

République Algérienne Démocratique et Populaire
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud Mammeri De Tizi-Ouzou



Faculté de Génie Electrique Et D'Informatique
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

*Présenté en vue de l'obtention du diplôme de MASTER en
Electronique*

Option : **Réseaux et Télécommunication**

Thème

**Mise en place d'une solution ToIP sous le réseau
Intranet d'Algérie Télécom.**

Dirigé par :

M^r LAHDIR M.

Réalisé par :

M^{elle} NOUALI Katia

M^{elle} MOUMOU Dyhia

Promotion 2017/2018

Remerciements

Au terme de ce travail, nous remercions en premier lieu le dieu puissant qui nous a donné le courage et la volonté pour réaliser ce mémoire.

Nous tenons à exprimer notre profonde gratitude et nos sincères remerciements à notre promoteur Mr LAHDIR pour son orientation, sa disponibilité et ces judicieux conseils.

Nos profonds remerciements vont à notre encadreur Mr HADOUS ainsi que toute l'équipe de travail du LET de Tizi-Ouzou pour leur soutien, leur patience et toute la documentation qu'ils nous ont fourni.

Nous remercions également les membres de jury qui nous font l'honneur de juger notre travail.

DÉDICACES

Je dédie ce modeste travail à :

A la mémoire de mon père que Dieu le compte parmi ces fidèles.

A ma très chère mère ma source de tendresse qui a tout sacrifié pour moi.

A mes chers frères JUBA, FERHAT et ALI.

A mon cher oncle RABAH.

A tout mes ami(e)s ainsi qu'à tous ce qui me sont chers.

A toute personne m'ayant fait part de son savoir.

MOUMOU DYHIA

DÉDICACES

Je dédie ce modeste travail à :

Mes très chers parents qui m'ont toujours soutenu.

Mes chers frères RAFIK, AMAYAS et NADIR.

Ma chère Grand-mère.

Tous mes chers ami(e)s ainsi qu'à tous ce qui me sont chers.

Tous ceux qui ont apporté de l'aide de près ou de loin pour la réalisation de ce travail.

NOUALI KATIA

Sommaire

Introduction.....	01
--------------------------	-----------

Chapitre I:Généralités sur le routage des réseaux

I.1.Préambule	02
I.2.Définition du routage IP.....	02
I.3.Méthodes de routage IP.....	03
I.4.Types de routage.....	05
I.4.1.Le routage statique.....	05
I.4.1.1.Avantages du routage statique.....	06
I.4.1.2.Inconvénients du routage statique.....	06
I.4.2.Le routage dynamique.....	06
I.4.2.1.Avantages du routage dynamique.....	06
I.4.2.2.Inconvénients du routage dynamique.....	07
I.4.3.Routage à système autonome.....	07
I.5.Les différents algorithmes de routage.....	07
I.6.Les différents protocoles de routage.....	08
I.6.1.Protocoles de routage interne	09
I.6.2 Les protocoles de routage externes	12
I.6.3.Les fonctions de base des protocoles de routage	13
I.6.4.Choix d'un protocole de routage.....	14
I.7.Les VLAN	14
I.7.1.Définition	14
I.7.2.Création des VLAN	14
I.7.3.Intérêts des VLAN	15
I.7.4.Principe de fonctionnement	15
I.7.5.Types des VLAN.....	15
I.7.5.1.Les VLAN par port (VLAN de niveau 1).....	15
I.7.5.2.Les VLAN par adresse MAC (VLAN de niveau 2).....	16
I.7.5.3.Les VLAN par protocole (VLAN niveau 3)	17
I.7.6.Avantages des VLAN	18
I.7.7.Routage inter VLAN	19

I.7.7.1.Routage inter VLAN physique	19
I.7.7.2.Routage inter-VLAN logique	20
I.7.7.3.Comparaison entre les deux techniques du routage inter-vlan	20
I.8.Discussion	21

Chapitre II : Généralités sur la ToIP

II.1.Préambule.....	22
II.2.Standard téléphonique IPBX.....	22
II.3. Définition de la téléphonie sur IP.....	22
II.4. Les notions de base de la ToIP.....	22
II.4.1.Principe de la ToIP	23
II.4.2.Fonctionnement de la ToIP	24
II.4.3.La téléphonie par circuits et par paquets	24
II.5.Le déroulement d'une communication téléphonique sur IP.....	26
II.5.1.Mise en place de la communication	26
II.5.2.Etablissement de la communication	27
II.5.3.Transport de l'information téléphonique.....	27
II.5.4.Changement de réseau.....	27
II.5.5.Arrivée au destinataire.....	27
II.6.Avantages et inconvénients de la téléphonie sur IP.....	28
II.6.1.Avantages.....	28
II.6.2.Inconvénients.....	28
II.7.Les protocoles utilisés pour la Téléphonie IP	29
II.8.Paramètres influant sur la transmission de la voix sur IP.....	29
II.8.1.Traitement de la voix	30
II.8.2.Bande passante	30
II.8.3.Latence.....	30
II.8.4.Gigue de phase.....	30
II.8.5.Echo	31
II.8.6.Perte des paquets	31
II.9.Les mesures de sécurité spécifiques à la téléphonie sur IP.....	31
II.10.Modes de déploiement.....	32
II.10.1.Codes d'accès utilisateur.....	32
II.10.2.Codes d'accès administrateur.....	33

II.10.3.Interfaces de communication.....	33
II.10.4.Services non essentiels.....	34
II.10.5.Informations techniques.....	34
II.10.6.Inscription des téléphones.....	34
II.11.Discussions.....	35

Chapitre III: Application (Router CISCO)

III.1.Préambule.....	36
III.2.Présentation de Packet Tracer.....	36
III.2.1.Pourquoi Packet Tracer.....	36
III.2.2.Présentation de la fenêtre principale.....	37
III.3.Présentation de la topologie du réseau du LET.....	38
III.4.L'implémentation de la solution VOIP sous le réseau Intranet d'Algérie Télécoms avec Packet Tracer.....	39
III.4.1.Architecture du réseau LET.....	39
III.4.2.Configuration du Switch.....	40
III.4.3.Configuration du Routeur.....	45
III.4.4. Définir le Routeur comme DHCP serveur	50
III.4.5. Configuration des paramètres Call Manager Express.....	52
III.4.6. Configuration des services téléphoniques	53
III.4.7. Interconnexion des deux sites (LET et Centrale d'Alger).....	54
III.4.8.Architecture du réseau du site d'Alger.....	56
III.5. La Configuration physique du Téléphone IP.....	57
III.6. Fonctionnalités de la téléphonie IP.....	64
III.7.Discussions.....	69
Conclusion.....	70

Bibliographie

Liste des figures

Figure I.1.figure d'un réseau	02
Figure I.2.Exemple d'une table de routage.....	05
Figure I.3.Classification des protocoles de routage dynamique.....	09
Figure I.4.Les VLAN par port.....	16
Figure I.5.Les VLAN par adresse MAC.....	17
Figure I.6.VLAN par sous réseau.....	17
Figure I.7.VLAN par protocole.....	18
Figure I.8.Routage physique.....	19
Figure I.9.Routage logique.....	20
Figure II.1.Numérisation de la voix.....	23
Figure II.2.Transport de la voix.....	24
Figure II.3.La technique de transfert des paquets.....	25
Figure II.4.Un flot de paquets téléphoniques.....	26
Figure II.5.Schéma illustratif de la communication ToIP.....	28
Figure III.1.Présentation de l'écran principal.....	37
Figure III.2.Le réseau du LET après la configuration des téléphone IP et les Vlan.....	38
Figure III.3.Présentation du réseau qui relie deux sites sous la solution ToIP.....	39
Figure III.4.Création des trois vlan 10,20 et 30.....	40
Figure III.5.Configuration des interfaces	42
Figure III.6.Accorder une passerelle par défaut au Switch.....	43
Figure III.7.Configuration de l'interface entre le Switch et le routeur En mode trunk.....	44
Figure III.8. L'établissement de la route entre les deux sites.....	46
Figure III.9.Etablissement de la route entre les deux sites.....	47
Figure III.10.Activation de l'interface 0/0.....	48
Figure III.11.Création des sous-interfaces pour les vlan 10 et 20.....	49
Figure III.12.Création de la sous-interface pour le vlan 50.....	49
Figure III.13.Vérification de la création des sous-interfaces	50
Figure.III.14.Configuration du DHCP serveur.....	51
Figure III.15.Configuration des paramètres Call Manager Express et l'activation de l'interface loopback	53
Figure III.16.Configuration des services téléphoniques.....	54

Figure III.17.L'interconnexion des deux appareils IPBX sur deux sites différents.....	55
Figure III.18.Visualisation de l'adresse IP attribué au PC par le DHCP.....	55
Figure III.19.Visualisation des services téléphoniques.....	56
Figure III.20.Redémarrage du poste IP.....	57
Figure III.21.Attribution d'une adresse au poste IP par le DHCP.....	57
Figure III.22.Saisir l'adresse sous forme HTTPS.....	58
Figure III.23.Accéder à l'interface du poste IP.....	58
Figure III.24.Saisie du mot de passe.....	59
Figure III.25.Menu administration.....	59
Figure III.26.SIP Environnement.....	60
Figure III.27.SIP Environnement (Sauvegarde des informations).....	61
Figure III.28.Qualité de service.....	62
Figure III.29.LAN Port Settings.....	63
Figure III.30.Affichage du numéro sur le poste IP.....	64
Figure III.31.Composant principaux d'un téléphone IP.....	65
Figure III.32.Accès à la liste des appels.....	67
Figure III.33.Affichage du nom de l'appelant.....	67
Figure III.34.Composer Un Double Appel.....	68
Figure III.35.Alterner entre deux communications.....	68
Figure III.36.Conférence établie.....	69

Liste des tableaux

Tableau I.1.Comparaison des techniques de routage.....	20
Tableau III.1.Fonctions des touches programmées.....	66

Glossaire

BGP: Border Gateway Protocol

CPU: Central Processing Unit

CLNS: Connectionless Network Service

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name Server

EGRP: Enhanced Interior Gateway Routing Protocol

EGP : Exterior Gateway Protocol

FAI : Fournisseur d'Accès à Internet

HTTP: Hyper Text Transport Protocol

IGRP: Interior Gateway Routing Protocol

IGP: Internal Gateway Protocol

IP: Internet Protocol

IS-IS: Système Intermediaries à Système Intermediaries

IPBX: IP Private Branch Exchange

LSP: Label Switched Path

LSA: Libre Service Actualités

LSDB: Life Science Databases

LAN: Local Area Network

L.E.T: Laboratoire des équipements de telecommunication

LIETF: Leverged and Inverse Exchange –Traded Fund

MAC: Media Access Control

MGCP: Media Gateway Control Protocol

NIC: Numéro Interne de Classement

OSPF: Open Shortest Path First

OSI: Open Systems Interconnexion

PCM: Pulse Code Modulation

PIN: Personal Identification Number

RAM: Random Access Memory
RIP: Routing Information Protocol
RFC: Request For Comments
RTP: Real Time Protocol
RTC : Réseau Téléphonique de Commuté
RTCP : Real Time Transport Control Protocol
RNIS : Réseau Numérique à Intégration de services (ISDN)
STP: Spanning Tree Protocol
SIP: Session Initiation Protocol
SPF: Sun Protection Factor
SS7: Signalling System number 7
TCP: Transport Contrôle Protocole
ToIP: Telephony over Internet Protocol
UDP: User Datagram Protocol
USB: Bus Série Universel
VoIP: Voice over IP
VLAN: Virtual local Area Network
WAN: Wide Area Network
Web : World Wide Web

INTRODUCTION

Le développement des technologies de transfert de la voix fondées sur le protocole IP constitue potentiellement un élément majeur de l'évolution du monde des télécommunications. Il ya quelques années, la téléphonie classique constituait l'exclusivité des télécommunications. De nos jours, la popularité de l'Internet, le plus grand réseau mondial, est en extension continue due à l'implémentation des technologies de routage avancé au sein de son architecture. Ce qui a donné naissance à la téléphonie sur IP.

Les entreprises Algériennes ont adaptés cette technologie. La problématique est que malgré son implémentation au cœur de leurs réseaux, il existe parfois un manque d'administration qualifié capable de configurer les différents composants des réseaux tel que les routeurs et les commutateurs Cisco.

Cisco est le plus célèbre des constructeurs de matériels dédié au routage. Il met a la disposition du marché mondial des routeurs et commutateurs intégrant des fonctions avancées qui leur permettent d'être implémentés au cœur des différents réseaux : les réseaux LAN ou Intranet.

Notre travail est donc la mise en place d'une solution téléphonie sur IP sous le réseau Intranet d'Algérie Télécom en utilisant un Routeur Cisco. Pour réaliser notre travail nous avons répartie notre mémoire en trois chapitres :

Dans le premier Chapitre, nous décrivons le routage dans les réseaux informatiques où en citant ces différents modes, ces différents types et protocoles utilisé dans les réseaux. Aussi, nous avons décrit les Vlans tout en expliquant leu principe de fonctionnement.

La téléphonie sur IP, son principe de fonctionnement ainsi que le déroulement de la communication téléphonique sur IP fait l'objet du deuxième chapitre.

Le troisième chapitre est divisé en deux parties :

La première partie est consacrée pour la simulation à l'aide de Packet Tracer d'un réseau Intranet d'Algérie Télécom reliant deux sites : le LET de Tizi-Ouzou (Laboratoire des Equipements de Télécommunication) et la Centrale d'Alger. Dans la deuxième partie, nous donnons la configuration physique de notre application, à savoir les fonctionnalités de la téléphonie.

Et nous terminant notre mémoire par une conclusion ainsi que par quelques perspectives pour améliorer notre travail.

CHAPITRE I

Le routage dans les réseaux
informatiques

I.1. Préambule

Le routage ou acheminement est le ciment permettant d'assurer la cohésion d'Internet. Sans lui, le trafic TCP/IP serait limité à un seul réseau local. Le routage est la façon de déterminer le trajet «optimal» des données entre l'émetteur et le récepteur. Le routage est basé sur un algorithme propre au protocole de routage. L'algorithme prend en considération les facteurs les plus importants comme la durée moyenne de transmission, la charge du réseau, la longueur totale du message... Il permet au trafic provenant d'un réseau local d'atteindre sa destination ou qu'elle se trouve dans le monde – après avoir probablement traversé plusieurs réseaux intermédiaires.

Le rôle décisif qui joue le routage et l'interconnexion complexe des réseaux Internet font de la conception des protocoles de routage un défi majeur que doivent relever les développeurs de logiciels réseau. Par conséquent, la plupart des études relatives au routage concerne la conception des protocoles ; très peu de traitement de la configuration correcte des protocoles de routage. Toutefois, nombre de problèmes quotidiens résultent plutôt d'une mauvaise configuration des routeurs utilisés que de l'emploi d'algorithmes mal conçus. C'est le rôle de l'administrateur réseau de s'assurer que la configuration du routage est correcte.

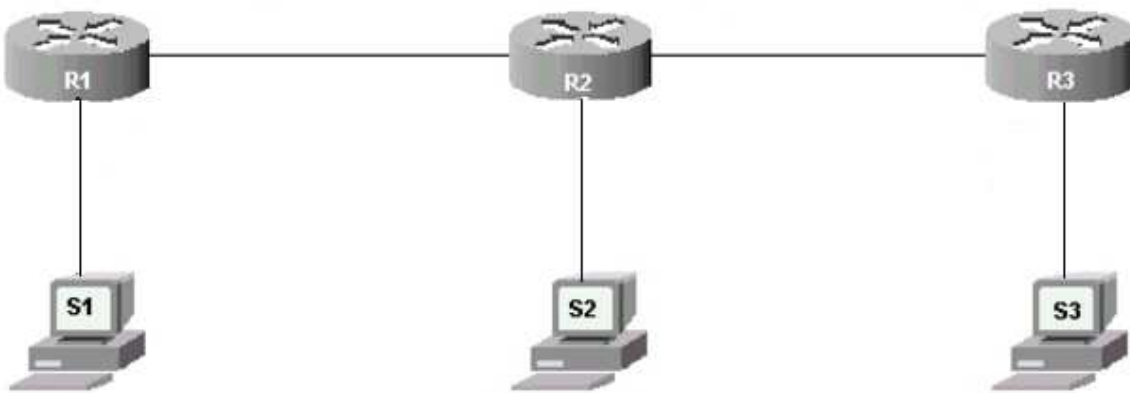


Figure I.1. figure d'un réseau

I.2. Définition du routage IP [1]

Internet repose sur le principe du routage. Sans le routage, le trafic sera limité à un seul câble physique. Le routage permet l'acheminement de l'information entre des équipements qui ne sont pas directement reliés à un même support. Son rôle est essentiel dans les réseaux de grande distance (WAN), qui présentent très souvent une topologie maillée. La

communication peut très bien traverser une succession de réseaux intermédiaires afin de s'établir entre les deux machines.

Autrement dit, le routage est le choix d'un chemin suivant lequel les paquets transiteront et le routeur désigne la machine effectuant ce choix. En théorie, le routage devrait se faire en tenant compte des paramètres difficiles à évaluer comme l'encombrement du réseau, la longueur du datagramme et le type de service mentionné dans l'en-tête du datagramme, mais en pratique l'acheminement des paquets se fait surtout en fonction de données statiques utilisées dans les algorithmes de calcul du plus court chemin.

Qu'il s'agit donc des réseaux de grandes distances ou des réseaux locaux, le routage est réalisé par des routeurs où chaque routeur peut relier deux ou plusieurs supports formant des réseaux distincts. A chaque réseau correspond une pile différente de protocoles, appelée interface. Un routeur dispose alors d'autant d'interface que des supports connectés.

I.3.Méthodes de routage IP [2]

a) Routage Direct

Le routage direct se produit quand la machine de destination se trouve sur le même réseau physique que la machine émettrice. Dans ce cas, un datagramme IP peut être émis directement, sans passer par un routeur, après avoir été encapsulé dans une trame correspondant au type du réseau local. C'est ce qu'on appelle la remise directe.

b) Routage Indirect

Si la machine de destination du datagramme ne se trouve pas sur le même réseau que la machine émettrice, il faut passer par un routeur. L'adresse de la première passerelle par laquelle il faut passer pour atteindre la destination est appelée la route indirecte.

En effet, la machine émettrice ne s'occupe pas de connaître le chemin complet jusqu'à la destination, elle doit juste connaître l'adresse de cette première passerelle.

Si la machine de destination se trouve sur le même réseau physique mais sur un sous-réseau différent, c'est le routage indirect qui sera illustré. Ce qui implique qu'un routeur est nécessaire pour acheminer le trafic entre les deux sous-réseaux.

Un routeur n'est pas nécessairement une machine séparée, Cela peut être bien une station de travail ordinaire, Plusieurs cas de routage indirecte peuvent se présenter :

b).1.Routage par table

Les machines communiquant avec TCP/IP possèdent une table de routage IP. Il s'agit d'un ensemble de correspondances entre une adresse de réseau IP et l'adresse de la première passerelle à emprunter. Quand une machine émet un datagramme, elle vérifie d'abord si

l'adresse du réseau de destination est reprise dans cette table. Si c'est le cas, elle peut y lire l'adresse de la passerelle vers laquelle il faut envoyer le datagramme.

❖ **Table de routage**

La table de routage est une structure de donnée utilisée par un routeur ou un ordinateur en réseau et qui associe des préfixes à des moyens d'acheminer les datagrammes vers leurs destinations. Evidemment, à cause de la structure localement arborescente d'Internet la plupart des tables de routage ne sont pas très grandes. Par contre les tables des routeurs interconnectant les grands réseaux peuvent atteindre des tailles très grandes ralentissant d'autant le trafic sur ces réseaux. D'un point de vue fonctionnel une table de routage contient des paires d'adresses de type (D, R) où D est l'adresse IP d'une machine ou d'un réseau de destination et R est l'adresse IP du routeur suivant sur la route menant à cette destination.

Une table de routage est constituée des éléments suivants :

- Méthode de routage : type de protocole qui a appris la route.
- Réseau et masque : destination.
- Distance administrative : Préférence d'une route par un protocole sur un autre. Chaque protocole a sa valeur par défaut.
- Valeur de métrique : valeur d'une route sur une autre parmi toutes celles apprises par un protocole de routage.
- Via prochaine interface (Gateway).
- Interface de la sortie du routeur.

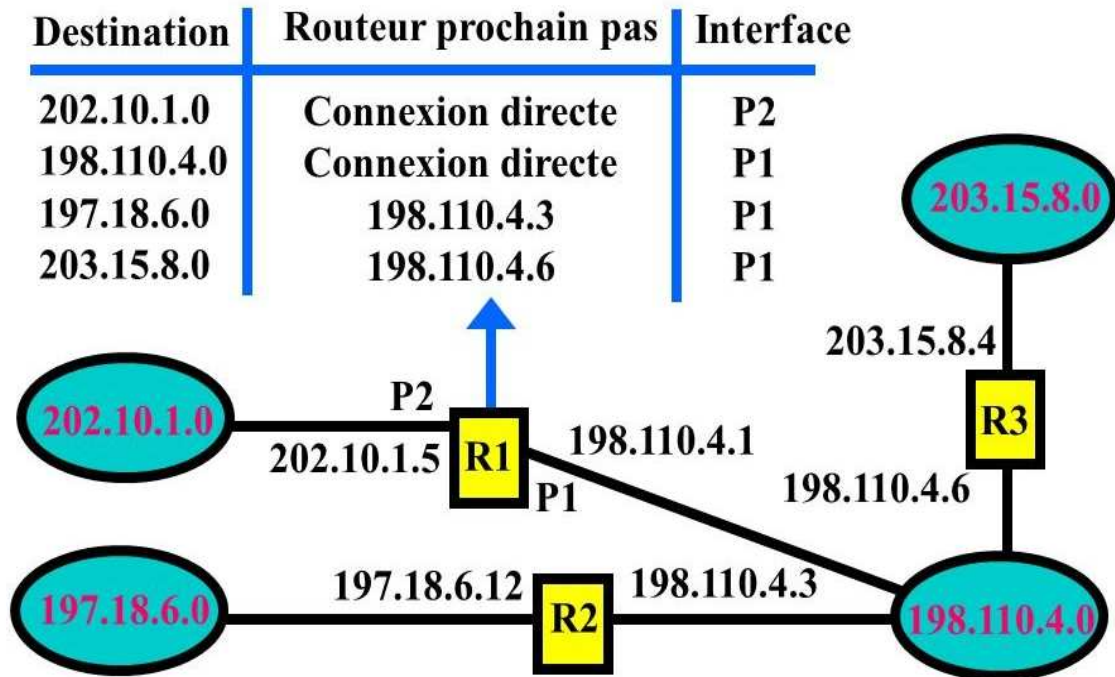


Figure I.2.Exemple d’une table de routage

b).2.Routage par défaut

Si la table de routage IP ne contient aucune entrée faisant référence à la destination du datagramme, celui-ci est alors envoyé vers une passerelle dite passerelle par défaut (Default Gateway), dont l’adresse est généralement stocké dans la table de routage.

I .4.Types de routage [3]

Il existe deux types de routage :

I.4.1.Le routage statique

Le routage statique est un routage mis en place par un administrateur du réseau qui permet de définir le chemin que doit emprunter un paquet afin qu’il puisse atteindre sa destination. Il doit gérer toutes les routes créées de chaque unité de routage du réseau. Ces routes statiques sont utilisées pour des raisons de sécurité en cas de dysfonctionnement.

Les opérations de routage statique s’articulent comme suit :

- L’administrateur réseau configure la route.
- Le routeur insère la route dans la table de routage.
- Les paquets sont acheminés à l’aide de la route statique.

I.4.1.1. Avantages du routage statique

Le routage statique présente plusieurs avantages :

- **Économie de bande passante** : Étant donné qu'aucune information ne transite entre les routeurs pour qu'ils se tiennent à jour, la bande passante n'est pas encombrée avec des messages d'information et de routage.
- **Sécurité** : Contrairement aux protocoles de routage dynamique, le routage statique ne diffuse pas d'information sur le réseau puisque les informations de routage sont directement saisies de manière définitive dans la configuration par l'administrateur.
- **Connaissance du chemin à l'avance** : L'administrateur ayant configuré l'ensemble de la topologie saura exactement par où passent les paquets pour aller d'un réseau à un autre, cela peut donc faciliter la compréhension d'un incident sur le réseau lors des transmissions des paquets.

I.4.1.2. Inconvénients du routage statique

Mais il représente aussi certains inconvénients :

- La configuration des réseaux de tailles importantes peut devenir assez longue et complexe, il faut en effet connaître l'intégralité de la topologie pour saisir les informations de manière exhaustive et correcte pour que les réseaux communiquent entre eux. Cela peut devenir une source d'erreur et de complexité supplémentaire quand la taille du réseau grandit.
- A chaque fois que le réseau évolue, il faut que chaque routeur soit au courant de l'évolution par une mise à jour manuelle de la part de l'administrateur qui doit modifier les routes selon l'évolution.

I.4.2. Le routage dynamique

Le routage dynamique permet de se mettre à jour de façon automatique. La définition d'un protocole de routage va permettre au routeur de se comprendre et d'échanger des informations de façon périodique ou événementielle afin que chaque routeur soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau. Concrètement, le protocole de routage fixe la façon dont les routeurs vont communiquer mais également la façon dont ils vont calculer les meilleures routes à emprunter.

I.4.2.1. Avantages du routage dynamique

Le routage dynamique présente les avantages suivants:

- Maintenance réduite par l'automatisation des échanges et des décisions de routage

- Modularité et une flexibilité accrue, il est plus facile de faire évoluer le réseau avec un réseau qui se met à jour automatiquement.
- Sa performance et sa mise en place ne dépendent pas de la taille du réseau.

I.4.2.2. Inconvénients du routage dynamique

Mais le routage dynamique présente aussi ces inconvénients :

- Il peut être plus compliqué à mettre en place lors de son initialisation.
- Il consomme de la bande passante de par les messages que les routeurs s'envoient périodiquement sur le réseau.
- La diffusion automatique des messages sur le réseau peut constituer un problème de sécurité car un attaquant peut obtenir des informations sur la topologie du réseau simplement en écoutant et en lisant ces messages d'information du protocole de routage et même en créer afin de se faire passer pour un membre du réseau.
- Le traitement des messages réseau et le calcul des meilleures routes à emprunter représentent une consommation de CPU et de RAM supplémentaire qui peut encombrer certains éléments du réseau.

I.4.3. Routage à système autonome

Un système autonome est constitué par un ensemble de réseaux interconnectés par des routeurs. Les systèmes autonomes sont reliés entre eux par des routeurs externes. Un système autonome correspond à un groupe de routeurs dépendant d'une même responsabilité administrative du point de vue du routage et appliquant une politique de routage unique. On distingue donc les protocoles de routage interne au sein d'un système autonome et des protocoles externes qui concernent le trafic entre systèmes autonomes. Les protocoles de routage externe privilégient les informations d'accessibilité par rapport aux informations de topologie du réseau. Un réseau IP appartient à un seul système autonome. Le principal protocole de routage externe est bien le BGP.

L'internet est composé donc d'un ensemble de systèmes autonomes reliés entre eux par des routeurs externes. Un système autonome utilise un protocole de routage interne tel que RIP, OSPF, ISIS ou IGRP. Les numéros de systèmes autonomes sont attribués par le NIC (Network Information Center). Ce numéro sur deux octets est appelé "Autonomous System Number". Les numéros du système autonome de 65412 à 65535 sont privés.

I.5. Les différents algorithmes de routage [4]

Du fait de la variété des objectifs qui sont visés, il existe plusieurs types d'algorithmes de routage. Ceux-ci peuvent correspondre à des politiques déterministes ou adaptatives selon

qu'elles s'adaptent ou non aux variations du trafic et de topologie du réseau. D'autre part, les algorithmes de routage peuvent être centralisés si les chemins sont définis par un nœud particulier. Dans le cas contraire, l'algorithme de routage est réparti entre tous les nœuds, ce qui est favorable du point de vue de la fiabilité, mais complique l'algorithme et rend plus difficile l'optimisation de l'acheminement des paquets. Le troisième paramètre à prendre en compte est le travail de routage effectué au niveau de chaque nœud, cela peut être le choix du prochain nœud ou l'indication de la route complète. Il existe enfin le routage par inondation ou aléatoire dans lequel le choix ne dépend pas de la topologie du réseau. Et parmi les algorithmes les plus classiques on peut citer celui l'algorithme de Bellman-Ford et l'algorithme de Dijkstra.

I.6. Les différents protocoles de routage [5]

Tous les protocoles de routage exécutent les mêmes fonctions de base. Ils déterminent la meilleure route vers chaque destination et distribuent au voisinage les informations d'acheminement entre les systèmes d'un réseau. Les modalités d'exécution de ces fonctions, en particulier les procédures de sélection des meilleures routes permettent de distinguer les différents protocoles.

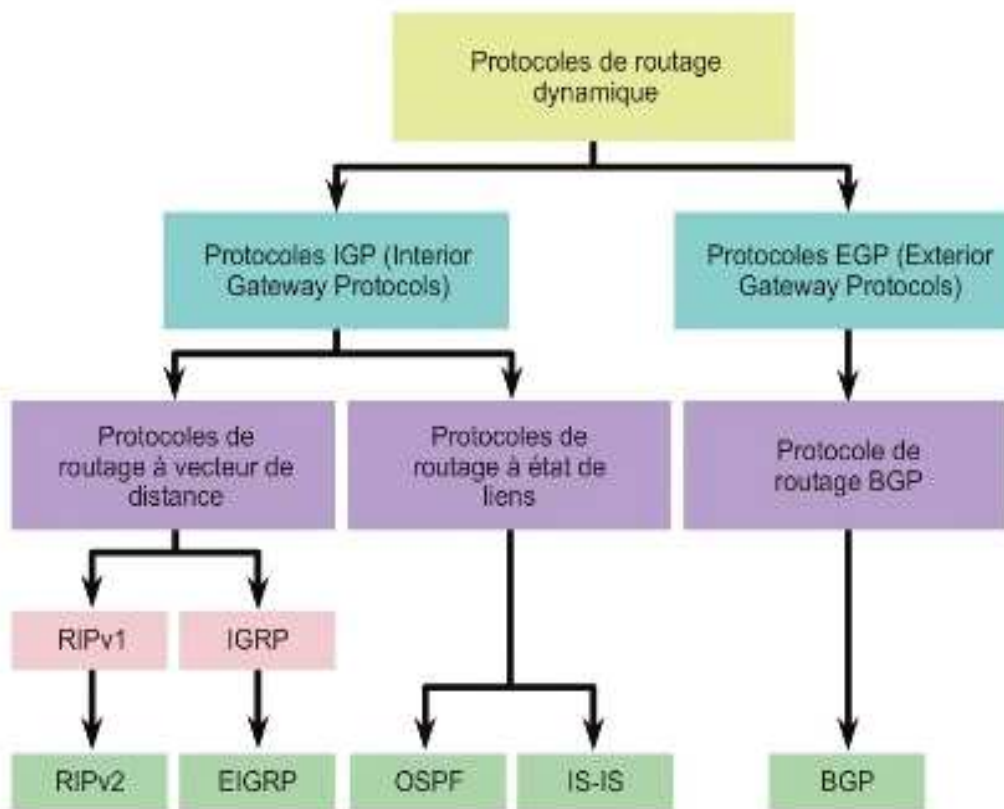


Figure I.3. Classification des protocoles de routage dynamique

I.6.1. Protocoles de routage interne (IGP : Internal Gateway Protocol)

Les protocoles du routage interne peuvent être classés dans deux différentes familles :

a) Les protocoles à vecteur de distance

Les protocoles de routage à vecteur de distances sont des protocoles permettant de construire des tables de routages où aucun routeur ne possède la vision globale du réseau, la diffusion des routes se faisant de proche en proche. Le terme « vecteur de distances » vient du fait que le protocole manipule des vecteurs (des tableaux) de distances vers les autres nœuds du réseau. La distance en question est le nombre de sauts permettant d'atteindre les routeurs voisins. Ces protocoles s'appuient sur l'algorithme de Ford-Bellman.

❖ RIP (Routing Information protocol)

RIP est le protocole le plus utilisé des protocoles de routage interne car il est inclus dans UNIX. Ce protocole sélectionne la route dont la longueur est la plus faible comme étant

la meilleure route. La longueur d'une route pour RIP est le nombre de passerelles que les données doivent franchir pour atteindre leurs destinations. RIP suppose que la meilleure route est celle qui utilise moins de passerelles.

La plus grande longueur pour RIP est de 15. Au-dessus de 15 RIP suppose que la destination n'est pas joignable (16 = infini). En supposant que la meilleure route est la plus courte, RIP ne prend donc pas en compte les problèmes de congestion.

➤ **Versions de RIP**

Il existe actuellement deux versions à ce jour, RIPv1 ainsi que RIPv2

▪ **RIPV1**

RIPv1 est défini dans la RFC 1058. Cette version ne prend pas en charge les masque des sous-réseaux de longueur variable ni de l'authentification des routeurs. Les routes sont envoyées en broadcast.

▪ **RIPV2**

RIPv2 est défini dans la RFC 2453. Cette version développée en 1993, a été conçue pour permettre au protocole de répondre aux contraintes des réseaux actuels (découpages des réseaux IP en sous-réseaux, authentification par mot de passe). Avec cette version, les routes sont envoyées à l'adresse multicast 224.0.0.9.

❖ **IGRP (Interior Gateway Routing Protocol)**

Il s'agit d'un protocole propriétaire de Cisco, pour palier les défauts de RIP, un seule métrique, nombre de saut limité. Il utilise comme RIP la diffusion périodique de mise à jour, mais en 90 secondes au lieu de 30 secondes pour RIP donc il encombre moins le réseau.

Son processus de routage et le choix d'une route est basé sur la prise en compte des paramètres suivants :

- Largeur de bande.
- Charge sur les liens.
- Délais sur la topologie.
- Fiabilité du chemin.
- Taille maximale des paquets.

IGRP permet de partager le trafic les chemins dont coûts sont presque égaux (load splitting), sans risquer de créer des boucles.

➤ Versions d'IGRP

On peut citer une seule version existante :

▪ EIGRP (Enhanced Interior Gateway Routing Protocol)

Enhanced IGRP représente une évolution de IGRP. C'est le résultat des changements des réseaux ainsi que des diverses demandes qu'on voulait de IGRP. EIGRP intègre les capacités du Link-State protocol avec le Distance-Vector protocol. Il comprend l'algorithme DUAL (Diffusing-Update Algorithme) développé à SRI international par Dr. Garcia-Luna-Aceves.

b) Protocoles à l'état de lien

Dans cette famille de protocoles chaque routeur communique avec tous les autres routeurs en échangeant des informations permettant à chacun de construire une vue complète de la topologie du réseau ainsi qu'une table de routage, prenant en compte les meilleures routes.

Tout paquet est transmis sur la meilleure route. Les métriques utilisées sont :

- La qualité du lien.
- Son encombrement.
- Le type de flux à transmettre.
- Les restrictions de qualité de service appliquées.
- Le coût financier.

Cette méthode de routage permet une construction plus rapide des tables de routage que le routage à vecteur de distance .

b).1. Avantages des protocoles à l'état de liens

- Chaque routeur crée sa propre carte topologique pour déterminer le chemin le plus court.
- L'inondation immédiate des paquets LSP permet d'obtenir une convergence plus rapide.
- Les LSP sont envoyés uniquement en cas de modification de la topologie et contiennent uniquement les informations concernant cette modification.
- La conception hiérarchique est utilisée lors de la mise à jour en œuvre de plusieurs zones.

b).2. Inconvénients des protocoles à l'état de liens

La mise à jour d'une base de données d'état de liens nécessite plus de mémoire.

La bande passante peut être affectée par l'inondation des paquets à l'état de liens.

❖ OSPF (Open Shortest Path First)

Dans le protocole OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier. Chaque routeur communique ensuite avec la liste des réseaux auxquels il est connecté par des messages Link-State Advertisement (LSA) propagés de proche en proche à tous les routeurs du réseau. L'ensemble des LSA forme une base de données de l'état des liens Link-State Database (LSDB) pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire. Chaque routeur utilise ensuite l'algorithme de Dijkstra Short Path First (SPF) pour déterminer la route la plus rapide vers chacun des réseaux connus dans la LSDB.

Le bon fonctionnement d'OSPF requiert donc une complète cohérence dans le calcul SPF, il n'est donc pas possible de filtrer des routes ou de les résumer à l'intérieur d'une aire.

En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur.

❖ IS-IS (Système Intermédiaire à système Intermédiaire)

Initialement conçu pour transporter des informations de routage respectant exclusivement le formalisme CLNS, la simplicité et la robustesse du protocole IS-IS ont motivé son adaptation au modèle IP. Cette adaptation a consisté à considérer les préfixes IP comme des feuilles d'un nouveau type RFC 1195. Elle propose trois modes d'utilisation possibles du protocole IS-IS :

- Le mode OSI-only.
- Le mode IP-only.
- Le mode Dual supportant simultanément deux formats d'adresses.

Quel que soit le mode d'utilisation retenu, ce protocole s'appuie sur un routage à deux niveaux hiérarchiques, le niveau L1 et le niveau L2 où chaque niveau est associé à une base topologique (LSDB) indépendante.

I.6.2 Les protocoles de routage externes

L'information la plus importante à retenir concernant les protocoles externes est que la plupart des systèmes ne l'exécutent jamais.

Les protocoles de routages externes sont utilisés pour échanger des informations d'acheminement entre les systèmes autonomes. Les informations d'acheminement transférées

entre ces systèmes s'appellent informations d'accessibilité. Les informations d'accessibilité correspondent simplement à des informations concernant les réseaux accessibles à travers un système autonome spécifique.

❖ **EGP (Exterior Gateway Protocol)**

C'est le plus utilisé des protocoles externes. Une passerelle qui utilise EGP annonce qu'elle peut atteindre les réseaux qui font partie de son système autonome. Contrairement aux protocoles internes, EGP n'essaie pas de choisir la meilleure route. EGP met à jour les informations de distance mais n'évalue pas ces informations. Ces informations de distance ne sont pas directement comparables parce que chaque système autonome utilise des critères différents pour évaluer ces valeurs.

Une structure de routage qui dépend d'un groupe de passerelles centralisées ne peut pas convenir à un accroissement rapide d'Internet. C'est l'une des raisons pour lesquelles Internet tend vers une architecture distribuée ou un processus de routage tourne sur chaque système autonome.

❖ **BGP (Border Gateway Protocol)**

Un autre protocole qui commence à remplacer EGP. Comme EGP, BGP échange des informations entre les systèmes autonomes mais BGP peut fournir plus d'informations pour chaque route et peut utiliser ces informations pour sélectionner la meilleure route. Une remarque importante à se rappeler est que la plupart des systèmes ne font pas tourner de protocoles externes. Ces protocoles ne sont utiles que pour les systèmes autonomes qui échangent des informations avec d'autres systèmes autonomes. La plupart des machines appartenant à un système autonome font tourner les protocoles de routage internes. Seules les passerelles reliant deux systèmes autonomes font tourner un protocole externe.

I.6.3. Les fonctions de base des protocoles de routage

En règle générale, un routeur détermine le chemin que doit emprunter un paquet entre deux liaisons à l'aide des deux fonctions de base suivantes :

- La détermination de chemin.
- La commutation.

➤ **La Détermination du chemin :**

La détermination du chemin se produit au niveau de la couche réseau. La fonction de détermination de chemin permet à un routeur d'évaluer les chemins vers une destination donnée et de définir le meilleur chemin pour traiter un paquet. Le routeur se sert de la table de

routage pour déterminer le meilleur chemin et transmet ensuite le paquet en utilisant la fonction de commutation.

➤ **La commutation :**

La fonction de commutation est le processus interne qu'utilise un routeur pour accepter un paquet sur une interface et le transmettre à une deuxième interface sur le même routeur. La fonction de commutation a pour responsabilité principale d'encapsuler les paquets dans le type de trame approprié pour la prochaine liaison.

Le routeur utilise la portion réseau de l'adresse pour sélectionner le chemin qui permettra de transmettre le paquet au prochain routeur situé sur le chemin et une fois arrivé au routeur local, il utilise la partie hôte pour déterminer le port vers lequel il va envoyer les paquets.

I.6.4.Choix d'un protocole de routage

Il est donc possible de choisir entre de nombreux protocoles de routage, mais la sélection de celui qui va être implanté et utilisé, dépend principalement de l'architecture du réseau. La plupart des protocoles de routage internes énumérés ci-dessus ont été développés afin de prendre en charge des problèmes d'acheminement spéciaux mis en évidence sur les réseaux de très grande taille. Certains des protocoles ont été uniquement utilisés pour les réseaux nationaux et régionaux de très grande taille. Pour les réseaux locaux, le protocole RIP constitue le choix le plus courant.

I.7.Les VLAN [6]

I.7.1.Définition

Les VLAN sont des regroupements logiques de périphériques au sein d'un même réseau physique, ils sont identifiés par un numéro.

Un groupe de périphériques dans un VLAN communiquent comme s'ils étaient reliés au même câble. Des appareils partageant une même connexion physique, mais isolés logiquement dans des VLAN différents, se comporteront comme s'ils étaient sur des réseaux indépendants.

Les diffusions (broadcast) sont communiquées uniquement à des périphériques d'un même VLAN et les paquets destinés aux stations n'appartenant pas à ce VLAN doivent être transférés par un routeur (ou un appareil ayant des capacités de routage).

I.7.2.Création des VLAN

Il existe deux méthodes :

- **Dynamique :** Un VLAN dynamique est Vlan qui va se créer automatiquement lors d'une tentative de connexion entre des machines de VLAN différents.

- **Statique :** Les VLAN statiques sont créées par l'affectation des ports à un VLAN. Quand une machine entre dans le réseau elle est automatiquement intégrée au VLAN du port.

I.7.3.Intérêts des VLAN

Les VLANS présentent les intérêts suivants :

- Améliorer la gestion du réseau.
- Optimiser la bande passante.
- Séparer les flux.
- Fragmentation : Réduire la taille d'un domaine de broadcast.
- Sécurité : Permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen pour communiquer entre des machines appartenant à des VLANS différents est alors de passer par un routeur.

I.7.4.Principe de fonctionnement

Un VLAN ou réseau virtuel est un regroupement de machine. Ces machines pourront communiquer comme si elles étaient sur le même segment. Un VLAN est assimilable à un domaine de diffusion. Ceci signifie que les messages de diffusion émis par une machine d'un VLAN ne sont reçus que par les machines de ce VLAN.

Les VLAN n'ont été réalisables qu'avec l'apparition des commutateurs (Switch). Avant, pour réaliser des domaines de diffusion, il était nécessaire de créer des réseaux physiques. Les VLAN permettent de continuer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, réseaux logiques qui auront les mêmes caractéristiques que des réseaux physiques.

I.7.5.Types de VLAN

Il existe 3 types de VLAN :

I.7.5.1.Les VLAN par port (VLAN de niveau 1)

On affecte chaque port des commutateurs à un VLAN.L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.

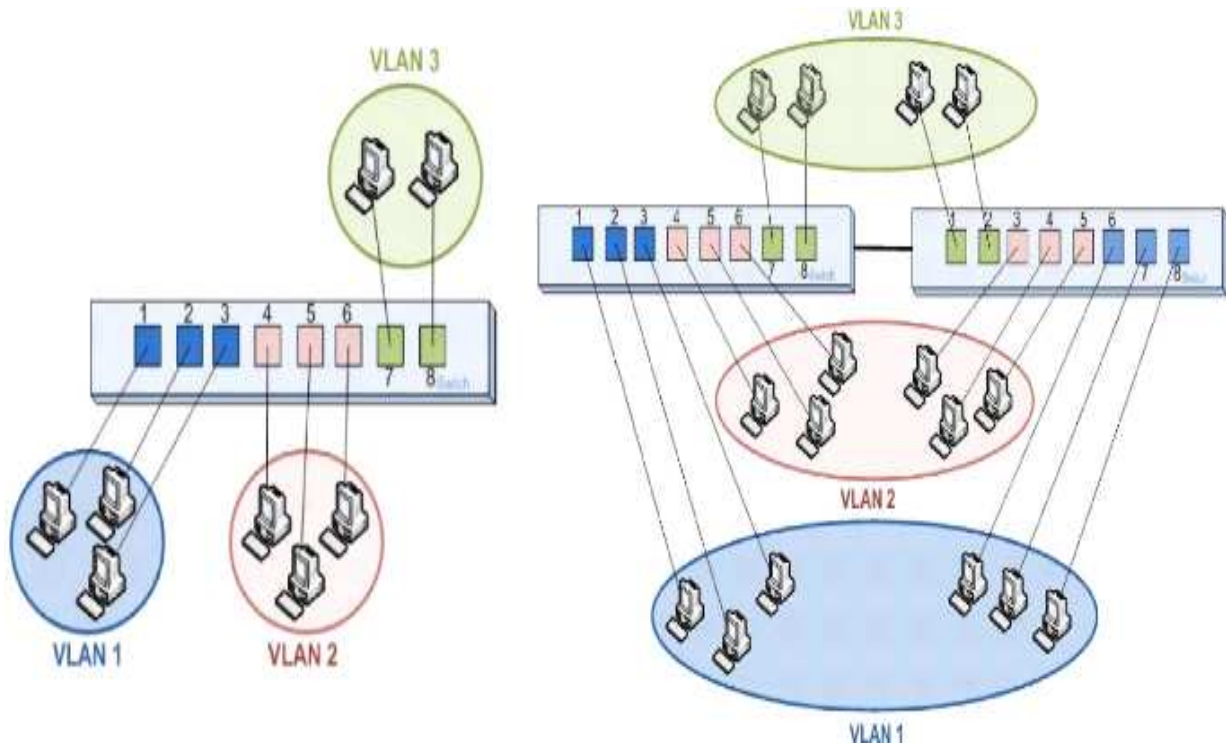


Figure I.4. Les VLAN par ports

I.7.5.2. Les VLAN par adresse MAC (VLAN de niveau 2) :

On affecte chaque adresse MAC à un VLAN. En effet, il s'agit d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.

L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne change pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables). Si on veut changer de vlan il faut modifier l'association mac/vlan.

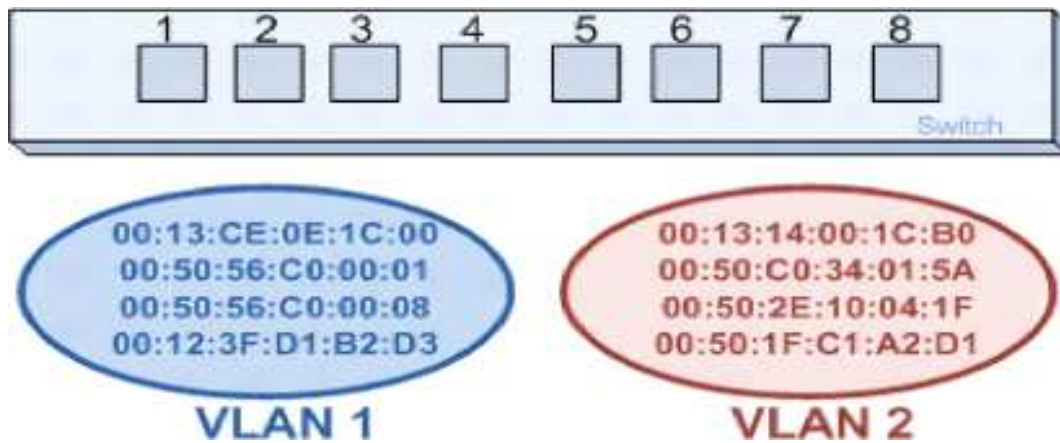


Figure I.5. Les VLAN par adresse MAC

I.7.5.3. Les VLAN par protocole (VLAN niveau 3)

Les vlan de niveau 3 se font de deux manières :

➤ **Le VLAN par sous-réseau (Network Address-Based VLAN)**

Associe des sous réseaux selon l'adresse IP source. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.

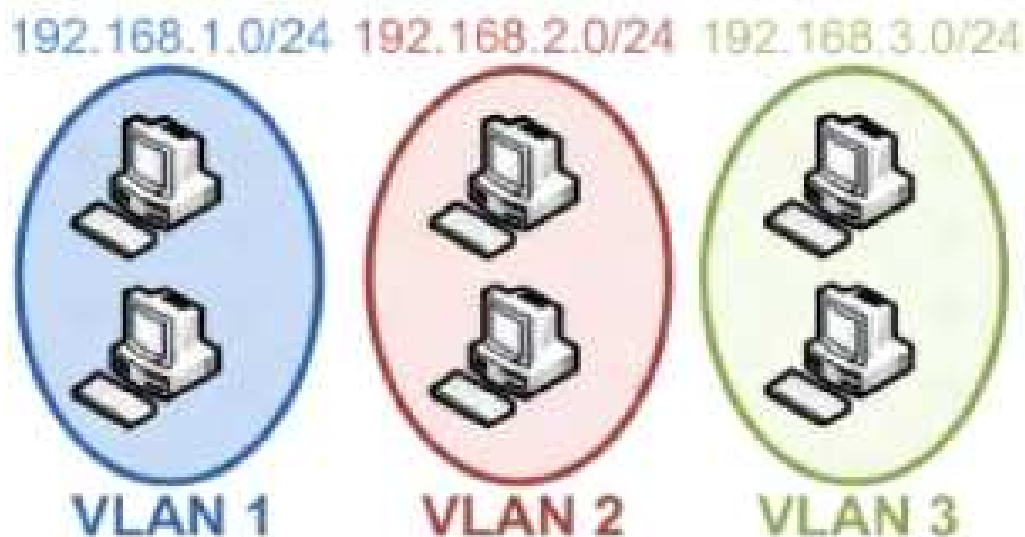


Figure I.6. VLAN par sous réseau

➤ **Le VLAN par protocole (Protocol-Based VLAN)**

Cette solution permet de créer un réseau virtuel par type de protocole (par ex : TCP/IP, IPX, AppleTalk, etc...), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau. Avec les réseaux VLAN basés sur les protocoles, c'est le protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN, cette méthode peut fonctionner dans un environnement où figurent plusieurs protocoles, mais n'est pas très pratique sur un réseau à prédominance IP.

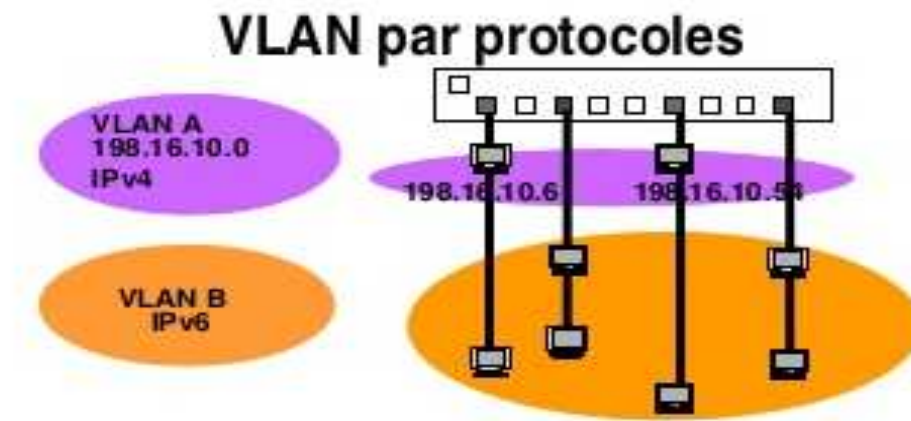


Figure I.7.VLAN par protocole

I.7.6. Avantages des VLAN :

Les réseaux virtuels amènent beaucoup d'avantages :

- Réduction de la diffusion du trafic.
- Création de groupes de travail indépendamment de l'infrastructure physique.
- Contrôle des échanges inter-VLAN pour le renforcement de la sécurité du réseau.
- Une meilleure utilisation des serveurs réseaux.
- L'augmentation considérable des performances du réseau.
- La simplification de la gestion.
- La flexibilité de segment du réseau.
- La technologie évolutive et la flexibilité de segmentation du réseau.
- La simplification de la gestion.
- Le renforcement de la sécurité du réseau.

Les messages de diffusion (broadcaste) sont limités à l'intérieur de chaque VLAN. Ainsi les broadcaste d'un serveur peuvent être limités aux clients de ce serveur.

Des groupes de stations peuvent être réalisés sans remettre en cause l'architecture physique du réseau. De plus, un membre de ce groupe peut se déplacer sans changer de réseau virtuel.

Les échanges inter-VLAN se réalisent tout comme des échanges inter-réseaux, c'est-à-dire au travers de routeurs. Il est par conséquent possible de mettre en œuvre un filtrage du trafic échangé entre les VLAN.

I.7.7. Routage inter VLAN

Il existe deux techniques de routage inter-vlan en utilisant un routeur :

- Routage physique
- Routage logique

I.7.7.1. Routage inter VLAN physique

Le routage inter VLAN physique consiste à associer une interface du routeur à chaque VLAN.

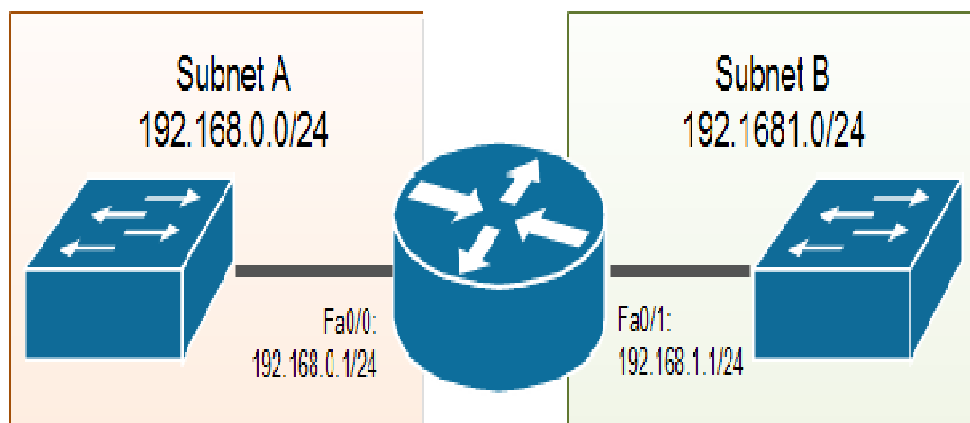


Figure I.8. Routage physique

Dans cet exemple nous avons deux VLAN donc deux liens physiques. Pour configurer le routage inter-VLAN, il nous faut d'abord configurer le Switch 2 pour que l'interface Fa0/3 soit dans le VLAN 10 et que l'interface Fa0/4 soit dans le VLAN 20.

Ensuite, on configure les adresses IP des interfaces du routeur pour qu'elles correspondent au bon sous-réseau.

I.7.7.2.Routage inter-VLAN logique

Cette technique consiste à diviser une interface physique d'un routeur en plusieurs sous interfaces logiques et associer à chaque VLAN une sous interface.

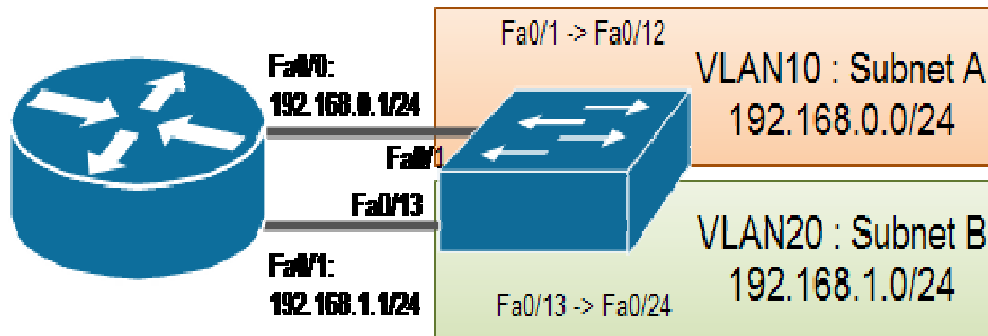


Figure I.9.Routage logique

Nous avons donc créé deux sous interfaces Fa0.10 et Fa0/0.20 l'une pour le vlan 10 et l'autre pour le VLAN 20. L'interface physique doit être allumée pour que le routage inter-VLAN fonctionne.

Notre routage inter-VLAN est configuré, les VLAN peuvent maintenant communiquer entre eux à condition de désigner comme passerelle par défaut des ordinateurs l'adresse IP de l'interface du routeur correspondant au VLAN auquel appartient l'ordinateur.

I.7.7.3.Comparaison entre les deux techniques du routage inter-vlan

Routage physique	Routage logique
Une interface physique par VLAN	une interface physique pour de nombreux VLAN
Aucun conflit de bande passante	Conflit de bande passante
Connectée au port de commutateur en mode d'accès	Connectée au port de commutateur en mode d'agrégation
Plus couteuse en termes de port	Moins couteuse en termes de port
Configuration de connexion plus complexe	Configuration de connexion moins complexe

Tableau I.1.Comparaison des techniques de routage

I.8. Discussions

On peut dire qu'Internet n'est rien d'autre qu'un immense réseau de lien et d'interconnexion entre plusieurs réseaux. Pour savoir le chemin à emprunter parmi tous ces liens pour aller d'un réseau à un autre, il faut qu'un protocole de routage soit mis en place. En final, on peut dire que le rôle principal du routage est de définir une route ou un chemin à un paquet quand celui-ci arrive sur un routeur ; d'où on peut dire que le routage s'effectue sur deux opérations:

La sélection de la meilleure voie.

Faire la distinction entre les protocoles de routage : comment réaliser l'acheminement des Paquets.

Parmi les différentes caractéristiques du routage on peut citer celles-ci :

- Le routage IP est basé uniquement sur l'adresse du destinataire.
- Chaque équipement du réseau sait atteindre un équipement d'un autre réseau, s'il existe au moins un équipement de routage pour acheminer les paquets à l'extérieur du réseau local.
- Les informations de routage sont mémorisées dans la table de routage des équipements (routeurs), cette table doit être périodiquement mise à jour :
 - Manuellement : routage statique
 - Automatiquement : routage dynamique.

Le but du routage est donc d'assurer qu'il existe toujours un chemin pour aller d'un réseau à un autre.

CHAPITRE II

La téléphonie sur IP

II.1. Préambule

Suite à l'explosion de la bande passante sur les réseaux IP et à l'avènement du haut débit chez les particuliers, de nouvelles techniques de communications sont apparues ces dernières années. L'une des plus en vogue actuellement, est ce que l'on appelle « Voix sur IP ».

II.2. Standard téléphonique IPBX [7]

Aujourd'hui, les standards téléphoniques utilisent de plus en plus souvent les technologies issues d'Internet. Ces technologies font appel à la notion et à la technologie désignée sous l'appellation « IP » (Internet Protocol) pour transporter les informations sur le réseau Internet.

Le marché des standards téléphoniques reflète l'intérêt croissant des entreprises pour ces nouvelles technologies. Il se divise en trois segments :

- a. Les systèmes traditionnels PABX à commutation, sur lesquels on peut raccorder des postes numériques et des terminaux analogiques.
- b. Les systèmes IPBX sur lesquels on peut raccorder des SOFTPHONES et des postes IP, ainsi que des terminaux analogiques. Ce que nous allons traiter dans ce mémoire.
- c. Les systèmes hybrides (numériques et IP).

II.3. Définition de la téléphonie sur IP [8]

Avant toute exploitation technique, il convient dans un premier temps, de présenter la téléphonie sur IP (ToIP signifie Telephony over IP) qui est de plus en plus utilisée dans les sociétés Algériennes. En effet, ses multiples atouts font de cette technologie une solution attirante pour les administrateurs, tant au niveau prise en charge qu'au niveau financier. La téléphonie sur IP utilise la transmission de la voix sur le réseau IP (VoIP signifie Voice over Internet Protocol) qui est une technologie permettant de communiquer en utilisant Internet et les réseaux IP au lieu des lignes téléphoniques standards.

II.4. Les notions de base de la ToIP [9]

Malgré la forte croissance des flux de données véhiculés dans l'entreprise, la téléphonie reste encore le média principal. La téléphonie classique repose sur une technologie de communication de circuits. Cette technologie est robuste et « bien rodée » d'où une forte disponibilité. La téléphonie sur IP utilise la technologie de voix sur IP qui transforme la voix en paquets de données et transmet les conversations via le même réseau que celui utilisé pour envoyer des fichiers et du courrier électronique.

Plus concrètement, la ToIP correspond au service téléphonique entre deux terminaux sur un réseau IP.

Sans la téléphonie sur IP il existe deux réseaux: Le réseau informatique par lequel transitent les données, et le réseau téléphonique par lequel transite la voix. Le but de la (ToIP) est d'unifier ces deux réseaux.

II.4.1.Principe de la ToIP

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

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

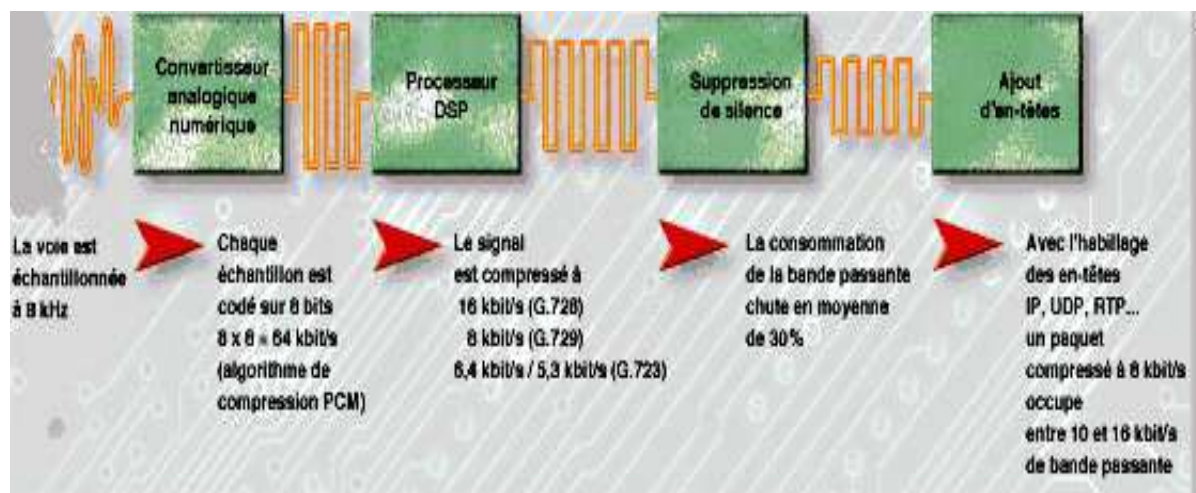


Figure II.1.Numérisation de la voix

A l'arrivée, les paquets transmis sont réassemblés en supprimant d'abord les entêtes. Le signal de données ainsi obtenu est décompressé puis converti en signal analogique afin que l'utilisateur puisse écouter le message d'origine.

La ToIP est une extension des possibilités de la VoIP. En effet, elle repose sur deux principes :

- Le découplage du flux voix numérisé en une suite de paquets.
- Transit sur le réseau IP.

II.4.2. Fonctionnement de la VoIP

Lorsqu'un utilisateur veut entrer en communication avec un autre, une connexion est alors établie entre les deux terminaux. L'utilisateur peut alors émettre un son par le biais d'un micro (signal analogique) qui est ensuite numérisé et compressé par la machine (signal par synthèse).

Une fois les données encapsulées dans un paquet, il est envoyé au destinataire qui procèdera aux opérations inverses assurant ainsi la mise en forme d'un message audible.

Schématiquement le transport de la voix se fait ainsi :

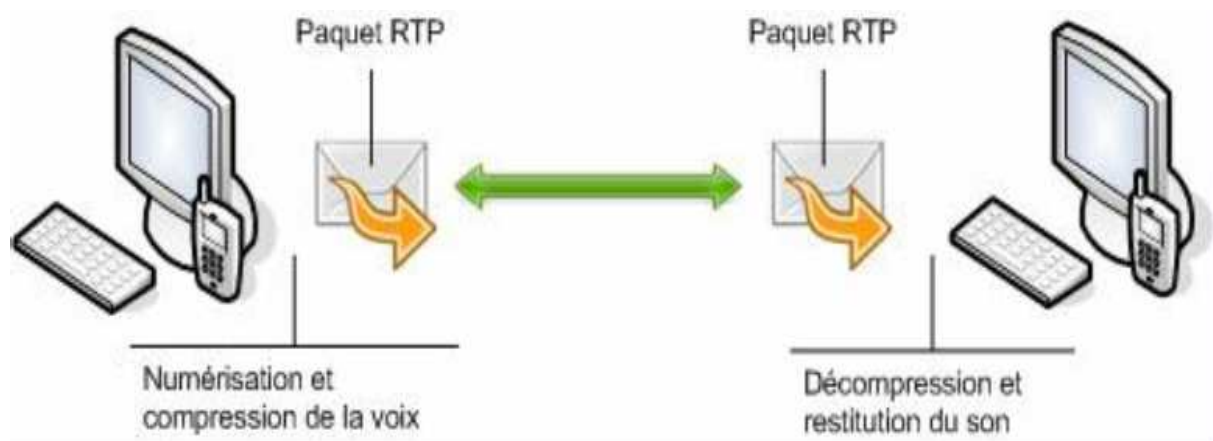


Figure II.2. Transport de la voix

II.4.3. La téléphonie par circuits et par paquets

Dans la communication à transfert des paquets, toutes les informations à transporter sont découpées en paquets pour être acheminées d'une extrémité à une autre du réseau.

L'équipement terminal A souhaite envoyer un message à l'équipement B. Le message est découpé en trois paquets, qui sont émis de l'équipement terminal vers le premier nœud du réseau, dans lequel on les envoie à un deuxième nœud, et ainsi de suite, jusqu'à ce qu'ils arrivent à l'équipement terminal B. où les paquets sont rassemblés pour reconstituer le message de départ.

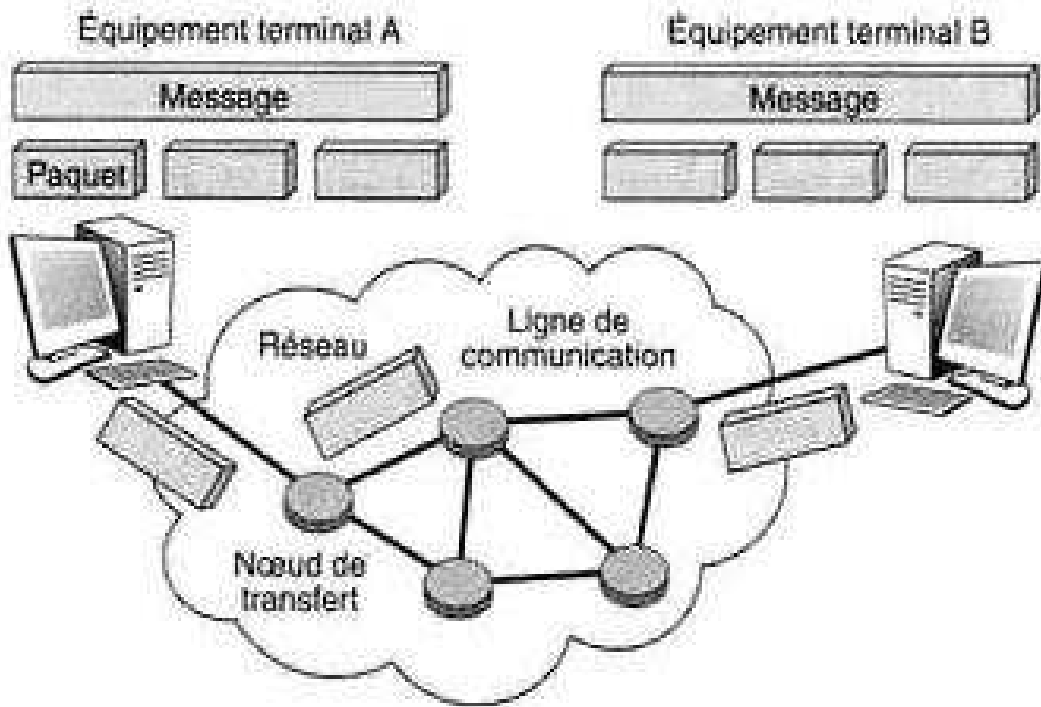


Figure II.3. La technique de transfert des paquets

Dans la parole téléphonique, l'information est regroupée pour être placée dans un paquet, comme illustré à la figure II.3. Le combiné téléphonique produit des octets, provenant de la numérisation de la parole, c'est-à-dire le passage d'un signal analogique à un signal sous forme de 0 et de 1, qui remplissent petit à petit le paquet. Dès que celui-ci est plein, il est émis vers le destinataire. Une fois le paquet arrivé à la station terminale, le processus inverse s'effectue, restituant les éléments binaires régulièrement à partir du paquet pour reconstituer la parole téléphonique.

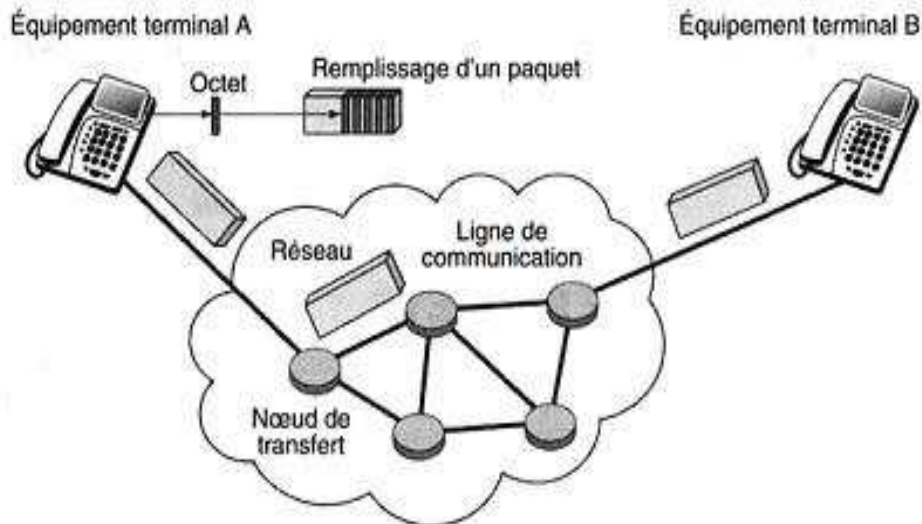


Figure II.4. Un flot de paquets téléphoniques

Le réseau de transfert est lui-même composé de nœuds, appelés nœuds de transfert reliés entre eux par des lignes de communication, sur lesquelles sont émis les éléments binaires constituant les paquets. Le travail d'un nœud de transfert consiste à recevoir des paquets et à déterminer vers quel nœud suivant ces derniers doivent être acheminés.

Le paquet forme donc l'entité de base, transférée de nœud en nœud jusqu'à atteindre le récepteur. Ce paquet est regroupé avec d'autres paquets pour reconstituer l'information transmise. L'action consistant à remplir un paquet avec des éléments binaires en général regroupés par octet ce qui s'appelle la mise en paquet, ou encore la paquetsation, et l'action inverse, consistant à retrouver un flot d'octets à partir d'un paquet, la dépaquetsation.

II.5. Le déroulement d'une communication téléphonique sur IP [10]

Une communication téléphonique se déroule dans un parcours contenant les cinq grandes étapes suivantes :

I.5.1. Mise en place de la communication

Une signalisation démarre la session. Le premier élément à considérer est la localisation du récepteur (User Location). Elle s'effectue par une conversion de l'adresse du destinataire (adresse IP ou adresse téléphonique classique) en une adresse IP d'une machine qui puisse joindre le destinataire (qui peut être le destinataire lui-même).

Le protocole DHCP (Dynamic Host Configuration Protocol) et les passerelles spécialisées (gatekeeper) sont employés à cette fin.

II.5.2.Etablissement de la communication

Cela passe par une acceptation du terminal destinataire, que ce dernier soit un téléphone, une boîte vocale ou un serveur Web. Plusieurs protocoles de signalisation sont utilisés pour cela, en particulier le protocole SIP (Session Initiation Protocol) de l'IETF.

II.5.3.Transport de l'information téléphonique

Le protocole RTP (Real-time Transport Protocol) prend le relais pour transporter l'information téléphonique proprement dite. Son rôle est d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie de façon à reformer le flot avec ses caractéristiques de départ (vérification du synchronisme, des pertes, etc.).

C'est un protocole de niveau transport, qui essaye de corriger les défauts apportés par le réseau.

II.5.4.Changement de réseau

Un autre lieu de transit important de la ToIP est constitué par les passerelles, qui permettent de passer d'un réseau à transfert de paquets à un réseau à commutation de circuits, en prenant en charge les problèmes d'adressage, de signalisation et de transcodage que cela pose. Ces passerelles ne cessent de se multiplier entre FAI et opérateurs télécoms.

II.5.5.Arrivée au destinataire

De nouveau, le protocole SIP envoie une requête à la passerelle pour déterminer si elle est capable de réaliser la liaison circuit de façon à atteindre le destinataire.

En théorie, chaque passerelle peut appeler n'importe quel numéro de téléphone. Cependant, pour réduire les coûts, mieux vaut choisir une passerelle locale, qui garantit que la partie du transport sur le réseau téléphonique classique est le moins cher possible.

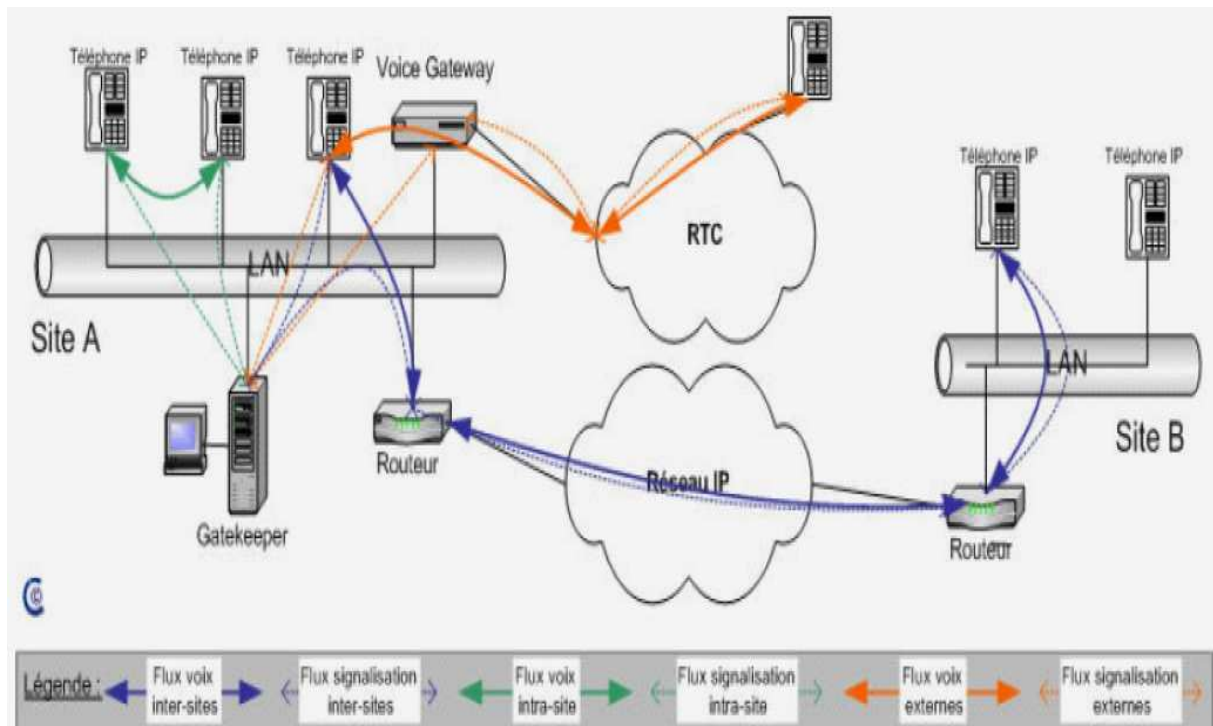


Figure II.5. Schéma illustratif de la communication ToIP

II.6. Avantages et inconvénients de la téléphonie sur IP [11]

II.6.1. Avantages

La téléphonie sur IP présente de nombreux avantages :

- Rapidité dans le traitement et l'acheminement des appels.
- Tarifs plus intéressants par rapport à ceux des appels traités par la technologie analogique traditionnelle.
- Une convergence téléphone/ordinateur optimisée puisque les deux systèmes utilisent la même technologie de communication et de transmission des données.

II.6.2. Inconvénients

Les inconvénients que présente la téléphonie IP sont :

- Peut nécessiter une connexion Internet permanente et de bonne qualité.
- Prix des postes IP supérieur à celui des postes téléphoniques classiques.

II.7. Les protocoles utilisés pour la Téléphonie IP [12]

Il existe plusieurs protocoles non propriétaires supportant la ToIP :

❖ Le H323

Certainement le plus connu, il se base sur les travaux de la série H.320 sur la visioconférence sur RNIS. Il regroupe un ensemble de protocoles de communication de la voix, de l'image et de données sur IP.

❖ Le SIP (Session Initiation Protocol)

Il s'agit d'un protocole standard ouvert de gestion de sessions souvent utilisé dans les télécommunications multimédia (son, image, etc.). Il est depuis 2007 le plus courant pour la téléphonie par internet (la ToIP). Ce protocole n'est pas seulement destiné à la ToIP ou la VoIP mais également à de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo.

❖ Le MGCP (Media Gateway Control Protocol)

Protocole complémentaire à H.323 ou SIP, il traite les problèmes d'interconnexion avec le monde téléphonique (SS7, RI).

❖ RTP (Real Time Transport Protocol) C'est un protocole dont le but est de fournir un moyen uniforme de transmission IP des données temps - réel. Il est utilisé pour le transport des données audio et vidéo appartenant à des applications bâties sur H.323 ou SIP.

❖ RTCP (Real Time Transport Control Protocol)

Ce protocole est celui du contrôle des flux RTP. Il est donc complémentaire à RTP et agit en envoyant à intervalles réguliers des paquets de contrôle contenant des statistiques et des informations sur la session ouverte.

II.8. Paramètres influant sur la transmission de la voix sur IP [13]

Le transport de la voix à travers un réseau IP ne comporte pas les mêmes exigences que celui des données. En effet, la voix exige un fonctionnement en temps réel et des mécanismes performants de maintien de la qualité de service. De plus, certains paramètres, qui dans le transport de données n'avaient presque pas d'importance, deviennent très déterminants en ToIP.

II.8.1. Traitement de la voix

Pour être transportée sur un réseau IP, la voix doit tout d'abord être numérisée puis compressée. Le standard le plus utilisé est le G.711 ou Pulse Code Modulation (PCM). Néanmoins, il existe actuellement des algorithmes de compression qui permettent de conserver une bonne qualité sonore avec des taux de compression élevés.

II.8.2. Bande passante

La bande passante est un élément important à prendre en compte dans la mise en place d'un service de ToIP. En effet, plus elle est faible, plus il y a des risques de congestions sur le réseau, ce qui cause des retards et des pertes de paquets. Toutes choses qui handicapent le bon fonctionnement du service téléphonique. De prime à bord, on pourrait penser à augmenter la bande passante disponible quand on envisage de mettre en place un service de téléphonie sur IP. Cependant, cela n'est pas très souvent une manœuvre utile. L'essentiel est de connaître l'ensemble des flux traversant le réseau. Une fois que cela est fait, il faut mettre en place une politique de gestion adéquate de la bande passante pour permettre un bon fonctionnement du service.

II.8.3. Latence

La latence définit le temps mis par un paquet pour aller de sa source à sa destination. Pour les applications temps réels et autres applications interactives, une très grande latence engendre des retards qui peuvent s'avérer compromettantes pour la qualité de service. En téléphonie IP, le besoin d'offrir un véritable mode conversationnel interdit la présence d'une latence élevée. Par ailleurs, la latence ne se résume pas uniquement au temps de transport des paquets de voix. Le temps de codage et de mise en paquets, le temps de traversée des routeurs, le temps de séjour dans les tampons ou buffers sont autant d'éléments qui jouent aussi sur elle. Sa valeur ne doit toutefois pas excéder 150 ms. La création de protocoles simplifiés de transport de la voix comme RTP et RTCP qui ont pour but de réduire la latence.

II.8.4. Gigue de phase

La gigue de phase représente la variation du temps de transit. Mathématiquement parlant, c'est la variance statistique du délai de transmission autrement dit, la variation de temps entre le moment où les deux paquets auraient dû arriver et le moment de leur arrivée effective. Elle découle du fait que tous les paquets ne traversent pas le réseau à la même vitesse. La gigue de phase est un phénomène totalement indépendant de la latence. En fait il peut même arriver qu'on observe une gigue excessive sur un réseau pourtant d'une bonne latence.

II.8.5.Echo

L'écho est un phénomène causé par les parties analogiques du système téléphonique IP. Il est lié principalement à des ruptures d'impédance lors du passage de 2 fils à 4 fils, autrement dit lors du passage des tronçons analogiques aux tronçons numériques des voies de communication. C'est donc un paramètre propre aux architectures hybrides. Sa valeur doit être inférieure à 50 ms. Pour corriger l'écho, il existe des méthodes. Malheureusement, ces correctifs comportent l'inconvénient de provoquer des sifflements. En effet, les correctifs sont liés au matériel utilisé. Ce qui les rend dépendant de celui - ci et les sifflements observés surviennent quand le matériel utilisé de part et d'autre n'est pas le même.

II.8.6.Perte des paquets

La perte des paquets est la conséquence de congestions sur le réseau ou de gigue excessives qui poussent certains éléments du réseau IP à rejeter certains paquets entrants en fonction de seuils prédéfinis. Cela a pour but de libérer de la bande passante. Cependant, bien que la ToIP supporte assez bien les pertes de paquets, il faut néanmoins que ces pertes restent inférieures à un certain seuil (généralement 1 à 2%). Sinon les utilisateurs observeront des coupures de conversation. Un problème majeur lié à la perte de paquets est le fait qu'il soit impossible, ou pour être plus exact, inutile de retransmettre les paquets perdus. En effet, un paquet réémis arriverait bien trop tard pour être d'une quelconque utilité. Afin de limiter les pertes de paquets, il y a des mécanismes de récupération des paquets perdus au niveau des éléments du réseau. Ces mécanismes sont couplés à des méthodes de correction d'erreurs qui injectent des informations redondantes dans les paquets transmis afin de reconstituer les paquets manquants. Toutefois, il faut être prudent en mettant en place de tels mécanismes car un mauvais paramétrage induira une importante latence.

II.9.Les mesures de sécurité spécifiques à la téléphonie sur IP [13]

Il est crucial d'appliquer le principe de défense en profondeur directement au niveau des téléphones.

Ces équipements peuvent être source de nombreuses vulnérabilités pour les raisons suivantes :

- Le système d'exploitation qu'ils utilisent peut être atypique.
- Leur nombre peut être très important au sein d'un même parc.
- Ils peuvent être répartis sur des sites géographiquement très éloignés.
- Ils ne sont pas nécessairement placés dans des lieux dont la sécurité physique est assurée.

- Le parc déployé peut être très hétérogène (différents modèles installés).
- Le renouvellement du parc n'est pas aussi fréquent que pour des postes informatiques.

II.10. Modes de déploiement [14]

Les téléphones IP peuvent être déployés de différentes manières. Le choix s'opère souvent en fonction des besoins et des contraintes métier de l'organisme.

La première solution consiste à attribuer nominativement un téléphone à chaque usager, cela suppose que les personnes ne soient pas mobiles dans les locaux et qu'elles disposent d'un espace physique de travail qui leur est propre.

La seconde option vise à banaliser les postes téléphoniques, un poste n'est pas affecté à un usager, il peut être utilisé par n'importe quel abonné dès lors qu'il s'est correctement authentifié sur l'équipement. Ce mode de déploiement est généralement désigné par le terme de free seating.

Les deux modes de déploiement peuvent être utilisés dans une même architecture de téléphonie sur des périmètres géographiques ou fonctionnels distincts mais, les mesures de sécurisation des téléphones IP doivent être appliquées de façon homogène à l'ensemble du parc.

II.10.1. Codes d'accès utilisateur

Quelle que soit la logique de déploiement retenue, il est recommandé de protéger les téléphones IP à l'aide de codes d'accès spécifiques à chaque utilisateur.

La saisie sur le poste, par l'utilisateur, de son identifiant et de son code personnel (ou PIN) lui permet d'accéder à son environnement personnel et de profiter de l'ensemble des services téléphoniques qui ont été affectés à son profil.

Voici quelques recommandations à respecter dans la gestion des codes PIN :

- A l'installation, un code PIN aléatoire doit être généré pour remplacer celui présent par défaut sur les postes. Ce code est communiqué à l'utilisateur pour qu'il puisse le modifier.
- Chaque utilisateur doit être contraint de modifier son code personnel lors du premier accès au service de téléphonie. L'idéal est d'activer une mesure technique obligeant l'utilisateur à changer son PIN. Si la solution de téléphonie employée ne dispose pas d'une telle fonctionnalité, une contrainte organisationnelle doit être mise en œuvre pour s'assurer que chaque usager a personnalisé son code d'accès.

- Une politique de gestion des codes d'accès doit être définie (complexité : a minima 5 caractères pour les codes PIN, fréquence de renouvellement, nombre de tentatives avant verrouillage du compte, etc.).

II.10.2.Codes d'accès administrateur

Les solutions de téléphonie offrent généralement la possibilité de configurer un code d'accès administrateur sur les postes afin de permettre la modification de certains éléments de configuration directement à partir de l'équipement (configuration du réseau, des services actifs, etc.).

L'idéal est de désactiver ce type d'accès une fois le déploiement terminé et de permettre la modification des paramètres des téléphones uniquement au niveau des serveurs de configuration centraux à partir desquels les postes téléchargent leur configuration. S'il n'est pas possible de désactiver les accès administrateur au niveau des téléphones, les recommandations de sécurité relatives à la génération des mots de passe doivent être appliqués lors de la configuration des postes.

II.10.3.Interfaces de communication

Désactiver l'ensemble des interfaces de communications non utilisées par les téléphones IP.

La surface d'attaque des téléphones IP doit être réduite au strict minimum, aussi bien au niveau physique qu'au niveau logiciel. Au niveau physique, l'ensemble des connectiques présentes sur les téléphones sont des vecteurs potentiels d'attaques.

À ce titre l'ensemble des interfaces de communication non utilisées doivent être désactivées, par exemple :

➤ **Port Ethernet Additionnel**

Certains modèles de téléphones IP disposent d'un port Ethernet supplémentaire permettant de raccorder un autre équipement au réseau via la fonctionnalité de commutateur intégré au poste. En application du principe de séparation des réseaux de téléphonie et de données, il est recommandé de désactiver le port Ethernet additionnel afin d'éviter tout raccordement (volontaire ou non) d'un équipement non autorisé aux réseaux de téléphonie.

➤ **Port USB**

Certains modèles de téléphones IP disposent d'un port USB, celui-ci peut être utilisé pour ajouter des fonctionnalités (connexion d'une caméra par exemple) ou pour réaliser des opérations de maintenance spécifiques. Il est recommandé de désactiver ce

port qui pourrait être employé par une personne mal intentionnée pour installer, par exemple, un système d'exploitation piégé sur les équipements.

II.10.4.Services non essentiels

Désactiver l'ensemble des services qui ne sont pas strictement nécessaires au fonctionnement des téléphones IP; en particulier les services non sécurisés et les mécanismes de prise de contrôle à distance des postes (web services, Telnet, etc.).

Les services non sécurisés doivent également être désactivés et remplacés par d'autres utilisant des mécanismes cryptographiques robustes, s'ils sont nécessaires au fonctionnement des téléphones.

II.10.5.Informations techniques

Masquer aux utilisateurs les informations techniques superflues affichées sur les postes téléphoniques.

Les informations techniques affichées sur les postes téléphoniques, lors de la séquence de démarrage ou via des menus, peuvent faciliter la mise au point de scénarios d'attaques par des personnes mal intentionnées. À ce titre, il est préférable de masquer aux utilisateurs les informations techniques qui ne leur sont pas utiles pour un usage quotidien (version logicielle, plan d'adressage, etc.).

II.10.6.Inscription des téléphones

La fonctionnalité d'inscription automatique des téléphones auprès des équipements centraux peut être employée mais, celle-ci doit être désactivée une fois le déploiement initial achevé.

Les solutions de téléphonie sur IP offrent généralement la possibilité d'inscrire automatiquement les postes téléphoniques, auprès des serveurs centraux, lors de leur installation. Cette fonctionnalité permet le déploiement rapide d'un parc composé de plusieurs centaines d'équipements, mais elle comporte des risques si elle reste activée après la phase de déploiement. Une personne mal intentionnée peut par exemple tenter de connecter au réseau un téléphone IP de modèle identique mais provenant de l'extérieur.

Si l'inscription du poste réussit, l'attaquant pourrait bénéficier de l'accès à de nombreux services et pourrait même compromettre entièrement l'infrastructure de téléphonie, voir l'ensemble du système d'information. L'inscription automatique des postes n'est pas déconseillée lors du déploiement d'un parc important, mais uniquement si des mécanismes de contrôle d'accès au réseau sont correctement mis en œuvre en complément.

Il est par contre recommandé de désactiver la fonctionnalité d'inscription automatique des postes une fois la phase d'installation du parc terminée. L'ajout d'un nouveau poste ou le remplacement d'un équipement défectueux devra ensuite contacter les responsables du cite centrale.

II.11.Discussions

Au final, la téléphonie IP peut être un facteur important en terme de valeur ajoutée au sein d'une organisation, du point de vue qu'elle permettrait de se moderniser vis-à-vis des dernières technologies de pointes, de réduire les coûts d'exploitation et de mettre à disposition un outil reliant téléphonie et réseau IP.

CHAPITRE III

Application (Routeur CISCO)

PARTIE 1

Mise en place d'une solution ToIP sous
le réseau Intranet d'Algérie Telecom

III.1.Préambule

A ce niveau, on va présenter notre travail, qui consiste à implémenter une solution de téléphonie IP. Pour cela on va utiliser le logiciel Packet Tracer afin de simuler l'implantation en virtuelle. (cas pratique au niveau d'Algérie Telecom) .

III.2.Présentation de Packet Tracer [15]

Packet Tracer est un programme de simulation des réseaux puissants qui permet de configurer les différents composants d'un réseau informatique.

Il permet aussi de configurer à l'aide d'interface graphique les différents matériels de la marque CISCO.

III.2.1.Pourquoi Packet Tracer ?

Packet Tracer constitue une solution parfaite pour la construction des réseaux ainsi que leurs test avant de les mettre en œuvre sur le terrain, il est simple a manipuler et son avantage le plus important est qu'il fonctionne en temps réel et il nous offre des blocs de tous les routeurs, commutateurs, ponts..... que Cisco a mit à disposition de ses clients .

III.2.2. Présentation de la fenêtre principale

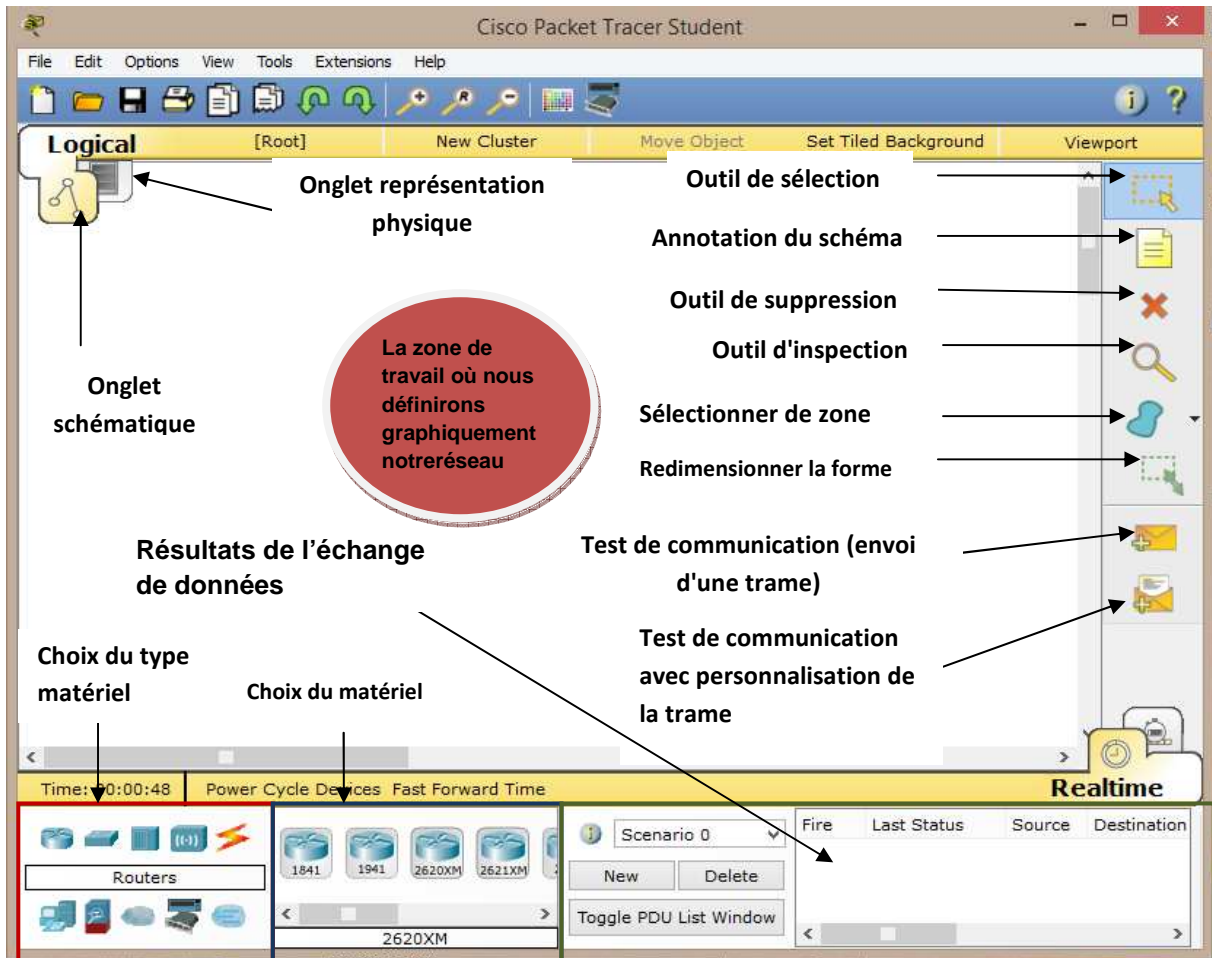


Figure III.1. Présentation de l'écran principale

Cette figure présente l'interface principale de Packet Tracer, Cette interface permet la création des schémas de réseau qu'on veut réaliser.

III.3.Présentation de la topologie du réseau du LET [16]

L'architecture du réseau est divisé en deux services, à savoir le service maintenance et celui du chef de centre on trouve aussi dans ce même diagramme la central qui ce trouve sur Alger. La topologie du réseau utilisé est sous forme d'une étoile

- ❖ **Centrale d'Alger:** C'est à son niveau qu'on trouve le serveur qui attribue une plage d'adresse fixe pour les postes IP et c'est dans ce même serveur que les Vlan (Vlan des téléphone IP) est déclarés.

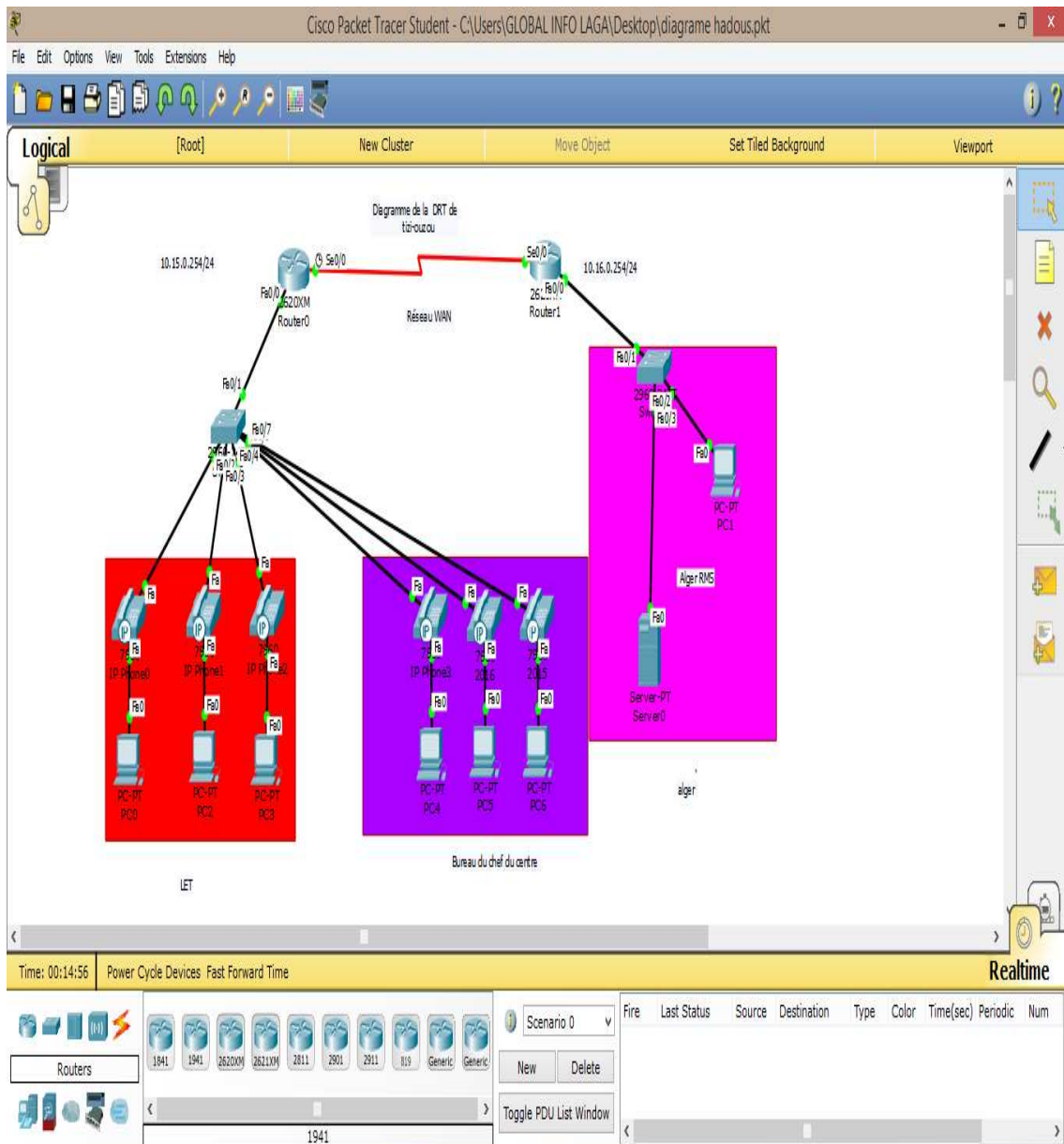


Figure III.2.Le Réseau du LET Après la configuration des téléphone IP Et les Vlan

III.4.L'implémentation de la solution ToIP sous le réseau Intranet d'Algérie Télécoms avec Packet Tracer

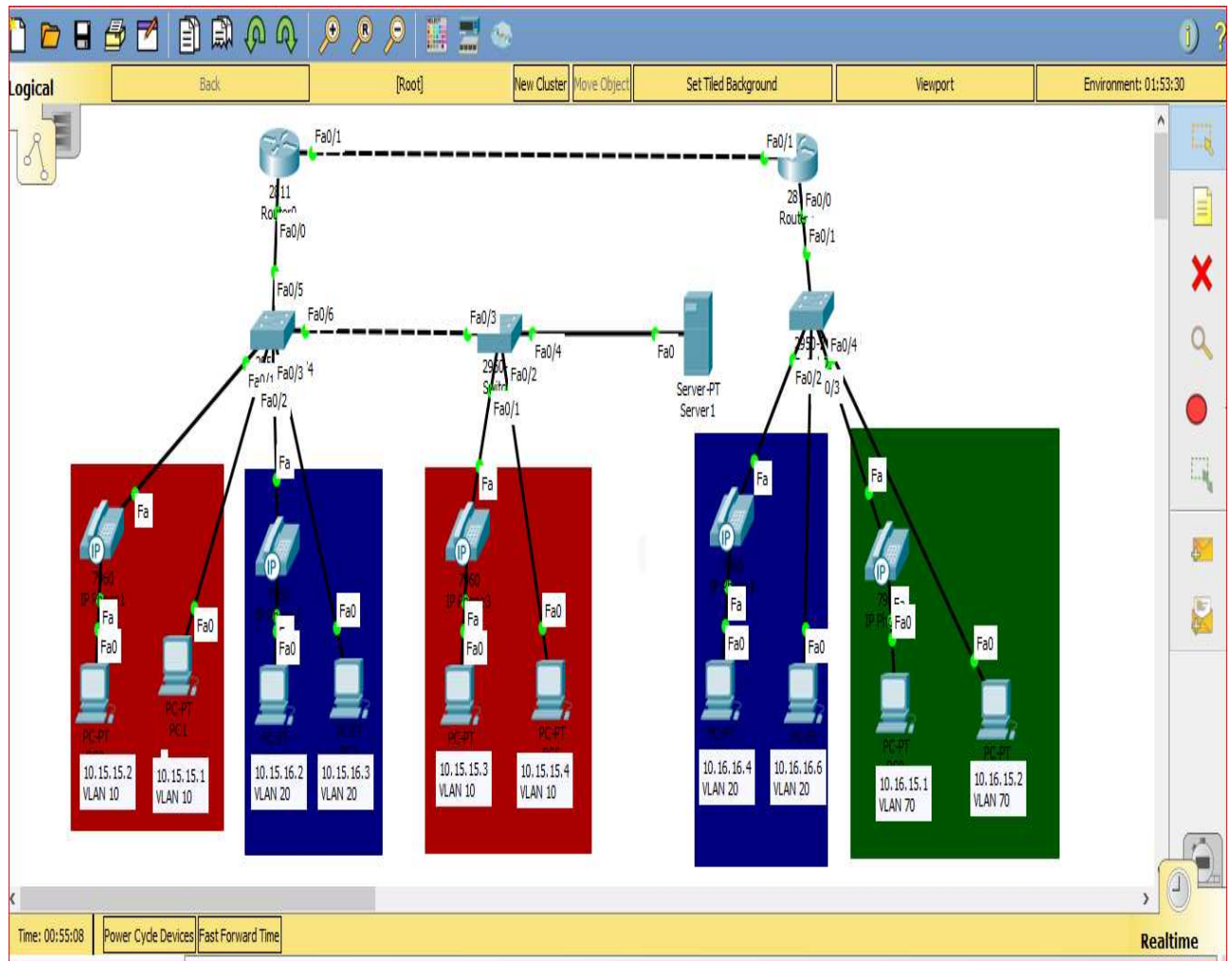


Figure III.3.Présentation du réseau qui relie deux sites sous la solution ToIP

Nous avons utilisé le logiciel Cisco Packet tracer pour simuler la solution ToIP et mieux expliquer les différentes configuration apportées aux équipements réseaux des deux sites Tizi Ouzou (LET) et Alger en suivant les étapes ci-dessus :

III.4.1.Architecture du réseau LET

Au niveau du réseau LET nous disposons d'un routeur, deux Switches, un serveur Intranet, appareils téléphoniques et des positions de travail.

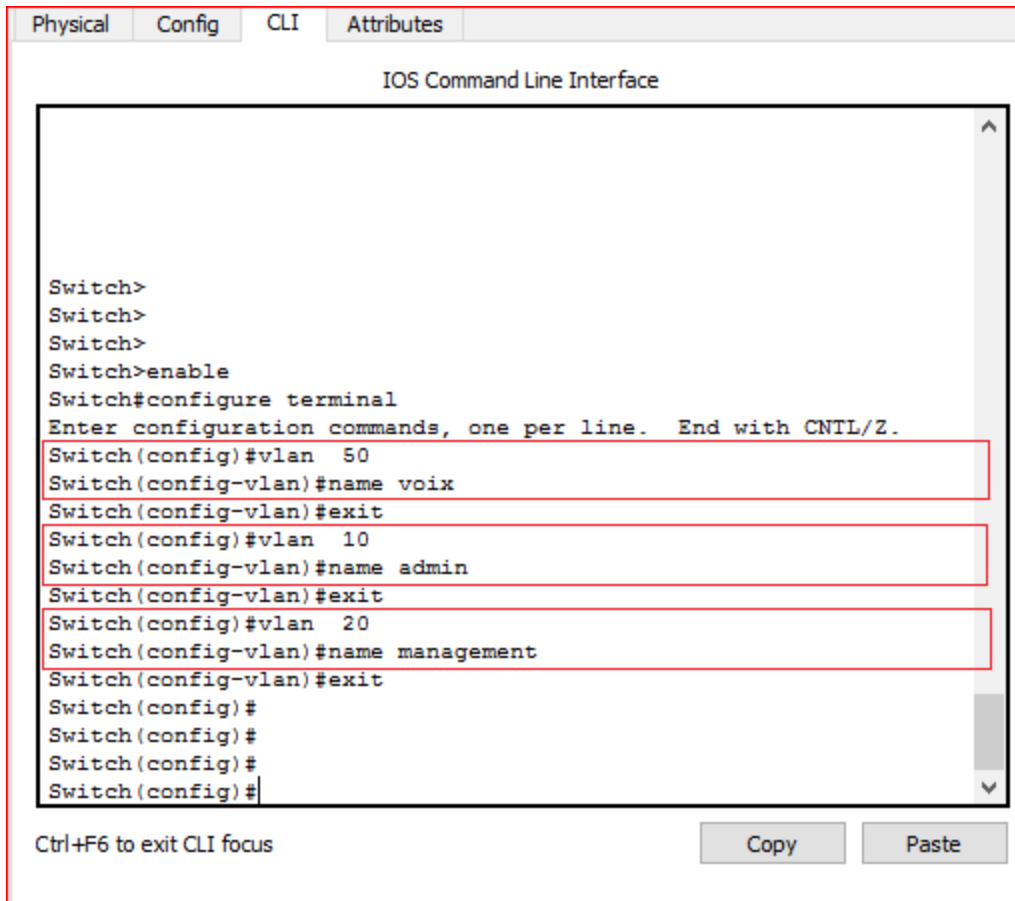
III.4.2. Configuration des Switches

➤ Switch 1

a) **Création des Vlan** : à ce niveau là on va créer trois vlan différents le vlan 50 pour la voix le 10 pour l'administration et le 20 pour le management, On utilisant les commandes suivantes :

- Switch>enable
- Switch # configure terminal
- Switch (config) # vlan 50
- Switch (config-vlan) # name voix
- Switch (config-vlan) #exit

➤ De la même façon on déclare le vlan 10 et le vlan 20



```
Physical Config CLI Attributes
IOS Command Line Interface

Switch>
Switch>
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name voix
Switch(config-vlan)#exit
Switch(config)#vlan 10
Switch(config-vlan)#name admin
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name management
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figure III.4. Création des trois vlan 10,20 et 50

b) Configuration des interfaces: Dans cette étape on va attribuer chaque port à son vlan et pour spécifier chaque port à son vlan on utilise le mode Access

Le mode Access [17] : ce mode est utilisé pour la connexion terminale d'un périphérique appartenant à un vlan.

Pour attribuer chaque port a un vlan on suit ces étapes :

- Switch(config) # interface fast Ethernet 0/1
 - Switch(config-if) # switchport mode access
 - Switch(config-if) # switchport access vlan 10
 - Switch(config-if) # switchport voice vlan 50
 - Switch(config-if) #Exit
- De la même façon on attribue le port fa0/2 au le vlan 10
- Switch(config) # interface fast Ethernet 0/3
 - Switch(config-if) # switchport mode access
 - Switch(config-if) # switchport access vlan 20
 - Switch(config-if) # switchport voice vlan 50
 - Switch(config-if) #Exit
- De la même façon on attribue le port fa0/4 au le vlan 20

```

Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 50
Switch(config-if)#exit
Switch(config)#interface fa 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fa 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#switchport voice vlan 50
Switch(config-if)#exit
Switch(config)#interface fa 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#

```

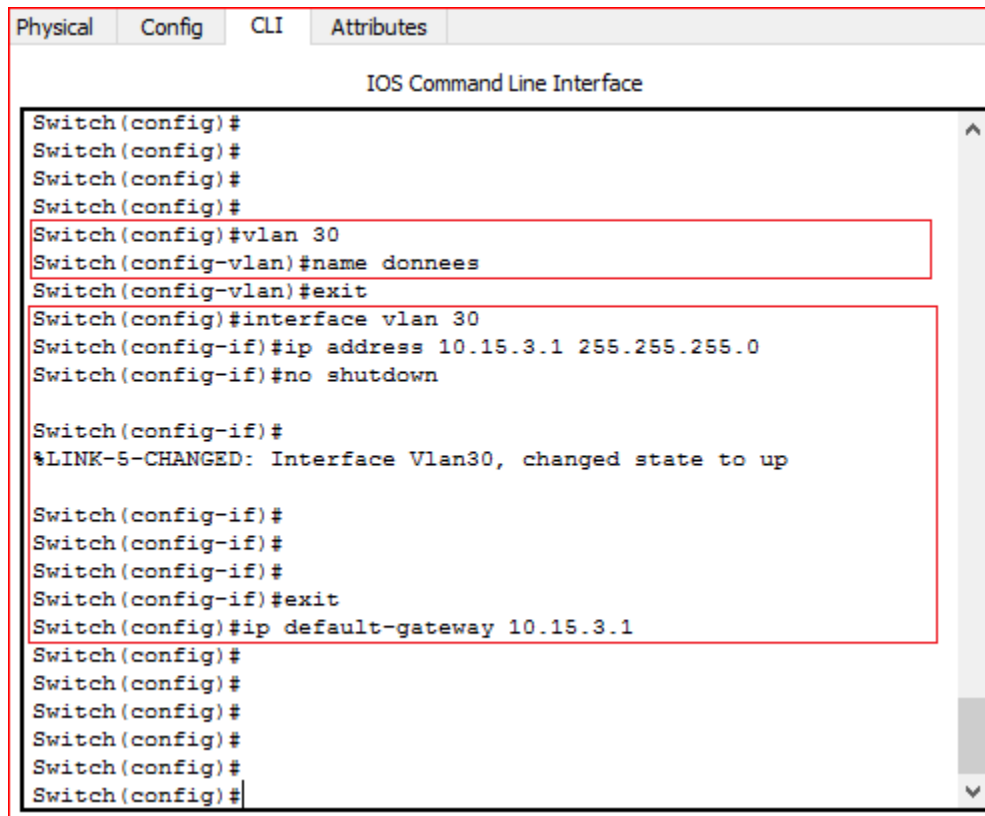
Figure III.5. Configuration des interfaces

c) Donner une passerelle par défaut au Switch : On donne au Switch une passerelle sur laquelle il pourra communiquer avec le routeur et pour réaliser cela on doit créer un nouveau vlan par exemple vlan 30 :

- Switch (config) # vlan 30
- Switch (config-vlan) # name donnees
- Switch (config-vlan) #exit

Et maintenant on attribue à l'interface du vlan 30 une adresse IP et une passerelle par défaut

- Switch(config) # interface vlan 30
- Switch(config-if) # ip address 10.15.3.1 255.255.255.0
- Switch(config-if) #No shutdown
- Switch(config-if) #exit
- Switch(config) #ip default-gateway 10.15.3.1



```
Physical  Config  CLI  Attributes
IOS Command Line Interface
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#vlan 30
Switch(config-vlan)#name donnees
Switch(config-vlan)#exit
Switch(config)#interface vlan 30
Switch(config-if)#ip address 10.15.3.1 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#ip default-gateway 10.15.3.1
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
```

Figure III.6. Accorder une passerelle par défaut au Switch

d) Configurer la liaison entre le Switch et le routeur : Afin de relier le switch et le routeur on utilise le mode trunk au niveau du switch

Le mode trunk [18]: ce mode est utilisé dans le cas où plusieurs vlans doivent transiter sur un même lien.

- Switch (config) #interface fa 0/5
- Switch (config-if) #switchport mode trunk
- Switch (config-if) #switchport trunk allowed vlan 50,20
- Switch (config-if) #exit

A ce niveau là on a permis qu'au vlan 50 et 20 de circuler

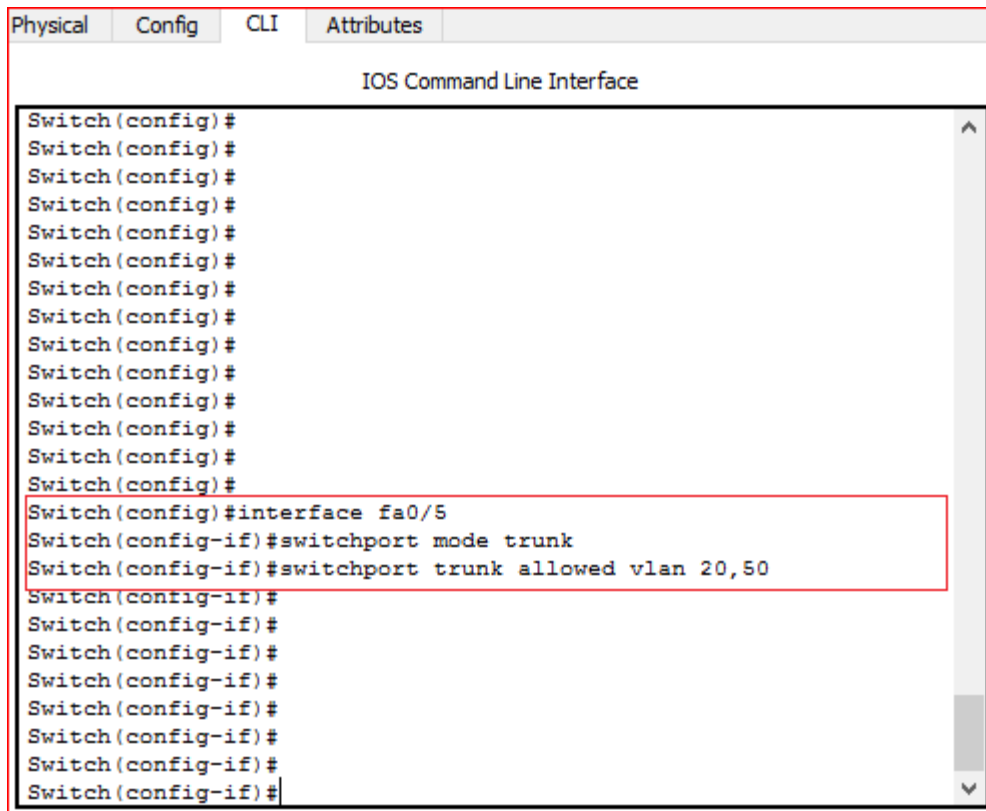
The image shows a screenshot of a Cisco IOS Command Line Interface (CLI) window. The window has four tabs: 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, and the title bar reads 'IOS Command Line Interface'. The terminal output shows a sequence of commands in configuration mode for a switch. The first 13 lines are 'Switch(config)#'. The 14th line is 'Switch(config)#interface fa0/5'. The 15th line is 'Switch(config-if)#switchport mode trunk'. The 16th line is 'Switch(config-if)#switchport trunk allowed vlan 20,50'. The following 7 lines are 'Switch(config-if)#'. The final line is 'Switch(config-if)#'. A red rectangular box highlights the three lines starting with 'Switch(config-if)#interface fa0/5'.

Figure III.7. Configuration de la liaison entre le switch et le routeur en mode trunk

➤ **Switch 2**

a) Création des Vlan : on suivant les étapes précédentes nous allons déclarer le vlan 10 :

- Switch>enable
- Switch # configure terminal
- Switch (config) # vlan 10
- Switch (config-vlan) # name admin
- Switch (config-vlan) #exit

b) Configuration des interfaces: nous allons maintenant attribuer les deux port fa0/1 et fa0/2 au vlan 10 et le port fa0/3 au serveur d'Intranet

- Switch(config) # interface fast Ethernet 0/1
- Switch(config-if) # switchport mode access
- Switch(config-if) # switchport access vlan 10
- Switch(config-if) # switchport voice vlan 50
- Switch(config-if) # switchport voice vlan 50

- Switch(config-if) #Exit

➤ De la même façon on attribue le port fa0/2 au vlan 10

On configure maintenant l'interface du serveur d'une manière à ce que uniquement le vlan 20 qui peut lui accéder.

- Switch(config) # interface fast Ethernet 0/4
- Switch(config-if) # switchport mode access
- Switch(config-if) # switchport access vlan 20

d) Configurer la liaison entre le Switch 1 et le switch 2: Dans ce cas là le switch2 va communiquer avec le router a travers le switch1 on doit donc trunker la liaison entre les deux switches, la configuration de cette liaison ce fait au niveau des deux interfaces fa0/3 et fa0/6 on suivant ces étapes :

Pour le switch 2 :

- Switch (config) #interface fa 0/3
- Switch (config-if) #switchport mode trunk
- Switch(config-if) #Exit

Pour le switch 1:

- Switch (config) #interface fa 0/6
- Switch (config-if) #switchport mode trunk
- Switch(config-if) #Exit

III.4.3. Configuration du Routeur

On peut configurer un router, en utilisant soit le mode console ou le mode administrateur,

Pour passer du mode privilège au mode administrateur il suffit de rentrer l'instruction

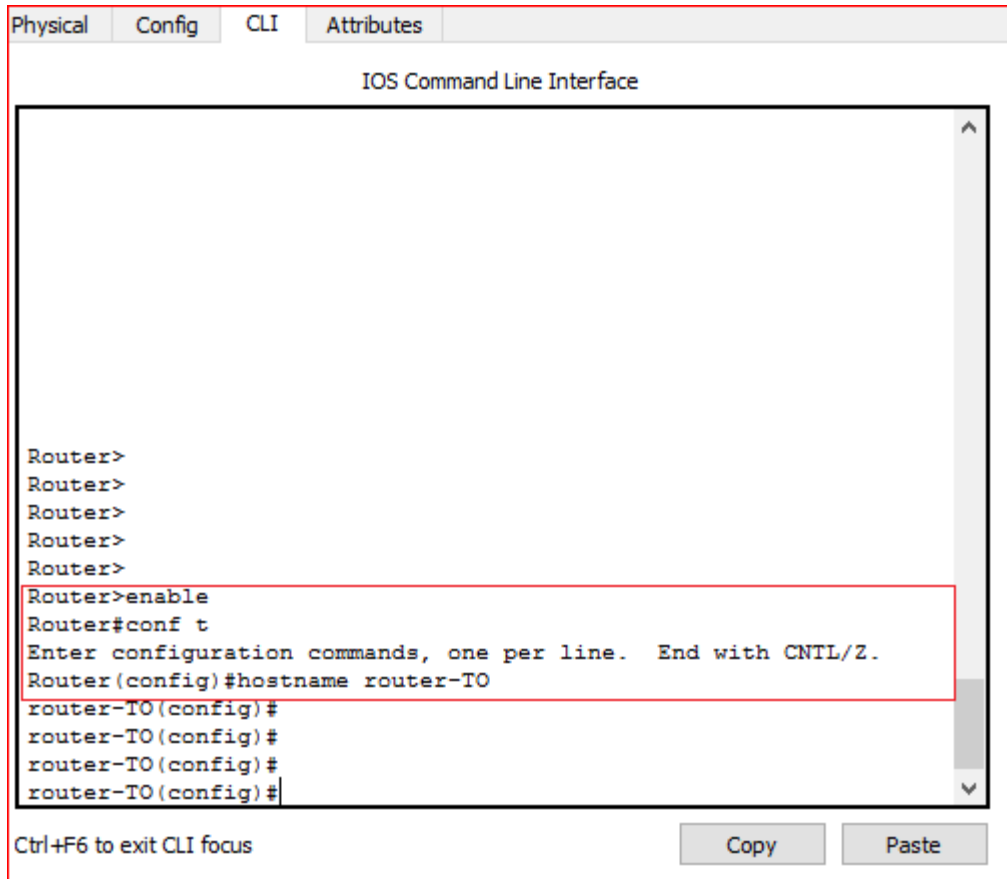
```
enable :
Router>enable
Router #
```

Les deux lignes précédentes nous ont permet de passer en mode administrateur, nous allons maintenant passer en mode con figuration du router :

```
Router # configure terminale
Router (config)#
```

a) Configuration du Nom du Routeur : Pour attribuer un nom au Routeur on utilise la commande suivante:

- Router>enable
- Router #configure terminal
- Router (config)# hostname Router-TO



```
Physical  Config  CLI  Attributes
IOS Command Line Interface

Router>
Router>
Router>
Router>
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname router-TO
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

Figure III.8. Attribution du nom au routeur

Pour interconnecter les deux sites il faut donner une route sur laquelle ils peuvent connecter entre eux et pour réaliser ce la on suit les commandes suivantes :

- Router-TO (config)#interface fa 0/1
- Router-TO (config-if)#ip address 192.168.10.1 255.255.255.0 (l'adresse du LET)
- Router-TO (config-if)#no shutdown
- Router-TO (config-if)#ip route 0.0.0.0 0.0.0.0 192.168.10.2 (l'adresse du site d'Alger)

```

Physical  Config  CLI  Attributes
IOS Command Line Interface
Router>
Router>
Router>
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname router-TO
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#interface fa 0/1
router-TO(config-if)#ip address 192.168.10.1 255.255.255.0
router-TO(config-if)#no shutdown

router-TO(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

router-TO(config-if)#
router-TO(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#

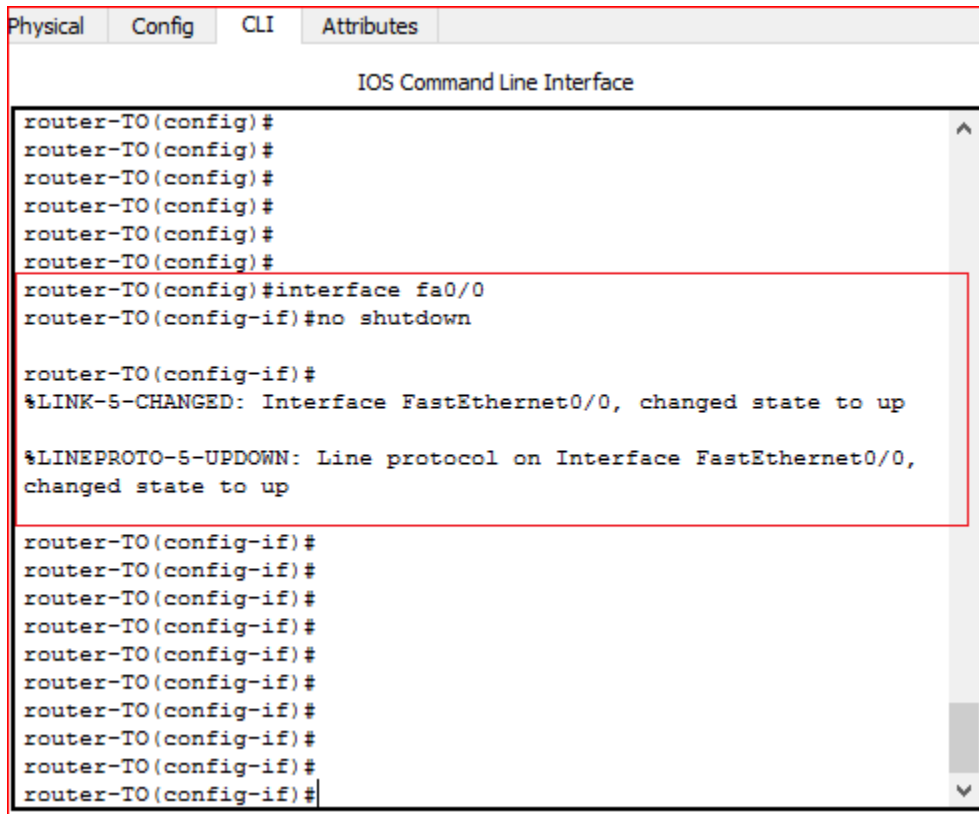
```

Figure III.9.Etablissement de la route entre les deux sites

b) Configurer l'interface 0/0 en créant des sous-interfaces pour chaque vlan:

- Pour le vlan 10
 - Router-TO (config) #interface Fast Ethernet 0/0
 - Router-TO (config-if) # interface Fast Ethernet 0/0.10
 - Router-TO (config-subif) # encapsulation dot1Q 10
 - Router-TO (config-subif) # ip address 10.15.15.1 255.255.255.0
 - Router-TO (config-subif) # exit
- Pour le vlan 20
 - Router-TO (config) #interface Fast Ethernet 0/0
 - Router-TO(config-if) # interface Fast Ethernet 0/0.20
 - Router-TO (config-subif) # encapsulation dot1Q 20
 - Router-TO (config-subif) # ip address 10.15.16.1 255.255.255.0
 - Router-TO (config-subif) # exit

- Pour le vlan 50
 - Router-TO (config) #interface Fast Ethernet 0/0
 - Router-TO (config-if) # interface Fast Ethernet 0/0.50
 - Router-TO (config-subif) # encapsulation dot1Q 50
 - Router-TO (config-subif) # ip address 10.15.5.1 255.255.255.0
 - Router-TO (config-subif) # exit



```
Physical  Config  CLI  Attributes
IOS Command Line Interface
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#interface fa0/0
router-TO(config-if)#no shutdown

router-TO(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

router-TO(config-if)#
router-TO(config-if)#
router-TO(config-if)#
router-TO(config-if)#
router-TO(config-if)#
router-TO(config-if)#
router-TO(config-if)#
router-TO(config-if)#
router-TO(config-if)#
router-TO(config-if)#
```

Figure III.10.Activation de l'interface 0/0


```

Physical  Config  CLI  Attributes
IOS Command Line Interface
router-TO(config)#
router-TO(config)#
router-TO(config)#interface fa0/0
router-TO(config-if)#interface fa0/0.10
router-TO(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.10, changed state to up

router-TO(config-subif)#encapsulation dot1Q 10
router-TO(config-subif)#ip address 10.15.15.1 255.255.255.0
router-TO(config-subif)#exit
router-TO(config)#interface fa0/0.20
router-TO(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.20, changed state to up

router-TO(config-subif)#encapsulation dot1Q 20
router-TO(config-subif)#ip address 10.15.16.1 255.255.255.0
router-TO(config-subif)#
    
```

Figure III.11.Création des sous-interfaces pour les vlan 10 et 20

```

Physical  Config  CLI  Attributes
IOS Command Line Interface
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#interface fa0/0
router-TO(config-if)#interface fa0/0.50
router-TO(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.50, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.50, changed state to up

router-TO(config-subif)#encapsulation dot1Q 50
router-TO(config-subif)#ip address 10.15.5.1 255.255.255.0
router-TO(config-subif)#
router-TO(config-subif)#
router-TO(config-subif)#
router-TO(config-subif)#
router-TO(config-subif)#
router-TO(config-subif)#
router-TO(config-subif)#
    
```

Figure III.12.Création de la sous-interface pour le vlan 50

c) **Vérification des sous-interfaces crée:** Pour vérifier la création des sous-interfaces on utilise la commande suivante:

- Router-TO# Show ip interface brief

```

IOS Command Line Interface

router-TO(config)#
router-TO(config)#
router-TO(config)#exit
router-TO#
%SYS-5-CONFIG_I: Configured from console by console

router-TO#
router-TO#
router-TO#
router-TO#show ip interface brief
Interface                IP-Address      OK? Method Status
Protocol
FastEthernet0/0          unassigned      YES unset  up
up
FastEthernet0/0.10       10.15.15.1      YES manual  up
up
FastEthernet0/0.20       10.15.16.1      YES manual  up
up
FastEthernet0/0.50       10.15.5.1       YES manual  up
up
FastEthernet0/1          192.168.10.1    YES manual  up
down
Vlan1                    unassigned      YES unset
administratively down
router-TO#

```

Figure III.13.Vérification de la création des sous-interfaces

III.4.4. Définir le Routeur comme DHCP serveur

Dans cette étape nous allons donner au routeur le rôle d'un serveur DHCP où ce dernier permet d'attribuer dynamiquement une adresse IP aux postes connectés au réseau.

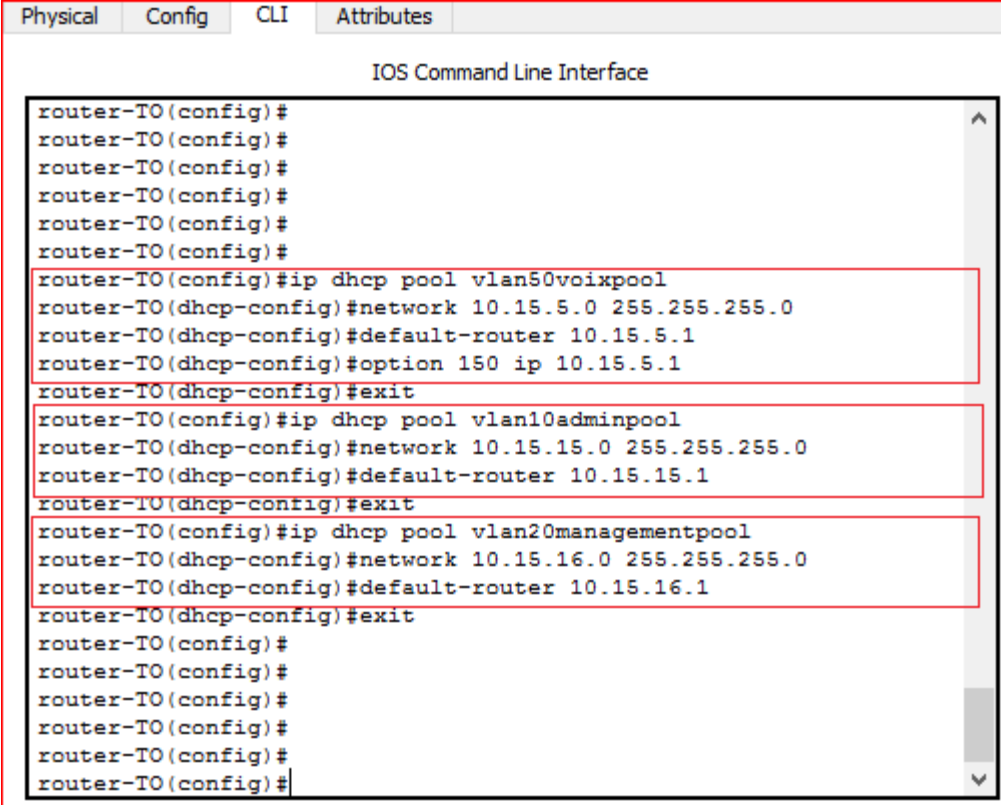
Le serveur DHCP fournit également d'autres informations, comme la passerelle par défaut et le DNS.

- Pour le vlan 50
 - Router-TO (config) # ip DHCP pool vlan10voixpool
 - Router-TO (dhcp-config) #network 10.15.5.0 255.255.255.0
 - Router-TO (dhcp-config) #default-router 10.15.5.1
 - Router-TO (dhcp-config) #option150 ip 10.15.5.1
 - Router-TO (dhcp-config) #exit

Option 150 [19] : Cette option est utilisé uniquement par les téléphones IP pour obtenir les informations fournit par le DHCP d'où ils peuvent télécharger les configurations requises.

- Pour le vlan 10
 - Routeur-VOIX (config) # ip DHCP pool vlan10voixpool
 - Routeur-VOIX (dhcp-config) #network 10.15.15.0 255.255.255.0
 - Routeur-VOIX (dhcp-config) #default-router 10.15.15.1
 - Routeur-VOIX (dhcp-config) #exit

- Pour le vlan 20
 - Routeur-VOIX (config) # ip DHCP pool vlan10voixpool
 - Routeur-VOIX (dhcp-config) #network 10.15.16.0 255.255.255.0
 - Routeur-VOIX (dhcp-config) #default-router 10.15.16.1
 - Routeur-VOIX (dhcp-config) #exit



```
Physical Config CLI Attributes
IOS Command Line Interface
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#ip dhcp pool vlan50voixpool
router-T0(dhcp-config)#network 10.15.5.0 255.255.255.0
router-T0(dhcp-config)#default-router 10.15.5.1
router-T0(dhcp-config)#option 150 ip 10.15.5.1
router-T0(dhcp-config)#exit
router-T0(config)#ip dhcp pool vlan10adminpool
router-T0(dhcp-config)#network 10.15.15.0 255.255.255.0
router-T0(dhcp-config)#default-router 10.15.15.1
router-T0(dhcp-config)#exit
router-T0(config)#ip dhcp pool vlan20managementpool
router-T0(dhcp-config)#network 10.15.16.0 255.255.255.0
router-T0(dhcp-config)#default-router 10.15.16.1
router-T0(dhcp-config)#exit
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
```

Figure.III.14.Configuration du DHCP serveur

III.4.5. Configuration des paramètres Call Manager Express :**a) Création de l'interface loopback [20]:**

IL s'agit d'une interface virtuelle, créée par configuration et qui a la particularité de toujours être up/up. D'un point de vue fonctionnement du routeur, cette interface est perçue comme une interface physique.

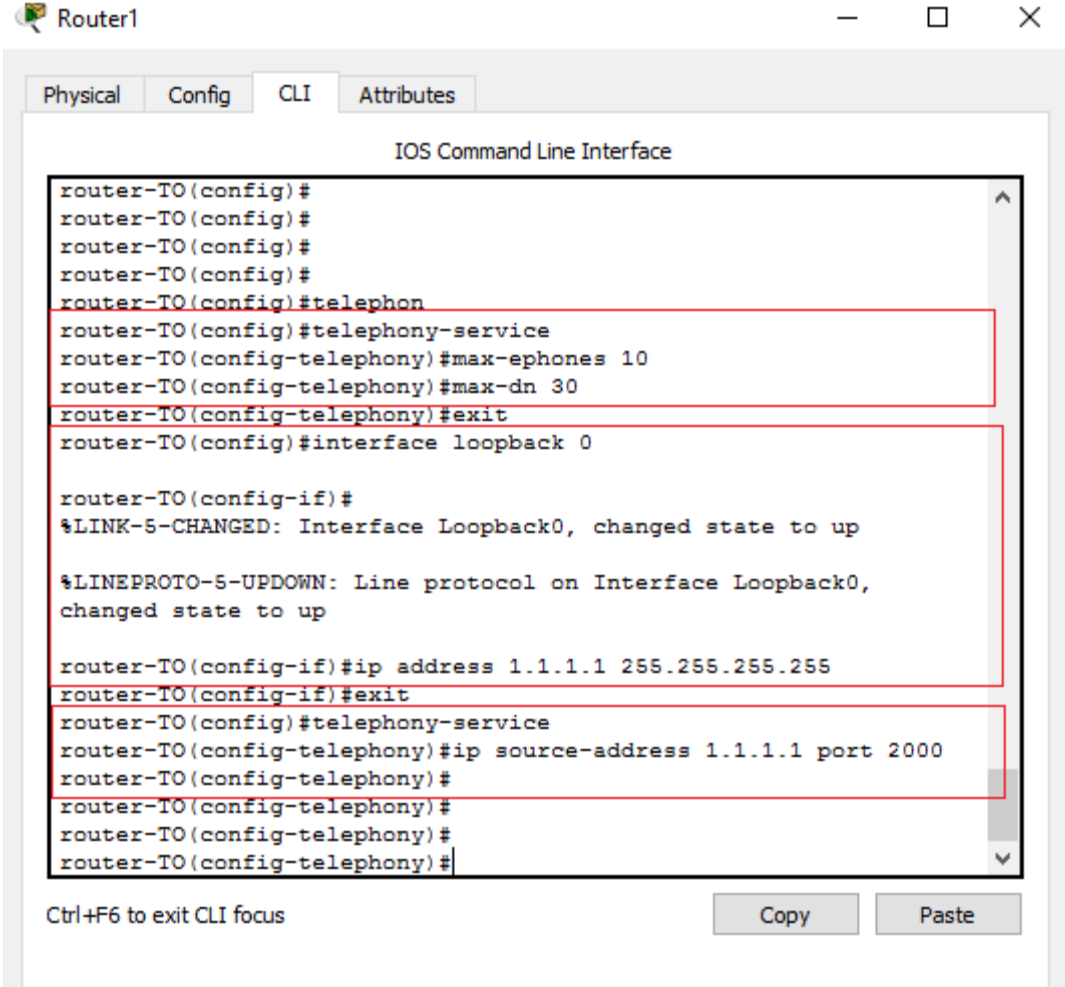
b) Configuration des paramètres du Call Manager Express [21]:

Ces configurations nous permet de limité le nombre de téléphone IP qui va être utilisé.

- Router-TO (config) # telephony-service
- Router-TO (config-telephony) # max-ephones 10
- Router-TO (config-telephony) # max-dn 30

c) Configurer l'interface loopback 0 : Dans cette étape on attribue une adresse IP de à l'interface loopback 0

- Router-TO (config) #interface loopback 0
- Router-TO (config-if) #ip address 1.1.1.1 255.255.255.255
- Router-TO (config-if) #exit
- Router-TO (config) #telephony-service
- Router-TO (config-telephony) #ip source-address 1.1.1.1 port 2000
- Router-TO (config-telephony) #exit



The screenshot shows a Cisco Router CLI window titled "Router1" with tabs for Physical, Config, CLI, and Attributes. The CLI window displays the following commands and their outputs:

```

router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#telephon
router-T0(config)#telephony-service
router-T0(config-telephony)#max-ephones 10
router-T0(config-telephony)#max-dn 30
router-T0(config-telephony)#exit
router-T0(config)#interface loopback 0

router-T0(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up

router-T0(config-if)#ip address 1.1.1.1 255.255.255.255
router-T0(config-if)#exit
router-T0(config)#telephony-service
router-T0(config-telephony)#ip source-address 1.1.1.1 port 2000
router-T0(config-telephony)#
router-T0(config-telephony)#
router-T0(config-telephony)#
router-T0(config-telephony)#

```

At the bottom of the CLI window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

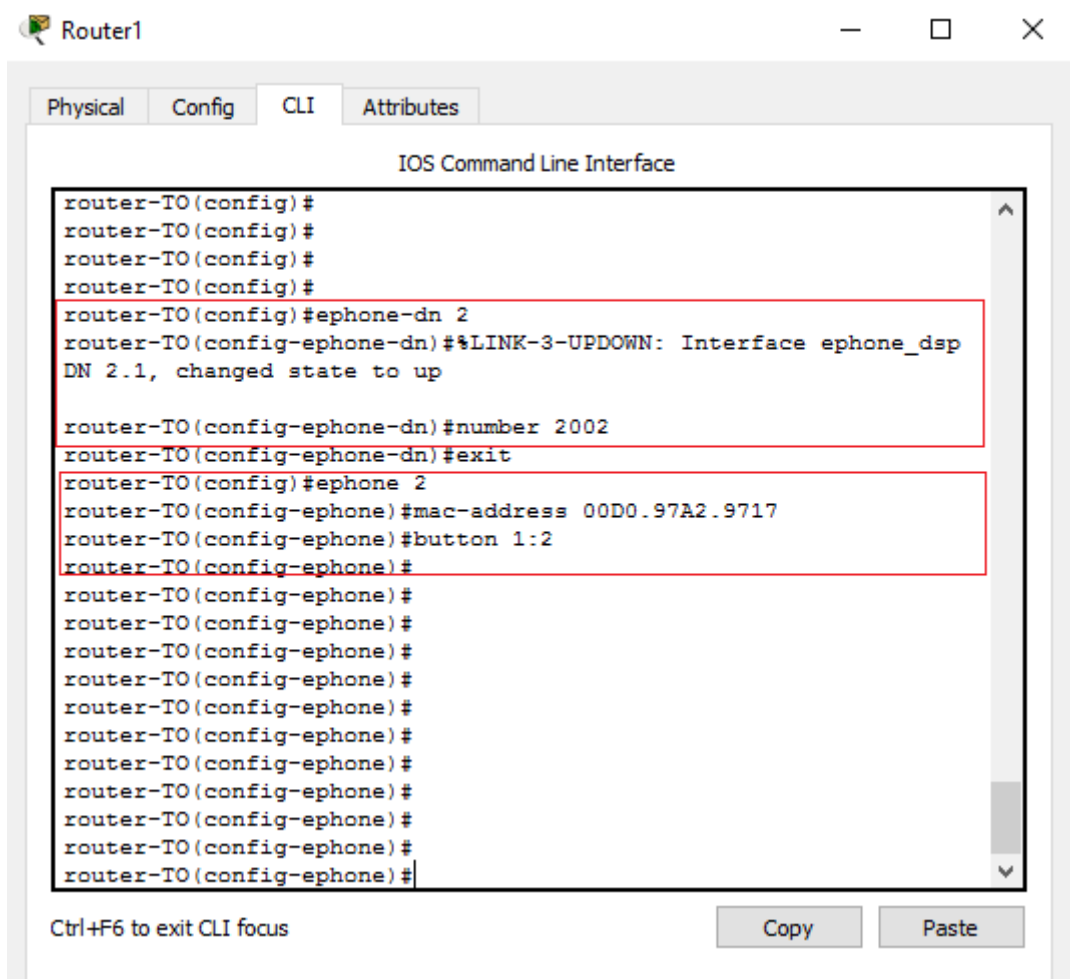
Figure III.15. Configuration des paramètres Call Manager Express et l'activation de l'interface loopback 0

III.4.6. Configuration des services téléphoniques

Dans cette étape on va configurer les différents paramètres de chaque téléphone dont on va introduire le numéro et l'adresse MAC qui identifie chaque téléphone :

- Router-T0 (config) #ephone-dn 1
- Router-T0 (config-ephone-dn)# number 2001
- Router-T0 (config-ephone-dn)#exit
- Router-T0 (config)# ephone 1
- Router-T0 (config-ephone)#introduire l'adresse MAC du téléphone
- Router-T0 (config-ephone)#button 1:1

Et de la même manière on introduit le numéro et l'adresse MAC pour les autres téléphones.



```
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#
router-TO(config)#ephone-dn 2
router-TO(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp
DN 2.1, changed state to up
router-TO(config-ephone-dn)#number 2002
router-TO(config-ephone-dn)#exit
router-TO(config)#ephone 2
router-TO(config-ephone)#mac-address 00D0.97A2.9717
router-TO(config-ephone)#button 1:2
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
router-TO(config-ephone)#
```

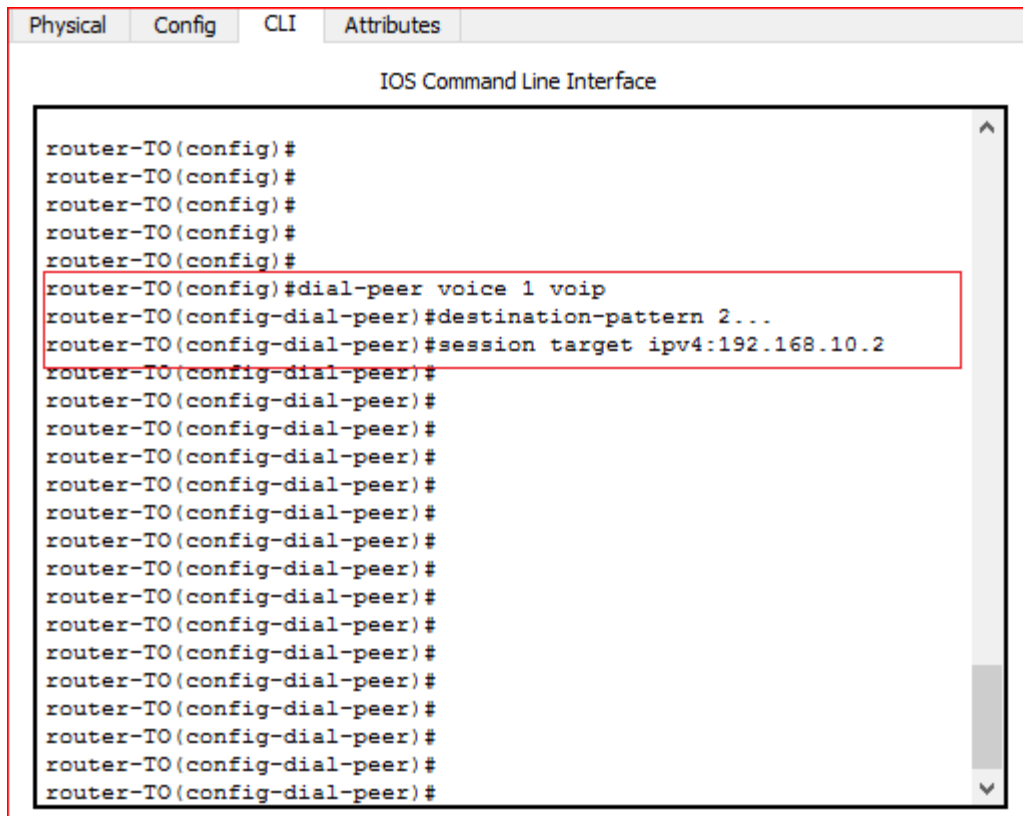
Ctrl+F6 to exit CLI focus

Copy Paste

Figure III.16. Configuration des services téléphoniques

III.4.7. Interconnexion des deux sites (LET et Centrale d'Alger)

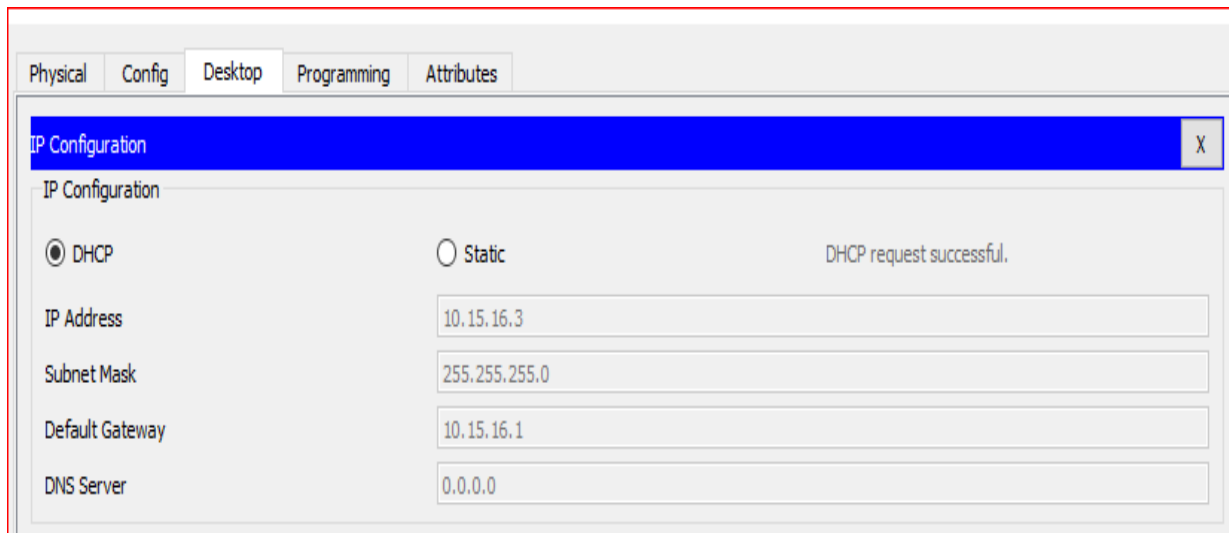
Afin d'interconnecter les deux sites il faut introduire cette commande au niveau des deux routeurs :



```
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#
router-T0(config)#dial-peer voice 1 voip
router-T0(config-dial-peer)#destination-pattern 2...
router-T0(config-dial-peer)#session target ipv4:192.168.10.2
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
router-T0(config-dial-peer)#
```

Figure III.17.L’interconnexion des deux appareils IPBX sur deux sites différents

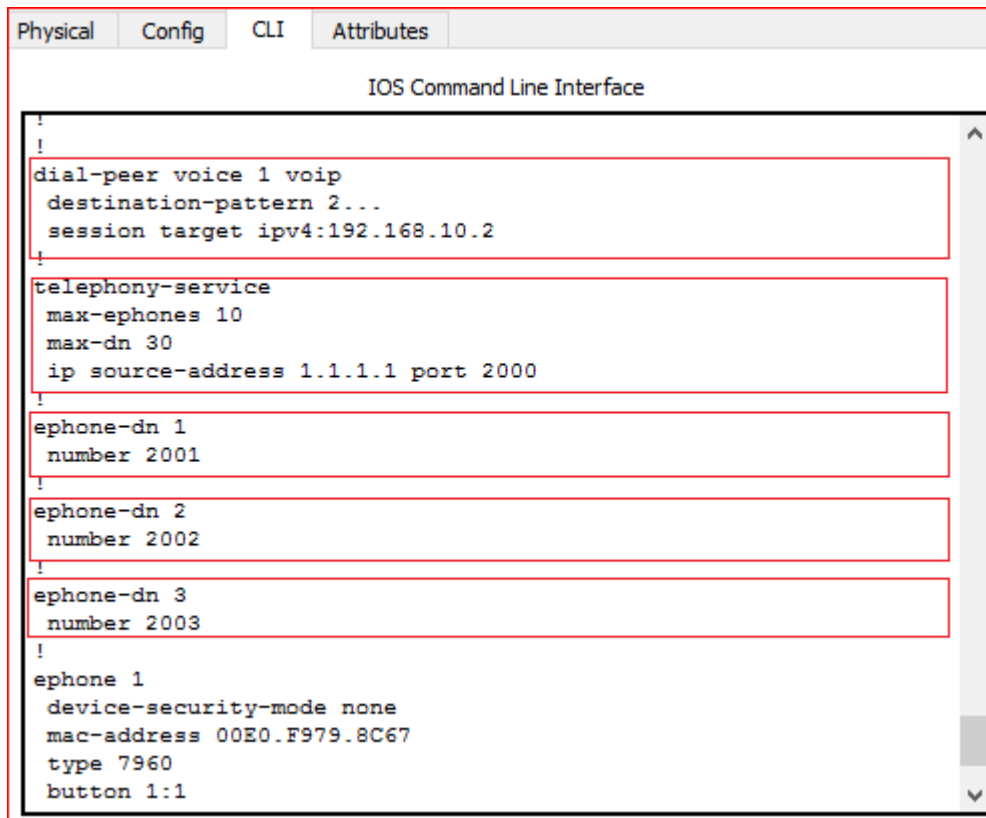
Dans ce cas chaque téléphone et chaque position se dispose d’un numéro et d’une adresse IP et d’une passerelle attribué par le DHCP comme nous montre la figure suivante :



IP Configuration

<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	DHCP request successful.
IP Address	10.15.16.3	
Subnet Mask	255.255.255.0	
Default Gateway	10.15.16.1	
DNS Server	0.0.0.0	

Figure III.18.Visualisation de l’adresse IP attribué au PC par le DHCP

The image shows a screenshot of the Cisco IOS Command Line Interface (CLI) configuration for telephony services. The interface has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The configuration is displayed in a text area with a scroll bar on the right. The configuration includes a dial-peer, telephony-service settings, three ephone-dn entries, and an ephone entry. Each configuration block is highlighted with a red rectangular box.

```
Physical Config CLI Attributes
IOS Command Line Interface
!
!
dial-peer voice 1 voip
 destination-pattern 2...
 session target ipv4:192.168.10.2
!
telephony-service
 max-ephones 10
 max-dn 30
 ip source-address 1.1.1.1 port 2000
!
ephone-dn 1
 number 2001
!
ephone-dn 2
 number 2002
!
ephone-dn 3
 number 2003
!
ephone 1
 device-security-mode none
 mac-address 00E0.F979.8C67
 type 7960
 button 1:1
```

Figure III.19. Visualisation des services téléphoniques

III.4.8. Architecture du réseau du site d'Alger

Au niveau de ce réseau nous disposons d'un routeur, un switch, des appareils téléphoniques et des positions de travail.

Nous avons presque apportés les mêmes configurations aux différents éléments du réseau d'où nous avons créé trois vlan 50 pour la voix, 20 pour l'administration et 70 pour la comptabilité on suivants les mêmes étapes cités avant.

Comme nous avons créé les sous-interfaces au niveau du router et nous avons déclaré le DHCP pool et nous avons configuré les interfaces loopback.

PARTIE 2

La configuration physique de la ToIP

III.5. La Configuration physique du Téléphone IP

Une fois la configuration du routeur et du Switch a été faite avec la méthode citée en dessous, On passe à la configuration physique du poste IP en suivant ces différents étapes :

Étape 1: L'appareil IP va se redémarrer et le DHCP va lui attribuer une adresse comme on peut le voir dans la figure suivante :

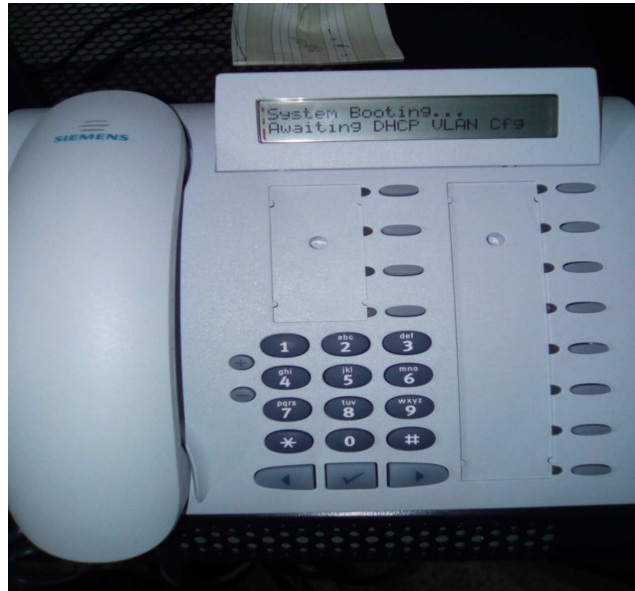


Figure III.20.Redémarrage du poste IP

Étape 2: Attribution de l'adresse 10.15.49.13 par le DHCP au poste IP Comme le montre la figure suivante :



Figure III.21.Attribution d'une adresse au poste IP par le DHCP

Etape 3: Saisir https://10.15.49.13 dans l'onglet de recherche comme le montre la figure suivante:

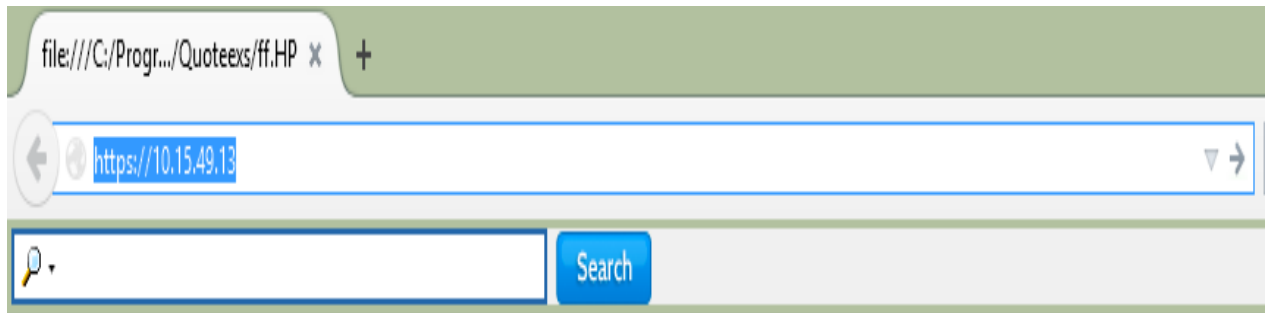


Figure III.22.Saisir l'adresse sous forme HTTPS

Etape 4: On accède directement à l'interface du poste IP puis on clique sur administrator.

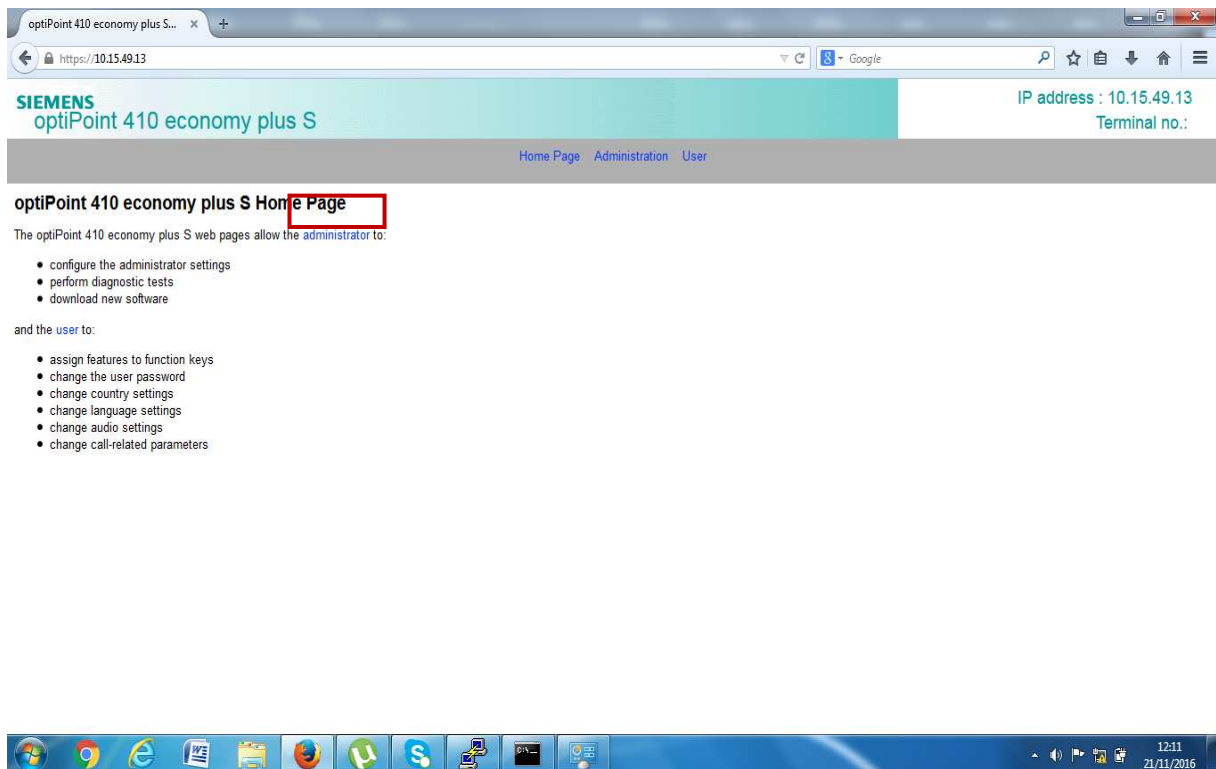


Figure III.23.Accéder à l'interface du poste IP

Etape 5: Une fenêtre de sécurité s'affiche. On saisi alors le mot de passe (123456) afin de pouvoir configurer le poste.

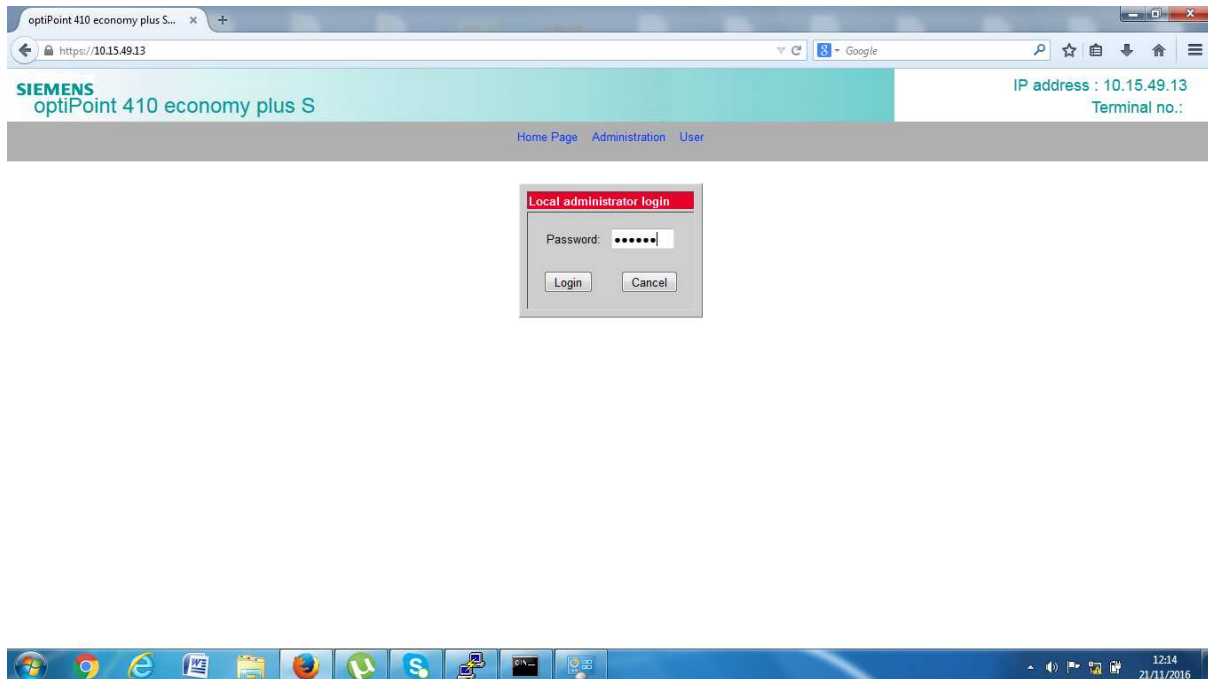


Figure III.24.Saisiedu mot de passe

Etape 6: Juste après la saisie du mot de passe la fenêtre menu d'administration s'affiche, On choisi alors SIP Environment.

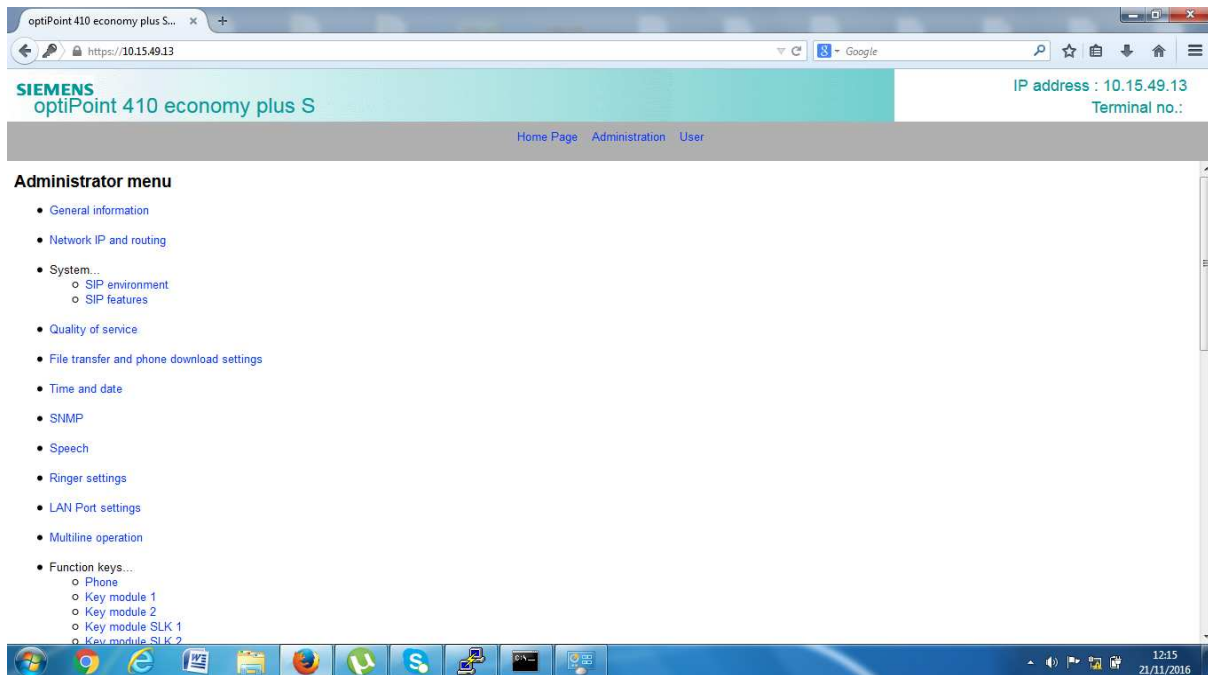


Figure III.25.Menu administration

Etape 7: On remplit les champs:

- phone number: 2050.
- register IP address or DNS name 10.100.33.5
- Server IP address or DNS name 10.100.33.5

L'adresse 10.100.33.5 est celle d'une carte aux niveaux du serveur sur Alger.

SIP Environment

WARNING
If you make changes to the fields marked with an asterisk (*) you will have to restart the terminal manually before they take effect.

Terminal details:

Phone number: 2050 *
Phone name: 2050 *
Register by name: *

SIP details:

SIP routing: Server *
Registrar IP address or DNS name: 10.100.33.5 * Port: 0 *
Server IP address or DNS name: 10.100.33.5 * Port: 0 *
Gateway IP address or DNS name: 0.0.0.0 * Port: 5060 *
SIP port: 5060 *
RTP Base port: 5004 *
Outbound proxy: *
Default OBP domain name: *
SIP transport: UDP *
SIP server type: Other *
SIP session timer enabled: *
SIP session timer value: 3600 seconds *
Registration timer value: 3600 seconds *
SIP realm: 10.100.33.5 *
SIP user ID: 2050 *
New SIP password: *
Confirm SIP password: *
Beep on SIP server error:

Miscellaneous:

Figure III.26.SIP Environnement

Etape 8: On clique sur Submit afin de sauvegarder les informations entrés et de passer à une nouvelle fenêtre. Comme le montre la figure suivante:

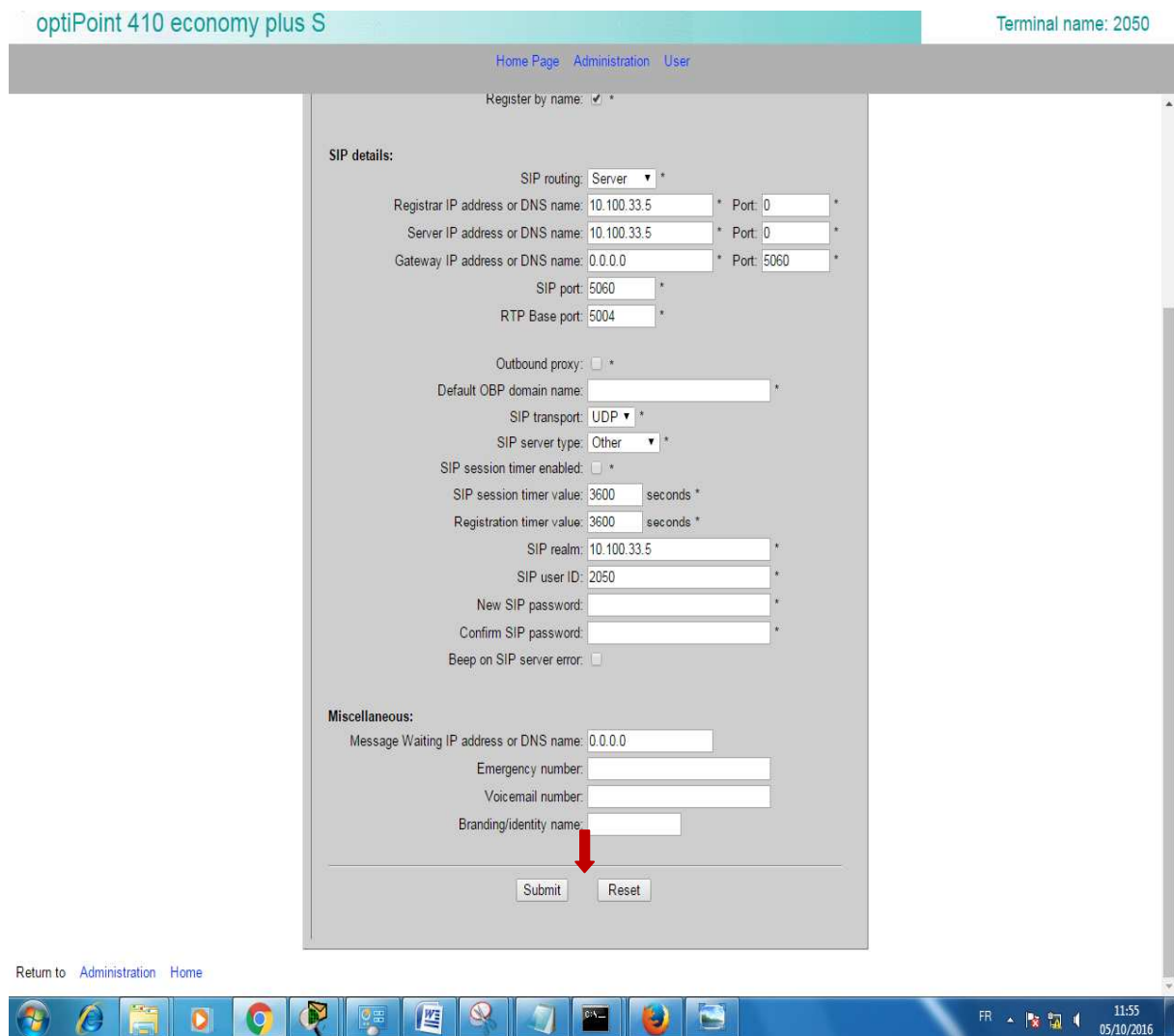


Figure III.27.SIP Environnement (Sauvegarde des informations)

Étape 9: Après avoir cliqué sur Submit en retourne à la fenêtre principale administrator menu, On choisi cette fois ci quality of service. C'est dans cette fenêtre qu'on à pu faire la description du VLAN 34, On change le champ VLAN discovery duDHCP ou manuel.

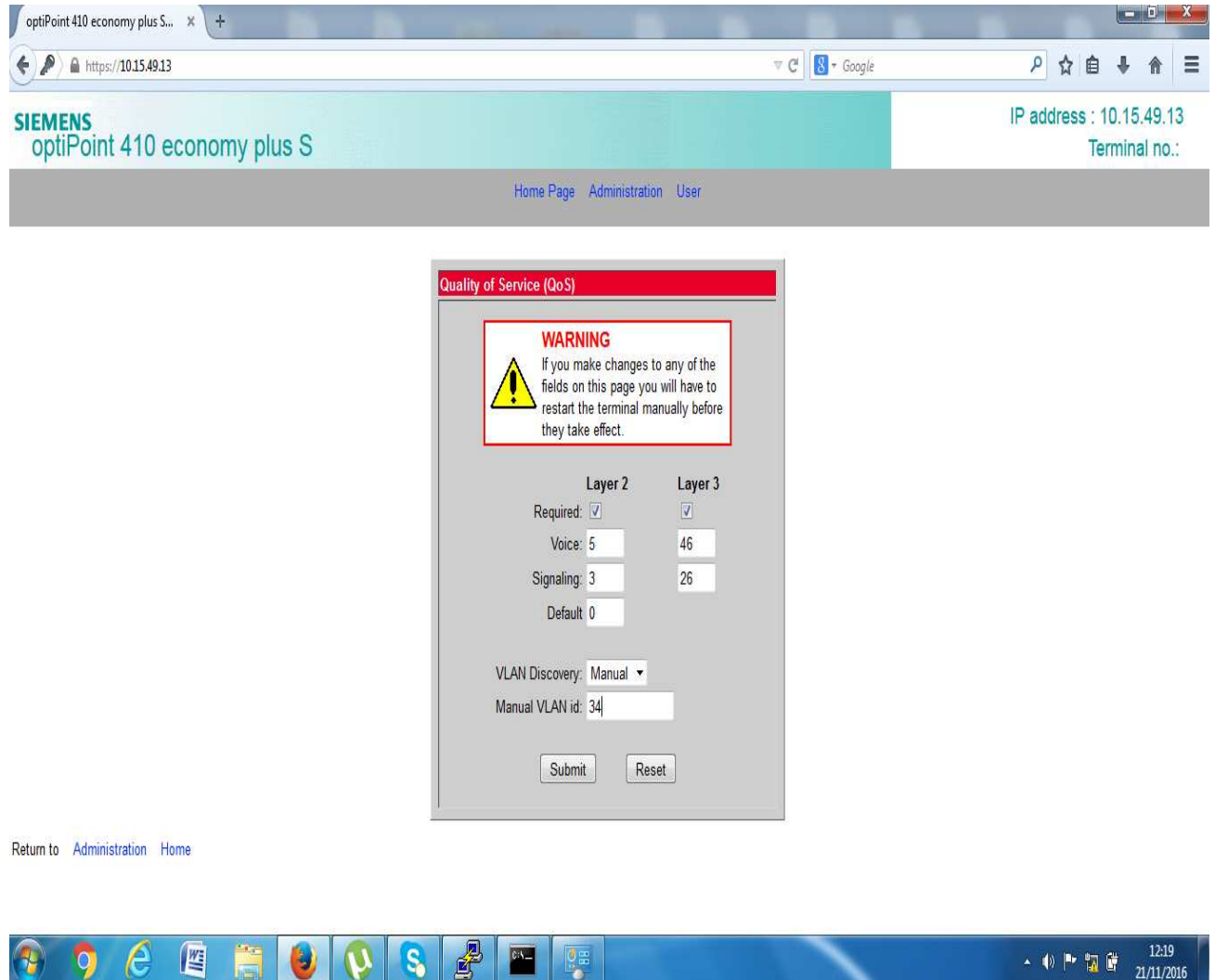


Figure III.28. Qualité de service

Etape 10: Après avoir cliqué sur Submitem retourne à l'interface principale et cette fois on choisi LAN port settings.

Dans cette fenêtre on choisi la vitesse maximum et on clique sur Submit pour finir.

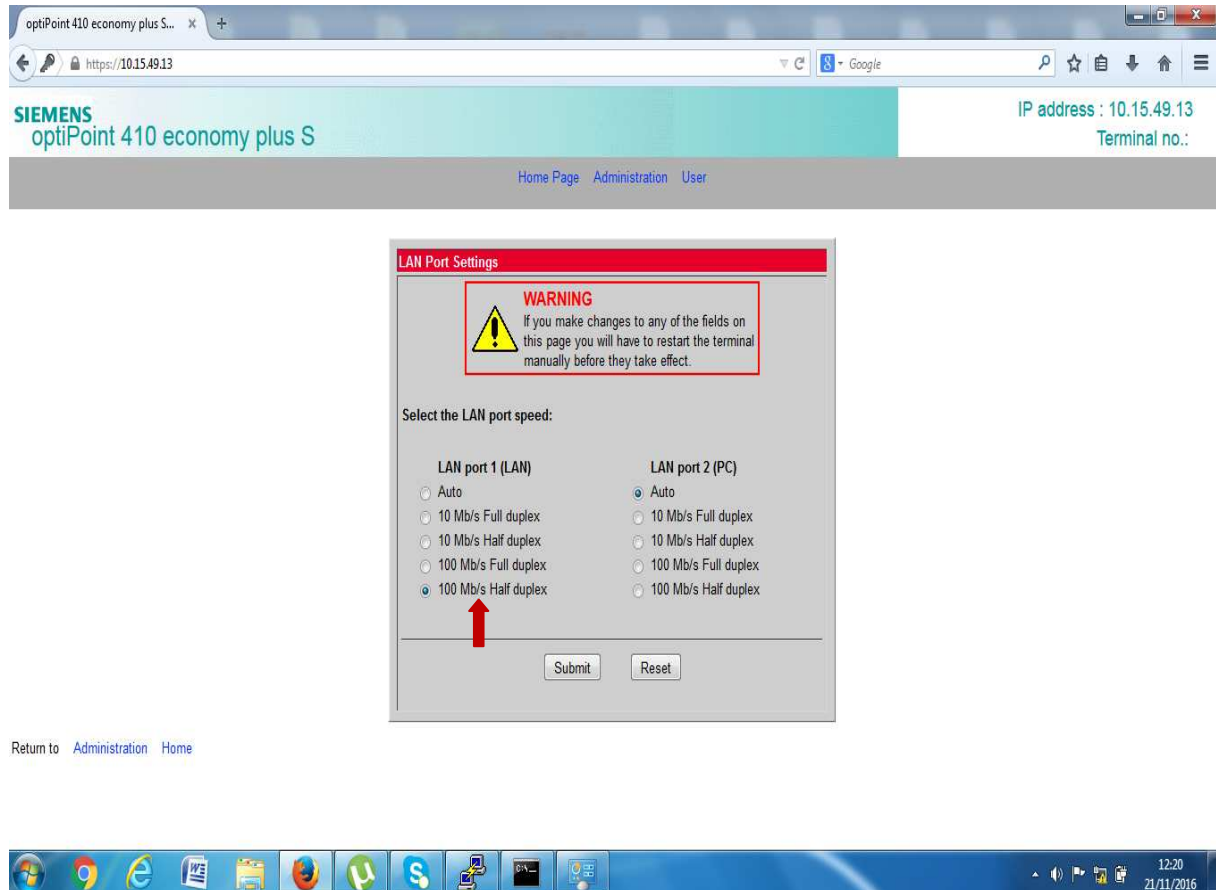


Figure III.29.LAN Port Settings

Etape 11: Une fois toute l'information est entrée, le poste IPBX va redémarrer automatiquement et affiche le numéro qu'on à entré en dessous. Comme le montre la figure suivante:



Figure III.30. Affichage du numéro sur le poste IP

III.6. Fonctionnalités de la téléphonie IP

La téléphonie IP possède plusieurs fonctionnalités tels que :

- Ecran alphanumérique de deux lignes.
- Affichage de l'heure et de la date.
- Equipement mains-libres (sauf sur Optipoint 410/420 Economy/Economy plus) et haut-parleur.
- Répétition de la numérotation et enregistrement des 20 derniers numéros.
- Numérotation sans décrocher.
- Textes de menus en différentes langues.
- 12 touches de fonction programmables sur deux niveaux.
- 3 touches de dialogue pour la commande du menu.

- Programmation sur les touches de numérotation de numéros de destination définis.
- Affichage du numéro ou du nom de l'appelant.
- Transfert, va-et-vient, mise en garde d'une communication.
- Protection par mot de passe des réglages utilisateur.
- Volume et mélodie de sonnerie variables.

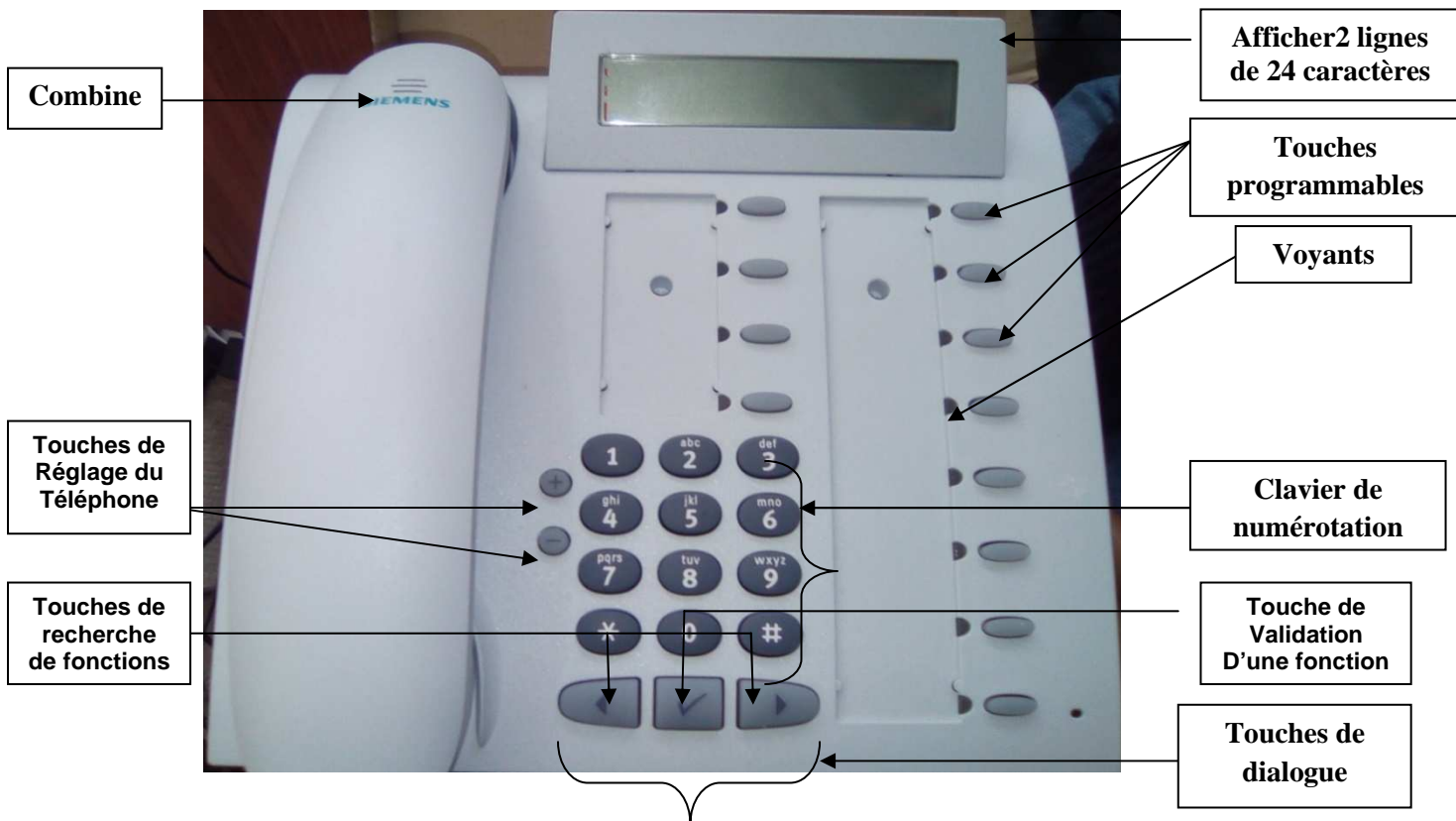


Figure III.31. Composant principaux d'un téléphone IP

➤ **Touches de fonctions programmables:**

Les touches de fonction sont pourvues d'une diode électroluminescente. Le téléphone IP est équipé de 12 touches de fonction sont toutes programmables au niveau de la centrale sur deux niveaux (les touches Annuler et Niveau doivent être conservés). Cinq de ces touches ont déjà une fonction par défaut sur le premier niveau.

Touche De Fonction	Fonction
1	Mettre en marche/Couper le haut-parleur du téléphone
2	Recomposer un des 20 derniers numéros composés.
3	Afficher les 20 derniers appels manqués en offrant des fonctions de sélection, modification et répétition de la numérotation.
11	Annuler la commande actuelle
12	Passer au deuxième niveau de touches

Tableau III.1 Fonctions des touches programmées

➤ **Transfert des appels vers un autre poste :**

En cours de la communication on peut visualiser sur l'afficheur l'information DOUBLE APPEL? Comme on peut chercher cette option dans le menu tournant à l'aide des touches ◀ ou ▶ et on peut valider ce choix par la touche √ le correspondant est mis alors en garde.

- **Interception d'appel:** Permet d'intercepter et de récupérer un appel sonnant sur le poste d'un collègue absent.
- **Liste des appelants :** Cette fonction permet de renseigner l'utilisateur des appels non décrochés reçus sur son poste. Garde l'historique des 10 derniers appels. Afin de voir cette liste on suit ces étapes :
 - On clique sur la touche de fonction et on peut voir le numéro affiché accompagné du nombre d'appelles.
 - On peut soit rappeler le numéro, ou bien passer un autre appel sur la liste à l'aide des touches de dialogue.
 - Pour sortir de la liste des appels on clique sur la dernière touche des pavés des touches programmables.



Figure III.32. Accès à la liste des appels

- **Affichage du nom :** Lorsqu'un collègue nous appelle, Il est identifié par l'IPBX et son nom s'affiche sur notre téléphone.



Figure III.33. Affichage du nom de l'appelant

- **Double appel:** En cours de la communication, On peut appeler un autre abonné pour faire un double appel tandis que notre communication avec le premier interlocuteur est en garde. Pour réaliser cela on clique sur Double Appel/Transfert et on sélectionne le deuxième abonné. La communication passe alors à l'état En garde.

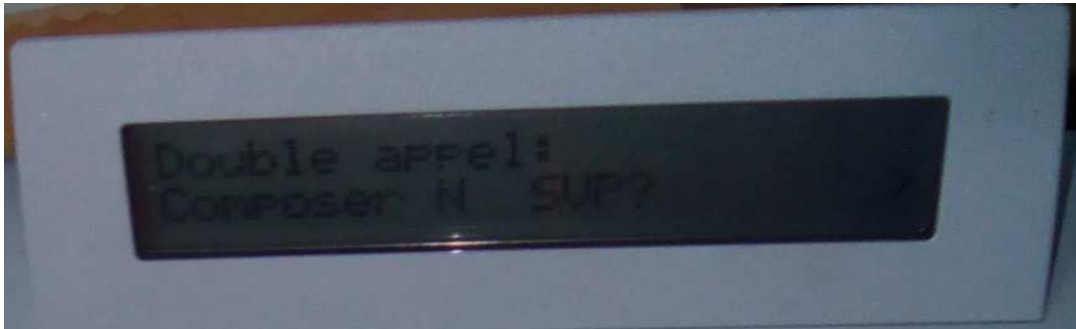


Figure III.34.Composer Un Double Appel

- **Alterner entre deux communications:** A l'ordre de mettre une communication en attente, tandis que nous parlons avec un deuxième interlocuteur. On peut nous adresser alternativement à l'un et l'autre des correspondants.

On navigue alors dans le menu à l'aide des touches jusqu'à l'apparition de l'indication sur l'afficheur : Va et vient ? Comme le montre la figure suivante:



Figure III.35.Alterner entre deux communications

- **Passer en conférence:** Il est possible d'établir une conférence avec 8 personnes. Pour réaliser la conférence on suit ces étapes :
 - Appeler le premier correspondant.
 - Sélectionner a l'aide des touches ◀ ou ▶ jusqu'à l'apparition de l'indication sur l'afficheur : activer conférence ?
 - Appuyer sur la touche √. Pour confirmer.
 - On appel le second correspondant (on informe de l'existence de la conférence.)
 - Indication sur l'afficheur : conférence ?
 - Appuyer Sur La Touche √. Pour Confirmer.

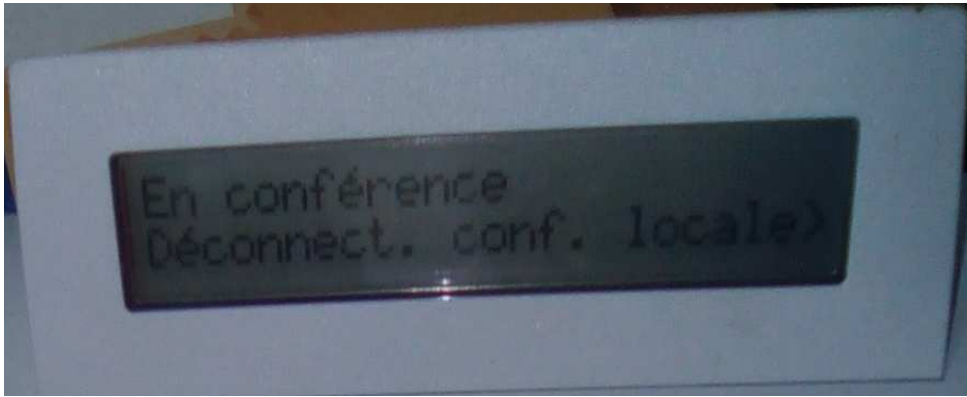


Figure III.36. Conférence établie

III.7. Discussions

Ce dernier chapitre et de loin le plus dense, Ceci est due au fait qu'il a été question du cœur du travail qui nous a été confié. Il traite l'implémentation de la solution IP et surtout de sa mise en place par la configuration d'un routeur, d'un Switch et des postes IP.

CONCLUSION

Ce mémoire s'inscrit dans le cadre d'un projet de fin d'étude. Il aboutie a l'implémentation d'une solution ToIP sous le réseau Intranet d'Algérie Télécom.

La ToIP présente de nombreux avantages mais elle doit néanmoins relever de nombreux défis et pallier certaines difficultés techniques notamment la qualité de service.

Malgré quelques inconvénients la ToIP reste une bonne solution en matière d'intégration, fiabilité, d'évolutivité et de coût et elle permet aussi une grande mobilité en la combinant avec d'autres technologies comme Wireless, Wifi, Bluetooth. Nous ne pouvons que réjouir de vivre l'essor de ses différentes technologies.

Nous pouvons donc vraisemblablement penser que bientôt nos téléphones seront tous IP et que le protocole IP deviendra un jour un standard unique permettant l'interopérabilité des réseaux mondialisés. C'est pourquoi l'intégration de la voix sur IP n'est qu'une étape vers Everything over IP (EoIP).

Ce projet à été une expérience fructueuse qui nous a permis de mieux s'approcher du milieu professionnel. Ça nous a permit de savoir comment gérer et optimiser le temps dans le but d'en profiter au maximum.

Bibliographie

Bibliographie

- [1] : <https://www.futura-sciences.com/tech/definitions/tech-routage-1305>
- [2] : <https://www.ibm.com/knowledgecenter/fr/routage%20scope=SSEQTP>
- [3] : <https://www.it-connect.fr/routage-statique-et-routage-dynamique-routage-systeme-autome>
- [4] : http://www.nicolasjean.com/pdf/essai_routage.pdf
- [5] : ouvrage Cisco protocoles, concept de routage et sécurité, Vacamps Andrés, 2011
- [6] : <http://www.lig-membres.imag.fr/sicard/crRES/Cours%2010%20vlan.pdf>
- [7] : <https://standardtelephoniques.expertmarket.fr/systeme-telephonique-IPBX>
- [8] : www.expert-telephonie-entreprise.fr/definition-toip-telephonie-ip.php
- [9] : Thèse : Optimisation de la téléphonie par la VoIP – Mr : Cavour Assong – Ecole nationale supérieure des postes et télécommunications -Yaoundé -2010
- [10] : https://www.forumaterna.org/files/livresblancs/Introduction_telephonieIP.pdf
- [11] : <http://www.info-entre-pros.com/telephonie-ip-entreprise>
- [12] : http://www.mi.parisdescartes.fr/~mea/cours/Mi/ToIP_securite.pdf
- [13] : Thèse : Sécurité de la téléphonie sur IP –Mr : Thomas Guillet –Institut Telecom Paris Tech - 2010
- [14] : <https://madinainfotech.com/article/conception-et-d%C3%A9ploiement-voip>
- [15] : [www-l2ti.univ-paris13.fr > ~saidi > reseau](http://www-l2ti.univ-paris13.fr/~saidi/reseau)
- [16] : Rapport de stage : La téléphonie sur IP avec logiciel Anée universitaire 2012/2013
- [17] : <https://www.clemaner.com >switch-vlan-Cisco.php>
- [18] : <https://www.commentcamarch.net /fourm/affich-3853519-Definition-de-trunk>
- [19] : <https://community .Cisco .com > td-p>
- [20] : <https://www.commentcamarch .net/fourm/affich-1702295-loopback>
- [21] : <https://oo2fr >informatique >Cisco call-manager-et-unity-mise-en-œuvre&ved=2ahuqewivs-vjx>
- [22] : <https://www.imesit.fr/fonctionnalites-voip>