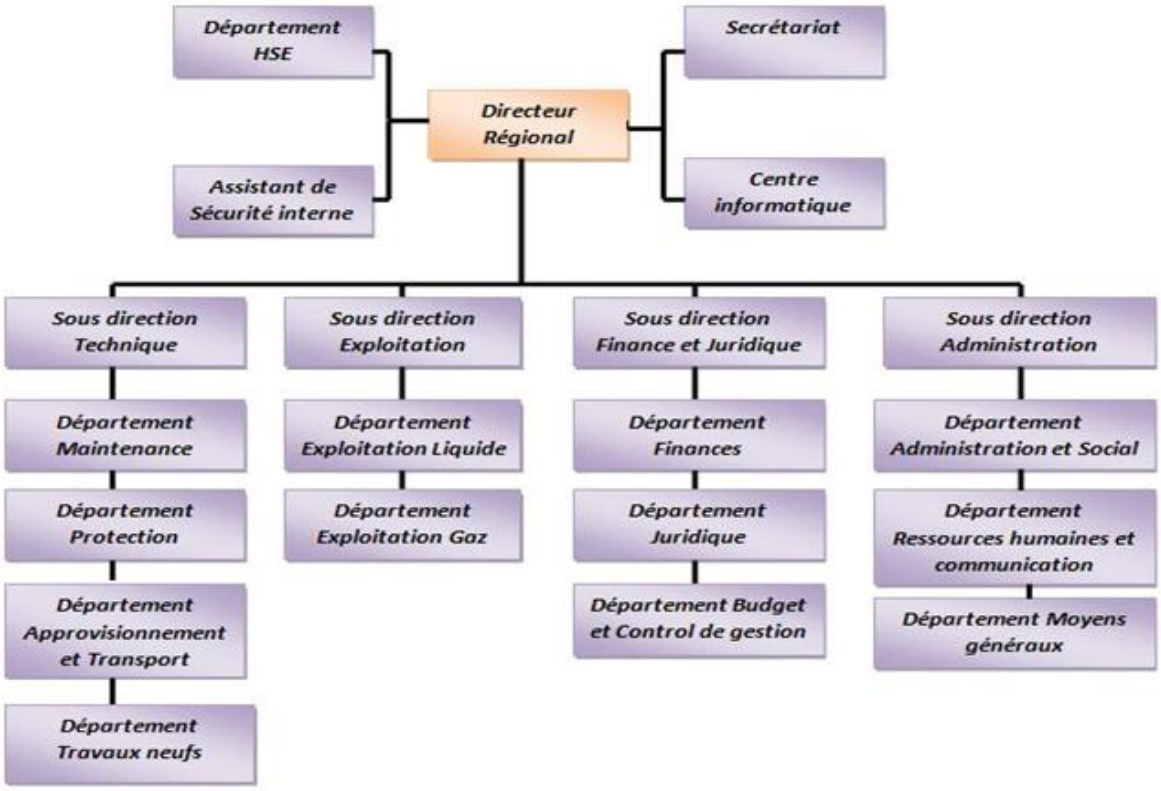

Figure 3.3-Organigramme de la RTC Bejaia.

3.6. Département maintenance(MTN)

Le département de maintenance est un élément très important au sein de l'entreprise SONATRACH**.** Il regroupe les différents services de l'entreprise et administre la gestion de ces derniers. Comme ilveille au maintien du bon état de fonctionnement des équipements et des installations techniques.

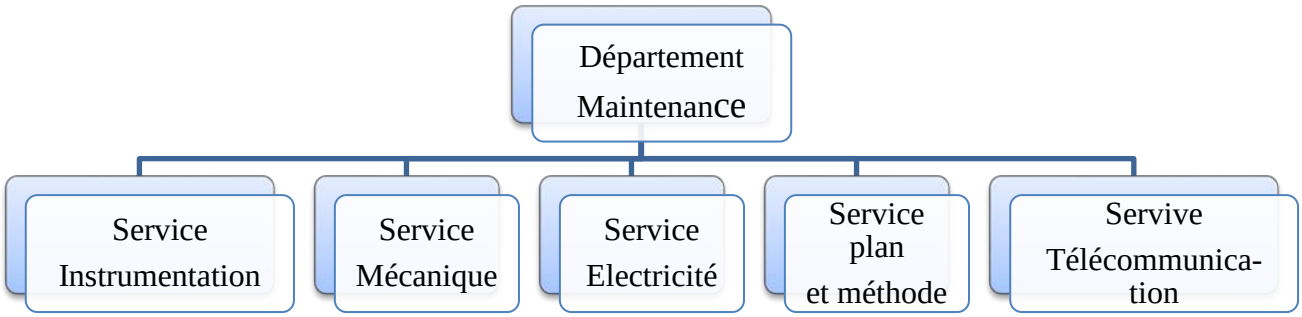

Figure 3.4-Organigramme du Département maintenance.

3.6.1. Service Télécommunication

Le transport des hydrocarbures depuis le pôle de production au sud HEH (HAOUD EL6HAMRA) vers le pôle de demande et de transformation au nord TMR (terminal marin de Bejaia (marché national e exportation)) nécessite une bonne transmission entre les stations.

La télécommunication indique l'ensemble des moyens techniques permettant la transmission à distance d'informations d'un point à un autre. Les télécommunications utilisent deux techniques : la transmission qui assure le transport de l'information et la commutation qui est la mise en relation de deux usagers.

Le service de télécom est non amputable au sein de l'entreprise SONATRACH vu sa mission principale d'assurer le bon fonctionnement des structures de la RTC et de ses activités ainsi que l'établissement d'une liaison permanente entre ses différents sièges (abonnées, stations…etc).

Ce service est composé de :

3.6.1.1. Réseau radio (MOTOROLA,CODANGP640)

La téléphonie occupe une place primordiale au sien de l'entreprise, c'est pour cela que la radio (Wireless) est un réseau indispensable notamment dans les situations où les fils téléphoniques sont en panne ou bien difficile à utiliser.

Figure 3.5-Radio.

Elle se compose de :

- **Un réseau HF :**La haute fréquence désigne les ondes radio dont la fréquence est comprise entre 3 MHz et 30 MHzet d'uneportée de plusieurs milliers km.
- **Un réseau radiocommunication VHF**
- **Un réseau radiocommunication UHF :** Permet les liaisons entre les différentes stations (mobile, portable, fixes).

3.6.1.2. Système commutation (Alcatel-Lucent)

La téléphonie représente une partie très importante au sein de l'entreprise, généralement composée d'un PABX (Private Automatic Branche Xchange), un répartiteur, des PC et des appareils téléphoniques tels que les post IP.

- **Le PABX (Private Automatice Branche Xchange)** : Le PABX est un autocommutateur téléphonique privé, permet de mettre en œuvre plusieurs fonctions comme les transferts d'appels ou conférences, fournis des services de couplage téléphonie-informatique, réduit leur cout unitaire, et gère les terminaux téléphoniques que ce soient des postes numériques ou analogiques. Son architecture hybride (circuit/voix sur IP) permet de garder la même infrastructure existante tout en bénéficiant des avantages de transport de la voix sur IP pour les communications inter site.

Figure 3.6-Armoire téléphone IP.

- **Téléphone IP (Alcatel –Lucent) :** Les téléphones IP sont des téléphones connectés en temps réel à d'autres équipements et applications. Ils offrent un ensemble complet de fonction de connectivité et de téléphonieIP, tout en regroupant les messages voix, e-mail et fax dans une seule et unique boite de réception multimédia.Ce type de téléphone offre des services très performantsen termes de fonctionnalités, de fiabilité et de qualité de service. [23]

Figure 3.7-Téléphone IP.

3.6.1.3. Système SCADA (Supervisory Control and Data Acquisition)

Le SCADA est un système de télémesure et de télé-contrôle, adopté par SONATRACH pour pallier aux exigences particulières de la gestion des puits, traite en temps réel un grand nombre de mesures et contrôle à distance les installations pétrolières. Grâce aux différentes fonctionnalités offertes par ce système, ce dernier peut être exploité afin de pallier aux problèmes liés à la production.

Figure 3.8-Armoire SCADA Terminal Arrivé Bejaia.

3.6.1.4. Système transmission par fibre optique (SAGEM, HUAWEI)

La fibre optique est un média puissant et l'un des plus rapides pour le transfert de données numériques. La transmission basée sur fibre optique assure l'échange ou le transport des informations utiles sur les trajets avec la meilleure qualité possible.

Le développement des applications sur internet et l'exposition du trafic qui en résulte demandent des transmissions et des équipements de réseaux de plus en plus performants. Sagem développe des solutions de transmissions et d'accès basées sur les technologies les plus performantes.

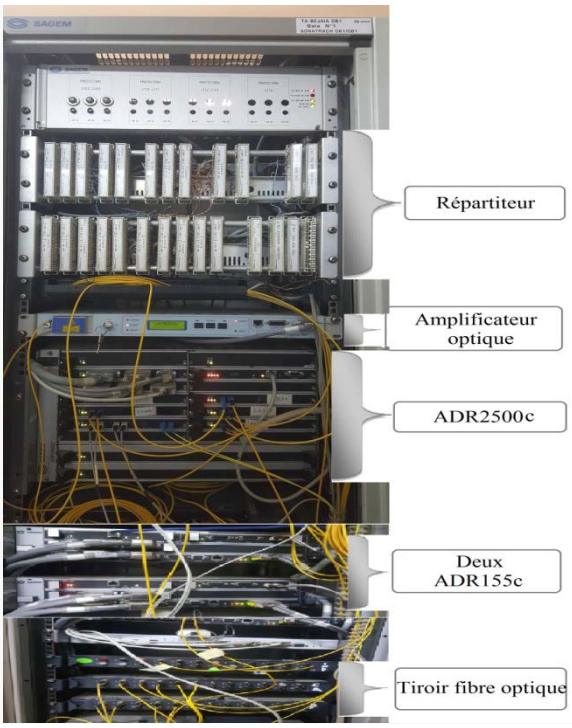

Figure 3.9-Equipements de transmissions fibre optique SAGEM.

- **L'ADR155c :** L'ADR155c (Add Drop Multiplexer 155 Mbit/s) est un multiplexeur STM1/STM4 utilisé pour construire des liaisons point à point STM1, des anneaux STM1/STM4 ou des réseaux maillés. Il assure le transport de liaison à 2 Mbit/s, 34 Mbit/s ou 45 Mbit/s, Ethernet et STM1. En outre, l'équipement est géré à partir d'un navigateur http soit : [3]

➢ Localement via son interface Ethernet.
➢ A distance par télé-exploitation.
➢ A partir du gestionnaire de réseau IONOS NMS avec un Protocol.
➢ SNMP qui permet la supervision globale du réseau.

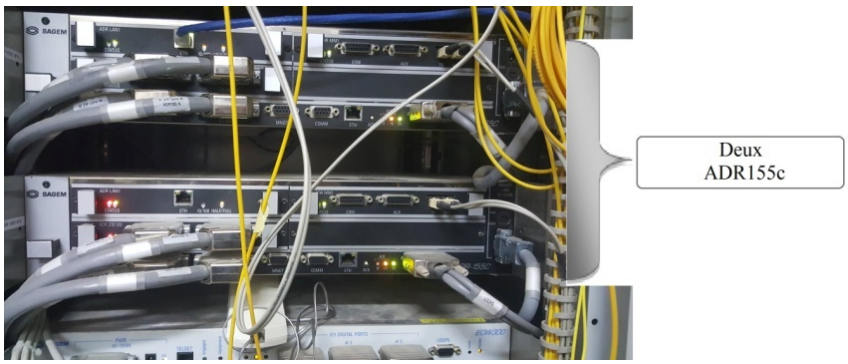

Figure 3.10-Equipement ADR155.

- **L'ADR 2500c [4]** :L'ADR2500c pour Add Drop Multiplexer 2500 Mbit/sa été conçu par SAGEM dans la continuité de SAGEM ADR 155c,est un multiplexeur add-drop optique STM-16 permettant de construire des liaisons point à point STM-16 (liaisons optique de la DRGB), des anneaux STM-16 ou des réseaux maillés. Il autorise le transport de 2 Mbit/s, 34 Mbit/s, 45 Mbit/s, 155 Mbit/s, 622 Mbit/s, Ethernet, Fast Ethernet, Gigabit Ethernet et Fibre Channel sur SDH.

L'ADR2500c peut être gérer :

- Par un terminal avec émulation VT100.
- Par un serveur HTTP.
- A distance par l'utilisation du protocole SNMP.

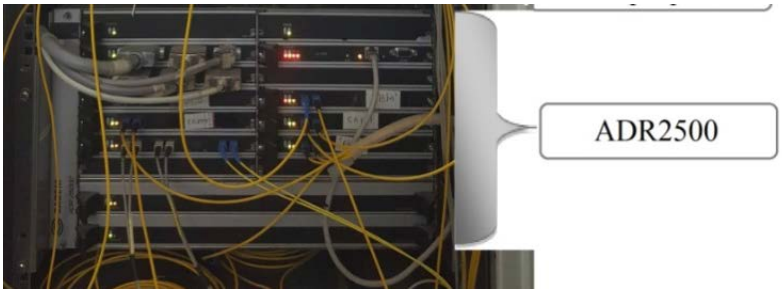

Figure 3.11-L'ADR2500c avec les différentes liaisons optiques.

- **SAGEM FMX12 [5] :** Brasseurs Multiplexeurs de circuit à 64 kbit/s et n*64 kbit/s assurent le regroupement, aiguillage, insertion/extraction et distribution d'information numérique, particulièrement adaptés à la réalisation de diverses formes de réseaux de transmission, les FMX sont spécialement conçu pour connecter les entreprises aux opérateurs.

Ils sont caractérisés par :

- **Panoplie complète d'interfaces :** les FMX disposent d'une grande variété d'interfaces normalisées : 2Mbits, RNIS, interfaces analogiques bas et haut débits et interfaces numériques.
- **Toute architecture de réseau :** les FMX s'adaptent à toutes les topologies (étoile et maillés) quel que soit le support (ligne cuivre, optique ou liaison hertzienne).
- **Flexible :** chaque FMX s configure sur mesure avec cartes de base ou carte d'interface selon les besoins.
- **Sécurité de fonctionnement :** de nombreux dispositifs garantissent le bon fonctionnement de l'équipement et assurent la surveillance de son environnement.

3.7. Architecture du réseau SONATRACH

Le réseau SONATRACH est constitué de deux Swicths cœur et des switchs d'accès répartis sur trois niveaux comme c'est illustré dans la figure suivante.

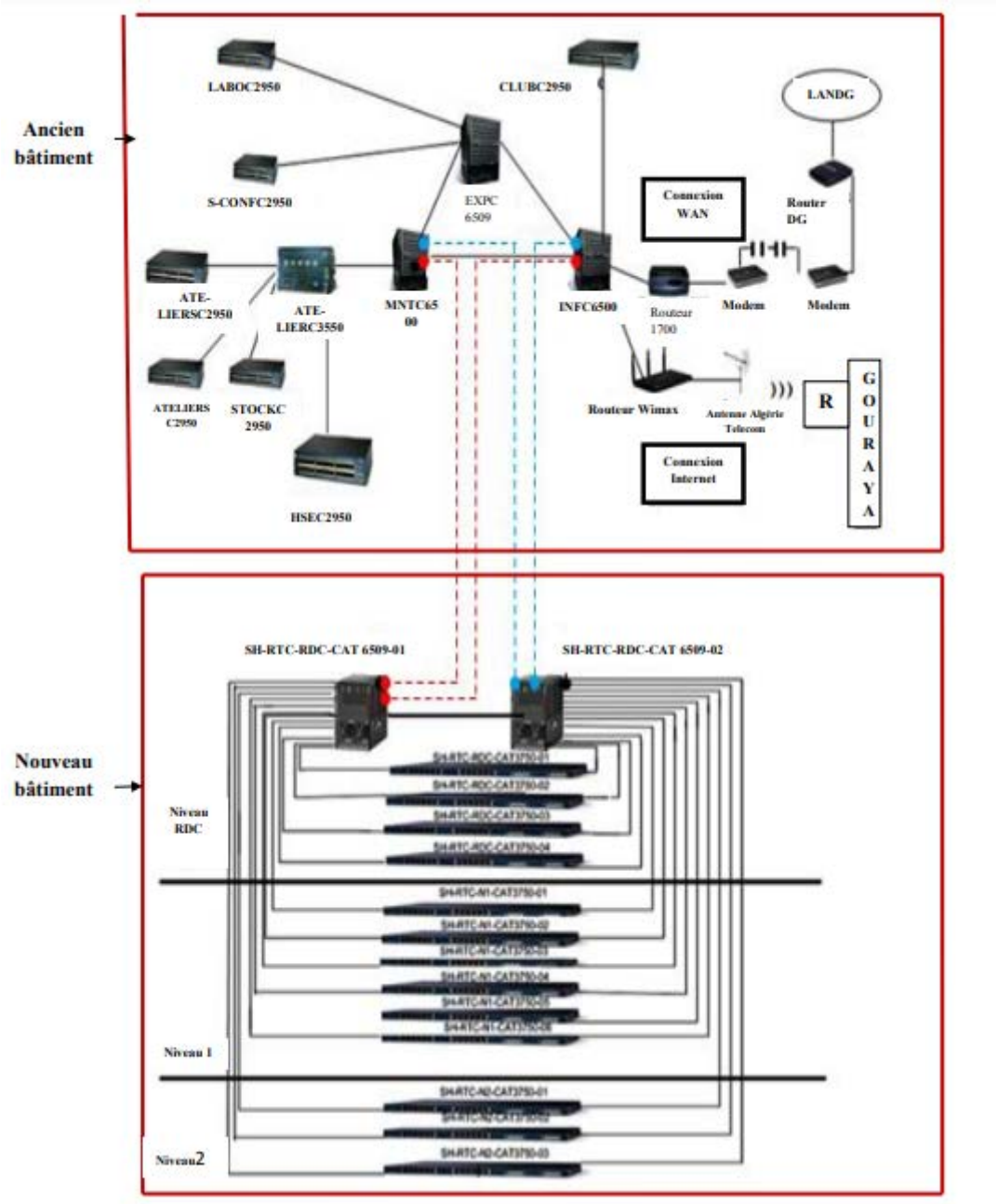

Figure 3.12-Liaison entre l'ancien et le nouveau bâtiment.

3.8. Présentation des équipements utilisés :

Pour réaliser notre réseau LAN nous avons utilisé les équipements qui sont récapitulés dans le tableau suivant :

Périphériques utilisés	Appellation
Commutateur cœur	Cisco Catalyst 3650
Commutateur Accès	Cisco Catalyst 3560
CME (Call Manager Express)	Routeur 2811
ISP (Internet Service Provider	Cloud PT
Terminal PC	Pc bureau, Laptop, TabletPC-PT
Téléphone IP	IP Phone 7960
Autre devices	Serveur, imprimante, AcessPoint

Tableau 3.1-Liste des équipements utilisés.

3.9. Nomination logique des équipements

Afin de faciliter la conception de notre réseau nous avons nommé les équipements par des noms significatifs, le tableau suivant indique les noms des équipements :

Couche cœur	Couche accès	équipements
Core1 Core2	Switch Accès 13	Laptop9, server0, server1, IP Phone0, IP Phone5
	Switch Accès 12	Merakiserver0, server2, IP Phone30, IP Phone31
	Switch Accès 11	Pc0, pc10, tablet-PC0, Laptop3, IP Phone32, IP phone33 ;accessPoint Répéteur
	Switch Accès 10	Pc2, Laptop3, printer, IP Phone7, IP Phone8
	Switch Accès 9	PC5(1),Laptop5(1),Laptop8,PC6(1) , IP Phone11, IP Phone12, IP Phone13
	Switch Accès 8	Laptop0,Laptop6,pc2,pc1,IP Phone14,IP Phone15,IP Phone16
	Switch Accès 7	Pc5,pc19,pc09,IP Phone17,IP Phone18,IP Phone19
	Switch Accès 6	pc5(2), pc6,printer2,Laptop1, IP Phone20, IP Phone21, IP Phone22
	Switch Accès 5	pc6(2), pc14, pc16,pc17, IP Phone23, IP Phone24, IP Phone25
	Switch Accès 4	Laptop5(2),Pc8,pc18,pc15,IP Phone26,IP Phone27,IP Phone28
	Switch Accès 3	Laptop7,pc7,pc12, pc13,IP Phone225,IP Phone226

	Switch Accès 2	Laptop4,pc11,IP Phone224
	Switch Accès 1	Pc4,Laptop022,printer,IP Phone221,IP Phone222,IP Phone224

Tableau 3.2-Nomination des équipements utilisés.

3.10. Conclusion

Ce chapitre a été axé sur la présentation de l’organisme d’accueil SONATRACH. Nous avons détaillé le département télécom à savoir ses services, les différents équipements utilisés, leurs nominations et nous avons présenté l’architecture globale du réseau SONATRACH qui sera réalisé dans le prochain chapitre.

CHAPITRE 4 :
CONCEPTION ET CONFIGURATION DU RESEAU SONATRACH

Ce chapitre est dédié à la conception et configuration du réseau SONATRACH, en se basant sur le simulateur Cisco Packet Tracer. Ainsi qu'à la vérification des résultats de configuration.

4.1. Introduction

Ce présent chapitre consiste en la présentation de la réalisation de l'architecture du réseau SONATRACH, en exposant les différentes configurations nécessaires à implémenter, en se basant sur le simulateur Cisco Packet Tracer.

Pour présenter les configurations que nous avons réalisées ,des étapes de configuration suivies des tests de validation sont illustrés .

4.2. Présentation de l'environnement de travail (Packet Tracer)

Packet Tracer est un simulateur de réseau puissant, développé par Cisco Système, permettant de construire un réseau physique virtuel et offre la possibilité de simuler le comportement des protocoles réseaux en temps réel. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs…etc. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux de configurer les adresses IP, les services disponibles, etc….

La figure ci-contre présente l'interface principale du simulateur Cisco Packet Tracer.

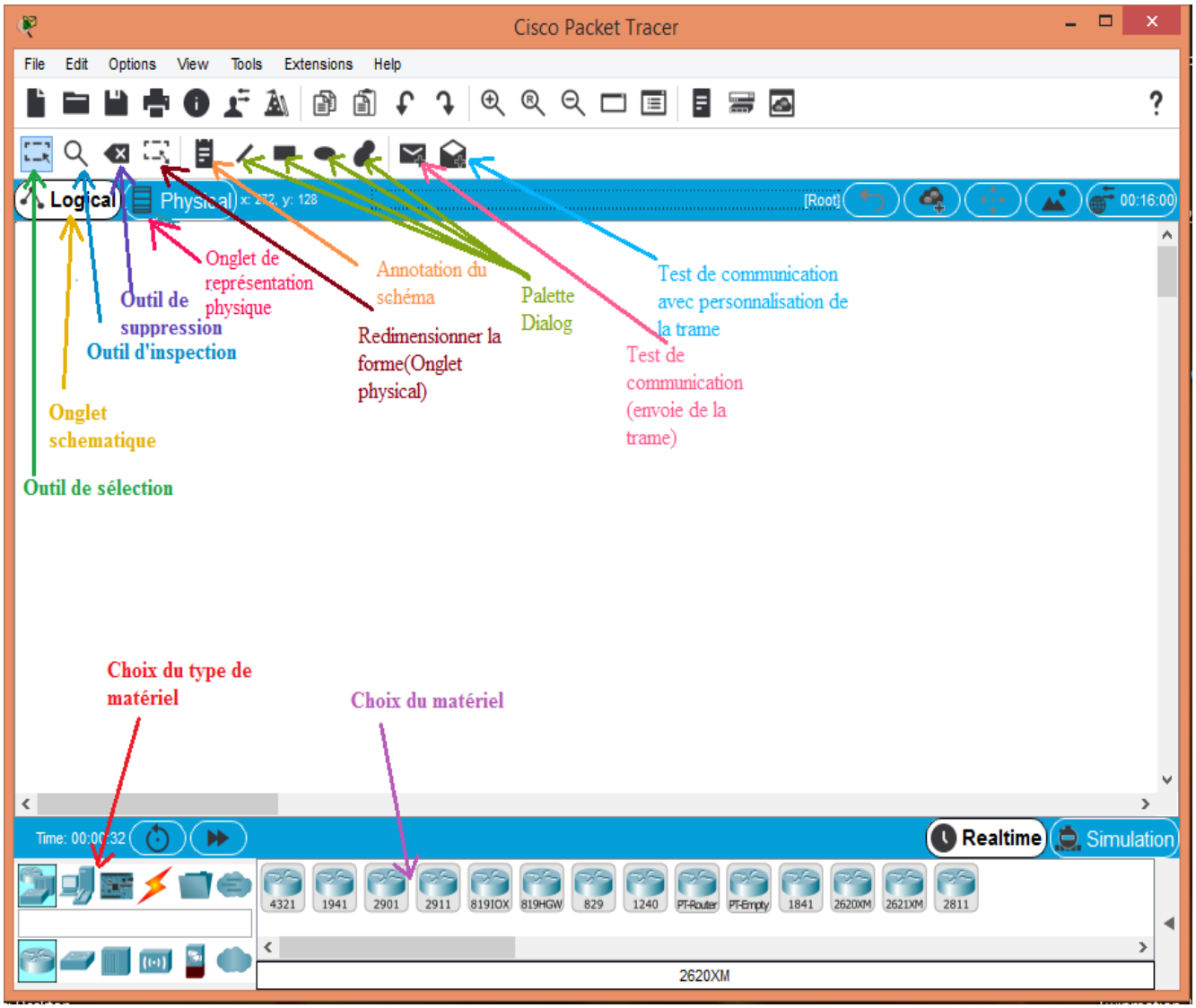

Figure 4.1-Présentation de l'écran principal.

4.3. Présentation de l'architecture du réseau sous Packet Tracer

La figure ci-dessous illustre l'architecture du réseau local que nous avons réalisé en se basant sur l'architecture du réseau SONATRACH avant configuration :

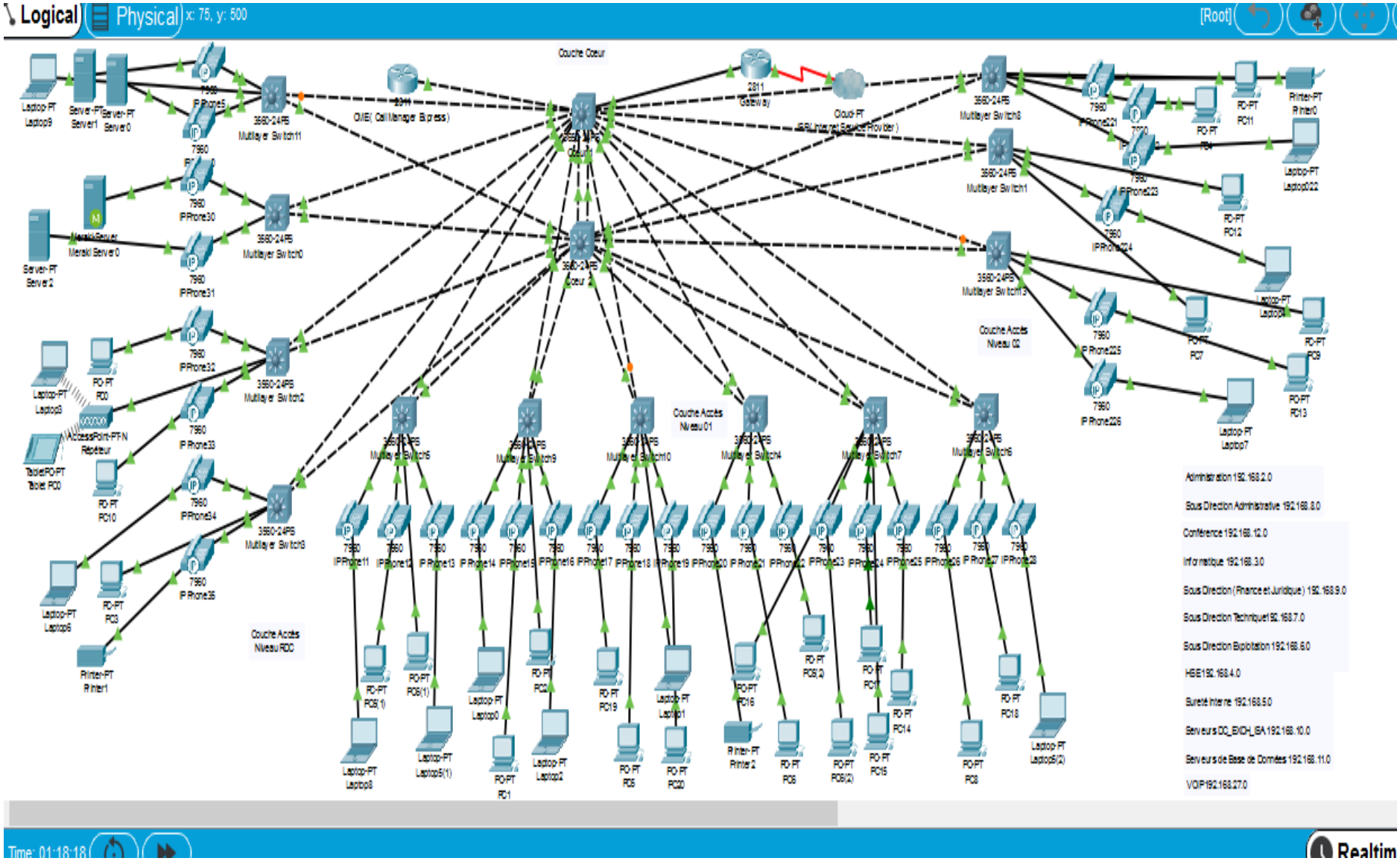

Figure 4.2-Architecture du réseau local avant configuration.

4.4. Segmentation VLANs

Le réseau a été réparti en plusieurs sections dont chacune représente un VLAN. Par conséquent, il y'aura naissance de 12 VLANs à savoir :

- Administration.
- Informatique.
- HSE.
- Sûreté interne.
- Sous-Direction exploitation.
- Sous-Direction technique.
- Sous-Direction administrative.
- Sous-Direction finance et juridique.
- Conférence.
- Sureté internet.
- Serveurs DC-EXCH.
- Serveurs de base de données.
- VoIP.

4.5. Adressage des VLANs

L'adresse du réseau est 192.168.0.0/24 avec une possibilité de création de 255 sous-réseaux, avec un masque 255.255.255.0, la répartition se fera comme suite :

Nom du VLAN	VLAN-ID	Adresse sous-réseau	Description
Administration	2	192.168.2.0/24	Vlan pour section direction administrative
Informatique	3	192.168.3.0/24	Vlan pour section Informatique
HSE	4	192.168.4.0/24	Vlan pour section HSE
Sureté Internet	5	192.168.5.0/24	Vlan pour section sureté Internet
Sous-Direction exploitation	6	192.168.6.0/24	Vlan pour section Sous-Direction exploitation
Sous-Direction technique	7	192.168.7.0/24	Vlan pour section Sous-Direction technique
Sous-direction administrative	8	192.168.8.0/24	Vlan pour section Sous-direction administrative
Sous-direction finance & juridique	9	192.168.9.0/24	Vlan pour section Sous-direction finance & juridique
Serveurs DC-EXCH	10	192.168.10.0/24	Vlan pour section Serveurs DC-EXCH
Serveurs de base de Données	11	192.168.11.0/24	Vlan pour section Serveurs de base de Données
Conférence	12	192.168.12.0/24	Vlan pour section Conférence
VOIP	27	192.168.27.0/24	Vlan pour section VOIP

Tableau 4.1-Liste des noms VLANs du réseau et leur plan d'adressage.

4.6. Configuration du réseau local

4.6.1. Interface commande de Packet Tracer

L'interface de commande CLI (Command Langage Interface) est une interface du simulateur Packet Tracer qui permet la configuration des équipements du réseau et qui se fait à l'aide des commandes spécifiques introduites par l'utilisateur du logiciel.

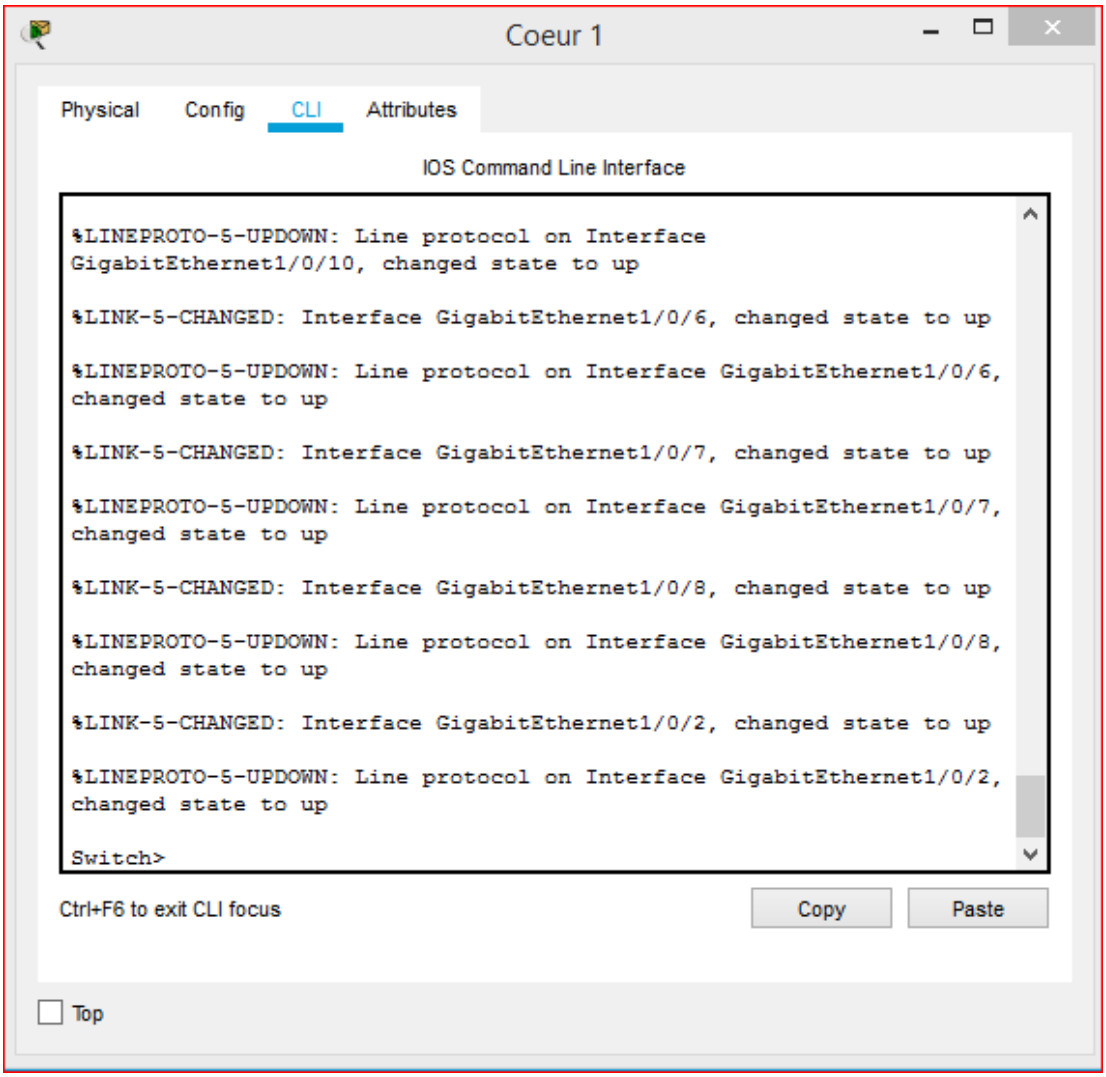

Figure 4.3-Interface CLI. Source : Auteur; 2019.

4.6.2. Configuration des équipements :

La configuration des équipements du réseau se fera au niveau des switchs de niveau 2 et niveau 3, d'un router CME de niveau 3, des téléphones IP, PCs et serveurs. Ces équipements constituent le réseau local des stations.

Un exemple de configuration de chaque équipement sera montré par la suite.

4.6.2.1. Configuration des Hostname

Cette configuration consiste à renommer les équipements par des noms significatifs, prenons comme exemple la nomination d'un switch cœur comme le montre la figure ci-dessous.

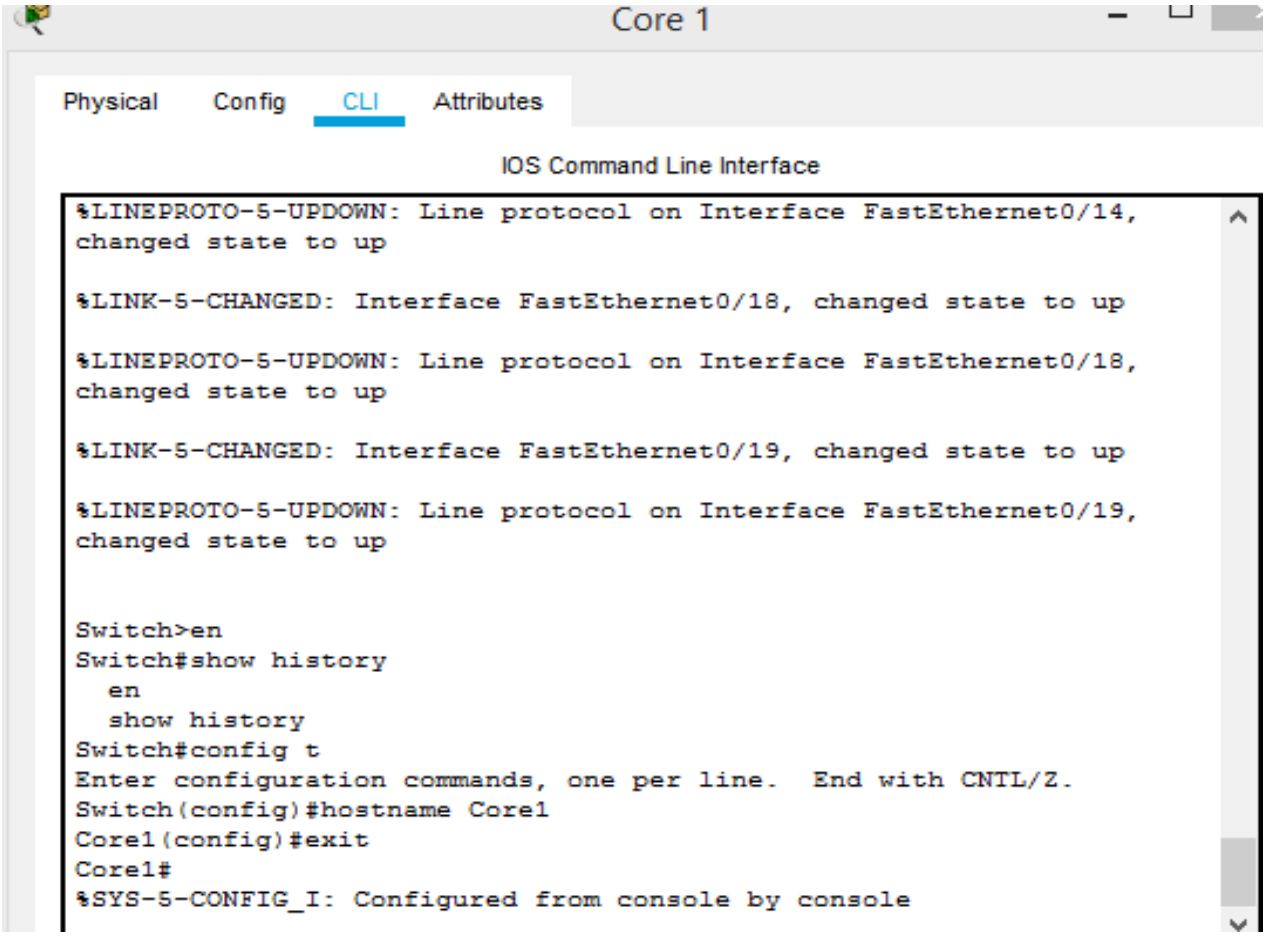

Figure 4.4-Configuration du Hostname.

4.6.2.2. Configurations des VLANS

La configuration des VLANs est une étape primodiale permettant la segmentation du réseau en plusieurs sections et qui se fait selon les étapes suivantes.

4.6.2.2.1. Création des VLANs :

La création des VLANs est faite au niveau des switchs Multilayer qui dans notre réseau représente les switchs cœurs comme le montre la figure suivante :

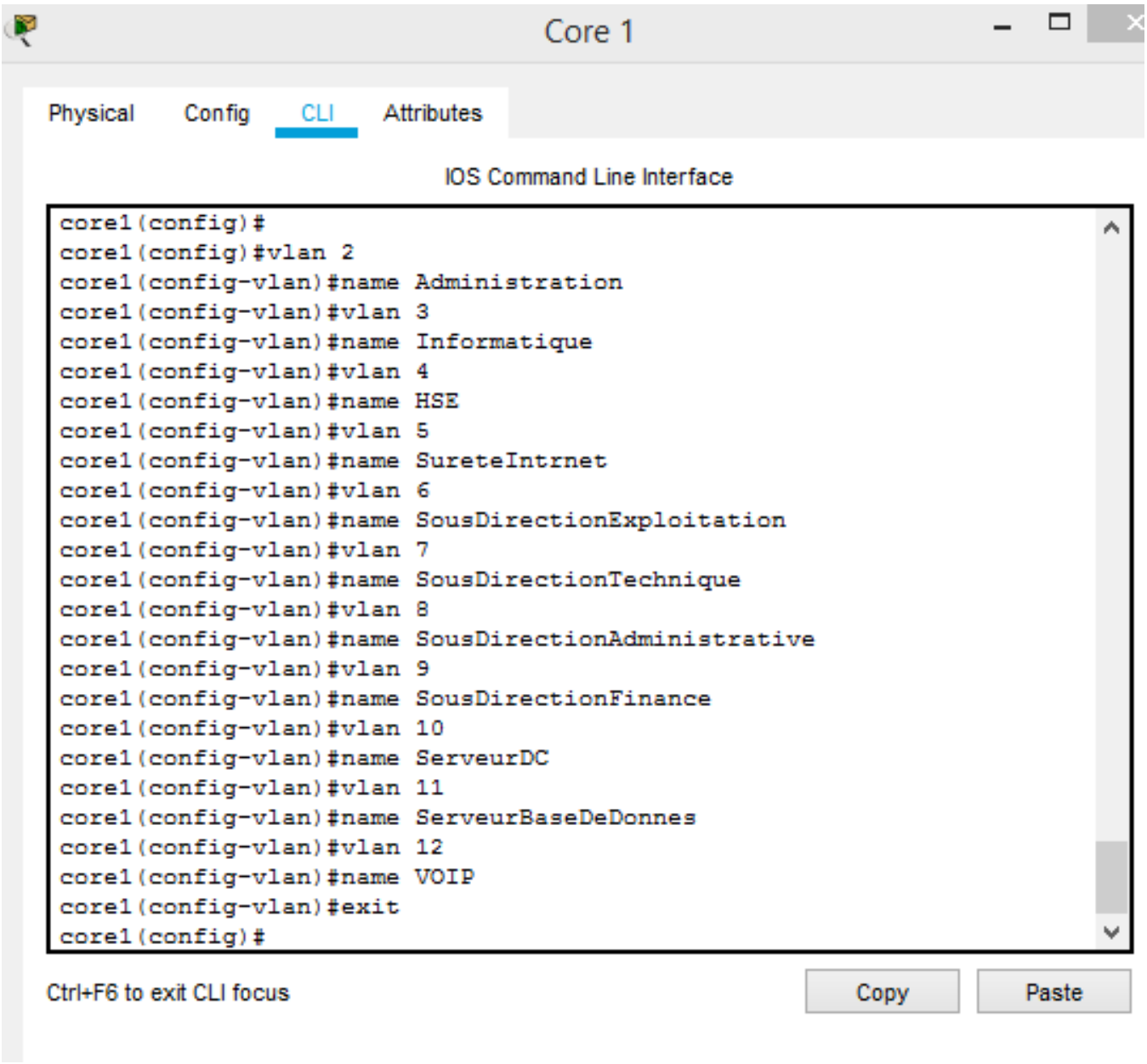

Figure 4.5-Création des VLANs.

4.6.2.2.2. Configuration des interfaces VLANs

La configuration des interfaces VLANs est faite au niveau des switchs cœurs en affectant des adresses IP pour chaque VLAN.

```
Core1(config)#int vlan 2
Core1(config-if)#ip address 192.168.2.1 255.255.255.0
Core1(config-if)#int vlan 3
Core1(config-if)#ip address 192.168.3.1 255.255.255.0
Core1(config-if)#int vlan 4
Core1(config-if)#ip address 192.168.4.1 255.255.255.0
Core1(config-if)#int vlan 5
Core1(config-if)#ip address 192.168.5.1 255.255.255.0
Core1(config-if)#int vlan 6
Core1(config-if)#ip address 192.168.6.1 255.255.255.0
Core1(config-if)#int vlan 7
Core1(config-if)#ip address 192.168.7.1 255.255.255.0
Core1(config-if)#int vlan 8
Core1(config-if)#ip address 192.168.8.1 255.255.255.0
Core1(config-if)#int vlan 9
Core1(config-if)#ip address 192.168.9.1 255.255.255.0
Core1(config-if)#int vlan 10
Core1(config-if)#ip address 192.168.10.1 255.255.255.0
Core1(config-if)#int vlan 11
Core1(config-if)#ip address 192.168.11.1 255.255.255.0
Core1(config-if)#int vlan 12
Core1(config-if)#ip address 192.168.12.1 255.255.255.0
core1 (config)#interface vlan 27
core1 (config-if)#ip address 192.168.27.1 255.255.255.0
core1 (config-if)#ip help
core1 (config-if)#ip helper-address 192.168.99.1
core1 (config-if)#exit
```

Figure 4.6-Configuration des interfaces VLAN.

Il faut ensuite activer le routage inter-VLAN

```
Core1(config-if)#exit
Core1(config)#ip routing
Core1(config)#ip route 0.0.0.0 0.0.0.0 0.0.0.0
Core1(config)#exit
Core1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 4.7-Routage inter-VLANs.

4.6.2.2.3. Configuration du DHCP

Le DHCP consiste à attribuer des adresses IP aux utilisateurs de façon dynamique au lieu de les configurer sur chaque poste client. La figure suivante illustre les commandes qui permettent de configurer ce protocole :

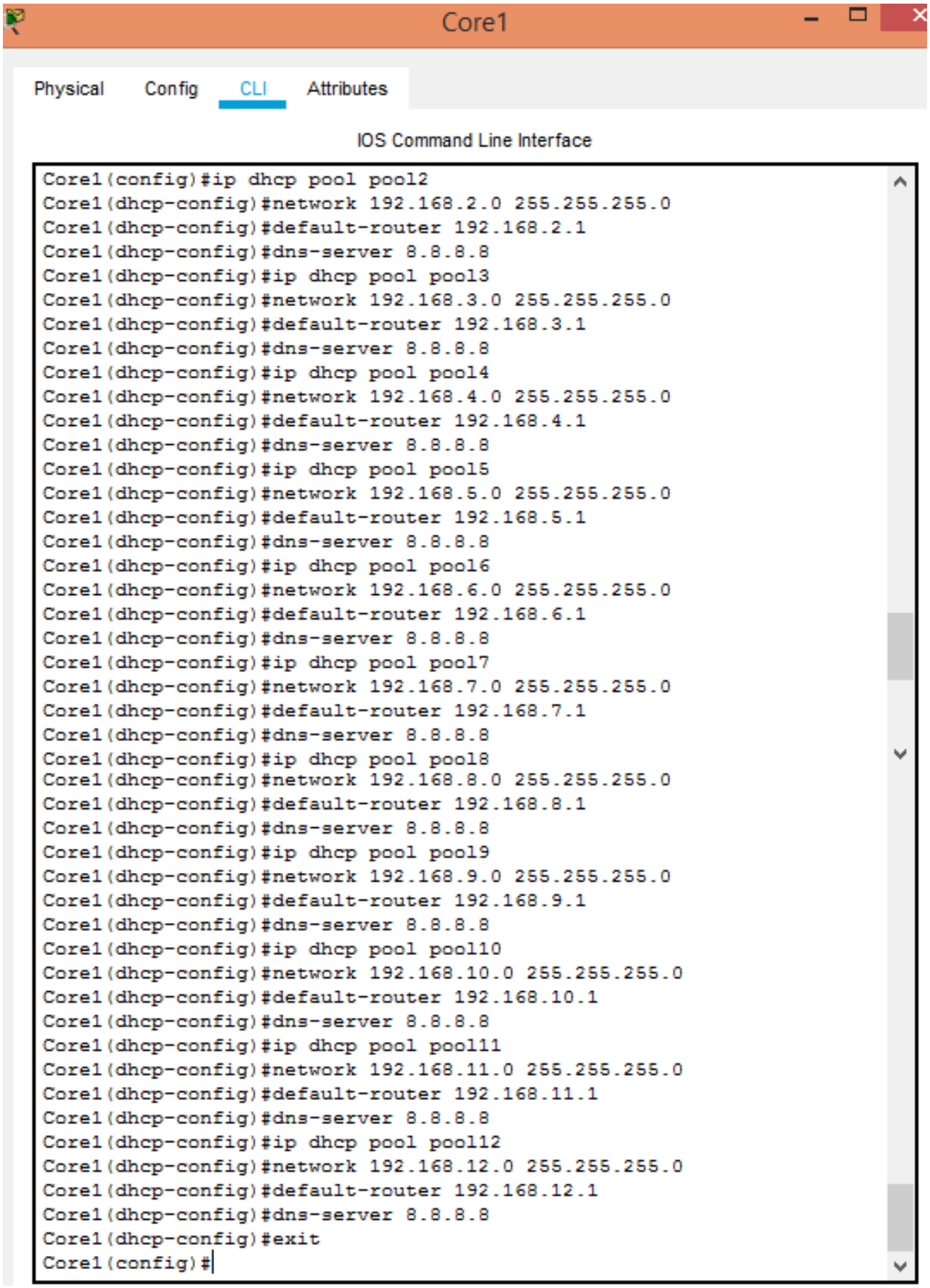

Figure 4.8-Configuration du DHCP.

4.6.2.2.4. Configuration des liens Trunk

Les liens Trunk existent entre l'ensemble des switchs d'accès et les switchs cœurs. Les commandes suivantes permettent la configuration en mode Trunk en s'appuyant sur la commande range qui pourra réunir toutes les interfaces en une seule fois.

```
Core1(config)#
Core1(config)#int range f0/23-24
Core1(config-if-range)#switchport trunk encapsulation dot1q
Core1(config-if-range)#switchport voice vlan 27
Core1(config-if-range)#exit
Core1(config)#
```

Figure 4.9-Configuration des interfaces du cœur en mode Trunk.

```
SwichAcce1>en
SwichAcce1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwichAcce1(config)#int range f0/1-2
SwichAcce1(config-if-range)#switchport mode trunk
SwichAcce1(config-if-range)#switchport voice vlan 27
SwichAcce1(config-if-range)#exit
SwichAcce1(config)#
```

Figure 4.10-Configuration des interfaces du switch d'accès en mode Trunk.

4.6.2.2.5. Attribution des ports des commutateurs au VLANs

Après avoir nommé les VLANs, on va assigner les ports au différents VLANs existants. L'affectation se fait au niveau des switchs d'accès.

Les commandes suivantes nous permettent d'associer les ports aux VLANs en mode Accès.

```
SwichAcce1(config)#
SwichAcce1(config)#int range f0/3-9
SwichAcce1(config-if-range)#switchport mode access
SwichAcce1(config-if-range)#switchport access vlan 2
SwichAcce1(config-if-range)#switchport voice vlan 27
SwichAcce1(config-if-range)#exit
SwichAcce1(config)#int range f0/3-9
SwichAcce1(config-if-range)#switchport mode access
SwichAcce1(config-if-range)#switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
SwichAcce1(config-if-range)#switchport access vlan 3
SwichAcce1(config-if-range)#switchport access vlan 27
SwichAcce1(config-if-range)#exit
SwichAcce1(config)#int f0/10
SwichAcce1(config-if)#switchport mode access
SwichAcce1(config-if)#switchport voice vlan 27
SwichAcce1(config-if)#exit
SwichAcce1(config)#
```

Figure 4.11-Configuration des interfaces du switch d'accès en mode Trunk.

4.6.2.2.6. Configuration du routeur CME

Le call manager nous a permis de configurer les téléphones IP en leurs attribuant des numéros et ceci à travers le DHCP et des commandes spécifiques afin d'établir la connexion entre tous les téléphones existants dans notre réseau.

La figure suivante illustre l'activation du routage pour tous les VLANs existans dans le réseau :

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CME
CME(config)#
CME(config)#interface FastEthernet0/0
CME(config-if)#ip address 192.168.99.1 255.255.255.0
CME(config-if)#ip address 192.168.99.1 255.255.255.0
CME(config-if)#no shutdown
CME(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

CME(config-if)#exit
CME(config)#ip dhcp pool VLAN27
CME(dhcp-config)#network 192.168.27.0 255.255.255.0
CME(dhcp-config)#default-router 192.168.27.1
CME(dhcp-config)#option 150 ip 192.168.99.1
CME(dhcp-config)#ip dhcp excluded-address 192.168.27.1
CME(config)#ip route 192.168.27.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.2.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.3.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.4.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.5.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.6.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.7.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.8.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.9.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.10.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.11.0 255.255.255.0 192.168.99.2
CME(config)#ip route 192.168.12.0 255.255.255.0 192.168.99.2
CME(config)#
```

Figure4. 12-Configuration du CME. Source : Auteur; 2019.

La figure si dessous montre les commandes nécessaires pour l'affectation des numéros aux téléphones IP :

```
CME(config)#telephony-service
CME(config-telephony)#max-ephones 32
CME(config-telephony)#max-dn 32
CME(config-telephony)#ip source-address 192.168.99.1 port 2000
CME(config-telephony)#auto assign 1 to 33
CME(config-telephony)#ephone-dn 1
CME(config-ephone-dn)#number 1001
CME(config-ephone-dn)#ephone-dn 2
CME(config-ephone-dn)#number 1002
CME(config-ephone-dn)#ephone-dn 3
CME(config-ephone-dn)#number 1003
CME(config-ephone-dn)#ephone-dn 4
CME(config-ephone-dn)#number 1004
CME(config-ephone-dn)#ephone-dn 5
CME(config-ephone-dn)#number 1005
CME(config-ephone-dn)#ephone-dn 6
CME(config-ephone-dn)#number 1006
CME(config-ephone-dn)#ephone-dn 7
CME(config-ephone-dn)#number 1007
CME(config-ephone-dn)#ephone-dn 8
CME(config-ephone-dn)#number 1008
CME(config-ephone-dn)#ephone-dn 9
CME(config-ephone-dn)#number 1009
CME(config-ephone-dn)#ephone-dn 10
CME(config-ephone-dn)#number 1010
CME(config-ephone-dn)#ephone-dn 11
CME(config-ephone-dn)#number 1011
CME(config-ephone-dn)#ephone-dn 12
CME(config-ephone-dn)#number 1012
CME(config-ephone-dn)#ephone-dn 13
CME(config-ephone-dn)#number 1013
CME(config-ephone-dn)#ephone-dn 14
CME(config-ephone-dn)#number 1014
CME(config-ephone-dn)#ephone-dn 15
CME(config-ephone-dn)#number 1015
CME(config-ephone-dn)#ephone-dn 16
CME(config-ephone-dn)#number 1016
CME(config-ephone-dn)#ephone-dn 17
CME(config-ephone-dn)#number 1017
CME(config-ephone-dn)#ephone-dn 18
CME(config-ephone-dn)#number 1018
CME(config-ephone-dn)#ephone-dn 19
CME(config-ephone-dn)#number 1019
CME(config-ephone-dn)#ephone-dn 20
CME(config-ephone-dn)#number 1020
CME(config-ephone-dn)#ephone-dn 21
CME(config-ephone-dn)#number 1021
CME(config-ephone-dn)#ephone-dn 22
CME(config-ephone-dn)#number 1022
CME(config-ephone-dn)#ephone-dn 23
CME(config-ephone-dn)#number 1023
CME(config-ephone-dn)#ephone-dn 24
CME(config-ephone-dn)#number 1024
CME(config-ephone-dn)#ephone-dn 26
CME(config-ephone-dn)#number 1026
CME(config-ephone-dn)#ephone-dn 27
CME(config-ephone-dn)#number 1027
CME(config-ephone-dn)#ephone-dn 28
CME(config-ephone-dn)#number 1028
CME(config-ephone-dn)#ephone-dn 29
CME(config-ephone-dn)#number 1029
CME(config-ephone-dn)#ephone-dn 30
CME(config-ephone-dn)#number 1030
CME(config-ephone-dn)#ephone-dn 31
CME(config-ephone-dn)#number 1031
CME(config-ephone-dn)#ephone-dn 32
```

Figure 4.13-Attribution des numéros aux téléphones IP.

4.6.2.2.7. Configuration du router Gateway

Ce router joue le rôle d'un fournisseur internet sa configuration et la suivante

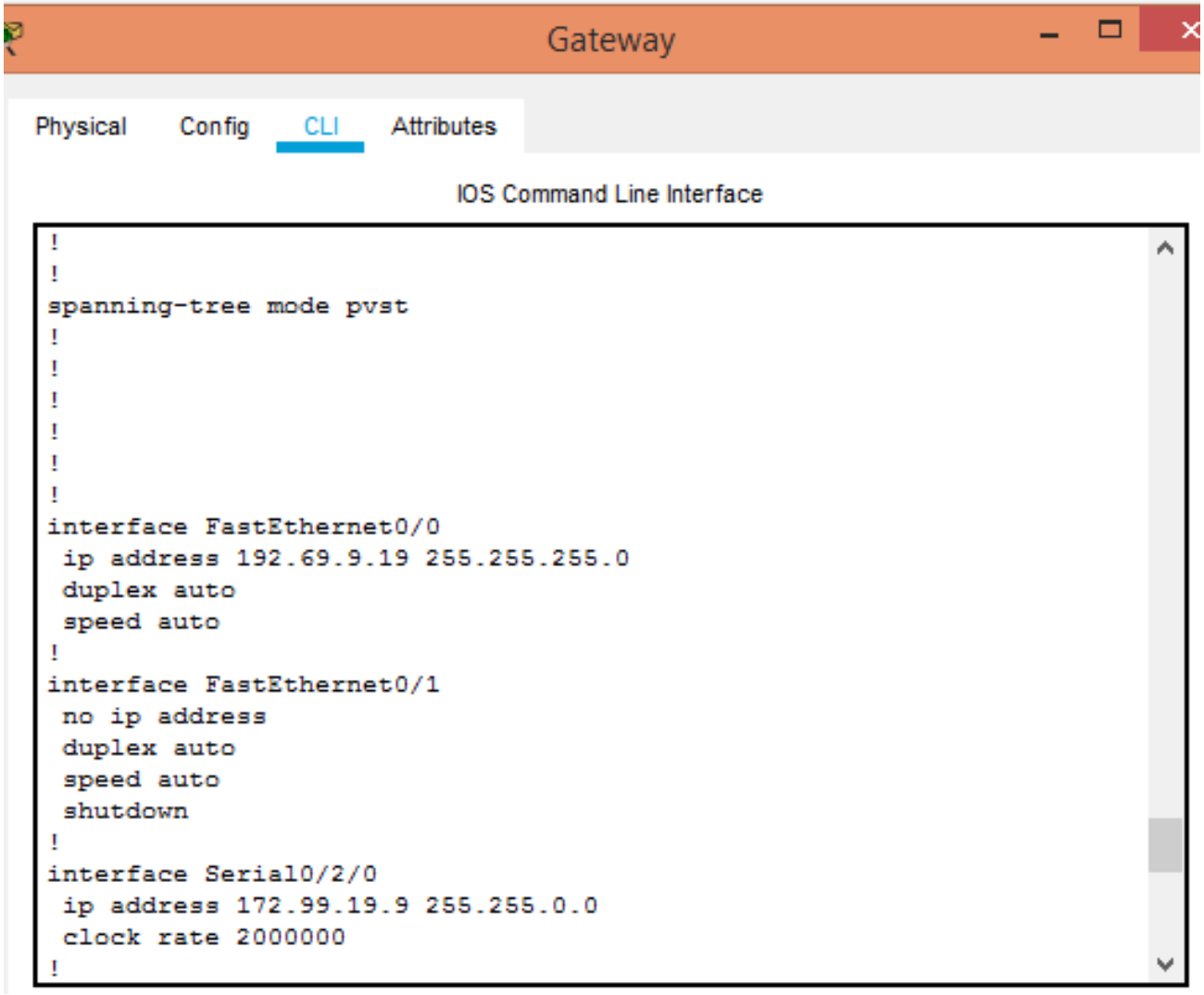

Figure 4.14-Configuration du Gateway.

4.7. Vérifications et tests de validation

4.7.1. Vérifications

Dans cette partie, nous avons vérifié la configuration de tous les équipements à l'aide des commandes de vérification.

La figure suivante montre le réseau LAN après avoir créé les VLANs et effectué la configuration pour assurer le bon fonctionnement entre les différentes entités.

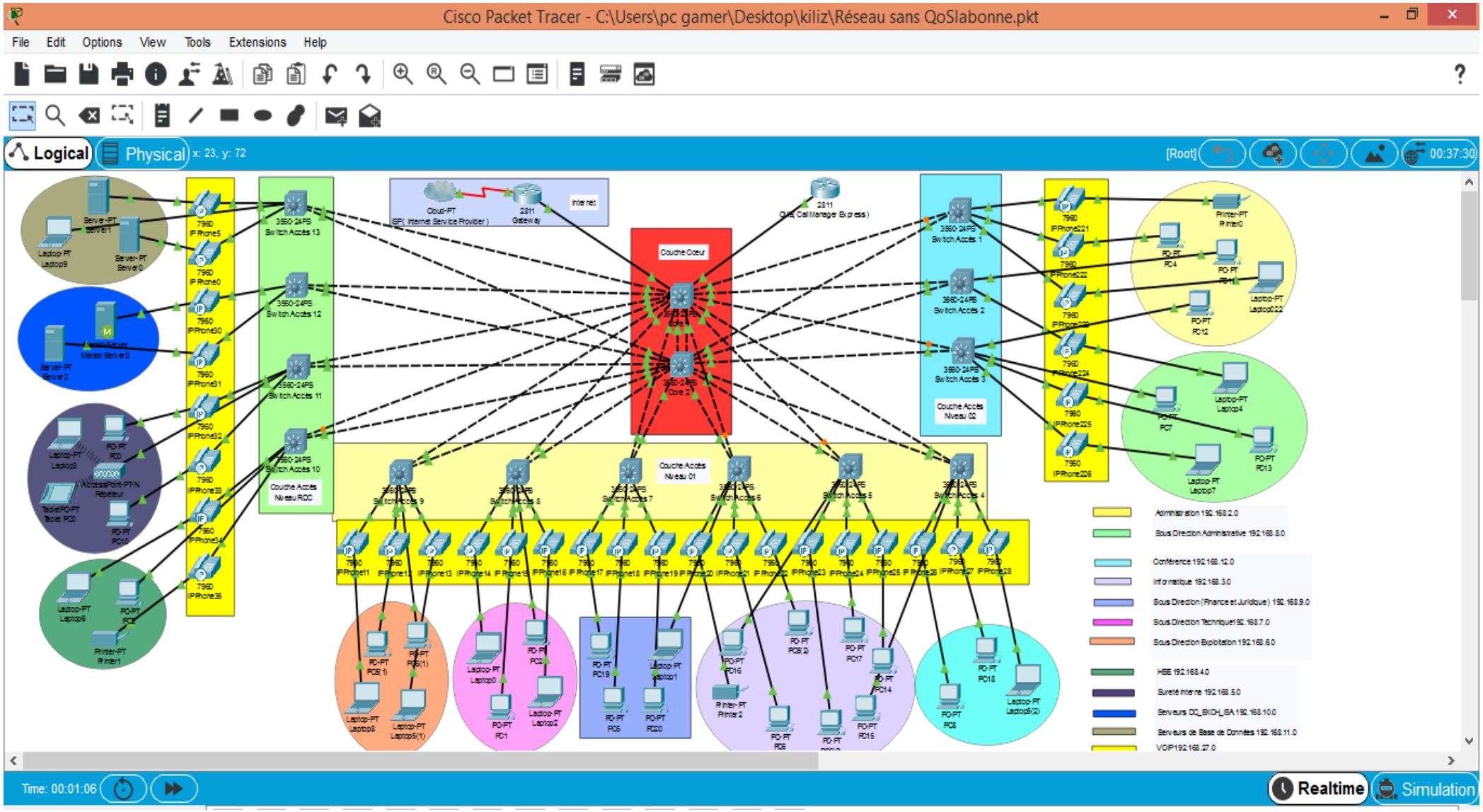

Figure 4.15-Architecture configurée.

4.7.1.1. Vérification du routage inter-VLANs

Cela est fait à l'aide de la commande **show IP interface brief.**

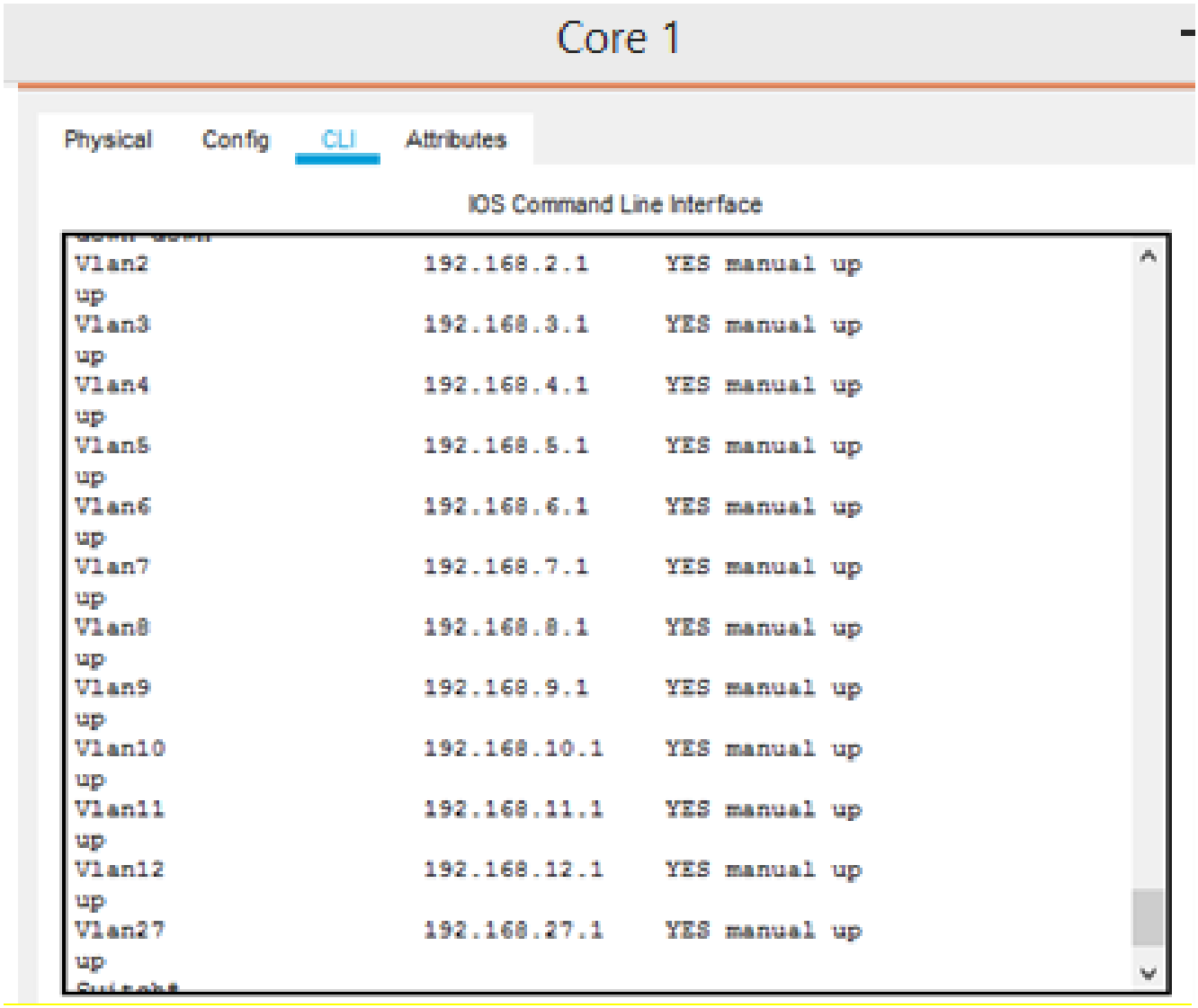

Figure 4.16-Vérification du routage inter-VLANs.

4.7.1.2. Vérification de la distribution des adresses IP avec le DHCP

La commande **show ip dhcp binding** nous permet de vérifier si les adresses IP ont été attribuées automatiquement grâce au serveur DHCP.

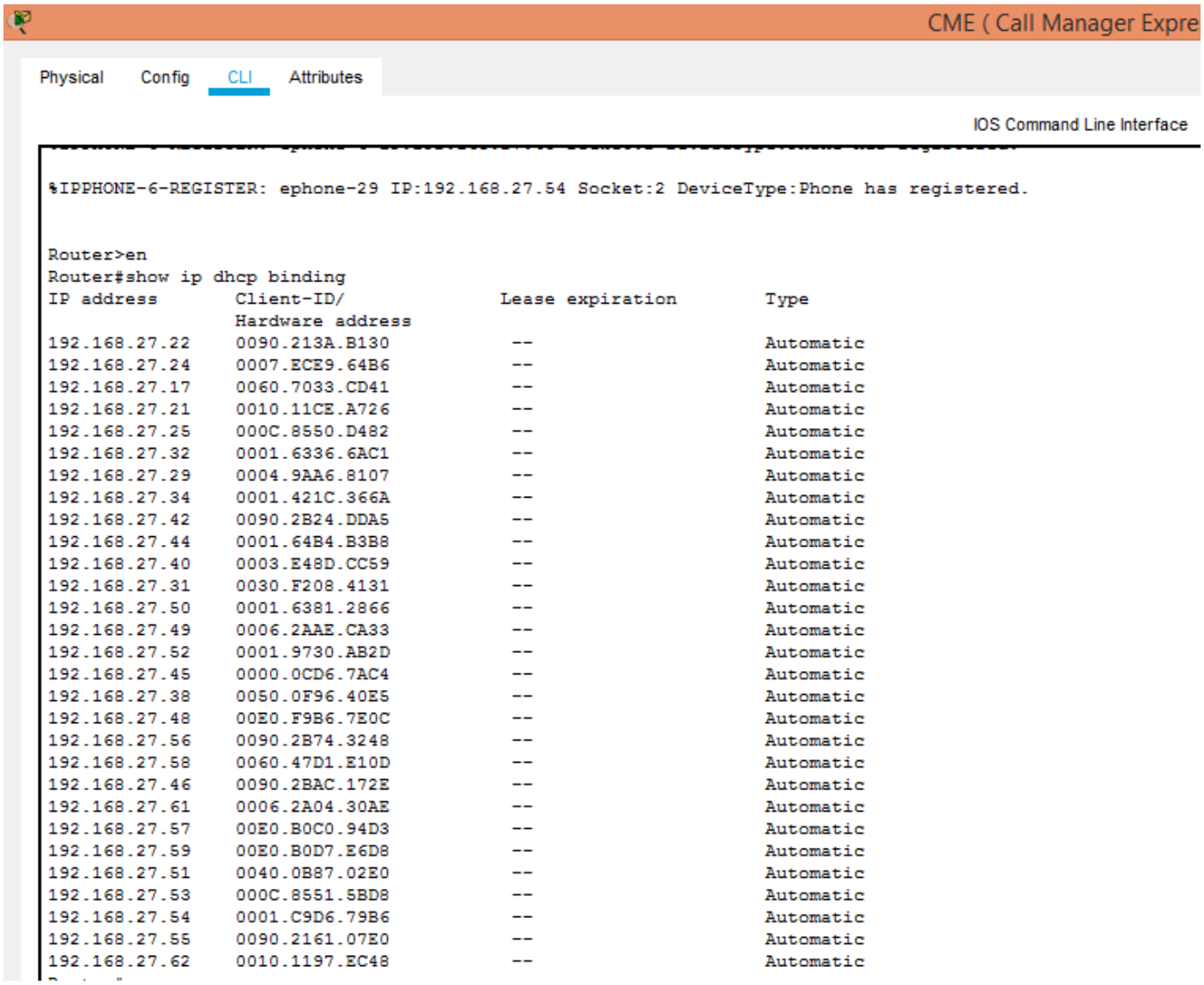

Figure 4.17-Vérification d'attribution des adresses IP avec DHCP.

4.7.2. Tests de validation

Dans cette partie, l'ensemble des tests de validation consiste à vérifier l'accessibilité de l'ensemble des équipements en utilisant la commande « Ping » qui teste la réponse d'un équipement sur le réseau .Donc, si un équipement veut communiquer avec un autre, le Ping permet d'envoyer des paquets au destinataire. Si l'équipement récepteur reçoit ces paquets, la communication est réussie.

4.7.2.1. Vérification des adresses IP des PCs et téléphones IP attribuées par le DHCP

- Exemple : PC6 (VLAN3) niveau 1.

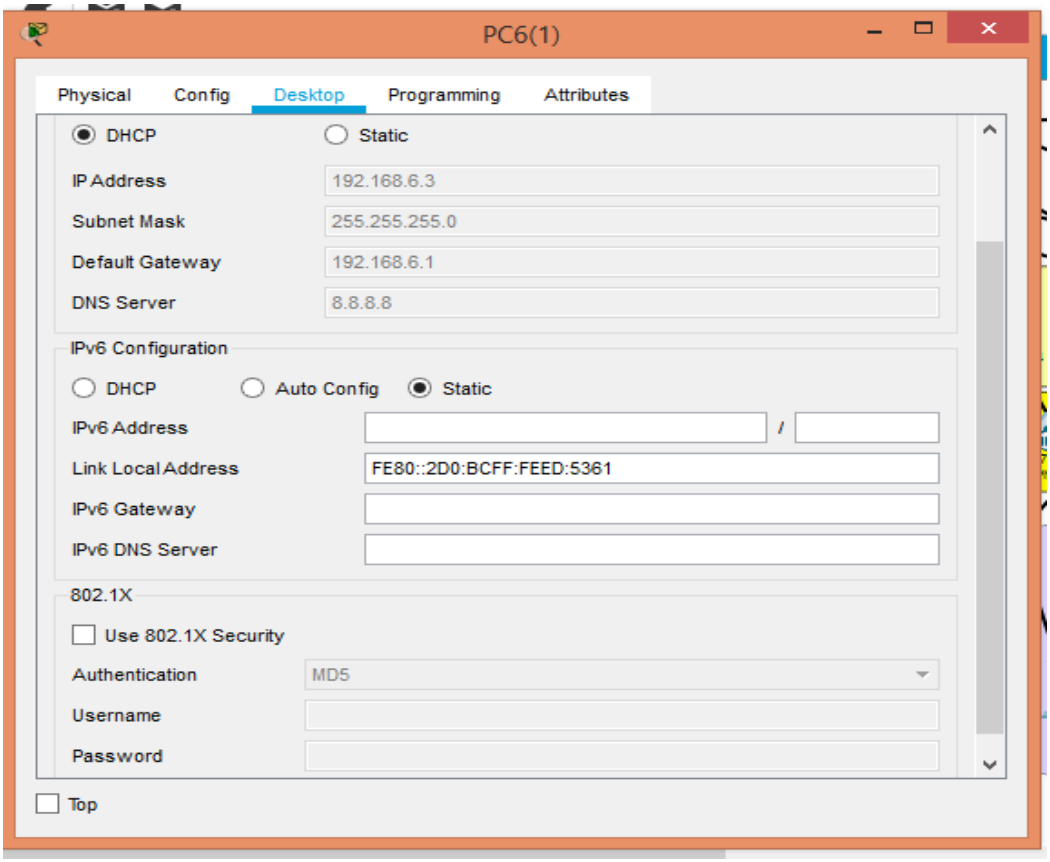

Figure 4.18-Adresse IP attribuée automatiquement.

- Exemple : Téléphone IP 11 niveau 1.

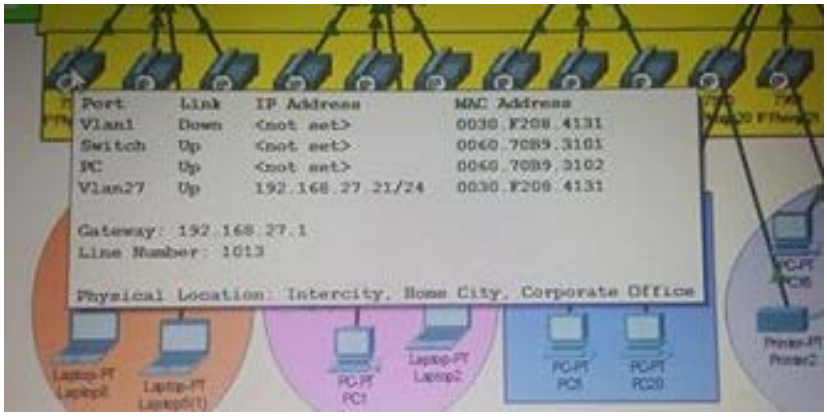

Figure 4.19-Adresse IP et numéro de téléphone attribué automatiquement.

Remarque : on voit bien que les adresses ont été attribuées au PC ainsi qu'au téléphone IP et un number line qui est de 1013 a été affecté à ce dernier.

4.7.2.2. Vérification de la communication

- **Test intra-VLANs**

Exemple : Tests réussis entre le PC18 (192.168.12.2) et le PC8 (192.168.12.4) qui appartient au même (Vlan12) niveau 1.

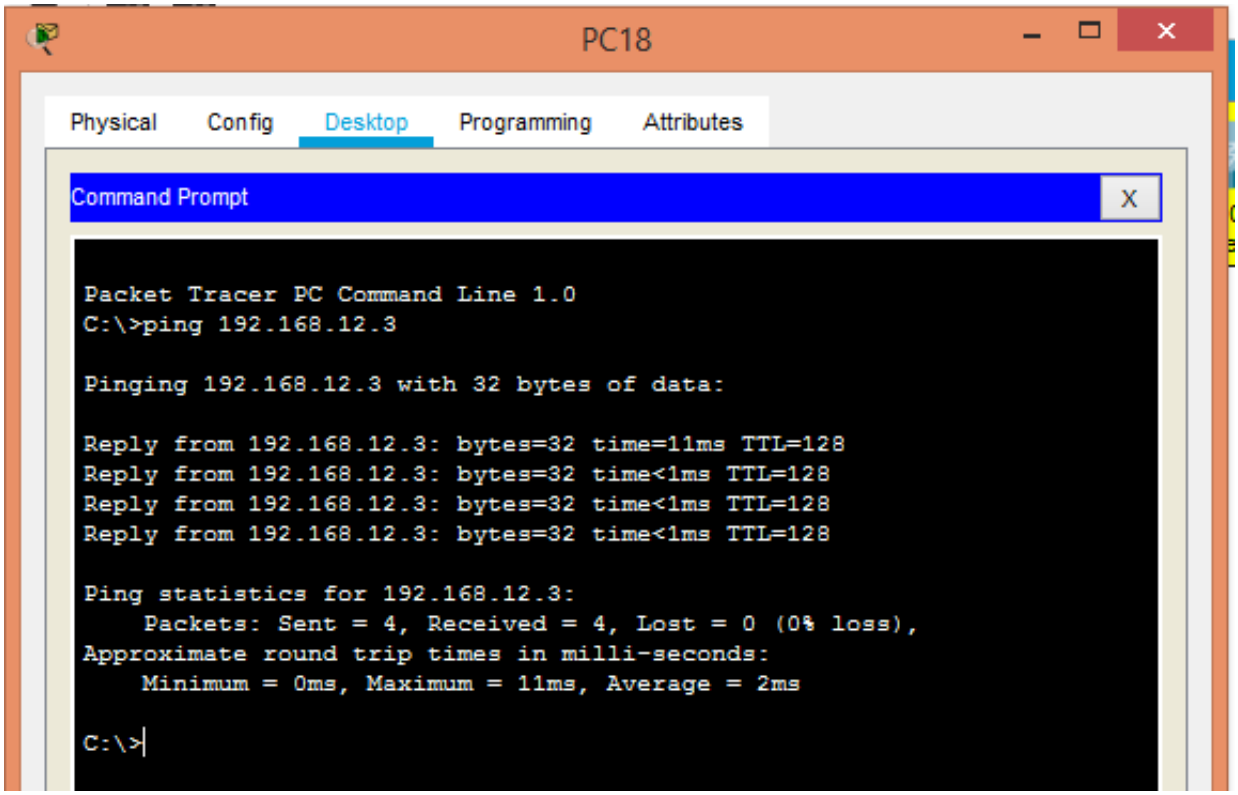

Figure 4.20-Test entre PC8 et PC 18.

Remarque : Après avoir effectué un Ping au niveau du PC18, on voit bien que les paquets ont été transmis avec succès (envoyé = 4, reçu = 4, perdu = 0) au destinataire PC3.

- **Test inter-VLANs**

  L'intérêt de ce test est d'envoyer des paquets qui appartiennent à des vlan différents.

Exemple : Test réussi entre PC0 du VLAN 5 (192.168.5.0) qui se trouve au niveau 0 (rez de chaussé) et le Laptop022 du VLAN2 (192.168.2.0) appartenant au niveau 2.

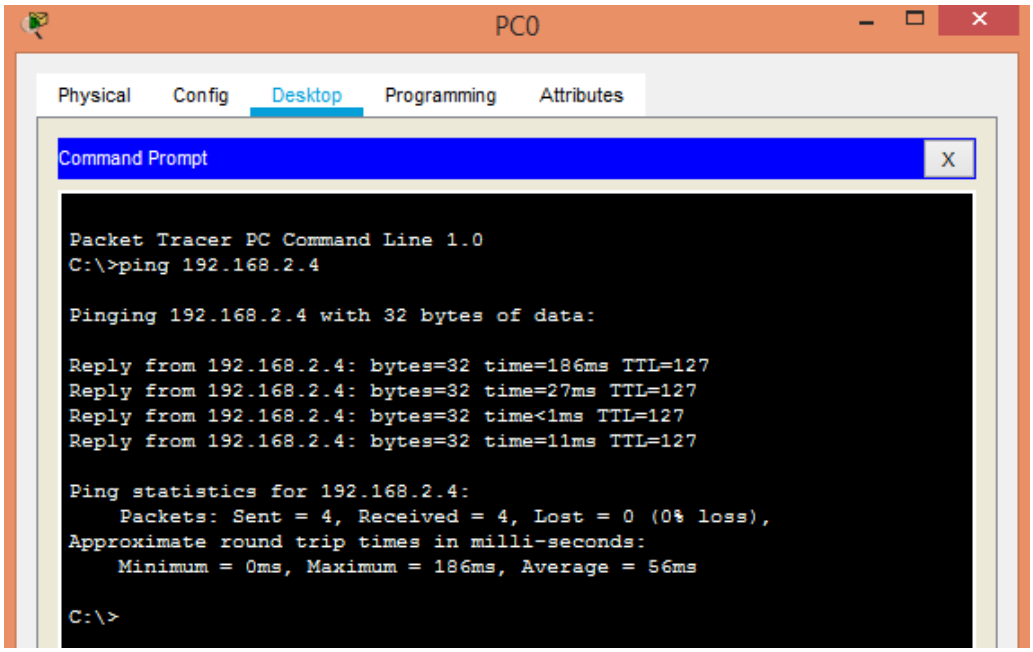

Figure 4.21-Test entre PC0et le Laptop022.

- **Test entre téléphones IP**

Exemple : Test réussi entre IP Phone225 et IP Phone32.

Figure 4.22-Test entre IP Phone225et IP phone 32.

Figure 4.23-Test réussi.

4.8. Conclusion

Dans ce chapitre nous avons commencé par introduire le simulateur Packet Tracer, puis présenté l'architecture de notre réseau suivie des configurations de chaque équipement. Et après plusieurs tests on a pu établir une connexion ente des téléphones IP et entre PCs appartenant au même VLAN ou à des VLANs différents répartis sur niveaux différents, qu'on a réussi à faire fonctionné même avec sa complexité.

CHAPITRE 5 :
IMPLEMENTATION DE LA QUALITE DE SERVICE PAR PRIORISATION DE FLUX

Dans ce chapitre nous allons procéder à l'implémentation de la qualité de service du réseau SONATRACH tout en se basant sur la priorisation de flux. Ainsi qu'la vérification des résultats de simulation du projet et à la confirmation de l'hypothèse posé au début de notre recherche.

5.1. Introduction

Dans ce chapitre nous allons procéder à l'implémentation de la qualité de service du réseau SONATRACH tout en se basant sur la priorisation des flux.

Dans une première partie, on va s'intéresser au filtrage de paquets en implémentant un Sniffer, ensuite la configuration de la priorité sur protocole et de la répartition de bande passante.

5.2. Implémentation de la qualité de service

5.2.1. Filtrage de paquets

Nous commençons donc avec un réseau sans QoS dont on a ajouté un équipement de la plateforme Packet Tracer, le « Sniffer » soit un analyseur ou renifleur de paquets, il nous servira à analyser les paquets entrants et sortants du lien dans lequel ce dernier se situe, l'image ci-dessous sera plus explicite :

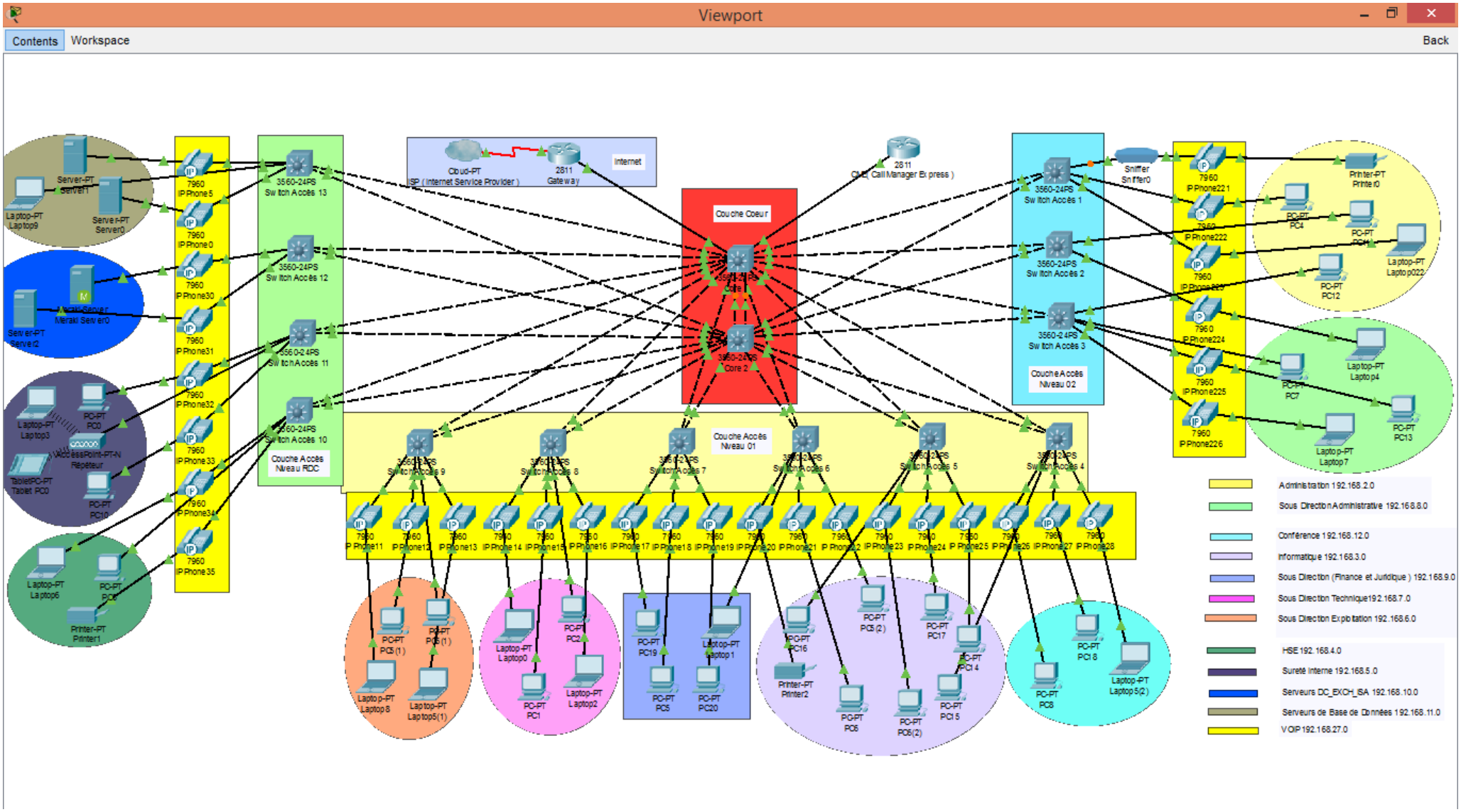

Figure 5.1- Le réseau en présence d'un Sniffer

La prochaine étape sera consacrée à la simulation d'une communication entre deux téléphones IP, pour que le Sniffer puisse se procurer le paquet RTP.

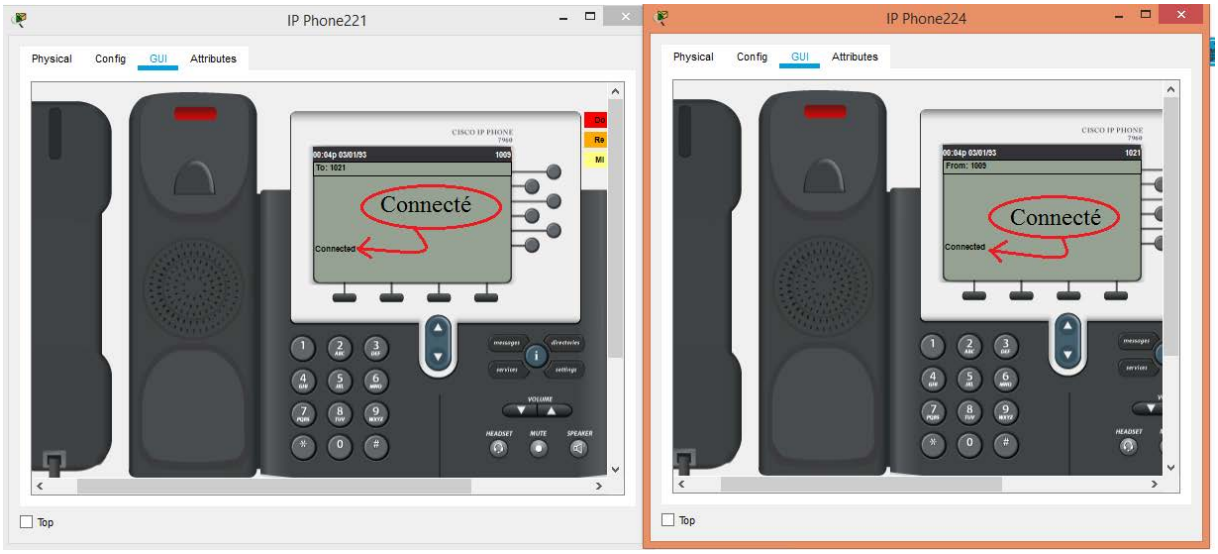

Figure 5.2-Test réussi entre téléphone IP.

Après que la connexion entre les deux téléphones ait été parfaitement établie, nous allons ensuite configurer le Sniffer de telle sorte à filtrer les paquets en gardant uniquement les paquets RTP, nous pouvons voir sur la figure ci-dessous que la communication VoIP est en cours et que le paquet contient des données VoIP.

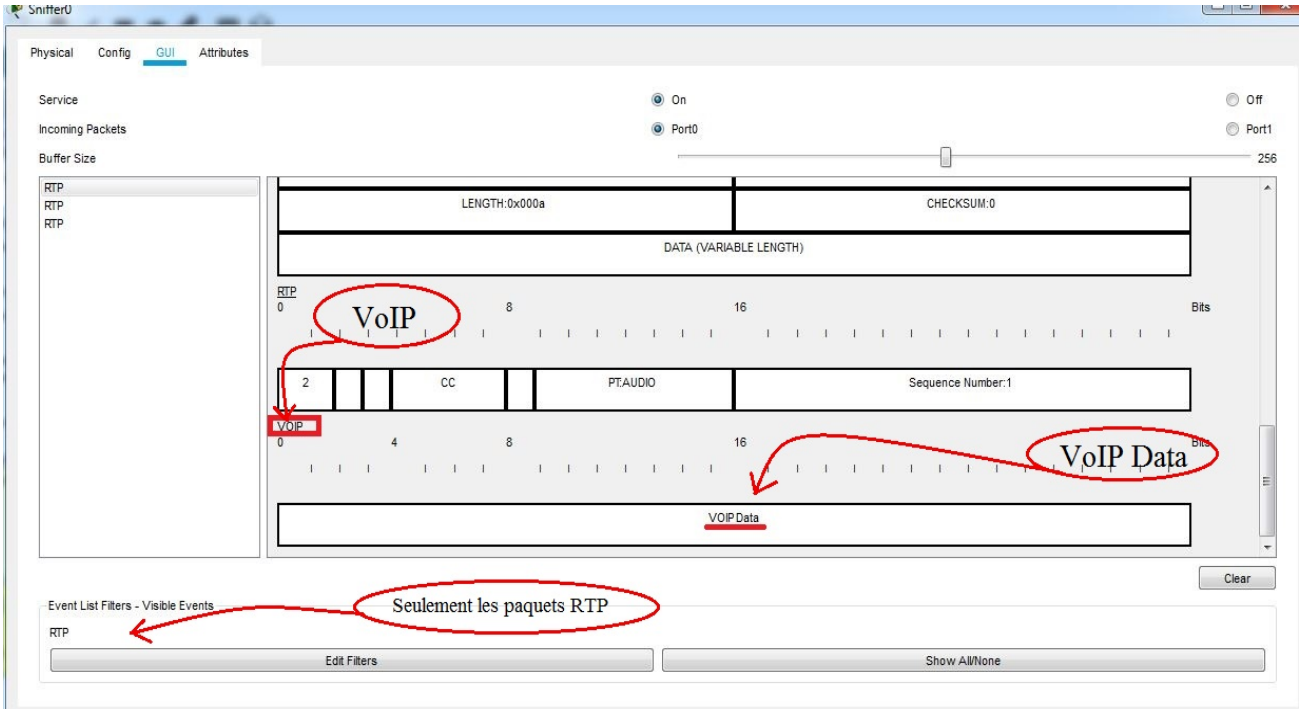

Figure 5.3-Vérification de communication VoIP sur le Sniffer.

Par la suite, notre attention sera portée sur le DSCP, que nous allons étudier avant et après pour les protocoles RTP, SCCP et ICMP, ce dernier est par défaut à zéro et sa valeur est décrite en hexadécimal :

- **Pour le RTP**

Nous allons filtrer les paquets de manière à ne garder que les paquets RTP qui a pour rôle d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie et puis les vérifier au niveau du Sniffer, nous pouvons voir sur l'image qui suit que le DSCP est à zéro, ce qui indique l'absence du paramètre QoS .

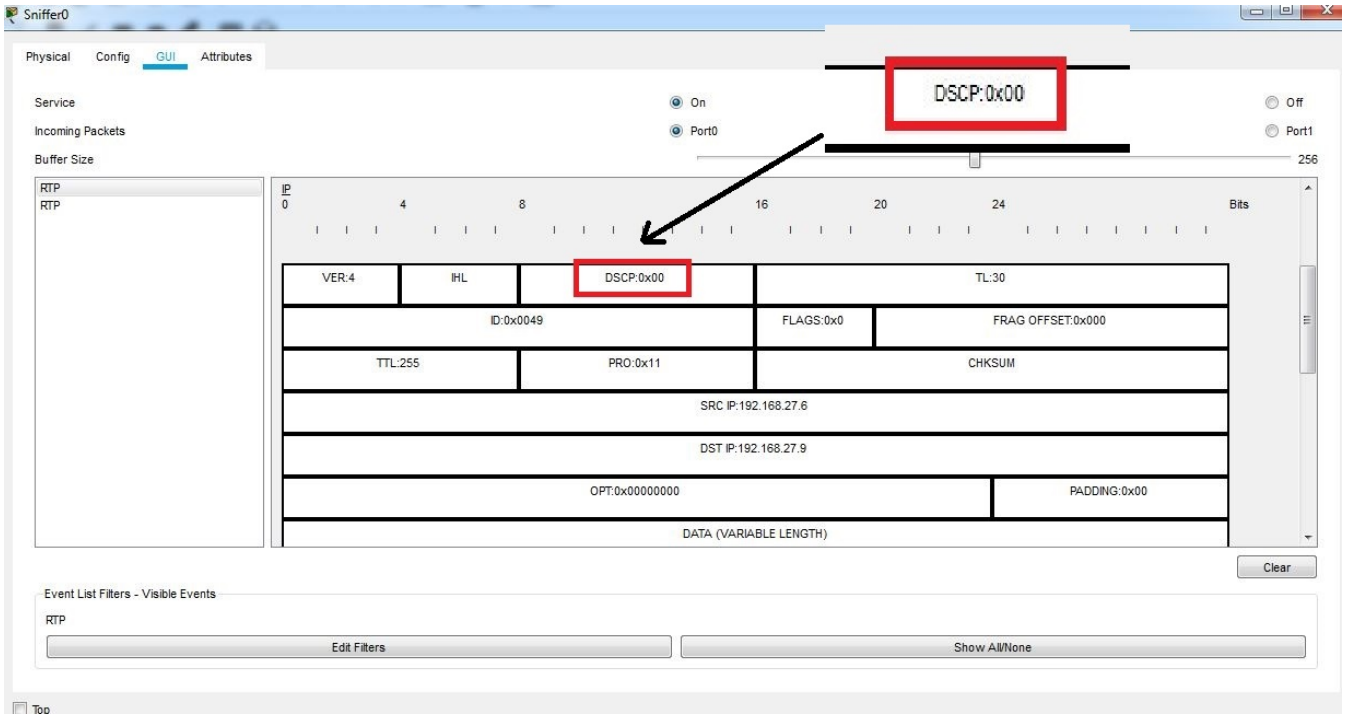

Figure 5.4-L'état DSCP avant l'installation du QoS.

- **Pour le SCCP**

Nous nous dirigerons ensuite à la partie simulation de notre réseau, nous filtrerons les paquets pour ne garder que les paquets SCCP, responsable des échanges entre le CME et les téléphones IP, nous pouvons voir sur l'image ci-dessous que le DSCP est à zéro dans ce cas aussi, et qu'il n'y a pas encore d'indicateur graphique d'une quelconque QoS ou d'une priorité accordée à ce paquet :

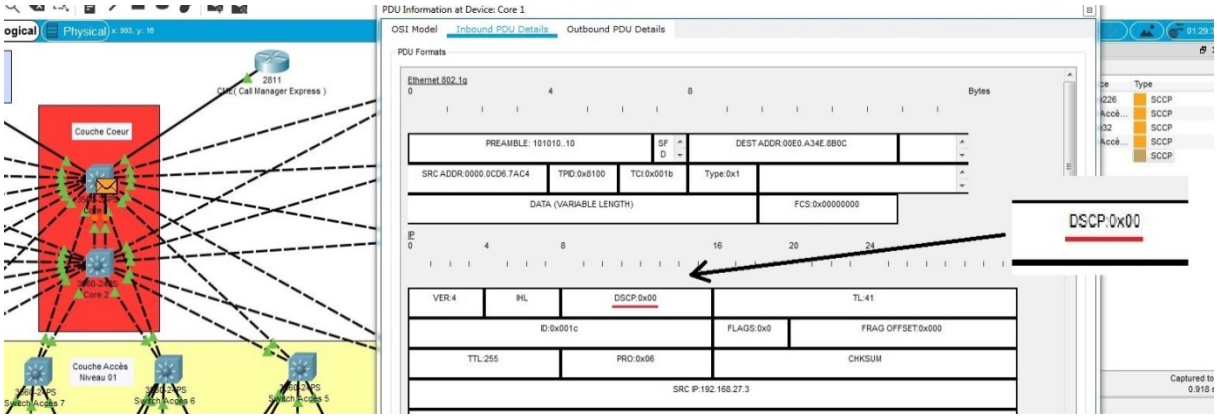

Figure 5. 5-L'état du DSCP au niveau du cœur 1 pour le SCCP.

- **Pour l'ICMP**

Toujours dans la partie simulation de notre réseau, on ne garde que les paquets ICMP qui permettent de gérer les informations relatives aux erreurs des machines connectées, nous pouvons voir sur l'image ci-contre que le code DSCP est à zéro :

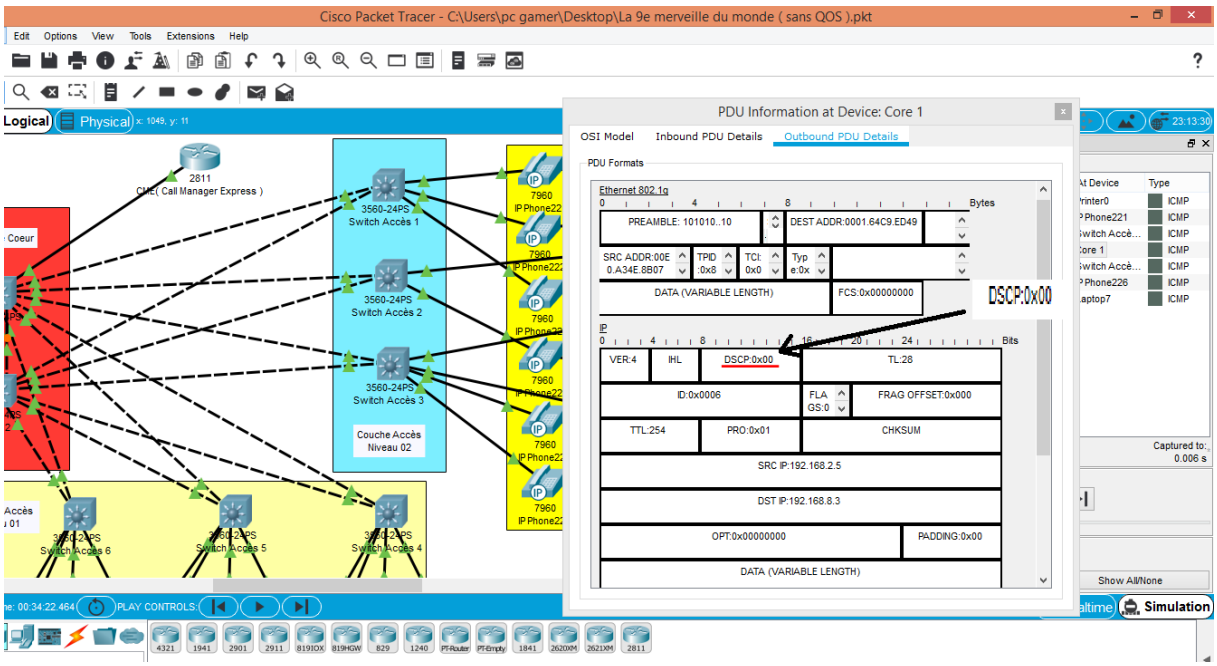

Figure 5.6-L'état du DSCP au niveau du cœur 1 pour l'ICMP.

Commentaire : On remarque que le marqueur DSCP du ping est 0x00 (Priorité 0) et qui correspond au code des trames par défaut.

5.2.2. Configuration de la priorité sur protocoles et répartition de la bande passante

Nous nous dirigeons alors vers notre switch cœur, pour implémenter la QoS qui possédera trois classes RTP et SCCP qui feront partie de notre police de priorité 7 soit la priorité maximale pouvant être accordée et de20% ,40% respectivement de la bande passante,

de l'ICMP d'une priorité de 5 et de 15% de la bande passante, et nous implémenteront ceci pour toutes les interfaces du switch cœur, ça sera une priorité accordée aux paquets entrants et sortants, le protocole RTP est transporté sur UDP donc nous choisirons le protocole UDP pour pourvoir implémenter notre priorité sur le protocole RTP :

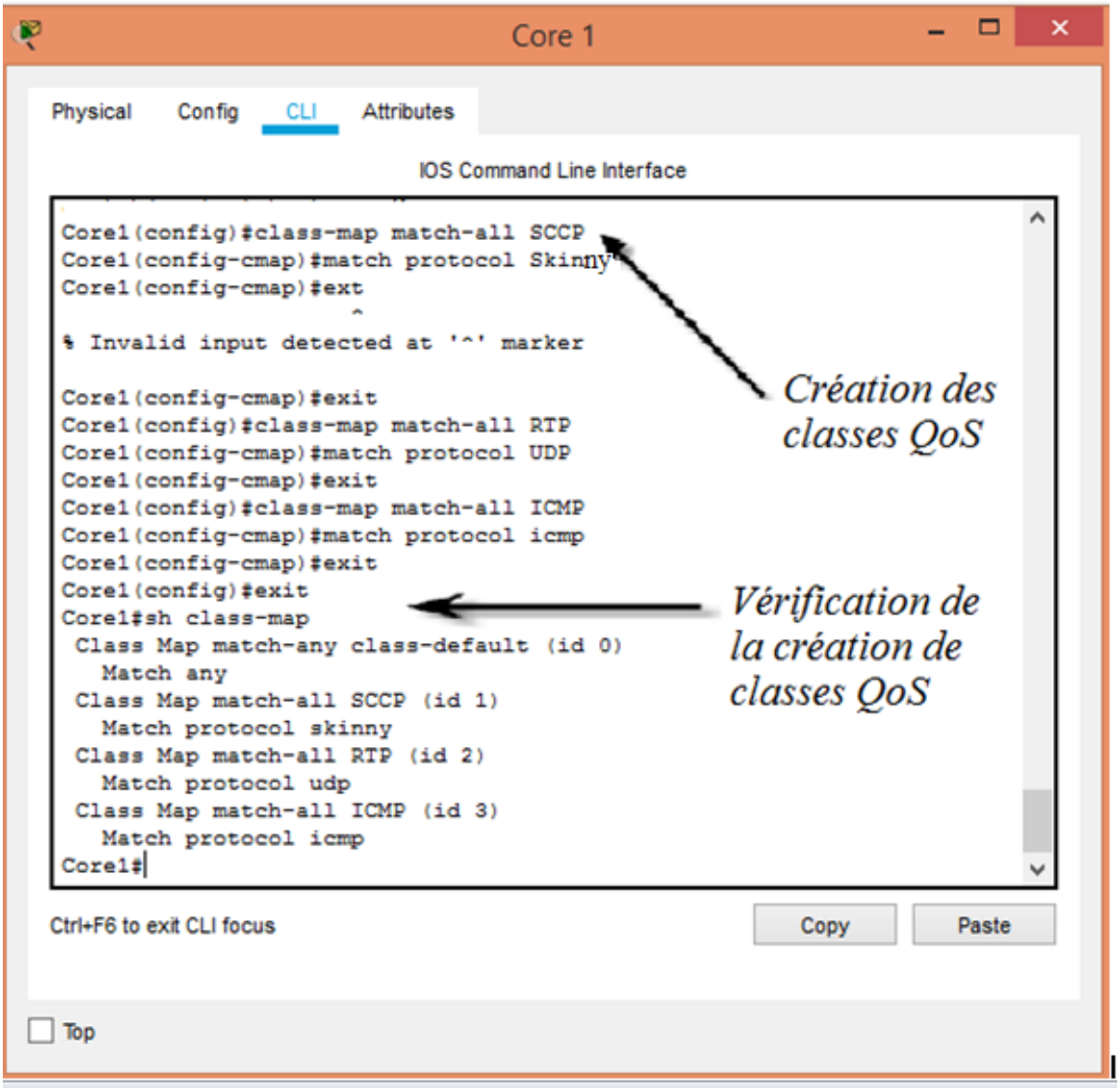

Figure 5.7-Création des classe QoS.

Concernant la suite de l'étape, nous allons créer deux stratégies comportant les différents trafiques à définir (en priorité et en pourcentage) sur la bande passante, que l'on va nommer « VoIP »et « SCCP ».

Ensuite on peut appliquer un **show**, pour voir si nos stratégie (**class-map**) ont bien étaient déclarées.

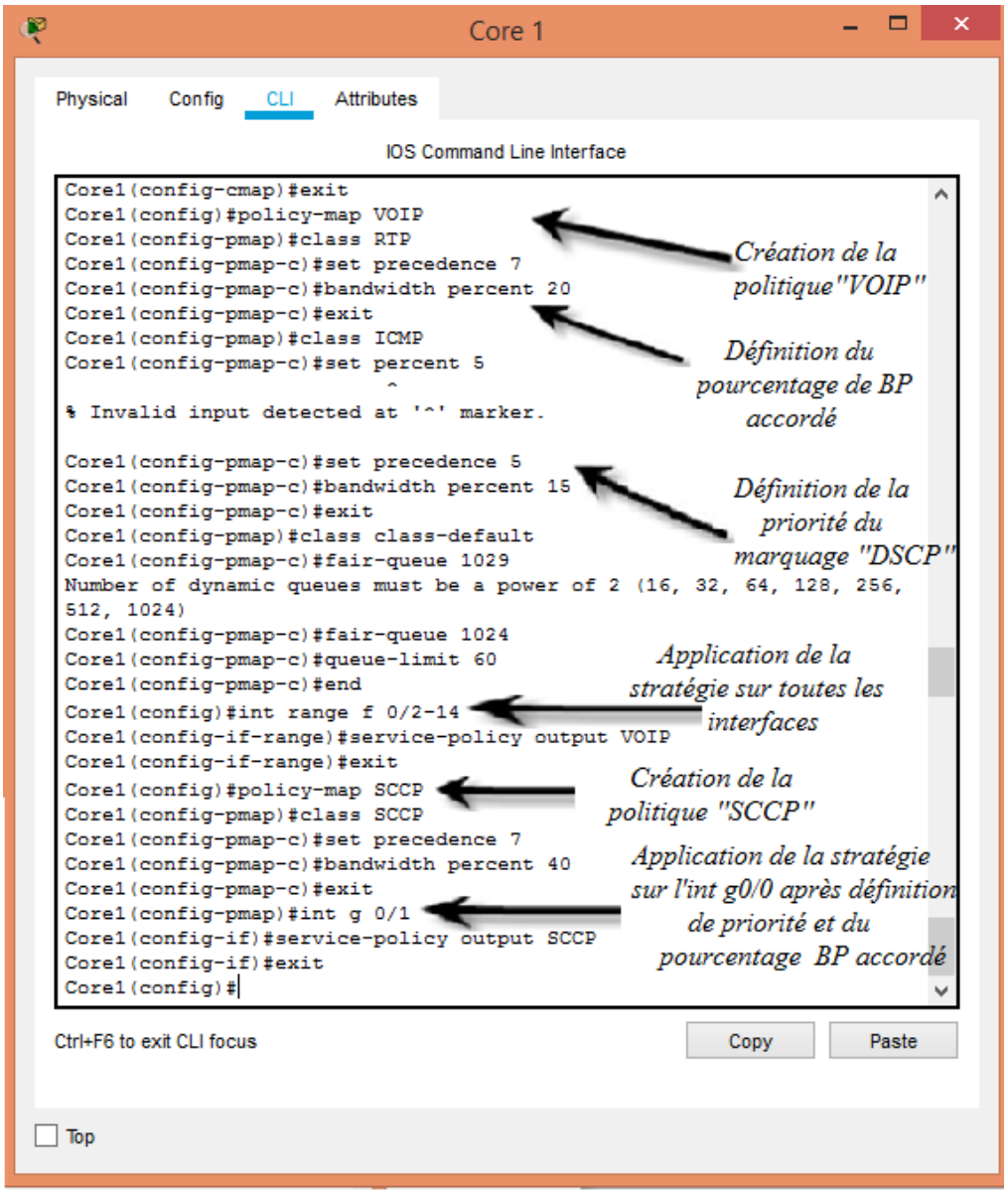

Figure 5.8-Création des politiques.

Remarque :

- On a défini sur la classe par défaut, le **WFQ** (Weighted Fair Queuing) pour donner des files d'attente (ici 1024 queues (file d'attente) en tout), contenant chacune maximum 60 paquets.
- Nous pouvons voir sur la figure ci-dessus que le nombre de file d'attente peut prendre que les valeurs suivante (16, 32, 64, 128, 256,512, 1024).
- Le **WFQ** consiste à séparer les connexions, et à leur attribuer successivement et équitablement une possibilité de faire passer leurs paquets : cela permet donc de s'assurer qu'aucune application, même très demandeuse de débit, n'en écrasera d'autres.

Nous vérifions sur l'une des interfaces que notre politique de priorité a bien été prise en compte et que la QoS a bien été implémentée.

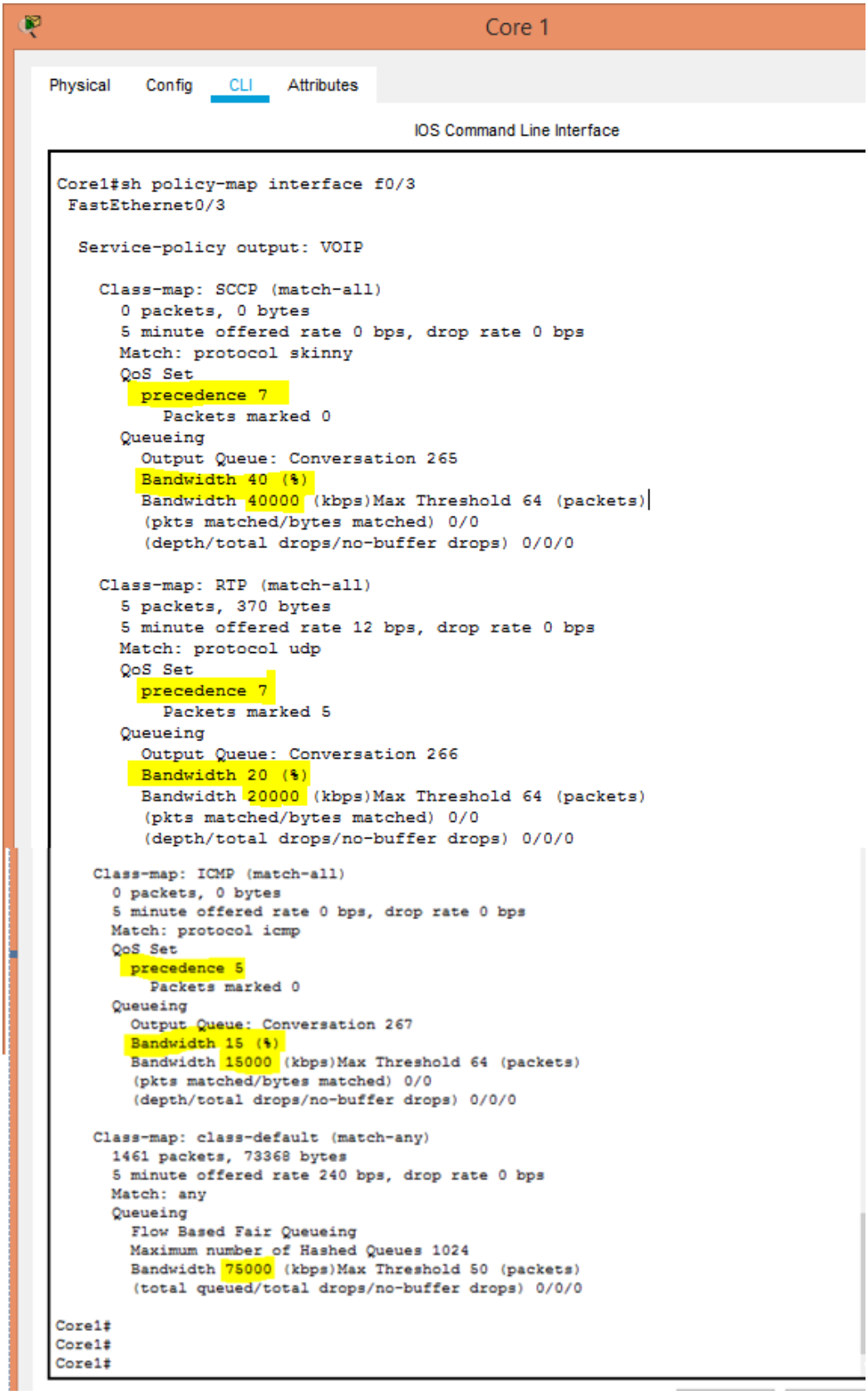

Figure 5.9-Vérification de la création de politiques.

Maintenant nous allons appliquer un test de communication (Ping) entre le PC2 (192.168.7.3) et le Serveur1 (192.168.11.2) pour vérifier que les paquets envoyés via le protocole ICMP sont indiqués sur le switch cœur.

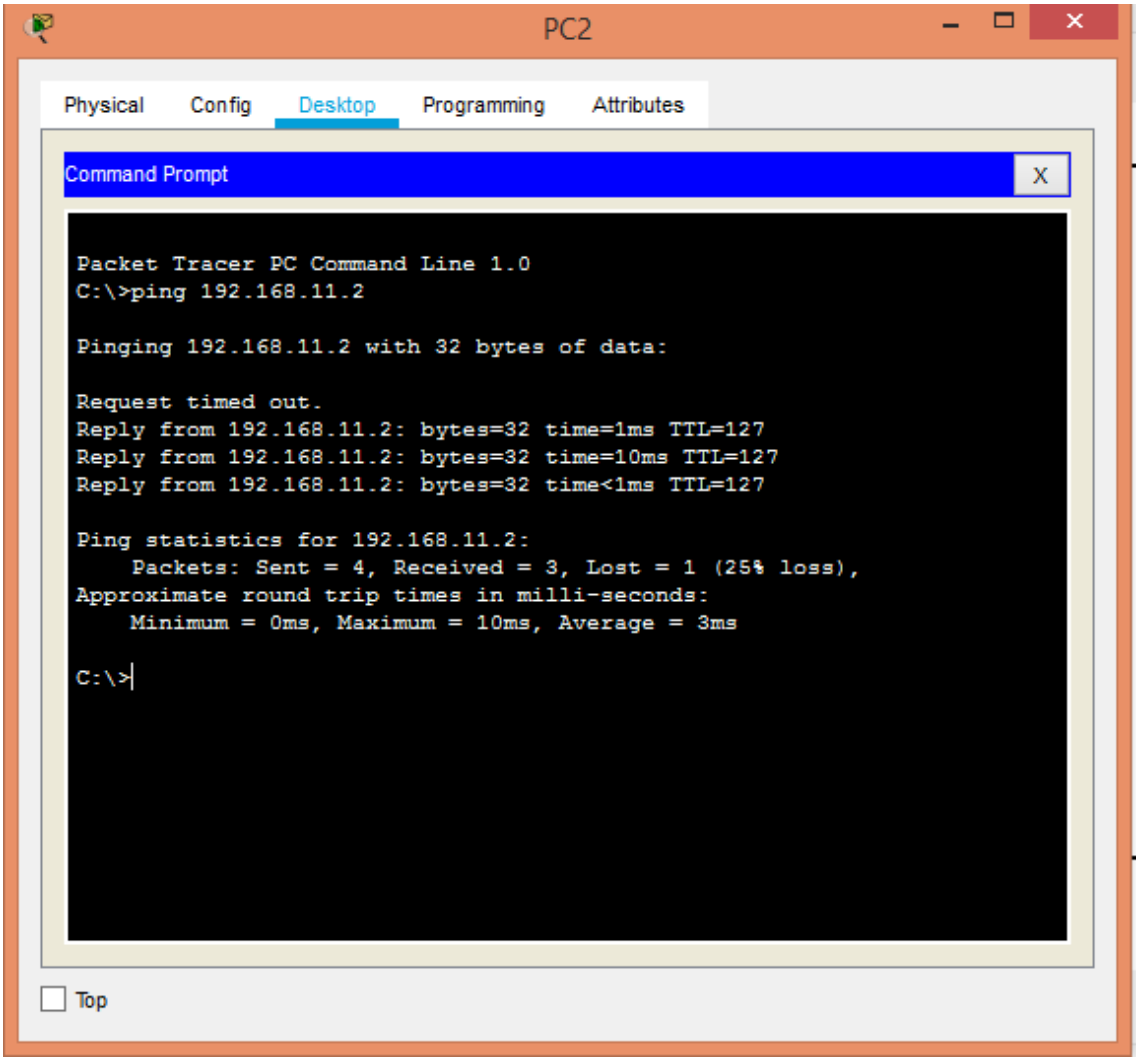

Figure 5.10-Test de communication entre le PC2 et le Serveur1.

Remarque : 4 paquets on était envoyées (trois reçus et un perdu). On sous-entend que le switch cœur devra ajouter 3 paquets sur la stratégie ICMP définie sur son interface Fastethernet 0/2.

On se dirige vers le switch cœur est on applique un **show policy-map interface fastethernet 0/2**

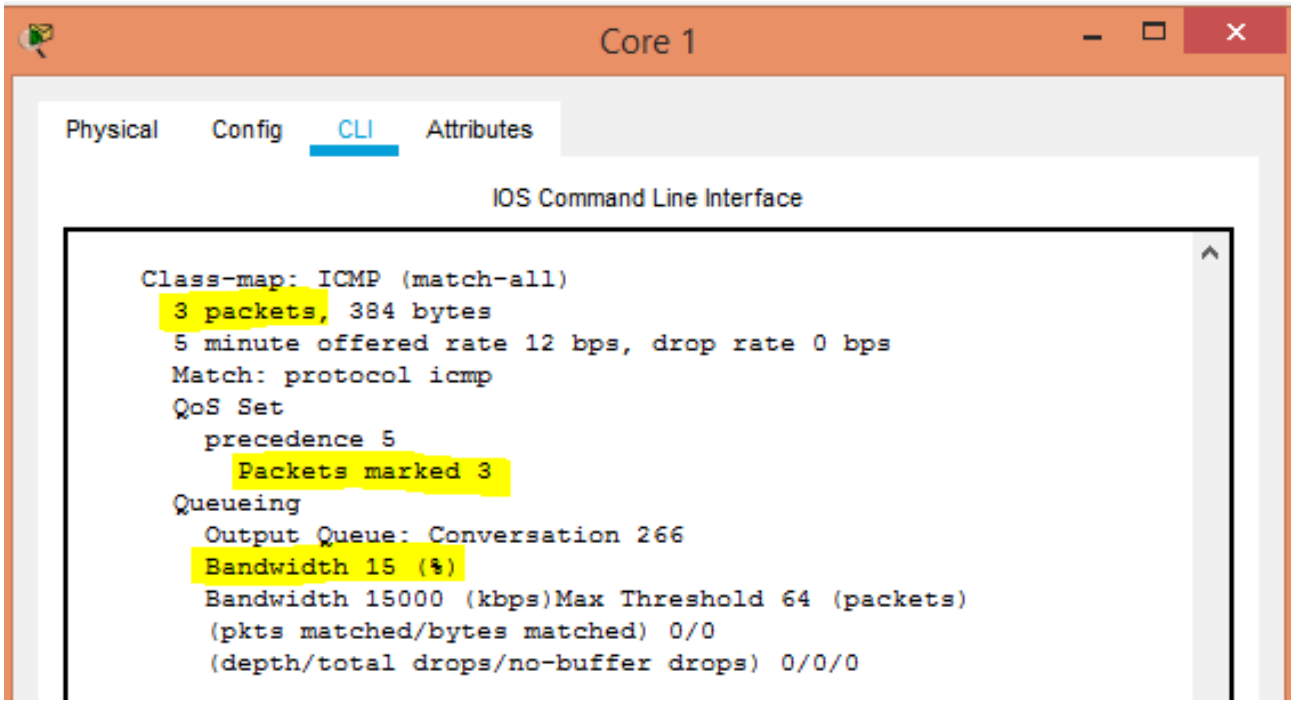

Figure 5.11-Test de communication entre le PC2 et le Serveur1.

On voit bien qu'au moment où les paquets ont traversé le switch cœur puis en sortant de l'interface fastethernet 0/2,les paquets sont ajoutés et marqués par une priorité de 5 sur la stratégie ICMP ,et donc par la suite établie les 15% de la bande passante.

Ce qui nous mène à constater que la déclaration de la stratégie ICMP est fonctionnelle.

Remarque : Le même test peut être établi pour les deux autres protocoles (RTP et SCCP).

Les politiques ont bien été appliquées pour tous les paquets entrants ou sortants des interfaces Fastethernet de 2 à 14 et Gigabitethernet 0/1 ainsi la QoS est appliquée, nous allons alors vérifier si c'est bien le cas sur le réseau.

- **Pour RTP**

Après avoir simuler une connexion entre deux téléphone IP, on remarque que l'échange entre ces deux derniers est prioritaire et l'on peut voir que cette priorité est représentée par la valeur de 7 du DSCP.

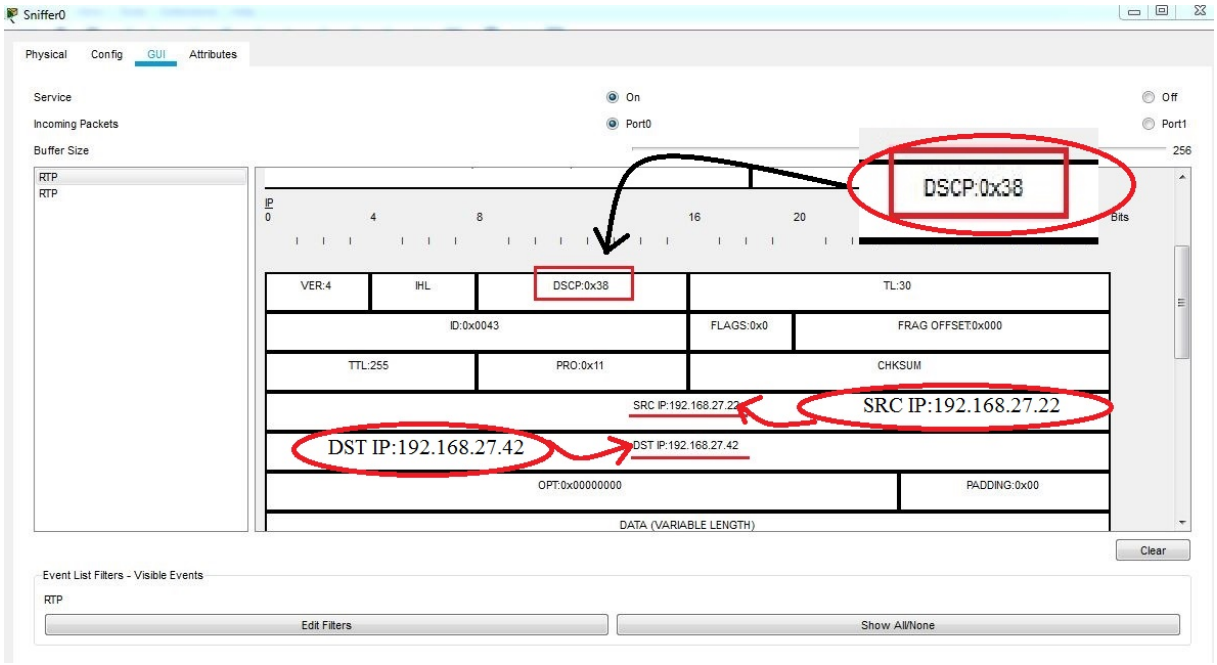

Figure 5.12-Vérification du Marquage DSCP au niveau du Sniffer.

- **Pour le paquet SCCP :**

Nous pouvons voir que le DSCP a changé et est passé de 0 à 7 en hexadécimal, qui représente la priorité que nous lui avons accordé, et nous remarquons aussi que notre trame est taguée (marquée) graphiquement avec un point vert, ce qui veut dire que ce paquet est prioritaire.

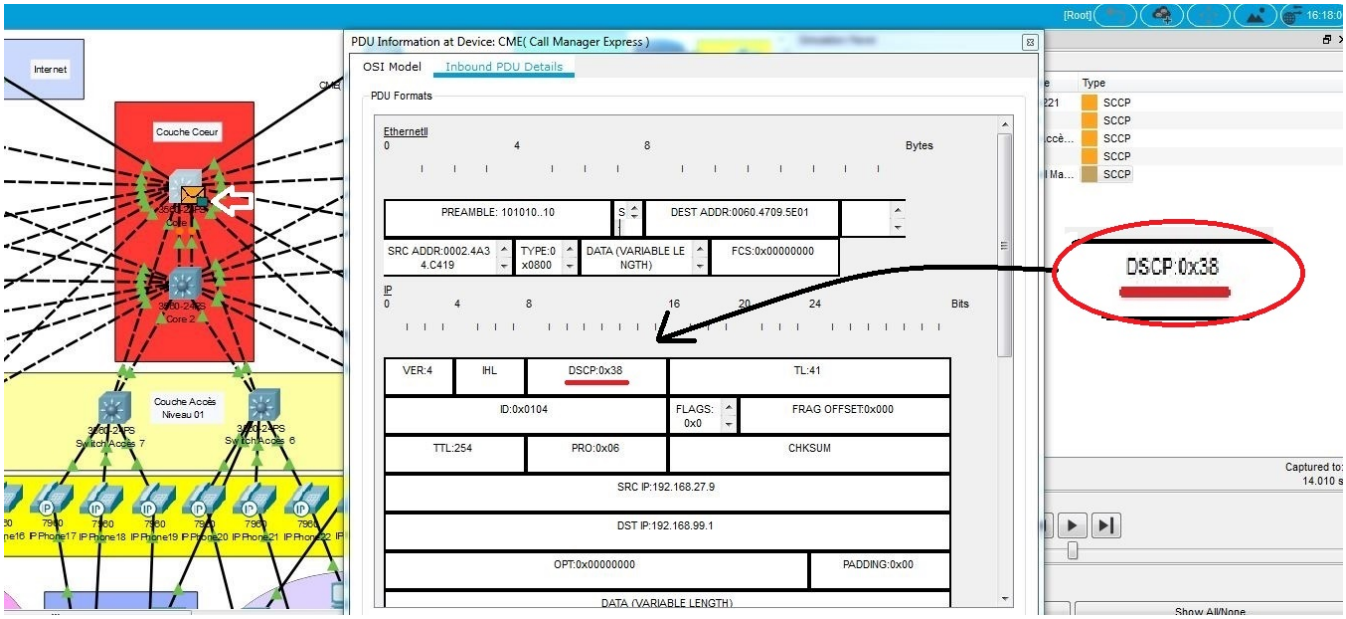

Figure 5.13-Vérification du Marquage DSCP au niveau du CME.

- **Pour l'ICMP**

Nous pouvons voir que le code DSCP est de 5 en hexadécimal, et nous remarquons aussi que notre trame est taguée (marquée) graphiquement avec un point bleu, ce qui veut dire que ce paquet est prioritaire.

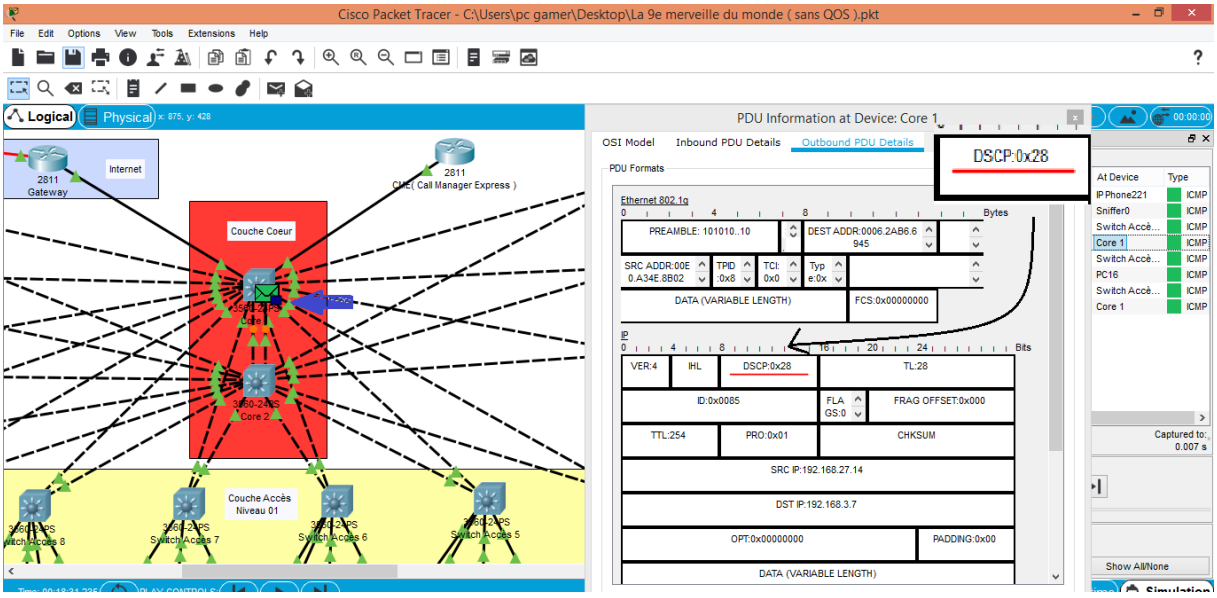

Figure 5.14-Vérification du Marquage DSCP au niveau du cœur.

Commentaire :

- IP précédence est la technique de la QoS la plus utilisé à cause de sa simplicité et de son interopérabilité avec les éléments du réseau, elle utilise les trois bits de poids fort du DSCP.
- La convention binaire de 0x28qui représente une valeur en hexadécimal donnera 101000 et en prenant les trois premiers bits à gauche, on trouve une valeur qui est égal à 5 qui représente l'apriorité 5.
- Le même calcul est appliqué à 0x38 ce qui nous donnera 111000 en binaire, en prenant les trois premiers bits on obtient une valeur de 7 qui représente notre priorité 7.

5.3. Conclusion

Durant ce chapitre, nous avons mis en place la QoS par priorisation de flux, définie par le champ de priorité ToS - en mode IP "precedence".

La procédure suivie était de définir plusieurs classes de flux, en fonction des protocoles concernés par ce dernier. Ensuite, créer des politiques de QoS dans lesquelles chaque classe de flux se voit attribuer un niveau de priorité puis appliquer cette politique sur l'ensemble d'interfaces du switch cœur et visualiser l'état des trames avant et après l'implémentation de

la QoS. Enfin, à travers plusieurs tests nous avons pu vérifier que cette procédure a été bien appliquée.

Le but de cette technique était de prioriser certains trafics relativement par rapport à d'autre notamment le trafic voix et ceci en fonction des protocoles et partage de la bande passante.

CONCLUSION GENERALE

Dans cette conclusion, nous synthétisons les résultats de cette étude.

Conclusion générale

La téléphonie sur protocole Internet (VoIP) est la voie de l'avenir. Elle peut considérablement réduire les coûts des appels téléphoniques par rapport au système traditionnel du réseau téléphonique public commuté (RTC) en raison des caractéristiques économiques de l'utilisation d'Internet. Ainsi, la technologie VoIP est la meilleure source de communication longue distance jusqu'à présent.

Nous avons essayé, par le biais de ce projet de configurer un réseau SONATRACH. Pour cela, nous avons acquis les connaissances nécessaires à la création d'un réseau d'entreprise efficace et extensible. Nous avons approfondi les fonctionnalités des commutateurs de niveau 2 et multi-niveaux tels que les VLANs, les Trunks, le routage inter-VLAN…etc. Par la suite, nous avons élaboré une technique basée sur la mise en œuvre de la QoS par priorisation de flux.

En effet, cette solution nous a permis d'assurer la non congestion du réseau en priorisant certains trafics par rapport à d'autres en fonction des protocoles et partage de la bande passante, selon les exigences des services.

Ce travail nous a donné l'occasion d'élargir et d'approfondir nos connaissances sur la voix sur IP, qui seront certainement utiles pour nous à l'avenir.

D'autres techniques de mise en place de la QoS, telles que la réservation de ressource (RSVP) et MPLS (MultiProtocol Label Switching) sont suggérées comme travaux dans le futur.

A l'avenir nous souhaitons aussi une vraie réalisation sur des équipements réels et matériels afin d'appliquer concrètement ce que nous avons fait au cours de ce mémoire.

BIBLIOGRAPHIES

Références bibliographiques

[1] BOOK ,F. Péron., *l'Europe dans la société de l'information*, édition Larcier ed.

[3] BOOK ,A. AKUE-KPAKPO., *La voix sur le réseau IP*.

[4] Journal Article,G. T. Cattoen François, Clément Le Tétour et Christophe Badot., "VOIP-la voix sur IP," *FRAMEIP.COM*.

[5] Journal Article,W.ABBESSI&A.GUEDDANA., "Architecture des réseaux de VoIP."

[7] BOOK,J. A.-X. H. Toral-Cruz, L. Estrada-Vargas and D., *An Introduction to VoIP: Endto- End Elements and QoS Parameters, VoIP Technologies,*, (2011) ed.

[8] BOOK ,PUJOLLE,"les réseaux",2011ed

[9] G. P. L.Ouakil, Eyrolles. , *"Téléphonie sur IP"*, 2014 ed., Paris, 2008.

[10] BOOK,abdulsattar VoIP ,"Voice over Internet Protocol Architecture and features",26/03/2007

[12] THESIS,Sciences, le protocole H323 : Equipements, avantages et inconvénients, wikimemories, 2001

[13] THESIS ,G. P. Laurent OUAKIL, Eyrolles. , *Téléphonie sur IP*, 2008 ed., Paris.

[14] MEMOIRE, M. ADNANE Nasser "Etude et Mise en Place D'une Solution VoIP Sécurisée Cas d'etude : Entreprise Portuaire de Béjaïa," Université A.Mira., 2016/2017.

[16] THESIS,Amélie Latourelle., "les avantages de la téléphonieIP," Juin 14, 2018

[17] THESIS, Informatique et Télécommunications , Etude et mise ne place d'un centre d'appels via IP, WikiMemoires, 27 mars 2011

[19] THESIS, D. T. . and "Etude d'implémentation d'une solution VOIP sécurisée dans un réseau informatique d'entreprise. Cas de l'ISTA de Kinshasa ,Institut supérieur de techniques appliquées de Kinshasa, 2012.

[20] Journal Article, S. Gangully. and *VoIP:wireless 2P2 and New Entreprise voice IP*

[22] BOOK,Student guide,Implementig CISCO Quality Of Service

[24] BOOK, Guide d'installation et d'utilisation, « ADR155c », SAGEM, Mai 2004

[25] BOOK,Guide d'installation et d'utilisation, *«* ADR2500c *»*, SAGEM, Mars 2004.

[26] BOOK,Guide d'installation et d'utilisation, «Brasseurs Multiplexeurs Flexibles Palier P4.3B», SAGEM FMX.

WEBOGRAPHIE

Références Webographie

[2] Web page,*l'essentiel de la voIP*. Available: http//www.monge.univ-mlv.fr

[6] Web page ,C. systems. *la téléphonie sur IP*. https://www.cisco.com/c/m/fr_dz/solutions/ip-telephony.html

[11] Web page ,Wikipedia, H323,URL https://fr.wikipedia.org/w/index.php?title=H.323&oldid=1496218

[15] Web page, "Introduction aux systèmes de présentation multimédia.", http://opera.inrialpes.fr/people/Loay.Sabry/these/ch02.toc.html

[21] Web page *AVANTAGES ET INCONVENIENTS DE LA TELEPHONIE SUR IP* . Available: https://www.memoireonline.com/09/13/7361/m_Etude-dimplementation-dune-solution-VOIP-securisee-dans-un-reseau-informatique-dentrepr39.html

[18] Web page, [Online] Avaible: http://faq.programmerworld.net/lang/fr/voip/voip-advantages-disadvantages.htm

[23] Web page ,ALCATEL LUCENT. Available :www.alcatel.lucent.com

ANNEXES

ANNEXE I : ADRESSAGE DES INTERFACES

Origination Port	rigination Port Statu	Destination Port	Origination Port	rigination Port Statu	Destination Port
Switch Accès 1:FastEthernet0/4	Green	IP Phone222:Switch	Switch Accès 8:FastEthernet0/23	Green	Core 2:FastEthernet0/5
Switch Accès 2:FastEthernet0/1	Green	Core 1:FastEthernet0/13	Switch Accès 7:FastEthernet0/23	Green	Core 2:FastEthernet0/6
Switch Accès 3:FastEthernet0/1	Green	Core 1:FastEthernet0/12	Switch Accès 6:FastEthernet0/23	Green	Core 2:FastEthernet0/8
Core 1:FastEthernet0/11	Green	Switch Accès 4:FastEthernet0/1	Switch Accès 5:FastEthernet0/23	Green	Core 2:FastEthernet0/14
Switch Accès 5:FastEthernet0/1	Green	Core 1:FastEthernet0/10	Switch Accès 4:FastEthernet0/23	Green	Core 2:FastEthernet0/23

Switch Accès 9:FastEthernet0/4	Green	IP Phone12:Switch	Switch Accès 10:FastEthernet0/3	Green	IP Phone34:Switch
Switch Accès 9:FastEthernet0/5	Green	IP Phone11:Switch	Switch Accès 10:FastEthernet0/4	Green	IP Phone35:Switch
Switch Accès 1:FastEthernet0/5	Green	IP Phone223:Switch	Switch Accès 10:FastEthernet0/5	Green	PC3:FastEthernet0
Switch Accès 2:FastEthernet0/10	Green	PC11:FastEthernet0	Switch Accès 11:FastEthernet0/5	Green	Répéteur:Port 0
Switch Accès 2:FastEthernet0/3	Green	IP Phone224:Switch	Switch Accès 9:FastEthernet0/3	Green	IP Phone13:Switch

Switch Accès 12:FastEthernet0/1	Green	Core 1:FastEthernet0/3	Switch Accès 6:FastEthernet0/1	Green	Core 1:FastEthernet0/9
Switch Accès 13:FastEthernet0/1	Green	Core 1:FastEthernet0/2	Switch Accès 8:FastEthernet0/1	Green	Core 1:FastEthernet0/7
Switch Accès 13:FastEthernet0/3	Green	IP Phone5:Switch	Switch Accès 9:FastEthernet0/1	Green	Core 1:FastEthernet0/6
Switch Accès 13:FastEthernet0/4	Green	Laptop9:FastEthernet0	Switch Accès 10:FastEthernet0/1	Green	Core 1:FastEthernet0/5
Switch Accès 13:FastEthernet0/5	Green	IP Phone0:Switch	Switch Accès 11:FastEthernet0/1	Green	Core 1:FastEthernet0/4

Switch Accès 13:FastEthernet0/5	Green	IP Phone0:Switch	Switch Accès 9:FastEthernet0/4	Green	IP Phone12:Switch
Switch Accès 12:FastEthernet0/3	Green	IP Phone30:Switch	Switch Accès 9:FastEthernet0/5	Green	IP Phone11:Switch
Switch Accès 12:FastEthernet0/4	Green	IP Phone31:Switch	Switch Accès 1:FastEthernet0/5	Green	IP Phone223:Switch
Switch Accès 11:FastEthernet0/3	Green	IP Phone32:Switch	Switch Accès 2:FastEthernet0/10	Green	PC11:FastEthernet0
Switch Accès 11:FastEthernet0/4	Green	IP Phone33:Switch	Switch Accès 2:FastEthernet0/3	Green	IP Phone224:Switch

Switch Accès 2:FastEthernet0/3	Green	IP Phone224:Switch	Switch Accès 4:FastEthernet0/3	Green	IP Phone28:Switch
Switch Accès 3:FastEthernet0/10	Green	PC12:FastEthernet0	Switch Accès 4:FastEthernet0/4	Green	IP Phone27:Switch
Switch Accès 3:FastEthernet0/3	Green	IP Phone225:Switch	Switch Accès 4:FastEthernet0/5	Green	IP Phone26:Switch
Switch Accès 3:FastEthernet0/4	Green	PC7:FastEthernet0	Switch Accès 4:FastEthernet0/10	Green	PC15:FastEthernet0
Switch Accès 3:FastEthernet0/5	Green	IP Phone226:Switch	Switch Accès 5:FastEthernet0/3	Green	IP Phone25:Switch

Switch Accès 5:FastEthernet0/4	Green	IP Phone24:Switch	Switch Accès 7:FastEthernet0/3	Green	IP Phone19:Switch
Switch Accès 5:FastEthernet0/5	Green	IP Phone23:Switch	Switch Accès 7:FastEthernet0/4	Green	IP Phone18:Switch
Switch Accès 6:FastEthernet0/3	Green	IP Phone22:Switch	Switch Accès 7:FastEthernet0/5	Green	IP Phone17:Switch
Switch Accès 6:FastEthernet0/4	Green	IP Phone21:Switch	Switch Accès 8:FastEthernet0/3	Green	IP Phone16:Switch
Switch Accès 6:FastEthernet0/5	Green	IP Phone20:Switch	Switch Accès 8:FastEthernet0/4	Green	IP Phone15:Switch

Switch Accès 8:FastEthernet0/5	Green	IP Phone14:Switch	Switch Accès 7:FastEthernet0/1	Green	Core 1:FastEthernet0/8
Switch Accès 6:FastEthernet0/10	Green	Laptop1:FastEthernet0	Switch Accès 1:FastEthernet0/3	Green	IP Phone221:Switch
Switch Accès 9:FastEthernet0/6	Green	PC6(1):FastEthernet0	Core 1:FastEthernet0/14	Green	Switch Accès 1:FastEthernet0/1
Switch Accès 8:FastEthernet0/6	Green	PC2:FastEthernet0	Core 1:FastEthernet0/18	Amber	Core 2:FastEthernet0/1
PC16:FastEthern...	Green	Switch Accès 5:FastEthernet0/6	Core 1:FastEthernet0/19	Amber	Core 2:FastEthernet0/2

			Origination Port	rigination Port Statu	Destination Port
Core 2:FastEthernet0/3	Green	Switch Accès 13:FastEthernet0/23	Switch Accès 8:FastEthernet0/23	Green	Core 2:FastEthernet0/5
Switch Accès 12:FastEthernet...	Green	Core 2:FastEthernet0/12	Switch Accès 7:FastEthernet0/23	Green	Core 2:FastEthernet0/6
Switch Accès 11:FastEthernet0...	Green	Core 2:FastEthernet0/11	Switch Accès 6:FastEthernet0/23	Green	Core 2:FastEthernet0/8
Switch Accès 10:FastEthernet...	Green	Core 2:FastEthernet0/21	Switch Accès 5:FastEthernet0/23	Green	Core 2:FastEthernet0/14
Switch Accès 9:FastEthernet0/23	Green	Core 2:FastEthernet0/7	Switch Accès 4:FastEthernet0/23	Green	Core 2:FastEthernet0/23

Switch Accès 3:FastEthernet0/23	Green	Core 2:FastEthernet0/9
Switch Accès 2:FastEthernet0/23	Green	Core 2:FastEthernet0/4
Switch Accès 1:FastEthernet0/23	Green	Core 2:FastEthernet0/10
Laptop3	Connected	Répéteur
Tablet PC0	Connected	Répéteur

Résumé

De nos jour, le problème majeur que rencontres les réseaux d'entreprise est la congestion .Les équipements de ces derniers ne donnent aucune priorité aux trafics qui circulent. Ils appliquent le principe du premier arrivé, premier sorti(FIFO).L'objectif de ce projet consiste à concevoir, configurer et implémenter la qualité de service (QoS) de la voix sur IP du réseau SONATRACH, tout en se basant sur la priorisation des flux afin d'assurer la non congestion en priorisant certains trafics par rapport à d'autres en fonction des protocoles et partage de la bande passante, selon les exigences des services. Pour mettre notre solution en pratique nous avons utilisé le simulateur Packet Tracer qui offre la possibilité de simuler le comportement des protocoles réseaux.

Mots clés : FIFO, voix sur IP, QoS, Priorisation de flux, Protocoles, Packet Tracer.

Abstract

Nowadays, the main problem encountered by business networks is congestion. Their equipment does not give priority to the traffic that circulates. They apply the principle of first-in, first-out (FIFO). The objective of this project is to design, configure and implement the SONATRACH voice over IP service quality while relying on the prioritization of the flows in order to to ensure non-congestion by prioritizing certain traffic over others according to the protocols and bandwidth sharing, according to the requirements of the services. To put our solution in practice we have used the Packet Tracer simulator which offers the possibility of simulate the behavior of network protocols.

Keywords : FIFO,voice over IP,QoS, prioritizing certain traffic, Packet Tracer.