Table des matières

Liste des figures

Acronymes

2G/3G : Deuxième/ Troisième génération

ADSL+ : Ligne d'abonné numérique asymétrique

ATM : Mode de transfert asynchrone

BGP: Border Gateway Protocol

BRAS: Serveur d'accès distant large bande

CATV : TV/câble

CMTS : Système de terminaison modem câble

DCS : Système de Communication numérique

DSL : Ligne d'abonné numérique

DWDM : Multiplexage en longueur d'onde dense

E-MAN : Réseau métropolitain Ethernet

FR : Relais de trames

FTTH : Fibre jusqu'à l'abonné

GGSN : Nœud de support GPRS de transit

GPRS : General Packet Radio Service

GW : Passerelle

MPLS: Multi Protocol Label Switching (Commutation multiprotocole avec étiquetage des flux)

NB-RAS : Serveur d'accès distant - bande étroite

NGN : Réseau de prochaine génération

OSPF : Open Shortest Path First

PON : Réseaux optiques passifs

PoP : Point de présence

PSTN : Réseau téléphonique public commuté

QdS : Qualité de Service

SDH : Hiérarchie numérique synchrone

SONET : Synchronous Optical NETwork (Réseau optique synchrone)

TDM : Multiplexage temporel

UMTS : Système de télécommunication mobile universel

VoIP : Voix sur IP

VPN : Réseau privé virtuel

WAN : Réseau étendu

IM : Instant messaging

CTI : couplage téléphonie Informatique

Hot desking : partage de bureau

Le cloud computing : c'est l'accès via le réseau, à la demande et en libre-service, à des ressources informatiques virtualisées et mutualisées.

Introduction générale

Les communications unifiées sont la convergence de plusieurs technologies de communication en une solution unique. Elles rassemblent plusieurs fonctionnalités et services en une plateforme unifiée et intégrée pour les communications textuelles, audio et vidéo, accessible par ordinateur ou terminaux mobiles. Ces technologies incluent la messagerie électronique, la messagerie instantanée, les appels et conférences audio et vidéo, mais aussi les annuaires, calendriers et tâches.

Au cours des dernières années, le secteur des affaires n'a pas tardé à explorer les solutions de communications unifiées mais avec certaines craintes. La principale raison à cela est qu'il n'y a pas encore de véritable solution « claire » chez les fournisseurs de communications unifiées qui s'étende à travers toutes les plateformes e les médiums de communication en un seul système unifié.
Dans ce contexte, les opérateurs télécom ne cessent d'améliorer d'avantage leurs infrastructures et leurs technologies de communications afin de présenter des solutions qui soient à la hauteur des attentes de ses clients.

C'est dans ce cadre que ce projet s'inscrit, il s'agit d'étudier l'expérience de l'opérateur historique en Tunisie qui est TUNISIE TELECOM avec la communication unifiée. Dans cette démarche vers la communication unifiée on s'intéresse principalement à la couche transport de cet opérateur qui a passé de la phase d'un réseau composé de plusieurs réseaux indépendants (IP, ATM, PDH, SDH) engendrant une complexité d'utilisation à un réseau unique facile et simple se basant principalement sur MPLS.

Dans une première partie, nous avons défini le concept de la communication unifiée, évoquer la nécessité de la mise à niveau de l'infrastructure du réseau de télécommunications coté équipements ainsi que coté protocoles afin qu'on puisse satisfaire la convergence de la voix et des données informatiques et présenter le NGN comme une solution capitale qui peut satisfaire ces exigences.

Ensuite, présenter l'expérience de Tunisie Télécom en tant qu'opérateur historique dans le secteur de la télécommunication en Tunisie avec la communication unifiée et les projets réalisés qui lui ont permis de passer d'un simple opérateur qui implémentait des solutions de gestion des appels se basant sur une architecture NGN au début du deuxième millénaire à un fournisseur de service VoIP.

Dans cette démarche vers la communication unifiée on s'intéresse principalement à la couche de transport qui a passé de la phase d'un réseau composé de plusieurs réseaux indépendants (IP, ATM, PDH, SDH) engendrant une complexité d'utilisation à un réseau unique facile et simple se basant sur **MPLS**.

La deuxième partie est consacrée à l'étude théorique de la solution MPLS/IP et la structure du Backbone de Tunisie Telecom. Dans cette même partie, nous avons conçu et configuré les routeurs de la couche transport afin de migrer vers une solution MPLS/IP au sein de la Backbone Tunisie Télécom. Les configurations au

cours de ce chapitre sont principalement conçu pour les routeurs qui relient la coté Backbone de Tunisie Telecom avec les différents réseaux (GSM, RTCP, ADSL, DATA, Business client,…).

Enfin, on termine notre projet par l'étude d'un cas particulier de VoIP pour Business client (cas SOTETEL) avec définition du réseau VPN reliant différents sites de l'entreprise, configuration du Call Manager et configuration de la partie trunk entre Voice Gateway et Softswitch.

Chapitre I : Eude du concept des communications unifiées et définition des besoins en infrastructure coté opérateur télécom

I. Introduction :

La Communication Unifiée est définie comme un processus dans lequel toutes les communications, les périphériques de communication et les médias sont intégrés, permettant aux utilisateurs de joindre tout le monde, depuis n'importe où et en temps réel.

Cette technologie permet de fusionner la voix et les données informatiques, permettant aux entreprises de simplifier le transport de l'information en temps réel et s'assurer de la facilité d'utilisation.

Une telle technologie nécessite la mise à niveau de l'infrastructure du réseau de télécommunications coté équipements ainsi que coté protocoles pour qu'elle puisse satisfaire la convergence de la voix et des données informatiques.

Les réseaux de la prochaine génération (*NGN* ou *Next Generation Network* en anglais) peuvent être une solution capitale pour ces exigences. Le *NGN*, avec leur architecture répartie, exploite pleinement des technologies de pointe pour offrir de nouveaux services sophistiqués et augmenter les recettes des opérateurs tout en réduisant leurs dépenses d'investissement et leurs coûts d'exploitation.

L'évolution d'un réseau existant vers cette nouvelle structure nécessitera une stratégie de migration progressive visant à réduire au minimum les dépenses d'investissement pendant la phase de transition, tout en tirant parti très tôt des avantages qu'elle présente.

Toute démarche entreprise lors de cette étape de transition devra simplifier l'évolution du réseau vers l'architecture *NGN* à commutation de paquets. Pendant plusieurs années encore, les Services de commutation traditionnels vont devoir coexister avec des éléments de réseau mettant en œuvre de nouvelles technologies.

II. Présentation de la communication unifiée :

1. **Définition :**

   La communication unifiée signifie faire converger la **voix**, la **vidéo** et les **données** en un système d'information sécurisé unique permettant de transmettre une information de n'importe quel type, n'importe où, à n'importe quel moment.

   L'intégration de toutes les méthodes de communication moderne en une seule plateforme simplifie considérablement le travail en équipe accélérant donc la productivité. L'utilisateur sait en un coup d'œil le moyen le mieux adapté pour correspondre avec un collègue. Le lien avec l'entreprise et son cœur de métier est accru [1].

2. **Fonctionnalité :**

   La communication Unifiée est un ensemble de fonctionnalités qui permettent de :

a. Partager et gérer l'information :

- Gestion documentaire
- Agendas partagés
- Plannings partagés
- Gestion d'informations : wiki, blog, lien, …
- Portails Intranet, Extranet, etc.

b. Mieux communiquer en interne :

- Réseau téléphonique d'entreprise
- Click to call
- Gestion de la présence
- Messagerie instantanée

c. Mieux communiquer avec les clients et les partenaires :

- Interactivité : Conférences, Webinars, …
- Virtualisation des centres d'appels
- Web conférence & Vidéo Conférence

d. Se réunir à distance

- Audioconférence
- Visio personnelle
- Visioconférence
- Web conférence

e. Gérer la mobilité

- Free seating
- Softphone
- Numéro unique
- Convergence fixe mobile

Figure 1.1 : Différents services de la communication unifiée

3. Différents services de la communication unifiée :

a. **Le routage d'appels intelligent :** Il existe trop de canaux de communication (Poste fixe, bureau, Poste fixe domicile, *GSM* entreprise, *GSM* privé, *IPphone* au bureau, *Softphone* sur le *Laptop*, Poste DECT ou *WiFi*, Répondeur/serveur vocal, etc.) ce qu'en résulte la perte souvent de beaucoup de temps pour arriver à joindre une personne.

La Communication Unifié permet une automatisation accrue :

- Utilisation de l'agenda (d'entreprise & personnel)
- Prise en compte de l'état de présence

- Création de règles CTI dynamique/contextuelle
- Intégration dans les processus/applications métiers

b. **La vidéo ou le web conférence :** La collaboration est souvent le résultat d'un processus d'escalade :

- Début d'une interaction (asynchrone) au travers d'échange d'émail
- Augmentation de l'interaction temps réel avec l'utilisation d'IM (Instant messaging)
- Passage à un appel téléphonique (Softphone ou CTI + IPphone)
- Création d'une audio conférence pour avoir ensembles les acteurs importants
- Discussions sur du contenu … et passage à la web-conférence

Figure 1.2 : La vidéo conférence

c. Le partage de contenus ou d'applications :

- Diversification du type de contenu partagé (Documents, Images, Site web,…).
- Recourt à une application (Formulaire, Tableau blanc, Logiciel métier,…).

Il existe deux modes de partage :

- Passif (visualisation only)
- Actif (prise de contrôle)

d. La nomadicité :

- Le découplage géographique de la ligne de téléphone
  - Quelque part sur le réseau informatique
  - Au siège central mais aussi au sein d'un site satellite/secondaire
  - Le concept de Flex Desk / Hot Desking
- L'utilisation mobile via les accès réseau sans fils
  - Wifi
  - 3G
  - Convergence Fixe Mobile

e. **La Messagerie Unifiée :** C'est la concentration des diverses sources d'information écrites (comptes e-mail, fax, SMS, MMS, recommandé, etc.) au sein d'une seule boîte accessible de partout.

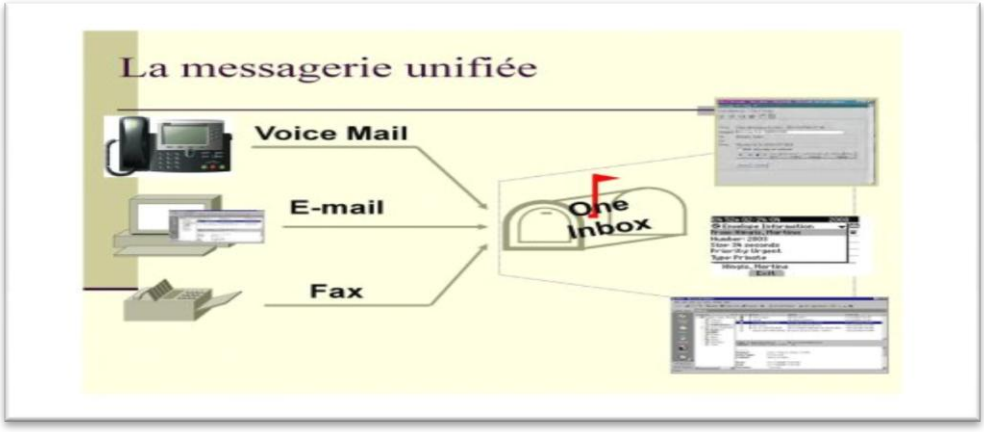

Figure 1.3 : La messagerie unifiée

4. **Conclusion :**

La communication unifiée est une philosophie de travail (Communiquer, échanger, collaborer, travailler en mode projet, …). La communication unifiée est avant tout un changement de mentalité!

III. Etude du concept NGN : définition et principes de base

1. **Définition :**

Le NGN est défini comme un réseau de transport en mode paquet permettant la convergence des réseaux Voix/données et Fixe/Mobile; ces réseaux permettront de fournir des services multimédia accessibles depuis différents réseaux d'accès [2].

Afin de s'adapter aux grandes tendances qui sont :

- La recherche de souplesse d'évolution de réseau,
- La distribution de l'intelligence dans le réseau,
- L'ouverture à des services tiers,

Les NGN sont basés sur une évolution progressive vers le « tout IP » et sont modélisés en couches indépendantes dialoguant via des interfaces ouvertes et normalisées.

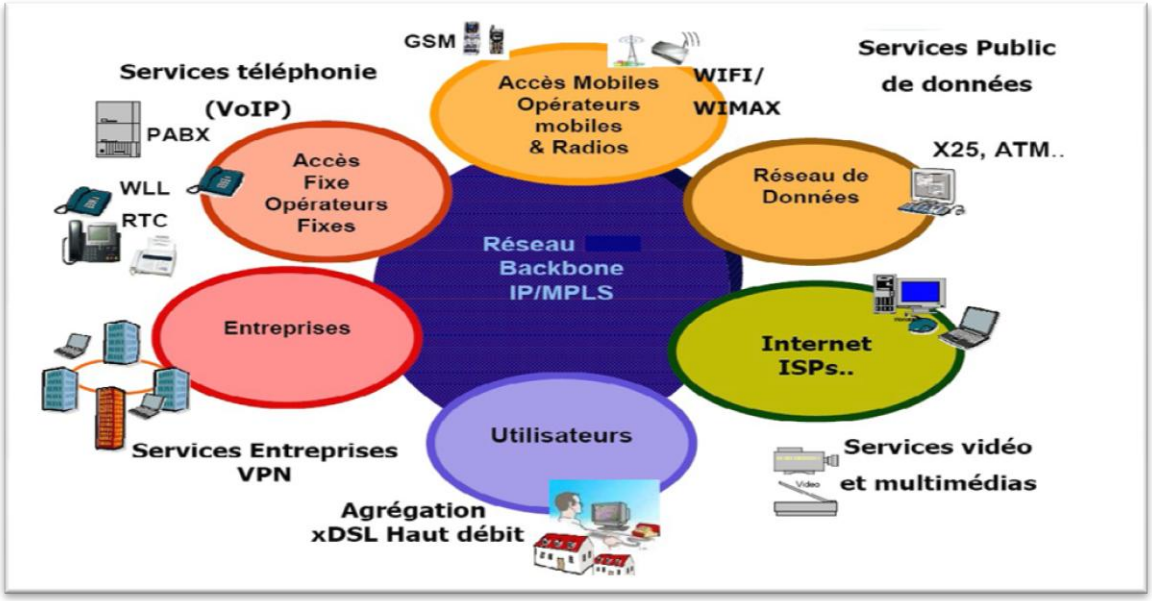

Figure 1.4 : Principe de consolidation du réseau

2. **Modèle d'architecture en couche :**

Le passage à une architecture de type NGN est notamment caractérisé par la séparation des fonctions de commutation physique et de contrôle d'appel. L'architecture NGN introduit un modèle en couches, qui scinde les fonctions et les équipements responsables du transport du trafic et du contrôle. Il est possible de définir un modèle architectural basé sur quatre couches successives :

- **La couche d'accès,** qui regroupe les fonctions et les équipements permettant de gérer l'accès des équipements utilisateurs au réseau, selon la technologie d'accès (téléphonie commutée, DSL, câble). Cette couche inclut par exemple les équipements DSLAM (DSL Access Multiplexer) fournissant l'accès DSL.
- **La couche de transport**, qui est responsable de l'acheminement du trafic voix ou données dans le cœur du réseau, selon le protocole utilisé. L'équipement important à ce niveau dans une architecture NGN est le Media Gateway (MGW) responsable de l'adaptation des protocoles de transport aux différents types de réseaux physiques disponibles (TDM, IP, ATM,..).
- **La couche de contrôle**, qui gère l'ensemble des fonctions de contrôle des services en général, et de contrôle d'appel en particulier pour le service voix. L'équipement important à ce niveau dans une architecture NGN est le serveur d'appel, plus communément appelé Softswitch, qui fournit, dans le cas de services vocaux, l'équivalent de la fonction de commutation.
- **La couche de services** qui regroupe les plates-formes d'exécution de services et de diffusion de contenus. Elle introduit les applications (services à valeur ajoutée) aux usagers. Dans ce cas, L'opérateur peut se positionner grâce à sa couche contrôle en tant qu'agrégateur de services offerts par l'opérateur lui-même ou par des tiers.

Toutes ces couches sont indépendantes et communiquent entre elles via des interfaces ouvertes. Cette structure en couches est sensée de garantir une meilleure flexibilité et une implémentation de nouveaux services plus efficaces. La mise en place d'interfaces ouvertes facilite l'intégration de nouveaux services développés sur un réseau d'opérateur mais peut aussi s'avérer essentielle pour assurer l'interconnexion d'un réseau NGN avec d'autres réseaux qu'ils soient NGN ou traditionnels.

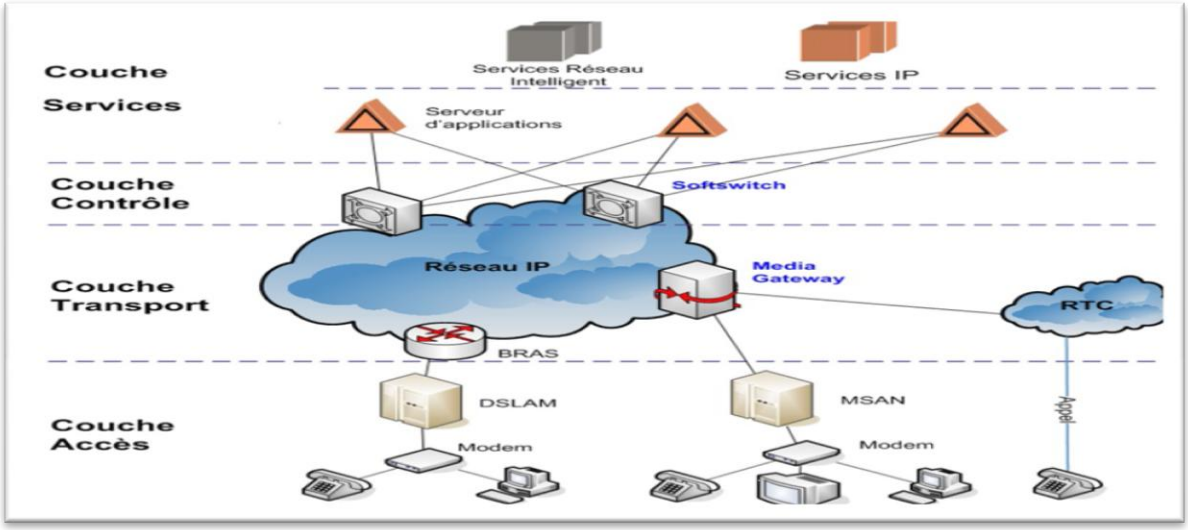

Figure 1.5 : Architecture en couche d un réseau NGN

3. **Cœur du réseau NGN (entités et protocoles) :**

L'utilisation d'un réseau de transport unique en mode paquet IP ainsi que la séparation entre les couches de transport et de contrôle des communications constituent les principales caractéristiques des réseaux *NGN* [3].

Une telle transformation nécessite l'introduction de nouvelles entités ainsi que de nouveaux protocoles qui peuvent être illustrés par la figure suivante :

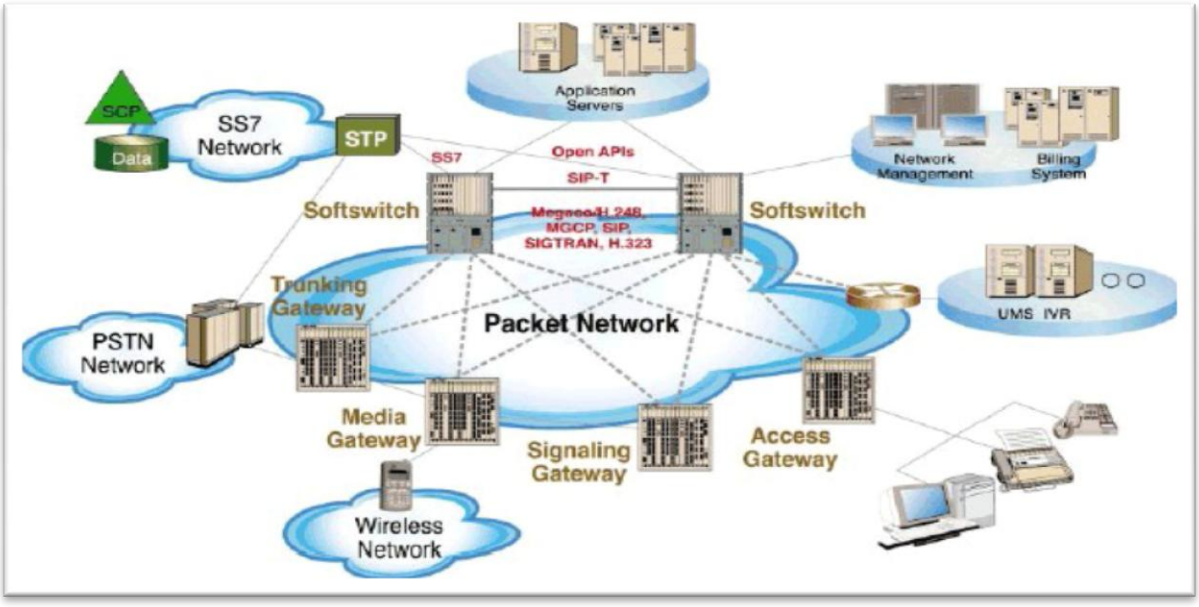

Figure 1.6 : entités et protocoles de NGN

a. **Entités fonctionnelles du réseau NGN :** Un réseau *NGN* utilise un ensemble d'équipements qui jouent le même rôle qu'un commutateur traditionnel, mais qui sont désormais séparés en trois composants distincts :

- **Le Softswitch ou le MGC (Media Gateway Controller) :** C'est la solution qui gère dans un réseau NGN l'intelligence du service de commutation. Toutefois, ce Softswitch n'est plus associé à un point physique du réseau, et ne gère plus les liens physiques du réseau, comme c'était le cas dans un réseau TDM. Il assure :
    - L'échange des messages de signalisation transmis de part et d'autre avec les passerelles de signalisation, et l'interprétation de cette signalisation.
    - Le routage d'un appel au sein du réseau.
    - Le traitement des appels : dialogue avec les terminaux et les serveurs d'application pour la fourniture des services.
    - Le choix et le contrôle de la MG de sortie selon l'adresse du destinataire, le type d'appel, la charge du réseau…etc.
    - La réservation des ressources selon le type d'appel.

  Physiquement, un Softswitch peut être implanté sur un serveur dédié ou bien être installé directement sur un équipement différent comme un Media Gateway ou même un commutateur traditionnel TDM. Dans ce cas, on parlera d'architecture complètement distribuée.
- **Le Media Gateway (MG) :** Son rôle est d'assurer la gestion (disponibilité, détection de fautes) de la couche physique du réseau. Cette couche physique peut être le réseau de transmission, ou le réseau d'accès.

  Dans le cas où il s'agit du réseau d'accès, la fonction de Media Gateway peut être embarquée dans l'équipement d'accès lui-même, comme c'est le cas pour **un MSAN** (*Multiservice Access Node*). Elle a pour rôle :
    - Le codage et la mise en paquets du flux média reçu de la part du réseau d'accès vers le réseau paquet et inversement, autrement dit, la conversion du trafic par exemple TDM/IP.
    - La transmission, suivant les instructions du Media Gateway Controller, des flux média reçus de part et d'autre. Le MG est piloté par le MGC.
- **Le Signalling Gateway (SG)** : Sa fonction est la conversion de la signalisation échangée entre le réseau de transport et le réseau externe interconnecté selon un format compréhensible par les équipements chargés de le traiter, mais sans en faire l'interprétation. Elle assure notamment, l'adaptation de la signalisation par rapport au protocole de transport utilisé (exemple adaptation TDM/IP).

b. **Protocoles de signalisation :** Le fait d'utiliser un réseau paquet pour transporter des flux multimédia, ayant des contraintes temps réel, a nécessité l'adaptation de la couche contrôle. Cette évolution a

logiquement généré de nouveaux protocoles, principalement concernant la gestion des flux média, au sein de la couche contrôle. Nous les classerons en trois grandes familles :

- **Protocoles de contrôle d'appel :** Ils permettent l'établissement d'une communication entre deux terminaux ou entre un terminal et un serveur ; les deux principaux protocoles sont H.323, norme de l'UIT et SIP standard développé par l'IETF.
    - **Le protocole H.323 :** H.323 est issue de la recommandation UIT-T H.320 qui traite de la visioconférence sur ISDN. Elle a été développée plus spécifiquement pour des réseaux ne garantissant pas une qualité de service, notamment Internet.

      H.323 normalise les procédures d'établissement et de gestion des appels, et établit une liste de codecs audio et vidéo obligatoires ou conseillés permettant aux deux parties de négocier entre elles et d'échanger des appels.

      H.323 s'articule autour de 4 composants majeurs qui interagissent dans un réseau de commutation par paquets :
        - Les terminaux H.323 qui sont des systèmes multimédia (téléphone, PC) permettant de communiquer en « temps réel ».
        - Le Gatekeeper qui gère les terminaux H.323 (identification et traduction d'adresses) et les établissements d'appels.
        - La passerelle H.323 ou Gateway H.323 qui permet d'interfacer le réseau IP avec le réseau téléphonique classique.
        - L'unité de contrôle qui gère les connexions multipoint (exemple : appels de conférence). Il se décompose en un Multipoint Controller (***MC***), affecté à la signalisation, et un Multipoint Processor (***MP***), dédié à la transmission proprement dite.
    - **Le protocole SIP :** SIP est un protocole de signalisation défini par l'IETF (Internet Engineering Task Force) permettant l'établissement, la libération et la modification de sessions multimédias. Il permet de prendre en charge la gestion des sessions d'application NGN basées sur un dorsal paquet, tels les services de gestion de présence, les services de messagerie instantanée etc. Il remplace donc à la fois les protocoles ISUP (ISDN User Part) et INAP (Intelligent Network Application Part) du monde de la téléphonie en apportant la capacité multimédia. La signalisation se fait par des messages en mode texte. Il hérite certaines fonctionnalités des protocoles http (Hyper Text Transport Protocol) utilisé pour naviguer sur le WEB, et SMTP (Simple Mail Transport Protocol) utilisé pour transmettre des messages électroniques (E-mails).

      L'adressage utilise le concept d'URL SIP (Uniform Resource Locator) qui ressemble à une adresse E-mail. Chaque participant dans un réseau SIP est donc adressable par une URL SIP.

SIP s'appuie sur un modèle transactionnel client/serveur. Les principales composantes sont :

- Le ***terminal (User Agent)*** : initie, accepte ou rejette les appels
- Le ***Proxy Server*** : reçoit les requêtes et les transfère au nœud suivant
- Le ***Redirect Server*** : retourne à l'émetteur la ou les adresses du nœud suivant à contacter directement.
- Le ***Registrar*** : gère les enregistrements des UA.

- **Protocoles de commande de Media Gateway :** Ces protocoles ont été engendrés par la séparation des couches Transport et Contrôle et permettent au Softswitch de gérer les Media Gateway. MGCP de l'IETF et MEGACO (*MEdia GAteway COntroller*) ou H.248, développés conjointement par l'UIT et l'IETF, prédominent actuellement.

  Le protocole MGCP possède une architecture centralisé : client, serveur. Le serveur de contrôle d'appel, le Call Agent, concentre l'intelligence du réseau et pilote en esclave les passerelles de média et assure la traduction de la signalisation entre SS7 des réseaux PSTN, d'un côté et H.323 ou SIP de l'autre coté.

  MGCP répond à un besoin spécifique, tel que le contrôle des *Gateways* dans les réseaux à grande échelle, il n'est pas fait pour piloter des applications comme les centres d'appel, les visioconférences en multipoint ou la diffusion de multimédia.

  Le protocole MEGACO/H.248 est un protocole dérivé du MGCP. Il offre des améliorations par rapport à ce dernier : il supporte les visioconférences et il utilise les protocoles UDP, TCP, IPsec et IP pour se charger des communications entre passerelles.
- **Protocoles de signalisation entre les Softswitchs :** L'interconnexion des réseaux de données avec les réseaux existants TDM utilisant la signalisation SS7, a nécessité le développement de protocoles dédiés à l'interconnexion des réseaux et au transport de la signalisation SS7 sur des réseaux en mode paquet.

  Ces protocoles permettent la gestion du plan contrôle et le dialogue entre les MGCs. Il s'agit essentiellement de : BICC (***B****earer* ***I****ndependant* ***C****all* ***C****ontrol*), SIGTRAN (***SIG****nalling* ***TRAN****sport*) et SIP-T (***SIP*** *pour la* ***T****éléphonie*) au niveau du cœur du réseau.

4. Différentes catégories de NGN :

On peut classer la solution NGN selon deux catégories : le NGN téléphonie et le NGN multimédia.

a. **NGN téléphoniques :** Ce sont des architectures de réseau offrant uniquement les services de téléphonie. Il s agit donc de NGN téléphonie. Dans le RTC, un commutateur class 4 est un centre de transit. Un commutateur Class 5 est un commutateur d'accès aussi appelé centre à autonomie d'acheminement. Le NGN class 4 (resp. NGN class 5) émule donc le réseau téléphonique au niveau transit (resp. au niveau accès) en transportant la voix sur un mode paquet.

- **NGN de transit :** Dans ce scénario, l'opérateur applique le concept NGN au niveau de la couche transport de son réseau, mais dès que l'on s'approche des commutateurs de class 5, le trafic

continue à être supporté par le réseau traditionnel. Cette démarche est mise en place par un grand nombre d'opérateurs mondiaux, précisément sur ses fonctions de transit que ce soit au niveau régional, national ou international. Il s'agit de la première étape de la migration d'un réseau traditionnel vers un réseau NGN pour nombre d'entre eux.

Concrètement, il s agit d'installer des Media Gateway assurant l'interfaçage entre le réseau IP de transport de données avec le réseau téléphonique TDM traditionnel. Les passerelles sont alors administrées à distance par un Softswitch dans le cadre d'une architecture centralisée en utilisant en général les protocoles MGCP/H.248.

- **NGN d'accès :** L'opérateur choisit de mettre en place une architecture NGN qui a pour vocation également à agréger le trafic local. Ce scénario constitue une prolongation naturelle du premier. D'un point de vue architectural, il s agit de la même solution que pour le scénario précédent à un niveau différent du réseau plus proche de l'abonné. En effet un commutateur de class 5 ne diffère d'un commutateur de classe 4 ou de niveau hiérarchique supérieur que par sa capacité de traitement de données. Il n'intègre aucune intelligence réseau.

  Les commutateurs de class 5 constituent le point de raccordement avec l'abonné pour la fourniture des services voix basiques. Les opérateurs historiques possèdent plusieurs milliers de ces commutateurs et de part leur position stratégique dans leur réseau ont été peu enclins jusqu'à présent à les remplacer par une solution NGN. Toutefois, compte tenu de la forte progression de la pénétration des services hauts débit et du déclin de la demande en services de téléphonie traditionnelle, les opérateurs considèrent de plus en plus l'opportunité de faire converger leur infrastructure d'accès vers une **plate-forme IP** commune tel que le déploiement de l'équipement **MSAN**.

  En conclusion, une migration de class 5 s'avère être un véritable « Big Bang » au niveau du réseau de l'opérateur et cela est d'autant plus coûteux et complexe que le réseau est important.

b. **NGN Multimédia :** C'est une architecture offrant les services multimédia puisque l'usager a un terminal IP multimédia. Cette solution est plus intéressante que les précédentes puisqu'elle permet à l'opérateur d'innover en termes de services par rapport à une solution NGN téléphonie qui se cantonne à offrir des services de téléphonie. Le Multimédia NGN connu sous le nom IMS permet d'offrir des services multimédia à des usagers disposant d'un accès large bande tel que xDSL, câble, Wifi/Wi-Max, EDGE/UMTS, etc.

5. Conclusion :

Ces dernières années, l'essor rapide du réseau de données global, notamment dans le domaine de la communication unifiée, a drainé des incohérences, des insuffisances et des déficiences qu'il faudra éliminer dans le réseau futur.

Le réseau évolutif continuera de répondre aux exigences diverses des clients et des marchés avec des solutions adaptées tout en redevenant plus cohérent, grâce à la rationalisation et au regroupement des

éléments de réseau de base. Dans le climat actuel, tout cela doit se faire en maintenant l'équilibre délicat entre recettes, dépenses d'investissement et dépenses d'exploitation.

Le succès futur des réseaux de données dépend du choix de la combinaison optimale de plusieurs solutions architecturales et technologiques flexibles et évolutives pour répondre aux besoins d'une clientèle très diverse.

Cette démarche fera l'objet du chapitre suivant qui va présenter l'expérience de Tunisie Télécom en tant qu'opérateur historique dans le secteur de la télécommunication en Tunisie avec la communication unifiée.

Chapitre II : L'expérience de Tunisie Telecom avec la communication unifiée

I. Introduction :

Tunisie Télécom est l'opérateur historique dans le secteur de télécommunication en Tunisie. C'est un opérateur global multiservices, ses services couvrent toutes les lignes de produit (fixe, mobile et data) et tous les segments du marché (particulier et entreprises de toute taille). Il possède une infrastructure de télécommunication performante utilisant les technologies de pointe

Tunisie Télécom est passée actuellement d'un simple opérateur qui implémente une solution de gestion des appels se basant sur une architecture NGN au début du deuxième millénaire à un fournisseur de service VoIP.

Cette nouvelle tendance a exigé l'instauration d'une nouvelle génération d'applications et d'équipement aussi gourmande en terme de bande passante. Tunisie Telecom a été dans l'obligation de prendre en compte une politique lui permettant de faire coexister ses nouveaux services avec son architecture interne et d'instaurer le concept **QoS** dans un réseau de télécom pareil.

II. Description de réseau de Tunisie Télécom :

Au passage à l'an 2000, le réseau de Tunisie Telecom était composé de plusieurs réseaux indépendants ce qui a engendré une complexité d'utilisation :

- Réseau fixe : essentiellement en TDM
- Réseau mobile : TDM
- Réseau Data : transmission de données basée sur ATM, IP, ADSL.

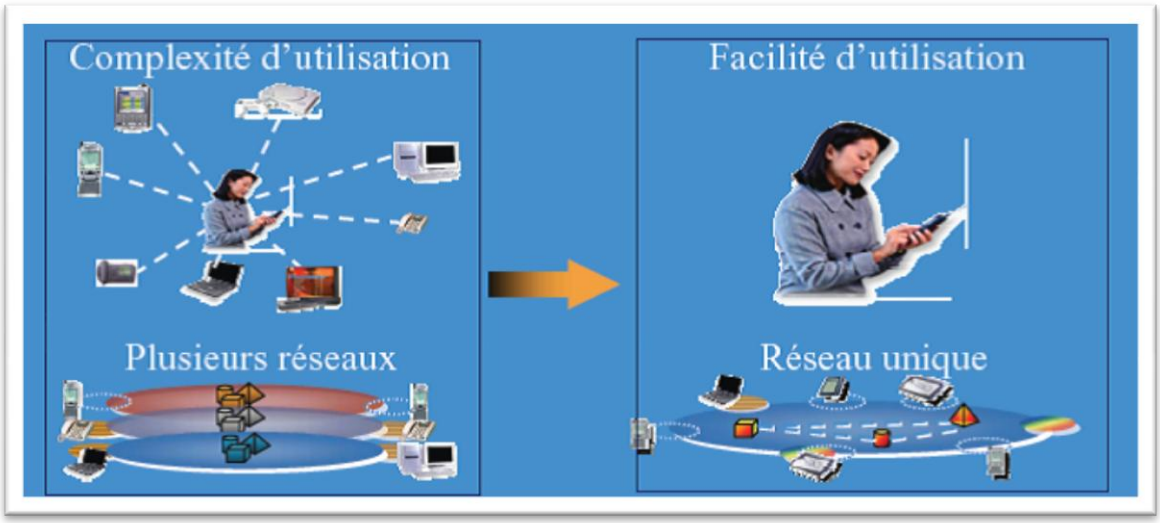

Figure 2.1 : Migration vers le réseau NGN

Un réseau qui satisfait les besoins d'une clientèle variée (abonnés particuliers, entreprises, organismes publiques,…) plus au moins exigeante en termes de débit et de qualité de service.

La clientèle de Tunisie Telecom est repartie comme suit :

Indicateurs 2011 :

Nombre d'abonnés au réseau téléphonique mobile/fixe	**4.5/1.25 M**
Bande passante internationale	**8.75 Gbps**
Liaisons Spécialisées	**5800**
Frame Relay	**7100**
ADSL Entreprise/Pro	**842/923**
X25	**281**
Fibre Optique (y compris les LLI)	**65**

1. Éléments déclencheurs du besoin en NGN :

Les éléments déclencheurs du besoin en NGN peuvent être repartis comme suit :

- **Éléments déclencheurs économiques :**
  - Développement des usages autour des données
  - Besoin de créer de nouveaux services et applications
  - Nécessité de réduire les coûts (CAPEX/OPEX)
- **Éléments déclencheurs techniques**
  - Convergence voix / données

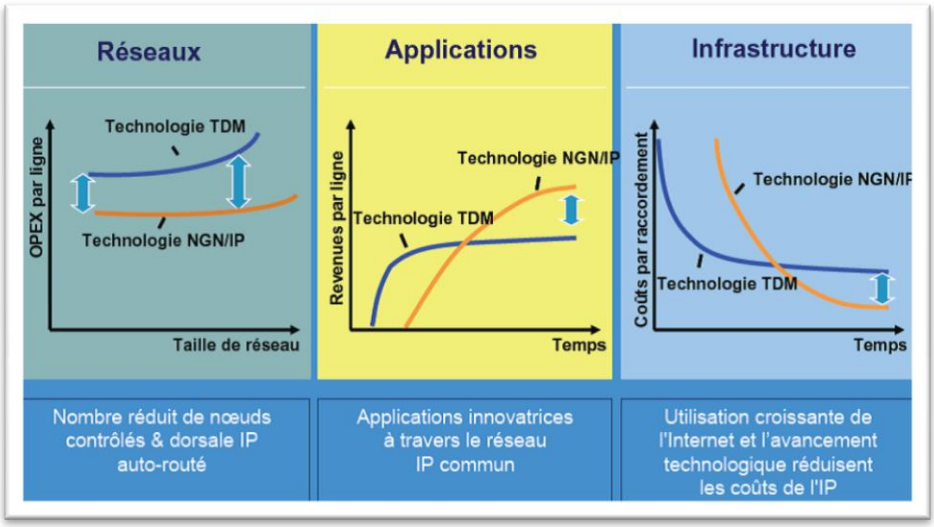

Figure 2.2 : valeur ajoutée du NGN

2. Cadre juridique :

Bien que la migration de Tunisie Télécom vers le *NGN* ait débuté depuis 2002, la publication du décret fixant les conditions de fourniture du service *VoIP* par les opérateurs de télécommunication en Tunisie n'a eu lieu qu'en Juillet 2008.

Il insiste sur :

- Les aspects réglementaires
- Les exigences au niveau de la plate-forme *VoIP* de l'opérateur : accès sécurisé, haute disponibilité, *QoS* :

- Délais de transmission < 100 ms,
- Gigue < 50 ms,
- Taux de perte de paquets IP < $10^{-}3$,
- Taux d'erreurs dans les paquets IP < $10^{-}4$

3. Migration vers NGN :

La migration vers un réseau NGN apparaît aujourd'hui comme un processus inévitable du fait de la convergence voix/données/images d'un côté et fixe/mobile d'un autre côté [7].

La migration de Tunisie Télécom vers le NGN depuis 2002 a suivi l'approche suivante :

- Tenir compte des réseaux existants.
- Migration en douceur :
  - Phase 1 : Coexistence des réseaux existants avec le réseau NGN
  - Phase 2 : Intégration des réseaux vers un seul réseau NGN offrant la multitude des services (voix, données, vidéo, etc.)
- Ne plus investir dans la commutation TDM de classe 4

L'opérateur historique a entamé cette migration à travers certains projets afin de maîtriser ce nouveau concept et mieux évaluer les bénéfices apportés

Figure 2.3a : Stratégie de Tunisie Télécom vers la convergence

Figure 2.3b : Stratégie de Tunisie Télécom vers la convergence

Cette migration a ciblé les clients suivants :

- Centres d'appels
- Entreprises dont l'activité est basée sur les technologies de la communication
- Entreprises administratives et économiques ayant des sites et des succursales multiples
- Instances et organisations internationales établies dans la république Tunisienne

III. Préparation de l'infrastructure de Tunisie Télécom :

La préparation de l'infrastructure appropriée permettant à Tunisie Télécom de converger vers le NGN a été basée sur les points suivants :

- Renforcement du cœur du réseau en terme de capacité des liens inter-nœuds et nombres d'interfaces
- Extension de la couche *Edge* du *Backbone IP MPLS* (acquisition de PE additionnels)
- Acquisition des équipements de connexion d'abonnés CPE
- Mise en place d'un réseau d'agrégation Métro Ethernet (en cours de déploiement)
- Acquisition d'un système de provisioning
- Acquisition de passerelle internationale permettant d'offrir un service IPVPN de bout en bout à l'échelle internationale

1. Projets NGN :

- **2002 : Projet Voix sur ATM (ENGINE) :**

Objectif :

Le réseau Voix sur ATM a été introduit dans le réseau de Tunisie Télécom en 2002 pour :

- Réaliser l'extension du réseau téléphonique
- Véhiculer le trafic Fixe-Fixe entre les différents nœuds de ce réseau en utilisant la technologie paquet VoATM.
- Communiquer avec le réseau PSTN existant

Principe

- Le réseau ENGINE est basé sur :
  - 8 Media Gateways : AXD301 (MGW).
  - Équipements d'accès (40.000 L).
  - 2 SoftSwitch : Telephony Server (TeS).
- Les appels téléphoniques sont convertis en paquets ATM par les MGWs, et contrôlés par un TeS
- Evolution vers la mise en place d'une seule infrastructure de commutation et de transport pour tous les services (voix fixe et mobile, données ...)
- Centralisation de la fonction de gestion des appels et des services au niveau des serveurs téléphoniques

- Exploitation de la technologie ATM pour optimiser l'utilisation de largeur de bande

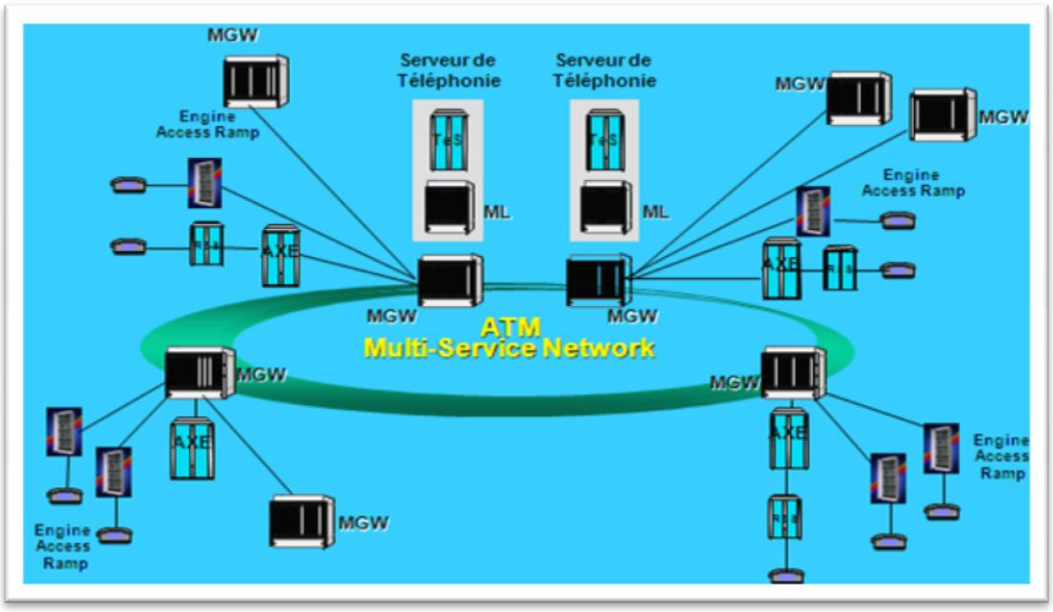

Figure 2.4 : Le réseau ATM

- **2004 : Réseau Backbone IP National**

Figure 2.5 : Le réseau Backbone IP National

- **2004 : Projet VoIP International :**
  - Introduction de la Voix sur IP, au niveau international avec les opérateurs suivants :
    - France Telecom.
    - Telecom Italia.
    - Gain en Bande Passante
  - Equipements : 1 SoftSwitch + 2 MGW / routeurs (CISCO)

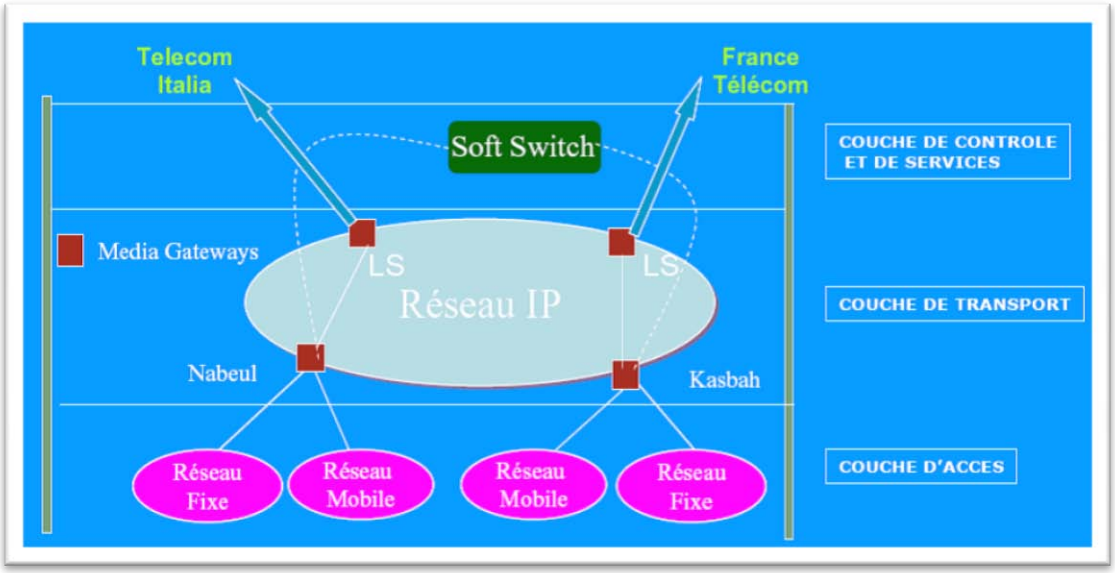

Figure 2.6 : Le réseau IP international

- **2005 : Projet VoIP National :**

Objectif :

- Assurer une plus grande flexibilité d'acheminement du trafic entre les centraux concernés (routage à travers un Backbone IP)
- Consolider le réseau de Transit National et véhiculer une partie du trafic en mode voix sur IP.
- Mettre en place un réseau VoIP pour véhiculer une partie du trafic Mobile-Mobile du grand Tunis et offrir un 1er niveau de souplesse de routage à travers les MGWs.
- Raccordement sur le Backbone IP/MPLS de Tunisie Télécom.

Portée du projet:

- Un Media Gateway Controller (HiE 9200)
- 7 Media Gateways (HiG 1200)

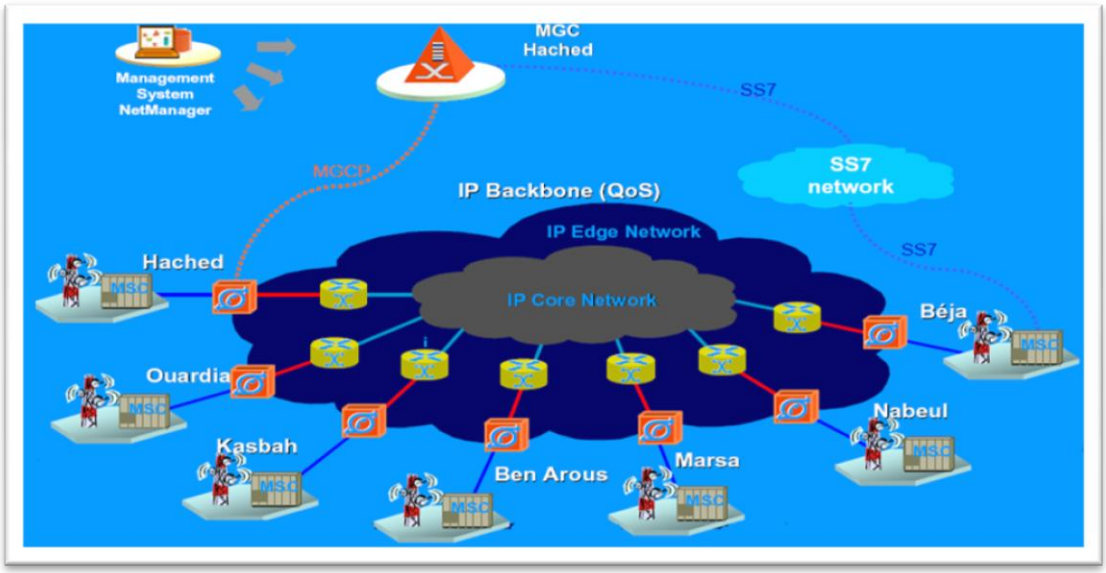

Figure 2.7 : Le Backbone IP national

- **2007 : Projet Réseau National :**

  Objectif :

  - Décharger le réseau de transport TDM du trafic Internet.
  - Véhiculer le trafic additionnel voix fixe et mobile, le trafic Internet haut débit et le trafic de transmission de données
  - Optimiser les ressources de transmission nationales
  - Introduction de nouveaux services: Centrex IP, Messagerie unifiée, Streaming, voix sur IP, etc.

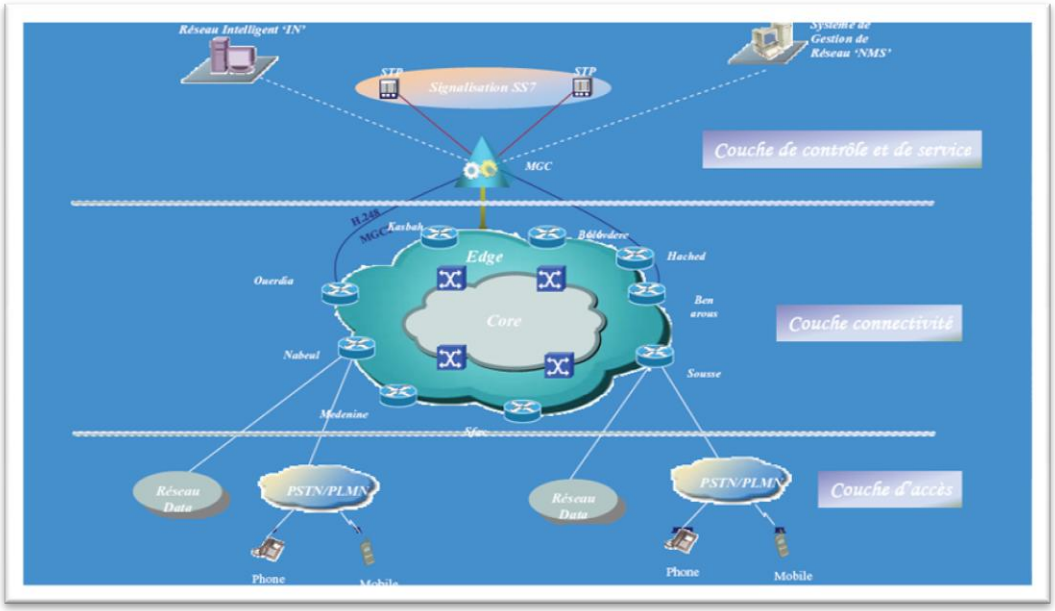

Figure 2.8 : Le réseau national

- **2010 : Réseau Métro-Ethernet :**

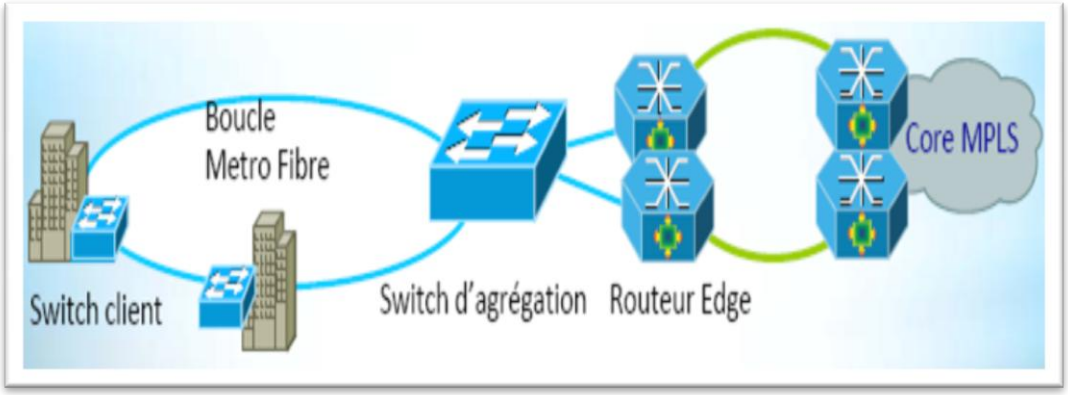

Figure 2.9 : Le réseau Métro-Ethernet

Objectif : mise en place d'un réseau d'accès à haut débit (jusqu'à 1 Gbps sur FO)

Avantages : débit scalable jusqu'à 1Gbps, bande passante symétrique, service flexible, QoS par profile client, réseau sécurisé

- 1ère phase : installation de boucles en FO pour le FTTB dans les villes de Grand Tunis, Sousse et Sfax et acquisition d'équipements d'agrégation Métro Ethernet et renforcement de la couverture (Mannouba, Monastir, Bizerte…)
- 2ème phase : installation de boucles FO pour le FTTH

2. Etapes de commercialisation du service VoIP :

- **1ère phase :** service VoIP sera destiné aux clients grands comptes multi-sites :
  - Clients doivent bénéficier au préalable du service VPN IP/MPLS : prise Platinium
  - Clients multi-sites : service VoIP seulement pour trafic inter-sites (continuer à utiliser le réseau PSTN pour le trafic téléphonique externe au VPN)
  - Serveur de communication (PABX IP) sera hébergé et géré par Tunisie Télécom (2 cas se présentent: le serveur de communication pourrait être dédié à un seul client ou mutualisé entre plusieurs clients)
- **2ème phase :** généralisation du service VoIP :

3. Architecture technique du réseau IP/MPLS de Tunisie Télécom : niveaux hiérarchiques

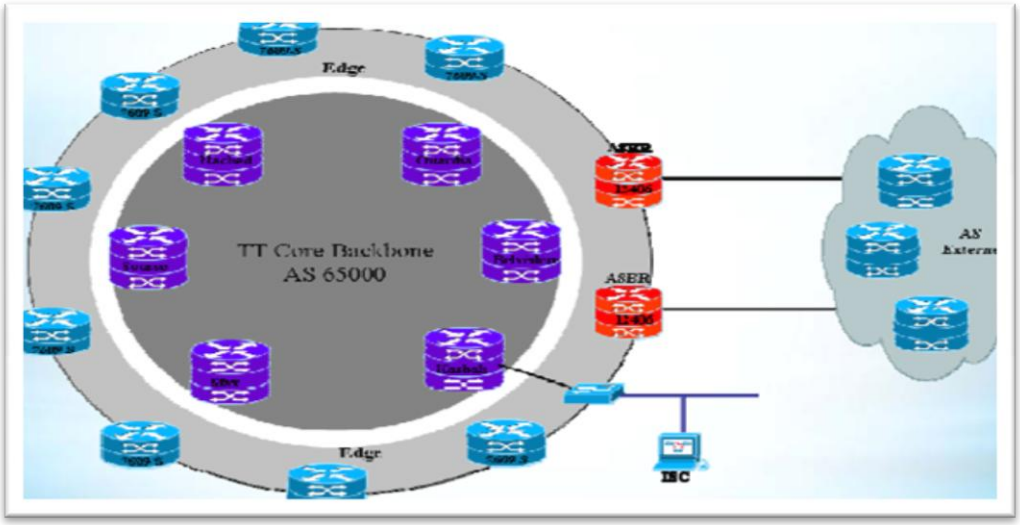

Figure 2.10 : Architecture technique du réseau IP/MPLS de Tunisie Télécom

4. Architecture technique de la solution VOIP :

- **Serveur de communication mutualisé**
  - Tunisie Télécom offre les accès MPLS avec classe de service Voix : prise Platinum, héberge et gère le serveur de communication (partagé entre plusieurs clients)
  - Mise à niveau du réseau de Tunisie Télécom : offrir le service IP Centrex pour les petites et moyennes entreprises

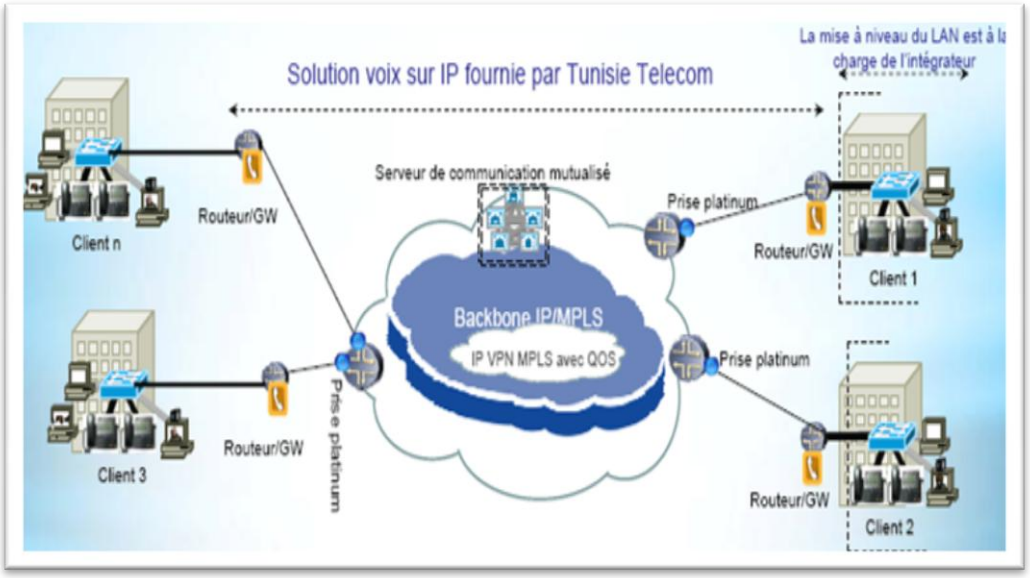

Figure 2.11 : Architecture technique de la solution VOIP_ Serveur de communication mutualisé

- **Serveur de communication dédié**
  - Plate-forme voix dédiée à un seul client grand compte

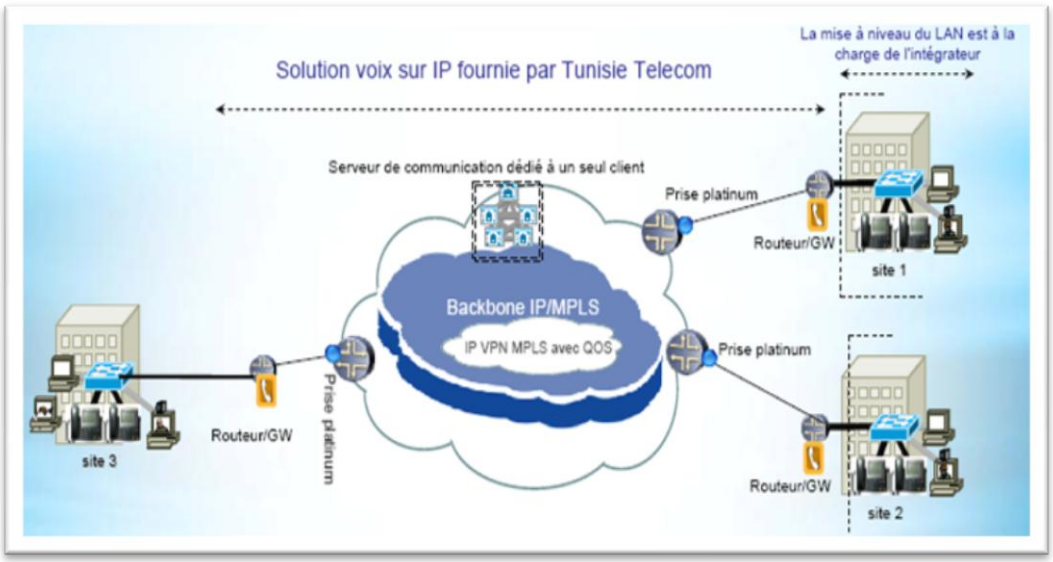

Figure 2.12 : Architecture technique de la solution VOIP_ Serveur de communication dédié

  - Exemple : projet pilote e-Santé :
    - **Objet :** modernisation du réseau de communication reliant les 280 sites relevant du Ministère de la Santé.
    - **Objectifs**
      - Raccordement des 280 sites au BB IP/MPLS de TT
      - Unifié les réseaux Data et voix inter-sites
      - Mise en place d'une solution VoIP dédiée (28 000 utilisateurs)
      - Mise en place d'une solution WiFi dans quelques sites
      - Offrir un service managé pour la voix et la data

- **Architecture cible :**

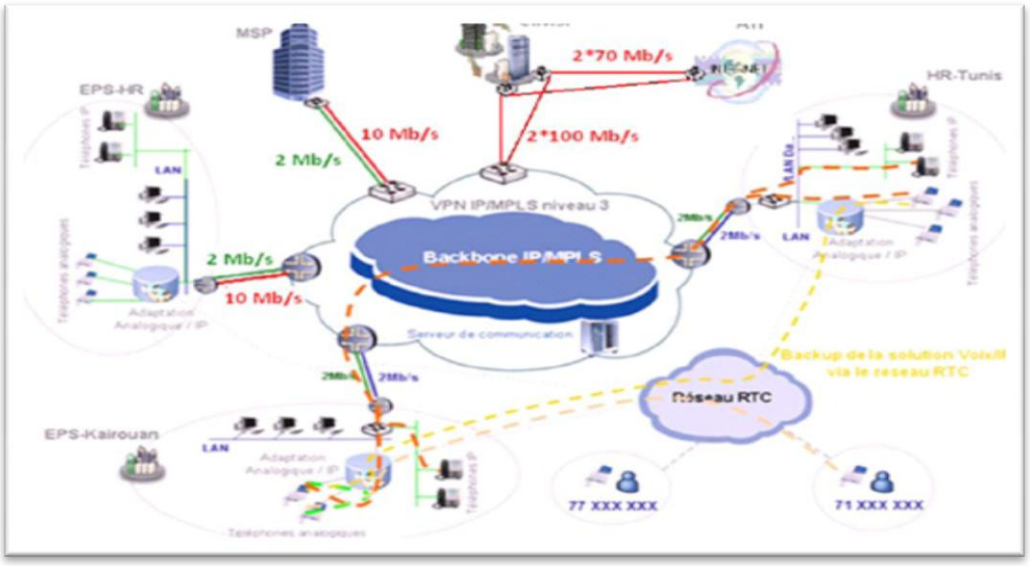

Figure 2.12 : Architecture cible du projet pilote e-Santé

IV. Développement des services de convergence :

Les études sont effectuées depuis 2004, les services NGN qui ont été pris en considération sont la voix sur IP, le Centrex IP, la messagerie unifiée, le VPN IP, la conférence multimédia, le vidéo à la demande, la fourniture de contenu, le Triple Play, … .

1. Le Centrex IP :

Objectif :

- Externalisation de l'autocommutateur privé de l'entreprise (PABX)
- Exploitation de la Voix sur IP
- Gratuité des communications inter sites
- Plan de numérotation unique
- Panoplie de services : messagerie unifiée, centre d'appel virtuel, favoriser le travail nomade, etc.

Avantages pour l'entreprise

- Coût des communications réduit
- Réduire les factures des communications mobiles
- Multitude de services offerts
- Collaborer avec les travailleurs nomades

Avantages pour l'opérateur

- Création de nouveaux services pour les consommateurs
- Améliorer le revenu en offrant de nouveaux services

2. La Messagerie unifiée :

Objectif :

- Regrouper sous une même interface : e-mail, fax, boîte vocale et SMS.

- Utilisation du même moyen de communication (internet, téléphone, WAP, client POP3).
- Ubiquité des services : accès rapide à tous les messages de n'importe où et n'importe quand.

Cibles : chefs d'entreprise, cadres, collaborateurs mobiles (remplacement du système actuel de messagerie).

3. **Le Triple play :**

Objectif : Abonnement haut débit comprenant :

- Accès Internet,
- Offre de téléphonie sur IP,
- Offre de flux vidéo (télévision sur IP)

Avantages pour Tunisie Télécom

- Convergence de 3 services en une seule offre
- Acquérir une nouvelle clientèle de fournisseurs de services
- Stimuler la demande pour l'accès haut débit

V. Conclusion :

On doit s'attendre à la cohabitation des technologies, des réseaux et des systèmes de signalisation issus du monde du TDM, de l'ATM, du FR et de l'IP durant plusieurs années, le tout interconnecté par des passerelles. Il faudra toutefois pour les opérateurs historiques une période de transition avant que la téléphonie résidentielle ne bascule entièrement sous IP.

Dans cette démarche vers la communication unifiée on s'intéresse ultérieurement à la couche de transport qui a passé de la phase d'un réseau composé de plusieurs réseaux indépendants (IP, ATM, PDH, SDH) engendrant une complexité d'utilisation à un réseau unique facile et simple se basant essentiellement sur MPLS.

L'étude théorique détaillée de la technique MPLS fera le thème principal du prochain chapitre.

I. Introduction :

MPLS (Multi Protocol Label Switching) est une technique réseau de commutation en cours de normalisation dont le rôle principal est de combiner les concepts du routage IP de niveau 3 et les mécanismes de la commutation de niveau 2 telles que implémentées dans ATM ou Frame Relay [4].
MPLS permet :

- d'améliorer le rapport performance/prix des équipements de routage,
- d'améliorer l'efficacité du routage (en particulier pour les grands réseaux)
- d'enrichir les services de routage (les nouveaux services étant transparents pour les mécanismes de commutation de label, ils peuvent être déployés sans modification sur le cœur du réseau).

Le but de MPLS était à l'origine de donner aux routeurs IP une plus grande puissance de commutation, en basant la décision de routage sur une information de label (ou tag) insérée entre le niveau 2 (couche liaison de données) et le niveau 3 (couche réseau). La transmission des paquets était ainsi réalisée en commutant les paquets en fonction du label, sans avoir à consulter l'entête de niveau 3 et la table de routage.
Toutefois, avec le développement de techniques de commutation comme CEF (*Cisco Express Forwarding*) et la mise au point de nouveaux ASIC (*Application Specific Interface Circuits*), les routeurs IP ont vu leurs performances améliorées sans le recours à MPLS. L'intérêt de MPLS n'est pas limité à la rapidité de commutation apportée mais aussi à l'offre de services qu'il permet, avec notamment les réseaux privés virtuels (VPN) et le Traffic Engineering (TE), qui ne sont pas réalisables sur des infrastructures IP traditionnelles.

II. Objectifs :

L'un des objectifs initiaux était d'accroître la vitesse du traitement des datagrammes dans l'ensemble des équipements intermédiaires. Cette volonté, avec l'introduction des giga routeurs, est désormais passée au second plan. Depuis, l'aspect "fonctionnalité" a largement pris le dessus sur l'aspect "performance", avec notamment les motivations suivantes :

- Intégration IP/ATM,
- Création de VPN,
- Flexibilité : possibilité d'utiliser plusieurs types de media (ATM, FR, Ethernet, PPP, SDH),
- Differential Services (DiffServ),
- Routage multicast,
- Transition facile vers l'Internet optique : MPLS n'étant pas lié à une technique de niveau 2 particulière, il peut être déployé sur des infrastructures hétérogènes (Ethernet, ATM, SDH, etc.). Avec la possibilité d'utiliser simultanément plusieurs protocoles de contrôle, MPLS peut faciliter l'utilisation de réseaux optiques en fonctionnant directement sur WDM.
- Traffic Engineering permettant de définir des chemins de routage explicites dans les réseaux IP (avec RSVP ou CR-LDP). Les labels peuvent être associés à un chemin, une destination, une source, une application, un critère de qualité de service, etc… ou une combinaison de ces différents éléments.

Autrement dit, le routage IP est considérablement enrichi sans pour autant voir ses performances dégradées. On peut imaginer qu'un des services les plus importants sera la possibilité de créer des réseaux privés virtuels (VPN) de niveau 3. Ainsi, des services de voix sur IP, de multicast ou d'hébergement de serveurs web pourront coexister sur une même infrastructure.

III. Le routage classique :

IP est un protocole de niveau réseau fonctionnant dans un mode non connecté, c'est-à dire que l'ensemble des paquets (ou datagrammes) constituant le message sont indépendants les uns des autres : les paquets d'un même message peuvent donc emprunter des chemins différents utilisant des protocoles IGP (*Interior Gateway Protocol*), tels que RIP ou OSPF, dans le cas où il s'agit d'un même système autonome. Ils peuvent aussi utiliser des protocoles EGP (*Exterior Gateway Protocol*), tel que BGP (*Border Gateway Protocol*) dans le cas où il s'agit de routage entre des systèmes autonomes différents. Chaque routeur maintient une table de routage, dans laquelle chaque ligne contient un réseau de destination, un port de sortie, et le prochain routeur relaie vers ce réseau de destination.
A la réception d'un datagramme, les nœuds intermédiaires (ou routeurs) déterminent le prochain saut (ou next-hop) le plus approprié pour que le paquet rallie sa destination en se basant sur la décision des protocoles de routage. Ensuite l'adresse mac destination (niveau 2 du modèle OSI) du datagramme est remplacée par l'adresse mac du routeur saut (ou nexthop), et l'adresse mac source du datagramme est remplacée par l'adresse mac du routeur courant, laissant sans changement les adresses IP (niveau 3 du model OSI) du datagramme afin que le prochain routeur effectue les mêmes opérations sur le paquet pour les sauts suivants. Ce calcul épuisant est effectué sur tous les datagrammes d'un même flux, et cela autant de fois qu'il y a de routeurs intermédiaires à traverser. Il est donc gourmand en terme de ressource machine. Le mode non connecté du protocole IP, qui était initialement l'un de ses atouts, en particulier pour sa scalabilité, est devenu aujourd'hui un frein à son évolution.
Les inconvénients du routage IP classique se résument dans ses points :

- Utilisation des protocoles de routages dans tous les équipements pour distribuer les informations de routage et acheminer les paquets ;
- L'acheminement des paquets se fait seulement en fonction de l'adresse de destination ;
- Chaque routeur dans le réseau prend une décision indépendante lors de l'acheminement des paquets.

MPLS aide à réduire le nombre de consultation de routage et peut changer le critère d'acheminement. Cette capacité élimine le besoin d'exécuter un protocole de routage particulier dans tous les équipements.

IV. Les concepts du MPLS :

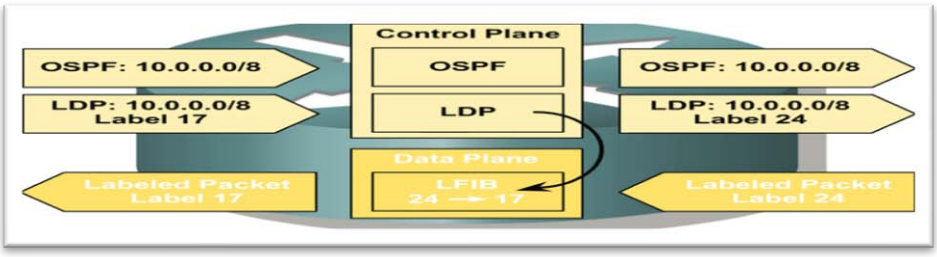

Figure 3. 1 Plan de contrôle et Plan de données

MPLS est un nouveau mécanisme de commutation qui utilise les labels pour acheminer les paquets. Le label correspond à l'adresse destination de la couche 3 ou à un autre paramètre comme la qualité de service, l'adresse source ou le circuit de couche 2.

MPLS se base sur deux principaux composants :

- Plan de contrôle : supervise l'échange des informations de routage et l'échange des labels entre les équipements. Un large nombre de protocole de routage est utilisé au niveau de ce plan comme OSPF, IGRP, EIGRP, BGP. Le plan de contrôle supporte aussi les protocoles d'échange de labels TDP (*Tag Distribution Protocol*) et LDP (*Label Distribution Protocol*) ;
- Plan de données : c'est un simple mécanisme d'acheminement des labels indépendant de type des protocoles de routage ou d'échange de label, il est basé sur la table LFIB (*Label Forwarding Information Base*) conçue par TDP ou LDP.

1. Label MPLS :

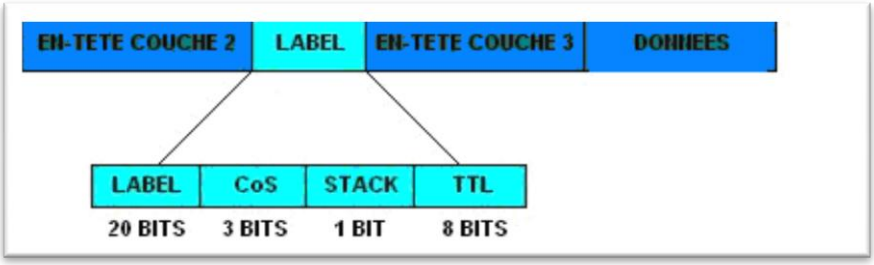

Figure 3. 2 Format du label MPLS

Le label est inséré entre la couche 2 (liaison de données) et la couche 3 (couche réseau). MPLS utilise un champ de 32 bits comme label, il contient les informations suivantes :

- LABEL : le label actuel (20 bits) ;
- CoS : champ expérimental (3 bits) : utilisé pour définir une classe de service ;
- STACK : indicateur du bas de la pile (1 bit) : MPLS permet l'insertion de plusieurs labels, ce bit détermine si le label est le dernier dans le paquet ou non ;
- TTL (8 bits) : similaire au TTL de l'entête IP.

2. Pile de label MPLS :

Comme c'est décrit précédemment, MPLS supporte plusieurs labels dans un seul paquet, les applications suivantes l'exigent :

- MPLS VPN : MP-BGP (MultiProtocol Border Gateway Protocol) est utilisé pour propagé un label secondaire en addition à celui propagé par TDP ou LDP ;
- MPLS TE : MPLS TE utilise RSVP (Ressource Reservation Protocol) pour établir un tunnel LSP (Label Switched Path). RSVP propage aussi un label en addition de celui propagé par TDP ou LDP.

Le champ STACK permet d'identifier le classement du label dans la pile, s'il est égal à 1 alors il s'agit du dernier label avant l'entête IP.

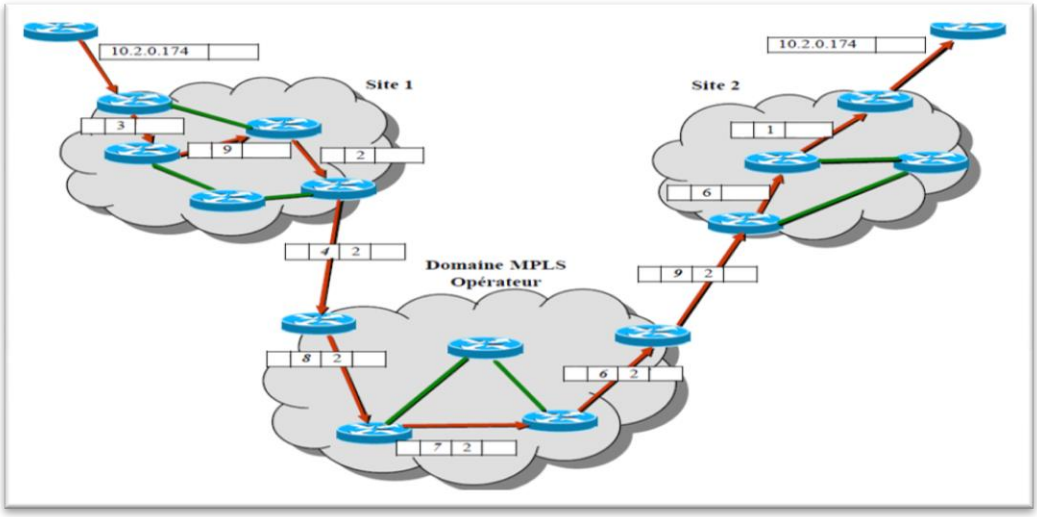

Figure 3. 3 Pile de Label à travers l'architecture MPLS

3. FEC (Forwarding Equivalency Class) :

Une classe d'équivalence de transmission (FEC) représente un groupe de paquets transmis de manière identique sur un réseau MPLS. Ces FEC peuvent par exemple correspondre à des types de services, des types de paquets ou même encore des sous réseaux.

Un label différent est attribué à chacun de ces FEC. Ainsi, dès son entrée dans un réseau MPLS, chaque paquet appartenant à un même groupe reçoit le même label, ce qui lui permet d'être acheminé vers la route qui lui a été réservée.

4. LSP (label switched path) :

C'est une séquence de LSR par la quelle les paquets labellisés appartenant à un FEC particulier seront acheminé. MPLS propose les deux solutions suivantes pour implémenter un LSP :

- Routage saut par saut : chaque LSP choisit indépendamment le saut suivant pour un FEC donné. Cette méthodologie est similaire à celle utilisée dans les réseaux IP courants,
- routage explicite : Le premier LSR détermine la liste des nœuds à suivre. Le chemin spécifié peut être non optimal. Le long de ce chemin, les ressources peuvent être réservées pour assurer la QoS voulue au trafic.

Un LSP est unidirectionnel et le trafic de retour doit donc prendre un autre LSP. Un IGP (*Interior Gateway Protocol*) est utilisé pour remplir les tables de routage dans un domaine MPLS. LDP ou TDP sont utilisés pour propager les labels pour ces réseaux et construire les LSP.

5. Terminologie :

- ***Label switching router (LSR)*** *:* il permet de commuter les paquets en se basant sur les labels.

  Toutes les interfaces d'un LSR doivent supporter MPLS. Les LSR exécutent les fonctions d'échange d'informations de routage de couche 3, l'échange des labels et la commutation des paquets ou des cellules.

- ***Edge LSR (LER) :*** c'est le premier dispositif qui affecte les labels ou les élimine, il se place à la frontière du Backbone. Il existe deux types de LER : in*gress LER* responsable de l'affectation des labels aux paquets et e*gress LER* responsable de l'élimination des labels, ce premier consulte donc seulement la table de routage IP classique pour acheminer le paquet à sa destination.

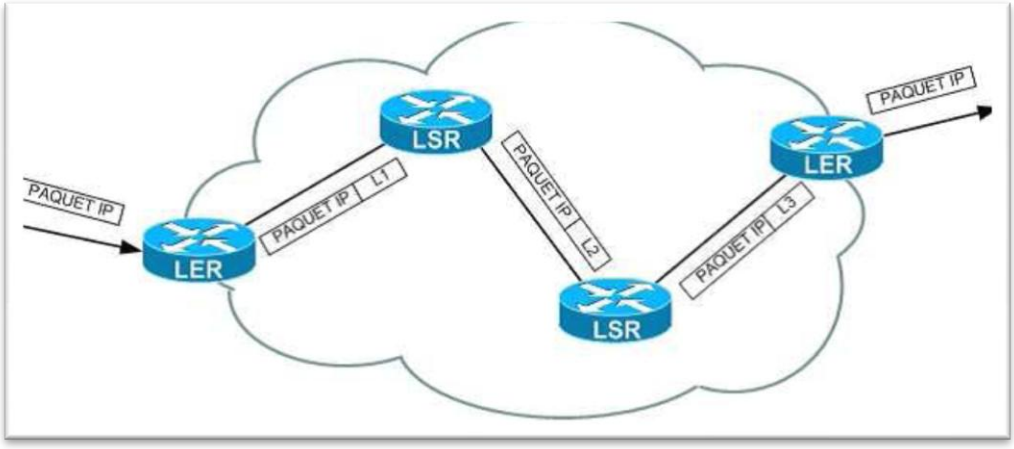

Figure 3. 4 Différents types de routeurs dans un domaine MPLS

6. Les structures de données des labels :

- ***LIB (Label Information Base)*** *:* se trouve au niveau de plan de contrôle, c'est la base de données utilisée par LDP. Elle contient pour chaque sous réseau IP la liste des labels affectés par les LSR voisins.
- ***LFIB (Label Forwarding Information Base)*** *:* À partir de la table LIB et de la table de routage IP, le routeur construit une table LFIB, qui sera utilisée pour commuter les paquets. Chaque réseau IP est appris par l'IGP, qui détermine le prochain saut ("nexthop") pour atteindre ce réseau. Le LSR choisit ainsi l'entrée de la table LIB qui correspond au réseau IP et sélectionne comme label de sortie le label annoncé par le voisin déterminé par l'IGP (plus court chemin).
- ***FIB (Forwarding Information Base) :*** *appartient au plan de données, c'est la base de donnée utilisée pour* acheminer les paquets non labellisés (routage IP classique). Un paquet à acheminer est labellisé si le label du saut suivant est valable pour le réseau de destination IP.

V. Fonctionnement de MPLS :

Les fonctionnalités de routage IP avec MPLS peuvent être divisées en 3 fonctions :

- *Échange d'information de routage en utilisant les protocoles de routage classique (OSPF, IS-IS, EIGRP) ;*
- *Génération de label local. Un unique label local est assigné par un routeur à chaque destination trouvée dans la table de routage global et enregistré dans la table LIB (label information base). Ce label n'a qu'une signification locale ;*
- *Propagation des labels locaux aux adjacents routeurs, qui vont être utilisé comme label du saut suivant* (enregistrement dans la table LFIB).

1. Distribution des labels (TDP / LDP) :

Les LSR se basent sur l'information de label pour commuter les paquets à travers un domaine MPLS. Chaque routeur, lorsqu'il reçoit un paquet taggué, utilise le label pour déterminer l'interface de sortie et le remplace par un autre correspondant au routeur du saut suivant. Il est donc nécessaire de propager les informations sur ces labels à tous les LSR. Pour cela, des protocoles de distributions de labels sont utilisés. Suivant le type des FEC, différents protocoles sont employés pour l'échange de labels entre LSR :

- TDP/LDP (*Tag/Label Distribution Protocol*): Mappage des adresses IP unicast ;
- RSVP (*Ressource Reservation Protocol*): utilisé en Trafic Engineering pour établir des LSP en fonction de critères de ressources et d'utilisation des liens ;
- MP-BGP (*MultiProtocol Border Gateway Protocol*) pour l'échange de routes VPN.

Il existe deux méthodes pour propager les labels entre LSR: *Upstream* et *Downstream*. Le schéma suivant explicite la notion d'*Upstream* voisin et de *Downstream* voisin par rapport à un réseau IP donné :

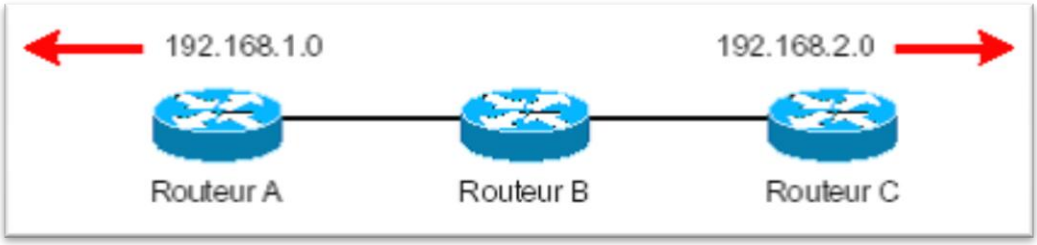

Figure 3. 5 Notion d'Upstream voisin et de Downstream voisin

Sur le schéma ci-dessus, le routeur A est un *Upstream* voisin par rapport au routeur B pour le réseau 192.168.2.0. Le routeur A est aussi *Downstream* voisin par rapport au routeur B pour le réseau 192.168.1.0. Une méthode de distribution des labels dite « *Downstream* » indique que la propagation des réseaux se fait du routeur le plus proche au routeur le plus éloigné (*Downstream* vers *Upstream*).

La méthode *Downstream*, avec deux variantes: *Unsollicited Downstream* et *Downstream on Demand*. Dans la première variante, les LSR *downstream* propagent systématiquement tous leurs labels à leurs voisins. Dans la deuxième, les LSR *upstream* demandent explicitement aux LSR *downstream* de leur fournir un label pour le sous réseau IP demandé. Le mode non sollicité est utilisé dans le cas d'interfaces en mode trame, le *Downstream on Demand* étant utilisé par les LSR ATM (mode cellule).

- ***Unsolicited Downstream :***

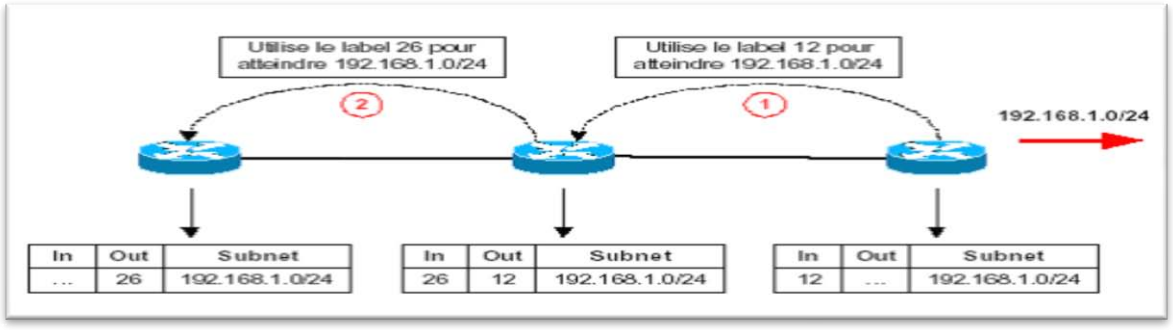

Figure 3. 6 Distribution de label avec Unsollicited Downstream

- **Downstream on demand :**

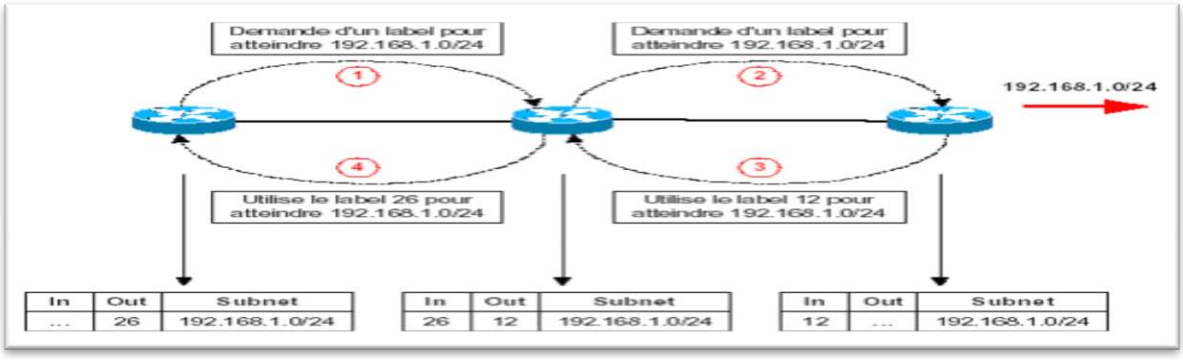

Figure 3. 7 Distribution de label avec Downstream on demand

2. PHP (Penultimate Hop Popping) :

Un "*egress*" LSR annonçant un réseau, qui lui est soit directement connecté, soit rattaché (appris par IGP, EGP, routage statique…) par une interface non tagguée, n'a pas besoin de recevoir de paquets taggués pour atteindre ce réseau. En effet, si les paquets reçus étaient taggués, le routeur *egress* devrait d'abord déterminer l'interface de sortie grâce à la table LFIB, puis effectuer une recherche dans la table de routage IP. L'opération de recherche sur le label dans la LFIB est inutile, car dans tous les cas le routeur devra effectuer une recherche dans la table de routage. Le routeur *egress* annonce donc ces réseaux IP avec le label "*implicit-null*" à ses voisins. Un LSR ayant comme label de sortie "*implicit-null*" aura ainsi pour but de dépiler le premier label du paquet et de faire suivre le paquet sur l'interface de sortie spécifiée. Le routeur *egress* n'aura alors plus qu'une recherche à faire dans sa table de routage.

3. Détection de boucle :

La technologie MPLS prévoit un mécanisme de détection de boucle utilisant le champ TTL du label. A l'entrée d'un domaine MPLS, l'*ingress* LER décrémente la valeur du champ TTL de l'entête IP puis copie cette valeur dans le champ TTL du label. Tous les autres LSR décrémentent seulement le TTL contenu dans le label. L'entête IP reste inchangé jusqu'à ce que le dernier label est éliminé alors la valeur restante du TTL associée au label MPLS est copiée en retour dans le champ correspondant de l'entête IP.

4. Rétention des labels :

Afin d'accélérer la convergence du réseau lors d'un changement de topologie (lien défectueux, dysfonctionnement d'un routeur), les LSR conservent dans leur table LIB la liste des labels annoncés pour chaque réseau IP par leurs voisins TDP, y compris de ceux n'étant pas les sauts suivants choisis par l'IGP. Ainsi, en cas de perte d'un lien ou d'un noeud, la sélection d'un nouveau label de sortie est immédiate : en effet, il suffit au routeur d'élire un nouveau saut et de sélectionner l'entrée correspondante dans la LIB, puis de mettre à jour la LFIB. Ce mode de fonctionnement est appelé mode libéral (liberal mode).

L'avantage de ce procédé est naturellement une convergence plus rapide lorsque les informations de routage au niveau 3 changent, avec pour inconvénients que davantage de mémoire est allouée dans les routeurs et que des labels supplémentaires sont utilisés.

VI. Les atouts de MPLS

1. MPLS trafic engineering :

La plupart des gros réseaux IP, en particulier ceux des opérateurs, disposent de liens de secours en cas de panne. Toutefois, il est assez difficile d'obtenir une répartition du trafic sur ces liens qui ne sont traditionnellement pas utilisés, car n'étant pas sélectionnés comme chemins optimaux par l'IGP. Le Trafic Engineering permet un meilleur emploi des liaisons, puisqu'il permet aux administrateurs réseau d'établir des tunnels LSP à travers le Backbone MPLS, indépendamment de l'IGP. Le protocole de routage interne (IGP) doit être un protocole à état de liens (*Link-State*). En effet, pour déterminer le chemin à emprunter par un tunnel, les routeurs doivent avoir la connaissance complète de la topologie du réseau. Les seuls protocoles supportant le TE sont donc OSPF et ISIS [5].

Les tunnels MPLS (appelés également *Trunks*) peuvent être créés en indiquant la liste des routeurs à emprunter (méthode explicite) ou bien en utilisant la notion d'affinité (méthode dynamique). La notion d'affinité est simplement une valeur sur 32 bits spécifiée sur les interfaces des routeurs MPLS. La sélection du chemin s'effectue alors en indiquant (sur le routeur initiant le tunnel) une affinité et un masque.

Pour permettre une gestion plus souple du trafic, chaque interface MPLS susceptible d'être un point de transit pour des tunnels MPLS dispose d'une notion de priorité, définie sur 8 niveaux. Lors de l'établissement d'un nouveau tunnel, si celui-ci a une priorité plus grande que les autres tunnels et que la bande passante totale utilisable pour le TE est insuffisante, alors un tunnel moins prioritaire sera fermé. Ce mode de fonctionnement est appelé préemption.

2. MPLS VPN

Pour satisfaire les besoins des opérateurs de services VPN, la gestion de VPN-IP à l'aide des protocoles MPLS a été définie dans une spécification référencée RFC 2547. Des tunnels sont créés entre des routeurs MPLS de périphérie appartenant à l'opérateur et dédiés à des groupes fermés d'usagers particuliers, qui constituent des VPN. Dans l'optique MPLS VPN, un VPN est un ensemble de sites placés sous la même autorité administrative, ou groupés suivant un intérêt particulier.

Dans l'intention de garantir un tel service pour sa clientèle, un ISP ou un operateur doit alors à l'essor pour répondre à deux problématiques fondamentales :

- Garantir la confidentialité de données acheminées
- Prendre en charge et tolérer le plan d'adressage privé, souvent identiques

Du reste, un réseau VPN est initialement reposé sur les fonctionnalisées suivantes :

- Systèmes Firewall afin de prémunir les sites client et offrir une interface sécurisée face à Internet.
- Un Système d'authentification pour contrôler la validité et l'authenticité des sites distant avec lesquels il y'aura échange d'information

- Un Système de cryptage pour contrarier l'écoute, l'analyse ou l'utilisation des données lors de leur acheminement sur Internet.
- Tunneling pour détecter tout intrus, et garantir un service de transport multi-protocole ainsi qu'un plan d'adressage privé.

MPLS est considéré dans l'affaire de tunneling comme leader, dans la mesure où le transfert des paquets n'est pas conçu sur l'adresse de destination du paquet IP, mais sur le label qui lui est déjà affecté. De ce fait, un Fournisseur de Service Internet (FSI ou ISP en anglais) peut déployer un VPN, en mettant en œuvre un groupe de LSP pour assurer la connectivité entre l'ensemble des sites du VPN d'un client donné. Chaque site du VPN signale à l'FSI l'ensemble des préfixes (c.à.d. adresses) disponible sur le site local. Par conséquent, Le système de routage de l'FSI révèle cette information aux autres sites distants de ce même VPN, via le protocole de distribution de labels. En fait, l'utilisation d'identifiant de VPN permet à un même système de routage de prendre en charge multiples VPN simultanément, avec un espace d'adressage éventuellement identique. Ainsi, chaque LER attribua le trafic en provenance d'un site à un LSP spécifique établi sur une association de l'adresse de destination du paquet et l'appartenance à un VPN donné [6].

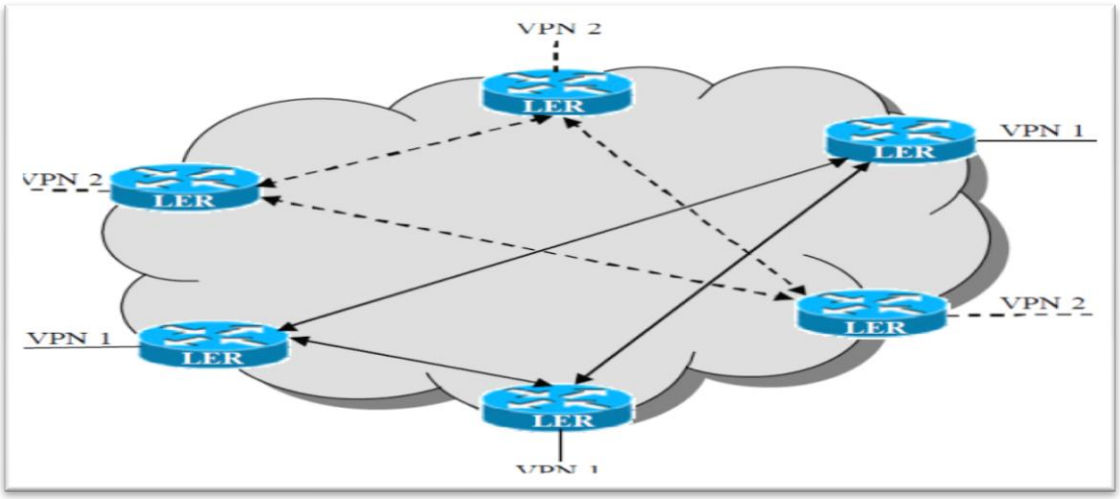

Figure 3.8 : MPLS VPN

Par ailleurs, pour pouvoir mettre en place des VPNs clients, (pour le cas de ce projet Les clients sont les différents réseaux d'accès), il est exigible d'isoler les flux de chaque clients. Dans ces conditions, le label MPLS est constitué de deux champs de labels: le premier a pour rôle d'identifier le chemin à suivre jusqu'a le LSR destination (Egress-LER) et qui continue à changer à chaque saut, le second désigne l'identifient du VPN (VPN-ID) assigné au VPN et qui demeure intouchable entre le LSR source et le LSR destination.

En effet, c'est le LER source qui prend en charge l'attribution des ces deux labels aux paquets lorsque un VPN est utilisé :

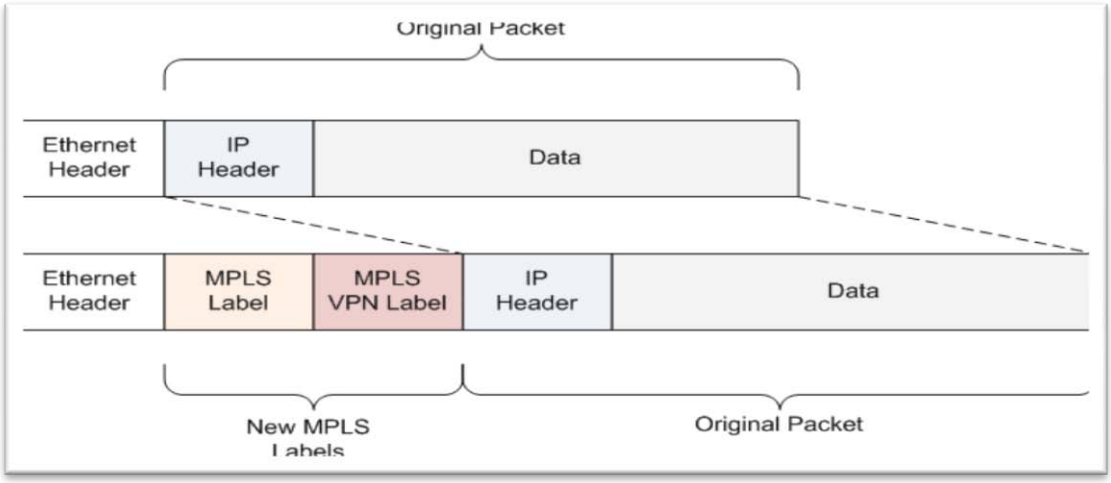

Figure 3.9 : Les entêtes additionnels au paquet IP

Du même, la gestion des VPNs au niveau du Backbone est assurée par l'opérateur à l'aide du biais des Ingress-LER. Chaque I-LER alloue, de manière statique, une table VRF (Virtual Routing and Forwording Table) à chacune de ses interfaces utilisateur. Un VRF est une table de routage assigné à un VPN spécifique qui fournit les routes vers les réseaux appartenant à ce VPN.

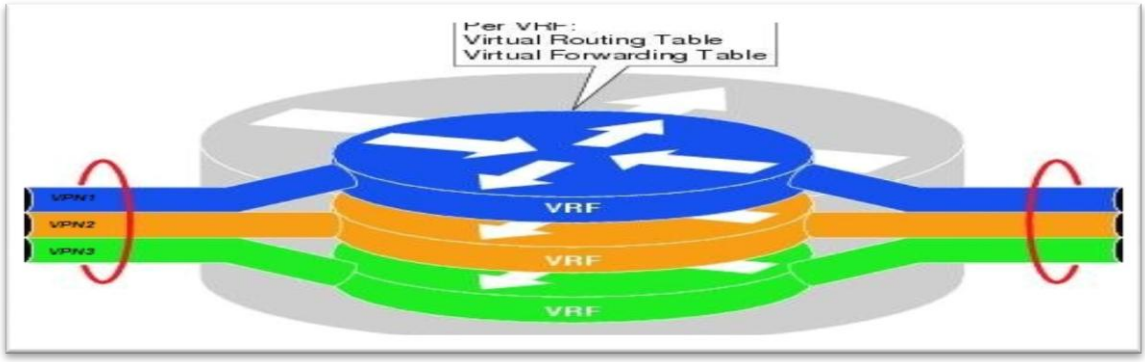

Figure 3.10 : Routeur Virtuel/ VRF

Chaque VRF est averti localement par le CE (Customer Edge router "les routeurs WAN des clients") rattaché à l'interface de la VRF.

Pour révéler les réseaux IP avec lesquels il communique, Le LER utilise, pour moins de 5 réseaux IP, du routage statique, et pour plus de 6 réseaux IP, eBGP(Border Gateway Protocol) qui est un protocole de routage dynamique .Ceci dans l'intension de ne pas avoir à traiter un grand nombre de routes.

Le I-LER attribut un label local pour tout ces réseaux IP et les stockes à la suite dans sa table de commutation [8].

En dernier lieu, il proclame l'appartenance au VPN de ces réseaux aussi que leur label local et leur LER de raccordement à l'ensemble des LER de la Backbone (Ce label est l'identifient du VPN auquel appartient un réseau IP).Pour cela, il envoi les informations pertinentes à l'ensemble des LER via le ***M**ulti **P**rotocol-**B**order **G**ateway **P**rotocol* (MP-BGP). Seuls les LER en contacte avec les CE appartenant au même VPN captureront ces informations qui seront a la suite inscrit dans la VRF associé au VPN en question et afin de mette à jour

la table de commutation. Les LER appartenant au même VPN, connaissent ainsi tous les réseaux IP membres du VPN par le biais de la VRF, ainsi que leur label local et leur PE de rattachement.

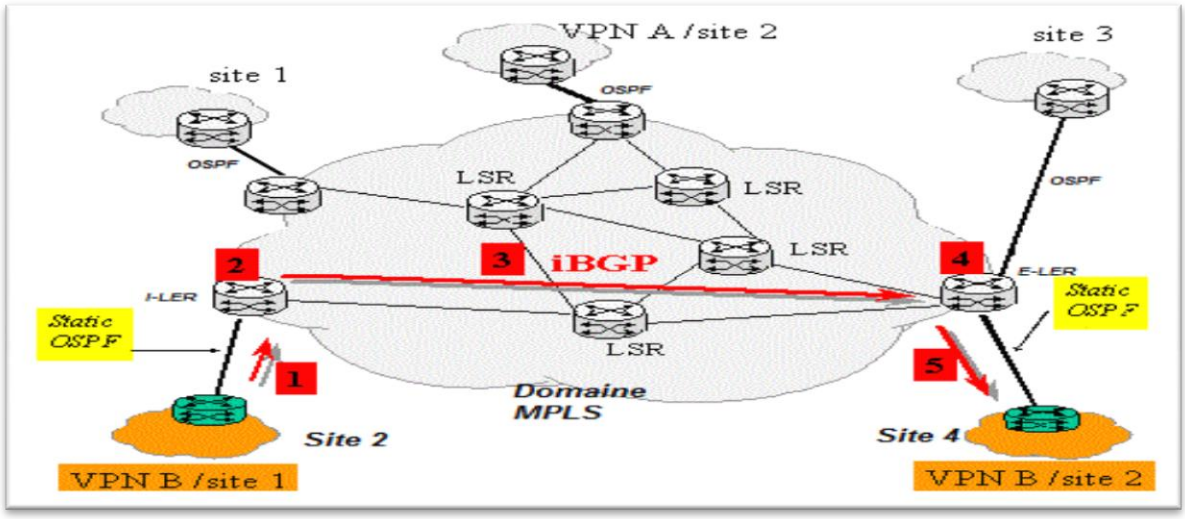

Figure 3.11 : acheminement des paquets via MPLS

3. MPLS QOS :

MPLS permet d'offrir plusieurs mécanismes de qualité de service à savoir : la classification du trafic, le marquage de différentes classes suivant des priorités et la gestion de la congestion. Pour garder la classe de service déjà définie dans un paquet entrant dans un domaine MPLS que ce soit au niveau du champ IP précédence ou DSCP du modèle Diffserv, la valeur de leurs trois bits du poids plus fort est copiée au niveau du champ EXP du label MPLS.

VII. Structure du Backbone TT:

L'un des principaux vecteurs de la communication unifié (voix, vidéo, et données), est de bien choisir la topologie à mettre en œuvre. Cette topologie doit être standardisée et respecte les normes universelles pour qu'elle soit évidente et sollicite tous les besoins, d'ou une architecture bien organisé et qui répond à toutes les exigences au sein de Tunisie Télécom.

Dans le chapitre suivant nous allons, configurer les routeurs de la Backbone, et ceux qu'ils la relient avec les différents réseaux d'accès de TT.A cet égard, et Afin d'évaluer l'apport de la technologie MPLS sur le Backbone de Tunisie Télécom. Et avant de franchir le pas il faut évoquer la structure de la Backbone TT sur l'échelle nationale.

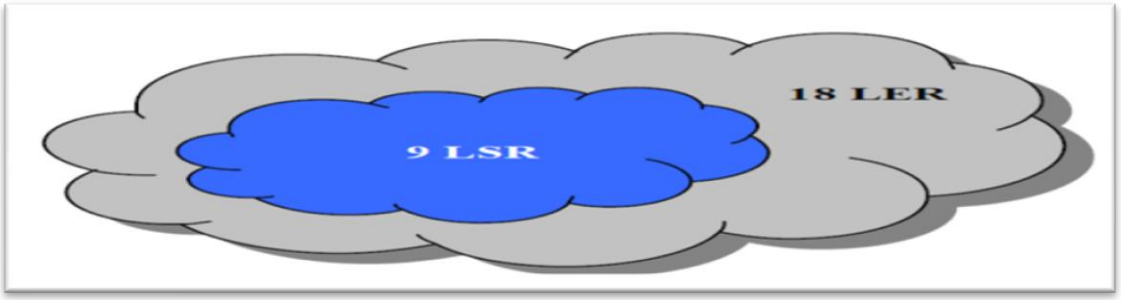

Figure 3.12 : La structure du Backbone de Tunisie Télécom

Le Backbone est constitué de 9 LSR et 18 LER :

- LSR se situant dans la Capitale et plus précisément à Kasbah, Belvédère, Hached, Ouardia.
- LSR situés dans les villes: Sfax, Sousse,, Kairouan, Béja, Gabes.
- 9 LER au voisinage des LSR
- 9 LER situés au Marsa, Ariana, Menzah, Ben Arous, Bardo, Bizerte, Nabeul, Moknine et Gafsa

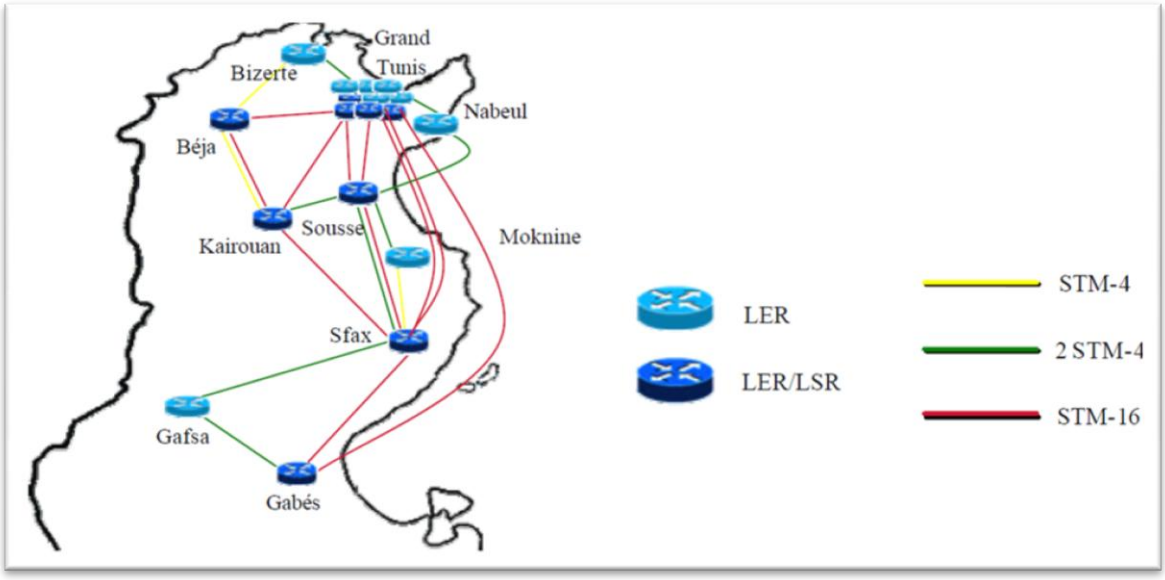

Figure 3.11 : La disposition géographique du Backbone de Tunisie Télécom

Dans cette figure, chaque LSR est co-localisé avec un LER. Pour la simplicité de la représentation, on schématisera chaque couple LSR/LER co-localisé par un seul routeur. Pour mieux appréhender cette topologie, on va plutôt considérer la disposition suivante :

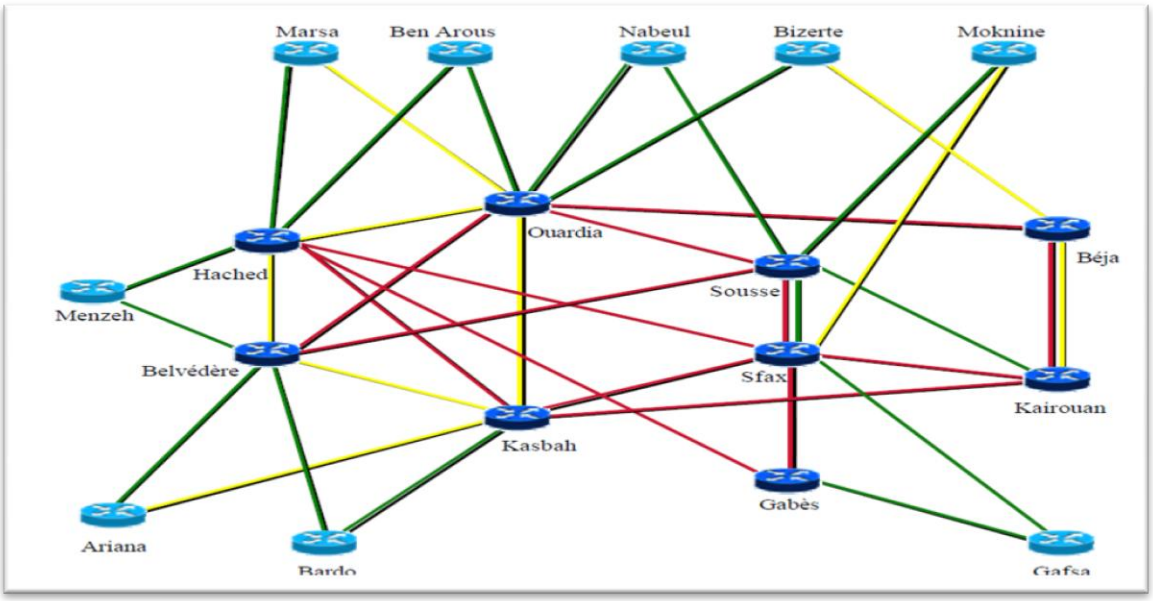

Figure 3.14 : Schéma représentatif du Backbone Tunisie Télécom

VIII. Conclusion

Le protocole MPLS semble intéressant pour l'avenir en tant que technique fédératrice, et de nombreux travaux sont menés pour éclairer les choix à faire. Bien que l'ensemble des spécifications nécessaires à l'interopérabilité de cette solution ne soient pas encore disponibles et que même des divergences fortes subsistent quant au mode de réalisation de certaines fonctions, MPLS est au cœur de la stratégie cible de la plupart des opérateurs aujourd'hui.

Grâce à ses mécanismes de commutation de labels avancés ainsi que par sa simplicité de mise en place sur des réseaux déjà existants, le MPLS est devenu une technologie phare de demain alliant souplesse, évolutivité et performance pour un coût réduit.

MPLS jouera un rôle important dans le routage, la commutation et le passage des paquets à travers les réseaux de nouvelles générations pour permettre la rencontre entre les besoins de service et les utilisateurs du réseau grâce à ses principaux avantages :

- Calcul unique au niveau de l'entrée du réseau,
- Rapidité dans le cœur de réseau,
- L'intelligence se trouve aux extrémités du réseau.

De plus, puisque cette nouvelle technologie permet d'implémenter facilement des technologies comme le QoS, les VPN et la VoIP, la majorité des fournisseurs d'accès à Internet ont décidé de faire évoluer progressivement l'ensemble de leurs réseaux vers des réseaux MPLS.

Dans le chapitre suivant, on se concentre à la simulation et la configuration d'une solution MPLS au sein de la Backbone Tunisie Télécom tout en mettant l'accent sur les concepts relatifs à cette technique en fonction des protocoles de routage internes et externes.

Chapitre IV : Implémentation d'une solution MPLS au sein du Backbone TT

I. Introduction :

L'application à configurer sera un outil pour migrer vers une solution MPLS/IP au sein de la Backbone TT. Tout au long de ce chapitre nous allons suivre ces étapes.

- l'implémentation de la nouvelle architecture sur le logiciel dédié.
- Configuration de Backbone MPLS/IP
- Configuration basique des routeurs de Backbone (LSR "P", LER "PE") : les interfaces et le mécanisme d'authentification
- Configuration de routage Dynamique via OSPF et BGP
- Configuration MPLS
- Configuration VPN : création et Configuration des VRF-Réseaux coté PE

II. Choix des outils de simulation :

Il existe actuellement une grande panoplie de logiciels de simulation réseau, quoiqu'une minorité prenne en charge la mise en œuvre d'une architecture MPLS, c'est pourquoi notre choix s'est reposé essentiellement sur GNS3.

En effet GNS3 est un simulateur d'équipements Cisco. Cet outil permet donc de charger de véritable IOS Cisco et de les utiliser en simulation complète sur un simple ordinateur. Néanmoins, afin de permettre des simulations plus ou moins complètes il est fortement lié aux logiciels suivants :

- **Dynamips** : C'est un logiciel servant à l'émulation d'une machine virtuelle des plateformes C7200 ou C3600. Il est supporté sous Linux et ses dérivés ou sous Windows XP/7. Pour qu'une machine virtuelle fonctionne, nous devons avoir un IOS valide téléchargeable par un compte Cisco CCO donc il est loin d'être gratuit.
- **Dynagen :** C'est une interface supplémentaire écrite en langage Python qui manipule l'interconnexion et la gestion d'un ensemble de machines virtuelles. Malgré qu'il soit possible de reconcevoir un environnement complet de laboratoire avec Dynamips, Dynagen autorise l'amélioration aisée d'une topologie.
- Ainsi, Dynamips / GNS3 / Dynagen sont des logiciels libres qui donnent la possibilité d'émuler des machines virtuelles Cisco. Contrairement aux simulateurs commerciaux tell que (Vizualiser Boson, Network, etc.) ou gratuits tel que le fameux (Packet Tracer) qui conçoivent le comportement des IOS et des machines, Dynamips / GNS3 / Dynagen aillent recours à un véritable IOS complètement fonctionnel. Ils simulent uniquement le Hardware. Quoique les performances d'un environnement de production ne puissent pas être parfaitement atteintes, il s'agit d'une alternative crédible à l'acquisition d'un laboratoire de test coûteux. Le résultat

obtenu s'approche de solutions d'émulation de PC telles que VMWare ou Xen. Avec GNS3, le projet devient extrêmement facile d'utilisation.

III. Configuration et simulation de la nouvelle architecture du Backbone :

1. Présentation de la topologie proposée :

Les configurations pour la topologie proposée sont principalement conçu pour les routeurs qui relient la coté Backbone de Tunisie Telecom avec les différents réseaux (GSM, RTCP, ADSL, DATA, Business client,…) comme indique la figure ci-dessous.

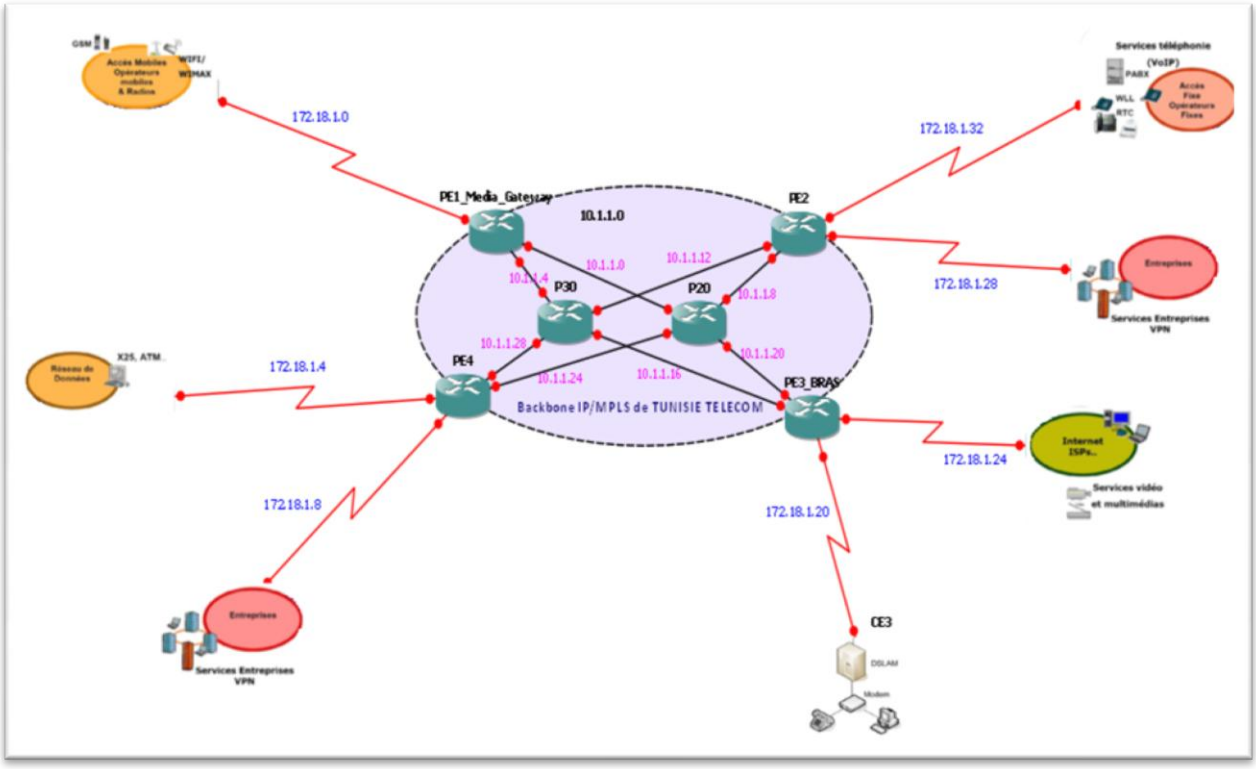

Figure 4.1: La nouvelle architecture du Backbone TT

2. Plan d'adressage :

En effet, le plan d'adressage est initialement établi a base du codage cidre, appelé notamment codage VLSM, notons que Tunisie Telecom possède au préalable une adresse privé 10.0.0.0/8, ainsi les inter-réseaux dans le Backbone aurons des adresses qui dérivent de celle-ci :

- ***Le réseau 10.1.1.0/30 entre les routeurs PE1 et P20.***
- ***Le réseau 10.1.1.4/30 entre les routeurs PE1 et P30.***
- ***Le réseau 10.1.1.8/30 entre les routeurs PE2 et P20.***
- ***Le réseau 10.1.1.12/30 entre les routeurs PE2 et P30.***
- ***Le réseau 10.1.1.16/30 entre les routeurs PE3 et P30.***
- ***Le réseau 10.1.1.20/30 entre les routeurs PE3 et P20.***
- ***Le réseau 10.1.1.24/30 entre les routeurs PE4 et P20.***
- ***Le réseau 10.1.1.28/30 entre les routeurs PE4 et P30.***

En ce qui concerne les WAN (entre les PE et CE), l'adresse 172.18.1.0/24 lui sera attribuée, ce qui donne lieu à cette distribution :

- *le réseau 172.18.1.0/30 entre le PE1 et CE1*
- *le réseau 172.18.1.4/30 entre le PE4 et CE2.*
- *le réseau 172.18.1.8/30 entre le PE4 et CE3.*
- *le réseau 172.18.1.20/30 entre le PE3 et CE4.*
- *le réseau 172.18.1.24/30 entre le PE3 et CE5.*
- *le réseau 172.18.1.28/30 entre le PE2 et CE6.*
- *le réseau 172.18.1.32/30 entre le PE2 et CE7.*

Le tableau ci-dessous sert comme un récapitulatifs de ce qui précède :

Routeurs	Interfaces	Adresse	Masque de sous-réseau
PE1	F0/0	10.1.1.1	255.255.255.252
	F0/1	10.1.1.4	255.255.255.252
	S0/0	172.18.1.2	255.255.252.252
PE2	F0/0	10.1.1.13	255.255.255.252
	F0/1	10.1.1.9	255.255.255.252
	S0/0	172.18.1.34	255.255.255.252
	S0/1	172.18.1.30	255.255.255.252
PE3	F0/0	10.1.1.17	255.255.255.252
	F0/1	10.1.1.21	255.255.255.252
	S0/0	172.18.1.26	255.255.255.252
	S0/1	172.18.1.22	255.255.255.252
PE4	F0/0	10.1.1.25	255.255.255.252
	F0/1	10.1.1.29	255.255.255.252
	S0/0	172.18.1.6	255.255.255.252
	S0/1	172.18.1.10	255.255.255.252
P20	F0/0	10.1.1.2	255.255.255.252
	F0/1	10.1.1.10	255.255.255.252
	F1/0	10.1.1.26	255.255.255.252
	F2/0	10.1.1.22	255.255.255.252
P30	F0/0	10.1.1.6	255.255.255.252
	F0/1	10.1.1.14	255.255.255.252
	F1/0	10.1.1.30	255.255.255.252
	F2/0	10.1.1.18	255.255.255.252

3. *Configuration basique des routeurs du Backbone*

Cette configuration consiste essentiellement à activer les interfaces des routeurs ainsi à l'attribution des noms a chacun d'eux dans cette partie nous allons citer juste la configuration pour PE1 :

- ***Configuration du nom de routeur***

```
Router>enable
Router#conf t
Router(config)#hostname PE1
PE1(config)#exit
```

- ***Configuration des interfaces de routeur PE1***

```
PE1(config)#interface Loopback0
 PE1(config-if) #ip address 172.16.1.1 255.255.255.0
PE1(config-if)  # no shutdown
PE1(config-if)  #interface FastEthernet0/0
PE1(config-if) # ip address 10.1.1.1 255.255.255.252
PE1(config-if)  #no shutdown
PE1(config-if) #full-duplex
PE1(config-if) #interface Serial0/0
PE1(config-if)  #ip address 172.18.1.2 255.255.255.252
PE1(config-if) # no shutdown
PE1(config-if)  #encapsulation ppp
PE1(config-if)  #clockrate 64000
PE1(config-if) #interface FastEthernet0/1
PE1(config-if)  #ip address 10.1.1.5 255.255.255.252
PE1(config-if)  #no shutdown
PE1(config-if) #full-duplex
PE1(config-if) #exit
PE1(config) #exit
PE1 #write
```

- ***Configuration de mot de passe pour les connexions console et Pour les connexions vty***

```
PE1(config)# line console 0
PE1(config-line)#password cisco
PE1(config-line)#login
PE1(config-line)#line vty 0 4
PE1(config-line)#password cisco
PE1(config-line)#login
PE1(config-line)#exit
PE1(config)#enable secret cisco
PE1(config) #exit
PE1#write
```

4. *Configuration : Routage dynamique.*

En effet, Les protocoles de routage sont classés en deux familles, les IGP et les EGP.

- **Les IGP** assurent le routage interne à un système autonome. Ils émettent usuellement leurs mises à jour à travers des paquets IP en mode diffusion. L'adresse de destination des paquets est de type broadcast (255.255.255.255) ou de type multicast (224.0.0.6 et 224.0.0.5 comme notre exemple le protocole OSPF.
- **Les EGP** assurent le routage entre des systèmes autonomes. Ils émettent des mises à jour à des voisins identifiés en établissant une connexion (couramment TCP) avec eux. Les mises à jour ne sont pas diffusées vers tous les routeurs mais routeur à routeur. Les informations véhiculés sont examinées et peuvent contenir des attributs de routage complexes dépendant du protocole en question. Pour notre application nous avons choisi le protocole de routage interne le OSPF et le protocole de routage externe le BGP.

- ***Configuration et vérification de protocole OSPF***

La configuration de protocole OSPF de notre application pour le routeur PE1 est comme suit :

```
PE1(config)#router ospf 1
PE1(config-router)# router-id 1.1.1.1
PE1(config-router)#network 10.1.1.0 0.0.0.3 area 0
PE1(config-router)# network 10.1.1.4 0.0.0.3 area 0
PE1(config-router)# network 172.16.1.0 0.0.0.255 area 0
PE1(config-router)#^z
PE1#wr
```

La table de routage OSPF est ci-dessous :

```
PE1#sh ip route ospf
      172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O     172.16.30.1/32 [110/11] via 10.1.1.6, 00:08:41, FastEthernet0/1
O     172.16.20.1/32 [110/11] via 10.1.1.2, 00:08:41, FastEthernet0/0
O     172.16.2.1/32 [110/21] via 10.1.1.6, 00:08:31, FastEthernet0/1
                     [110/21] via 10.1.1.2, 00:08:31, FastEthernet0/0
                     10.0.0.0/30 is subnetted, 4 subnets
O     10.1.1.8 [110/20] via 10.1.1.2, 00:08:42, FastEthernet0/0
O     10.1.1.12 [110/20] via 10.1.1.6, 00:08:42, FastEthernet0/1
```

Après la configuration et pour tester le bon fonctionnement du protocole OSPF on exécute la commande s**how ip route OSPF** qui nous montre la table de routage de routeur PE1 : La lettre "O" représente les liens connectés par le protocole OSPF : tels que les adresses 172.16.30.1 et 172.16.20.1 s'agissant des adresses loopback des routeurs voisins P20 et P30 qui sont connectées directement avec des connexions FastEthernet, tant que l'adresse 172.16.2.1 représente l'adresse du routeur PE2 qui se sert d'OSPF passant

par l'interface Fastethernet 10.1.1.6 du routeur P30 ou bien par l'interface FastEthernet 10.1.1.2 du routeur P20.

- ***Configuration* et vérification de protocole BGP**

Pour s'assurer de la communication externe des routeurs de notre application nous allons configurer dans une deuxième étape le protocole de routage externe : le protocole BGP en appliquant les commandes suivantes :

```
PE1(config)#router bgp 100
PE1(config-)# no synchronization
PE1(config-)# bgp log-neighbor-changes
PE1(config-)# network 172.16.1.0 mask 255.255.255.0
PE1(config-)# neighbor 172.16.20.1 remote-as 100
PE1(config-)# neighbor 172.16.20.1 update-source Loopback0
PE1(config-)# neighbor 172.16.30.1 remote-as 100
PE1(config-)# neighbor 172.16.30.1 update-source Loopback0
PE1(config-)#exit
```

- **Le *résultat de* test pour le routeur PE1 et P20 :**

Pour visualiser le résultat du test de protocole BGP nous avons utilisée trois commandes la première c'est **show ip bgp summary** qui nous dévoile toutes les informations relative à ce protocole tels que l'adresse loopback du routeur, le numéro de système autonome, la version du table de routage , le nombre des liens et des routes, et affecte pour chacun d'eux une espace mémoire prédéfinie En outre, cette commande nous indique les adresses des routeurs voisins dans l'architecture .

- ***Le résultat de configuration sur le routeur PE1***

```
PE1#show ip bgp summary
BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 5, main routing table version 5
4 network entries using 480 bytes of memory
5 path entries using 260 bytes of memory
7/2 BGP path/bestpath attribute entries using 868 bytes of memory
2 BGP rrinfo entries using 48 bytes of memory
2 BGP extended community entries using 80 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1768 total bytes of memory
BGP activity 13/0 prefixes, 21/1 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.20.1     4   100      27      24        5    0    0 00:15:06        2
172.16.30.1     4   100      27      24        5    0    0 00:15:15        2
PE1#
```

Les adresses de réseau affichées dans la table de routage de protocole BGP telle que 172.16.20.1 et 172.16.30.1 représentent les routeurs voisins qui sont en relation directe avec PE1.

- ***Le résultat de configuration sur le routeur P20***

```
P20#show ip bgp summary
BGP router identifier 172.16.20.1, local AS number 100
BGP table version is 4, main routing table version 4
3 network entries using 360 bytes of memory
3 path entries using 156 bytes of memory
7/2 BGP path/bestpath attribute entries using 868 bytes of memory
2 BGP extended community entries using 80 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1496 total bytes of memory
BGP activity 12/0 prefixes, 13/1 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.1      4   100      27      30        4    0    0 00:20:50        1
172.16.2.1      4   100      26      30        4    0    0 00:20:52        1
P20#
```

La deuxième étape de vérification associée au protocole BGP consiste à exécuter la commande **show ip BGP**, cette commande permet de tester les tables de routages BGP en montrant en premier lieu l'identificateur du routeur locale et la version de la table de routage ,en second lieu elle nous indique l'adresse de réseau, le saut suivant, le nombre de saut, le type de lien et le numéro de système autonome .toutes ces références sont reformulé dans une table de routage. Voir ci-dessous.

- ***Résultat de configuration sur le routeur PE1***

```
PE1#show ip bgp
BGP table version is 5, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? – incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
* i 172.16.2.0/24    172.16.2.1               0    100      0 i
*>i                  172.16.3.1               0    100      0 i
*>i 172.16.20.0/24   172.16.20.1              0    100      0 i
*>i 172.16.30.0/24   172.16.30.1              0    100      0 i
PE1#
```

Chaque adresse de réseau figurant dans la table de routage est associée à une route sur laquelle il va être acheminé. Notons l'exemple du routeur PE2 qui est identifié par son adresse loopback 172.16.2.0, le routeur

PE1 peut l'atteindre par de deux manières, soit en passant par l'adresse 172.16.20.1 ou bien en passant par l'adresse 172.16.30.

- ***Le résultat de configuration sur le routeur P20***

```
P20#show ip bgp
BGP table version is 4, local router ID is 172.16.20.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? – incomplete
  Network          Next Hop          Metric  LocPrf  Weight  Path
*>i172.16.1.0/24   172.16.1.1             0     100       0     i
*>i172.16.2.0/24   172.16.2.1             0     100       0     i
*> 172.16.20.0/24  0.0.0.0                0               32768 i
P20#
```

Et pour terminer la vérification du bon fonctionnement du protocole BGP on utilise la commande **show ip route BGP** .Nous obtenons à la suite toutes les routes crées par ce protocole.

- ***Le résultat de configuration sur le routeur PE1***

```
PE1#sh ip route bgp
     172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
B       172.16.30.0/24 [200/0] via 172.16.30.1, 00:24:39
B       172.16.20.0/24 [200/0] via 172.16.20.1, 00:24:39
B       172.16.2.0/24 [200/0] via 172.16.2.1, 00:24:39
PE1#
```

La lettre **B** représente les routes qui sont crées par le protocole BGP. L'adresse 172.16.20.0 représente l'identifiant du routeur P20 qui est attaché également avec la passerelle par défaut 172.16.20.1

- ***Le résultat de configuration sur le routeur P20***

```
P20#sh  ip route bgp
    172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
B       172.16.1.0/24 [200/0] via 172.16.1.1, 00:33:31
B       172.16.2.0/24 [200/0] via 172.16.2.1, 00:33:31
P20#
```

5. Configuration MPLS :

La configuration du protocole MPLS/IP suivra 3 étapes pour fonctionner correctement. Il faut tout d'abord : l'activer par la commande **MPLS IP** ensuite il faut affecter les labels aux paquets IP lors d'un trafic entrant par la commande **MPLS label-protocol LDP** et en fin on applique la commande **MPLS LDP router-id loopback 0 force** pour utiliser les adresses loopbacks comme des identifiants des routeurs lors de l'acheminement des paquets et non pas les routeur–id.

- **Configuration MPLS :**

```
PE1(config)#MPLS IP
PE1(config)#mpls label protocol ldp
PE1(config)#mpls ldp router-id Loopback0 force
PE1(config)#no ftp-server write-enable
PE1(config)#int F0/0
PE1(config-if)#mpls ip
PE1(config)#int F0/1
PE1(config-if)#mpls ip
PE1(config-if)#^z
PE1#wr
```

- **Test et vérification :**

Pour tester le bon fonctionnement du protocole MPLS/IP on utilise les deux commandes suivantes :

a. La commande **show mpls ldp neighbor** a pour rôle de découvrir les voisins crée par le protocole MPLS.

✓ ***Le résultat de configuration sur le routeur PE1***

```
PE1# show  mpls ldp neighbor
   Peer LDP Ident: 172.16.20.1:0; Local LDP Ident 172.16.1.1:0
        TCP connection: 172.16.20.1.55676 - 172.16.1.1.646
        State: Oper; Msgs sent/rcvd: 62/66; Downstream
        Up time: 00:44:39
        LDP discovery sources:
        FastEthernet0/0, Src IP addr: 10.1.1.2
       Addresses bound to peer LDP Ident:
      10.1.1.2       172.16.20.1     10.1.1.10
   Peer LDP Ident: 172.16.30.1:0; Local LDP Ident 172.16.1.1:0
      TCP connection: 172.16.30.1.64580 - 172.16.1.1.646
      State: Oper; Msgs sent/rcvd: 61/65; Downstream
      Up time: 00:44:21
      LDP discovery sources:
     FastEthernet0/1, Src IP addr: 10.1.1.6
     Addresses bound to peer LDP Ident:
     10.1.1.6       172.16.30.1     10.1.1.14
PE1#
```

Comme l'indique le résultat de configuration ci-dessus, les voisins de routeur PE1 découvert par le protocole LDP sont 172.16.20.0 (l'adresse loopback de P20) via l'interface F0/0 et 172.16.30.0 (l'adresse loopback de P30) via l'interface F0/1 du routeur PE1.

b. La deuxième commande de test de protocole MPLS est **show mpls forwording-table** qui permet de voir l'affectation des labelles aux adresses qui se trouvent dans la table FEC.

✓ ***Le résultat de configuration sur le routeur P20***

```
PE1#show mpls forwarding-table
Local  Outgoing   Prefix          Bytes tag   Outgoing    Next Hop
tag    tag or VC  or Tunnel Id    switched    interface
16     Untagged   172.16.30.1/32  0           Fa0/1       10.1.1.6
17     Untagged   172.16.20.1/32  0           Fa0/0       10.1.1.2
18     Pop tag    10.1.1.8/30     0           Fa0/0       10.1.1.2
19     Pop tag    10.1.1.12/30    0           Fa0/1       10.1.1.6
20     20         172.16.2.1/32   0           Fa0/1       10.1.1.6
       20         172.16.2.1/32   0           Fa0/0       10.1.1.2
21     Aggregate  172.18.1.0/30[V] 0
22     Untagged   172.18.1.1/32[V] 0          Se0/0       point2point
23     Untagged   172.20.1.0/24[V] 0          Se0/0       point2point
PE1#
```

Le résultat de vérification nous indique les labelles affecté aux adresses réseau pour qu'ils puissent circuler dans le réseau MPLS/IP, prenons l'exemple l'adresse 172.16.2.1, le protocole LDP affecte le labelle 20.

6. Le Concept MPLS/VPN

- Configuration VPN

La configuration du concept MPLS/VPN toujours s'effectue sous l'autorité du protocole BGP en activant la configuration suivante :

```
PE1(config)#Router Bgp 100
PE1(config-router )#address-family vpnv4 unicast
PE1(config-router-family)# neighbor 172.16.20.1 activate
PE1(config-router-family)# neighbor 172.16.20.1 send-community both
PE1(config-router-family)# neighbor 172.16.30.1 activate
PE1(config-router-family)# neighbor 172.16.30.1 send-community both
PE1(config-router)# ^z
PE1#write
```

Après chaque configuration d'un routeur fédérateur comme P20 ou bien P30 on ajoute la commande suivante à chaque adresse voisine traitée.

```
P20 (config-router-family)# neighbor 172.16.30.1 route-reflector-client
```

7. *Le Concept VRF (Virtual Routing and Forwarding)*

VRF est une technologie incluse à IP et qui permet à un seul routeurs réseau d'avoir plusieurs instances de table de routage dont il peut s'en servir simultanément. Cette fonctionnalité permet d'accroitre le nombre de chemin d'accès réseau et de les segmenter sans avoir recours a de dispositifs multiples de telle sorte qu'un seul routeur lié a plusieurs site en attribuant à chacun d'eux une table de routage spécifique (VRF) est désormais possible. Ainsi, chaque interface de Pe (Ingress LER), reliée à un site client, est rattachée à une VRF particulière. Suite à la réception d'un paquet IP sur une interface client, le routeur I-LER procède à un examen de la table de routage de la VRF à laquelle est rattachée l'interface et par conséquent ne consulte pas sa table de routage globale.

Cette possibilité d'utiliser plusieurs tables de routage indépendantes permet de gérer un plan d'adressage par sites, même en cas de recouvrement d'adresses entre VPN différents, ce qui accentue la sécurité du réseau et atténue également la nécessité de chiffrement et d'authentification.

En effet, VRF agit comment un routeur logique (virtuel), du moins il n'utilise qu'une seule table de routage.

- **Configuration de protocole VRF coté PE**

La configuration du protocole VRF nécessite l'utilisation simultanée du protocole OSPF et du protocole BGP

- ***Configuration de protocole VRF sur PE1***

```
PE1#conf t
PE1(config)#ip cef
PE1(config)#ip  vrf  RESEAUX
PE1(config)#rd 200 :1
PE1(config)#route-target both 200:1
PE1(config)#exit
PE1#wr
PE1#conf t
PE1(config)#router ospf 10 vrf RESEAUX
PE1(config-router )#network 172.18.1.0 0.0.0.3 area 1
PE1(config-router )#redistribut bgp 100 subnets
PE1(config-router )#exit
PE1(config)#router bgp 100
PE1(config-router )#addess-family ipv4 vrf RESEAUX
PE1(config-router )# redistribut ospf 10 vrf RESEAUX
PE1(config-router )#exit
PE1(config)#int s0/0
PE1(config-if)#no shut
PE1(config-if)#encapsulation ppp
PE1(config-if)#clock rate 64000
PE1(config-if)#ip vrf forwording RESEAUX
```

PE1(config-if)#ip add 172.18.1.2 255.255.255.252

PE1(config-if)#exit

PE1(config)#exit

PE1#wr

- ***Test de configuration***

Pour tester le bon fonctionnement du processus VRF coté fournisseur il faut appliquer les commandes de teste suivantes :

- ✓ Show ip route vrf RESEAUX : pour avoir les tables des routes VRF.
- ✓ Show ip bgp vpn v4 vrf RESEAUX: pour avoir les tables BGP VPN qui sont en relation directe avec le processus VRF.

➢ ***Vérification sur le simulateur***

- ***La table de routage VRF de PE1***

```
PE1#sh ip route vrf RESEAUX
Routing Table: RESEAUX
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS leve
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.18.0.0/16 is variably subnetted, 6 subnets, 2 masks
B       172.18.1.33/32 [200/0] via 172.16.2.1, 00:13:02
B       172.18.1.32/30 [200/0] via 172.16.2.1, 00:13:02
B       172.18.1.29/32 [200/0] via 172.16.2.1, 00:13:02
B       172.18.1.28/30 [200/0] via 172.16.2.1, 00:13:02
C       172.18.1.1/32 is directly connected, Serial0/0
C       172.18.1.0/30 is directly connected, Serial0/0
     172.21.0.0/24 is subnetted, 2 subnets
B       172.21.5.0 [200/74] via 172.16.2.1, 00:13:03
B       172.21.6.0 [200/74] via 172.16.2.1, 00:13:03
     172.20.0.0/24 is subnetted, 1 subnets
O       172.20.1.0 [110/74] via 172.18.1.1, 00:34:22, Serial0/0
PE1#
```

- ***La table de routage VRF de PE2***

```
PE2#sh ip route vrf RESEAUX
*Mar  1 00:36:39.671: %LDP-5-NBRCHG: LDP Neighbor 172.16.30.1:0 (1) is DOWN
```

```
eived error notification from peer: Holddown time expired)
*Mar  1 00:36:39.727: %LDP-5-NBRCHG: LDP Neighbor 172.16.20.1:0 (3) is DOWN
eived error notification from peer: Holddown time expired)H
Routing Table: RESEAUX
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
       ia - IS-IS inter area, * - candidate default, U - per-user static ro
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.18.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.18.1.33/32 is directly connected, Serial0/1
C       172.18.1.32/30 is directly connected, Serial0/1
C       172.18.1.29/32 is directly connected, Serial0/0
C       172.18.1.28/30 is directly connected, Serial0/0
B       172.18.1.1/32 [200/0] via 172.16.1.1, 00:17:08
B       172.18.1.0/30 [200/0] via 172.16.1.1, 00:17:08
     172.21.0.0/24 is subnetted, 2 subnets
O       172.21.5.0 [110/74] via 172.18.1.29, 00:35:39, Serial0/0
O       172.21.6.0 [110/74] via 172.18.1.33, 00:35:39, Serial0/1
     172.20.0.0/24 is subnetted, 1 subnets
B       172.20.1.0 [200/74] via 172.16.1.1, 00:17:10
PE2#
```

- ***Table VPN/BGP pour le VRF RESEAUX sur PE1***

```
PE1#sh ip bgp vpnv4 vrf RESEAUX
BGP table version is 31, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network     Next Hop     Metric  LocPrf  Weight     Path
Route Distinguisher: 200:1 (default for vrf RESEAUX)
*> 172.18.1.0/30   0.0.0.0                0        32768      ?
*> 172.18.1.1/32   0.0.0.0                0        32768      ?
* i172.18.1.28/30  172.16.2.1            0   100      0      ?
*>i                 172.16.2.1            0   100      0      ?
* i172.18.1.29/32  172.16.2.1            0   100      0      ?
*>i                 172.16.2.1            0   100      0      ?
```

```
* i172.18.1.32/30   172.16.2.1          0    100      0          ?
*>i                 172.16.2.1          0    100      0          ?
* i172.18.1.33/32   172.16.2.1          0    100      0          ?
*>i                 172.16.2.1          0    100      0          ?
*> 172.20.1.0/24    172.18.1.1          74         32768         ?
* i172.21.5.0/24    172.16.2.1          74    100      0          ?
*>i                 172.16.2.1          74    100      0          ?
* i172.21.6.0/24    172.16.2.1          74    100      0          ?
*>i                 172.16.2.1          74    100      0          ?
PE1#
```

IV. Conclusion :

Dans ce chapitre on a exhibé la simulation et la configuration d'une solution MPLS au sein de la Backbone Tunisie Télécom tout en mettant l'accent sur les concepts relatifs à ce protocole en fonction des protocoles de routage internes et externes tel qu'OSPF et BGP.

Nous avons vu depuis le chapitre précédent, les apports de cette solution à la bonne gestion de la bande passante puisque la vérification des paquets s'effectue essentiellement une seule fois via la notion du label, ainsi que la prise en considération de la sécurité a l'aide des VPNs et la virtualisation a l'aide des VRFs.

Dans le chapitre suivant, on étudiera un cas particulier de VoIP pour Business client (cas SOTETEL) avec définition du réseau VPN reliant différents sites de l'entreprise, configuration du Call Manager et configuration de la partie trunk entre Voice Gateway et Softswitch.

Chapitre V : Etude de cas VoIP pour Business client (SOTETEL)

I. Introduction :

Il est aujourd'hui largement reconnu que la Voix sur IP (Voice over Internet Protocol VoIP) a le pouvoir de changer radicalement les modes de communications dans le monde des affaires. L'utilisation de la VoIP (Voice over Internet Protocol) dans l'entreprise n'est plus aujourd'hui l'apanage des grandes sociétés et organismes publiques. Même les PME sont déjà concernées par les services de VoIP, et elles sont de plus en plus nombreuses à le faire.

Le recours à la VoIP permet également à l'entreprise de simplifier la gestion de son réseau interne, en conservant le matériel dont elle dispose déjà.

La SOTETEL qui se présente comme acteur de référence dans le domaine des télécommunications en Tunisie et à l'étranger et qui se positionne comme le partenaire privilégié des principaux équipementiers internationaux opérant en Tunisie, sera prise comme échantillon des entreprises qui ont déjà souscrit un abonnement de téléphonie basé sur des services de VoIP.

La SOTEETL est une entreprise qui possède actuellement, appart le siège localisé à la zone industrielle de Charguia, trois agences à Sousse, Sfax et Médenine.

II. Architecture du réseau de la SOTETEL :

1. Ancienne architecture:

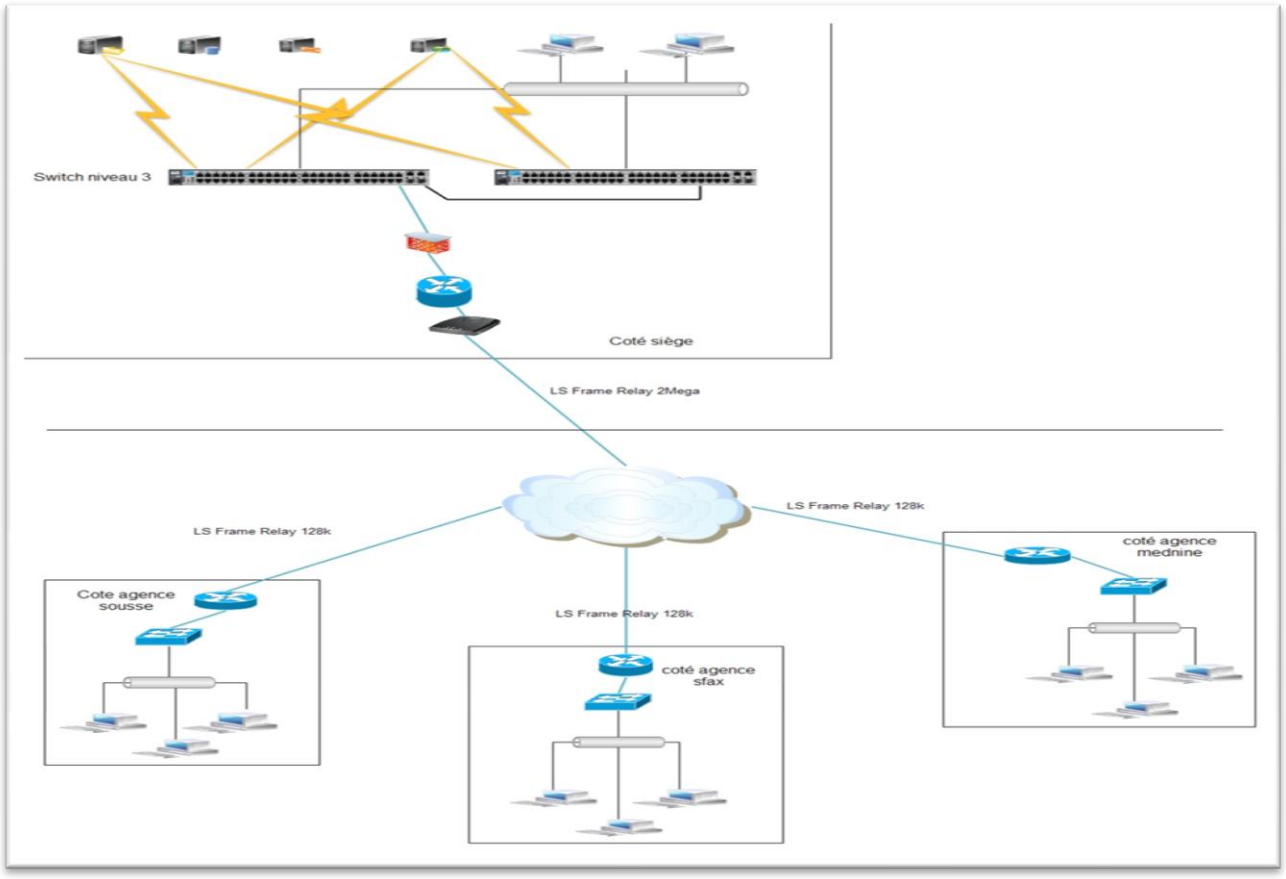

Figure 5.1: ancienne architecture

L'ancienne architecture de la SOTETEL, basée essentiellement sur des liaisons Frame Relay, pose un principal problème en terme de limitation de débit (128 bps) et de coût élevé pour la téléphonie (et pour ADSL/FR). Pour cette raison la SOTETEL s'est trouvée dans l'obligation de migrer vers une nouvelle solution moins chère et plus performante.

2. Nouvelle architecture:

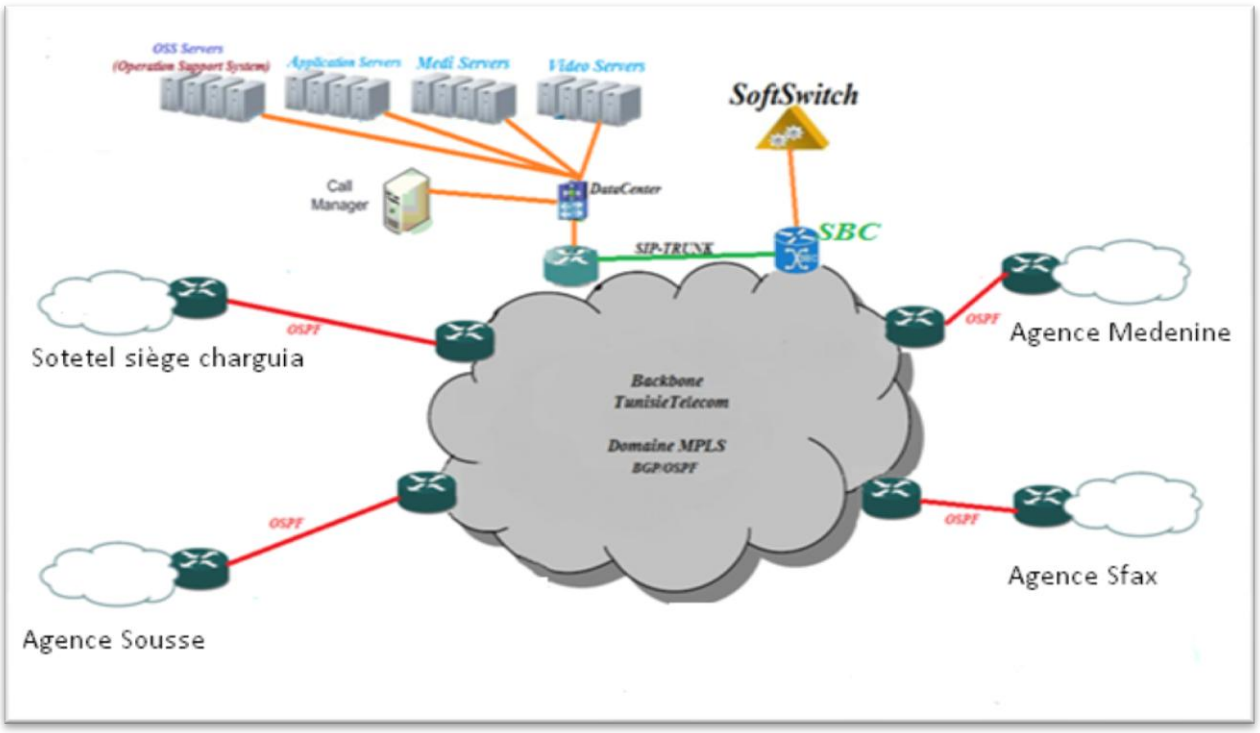

Figure 5.2 : Nouvelle architecture

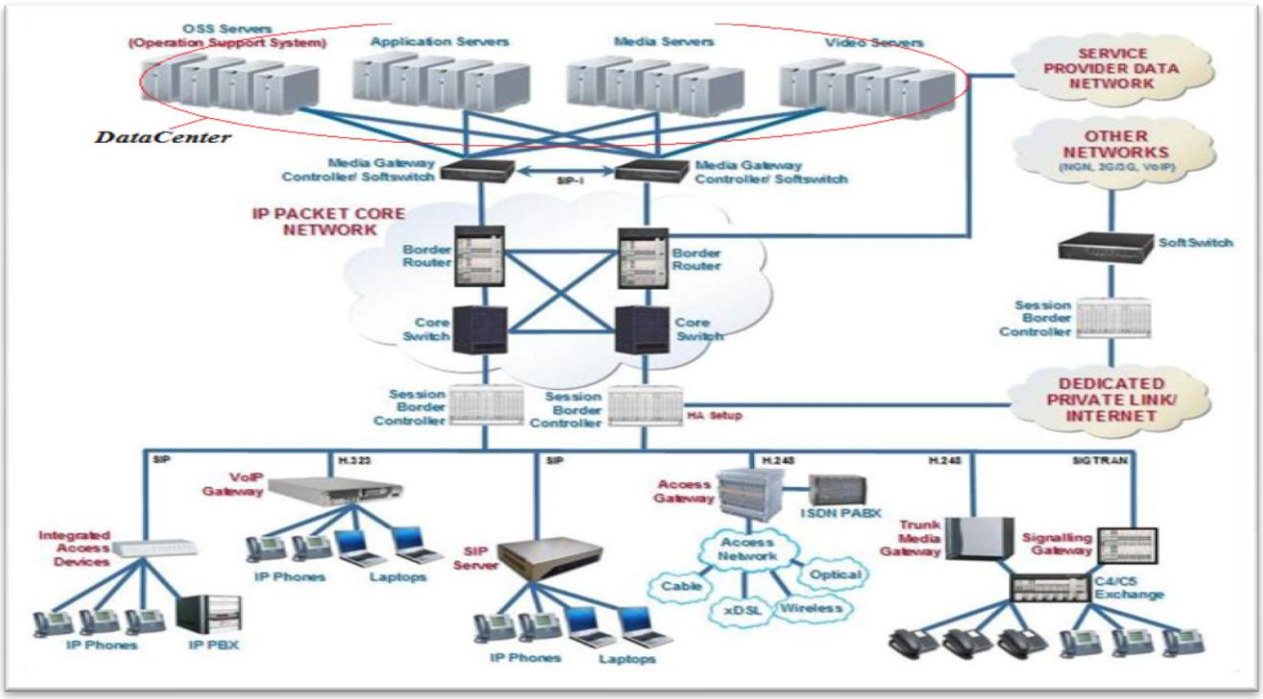

Figure 5.3 : Architecture SIP de la solution

III. Présentation du Matériel de la solution VoIP :

3. Le Datacenter :

Un centre de traitement des données (Data center en anglais) est un site physique sur lequel se trouvent regroupés des équipements constituants du système d'information de l'entreprise (mainframes, serveurs, baies de stockage, équipements réseaux et de télécommunications…). Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien de prestataires. C'est un service généralement utilisé pour remplir une mission critique relative à l'informatique.

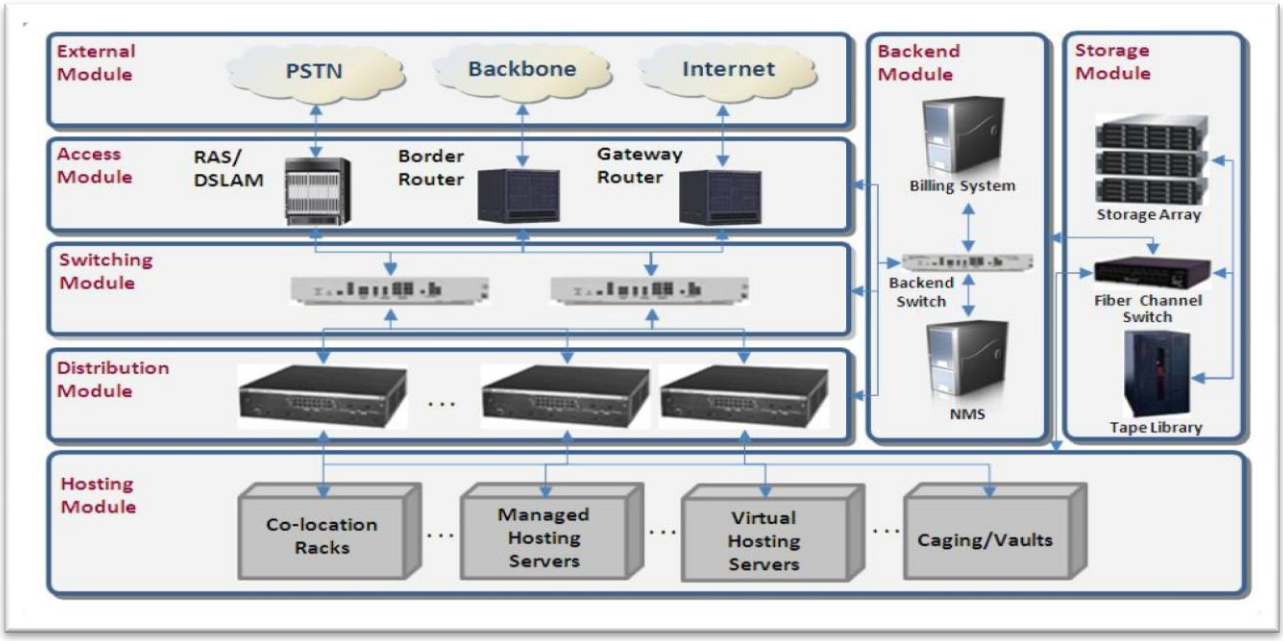

Figure 5.4 : Squelette du Datacenter

La sécurité de l'information est aussi une préoccupation, c'est pour cette raison qu'un Datacenter doit offrir un environnement sécurisé qui atténuera les risques d'une atteinte à la sécurité. Un Datacenter doit donc maintenir des normes élevées pour assurer l'intégrité et la fonctionnalité de ses environnements hébergés.

4. Le SBC (Session Border Controller) :

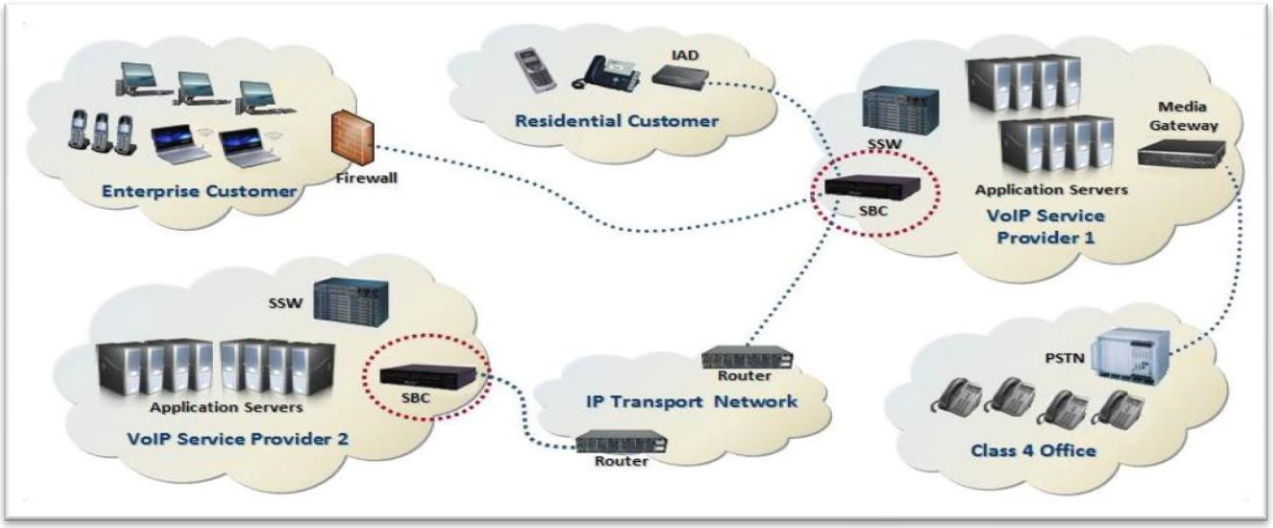

Figure 5.5: Session Border Controller

Aujourd'hui, il n'existe pas de VoIP sécurisée sans SBC(le firewall de la VoIP). Un firewall contrôle l'IP mais ne contrôle pas le SIP, d'où la porte ouverte à toute requête malveillante par ce biais. Le gros point fort d'un SBC se révèle lors d'un cas de requêtes malveillantes. Dans ce cas, leSBC bloque les accès, ce qui n'est pas le cas des meilleurs firewalls.

Un SBC est composé de deux modules :

- Un module *SBC Signalisation* chargé de contrôler l'accès des messages de signalisation VoIP au réseau
- Un module *SBC Media* chargé de contrôler l'accès des paquets RTP au réseau. Ce module fait office de *proxy* RTP.

5. Call Manager :

Basé sur un serveur dédié, Call Manager apporte les fonctions de téléphonie aux réseaux locaux et étendus d'entreprise. Avec une centaine à plusieurs milliers de téléphones gérés, Call Manager permet de réaliser un plan de numérotation unique sur plusieurs sites avec une gestion centralisée du système de téléphonie. Couplé à la fonction SRST des routeurs Cisco, Call Manager offrira le même niveau de fonctionnalité sur tous les sites de l'entreprise sans être obligé de déployer un autocommutateur sur chaque site. Les applications liées à Call Manager comme la messagerie unifiée, les centres de contacts et la vidéo téléphonie seront mises en œuvre pour tous les utilisateurs du réseau, quelque soit leur emplacement géographique.

Les APIs (Interfaces de Programmation d'Application) de Call Manager permettent à la téléphonie d'interagir pleinement avec les applications Cisco ou tierces disponibles sur le réseau.

Call Manager peut s'intégrer à un système de téléphonie traditionnelle pour permettre de migrer en douceur vers un réseau convergent [8].

6. Softswitch :

Le Softswitch ou le contrôleur d'appel ou bien aussi MGC (Media Gateway Controller) est l'équipement principale de la couche contrôle. Il permet :

- De contrôler le fonctionnement des passerelles de signalisation(SGW) et des passerelles de médias (MGW).
- D'allouer les ressources nécessaires à l'établissement des appels ou des sessions multimédias sur le réseau de transport (réseau cœur IP).
- D'assurer l'accès aux différentes plateformes et capacités de service de la couche service.
- D'assurer l'authentification des abonnés et la facturation des communications.

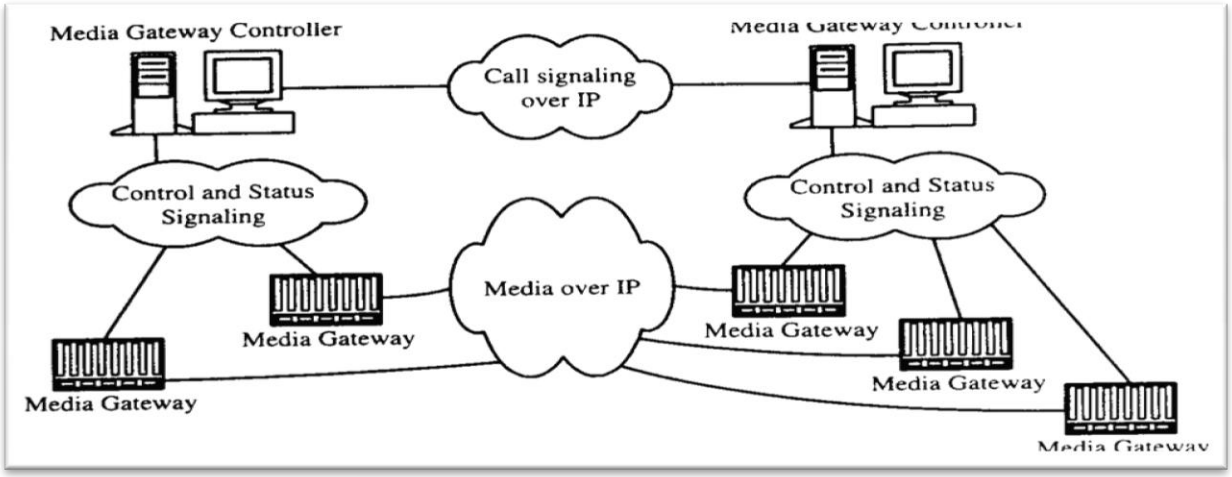

Figure 5.6: L'architecture Softswitch

7. Cisco 2811 :

Le routeur intégré de services de Cisco 2811 fournit l'appui suivant :

- Densité accrue par les logements pour carte à grande vitesse d'interface de WAN
- Fente augmentée de module de réseau
- Appui facultatif de commutation de la couche 2 avec la puissance au-dessus de l'Ethernet (Poe) (comme option)
- Sécurité
  - Appui de 1 jusqu'à 1500 tunnels de VPN avec le module d'AIM-EPII-PLUS
  - Appui de la défense d'antivirus par la commande d'admission de réseau (le Conseil de l'Atlantique nord)
  - Empêchement d'intrusion aussi bien que l'appui stateful de mur à l'épreuve du feu d'IOS de Cisco et beaucoup plus de dispositifs de sécurité essentiels
- Voix
  - Appui analogue et numérique d'appel vocal
  - Appui facultatif d'audio-messagerie
  - Le soutien facultatif de Cisco Call Manager express (Cisco CME) pour le traitement d'appel local dans de seules affaires de stand pour IP to 36 haut téléphone
  - Soutien facultatif de soutien capable de survie de téléphonie d'emplacement à distance du traitement d'appel local dans des succursales de petite entreprise pour jusqu'à 36 téléphones d'IP

Figure 5.7: Cisco 2811

8. Commutateur Catalyst2960 48 10/100 PoE 2 1000BT

Le Catalyst2960 est un Commutateur 48 ports qui supporte Power Over Ethernet et Quality of Service. Ces deux fonctionnalités sont importantes dans notre cas car elles permettent respectivement d'alimenter les

téléphones IP et les points d'accès au travers du réseau, supprimant le besoin d'adaptateurs secteurs supplémentaires; et s'assurent que le trafic réseau est correctement classifié, évitant de la meilleure manière possible tout congestion.

Figure 5.8: Commutateur Catalyst 2960 48 PoE

9. Cisco Unified IP Phones :

Le suffixe –GE veut simplement dire que le commutateur interne du téléphone IP supporte les liens Gigabit. Ce téléphone IP possède un écran LCD assez large, ce qui le rend plutôt confortable à utiliser. Il est intéressant de noter que le 7941G-GE utilise Java.

Figure 5.9: Cisco Unified IP Phone 7941G-GE

IV. Partie configuration :

1. Configuration du commutateur catalyst 2960

- **Création de vlan :**

Avant de passer à la configuration du Call Manager, on doit tout d'abord préparer le commutateur où seront reliés tous nos matériels (IPphones, pc, routeur, ..). On commence par la création de deux vlan, un pour la voix et l'autre pour la data. Si on fait un show vlan on pourra savoir les différents vlan existant et les ports qui leur appartient.

```
Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Création du vlan voix et data

Switch (conf)# vlan 10
Switch (config-vlan)# name voice
Switch (conf)# vlan 20
Switch (config-vlan)# name data

Un autre sh vlan nous montrera l'état des vlans créer et de vérifier aussi qu'on n'a pas deux VLANs de même nom car dans ce cas il s'avère s'obtenir qu'on aura un disfonctionnement du commutateur.

```
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                   Gig1/1, Gig1/2
10   voice                               active
20   data                                active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup
```

- **Attribution des ports**

On passe maintenant à l'attribution des ports aux différents vlan, en utilisant la commande interface range pour sélectionner plusieurs interfaces en même temps, et la commande switchport pour modifier l'état du port pour que tout les équipements bénéficient de la voix, alors, il faut que tout les ports utilisés appartiennent à la fois au vlan data et vlan voix.

```
Switch (config)# interface range fastethernet0/1-23
Switch (config-if-range)# switchport mode access
Switch (config-if-range)# switchport access vlan 20
Switch (config-if-range)# switchport voice  vlan 10
Switch (config-if-range)# ^Z
```

Un autre sh vlan nous montrera les nouveaux vlan et leurs ports

```
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/24, Gig0/1, Gig0/2
10   voice                               active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23
20   data                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup
```

- **Configuration de base du 2811**

```
Current configuration: 4591 bytes
!
! Last configuration change at 05:40:46 UTC Fri Jul 20 2012 by sotetel
! NVRAM config last updated at 05:40:49 UTC Fri Jul 20 2012 by sotetel
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SRST_Tunis
!
```

```
boot-start-marker
boot-end-marker
!
card type e1 0 2
!
no aaa new-model
no network-clock-participate wic 2
dot11 syslog
!
--More--        ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.10
ip dhcp excluded-address 10.10.10.254
!
ip dhcp pool Voice
  network 10.10.10.0 255.255.255.0
  default-router 10.10.10.254
  option 150 ip 10.10.10.2
!
multilink bundle-name authenticated
!
voice-card 0
 no dspfarm
!
crypto pki trustpoint TP-self-signed-1188424807
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1188424807
 revocation-check none
 rsakeypair TP-self-signed-1188424807
!
archive
 log config
 --More--        hidekeys
!
controller E1 0/2/0
!
interface Loopback1
 ip address 10.10.11.251 255.255.255.0
!
interface Tunnel0
 ip address 192.168.50.1 255.255.255.252
 tunnel source 172.16.82.2
 tunnel destination 172.16.82.6
!
interface Tunnel1
 ip address 192.168.50.13 255.255.255.252
 tunnel source 172.16.82.2
 tunnel destination 172.16.82.14
 --More--        !
interface Tunnel2
 ip address 192.168.50.9 255.255.255.252
 tunnel source 172.16.82.2
 tunnel destination 172.16.82.10
!
interface Tunnel3
 ip address 192.168.50.17 255.255.255.252
 tunnel source 172.16.82.2
 tunnel destination 172.16.82.18
!
```

```
interface FastEthernet0/0
 ip address 10.10.10.254 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description $ES_LAN$
 ip address 192.168.100.2 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/1/0
 --More--        ip address 172.16.82.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
ip forward-protocol nd
ip route 10.2.0.0 255.255.255.0 Serial0/1/0
ip route 10.3.0.0 255.255.255.0 Serial0/1/0
ip route 10.4.0.0 255.255.255.0 Serial0/1/0
ip route 10.5.0.0 255.255.255.0 Serial0/1/0
ip route 192.168.1.0 255.255.255.0 192.168.1.9
ip route 192.168.3.0 255.255.255.0 192.168.100.1
ip route 192.168.4.0 255.255.255.0 192.168.100.1
ip route 192.168.5.0 255.255.255.0 192.168.100.1
ip route 192.168.12.0 255.255.255.0 Tunnel3
ip route 192.168.13.0 255.255.255.0 Tunnel0
ip route 192.168.14.0 255.255.255.0 Tunnel2
ip route 192.168.15.0 255.255.255.0 Tunnel1
ip route 192.168.100.0 255.255.255.0 FastEthernet0/1
!
ip http server
no ip http secure-server
!
control-plane
!
voice-port 0/3/0
 timing hookflash-out 50
!
voice-port 0/3/1
 supervisory disconnect dualtone mid-call
 no battery-reversal
 timeouts call-disconnect 0
 timeouts wait-release 5
 timing hookflash-out 50
 connection plar 1111
 description ligne pour tunisie telecom 71941700
 caller-id enable
!
 --More--        voice-port 0/3/2
 timing hookflash-out 50
!
voice-port 0/3/3
 timing hookflash-out 50
 connection plar 1111
 description ligne pour standard sotetel N 2999
 caller-id enable
!
ccm-manager fallback-mgcp
```

```
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.10.10.2
ccm-manager config
!
mgcp
mgcp call-agent 10.10.10.2 2427 service-type mgcp version 0.1
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode nse
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp package-capability pre-package
no mgcp package-capability res-package
 --More--        no mgcp timer receive-rtcp
mgcp sdp simple
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
dial-peer voice 999030 pots
 service mgcpapp
 port 0/3/0
!
dial-peer voice 999031 pots
 service mgcpapp
 direct-inward-dial
 port 0/3/1
!
dial-peer voice 999032 pots
 service mgcpapp
 port 0/3/2
!
dial-peer voice 999033 pots
 service mgcpapp
 --More--        port 0/3/3
!
dial-peer voice 100 pots
 destination-pattern 0.T
 port 0/3/1
!
dial-peer voice 1500 voip
 destination-pattern 15..
 session target ipv4:10.5.0.1
!
dial-peer voice 1300 voip
 destination-pattern 13..
 session target ipv4:10.3.0.1
!
dial-peer voice 111 pots
 destination-pattern 0.T
 port 0/3/1
!
credentials
 ip source-address 10.10.10.254 port 2445
!
call-manager-fallback
 max-conferences 8 gain -6
 transfer-system full-consult
 ip source-address 10.10.10.2 port 2000
```

```
 max-ephones 42
 max-dn 144
!
!
line con 0
line aux 0
line vty 0 4
 login local
!
scheduler allocate 20000 1000
ntp source FastEthernet0/1
ntp master
ntp update-calendar
ntp server 10.10.11.251
ntp server 10.10.10.252
!
end
```

- **NTP :**

La configuration de l'heure est importante, les téléphones IP se synchroniseront avec le serveur NTP interne du routeur :

```
Router (config)# clock timezone CET 1
Router# clock  set 10:24:00  20 jul  2012
```

- **DHCP :**
  - **DHCP voix dynamique**

    Le routeur jouera également le rôle de serveur DHCP. C'est lui qui distribuera les adresses IP aux téléphones :

    Deux remarques importantes. Tout d'abord, la commande option permet de spécifier une option DHCP, dans notre cas l'option 150 qui correspond à l'adresse IP du serveur TFTP. Les téléphones IP utilisent ce serveur TFTP pour récupérer tous les fichiers dont ils ont besoin, comme leur fichier de configuration, sonneries, ... Nous avons préféré l'utilisation du serveur TFTP fourni par l'IOS, c'est pourquoi l'adresse IP spécifiée dans la commande est celle du routeur. La deuxième commande importante est ip dhcp excluded-address ; elle empêche le routeur de distribuer une plage d'adresses IP, généralement réservé aux autre équipements ou interfaces.
  - **DHCP voix statique**

    Il est également possible de faire des assignations statiques d'adresses IP basée sur l'adresse MAC du client. Dans ce cas, un pool DHCP doit être créé pour chaque client.
  - **DHCP données**

    Le routeur jouera également le rôle de serveur DHCP. C'est lui qui distribuera les adresses IP aux PCs.

2. *Configuration du Call Manager*

Figure 5.10 : authentification

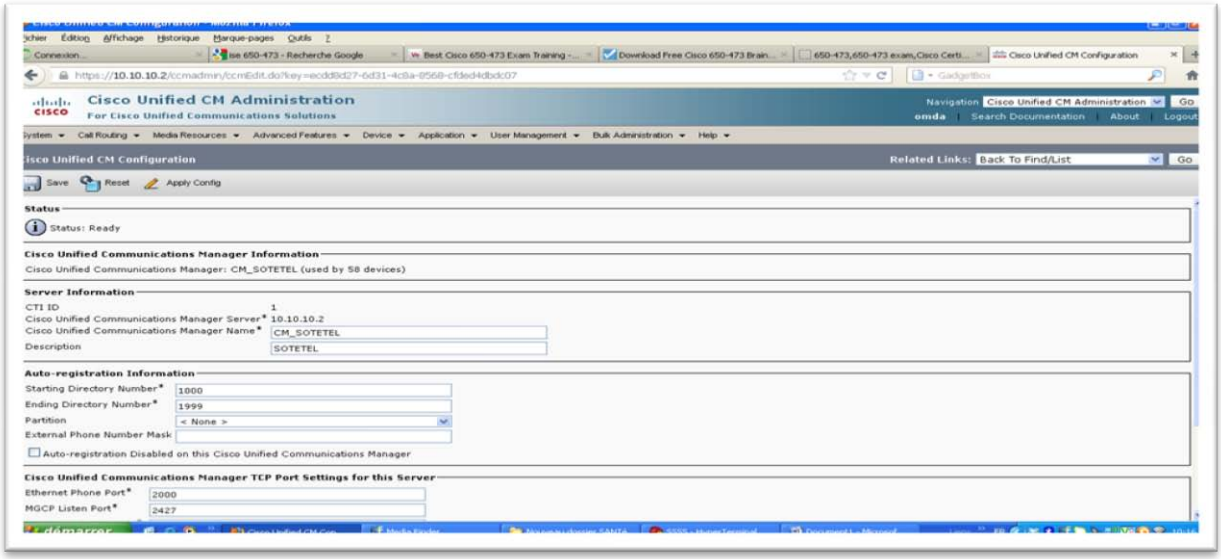

Figure 5.11a : configuration de base du Call Manager

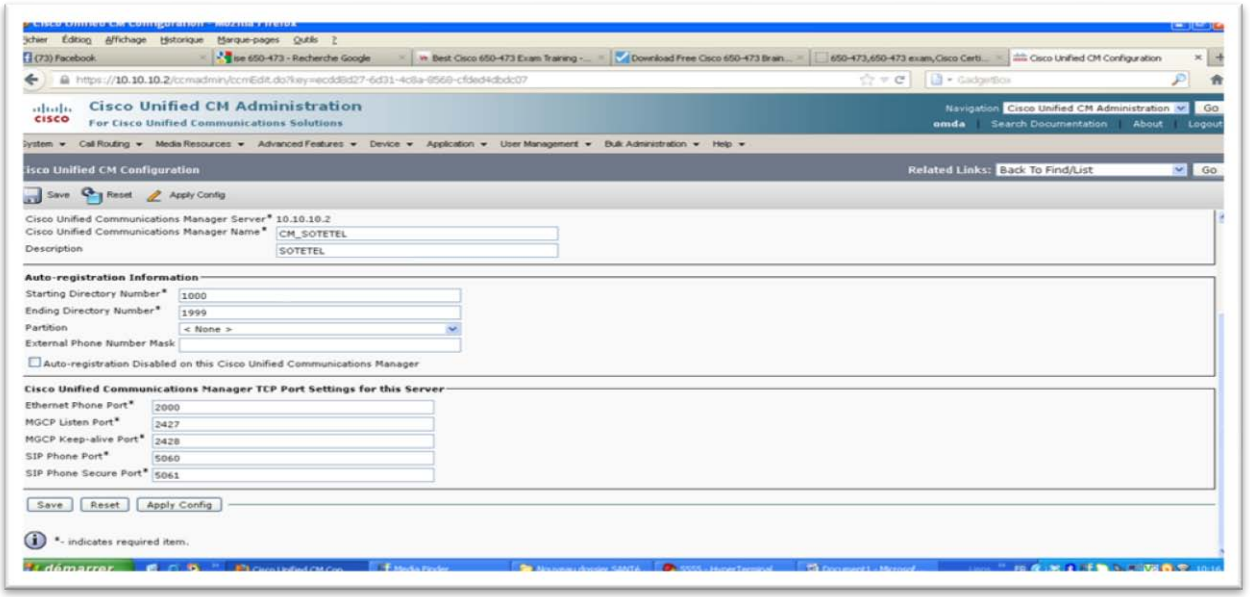

Figure 5.11b : configuration de base du Call Manager

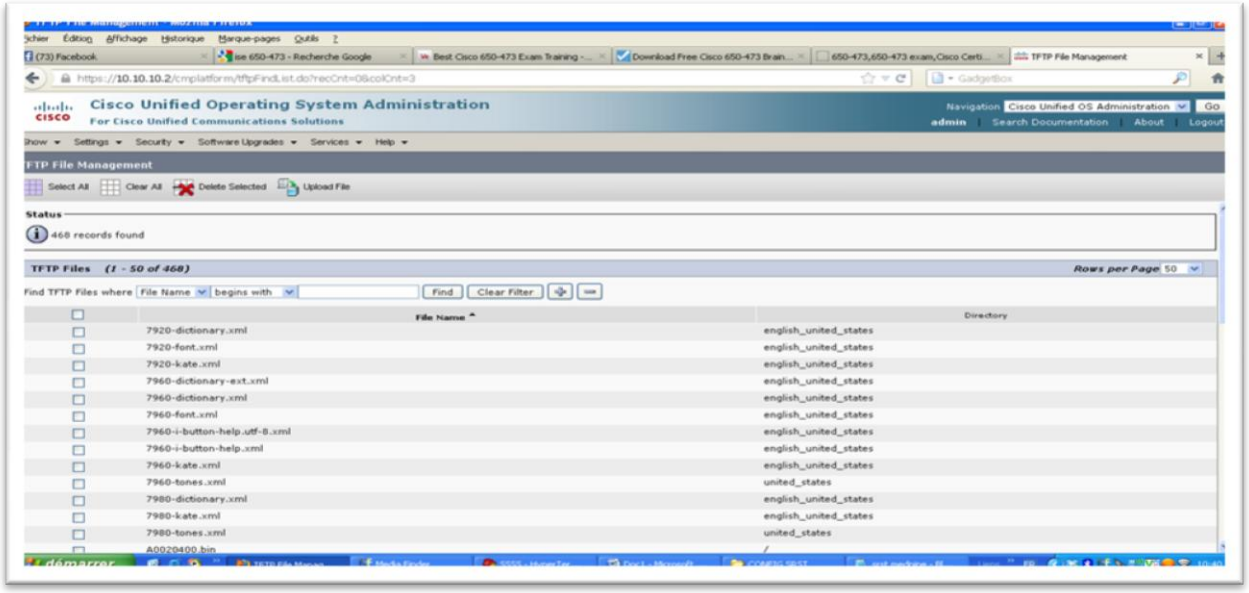

Figure 5.12 : configuration de la partie TFTP

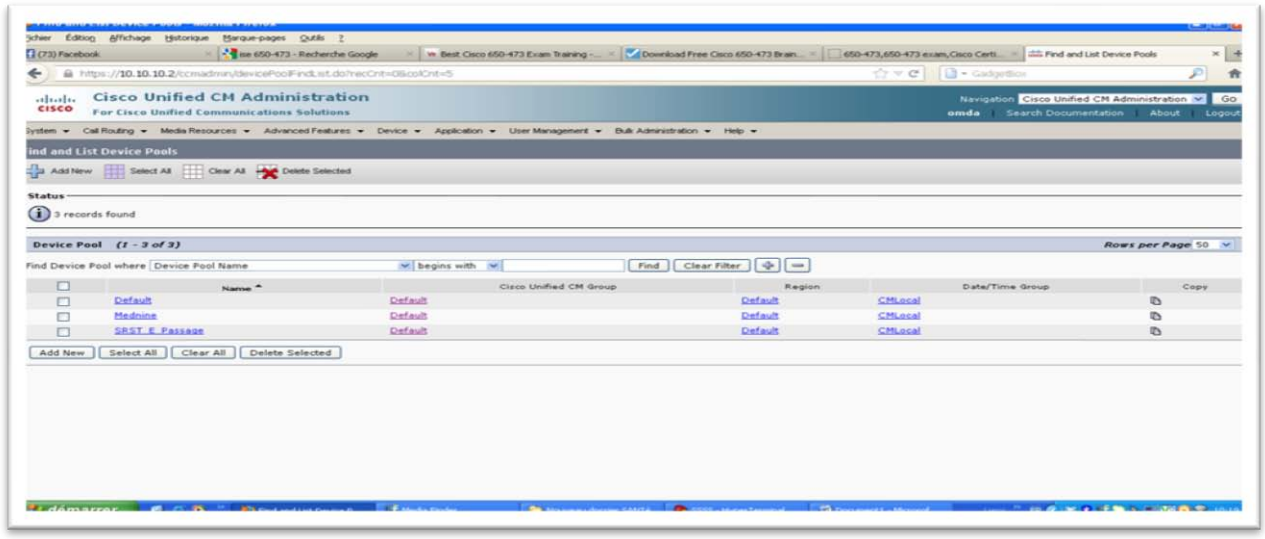

Figure 5.13 : création des pools relatifs aux différentes agences de la SOTETEL

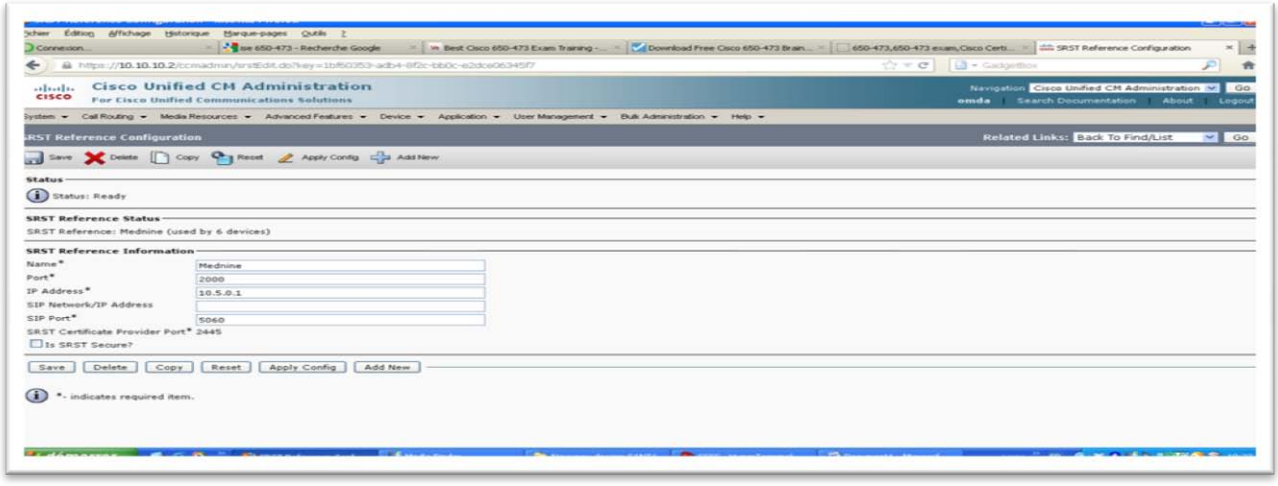

Figure 5.14 : configuration De l'SRST Médenine

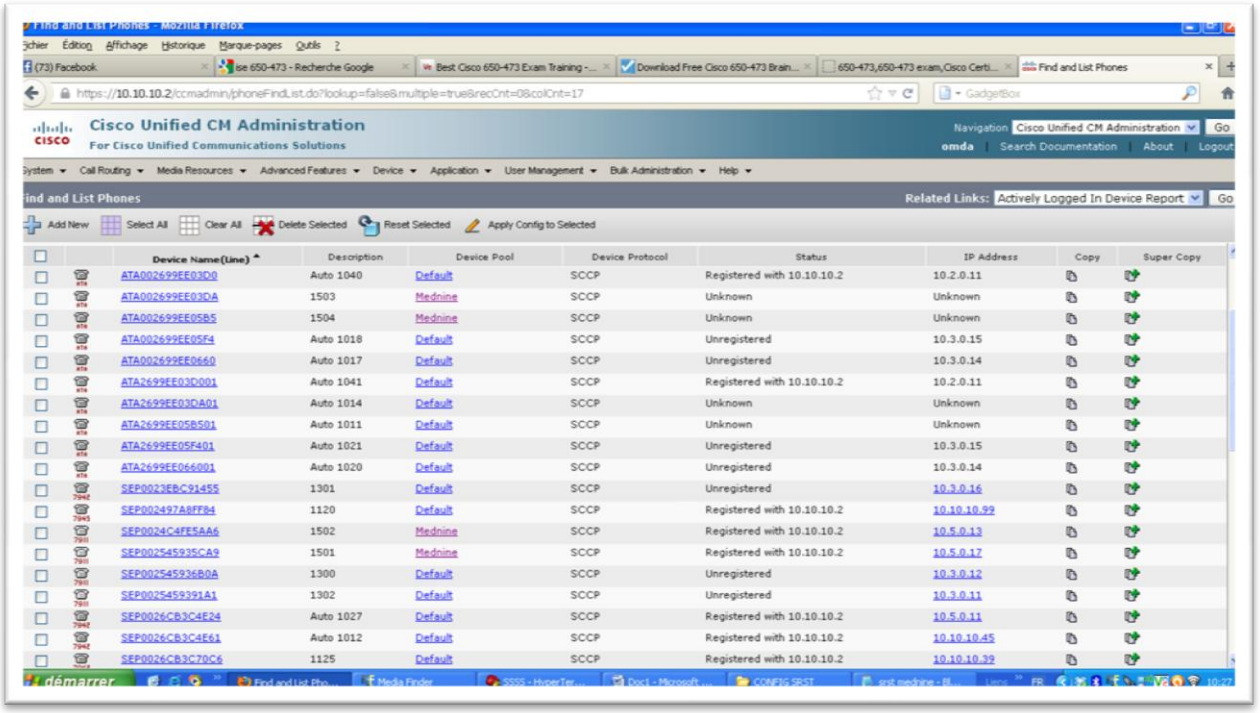

Figure 5.15 : Création des IP Phones

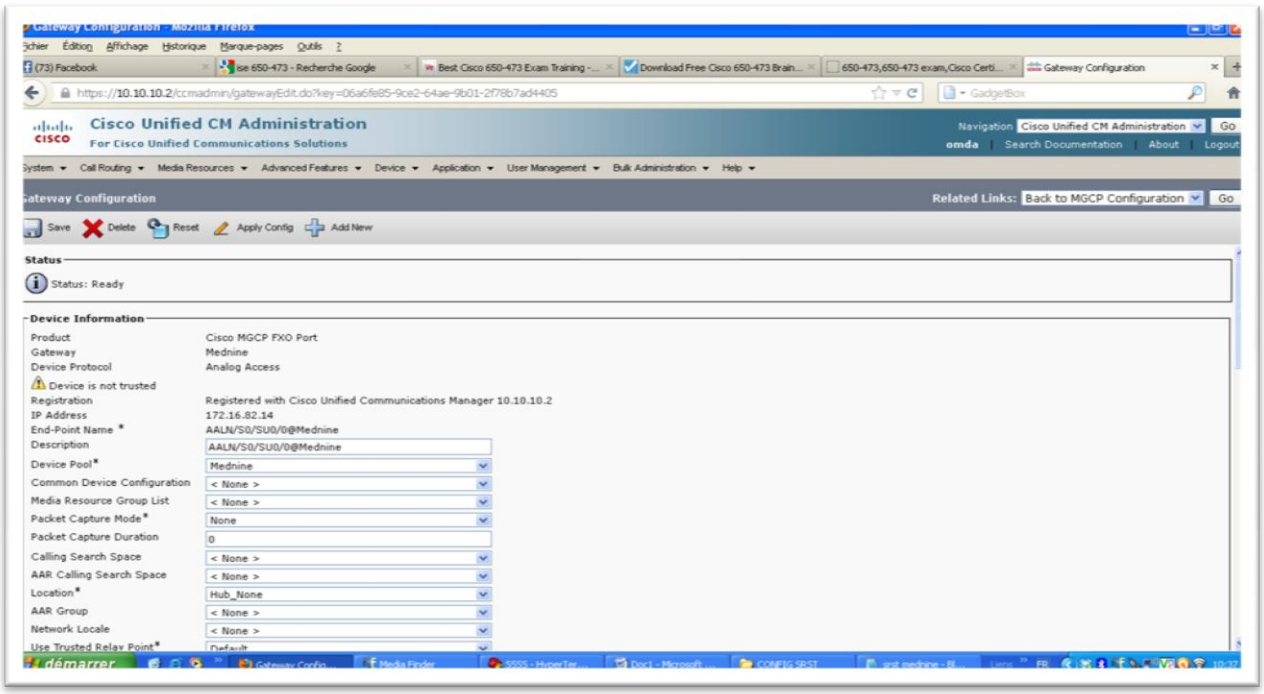

Figure 5.16 : configuration du MGCP FXO Port[1]

1 : permet de faire des communications avec la téléphonie analogique en cas de besoin.

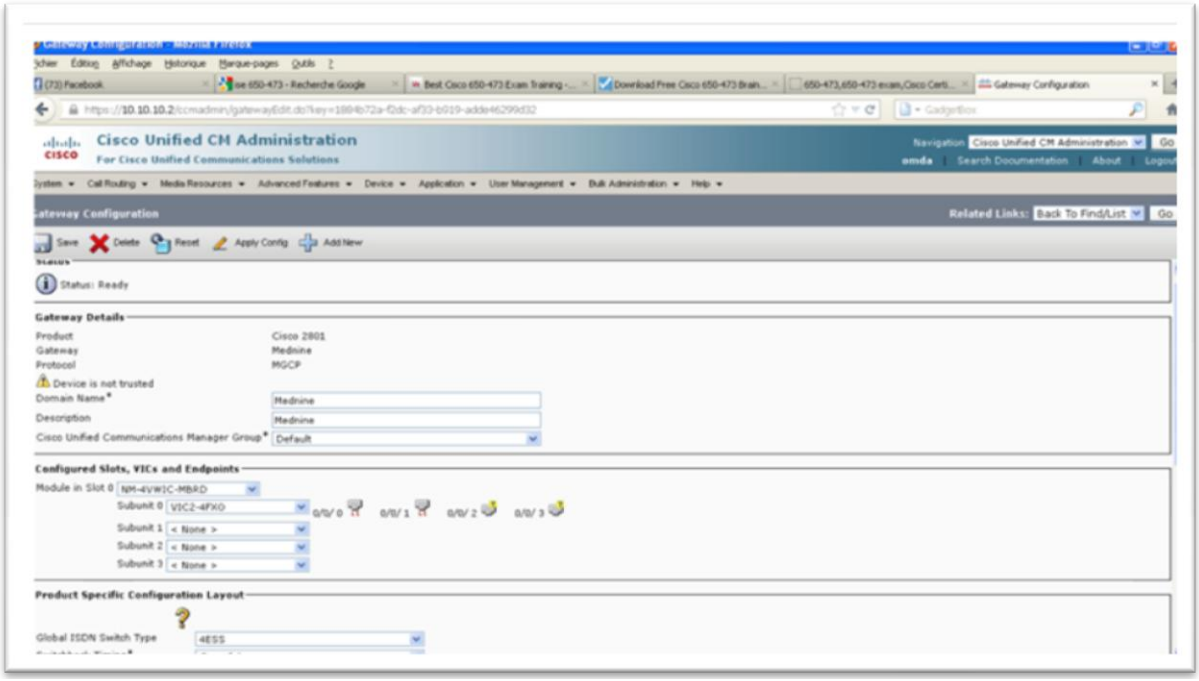

Figure 5.17 : Configuration du MGCP FXO Port

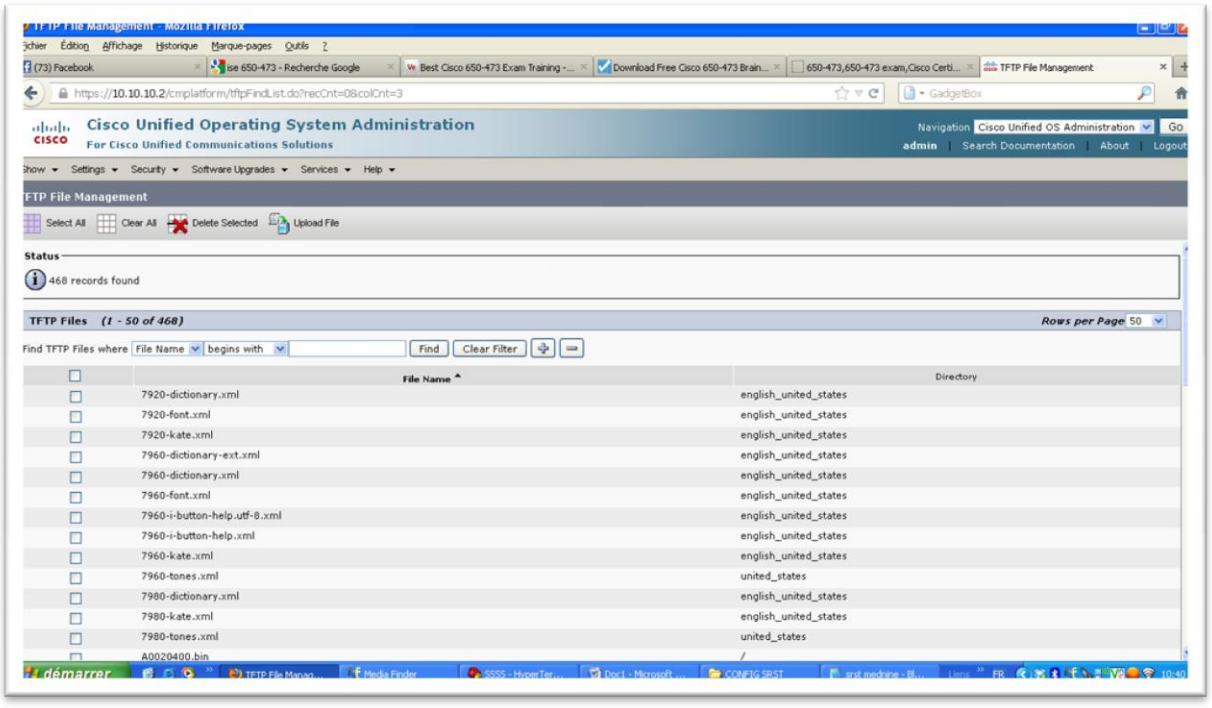

Figure 5.18 : configuration de la partie TFTP firmware

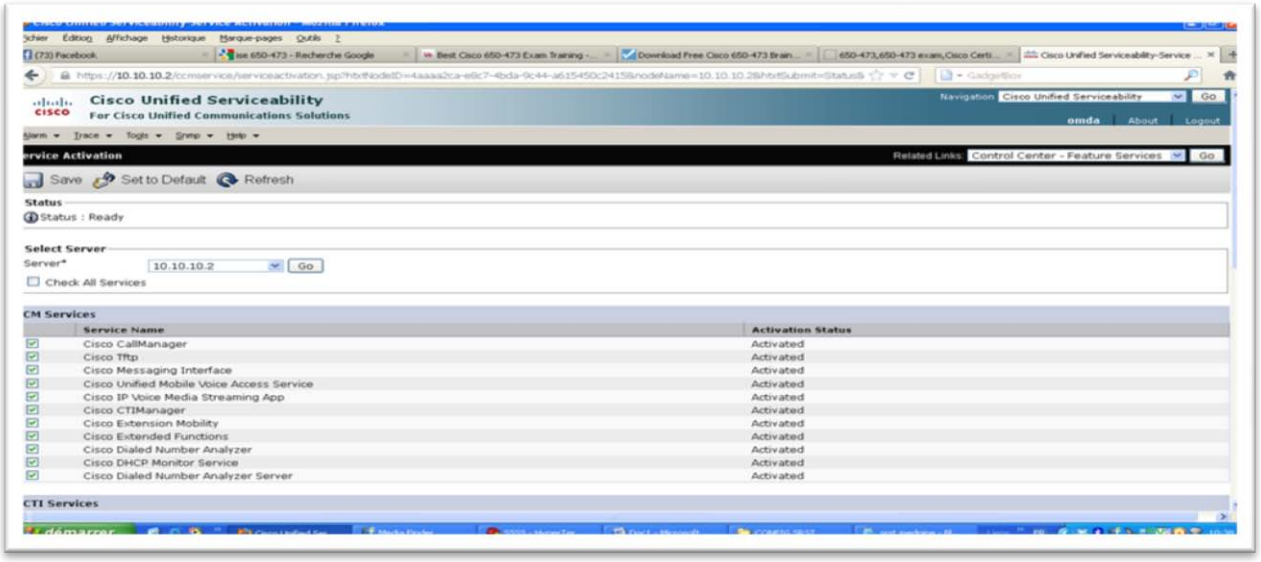

Figure 5.19 : sélection du Call Manager Services

3. Configuration de la partie SIP-trunk entre Voice Gateway et Softswitch.

Un « Trunk IP » ou « Trunk SIP », est un service fourni par un opérateur de téléphonie sur IP, permettant aux entreprises qui ont une standard IP (IPBX / PBX IP) d'utiliser la VoIP afin de faire transiter leurs appels entrants et/ou sortants, à partir d'une connexion sur le réseau Internet Haut Débit via le protocole SIP.

Dans cette partie nous allons nous concentrer sur une solution VOIP permettant la connexion du client qui'est dans notre cas la SOTETEL avec le réseau téléphonique commuté (PSTN).

- **Architecture :**

Nous proposons donc une architecture basée sur le trunk SIP et adaptée a notre solution MPLS/IP comme la montre la figure ci-dessous :

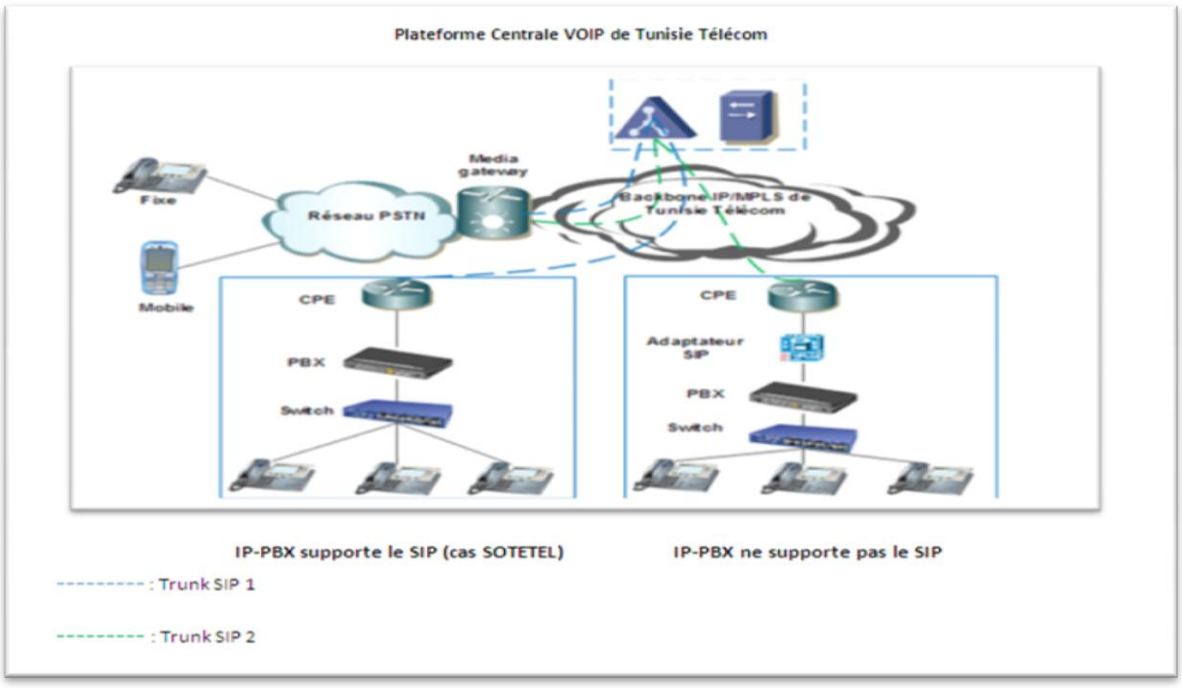

Figure 5.20 : Architecture de la solution Trunk SIP

L’architecture repose sur :

- Une plate-forme VOIP centrale Tunisie Télécom : Soft-Switch
- Des passerelles(les media Gateway) assurant l’interconnexion entre réseau IP et le réseau téléphonique commuté (PSTN)
- Les sites des clients seront raccordés au Backbone via des accès MPLS Corporate VPN
- des adaptateurs SIP.

- **Configuration :**

Pour mettre en évidence la connexion d’un client donné au PSTN nous avons effectué la configuration d’un Trunk SIP pour notre client qu’on nommera SOTETEL au niveau de la plate-forme centrale VOIP de Tunisie Télécom (SOFT-Switch) basée à Ouardia.

Les figures si dessous montrent les différentes étapes de configuration du Trunk SIP :

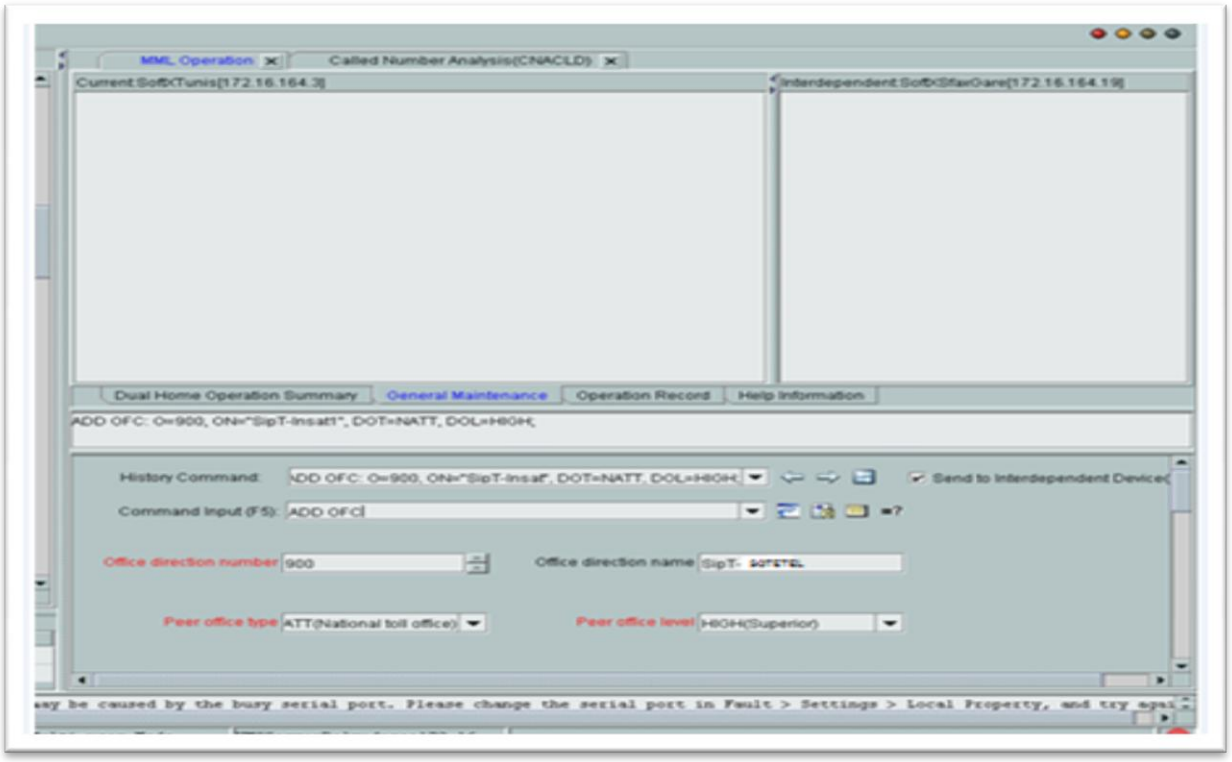

Figure 5.20 : Ajout d’un Trunk SIP

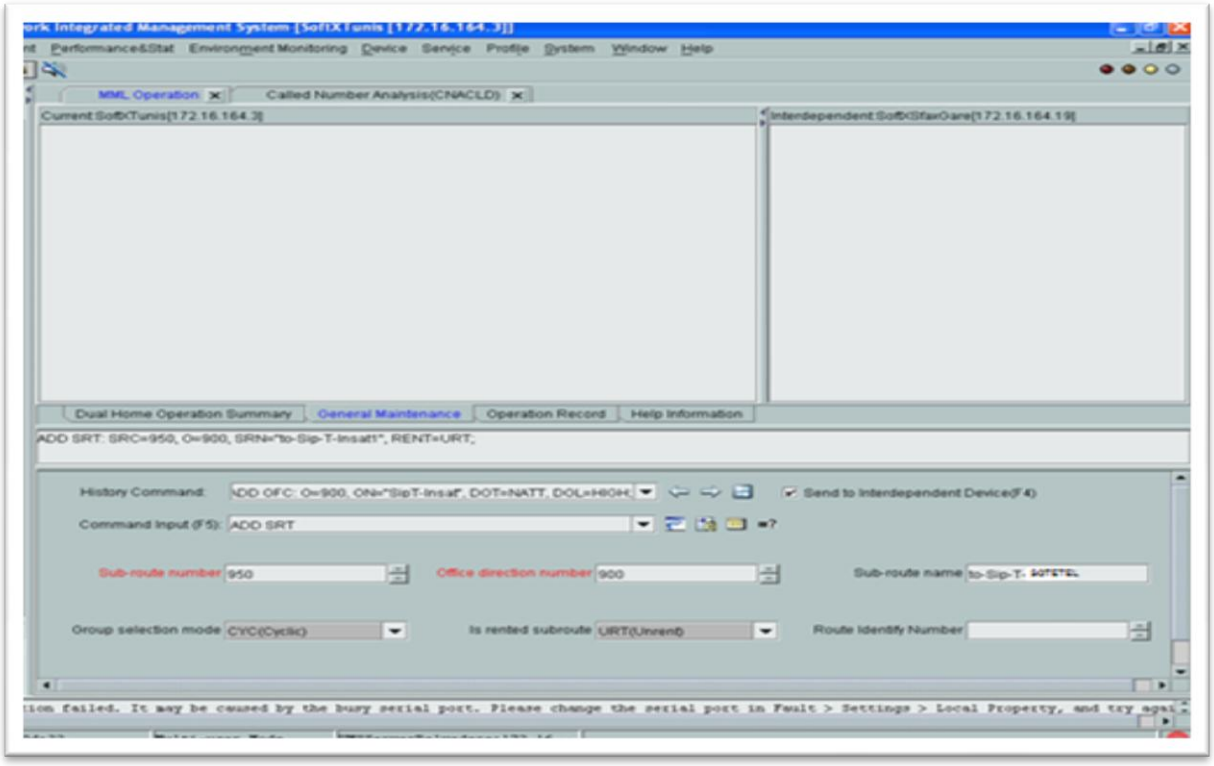

Figure 5.21 : Attribution d'une route

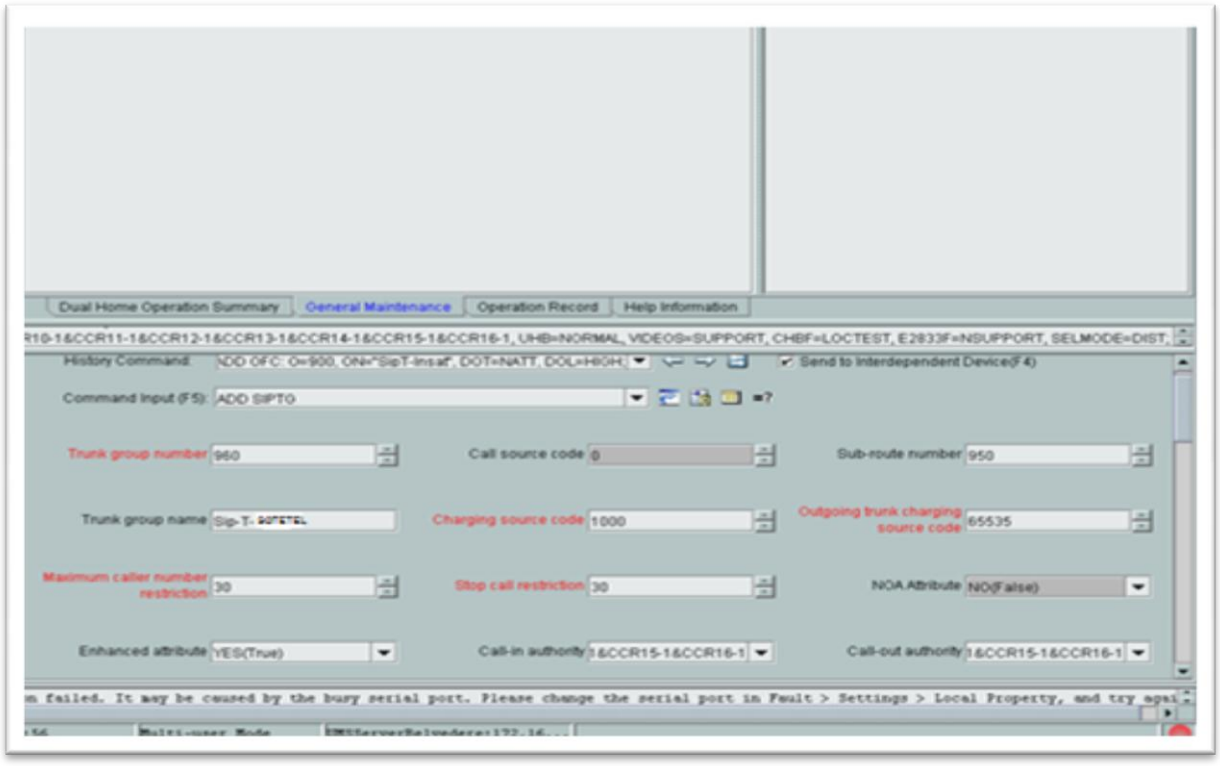

Figure 5.22: Choix des paramètres spécifiques au client

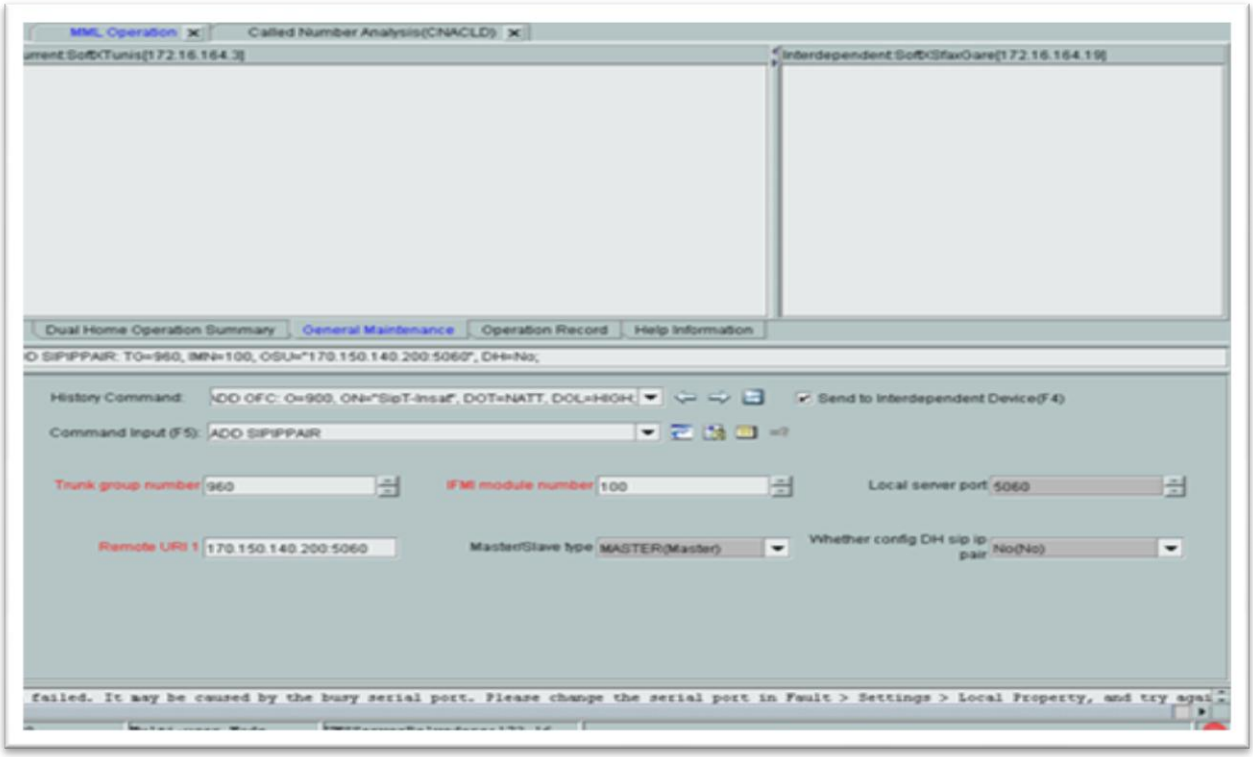

Figure 5.23: Attribution d'une adresse IP au Trunk SIP

V. Conclusion :

La VoIP est une application informatique comme les autres. A ce titre, elle est vulnérable et soumise à de nombreux risques, qui sont pour ainsi dire inexistants sur les réseaux « classiques », qu'il faut prendre en compte. La VoIP est une technique utilisée pour transporter de la voix sur tout réseau appliquant le protocole Internet par numérisation en paquets (données). Elle est, par conséquent, exposée aux mêmes menaces que celles touchant le transport de données, à savoir l'utilisation non autorisée des ressources, l'altération des données, l'introduction de données pirates, le détournement d'information, plus ou moins sensibles. Compte tenu de ces risques, il est essentiel que l'entreprise qui choisit de recourir à la VoIP mesure précisément l'étendue des atteintes potentielles à son activité et prenne les contremesures adaptées.

Conclusion générale

Au cours de ce projet, l'objectif était d'étudier, concevoir et mettre en place une solution de communication unifiée chez TUNISIE TELECOM. Dans cette démarche vers la communication unifiée on s'est intéressé principalement à la couche de transport par la conception et la configuration des routeurs au niveau de cette couche afin de migrer vers une solution MPLS/IP au sein de la Backbone Tunisie Télécom.

La simulation de cette solution a été testée avec succès, néanmoins cette solution peut être améliorée d'avantage en ne s'arrêtant pas au niveau de la couche transport et en tenant compte des nouveaux concepts qui se présentent actuellement a savoir le Cloud Computing.

Donc, ce travail peut être un début pour d'autres travaux qui peuvent nous présenter des solutions plus exhaustives qui s'étalent de la couche d'accès jusqu'à la couche des services.

Bibliographie

[1] Nemertes Research, *Concepts de communications en temps réel et applications commerciales*

[2] http://www.efort.com, *Réseaux et Services de Télécommunication Concepts, Principes et Architectures*

[3] Etude réalisée par le cabinet Ovum pour le compte de l Autorité de régulation des Communications électroniques et des Postes, *L'évolution du cœur de réseau des opérateurs fixes, Janvier 2006*.

[4] *Revue des Télécommunications d'Alcatel - 3e trimestre 2002*

[5] T. Berger, G. Marx: *"Une véritable évolutivité ", Revue des télécommunications d'Alcatel, 3e trimestre 2002, pp. 194-198 (ce numéro).*

[6] F. Jahanian et al: *"Experimental study of Internet stability and Wide Area Backbone failures", University of Michigan, 1999.*

[7] Séminaire régional UIT/BDT pour la région arabe sur la convergence des services fixes et mobiles et les nouvelles architectures des réseaux, *Nouvelles générations des réseaux favorisant la convergence des services "Expérience de Tunisie Télécom*

[8] *http://labo-cisco.com/uploads/concepts/pdf/labocisco_2007_Architecture_reseau_MPLS.pdf*

Annexe : commandes CISCO

Commande Cisco	Description
router (config) # router OSPF *process-id*	activer le protocole OSPF sur le routeur avec le choix d'un numéro de processus.
router (config) # router OSPF *process-id* **vrf** *vrf-name*	Activer le protocole OSPF avec une vrf particulière
router (config-router) # network *address wildcard-mask* **area** *area-id*	ajouter un réseau pour le routage OSPF. *Address :* Peut être une adresse réseau, sous réseau ou une adresse d'interface *wildcard-mask :* C'est le masque générique *Area-id :* Spécifier l'area associé à l'adresse
router (config) # router BGP *as-number*	activer le protocole de routage en spécifiant le nombre du système autonome.
router (config-router) # Address-family ipv4 vrf *vrf-name*	sélectionner du protocole de routage une instance de VRF.
router (config-router) # Address-family vpnv4	sélection de la configuration d'une VRF pour le protocole de routage BGP
router (config-if) # Ip vrf forwarding *vrf-name*	Assigner une l'interface à une VRF
router (config) # Ip vrf *vrf-name*	Créer une VRF
router (config-router-af) # Neighbour *ip-address* **activate**	Activer l'échange des routes vpnv4 avec le voisin spécifié
router (config-	le saut suivant pour le
Neighbour *ip-addres*	
router (config-route *ip-address* **remote-as**	e des voisins pour MP

router (config-router-af) # Neighbour *ip-address* **send-community both**	Spécifier la nature de la communité qui doit être envoyée au voisin BGP
router (config-router) # Neighbour *ip-address* **update-source**	Permettre la session IBGP d'utiliser n'importe quelle interface opérationnelle pour les connexions TCP
router (config-vrf) # Rd *value*	Assigner un RD à une VRF
router(config-vrf) # Route-target import | export *value*	Assigner un RT à une VRF
router (config) # ip cef	permettre l'utilisation de la technique de commutation Cisco Express Forwading (CEF).
router (config-subif) # mpls ip	activer la commutation MPLS
router (config-subif) # mpls label protocol {ldp | tdp | both}	spécifier le protocole de distribution de label sur l'interface approprié.
router (config) # redistribute bgp *as-number* **subnets**	Redistribuer les routes BGP (incluant celles des sous réseaux) en OSPF