MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention du diplôme d'Ingénieur d'Etat en Electronique

Option : Communication

Thème

L'étude des protocoles IP, application à l'établissement d'une connexion entre le softswitch de Tizi ouzou et le media Gateway de Boumerdes.

Présenté par :

M^elle^ Y. ZOHRA
M^elle^ S. ANIA

Proposé par :

Mr. KAROUCHE
Mr. YASSA

Dirigé par :

Mr. AIT BACHIR

PROMOTION 2010/2011

Remerciements

Nous tenons avant tout de remercier le bon DIEU qui nous a donnée le courage pour terminer nos études et élaborer ce modeste travail.

C'est un devoir bien agréable que de venir rendre hommage, au terme de ce travail, ceux sans lesquels il n'aurait pas pu être réalisé.
L'occasion nous est offerte de remercier, les personnes qui nous feront l'honneur de participer au jury chargé de juger ce travail.

Nous tenons tout particulièrement à exprimer notre profonde gratitude à **Mr AIT BACHIR,** Notre promoteur pour son aide précieux, son soutien et son professionnalisme.

Nous tenons en outre à remercier **Mr KAROUCHE** et **Mr YASSA,** d'avoir acceptés de nous encadrer et nous guider tout au long de ce projet, et pour leurs attentions qu'ils ont bien voulu nous accorder aux diverses étapes de son élaboration, pour leurs estimables aides et leurs précieux conseils.

Nous ne manquerons pas de saluer tous ceux qui ont de près ou de loin participé à l'accomplissement de ce travail.

Dédicace

A mes Chers Parents

Aucun hommage ne pourrait être à la hauteur de l'amour

Et de l'affection dont ils ne cessent de me combler.

Qu'ils trouvent dans ce travail

Un Témoignage de mon profond amour et éternelle reconnaissance.

Que dieu leur procure bonne santé et longue vie.

A mes chers frères : Hanin et Assalas

A ma chère sœur Massicilia

A tous mes cousins et mes cousines

A toute ma famille ;

A toutes mes copines: Zoro, Kary, Djomaila, Souàde…

A tous mes amis

A tous ceux qui m'aiment

A tous ceux que j'aime.

Je dédie ce modeste travail

Ania.

Dédicace

A la mémoire de mon cher Père Rachid

A ma chère Mère Ouisa

Aucun hommage ne pourrait être à la hauteur de l'amour

Et de l'affection dont ils ne cessent de me combler.

Qu'ils trouvent dans ce travail

Un Témoignage de mon profond amour et éternelle reconnaissance.

Que dieu leur procure bonne santé et longue vie.

A ma chère grand-mère : Sadia

A mes chers frères : Ahmed, Mustapha et Atman

A ma chère sœur : Lila

A ma chère belle sœur : Chahrazed

A ma petite nièce que j'adore : Malek

A mon cher fiancé :Mouh et toute sa famille.

A toute ma famille ;

A toutes mes copines : Ania, Tato, Zineb ,Koka

A tous mes amis : Mourade…

A tous ceux qui m'aiment

A tous ceux que j'aime.

Je dédie ce modeste travail

Zoro.

Sommaire

Introduction générale ……. 1

Chapitre I : Les réseaux de télécommunications

Introduction …….. 3

1 - Le réseau …….. 3

1.1 - Buts d'un réseau …… 3

1.2 - Eléments des réseaux ……. 3

1.3 - Les fonctions d'un réseau …….. 4

1.4 - Architecture physique des réseaux …… 4

2- Réseau de communication …… 4

2.1- Réseaux d'ordinateurs …… 4

2.1.1- Classifications et aperçus des réseaux ……. 5

2.1.2- Eléments dédiés ……. 5

2.1.3- Topologie des réseaux locaux LAN ……. 6

2.1.3.1- Configuration en BUS …… 7

2.1.3.2- Configuration en anneau ……. 7

2.1.3.3- Configuration en étoile ……. 8

2.2-Réseaux de télécommunication …… 8

2.2.1- Réseau téléphonique commuté (RTC) …….. 8

2.2.2- Réseaux NGN …… 9

2.2.2.1 - Définition de NGN ……. 10

2.2.2.2- Pourquoi le NGN ? …….. 12

2.2.2.3- Architecture de NGN ……... 12

2.2.2.4- Les entités fonctionnelles du cœur de réseau NGN ……. 14

2.2.2.5- Types d'NGN ……... 15

2.2.2.6-Avantages du NGN ……... 16

2.2.2.7- Les familles des protocoles d'un réseau NGN …… 16

2.2.2.8- Les services offerts par les NGN …… 19

Conclusion …… 21

Chapitre II : Les réseaux IP

Introduction …….. 22

1- Protocole TCP/IP ……. 22

1.1- L'origine de TCP/IP …… 22

1.2- La suite des protocoles de TCP/IP ……. 23

1.3 - Les protocoles de la couche transport …….. 24

1.3.1- Protocole TCP …… 24

1.3.2 - Le protocole UDP ……. 27

1.4 - Les protocoles de la couche réseau …… 28

14.1- Protocole IP …… 28

1.4.2- Le protocole ICMP …….. 31

1.4.3- Protocole IGMP …… 32

1.5 - Les protocoles de la couche physique …… 32

1.5.1- Le protocole ARP ……. 32

1.5.2- Le protocole RARP …….. 32

1.6 - Les protocoles de la couche application …….. 33

1.6.1- Le protocole FTP ……..…….. 33

1.6.2- Le protocole HTTP ……..……. 33

1.6.3- Le protocole Telnet ……..……. 33

1.6.4- Protocole RIP2 ……..…… 33

1.6.5- Protocoles SLIP et PPP ……..…… 34

1.6.5.1- Le protocole SLIP ……..…….. 34

1.6.5.2- Le protocole PPP : Point To Point Protocol ……..……..... 34

1.6.6- Domain Name System (DNS) ……..…… 34

1.7 - Protocole IPv6 (l'avenir d'IP) ……..……..... 34

2- Adressage IP ……..……..... 35

2.1- L'espace d'adressage ……..……..... 36

2.2- Le masque de sous réseau ……..……..... 37

2.3- L'adresse de diffusion (broadcast) …..……..... 38

2.4- Le sous adressage …..……..... 38

2.5- Les classe d'adresses IP ……..... 38

2.6- Les adresses IP conventionnelles (Adresses réservées) 41

2.7- Le ROUTAGE ……..... 42
2.7.1- Routage IP ……..... 42
2.7.2-Tables de routage ……..... 42
2.7.3- Routage dynamique ……..... 42
2.7.4- Routage statique ……..... 43
2.7.5- Le routage inter domaine sans classe 43
2.8- Types d'adresses ……..... 43
2.8.1- L'adresse de broadcaste d'un réseau local 43
2.8.2- Adresse multicast ……..... 43
2.8.3- Adresse unicast ……..... 44
Conclusion ……..... 44

Chapitre III : Généralités sur la VOIP et les protocoles de signalisations

Introduction ….....
1- La voix sur IP 45
1.1- Définition et vue d'ensemble 45
1.2- Fonctionnement 46
1.3- Le processus de traitement de la voix IP 47
1.4- Les paramètres de la voix sur IP 48
1.4.1- Les différents échantillonnages 49
1.4.2- Optimisation de la bande passante 49
1.4.3- La gigue de phase 49
1.4.4- Le phénomène d'écho 49
1.4.5- Les pertes de paquets 49
1.4.6- La sécurité 49
1.5- Les protocoles de transport de la VOIP 50
1.6- Quel est l'avantage de VOIP sur RTCP 50
1.7 - Caractéristique de la voix 50
1.8- Les modes d'accès différentes architectures 51
1.8.1- D'un ordinateur à un ordinateur 51
1.8.2- Dun PC à un poste téléphonique 52
1.8.3-Poste téléphonique à un poste téléphonique 52
1.9 - Avantages et inconvénients de la téléphonie IP 53

1.10- Avenir de téléphonie IP 54
2- Les protocoles de la voix IP 54
2.1- Le Standard H.323 54
2.1.1- Les élément 54
2.1.2-Protocoles et procédures 56
2.1.3- La pile H323 58
2.1.4- Conférence de données 59
2.1.5- Mécanismes de contrôle et de signalisation 59
2.2- Standard SIP 62
2.2.1- Capacités de SIP 63
2.2.2- Composants SIP 63
2.2.3- Comment SIP fonctionne 65
2.2.3.1- Comment SIP fonctionne avec un Proxy Server 66
2.2.3.2- Comment SIP fonctionne avec un Redirect Server 67
2.2.4- Communications SIP 68
Conclusion 73

Chapitre IV : Partie pratique

Introduction …….. 74
1- Simulation par le logiciel Packet tracer 74
1.1-Représentation de logiciel packet tracer 75
1.1.1- Les étapes à suivre 76
1.1.2- Procédure de configuration du routeur R1 78
1.1.3- Procédure de configuration du routeurR2 78
1.1.4- Résultats Obtenus De Configuration Des Routeurs et les swicths 79
2- L'architecture de système du traceur d'appels 84
2.1- Architecture logique 84
2.2- Architecture matériel 85
2.3- Partie pratique 85
2.3.1- Résultats de traceur d'appel de protocole SIP 85
Conclusion …… 94
Conclusion générale 95
Bibliographie 100

Liste des figures

Chapitre I : Les réseaux de télécommunications

Figure I.1 : Topologie bus ……... 6

Figure I.2 : Topologie Anneau ……..... 6

Figure I .3 : Topologie Etoile ……..... 7

Figure I.4 : Réseau RTC ……..... 8

Figure I.5 : Architecture en couche de réseau NGN ……..... 10

Figure I.6 : Architecture simplifiée des NGN ……..... 12

Figure I.7 : Les familles de protocoles d'un réseau NGN ……..... 16

Chapitre II : Les réseaux IP

Figure II.1 : La suite de protocole TCP / IP ……..... 23

Figure II.2 : En-tête TCP ……..... 25

Figure II.3 : En-tête UDP ……..... 28

Figure II.4 : En-tête IP ……..... 30

Figure II.5 : Forma d'adressage (classe A) ……..... 39

Figure II.6 : Forma d'adressage (classe B) ……..... 39

Figure II.7 : Forma d'adressage (classe C) ……..... 40

Figure II.8 : Forma d'adressage (classe D) ……..... 40

Chapitre III : Généralités sur la VOIP et les protocoles de signalisations

Figure III.I : Processus de traitement de la VOIP 47

Figure III.2 : Téléphonie de PC à PC ……..... 52

Figure III.3 : Téléphonie entre PC et poste téléphonique 52

Figure III.4 : Téléphonie entre postes téléphoniques 53

Figure III.5 : La pile de protocole du terminal H.323 58

Figure III.6 : L'architecture d'un réseau SIP 64

Figure III.7 : Requête SIP à travers un Proxy Server 66

Figure III.8 : Requête SIP à travers un Proxy Server 66

Figure III.9 : Requête SIP à travers un Proxy Server 67

Figure III.10 : Requête SIP à travers un Redirect Server 67

Figure III.11 : Requête SIP à travers un Redirect Server 68

Chapitre IV : Partie pratique

Figure IV.1 : simulation d'un réseau par packet tracer 75

Figure IV.2 : Représentation de packet tracer version 5.0 76

Figure IV 3 : Architecture de logiciel traceur d'appel 84

Le développement rapide de l'internet et l'utilisation croissante des réseaux fondés sur le protocole Internet (IP) pour les services de communications, y compris pour les applications telles que la téléphonie, sont devenus des domaines importants pour l'industrie des télécommunications. La possibilité d'acheminer du trafic vocal et de la voix-données constitue un point de convergence entre deux technologies : la commutation de circuits et la commutation de paquet.

L'apparition récente de la transmission de la voix et de la vidéo sur IP représente une avancée technologique importante dans le domaine du multimédia et offre un service conçu pour permettre aux compagnies d'utiliser leurs réseaux Internet pour y faire passer leur trafic de la voix sans nécessiter de changement des équipements ou réseaux existants.

En d'autre terme, l'ajout de quelques équipements tels que les passerelles permettent de garder les mêmes supports, utilisés auparavant pour acheminer les communications téléphoniques, pour véhiculer la voix, la vidéo et les données. Cette technologie exige des protocoles spécialisés dédiés à ce genre d'applications, comme le protocole de transport en temps réel RTP utilisé en parallèle avec d'autres protocoles qui concernent surtout la signalisation, la demande de réservation de ressources, la négociation de capacité comme le standard H.323 et le Protocole d'Initiation de sessions (SIP).

Aujourd'hui, la technologie de la téléphonie sur IP a produit plusieurs services basés sur les différents scénarios de communication (téléphonie PC à PC, téléphonie entre un PC et un poste téléphonique et téléphonie entre postes téléphoniques ou fax). En conséquence, cette technologie est devenue un outil de communication multimédia basé sur le réseau internet, intégrant des outils d'interfaces avec les réseaux téléphoniques traditionnels.

Les analystes spécialistes des questions techniques annoncent depuis plusieurs années que toutes les formes de communications fusionneront tôt ou tard en une plate- forme unique et, depuis quelques années, il semble évident qu'avec la technologie IP adoptée, qu'elle soit bien la plate-forme unificatrice de tous les réseaux de communications sur internet. De même, le marché de la voix et de la vidéo sur IP a ouvert plusieurs perspectives en ce qui a trait à la téléphonie sur IP, téléconférence, transferts de données etc. Et a contribué à la réduction des prix des communications internationales grâce à la concurrence. L'importance de cette technologie et l'avenir qui lui est réservé nous a encouragés à s'impliquer dans ce domaine avec enthousiasme.

Notre objectif majeur derrière ce travail est la conception d'un modèle théorique du protocole de signalisation SIP et H.323.

Ces deux protocoles sont utilisés dans des applications de voix et vidéo conférence. Nous passerons en revue aussi les protocoles de transmission et de contrôle en temps réel RTP et RTCP qui sont mis en jeu dans la transmission et la réception des données en temps réel et le contrôle des flux.

Ce mémoire est organisé en quatre chapitres.

Le chapitre I, présente une généralité sur les réseaux de télécommunication ainsi que nous donnons un petit aperçu sur les réseaux téléphonique commuté (RTC) et sa migration vers NGN.

Le chapitre II, est consacré à une brève étude sur la suite de protocole TCP/IP. Puis un petit aperçu sur les adressages IP.

Le chapitre III, concerne des généralités sur les voix IP et une brève étude sur les protocoles de signalisation H.323 et SIP.

Le chapitre IV, est consacré à la partit pratique qui consiste au résultat obtenus de logiciel tracer d'appels et ensuite nous parlerons de la simulation par packet tracer.

Nous finirons ce mémoire par une conclusion générale.

Introduction:

Le domaine des télécommunications est vaste et varié. Le premier risque à éviter est celui de la confusion. Il est donc nécessaire d'organiser l'approche de ce domaine en posant des définitions claire

1 - Le réseau :

L'ensemble des moyens physiques utilisables par des usagers qui bénéficient d'un même service s'appelle un réseau. Certains types de réseau sont utilisés pour des services de diffusion (radio, télévision) ou de collecte (télémesure, télésurveillance) qui sont des services unilatéraux.

1.1 - Buts d'un réseau :

-Echanges entre personnes : Messagerie, news, Internet, transfert de fichiers, accès à des bases de données (bibliothèques).

-Partage d'équipements (souvent coûteux) : Imprimantes, disques, super calculateurs.

1.2 - Eléments des réseaux :

- *Objets matériels* :
  - → Liens : Support : paire torsadée, câble coaxial, fibre optique, ondes hertziennes.
- Domaine privé ou public (opérateur Algérie Télécom).
  - → Boites pour connecter ou interconnecter les liaisons : nœuds, routeurs, commutateurs, répéteurs, …
- *Langages : Protocole* :
  - → Pour que chaque élément puisse dialoguer avec son homologue. A tout "niveau" : Signaux électriques, trame, fonctions dans les applications.
  - *Lois internationales* : Normes et Standards : Pour assurer la possible hétérogénéité des éléments, la pérennité et l'ouverture.

1.3 - Les fonctions d'un réseau :

- La transmission : Point à point ou diffusion.
- La commutation : Comment mettre en relation un utilisateur avec n'importe quel autre ?
- La signalisation : Repose sur l'échange d'informations de « services »
- L'administration et la gestion : Détection des fautes
- Facturation au prix juste
    - Configuration : nouveaux matériels, nouveaux utilisateurs
    - Performances et qualité de services
    - Sécurité

1.4 - Architecture physique des réseaux

Du point de vue de l'utilisateur deux grands réseaux s'imposent :

- Le réseau téléphonique ;
- Le réseau Internet.

Ces deux exemples sont typiques de deux classes de réseaux :

- Les réseaux de télécommunication ;
- Les réseaux d'ordinateurs.

On parle depuis 30 ans de convergence entre les télécommunications et l'informatique mais les deux types de réseaux, bien que basés sur les mêmes technologies et malgré leur complémentarité et leur interdépendance, restent assez différents en termes de services rendus, terminaux employés et coûts d'utilisation.

2- Réseau de communication:

Ensemble de ressources (artères de transmission, commutateurs, …) mis à la disposition d'équipements terminaux pour leur permettre d'échanger de l'information

2.1- Réseaux d'ordinateurs :

- Ensemble d'ordinateurs autonomes interconnectés au moyen d'une seule technologie.
- Applications situées sur les ordinateurs.
- Permet la transmission de textes, images, vidéos, sons entre les ordinateurs.

2.1.1- Classifications et aperçus des réseaux :

Selon la taille :

- PAN - *Personal Area Network* - réseau personnel.
  - 1 m : liaison sans fil ordinateur/souris, clavier, imprimante, …
  - contrôle appareil auditif, stimulateur cardiaque, …
- **LAN** - *Local Area Network* - réseau local.
  - 10 m/1 km : salle/immeuble/campus
- **MAN** - *Metropolitan Area Network* - réseau métropolitain.
  - 10 km : ville
- **WAN** - *Wide Area Network* - réseau longue distance.
  - 100 km/1 000 km : pays/continent
- **Internet**
  - 10 000 km : planète, interconnexion de réseaux.

2.1.2- Eléments dédiés :

- Concentrateur :
  - Il permet le partage de voies entre plusieurs utilisateurs.
  - Il analyse le contenu de la trame.
  - Peut effectuer des conversions de protocoles.
  - Peut effectuer des opérations d'aiguillage.
- Modems :
  - Modulation/démodulation des signaux numériques.
  - Fonctionne au niveau de la couche physique.
- Répéteur :

  Amplificateur de signal.
  - Pallier au problème de l'atténuation du signal.
  - Reproduit un signal provenant d'un port sur les autres ports.
  - Fonctionne au niveau de la couche physique.
  - Pas de filtrage, pas d'interprétation du signal.
- Hub :
  - Appareil qui diffuse un signal reçu sur un port sur tous les autres ports. C'est un concentrateur de câblage.
  - Hub passif : espèce de prise multiple, pas de composants électroniques.

- Hub actif : analyse et contrôle du flux d'information ; capable d'épurer et d'amplifier les signaux électroniques.

- Pont :

  - Appareil qui mémorise et retransmet des trames au niveau local.

  - Certains peuvent effectuer du filtrage voire même du routage.

    - Le répéteur passe tous les signaux tandis que le pont est plus sélectif et ne passe que les signaux destinés à un ordinateur situé de l'autre côté.
    - Il opère au niveau de la couche MAC (sous-couche de la couche Liaison).

- Routeur :

  - Appareil qui transmet des paquets d'un réseau à un autre.
    - Couche réseau du modèle OSI.
    - Le routeur est l'équipement le plus adapté aux interconnexions longues distances (WAN).
    - Cependant, il peut dans certains cas faire office de pont.

- Passerelle :

  -Appareil qui convertit les paquets d'un protocole en paquet d'un autre protocole.

  - Couche transport ou supérieure du modèle OSI.

2.1.3- Topologie des réseaux locaux LAN :

La topologie définie la façon dont seront connectés (le câblage) les différents ordinateurs composant le réseau.

2.1.3.1- Configuration en BUS :

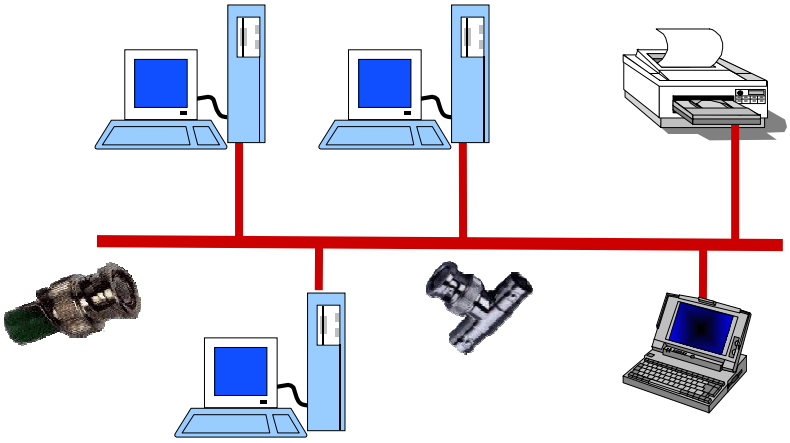


Figure I.1: Topologie bus

Le réseau Bus. C'est un réseau où tous les correspondants sont reliés à un même support de communication. C'est aussi une des architectures les plus évolutives car il suffit de se« piquer » au réseau pour ajouter un nœud.

2.1.3.2- Configuration en anneau :

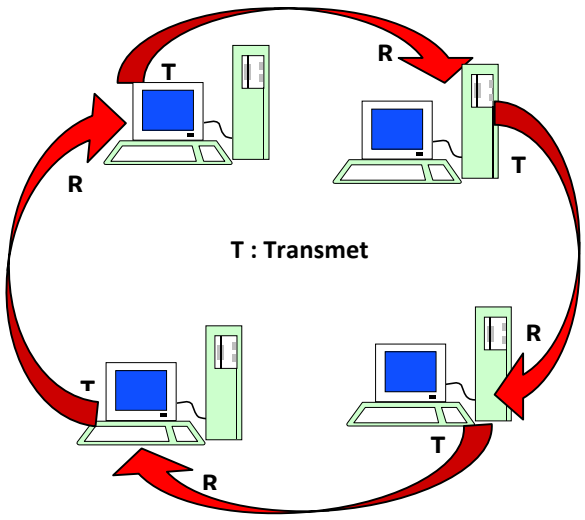


Figure I.2: Topologie Anneau

Le réseau en ***Anneau***. C'est une architecture où chaque site est relié à un suivant, et ne transmet des messages qu'à ce dernier. Comme le réseau est bouclé sur lui-même, tout message peut passer depuis tout site source vers toute destination.

2.1.3.3- Configuration en étoile :

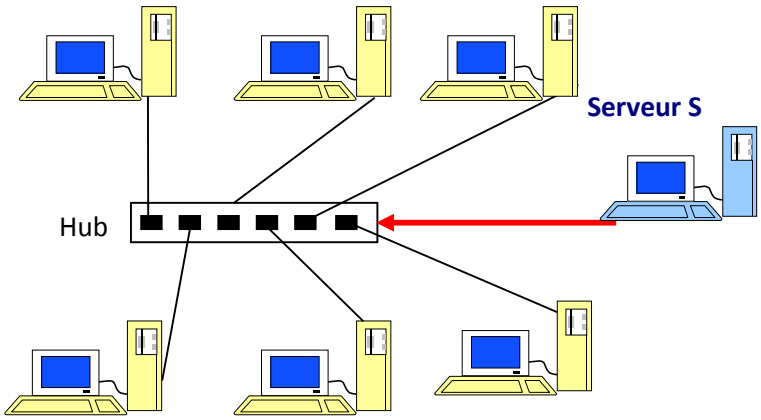


Figure I .3 : Topologie Etoile

C'est une architecture où tous les messages transmis passent par un serveur (S) qui redistribue ensuite les messages entre les sites tout en gérant le réseau et les périphériques.

Équipement spécial : ***hub***

2.2-Réseaux de télécommunication :

2.2.1- Réseau téléphonique commuté (RTC) :

C'est un réseau du téléphone fixe dans lequel un poste d'abonné est relié à un central téléphonique par une paire de fils alimentée en batterie centrale (la boucle locale) les centraux sont eux-mêmes relies entre eux par des liens offrant un débit de 2Mb/s.

Le RTC appelé aussi réseau téléphonique tradition, utilise la commutation de circuit (aussi nommé transmission TDM) est caractérisé par l'établissement d'une liaison bidirectionnelle entre deux extrémités du réseau pendant toute la durée de la communication, assurant la continuité du transfert de l'information en temps réel.

Le principal inconvénient de cette méthode de commutation est qu'elle gaspille de la capacité en bande passante puisque la ligne ne peut être utilisée que pour cette communication.

Le réseau RTC est ainsi divisé en plusieurs sous-ensembles suivant un découplage en différentes zones :

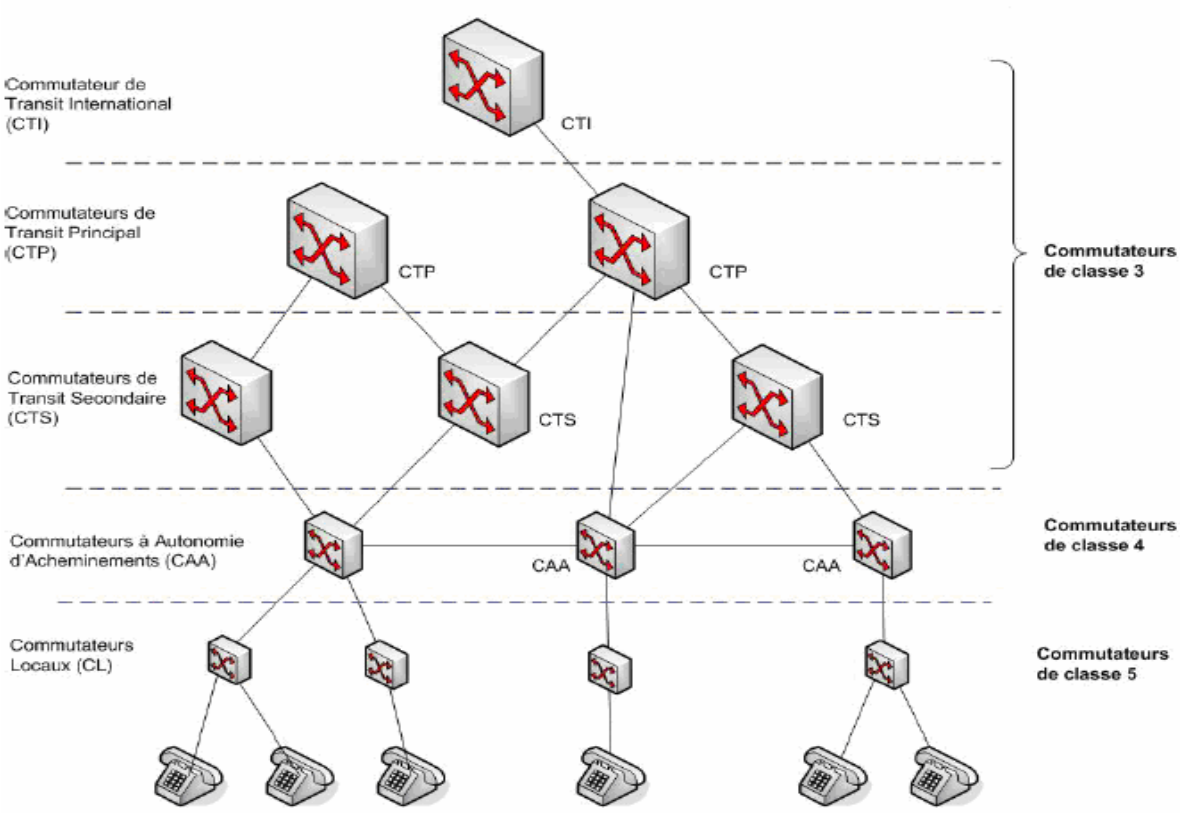


Figure I.4: Réseau RTC

- Zone Locale (ZL) :

Dans la zone locale, les abonnés sont raccordés à un même commutateur local (CL). Les CL établissent les connexions entre les lignes d'abonnés et leurs CAA (Commutateur à Autonomie d'Acheminement). Dans l'étude, nous parlerons de commutateurs de classe 5 en référence au CL.

- Zone à Autonomie d'Acheminement (ZAA) :

Une zone ZAA est une zone géographique formée par un ensemble de ZL appartenant à une même zone. Les commutateurs qui équipent une ZAA sont des CAA. Ils

gèrent la commutation de circuit et l'acheminement du trafic entre différentes ZL et entre différents CAA d'une même zone ZAA.

Dans l'étude, nous parlerons de commutateurs de classe 4 en référence aux CAA.

- Zone de Transite (ZT) :

Il y a plusieurs zones de transit selon que l'on se trouve à un niveau régional, national ou international.

- Zone de Transit Secondaire (ZTS) :

Une « ZTS » est délimitée par un ou plusieurs « CTS » (Commutateurs Transit Secondaires) qui gèrent un ensemble de « CAA » situés dans la zone considérée.

Les commutateurs « CTS » n'intègrent aucune intelligence et assurent uniquement le brassage des circuits lorsqu'un « CAA » peut directement atteindre le CAA du destinataire.

- Zone de Transit Principale (ZTP) :

Une « ZTP » regroupe plusieurs « ZTS » est inclues un « CTP » (Commutateur de Transit Principal) qui gèrent les « CTS » de la zone. Cette zone assure la commutation des liaisons longue distance.

- Zone de Transit International (ZTI) :

Elle est reliée à un Commutateur de Transit International (CTI) permettant de traiter le trafic provenant ou à destination de l'international.

La problématique de passage à une architecture « NGN » (Next Generation Network) du cœur de réseau fixe des opérateurs historiques s'inscrit avant tout dans une logique de diminution des coûts avec le passage à une infrastructure basée sur IP pour le transport de tout type de flux, voix et données, et pour toute technologie d'accès (DSL, RTC, Wifi, …). L'impact majeur d'un passage à une architecture NGN pour les réseaux de téléphonie commutée et que le commutateur traditionnel est scindé en deux éléments logiques distincts : le média Gateway pour assurer le transport et le softwitchen pour assurer le contrôle d'appel.

Cette évolution permet théoriquement des gains en termes de performance et d'optimisation des coûts, mais elle peut aussi faciliter le déploiement de nouveaux services.

2.2.2- Réseaux NGN

2.2.2.1 - Définition de NGN :

Il s'agit d'un réseau en mode paquet faisant intervenir plusieurs technologies de transit large bande à qualité de service imposé, qui permet aux utilisateurs d'avoir accès sans restriction aux réseaux et aux fournisseurs de service concurrents de leurs choix.

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

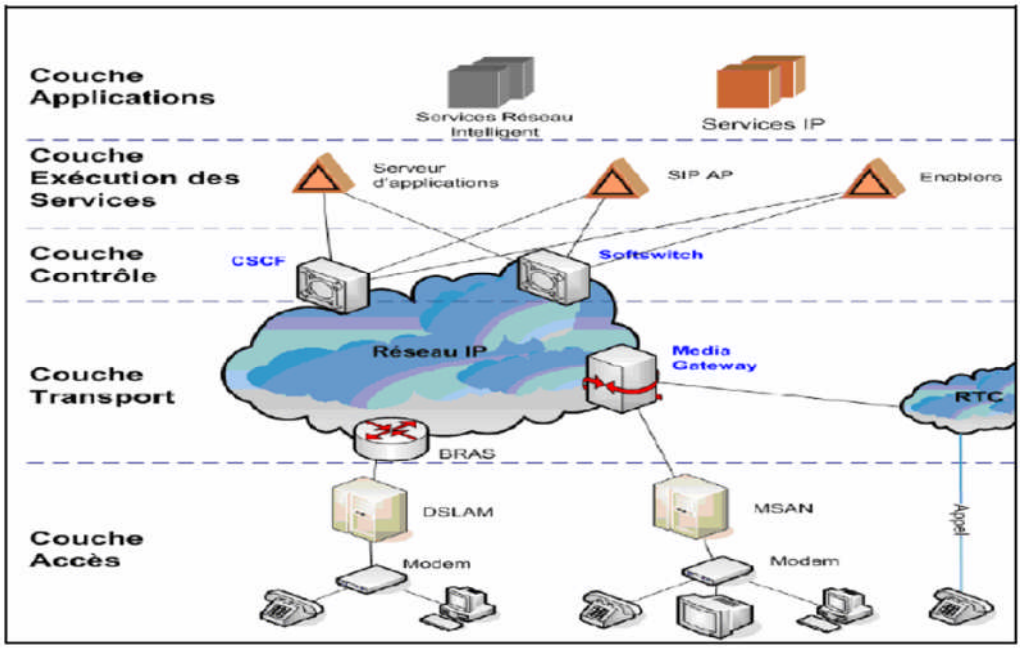


Figure I.5: Architecture en couche de réseau NGN

Couche d'accès :

Elle permet l'accès de l'utilisateur aux services via des supports de transmission et collecte divers : câble, cuivre, fibre optique, boucle locale radio, x DSL, réseau mobiles.

Couche transport :

Elle gère l'acheminement du trafic vers sa destination. En loi dure de réseau de transport des « Média Galway » et des « Signalling Gateway » gèrent respectivement la

conversion de flux de données et de signalisation aux interfaces avec les autres ensembles réseaux ou les réseaux tiers interconnectés.

Couche de contrôle :

Elle se compose de serveurs dits « Softswich » gérant d'une part les mécanismes de contrôle d'appel (pilotage de la couche transport, gestion d'adresses) et d'autre part l'accès aux services (profils d'abonnés, accès aux plates-formes de services à valeurs ajoutées).

Couche de service :

Elle regroupe les plates formes d'exécution de services et de diffusion de contenant. Elle communique avec la couche contrôle du cœur de réseau via des interfaces ouvertes et normalisées, indépendantes de la nature du réseau d'accès utilisé.

2.2.2.2- Pourquoi le NGN ?

Dans certaines parties dans le monde, le trafic de données prend rapidement le pas sur le trafic vocal et la tendance est nettement à l'augmentation en bande passante pour les données, tandis que la voix peut se satisfaire d'une bande passante de 64Kbit/s. Les opérateurs possédant deux types de réseaux (réseaux voix et réseau de données) utilisant cet argument pour commencer à les réunir. Il est clair d'après les limites du réseau TDM (Time Division multiplexing) que le réseau de données survivra alors que le réseau TDM quittera la scène. Facteur non moins important, le nouveau besoin chez les usagers d'une variété encore plus grande d'application et de service sophistiqués (conférence audio et vidéo, messagerie unifiée, chat) dont la plupart n'étaient même pas envisagés lors de la création des réseaux actuels.

Pour les opérateurs, l'accès et le transport ne sont plus assez lucratif, et pour rester compétitif, il leur faudra donc offrir aux usagers toute une gamme de services utiles, faciles à utiliser et rémunérateurs. Par conséquent, les NGN seront axés sur les services, et fourniront tous les moyens nécessaires pour offrir de nouveaux et adapter les existants pour augmenter les recettes.

2.2.2.3- Architecture de NGN :

Les principales caractéristiques des réseaux NGN sont l'utilisation d'un unique réseau de transport en mode paquet (IP, ATM) ainsi que la séparation des couches de transport des flux et de contrôle des communications, qui sont implémentées dans un même équipement.

Pour un commutateur traditionnel. Ces grands principes et concernant les équipements actifs du cœur de réseau NGN se déclinent techniquement comme suit :

- Remplacement des commutateurs traditionnels par deux équipements distincts :
  - D'une part des serveurs de contrôle d'appel dits Softswitch ou Media Gateway Controller (correspondant schématiquement aux ressources processeur et mémoire des commutateurs voix traditionnels) .
  - D'autre part des équipements de médiation et de routage dits Media Gateway (correspondant schématiquement aux cartes d'interfaces et de signalisation et aux matrices de commutation des commutateurs voix traditionnels), qui s'appuient sur le réseau de transport mutualisé NGN.
- Apparition de nouveaux protocoles de contrôle d'appel et de signalisation entre ces équipements (de serveur à serveur, et de serveur à Media Gateway).

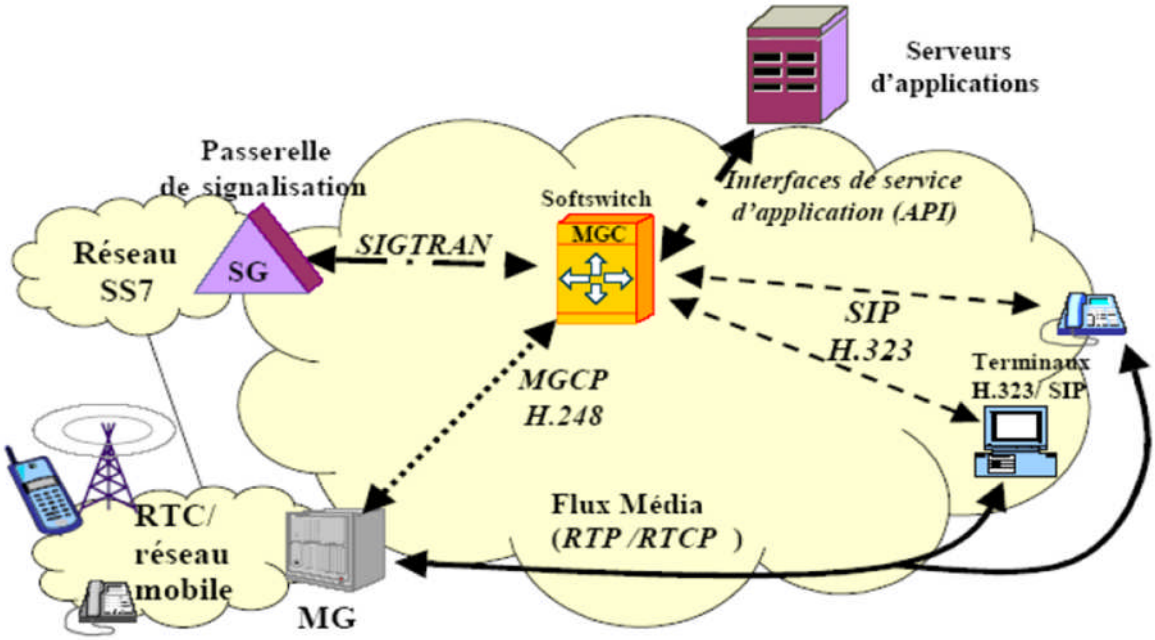


Figure I.6: Architecture simplifiée des NGN

La figure(I.6), représente la structure physique d'un réseau NGN avec les différentes entités fonctionnelles, les principaux réseaux d'accès ainsi que les différents protocoles mis en œuvre.

2.2.2.4- Les entités fonctionnelles du cœur de réseau NGN :

- Media Gateway (MG) :

Media Gateway constitue un élément essentiel déployé dans un réseau NGN. Il peut par exemple positionner entre le réseau de commutation de circuit et le réseau de commutation de paquet. Dans ce cas les médias Gateway transforment le trafic circuit TDM en paquets, la plupart du temps IP ou ATM, pour que ce trafic puisse ensuite être géré par le réseau NGN. En conséquence, plusieurs types de média Gateway sont disponibles sur le marché, en fonction du type de solution voix choisir l'opérateur et le rôle de ce média Gateway :

- Les passerelles VoIP pour convertir les lignes d'accès TDM en flux IP.
- Les passerelles VoATM pour convertir les lignes d'accès TDM en flux ATM.

D'une manière générale, une passerelle de média a pour rôle :

- Le codage et la mise en paquets du flux média reçu du RTC et vice-versa (conversion du trafic TDM / IP) .

- Signaling Gateway (SG) :

La fonction Singnaling Gateway a pour rôle de convertir la signalisation échangée entre le réseau NGN et le réseau externe interconnecté selon un format compréhensible par les équipements chargés de traiter, mais sans l'interpréter (ce rôle étant réservé au média Gateway contrôler.

Notamment, elle assure l'adaptation de la signalisation par rapport au protocole de transport utilisé (exemple : adaptation TDM/IP). Cette fonction est souvent implémentée physiquement dans le même équipement que le média Gateway.

Les Gateway ont un rôle essentiel : elles assurent non seulement l'acheminement du trafic, mais aussi l'interfonctionnement avec les réseaux externes et avec les divers réseaux d'accès en réalisant :

- La conversation du trafic (entité fonctionnelle média Gateway).
- La conversion de la signalisation associée (entité fonctionnel singnaling Gateway).

- Le Serveur d'Appel ou média Gateway (MGC) Controller :

Dans l'architecture des réseaux NGN, le serveur d'appel, aussi appelé « softswich » ou « media Gateway contrôler (MGC) » est le nœud central qui support l'intelligence de communication. Il s'agit d'un serveur informatique doté d'un logiciel de traitement d'appels vocaux. Il permet de gérer :

- L'échange de message de signalisation transmise de par et d'autre avec les passerelles de signalisation, et l'interprétation de la signalisation .
- Le traitement des appels : dialogue avec les terminaux H.323, SIP et MGCP, communication avec les serveurs d'application pour la fourniture des services .
- Le réservoir de ressources dans le MG et le contrôle des connexions internes au MG (commande des média Gateway) physiquement sofswitch peut être implanté sur un serveur dédié où bien être installé directement sur un équipement différent comme un média Gateway ou même un commutateur traditionnel TDM. Dans ce cas on parlera d'architecture complètement distribuée.

2.2.2.5- Types de NGN :

Il existe trois types de NGN, NGN classe 4, NGN classe 5 et NGN multimédia.

Les NGN classe 4 et 5, sont des architectures de réseau offrant uniquement les services de téléphonie. Il s'agit donc de NGN téléphonie.

Le NGN multimédia est une architecture offrant les services multimédia (messagerie vocale/vidéo, conférence audio/vidéo, voix/vidéo) puisque l'usager à un terminal IP multimédia. Cette solution est intéressante que les précédentes puisqu'elle permet à l'opérateur d'apporter en termes de services par rapport à une solution NGN téléphonie.

- La class 4 NGN permet :
    - Le remplacement des centres de transit de téléphonique (classe 4 Switch) .
    - La croissance du trafic téléphonique en transite.
- La class 5 NGN permet :
    - Le remplacement des centres téléphoniques d'accès (class 5 Switch).
    - La croissance du trafic téléphonique à l'accès.

Le NGN multimédia permet d'offrir des services multimédia à des usagers disposant d'un accès large bande tel que « xDSL, câble, wifi ».

2.2.2.6-Avantages de NGN :

Cette nouvelle topologie offres les avantages suivants :

- Grâce au NGN, l'opérateur dispose d'un réseau multi service permettant d'interfacer n'importe quel type d'accès (boucle local, PABX, commutateur d'accès téléphonique, accès ADSL, accès mobile GSM, téléphone IP, …).
- L'opérateur n'aura plus à terme qu'a exploiter un seul réseau multiservice .
- Elle utilise le transport comme IP ou l'ATM ignorant les limites de réseau TDM (Time Division Multiplixing) à 64Kbit/sc.
- Est une topologie ouverte qui peut transporter aussi bien les services téléphoniques que les services de multimédia (vidéo, données temps réel) .

2.2.2.7- Les familles des protocoles d'un réseau NGN :

Le fait d'utiliser un réseau paquet pour transporter des flux multimédia, ayant des contraintes « temps réel » à nécessité l'adaptation de la couche contrôle. Il faut noter que ces réseaux de transport uniquement, en ce sens n'offraient pas de services permettant la gestion des appels et des communications multimédia, cette évolution à logiquement générée de nouveau protocoles, principalement concernant la gestion des flux multimédia, au sein de la couche contrôle. Nous les classerons en trois grandes familles : Les protocoles de « contrôles d'appels » qui regroupent essentiellement « H.323 et SIP », les protocoles de « média Gateway » constitués par « MEGACO et MGCP » et les protocoles de « signalisation » entre MGC ,BICC, SIP-T, SIGTRAN.

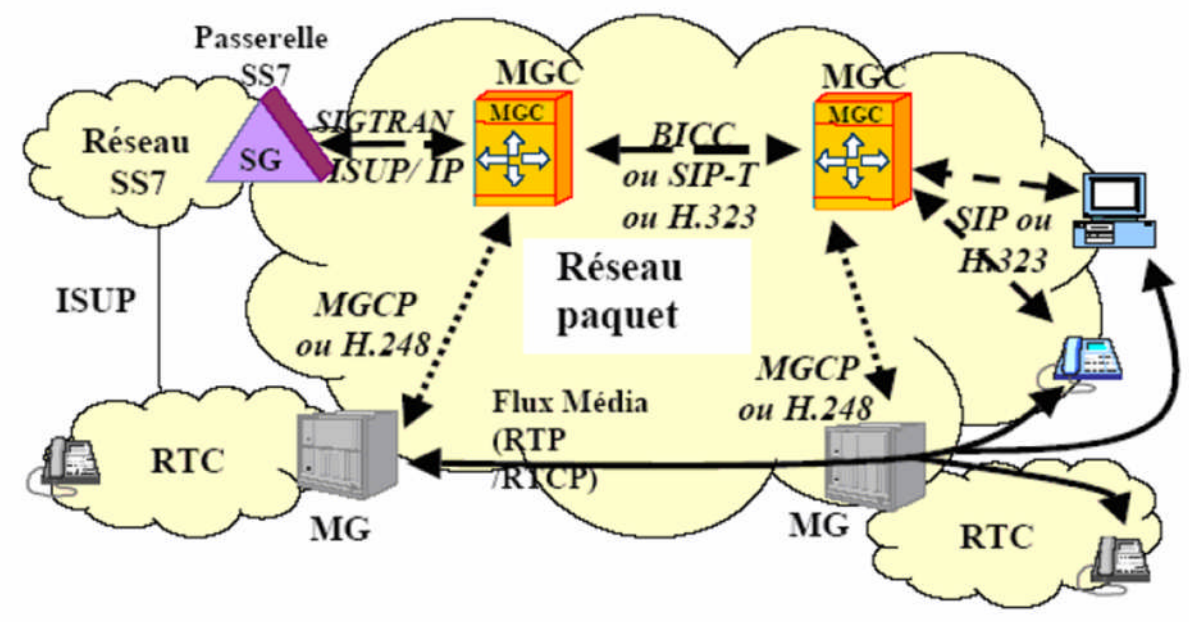


Figure I.7 : Les familles de protocoles d'un réseau NGN

➢ Les protocoles de contrôle d'appels :

Ils permettent l'établissement d'une communication entre deux terminaux et un serveur, les deux principaux protocoles concurrents sont H.323, norme de l'UIT et SIP standard développé à l'IETF. Etudions leurs spécifications respectives :

H.323 :

La recommandation « H.323 » décrit les procédures pour les communications audio et vidéo sur des réseaux en mode paquet sans garantie de service.

Les principales entités nécessaires à la réalisation d'un service de communication multimédia sur des réseaux de données sont :

- 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 » qui permet d'interfacer le réseau IP avec le réseau téléphonique classique.

- L'unité de contrôle MCU (Multipoint Contrôler Unit) qui gère les connexions multipoints (exemple : appels de conférence).

SIP :

Le protocole « SIP » (Session Initiation Protocol) de l'IETF, est un protocole de signalisation pour établissement d'appels et de conférences temps réel sur des réseaux IP. L'architecture du SIP est basée sur des relations client / serveur, les principales composantes sont le terminal (User Equipement), le proxy Serveur, le Redirect Serveur.

Les terminaux sont considérés comme clients lorsqu'ils effectuent une requête, et comme des serveurs lorsqu'ils y répondent. Les terminaux peuvent communiquer directement entre eux ou par l'intermédiaire d'autres serveurs. Les serveurs SIP intermédiaires peuvent se comporter comme Proxy serveur ou Reirect Serveur.

- **Les protocoles de signalisation entre les Softwitch :**

L'interconnexion des réseaux de données avec les réseaux existants TDM utilisant la signalisation SS7, à nécessité le développement du protocole dédié à l'interconnexion des réseaux et aux transports de la signalisation SS7 sur des réseaux en mode paquet.

Ces protocoles permettant la gestion du plan contrôle, ce sont essentiellement :

- BICC (Bearer Independant Call Control), SIP-T (SIP pour la téléphonie) et H.323, au niveau du cœur de réseau.
- SIGTRAN (Signalling Transport), à l'interconnexion avec les réseaux de signalisation SS7, généralement via des passerelles de signalisation ou Signaling.

- **Les protocoles de commande de Media Gateway :**

Ces protocoles ont été engendrés par la séparation des couches transport et contrôle et permettent ou Softswitch de gérer les média Gateway. MGCP de l'IEFT et MEGACO ou H.248, développés conjointement par l'UIT et l'IETE, prédominent actuellement. Ces protocoles représentent le canal de communication utilisé pour coordonner le plan contrôle et le plan transport.

Les principales fonctions de ce canal sont :

- La réservation des ressources de la MG par le MGC nécessaire pour satisfaire les demandes reçues par les messages de signalisation.
- Le traitement des connexions dans les MG par le MGC.
- La notification par le MG d'évènement survenus au niveau média (détection DTMF).

2.2.2.8- Les services offerts par les NGN :

Les NGN offrent les capacités en termes d'infrastructure de protocole et de gestion, de créer et déployer de nouveaux services multimédia sur des réseaux en mode paquet.

La grande diversité des services est due aux multiples possibilités offertes par les réseaux NGN en termes de :

- Support multimédia (données, texte, audio) ;
- Mode de commutation, unicast (commutation point à point), broadcast (diffusion) .
- Mobilité (services disponibles partout et tout le temps) .
- Portabilité sur les différents terminaux.

Parmi ces services offerts nous citons :

La voix sur IP :

La voix sur IP est un service directement lié à l'évolution vers les réseaux NGN, c'est une application qui est apparue depuis longtemps mais qui n'a pas encore eu le succès escompté, et cela pour différentes raisons :

- La jeunesse des protocoles de signalisation (SIP , H.323, MEGACO) de voix sur IP et la gestion de la qualité de service qui commence seulement maintenant à être nature ne permettaient pas de déployer des services téléphoniques sur IP .
- Le seul fait de transporter de la voix classique, les services associes à la voix sur IP n'ont pas encore la maturité nécessaire pour pousser l'évolution vers ces nouveaux réseaux .

- La nécessité d'interconnecter les réseaux IP aux TDM/SS7 implique des coûts liés aux équipements d'interconnexion (passerelle) et le prix des terminaux IP (IP phones) annihile l'avantage financier apporté par le transport en IP .
- Le coût des terminaux IP reste encore supérieur à celui des équipements classiques (pas encore d'économies d'échelle suffisante).

Cependant l'évolution de la technologie et des protocoles et l'apparition des services au monde IP devraient permettre l'émergence de la voix sur IP. De plus, l'évolution des terminaux communicants multimédia est un argument supplémentaire à l'évolution des réseaux téléphoniques vers la voix sur IP.

La diffusion de contenus multimédia :

La diffusion de contenu multimédia regroupe deux activités, l'une focalisée sur la mise en forme des contenus multimédia, l'autre centrée sur l'agrégation de ces divers via des portails.

Les outils technologiques, tels que le multimédia streaming (gestion d'un flux multimédia en termes de bande passante et synchronisation des données) et le protocole multicast, doivent permettre de fournir un service de diffusion de contenu aux utilisateurs finaux.

La messagerie unifiée :

La messagerie unifiée est l'un des services le plus avancés : c'est le premier exemple de convergence et d'accès à l'information à partir des différents moyens d'accès, le principe est de centraliser tous les types de passage vocaux (téléphoniques), écrits (email, SMS), multimédia sur un secteur, ce dernier ayant la charge de fournir un accès aux message adapté au type du terminal de l'utilisateur. Ainsi, un email peut être traduit en message vocal par une passerelle « text-to-speeck » ou inversement un message vocal sera traduit en mode texte.

La messagerie instantanée :

Cette application est déjà un grand succès auprès des internautes : elle permet de dialoguer en temps réel à plusieurs, sur un terminal IP (généralement un PC) ayant accès à l'internet via une interface texte. Cependant, il est nécessaire d'installer sur son terminal un

logiciel propriétaire permettant de se connecter à un fournisseur d'accès, il n'est alors possible de communiquer qu'avec les utilisateurs souscrivons au même service. L'évolution des réseaux devrait permettre de standardisation de cette application et la communication entre tous (ouverture de service) à partir de n'importe quel terminal.

Les services associés à la géo-localisation :

La possibilité de localisation géographiquement les terminaux mobiles à été rapidement perçue comme une source de revenus supplémentaire. En effet, la géo-localisation permet de proposer aux utilisateurs finaux des services très ciblés à haute valeurs ajoutées liés au contexte (exemple : horaire, climat et au lieu).

Actuellement plusieurs solutions techniques existent et sont même en cours d'implémentation dans les réseaux d'opérateurs mobiles, il n'existe pas encore d'interfaces permettant l'exploitation de ces données par les applications de services, ou de réel volonté des opérateurs d'ouvrir leur serveurs de la localisation à des fournisseurs de services tiers, afin d'utiliser cette fonction de localisation comme « service capability server » (élément de base de support à la réalisation des services).

Conclusion :

La connaissance des principes sur lesquels sont fondés les NGN, les types de réseaux NGN existant et leur protocoles ainsi que les différents services réellement pertinents dans ce cadre, ce sont des étapes nécessaires pour pouvoir comprendre les stratégies d'évolution des réseaux actuels fixes ou mobiles vers une architecture multiservice.

Introduction

Qu’est-ce qu’un protocole ?

Le but des réseaux est de faire communiquer plusieurs ordinateurs ensemble. Si les hommes communiquent entre eux grâce aux différentes langues, les ordinateurs utilisent différents protocoles. Les communications sont souvent internationales, et comme pour les hommes, il n'existe pas de protocole universel. Certains sont plus utilisés que d'autres, il en existe cependant un très grand nombre, chacun cherchant à imposer sa propre norme.

Comment expliquer clairement ce qu'est un protocole ? Supposons que quelqu'un veuille envoyer une lettre à quelqu'un d'autre. On va placer cette lettre dans une enveloppe et on y notera l'adresse. Pour l'acheminement du courrier, le contenu de la lettre n'est d'aucune utilité. Les différents services de la poste regardent les différents champs de l'adresse et dirigent l'enveloppe, donc son contenu dans la bonne direction.

Il en est de même quand un ordinateur veut envoyer des données à un autre ordinateur. Les données sont enfermées (on dit encapsulées) dans une enveloppe qui contient les informations permettant l'acheminement des données. Un protocole, c'est la façon dont l'adresse est écrite sur l'enveloppe, le fait de mettre d'abord le nom, puis la rue et enfin la ville. Un autre protocole, c'est aussi le fait de mettre le lieu et la date en haut à droite et la signature en bas.

Enfin, un protocole est une description formelle de règles et de conventions à suivre dans un échange d'informations, que ce soit pour acheminer les données jusqu'au destinataire ou pour que le destinataire comprenne comment il doit utiliser les données qu'il a reçues.

1- Protocole TCP/IP :

1.1- L’origine de TCP/IP :

TCP/IP est une suite de protocoles permettant à des ordinateurs de partager des ressources à travers un réseau. Il a été développé par un groupe de chercheurs, essentiellement autour du projet ARPAnet. ARPAnet est certainement le plus renommé des réseaux TCP/IP. Cependant, dés juin 87, plusieurs fournisseurs proposaient déjà des produits TCP/IP, et des milliers de réseaux l’utilisaient.

Le nom le plus approprié pour cette suite de protocoles est certainement « l'ensemble de protocoles Internet », TCP et IP sont deux protocoles de cet ensemble. Nous pouvons par exemple associer à tort NFS avec TCP\IP, alors qu'il ne se base pas sur le protocole TCP (il utilise IP mais aussi un autre protocole, UDP plutôt que TCP.)

TCP/IP est donc une famille de protocoles. Certains implémentent des fonctions de bas niveau utilisées par de nombreuses applications. Ceux-ci sont les protocoles IP, TCP et UDP. D'autres sont des protocoles conçus pour des applications particulières telles que le transfert de fichiers entre ordinateurs, l'envoi de courrier électronique ou l'identification de la personne connectée sur un ordinateur particulier.

1.2- La suite des protocoles de TCP/IP :

TCP/IP est un ensemble de protocoles en « couches », lies entre aux.

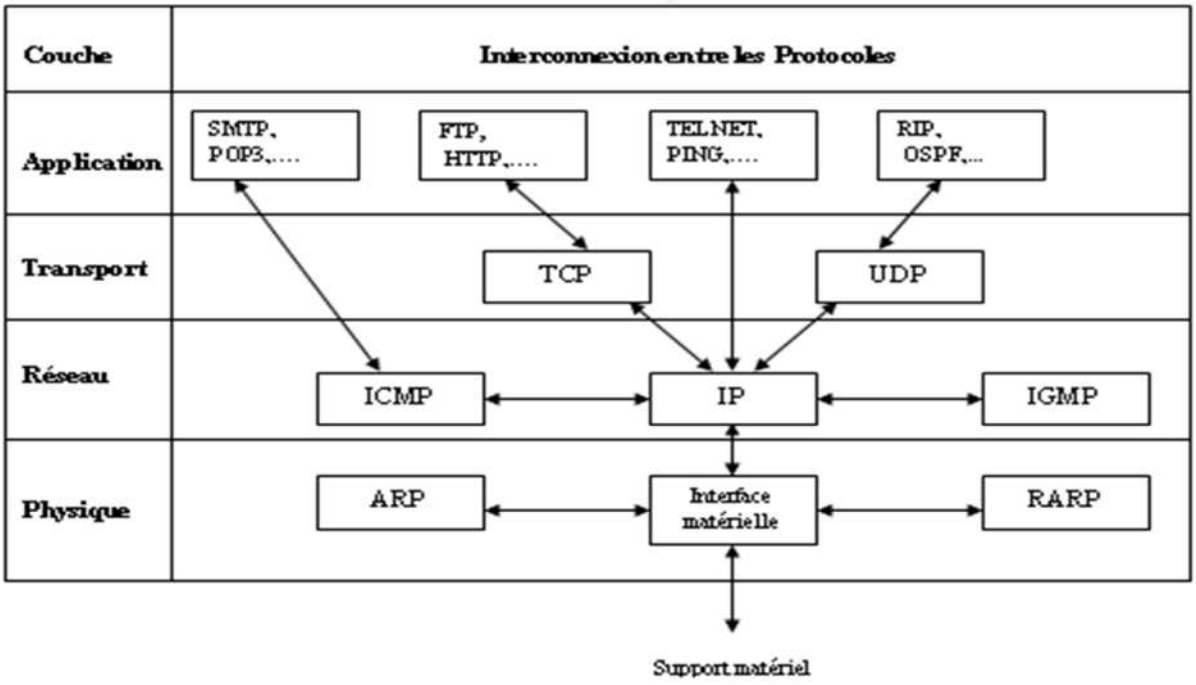


Figure II.1 : La suite de protocole TCP / IP

1.3 - Les protocoles de la couche transport :

1.3.1- Protocole TCP :

Le protocole TCP est défini dans le but de fournir un service de transfert de données de haute fiabilité entre deux ordinateurs "maîtres" raccordés sur un réseau de type "Paquets commutés", et sur tout système résultant de l'interconnexion de ce type de réseaux

- **Motivation :**

  TCP est un protocole sécurisé orienté connexion conçu pour s'implanter dans un ensemble de protocoles multicouches, supportant le fonctionnement de réseaux hétérogènes. TCP s'intègre dans une architecture multicouche des protocoles, juste au-dessus du protocole Internet IP. Ce dernier permet à TCP l'envoi et la réception de segments de longueur variable, encapsulés dans un paquet Internet appelé aussi "datagramme".

- **Spécifications fonctionnelles de TCP**

-Format des segments TCP :

Les paquets TCP sont envoyés sous forme de datagrammes Internet. L'en-tête IP transmet un certain nombre de paramètres, tels que les adresses Internet source et destinataires.

0 **32**

<table>
<tr><td colspan="8">Port source</td><td colspan="8">Port destination</td></tr>
<tr><td colspan="16">Numéro de séquence</td></tr>
<tr><td colspan="16">Accusé de réception</td></tr>
<tr><td colspan="16"></td></tr>
<tr><td>Data Offset</td><td colspan="3">Réservé</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td colspan="8">Fenêtre</td></tr>
<tr><td colspan="8">Checksum</td><td colspan="8">Pointeur données urgentes</td></tr>
<tr><td colspan="8">Option</td><td colspan="8">Bourrage</td></tr>
<tr><td colspan="16">Data</td></tr>
</table>

Figure II.2: En-tête TCP

Définition des différents champs :

- **Port source** : (16 bits) Le numéro de port de la source.
- **Port Destinataire** : (16 bits) Le numéro de port du destinataire.
- **Numéro de séquence** : (32 bits) Le numéro du premier octet de données par rapport au début de la transmission (sauf si SYN est marqué).
- **Accusé de réception :** (32 bits) Si ACK est marqué ce champ contient le numéro de séquence du prochain octet que le récepteur s'attend à recevoir.
- **Data Offset** : (4 bits) La taille de l'en-tête TCP en nombre de mots de 32 bits. Il indique là ou commence les données.
- **Réservé** : (6 bits) Réservés pour usage futur. Doivent nécessairement être à 0.
- **Bits de contrôle** : (6 bits) (de gauche à droite): URG: Pointeur de données urgentes significatif, ACK: Accusé de réception significatif, PSH: Fonction Push, RST: Réinitialisation de la connexion, SYN: Synchronisation des numéros de séquence FIN: Fin de transmission
- **Fenêtre** : (16 bits) Le nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir.
- **Checksum** : (16 bits) Le Checksum est constitué en calculant le complément à 1 sur 16 bits de la somme des compléments à 1 des octets de l'en-tête et des données pris deux par deux mots de 16 bits.

- **Pointeur de données urgentes** : (16 bits) Communique la position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence.
- **Options** :(variable) Les champs d'option peuvent occuper un espace de taille variable à la fin de l'en-tête TCP.
- **Bourrage (padding)**: (variable) Les octets de bourrage terminent l'en-tête TCP: de sorte que le nombre d'octet de celle-ci soit toujours multiple de 4 (32 bits).

➢ **Établissement et rupture des connexions TCP :**

TCP indique un identificateur de port. Comme ces identificateurs sont choisis indépendamment par chaque extrémité, ils peuvent se révéler identiques. L'adresse unique d'une communication TCP est obtenue par la concaténation de l'adresse Internet avec l'identificateur du port sélectionné, constituant ainsi ce que l'on nome un "socket". Ce socket est alors unique dans l'ensemble du réseau.

Une connexion est demandée par activation de la commande OPEN indiquant le port local et les paramètres du socket distant. En retour, TCP répond par un nom local (court) symbolique que l'application utilisera dans ses prochains appels. La commande OPEN spécifie en outre si le processus de connexion doit être effectué jusqu'à son terme, ou s'il s'agit d'une ouverture en mode passif.

Les processus peuvent ouvrir une connexion passive et attendre qu'une connexion active les impliquant provienne d'une autre machine. TCP aura la charge d'avertir l'application qu'une communication est établie. Deux processus émettant au même moment une requête de connexion l'un vers l'autre se retrouveront normalement connecté. Cette souplesse est indispensable pour assurer un bon fonctionnement du réseau composé d'éléments totalement asynchrones.

La correspondance entre le socket arrivé et le socket attendu détermine l'opportunité de la connexion. Celle-ci ne devient réellement établie que lorsque les deux numéros de séquence ont été synchronisés dans les deux directions."La rupture" d'une connexion suppose l'émission de segments, marqués du bit FIN.

➢ Modèle de fonctionnement

Les processus transmettent les données en faisant appel à TCP et en passant des tampons de données comme arguments.

Le protocole TCP inclut les informations nécessaires à la "reconstruction" en bon ordre des données originales. Le modèle d'une communication Internet fait qu'il existe pour chaque TCP actif un module de protocole Internet chargé de l'acheminement de données. Ce module Internet "encapsule" à son tour les paquets TCP sous la forme de paquets Internet, transmis à un module Internet distant via des "routeurs.

- **Fiabilité de communication :**

Un flux de donnée s'appuyant sur une connexion TCP doit être pouvoir considéré comme "fiable". La fiabilité de cette transmission s'appuie sur l'utilisation de numéros de séquence et sur un mécanisme d'accusés de réception.

1.3.2 - Le protocole UDP :

Le protocole UDP est comme TCP, un protocole de transport des données. Cependant, contrairement à TCP, on qualifie l'UDP de transmission "en mode non connecté et non fiable" ou encore de protocole "non orienté connexion". Ceci signifie simplement que la machine émettrice envoie des données sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première. Les données sont ainsi envoyées sous forme de blocs (datagrammes). Il n'y a pas de contrôle d'erreur. C'est un mécanisme simple d'échange de données entre applications.

Le protocole UDP est utilisé en place de TCP pour un transport rapide et léger des données.

- **Structure de l'en-tête UDP :**

Le paquet UDP est conçu pour être encapsulé dans un datagramme IP et permettre un échange de données entre deux applications, sans échange préliminaire. Ainsi, si les données à transmettre n'obligent pas IP à fragmenter un paquet UDP génère un datagramme IP et c'est tout.

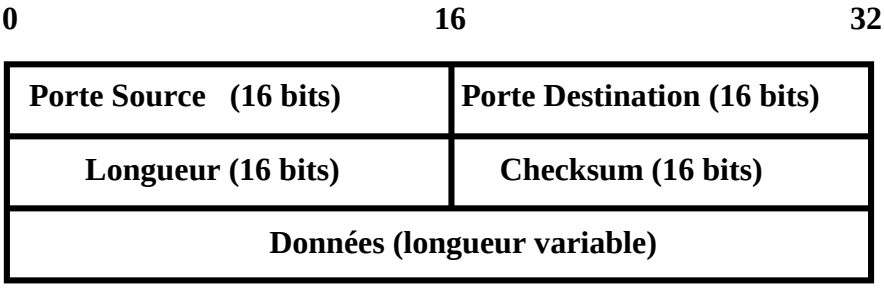


Figure II.3 : En-tête UDP

Définition des différents champs :

- **Port source** : (16bits) Le champ Port source est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine source.
- **Port destination** : (16bits) champ Port destination est codé sur 16 bits et il correspond au port relatif à l'application en cours sur la machine de destination.
- **Longueur** : (16bits) Le champ Longueur est codé sur 16 bits et il représente la taille de l'entête et des données. Sont unité est l'octet et sa valeur maximale est 64 k Octets (2^{16}).
- **Checksum** : (16bits) Le champ Checksum est codé sur 16 bits et représente la validité du paquet d'UDP.

- **Applications du Protocole :**

Ce protocole sera utilisé principalement pour les communications avec les serveurs de noms de domaines, et dans les transactions utilisant le protocole Trivial File Transfer.

1.4 - Les protocoles de la couche réseau

14.1- Protocole IP :

Le Protocole Internet est conçu pour supporter l'intercommunication de systèmes informatiques sur une base de réseau par commutation de paquets.

Le rôle du protocole Internet est la transmission de blocs de données, appelés datagrammes, d'une source vers une destination, la source et la destination étant des ordinateurs hôtes identifiés par une adresse de longueur fixe. Le protocole Internet dispose des mécanismes permettant la fragmentation de longs datagrammes et leur réassemblage, lors de leur transmission à travers des réseaux de "dimension" inférieure.

- **Motivation :**

Le protocole Internet est limité aux fonctions nécessaires à l'acheminement d'un paquet de bits (un datagramme Internet) depuis une source vers une destination via un ensemble de réseaux interconnectés. Le protocole Internet capitalisera les services des réseaux qui le supportent pour offrir divers types et qualités de service.

- **Description fonctionnelle du protocole IP**

La fonction ou rôle du Protocole Internet est d'acheminer les datagrammes à travers un ensemble de réseaux interconnectés. Ceci est réalisé en transférant les datagrammes d'un module Internet à l'autre jusqu'à atteindre la destination. Les modules Internet sont des programmes exécutés dans des hôtes et des routeurs du réseau Internet. Les datagrammes sont transférés d'un module Internet à l'autre sur un segment particulier de réseau selon l'interprétation d'une adresse Internet. De ce fait, un des plus importants mécanismes du protocole Internet est la gestion de cette adresse Internet.

-Spécification d'IP

- Format de l'en-tête IP :

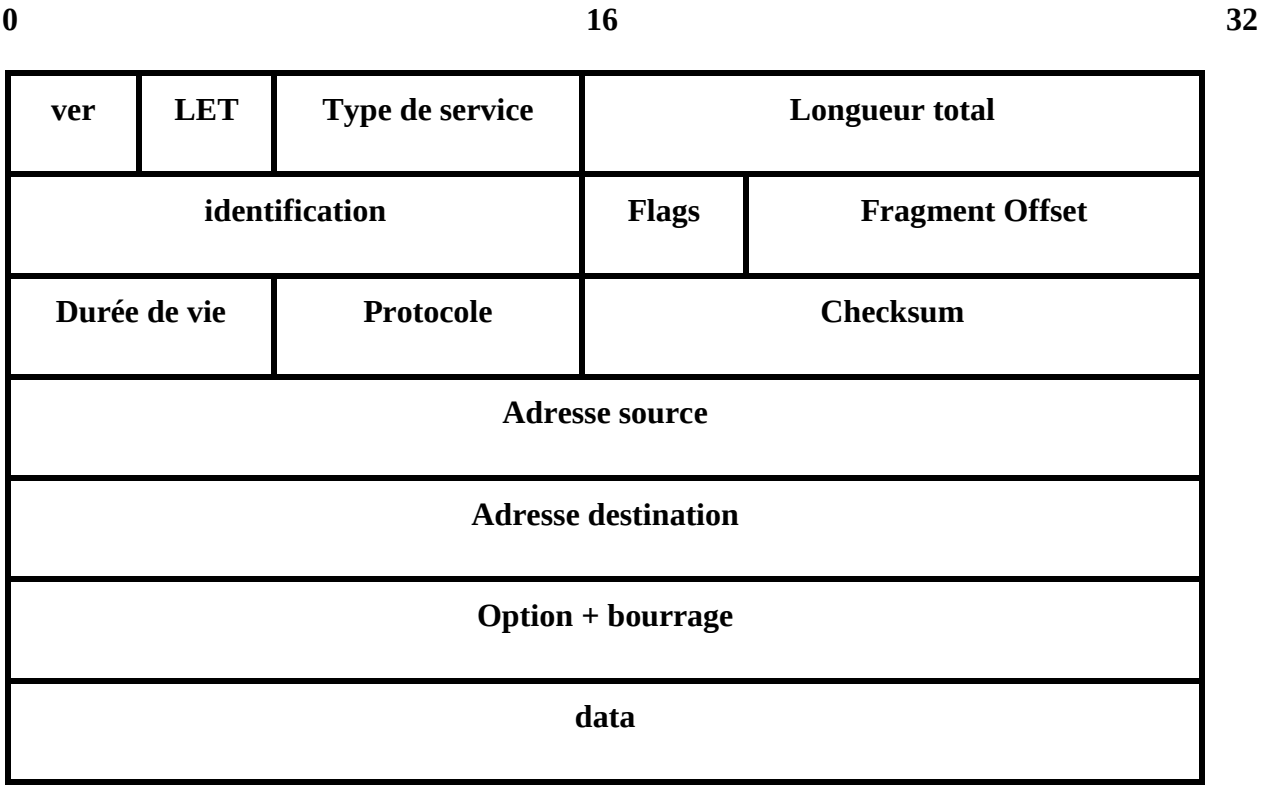


Figure II.4: En-tête IP

- **Définition des différents champs :**

- **Version** : (4 bits), Le champ Version renseigne sur le format de l'en-tête Internet. Ce document décrit le format de la version 4 du protocole.
- **Longueur d'En-tête** : (4 bits) Le champ longueur d'En-tête (LET) code la longueur de l'en-tête Internet, l'unité étant le mot de 32 bits, et de ce fait, marque le début des données.
- **Type de Service** : (8 bits) "Le Type de Service" donne une indication sur la qualité de service souhaitée, qui reste cependant un paramètre "abstrait".
- **Longueur Totale** : (16 bits) Le champ "Longueur Totale" est la longueur du datagramme entier y compris en-tête et données, mesurée en octets.
- **Identification** : (16 bits) Une valeur d'identification assignée par l'émetteur pour identifier les fragments d'un même datagramme.

- **Flags** : (3 bits) Divers commutateurs de contrôle.
- **Fragment Offset** : (13 bits) Ce champ indique le décalage du premier octet du fragment par rapport au datagramme complet.
- **Durée de vie** : (8 bits) Ce champ permet de limiter le temps pendant lequel un datagramme reste dans le réseau.
- **Protocole** : (8 bits) Ce champ indique quel protocole de niveau supérieur est utilisé dans la section donnée du datagramme Internet.
- **Checksum d'en-tête** : (16 bits) Un Checksum calculé sur l'en-tête uniquement.
- **Adresse source** : (32 bits) l'adresse Internet de la source.
- **Adresse destination** : (32 bits) L'adresse Internet du destinataire.
- **Options** :(variable) Les datagrammes peuvent contenir des options. Celles-ci doivent être implémentées par tous les modules IP (hôtes et routeur). Dans certains environnements, l'option de sécurité peut être obligatoire dans tous les

- **Modèle de fonctionnement :**

Le modèle de fonctionnement de la transmission d'un datagramme d'un programme d'application vers un autre est illustré par le scénario suivant :

Nous supposons ici que la transmission traverse un routeur intermédiaire. L'application émettrice prépare les données à envoyer et appelle son module Internet local pour envoyer un datagramme en lui passant l'adresse de destination et quelques autres paramètres comme arguments.

Le module Internet prépare un en-tête de datagramme et lui ajoute les données. Ce module détermine à quel programme applicatif le datagramme est destiné. Il passe alors les données au programme applicatif en réponse à un appel système, accompagné de l'adresse de la source et de quelques autres paramètres.

1.4.2 - Le protocole ICMP :

Occasionnellement, un routeur ou un hôte destinataire peut avoir à communiquer vers l'émetteur du datagramme, par exemple, pour signaler une erreur de traitement du datagramme. C'est dans cette perspective qu'a été mis en place le protocole Internet Control Message Protocol (ICMP). Il s'appuie sur le support de base fourni par IP comme s'il s'agissait d'un protocole d'une couche supérieure.

Les messages ICMP sont envoyés dans diverses situations: par exemple, lorsqu'un datagramme ne peut pas atteindre sa destination, lorsque le routeur manque de réserve de mémoire pour retransmettre correctement le datagramme, ou lorsque le routeur décode de viser l'hôte destinataire via une route alternative pour optimiser le trafic.

Les messages ICMP reportent principalement des erreurs concernant le traitement d'un datagramme dans un module IP

1.4.3- Protocole IGMP :

Il spécifie non seulement la marche à suivre pour rejoindre ou quitter un groupe multicast, mais également comment se déclarer membre multicast auprès du routeur le plus proche pour que les trames multicast parviennent jusqu'à lui.

1.5 - Les protocoles de la couche physique :

1.5.1- Le protocole ARP :

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse (en anglais ARP signifie Address Resolution Protocol).

1.5.2- Le protocole RARP :

Le protocole RARP est beaucoup moins utilisé, il signifie Protocole ARP inversé, il s'agit donc d'une sorte d'annuaire inversé des adresses logiques et physiques.

Le protocole RARP permet à une station de connaître son adresse IP à partir d'une table de correspondance entre adresse MAC (adresse physique) et adresses IP hébergée par une passerelle (Gateway) située sur le même réseau local (LAN). Pour cela il faut que l'administrateur paramètre le Gateway (routeur) avec la table de correspondance des adresses MAC/IP. En effet, à la différence d'ARP ce protocole est statique. Il faut donc que la table de correspondance soit toujours à jour pour permettre la connexion de nouvelles cartes réseau.

1.6 - Les protocoles de la couche application :

1.6.1- Le protocole FTP :

Le protocole FTP (File Transfer Protocol) est, comme son nom l'indique, un protocole de transfert de fichier. Il permet :

-Un partage de fichiers entre machine distante .

-Une indépendance aux systèmes de fichiers des machines clientes et serveur .

-Le transfère des données de manière efficace.

1.6.2- Le protocole HTTP :

- Le protocole HTTP (Hyper Text Transfer Protocol) est le protocole le plus utilisé sur Internet depuis 1990.
- Le but du protocole HTTP est de permettre un transfert de fichiers (essentiellement au format HTML) localisé grâce à une chaîne de caractères appelée URL entre un navigateur (le client) et un serveur Web (appelé d'ailleurs http)

1.6.3- Le protocole Telnet :

Le protocole Telnet est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un interpréteur de commande (côté serveur).

1.6.4- Protocole RIP2 :

RIP2 est utilisé pour échanger des informations de routage. Il dérive d'un premier protocole développé par Xerox (RIP). Chaque machine qui utilise un protocole RIP2 a un processus qui envoie et reçoit des datagrammes transportés par de l'UDP port numéro 520.

1.6.5- Protocoles SLIP et PPP

1.6.5.1-Le protocole SLIP :

SLIP signifie Serial Link Internet Protocol, traduisez protocole Internet de liaison en série. SLIP est le résultat de l'intégration des protocoles modems précédent à la suite de protocoles TCP/IP.

Il s'agit d'un protocole de liaison Internet simple n'effectuant ni contrôle d'adresse, ni contrôle d'erreur, c'est la raison pour laquelle il est vite devenu obsolète par rapport à PPP.

1.6.5.2- Le protocole PPP : Point To Point Protocol :

Ce protocole encapsule des paquets IP dans des trames PPP, puis transmet ces paquets PPP encapsulés à travers la liaison point à point. PPP est donc utilisé entre un client distant et un serveur d'accès distant.

1.6.6- Domain Name System (DNS) :

Est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine.

Quand un utilisateur souhaite accéder à un site, comme par exemple www.free.fr, son ordinateur émet une requête spéciale à un serveur DNS, demandant 'Quelle est l'adresse de www.free.fr ?'. Le serveur répond en retournant l'adresse IP du serveur.

Il est également possible de poser la question inverse, à savoir 'Quel est le nom de domaine de telle adresse IP ?'. On parle alors de résolution inverse.

1.7 - Protocole IPv6 (l'avenir d'IP) :

Le protocole IPV6 (Internet Protocole Version 6) est la sixième version du protocole Internet. Aussi connu sous le nom d'IPng (Internet Protocole new generation), il est le successeur de l'IPV4. IL a été conçut pour mettre à niveau l'IPV4, l'améliorer, lui apporter les modifications nécessaires et prend en compte l'évolution des besoins des utilisateurs.

Les objectifs principaux de ce nouveau protocole :

- Supporter des milliards d'ordinateurs, en se libérant de l'inefficacité de l'espace des adresses IP actuelles .
- Réduire la taille des tables de routage .
- Simplifier le protocole, pour permettre aux routeurs de router les datagrammes plus rapidement.
- Fournir une meilleure sécurité (authentification et confidentialité) que l'actuel protocole IP.
- Donner la possibilité à un ordinateur de se déplacer sans changer son adresse.

En général, IPv6 n'est pas compatible avec IPv4, mais est compatible avec tous les autres protocoles Internet, dont TCP, UDP, ICMP, IGMP et DNS ; quelque fois, de légères modifications sont requises (notamment pour fonctionner avec de longues adresses).

2- Adressage IP :

L'adresse IP est un nombre de 32 bits qui identifie, de manière unique, un nœud (ordinateur, imprimante, routeur, etc.) d'un réseau TCP/IP. Les adresses IP sont généralement exprimées dans un format décimal pointé, fait de quatre nombres séparés par des points, par exemple 192.168.100.85. Le fonctionnement d'un réseau étendu composé de plusieurs réseaux TCP/IP n'exige pas que les routeurs chargés de faire passer les données entre les réseaux connaissent l'adresse exacte de l'hôte auquel est destiné un paquet. Tout ce que doivent connaître les routeurs, c'est le réseau auquel appartient cet hôte; ils utilisent les données de leurs tables de routage pour déterminer la façon d'envoyer le paquet au réseau contenant l'hôte cible. Une fois le paquet remis au réseau du récepteur, il sera ensuite livré au bon hôte. Ce processus repose sur la décomposition de l'adresse IP en deux parties: ID de réseau et ID d'hôte.

2.1- L’espace d’adressage :

L’espace d’adressage est définie en fonction du nombre de bit nécessaire pour exprimer une adresse IP. Plus le nombre de bit est important, et plus le nombre de possibilité est important.

Il existe deux espaces d’adressage pour les adresses IP :

- L’espace d’adressage de 32 bits qui correspond au système d’adresses IP actuelles (Ipv4).
- L’espace d’adressage de 128 bits qui correspond au prochain système d’adresses IP qui est en train d’être élaboré (Ipv6 pour IP version 6 ou IPNG pour IP New Génération) Ipv6 disposera de fonctionnalités natives d’authentification et de cryptage.

- L’espace d’adressage 32bits :

L’espace d’adressage 32 bits est constitué de 4 Octets de 8 bits chacun (4x8 = 32). Chaque octet est constitué de huit bits, et chaque bit peut prendre la valeur binaire 1 ou 0. Ainsi, la valeur décimale de chaque octet peut être comprise en 0 et 255 (256 possibilités = 2 à la puissance 8), et l’espace d’adressage est compris entre 1 et 4 294 967 296 (2 à la puissance 32 moins 1).

Les adresses IP sont généralement exprimées dans la « notation décimale pointée » (c’est à dire que chaque octet est séparé de l’autre par un point).

Le tableau suivant représente la comparaison entre les deux espaces d'adressage:

L'espace d'adressage IP		
	IPV4	**IPV6**
Espace d'adressage	Une adresse sur 32 bits	Une adresse sur 128 bits
Structure de l'adresse	**4 mots** (x.x.x.x)	**8 mots** (x.x.x.x.x.x.x.x)
Notation	Décimale pointée	Hexadécimale pointée
Définition d'un mot	Un mot = 1 octet= 8 bits	Un mot = 4 hexadécimales = 16 bits
Dimension pour un mot	0 à 255 (en base 10)	0000 à FFFF (en base 16)
Possibilité par mot	2 puissances 8 = 256	16 puissance 4 = 65 536 2 puissance 16 = 65 536
Possibilité d'adresse	256 puissance 4 = 2^32 2^32 = 4 294 967 296	65 536 puissance 8 = 2^128 2^128 = un nombre très grand

Tableau II.1: L'espace d'adressage IP

2.2- Le masque de sous réseau :

Le masque de sous réseau permet de savoir qu'elle est la partie de 32 bits qui est utilisé pour identifier le réseau. Les bits du masque de sous réseau sont à 1 pour indiquer « la partie réseau » et sont à 0 pour indiquer « la partie station ». Les bits de « la partie station » n'utilisent jamais les valeurs extrêmes, 0 et 255 pour ne pas être confondus avec « la partie réseau ». Pour identifier une station sur le réseau Internet, il faut connaître deux adresses IP :

- Le masque de sous réseau
- L'adresse IP

Par exemple:

- L'adresse IP : 192.168.100.1
- Le masque de sous réseau : 255.255.255.0

- La partie réseau : 192.168.100.0
- La partie station : 0.0.0.1

L'adresse du réseau dans Internet est 192.168.100.0 et l'adresse de la première station à l'intérieur de ce réseau est 192.168.100.1.

2.3- L'adresse de diffusion (broadcast) :

Chaque réseau possède une adresse particulière dite de diffusion. Tous les hôtes du réseau «écoutent» cette adresse en plus de la leur. Certaines informations telles que les annonces de service ou les messages d'alerte sont utiles à l'ensemble des hôtes du réseau

2.4- Le sous adressage :

Le sous adressage consiste à utiliser une partie de « la partie station » pour l'incorporer à « la partie réseau » et ainsi agrandir celle-ci. Le nombre de sous réseau sera plus important, mais le nombre de station par sous réseau le sera moins.

2.5- Les classe d'adresses IP :

La partie réseau de l'espace d'adressage 32 bits est divisée en classes.

- Les adresses de classe A
- Les adresses de classe B
- Les adresses de classe C
- Les adresses de classe D
- Les adresses de classe E

- **Classe A**

Le premier octet a une valeur strictement inférieure à 128 (valeur du bit de poids fort égal à 0). Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

Classe A			
Partie réseau	**Partie hôte**		
0xx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Figure II.5: Forma d'adressage (classe A)

- **Classe B**

Le premier octet a une valeur comprise entre 128 et 192 (valeur des 2 bits de poids fort égale à 10). Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

Classe B			
Partie réseau		**Partie hôte**	
10x.xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Figure II.6 : Forma d'adressage (classe B)

- **Classe C**

Le premier octet a une valeur comprise entre 192 et 223 (valeur des 3 bits de poids fort égale à 110). Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

Classe C			
Partie réseau			Partie hôte
110. xxx.xxx.xxx.xxx	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Figure II.7 : Forma d'adressage (classe C)

- **Classe D**

Le premier octet a une valeur comprise entre 224 et 239 (valeur des 3 bits de poids fort égale à 111). Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (*host groups*).

Classe D			
Adresse multidiffusion			
111. xxx.xxx.xxx.xxx	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**	**xxx.xxx.xxx.xxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Figure II.8 : Forma d'adressage (classe D)

- **Classe E**

Le premier octet a une valeur supérieure à 240. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

A chaque classe correspond un nombre maximum de réseau pouvant appartenir à cette classe, et à chaque réseau d'une certaine classe, correspond un nombre maximum

d'adresses, c'est à dire un nombre maximum de stations pouvant bénéficiées d'un adresse fixe à l'intérieur de ce réseau.

Le tableau suivant représente les propriétés des différentes classes :

Les classes des adresses IP					
	Classe A	**Classe B**	**Classe C**	**Classe D**	**Classe E**
Fonction	Multinationales	Grande entreprises	Petites entreprises	Multicasting	Recherche expérimentale
Réseau	Sur 1 octet	Sur 2 octets	Sur 3 octets		
Station	Sur 3 octets	Sur 2 octets	Sur 1 octet		
Structure de la partie réseau	1.0.0.0 à 126.0.0.0	128.1.0.0 à 191.254.0.0	192.0.1.0 à 223.254.254.0		
Valeur du 1er octet en binaire	00000001 à 01111110	10000000 à 10111111	11000000 à 11011111		
Nombre de machines par réseau	16 millions	65 536	256		

Tableau II.2: Les classes d'adressage.

2.6- Les adresses IP conventionnelles (Adresses réservées) :

Certaines adresses sont réservées pour une utilisation conventionnelle :

- 0.0.0.0 est utilisée par les machines pendant la procédure de démarrage de l'ordinateur ;
- 127.0.0.0 est utilisée pour tester une adresse IP ;

- 192.168.0.0 n'existe pas sur Internet, afin d'être réservée pour les réseaux locaux sous TCP/IP ;
- 255.255.255.255 est utilisée comme adresse de broadcast générale.

2.7- Le Routage

2.7.1- Routage IP :

En règle générale, le routage est le processus de transmission des paquets entre les réseaux connectés. Pour les réseaux TCP/IP, le routage fait partie du protocole IP et est utilisé en combinaison avec d'autres services de protocole réseau pour fournir des capacités de transmission entre les hôtes situés sur des segments de réseau distincts dans un réseau TCP/IP plus grand.

2.7.2 Tables de routage :

Les hôtes TCP/IP utilisent une table de routage pour gérer les informations sur les autres réseaux et hôtes IP. Les réseaux et les hôtes sont identifiés en utilisant une adresse IP et un masque de sous-réseau. De plus, les tables de routage sont importantes car elles fournissent les informations nécessaires à chaque hôte local en indiquant comment communiquer avec les réseaux et hôtes distants.

Il est possible, pour chaque ordinateur d'un réseau IP, de gérer une table de routage comportant une entrée pour chaque autre ordinateur ou réseau avec lequel l'ordinateur local communique.

2.7.3- Routage dynamique :

Lorsqu'un réseau atteint une taille assez importante, il est très lourd de devoir ajouter les entrées dans les tables de routage à la main. La solution est le routage dynamique. Cela permet de mettre à jour les entrées dans les différentes tables de routage de façon dynamique.

2.7.4- Routage statique :

Par opposition au routage dynamique, consiste à saisir manuellement les routes dans le routeur.

2.7.5- Le routage inter domaine sans classe :

Le routage inter domaine sans classe (Classeless Inter-Domain Routing ou CIDR) est une méthode permettant de contourner la limitation de l'allocation des adresses IP par classe, et de pallier la pénurie des adresses IP version 4 des classes B et C. Les entreprises disposant d'une classe B alors qu'elles n'ont qu'un petit nombre de stations « gaspillent » des adresses IP potentielles. Par ailleurs, le saut d'une classe à une autre est très important, à la fois en terme de coût et en terme de nombre d'adresse.

Le CIDR permet essentiellement de combiner deux adresses de réseaux de classe C pour ne former qu'un seul réseau.

2.8- Types d'adresses

2.8.1- L'adresse de broadcast d'un réseau local :

L'adresse de broadcast d'un réseau local est l'adresse de diffusion générale à toutes les stations du réseau. L'adresse de broadcast est en général la dernière adresse du réseau.

L'adresse IP se compose de « la partie réseau » qui identifie le réseau, et de « la partie machine » qui identifie une station à l'intérieur de ce réseau. Par exemple, 192.168.100.0 pour la partie réseau, et 192.168.100.x avec x allant de 1 à 255 pour la partie machine. Ainsi, l'adresse de broadcast d'un tel réseau serait 192.168.100.255.

2.8.2- Adresse multicast :

Plutôt que d'envoyer les fichiers du serveur vers chacune des machines clientes (unicast) on peut n'envoyer l'information qu'une seule fois et chaque ordinateur client la récupère. Les clients écoutent ce qui arrive sur cette adresse et suivent la procédure décrite par le protocole multicast implémenté.

2.8.3- Adresse unicast :

C’est le principe le plus utilisé et le plus simple. Les ordinateurs possédant chacun une adresse IP, on peut envoyer les trames en spécifiant l’adresse IP de l’ordinateur à qui on veut envoyer les informations.

Conclusion :

Le logiciel d’un réseau est composé de protocoles, règles qui permettent à des processus de communiqué. Ces protocoles peuvent être sans connexion ou orientés connexion. La plupart des réseaux disposent d’une hiérarchie de supérieure sans avoir à connaître les détails des protocoles des couches inférieures.

L’adressage IP, où Chaque nœud d'un réseau TCP/IP doit avoir une adresse IP unique. Les réseaux TCP/IP se divisent habituellement en trois grandes classes qui ont des tailles prédéfinies. II est possible de diviser un réseau en plusieurs sous réseaux, en utilisant un masque de sous réseau qui sépare en deux parties l'adresse IP: une partie identifie l’hôte (la machine), alors que l'autre identifie le réseau contenant l'hôte. Chaque hôte TCP/IP est identifié par une adresse IP logique, qui est une adresse de couche Réseau indépendante de toute adresse de couche Liaison (telle que l'adresse physique de la carte réseau).

Introduction :

La généralisation des infrastructures IP et la diffusion d'Internet presque dans tous les foyers, entreprises, et surtout l'amélioration du débit et de la bande passante, ces dernières années ont contribuées à la révolution de la voix sur IP et à l'extension de ce compte de la théorie vers l'utilisation professionnelle et même domestique.

La voix sur IP (en anglais, Voice over IP ou VOIP) est le nom d'une nouvelle technologie de télécommunication vocale en plaine émergence qui transforme la téléphonie. Cette technologie marque un tournant dans le monde de télécommunication en permettant de transmettre la voix sur un réseau numérique et sur Internet.

La voix sur IP est utilisée avec différentes architectures et deux principaux protocoles définissent son fonctionnement, elle dépend de plusieurs contraintes. La voix présente plusieurs avantages et nécessite encore plus d'efforts pour innover et essayer de réduire les failles et les inconvénients qui y existent encore. Dans ce chapitre nous allons découvrir les différentes contraintes qui agissent sur le transport de la voix sur un réseau IP.

- Généralités sur la voix IP (VOIP) :

1 - La voix sur IP :

1. 1- Définition et vue d'ensemble :

VOIP signifie textuellement « Voice over IP », en français « Voix sur IP ». Le principe consiste à encapsuler un signal audio numérisé (en général la voix) dans le protocole IP. La principale application de ce principe est la téléphonie Internet (téléphonie IP). A la différence de la téléphonie analogique filaires (RTC) distribués par les centraux téléphoniques, la VOIP permet d'étendre la téléphonie sur tout réseau numérique ou analogique acceptant le protocole TCP/IP (Internet, RNIS, PPP, etc.).

Vu l'évolution profonde du secteur de télécommunication et l'introduction du concept de NGN, la voix sur IP est considérée un service directement lié ce nouveau paradigme, c'est un service qui est apparue depuis longtemps, mais qui n'a pas encore eu le succès escompte, et cela pour différentes raisons :

- Les protocoles de signalisation (SIP, H.323) de voix sur IP et la gestion de la qualité de service qui commence seulement maintenant à être nature et ne permettaient pas de déployer des services téléphoniques sur IP.
- Le coût des terminaux IP reste encore supérieur à celui des équipements classiques.
- La nécessité d'interconnecter les réseaux IP au réseau TDM/SS7 implique des coûts liés aux équipements d'interconnections (passerelle).

1. 2- Fonctionnement :

Contrairement à la téléphonie classique, par commutation de circuits, qui repose exclusivement sur un réseau téléphonique commuté, la technologie VoIP permet de téléphoner sur des réseaux spécialisés ou sans fil, y compris des réseaux informatiques. Ces nouveaux types de réseaux utilisent des protocoles« commutation par paquets ». En plus des données vocales (voix numérisée), un paquet comporte les adresses réseaux de l'expéditeur et du destinataire. Les paquets VoIP sont transmis à travers n'importe quel réseau compatible VoIP et peuvent être acheminés par des chemins différents, la VoIP est donc interopérable. Par la suite, une application se chargera de la transformation inverse (des paquets vers la voix). En effet, toutes les informations à transmettre sur le réseau sont divisées en paquets de données. Chaque paquet se compose :

- d'un en-tête indiquant sa source et sa destination,
- d'un numéro de séquence,
- d'un bloc de données,
- d'un code de vérification des erreurs,

Cette nouvelle technologie pourrait permettre à une organisation de fusionner, sur un seul et même réseau, le réseau informatique et le réseau téléphonique.

De plus, la téléphonie sur IP permet les fonctionnalités les plus populaires du PABX traditionnel (*Private Automatic Branch eXchange ou central téléphonique privé*).

Parmi celles-ci, mentionnons entre autres :

- renvoi d'appel,
- mise en attente d'appels,
- affichage du numéro et du nom de l'appelant,
- sonnerie distincte (appel interne vers externe),
- indicateur de message en attente,

- conférence et transfert.

1.3- Le processus de traitement de la voix IP :

Dans ce paragraphe, on va présenter le principe de traitement de la VOIP, et les standards qui permettent de véhiculer la voix IP.

- Principe du transfert de la VOIP :

Le codec audio de l'émetteur numérise et compresse la voix. Ces données numériques, après la suppression du silence et l'ajout des en-têtes, sont acheminées jusqu'au destinataire des paquets IP. Ce processus est représenté par la figure :

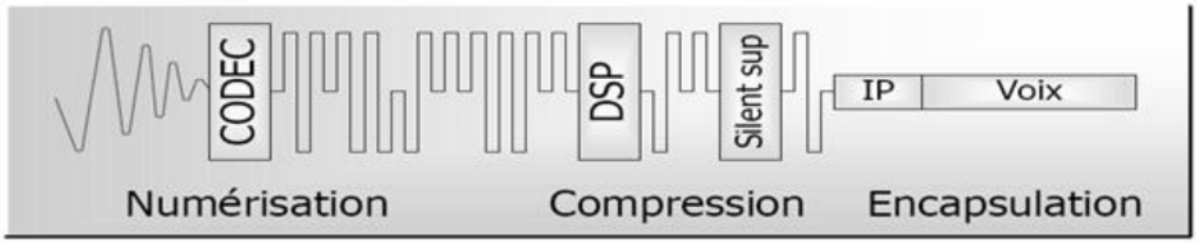


Figure III.1 : Processus de traitement de la VOIP

➢ Numérisation :

La bande voix qui est un signal électrique utilise une bande de fréquence de 300 à 3400 Hz. Ce signal doit d'abord être converti sous forme numérique suivant le format PCM (Pulse Code Mudulation), ou G.711 à 64Kbps. Si l'interface téléphonique est numérique (accès RNIS, par exemple), cette fonction est négligée. En effet, le signal est échantillonné à 8KHz selon la théorie de « Shannon », soit un échantillon toutes les 125ms. Chaque échantillon est ensuite codé sur 8 bits, ce qui donne un débit linaire de 8*8000 = 64 Kbit/s, ce débit linaire correspond à une voix numérique non compressée.

➢ Compression numérique :

De nombreux algorithmes permettent de réduire le besoin en bande passante à des débits nettement inférieurs (16,8 et même 4kbit/s) et d'augmenter ainsi l'efficacité du transport de la voix sur les réseaux informatiques orientés paquets.

Généralement, plus le taux de compression est élevé par rapport à la référence de 64Kbit/s, moins la qualité de la voix est bonne. Toutefois, les algorithmes de compression récents permettent d'obtenir des taux de compression élevé, tout en maintenant une qualité la voix acceptable. L'acceptabilité par l'oreille humaine des différents algorithmes est définie selon le critère MOS (Mean Operational Score), définie par l'organisme de normalisation international ITU (International Télécommunication Union). Pour la voix, le codec le plus utilisé et le G.711.

Mode de compression	Débit	Score d'écoute
G:711	64kbps	82%
G:726	32kbps	77%
G:728	16kbps	72%
G:729	8kbps	78%
G:723:1	6:3kbps	78%

Tableau III.1 : Liste des codes audio.

1. 4- Les paramètres de la voix sur IP :

Le problème de qualité de la voix sur IP est particulier. En effet la transmission de données qui autorise une dérive plus ou moins importante en terme de durée d'acheminement mais ne support aucune perte de données qui entraine de grave conséquences pour l'interprétation et l'utilisation de ces données l'équipement récepteur. Bien au contraire, la transmission de la voix agrée 1 % ou 2% de perte de données, mais en revanche un retard de 100ms est catastrophique et rend le service inutilisable. La voix attend donc du transport IP l'inverse de ce qu'exigent les données.

Plusieurs paramètres influent dans la transmission de la voix sur IP parmi les quelles :

1.4.1- Les différents échantillonnages :

Les paramètres d'échantillonnage ou codec (pour compression / décompression) est structurant en VOIP. Le codec détermine à quelle vitesse la voix est échantillonnée et dimensionnée par la même le flux de données numériques qui va générer la transformation d'un échantillon temporel de voix analogique. Les stocks sont répertoriés par leur nom à l'ITU (International Telecomunication Union).

1.4.2- Optimisation de la bande passante :

Pour un bon partage de la bande passante, il faut connaître l'ensemble des flux pouvant avoir une influence importante sur le transport de la voix.

1.4.3- La gigue de phase :

La gigue de phase ou variation de temps de transit est la conséquence du fait que tous les paquets contenant des échantillons de voix ne vont pas traverser le réseau à la même vitesse. Cela crée une déformation de la voix où la gigue est une conséquence de congestions sur le réseau, se dernier ne pouvant plus transporter les données de manières constante dans le temps.

1. 4.4- Le phénomène d'écho :

C'est le délai entre l'émission du signal et la réception du même signal en réflexion. Cet écho est causé par les composants électroniques des parties analogiques.

1. 4.5- Les pertes de paquets :

Lorsque les routeurs IP sont congestionnés, ils « libèrent » automatiquement de la bande passante en se débarrassant d'une certaine proportion des paquets entrants en fonction de seuils prédéfinis. Cela permet également d'envoyer un signal implicite aux sources TCP qui diminue d'autant leur débit au vu d'acquittements négatifs émis par la destinataire qui ne reçoit plus les paquets.

1.4.6- La sécurité :

Tous les postes téléphoniques deviennent accessibles depuis l'extérieur, par écoute de la conversation, déni de service, alors il n'y a aucune importance si l'information transmise ou non tant qu'elle sera attaquée.

En conclusion, le transport de la VOIP ne doit suffire d'aucun retard de la transmission, ni d'altération, ni de perte de paquets ce qui n'est pas réellement appliqué.

1.5- Les protocoles de transport de la VOIP :

Le transport de la VOIP met en jeu de nombreux protocoles de couches inférieures à celle qui contient l'information voix qui parmi lesquels TCP (Transmission Contrôle Protocole), UDP (User Datagramme Protocol) et RTP (Real Time Protocol). Les protocoles de transport classiquement utilisée pour transporter des données sont TCP et UDP. Le protocole TCP assure un bon contrôle de l'intégrité des informations transportées (mécanisme d'accusé de réception), mais n'est pas particulièrement performant en termes de ce fait, de meilleurs performances moyennes, car il permet l'envoi de paquets sans contrôle de réception (pas d'acquittement).

Le transport de la voix répond à des exigences différentes de celle relative au transport de données, à savoir les délais, sans garantie aussi forte de fiabilité. Le protocole répondant à ces exigences et le protocole RTP utilisé pour les flux temps réel encapsulés dans des paquets UDP. Le protocole RTCP (Real Time Contrôle Protocole) est associé à RTP afin de lui fournir les fonctionnalités de contrôle de la QOS (Quality Of Service) qui lui manquent.

1.6- Quel est l'avantage de VOIP sur RTCP :

Quand vous utiliser une ligne de RTCP, vous payer généralement le temps de communication à la société qui gère la ligne téléphonique, plus vous passer le temps au téléphone et plus vous payez. De plus, vous nous pouvez parler qu'à une personne à la fois.

La VOIP vous permet au contraire, à tout moment de parler à la personne que vous souhaitez (pourvu qu'elle soit à l'Internet au même moment), aussi longtemps que vous le souhaitez (sans coût supplémentaire) et de plus, vous pouvez parler à plusieurs personnes en même temps.

Si vous n'êtes pas encore convaincu, considérez qu'il est possible en simultané, d'échanger des données avec vos interlocuteurs, d'envoyer des images, des graphiques et des vidéos.

1.7 - Caractéristique de la voix :

Le système vocal est complexe est basé sur des ondes sonores de différentes fréquences. Le spectre des fréquences perçues par l'oreille humaine s'étale de 100Hz à 20 KHz. Cette fourchette est cependant à réduire si l'on peut distinguer les fréquences utiles des fréquences audio.

- **La conversation orale : une exigence d'interactivité :**

Une conversation entre deux personnes respecte deux principes : intelligibilité et interactivité. Couper la parole à quelqu'un ne se fait pas, mais c'est un gage d'interactivité et de dialogue. En termes de transmission numérique, cela se traduit par le terme duplex. Une conversation full duplex assure cette interactivité car chaque locuteur peut parler en même temps, ce qui arrive quand deux personnes parlent de leurs propres expériences sans s'écouter.

1.8- Les modes d'accès:

Le mixage de l'ensemble des services et équipements divers introduit l'intégration de la voix et des données.

En effet, il existe trois (03) différents scénarios d'architectures possibles qui répondent aisément à un besoin ou à un objectif différent.

1.8.1-Téléphonie de PC à PC :

Dans ce scénario, les deux correspondants utilisent un PC rattaché au réseau Internet par l'intermédiaire d'un fournisseur d'accès Internet. Cette technique nécessite des participants à la communication d'avoir un PC muni d'un modem, d'une carte réseau, d'un microphone, d'un haut-parleur et d'un logiciel de téléphonie IP compatible de chaque côté. La voix est comprimée et décomprimée par un logiciel de compression. Ce mode de fonctionnement

nécessitait auparavant que les correspondants se fixent un rendez-vous préalable sur Internet ou soient connectés en permanence.

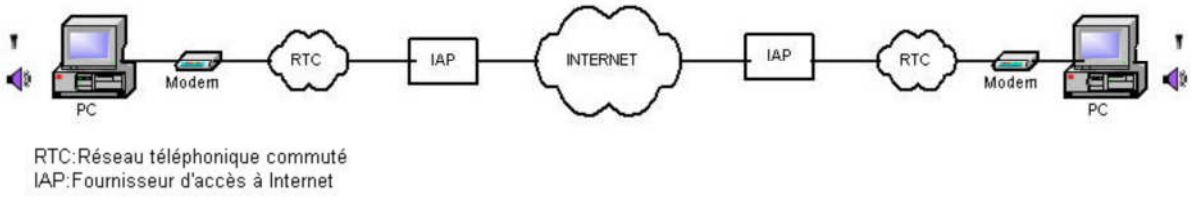


Figure III.2 : Téléphonie de PC à PC

1.8.2-Téléphonie entre PC et poste téléphonique et vis-versa :

Dans ce scénario, l'un des correspondants utilise un PC rattaché au réseau Internet par un fournisseur d'accès Internet, l'autre correspondant utilise un téléphone rattaché au réseau téléphonique commuté. Une passerelle est nécessaire ente les deux réseaux pour rendre possible cette technique et faire la conversion entre réseaux (dans ce cas elle fait la conversion Internet-RTC et vis versa).

Elle se charge également de l'appel du correspondant et de l'ensemble de la signalisation relative à la communication téléphonique du côté du correspondant demandé. Du côté PC, une signalisation d'appels est nécessaire pour établir une communication et négocier les paramètres de communication multimédia.

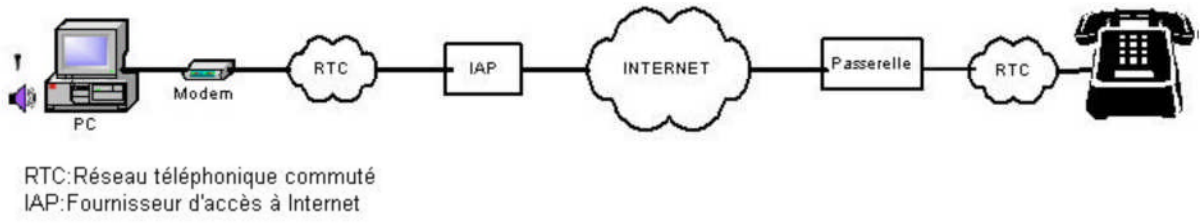


Figure III.3 : Téléphonie entre PC et poste téléphonique

1.8.3- Téléphonie entre postes téléphoniques :

Dans ce cas les deux correspondants utilisent un téléphone conventionnel via le réseau téléphonique commuté. Une passerelle est utilisée de chaque côté entre ce réseau et le réseau

Internet pour convertir la voix IP en voix et vis-versa. Le réseau Internet est utilisé pour la connexion longue distance.

RTC:Réseau téléphonique commuté
IAP:Fournisseur d'accès à Internet

Figure III.4 : Téléphonie entre postes téléphoniques

1.9 - Avantages et inconvénients de la téléphonie IP :

Il est facile de constater que les offres concernant la VoIP foisonnent. L'industrie de la téléphonie se trouve, aujourd'hui, plongée dans un nouveau paradigme technologique.
Des solutions fonctionnelles existent et les bénéfices anticipés que nous présentent les différents fournisseurs semblent fort alléchants. Mais des inconvénients se retrouvent également parmi ce lot de bénéfices. Voici donc les principaux avantages et inconvénients repérés.

- ***Avantage :***

La VoIP offre plusieurs nouvelles possibilités aux opérateurs et aux utilisateurs qui bénéficient d'un réseau basé sur IP. Ses avantages les plus marqués sont les suivants :

- Flexibilité
- Réduction des coûts
- Simplification de la gestion des réseaux voix, données et vidéo
- Amélioration de la productivité et du service à la clientèle
- L'accessibilité

- ***Inconvénients :***

Vendeurs et critiques présentent souvent une image très « rose » des centres de relations IP et de ses bénéfices. Néanmoins, même si les bénéfices peuvent être significatifs, les gestionnaires des centres de relations clientèle demeurent préoccupés par la rentabilité, l'interopérabilité et la qualité sonore des différentes solutions IP.

- Fiabilité et qualité sonore
- Technologie émergente et constante évolution des normes
- Dépendance de l'infrastructure technologique et support administratif exigeant.

Prendre en considération que la qualité sonore sera différente (un peu comme quand les cellulaires numériques sont arrivés) et que cette technologie dépend d'Internet (légers délais à prévoir, pannes, etc).

1.10-Avenir de téléphonie IP :

La téléphonie IP est une bonne solution en matière d'intégration, de fiabilité, d'évolution et de coût. Elle fera vraisemblablement partie intégrante des intranets d'entreprises dans les années à venir et apparaîtra aussi dans la téléphonie publique pour permettre des communications à bas coût.

Le résultat montrent que le phénomène de migration vers les systèmes de téléphonie sur IP en entreprise est actuellement engagé, et ce qu'il s'agisse d'entreprises multi sites.

De nombreuses entreprises connaissent la téléphonie sur IP. Cependant, la majorité des organisations sont au même stade. On peut vraisemblablement penser que le protocole IP deviendra un jour un standard mondialisé.

2-Les protocoles de la voix IP

2.1-Le Standard H.323 :

Le standard H.323, développé par l'ITU–T, est défini comme étant le standard spécifiant les éléments, les protocoles et les procédures pour réaliser des communications audio, vidéo et autres données en temps réel sur les réseaux de paquets.

Il décrit également les terminaux, équipements, et services nécessaires à l'établissement d'une communication multimédia sur un réseau local ne garantissant pas une qualité de service optimale.

Il spécifie aussi les protocoles, les méthodes et les éléments des réseaux qui sont nécessaire à l'établissement de connections multimédia point à point, multipoint et de conférences multimédia entre trois parties et plus.

2.1.1- Les éléments du H.323 :

Les éléments de base du standard H.323 sont les terminaux, les gardes-barrières, les passerelles et les unités de contrôle multipoint MCUs. Les MCUs sont cités séparément, mais en pratique ils font souvent partie des gardes-barrières ou des ordinateurs rapides qui servent plusieurs utilisateurs

- Terminaux :

Un terminal est un périphérique qui supporte les communications multimédia Bidirectionnelles en temps réel.

Tous les terminaux H.323 doivent supporter H.245, RAS (Registration Admission Status) et RTP (Real Time Transport Protocol).

Un terminal H.323 fournit les services suivants :

- Services H.245 : l'échange de capacités et la gestion des canaux logiques.
- Services H.225 : gestion de la signalisation des appels.
- Services RAS : l'enregistrement auprès du garde-barrière.
- Services RTP / RTCP : Séquencement des paquets audio et vidéo.

- Gardes-barrières :

Le garde-barrière est un élément vital dans un système H.323. Il joue le rôle de contrôleur pour tous les appels à l'intérieur de la zone H.323 (une zone H.323 est une agrégation de garde-barrière et de tous les autres éléments terminaux et MCU qui son enregistré auprès de lui). Il fournit les services aux éléments qui sont enregistrés enregistré auprès de lui). Il fournit les services aux éléments qui sont enregistrés t'auprès de lui tel que la conversion des adresses, le contrôle d'admission, la gestion de la bande passante et la capacité de routage

- Passerelles :

Une passerelle H323 est un élément du réseau qui assure la conversion voulue entre la bande passante et la capacité de routage les formats de transmission (par exemple, du format H.225.0 au format H.221 ou vice versa) ainsi qu'entre les protocoles de communication (par exemple du protocole H.245 au protocole H.242 ou vice versa). La passerelle assure aussi l'établissement et la libération des communications tant du côté réseau à commutations de paquets que du côté réseau à commutation de circuits.

-Les unités de contrôle multipoint (MCUs) :

Le MCU est un élément du réseau qui fournit les capacités à plusieurs terminaux et passerelles pour participer à une conférence multipoint. En d'autres termes, un MCU gère les ressources de la conférence et les échanges de capacités. Le MCU se compose de deux

parties : un contrôleur multipoint obligatoire qui assure la gestion d'au moins trois terminaux participants à une conférence multipoint. Le contrôleur multipoint permet de négocier avec tous les terminaux les moyens à mettre en Ouvre pour parvenir à établir des communications multimédia. Il peut également exercer un contrôle au niveau des ressources de la conférence pour déterminer par exemple l'entité qui transmet en multicast. La deuxième partie est le processeur multipoint facultatif qui assure le traitement centralisé des flux de données dans une conférence multipoint.

2.1.2- Protocoles et procédures

La recommandation H323 enveloppe d'autres recommandations pour permettre les communications en temps réel.

Le tableau IV résume quelques unes d'entre elles :

Recommandation	**Aperçu**
Codecs Audio G.723. G.711 G.729	Recommandations du H323 Encode le signal selon les lois A ou ì en 64 Kbit/s Encode et compresse le signal vocal en 8 et 13 Kbits/s
Codecs Vidéo H.261 H.263	Encode et compresse la vidéo en 64 kb/s
Communication de données T.120	Protocole de données pour les conférences multimédia
Contrôle H.245 H.225.0 Transport temps réel RTP / RTCP	Protocole de contrôle pour les communications de Données Protocole de signalisation des appels
Sécurité H.235	Sécurité, cryptage pour les terminaux des séries H32x
Sécurité H.235	Sécurité, cryptage pour les terminaux des
Services supplémentaires H.450.1 H.450.2 et H. 450.3	1 Protocole pour les services supplémentaire Transfert d'appels et autres services supplémentaires

Tableau III.2 : Recommandations du H323

2.1.3- La pile H323 :

La figure (III.8) montre la pile des protocoles spécifiés par le standard H323

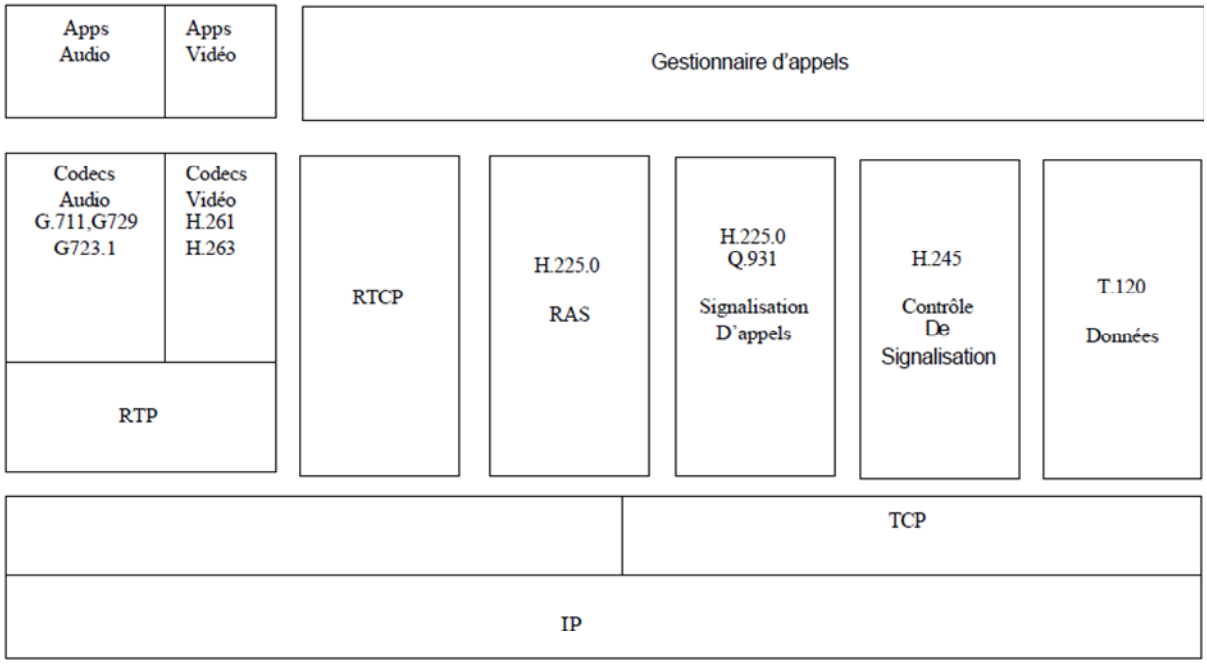


Figure III.5 : La pile de protocole du terminal H.323

Cette pile est indépendante des réseaux et des protocoles de transport utilisés.

Si le protocole IP est utilisé (ce qui est le plus souvent le cas) alors les paquets audio, vidéo et H.225.0 RAS utilisent UDP comme protocole de transport alors que les paquets de contrôle (H.245 et H.225.0 call signaling) utilisent TCP.

La pile H323 est constituée des éléments décrits ci-dessous :

- **Les codecs Audio :**

H323 spécifie une série de codecs audio classés par débits allant de 5.3 à 64 kb/s. G.711 est le codec le plus populaire conçu pour les réseaux de téléphonie. Aujourd'hui, les terminaux H323 supportent le codec G.723.1 qui est plus efficace et produit une Appels Audio meilleure qualité audio à 5.3 kb/s et 6.3 kb/s. Les codecs G.729 utilisent la quantification à prédiction linéaire pour produire une qualité supérieure à des taux de16 kb/s et 8 kb/s

- **Les codecs Vidéo :**

La communication vidéo nécessite une bande passante importante, d'où l'intérêt d'avoir des techniques de compression et de décompression performante.

H323 spécifie deux codecs vidéo : H.261 et H.263.

- Les codecs H.261 produisent la transmission vidéo pour des canaux avec une bande passante de p x 64 kb/s (p est une constante qui varie de 1 à 30)
- Les codecs H.263 sont conçus pour des transmissions à faible débit sans perte de qualité.

2.1.4- Conférence de données :

Les capacités de la conférence de données en temps réel sont requises pour des activités telles que le partage d'applications, le transfert de fichiers, la transmission de fax, la messagerie instantanée. La recommandation T.120 fournit ces capacités optionnelles au H.323

2.1.5- Mécanismes de contrôle et de signalisation :

Le flux d'informations dans les réseaux H323 est un mixage de paquets audio, vidéo, données et de contrôle. L'information de contrôle est essentielle pour l'établissement et la rupture des appels, l'échange et la négociation des capacités. H323 utilise trois protocoles de contrôles : Contrôle multimédia H.245, signalisation d'appel H.225/ et H.225.0 RAS.

- **La signalisation :**

La signalisation est indispensable pour établir une communication téléphonique. Elle permet dans un premier temps d'envoyer des messages avant la communication, d'avertir l'utilisateur et de connaître la progression de l'appel enfin de mettre un terme à la communication.

Il existe actuellement deux protocoles de signalisation pour les réseaux IP, la signalisation H.225 qui fait partie du standard H323 et le récent protocole SIP.

-Signalisation des appels H.225 :

La signalisation des appels est importante pour établir et rompre une connexion entre deux entités. Q.931 a été développé initialement pour la signalisation dans les Réseaux Numériques à Intégration de Service (ISDN). H.225.0 a adopté la signalisation Q.931 en l'incluant dans le format de ses messages.

Deux entités désirant établir une connexion doivent ouvrir un canal de signalisation. La signalisation d'appels H.225.0 est envoyée directement entre les entités périphériques quand aucun garde-barrière n'est utilisé. Si un garde-barrière est utilisé alors la signalisation d'appels H.225.0 doit être routée à travers ce garde-barrière.

-H.225.0 RAS :

Les messages H.225.0 RAS (registration, admission, status) définissent une communication entre les terminaux et un garde-barrière. H.225.0 RAS s'occupe de la communication entre le garde-barrière et les différents terminaux. Elle gère les opérations

suivantes : l'inscription, le contrôle d'admission, la gestion de la bande passante. Un canal de signalisation est utilisé afin de transporter les différents messages RAS.

-Le protocole de contrôle de signalisation H.245 :

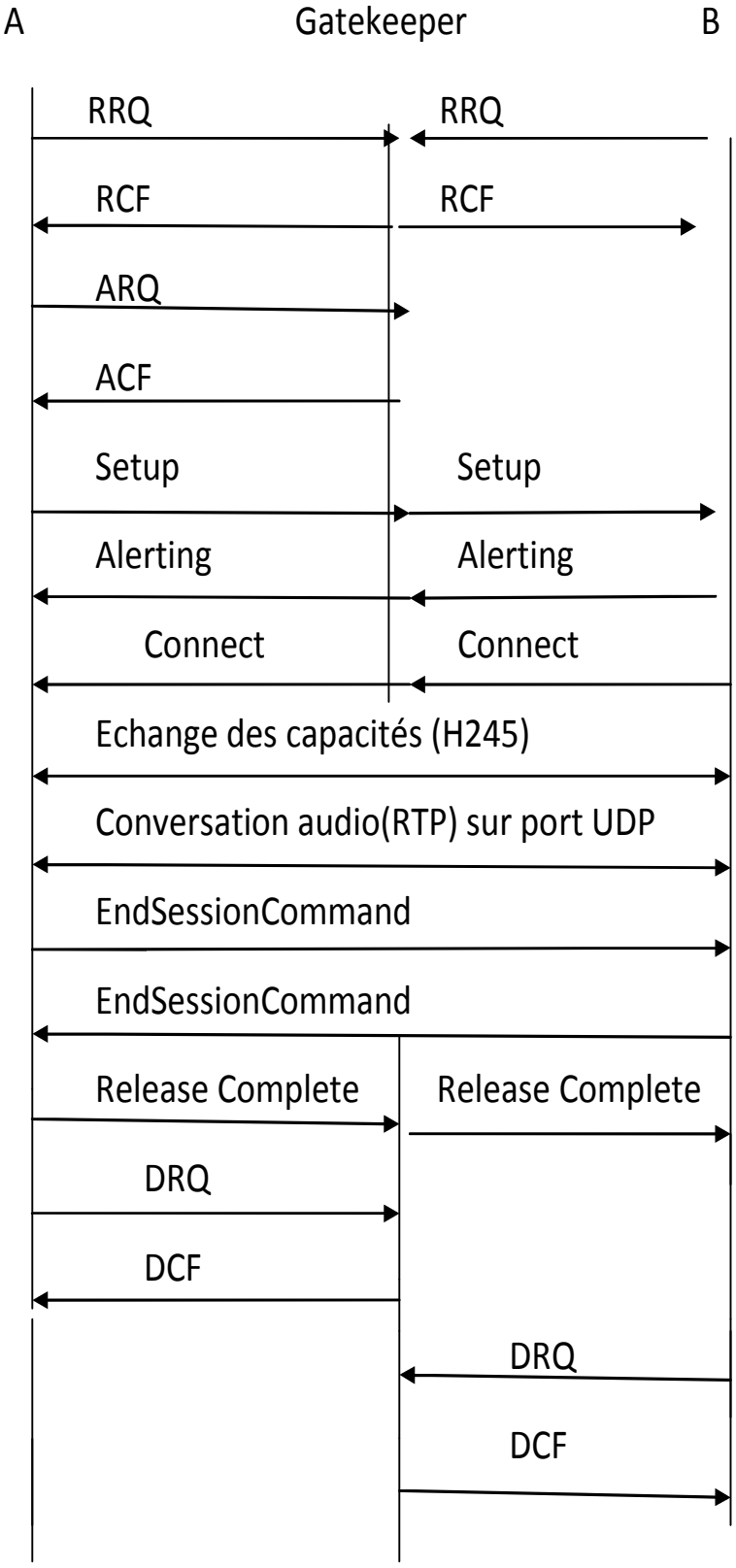
La flexibilité de H.323 nécessite que les différends terminaux négocient les capacités avant que les liens de la communication audio, vidéo et/ou données ne soit établit.

H.245 utilise les messages de contrôle et de commandes qui sont échangés durant l'appel. Ces messages sont classés en quatre catégories :

Messages d'échanges de capacités :

1. Messages pour la gestion des canaux logiques.
2. Messages pour la gestion des flux de contrôle.
3. Commandes générales et indications.

- **Etapes d'une communication entre deux terminaux H323.**



RRQ (Registration Request) : les deux terminaux envoient RRQ au Gatekeeper pour les enregistrer.

RCF (Registration Confirm) : Le Gatekeeper repend par le message RCF que la demande est effectué.

ARQ (Admission Request) : Le terminal A envoie au Gatekeeper le message ARQ pour lui permet de faire l'appel.

ACF (Admission confirm) : Le Gatekeeper envoie une repense oui (ACF) au terminal A.

SETUP : Le terminal A envoie un message d'initialisation (Setup) au Gatekeeper et il renvoie une confirmation à A et transmet le message d'initialisation reçu au terminal B.

Alerting : En attendant que B décroche, le Gatekeeper envoie au terminal A des message « Sonnerie et Traitement d'appel en cour »(Alerting),pour indiquer la progression de l'appel.

Connect : Une fois que B décroche les échanges de message H.245, pour la détermination des formats des médias et l'ouverture des canaux RTP/RTCP, B indique à A ou ce dernier peut envoyer ses données RTP et ses données de contrôle RTCP.

Echange des capacités(H245) : chaque terminal envoie ce message à l'autre, indique l'accuser de réception.

Conversation audio : Echange de conversations entre les deux terminaux.

EndSessionCommande : Celui qui raccroche envoie un message H.245(EndSessionCommande), attend de recevoir le même message de son interlocuteur et ferme le canal de control H.245.

Release Complete : si un canal de signalisation à été ouvert, chaque terminal doit envoyer au Gatekeeper un message Release Complete avant de les fermer.

DRQ : les deux terminaux envoient le message DRQ au Gatekeeper informant que la session prenne la fin.

DCF : les deux terminaux envoient le message DCF au Gatekeeper informant que la session est fermée.

2.2-Standard SIP:

SIP (Session Initiation Protocol) est un protocole de contrôle de couche application basé sur l'ASCII qui peut être utilisé pour établir, maintenir, libérer des appels entre deux ou plusieurs points d'extrémités. SIP est un protocole alternatif développé par l'IETF (Internet Engineering Task Force) pour de la conférence multimédia sur IP. Les fonctionnalités de SIP sont conformes avec le RFC 2543, SIP Session Initiation Protocol, publié en Mars 1997.

L'implémentation SIP de Cisco permet aux plateformes Cisco supportées de signaler l'établissement d'appels pour la voix et le multimédia sur des réseaux IP.

Comme d'autres protocoles VoIP, SIP est conçu pour répondre aux fonctions de gestion de la signalisation et de session dans un réseau de téléphonie par paquets. La signalisation permet aux informations d'appel d'être transportées à travers le réseau. La gestion de session fournit la possibilité de contrôler les attributs d'une communication de bout en bout.

2.2.1-Capacités de SIP : SIP a les capacités suivantes:

-Localise l'extrémité cible SIP supporte la résolution d'adresse, le lapping de nom et la redirection d'appel.

-Détermine les capacités média de l'extrémité cible SIP détermine le niveau de service commun le plus bas entre les deux extrémités au travers de SDP (Session Description Protocol). Les conférences sont établies en utilisant les capacités média qui peuvent être supportées par les deux extrémités.

-Détermine la disponibilité de l'extrémité Si un appel ne peut pas aboutir car l'extrémité cible est indisponible, SIP détermine si l'extrémité appelée est déjà connectée avec un appel en cours ou ne répond pas après le nombre de sonneries paramétré.

-Etablit une session entre les extrémités origine et cible si l'appel peut aboutir, SIP établit une session entre les extrémités.SIP supporte également les modifications en cours de communication telles que l'addition d'une autre extrémité à la conférence, le changement de caractéristique de média ou de codec.

- Gère le transfert et la fin de communication SIP supporte le transfert d'appel d'une extrémité vers une autre. Pendant le transfert d'appels, SIP établit une session entre le transféré et la nouvelle extrémité (spécifiée par la partie transférante) et termine la session entre le transféré et la partie transférante. A la fin de la session SIP ferme les sessions entre toutes les parties.

2.2.2- Composants SIP :

SIP est un protocole d'égal à égal (Peer-to-Peer). Les extrémités dans une session sont appelées agents utilisateurs (User Agents). Un agent utilisateur peut avoir un des rôles suivants:

-User-Agent Client (UAC) Une application cliente qui initie une requête SIP.

-User-Agent-Server (UAS) Une application serveur qui contacte l'utilisateur quand une requête SIP est reçue et qui retourne une réponse à la demande de l'utilisateur.

Typiquement, une extrémité SIP est capable de fonctionner dans les modes UAC et UAS, mais fonctionne dans l'un ou l'autre mode par transaction. Que l'extrémité fonctionne comme un UAC ou un UAS dépend de l'agent utilisateur d'un point de vue architectural, les composants physiques d'un réseau SIP peuvent être groupés en deux catégories: Clients (extrémités) et Serveurs. La figure suivante illustre l'architecture d'un réseau SIP.

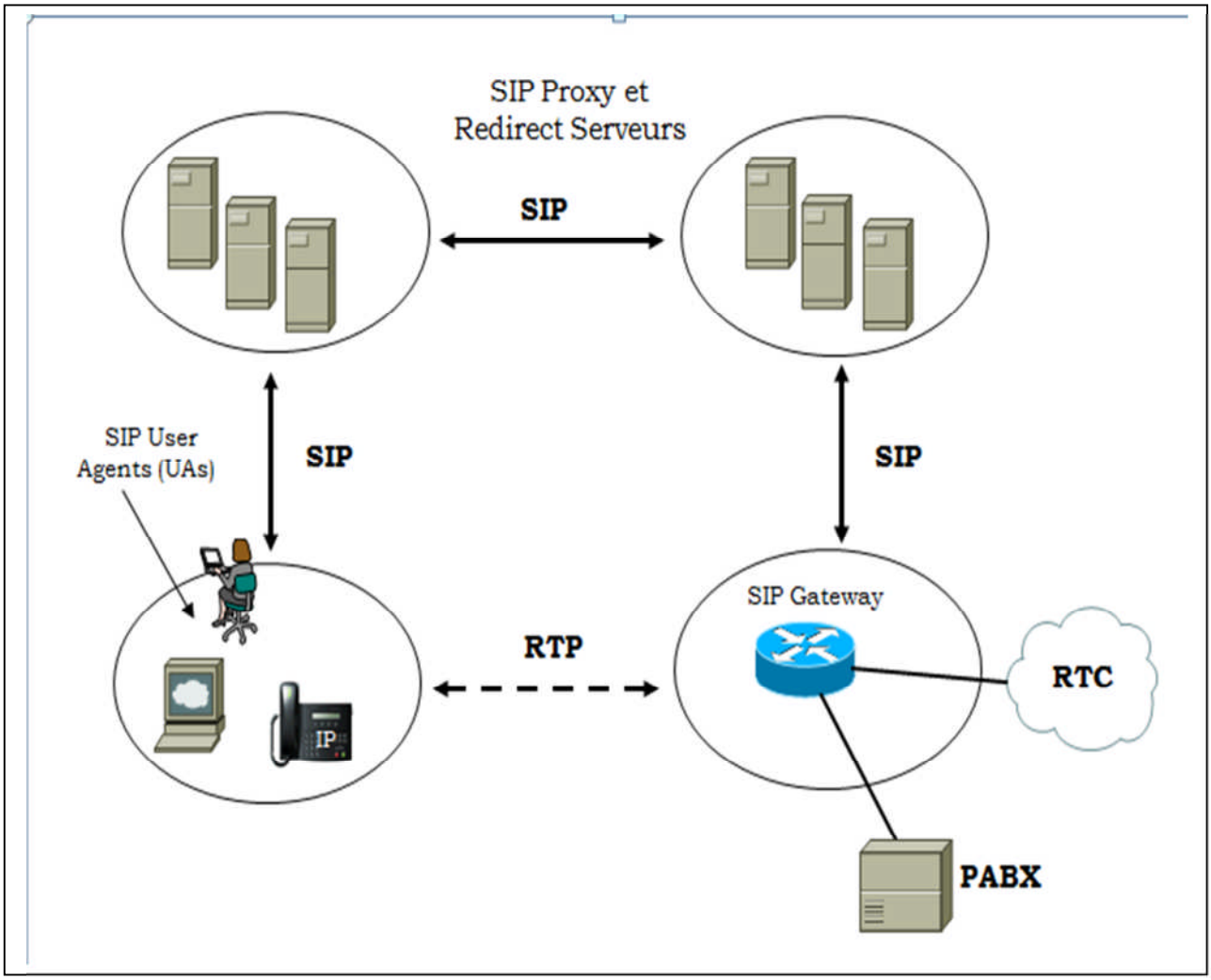


Figure III.6 : L'architecture d'un réseau SIP.

- **Clients SIP :**

- Téléphones Peuvent agir comme UAC ou UAS.

- Des Soft phones (PCs avec des fonctions téléphone installées) et des téléphones Cisco SIP IP peuvent initier des requêtes SIP et répondre aux requêtes.

- Ephones - Téléphones IP non configurés sur la passerelle.

-Passerelles (Gateways) - Fournissent le contrôle d'appel. Les passerelles fournissent plusieurs services, le plus commun étant une fonction de traduction entre les extrémités de conférence SIP et d'autres types de terminaux. Cette fonction comprend la traduction des formats de transmission et des procédures de communication. En plus la passerelle traduit entre codecs audio et vidéo, réalise l'établissement d'appel et la libération de communication du côté LAN et du côté réseau à commutation de circuits.

- **Serveurs SIP :**

-Proxy Server Reçoit les requêtes SIP d'un client et les achemine vers l'autre client. De manière basique, les serveurs proxy reçoivent des messages SIP et les acheminent vers le prochain serveur SIP dans le réseau. Les serveurs proxy peuvent fournir des fonctions telles que l'authentification, l'autorisation, le contrôle d'accès réseau, du routage, la retransmission fiable de requête et la sécurité.

2.2.3-Comment SIP fonctionne :

SIP est un protocole simple, basé sur l'ASCII, qui utilise des requêtes et des réponses pour établir des communications parmi les divers composants d'un réseau et optionnellement d'établir une conférence entre deux ou plusieurs extrémités. Les utilisateurs d'un réseau SIP sont identifiés par une adresse SIP unique. Une adresse SIP est similaire à une adresse e-mail dont le format est: sip:*userID@gateway.com*. L'user ID peut être soit un nom d'utilisateur soit une adresse E164. Les utilisateurs s'enregistrent avec un serveur d'enregistrement en utilisant leur adresse SIP affectée. Le serveur d'enregistrement fournit cette information au serveur de localisation sur requête.

Quand un utilisateur initie un appel, une requête SIP est transmise vers un serveur SIP, la localisation d'un utilisateur peut être enregistrée dynamiquement avec un serveur SIP. Le serveur de localisation peut utiliser un ou plusieurs protocoles pour localiser l'utilisateur. Comme l'utilisateur peut être connecté sur plusieurs stations et que le serveur de localisation peut avoir quelque fois des informations imprécises, celui-ci peut retourner plusieurs adresses pour l'utilisateur.

2.2.3.1-Comment SIP fonctionne avec un Proxy Server :

Si un Proxy server est utilisé, l'agent utilisateur de l'appelant transmet une requête INVITE au Proxy server, le proxy server détermine le chemin et achemine la requête vers la partie appelée.

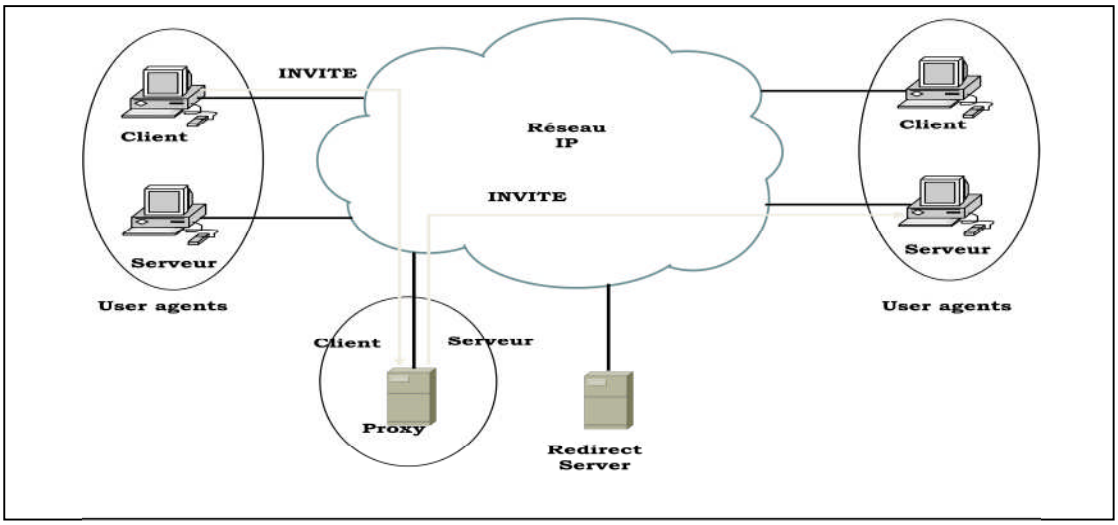


Figure III.7 : Requête SIP à travers un Proxy Server

La partie appelée répond au Proxy Server qui à son tour achemine la réponse vers l'appelant.

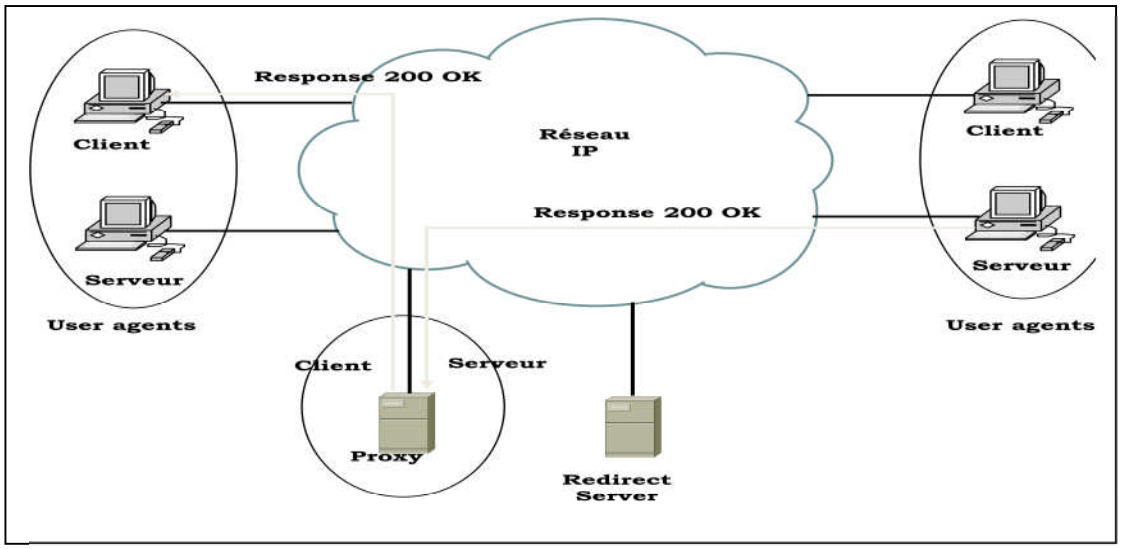


Figure III.8 : Requête SIP à travers un Proxy Server

Le Proxy Server achemine les acquittements des deux parties. Une session est ensuite établie entre les parties appelante et appelée. RTP (Real-time Transfer Protocol) est utilisé pour la communication entre les parties appelante et appelée.

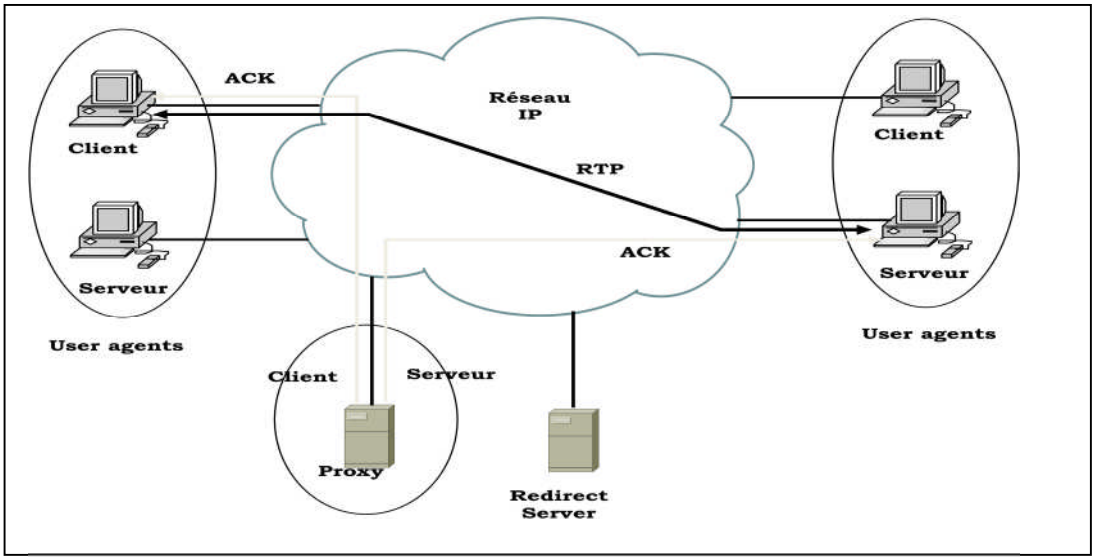


Figure III.9 : Requête SIP à travers un Proxy Server

2.2.3.2-Comment SIP fonctionne avec un Redirect Server :

Si un Redirect Server est utilisé, l'agent utilisateur de l'appelant transmet une requête INVITE au Redirect Server, le Reditrect Server contacte le serveur de localisation pour déterminer le chemin vers la partie appelée et ensuite le Redirect Server renvoie l'information vers l'appelant. L'appelant acquitte la réception de l'information.

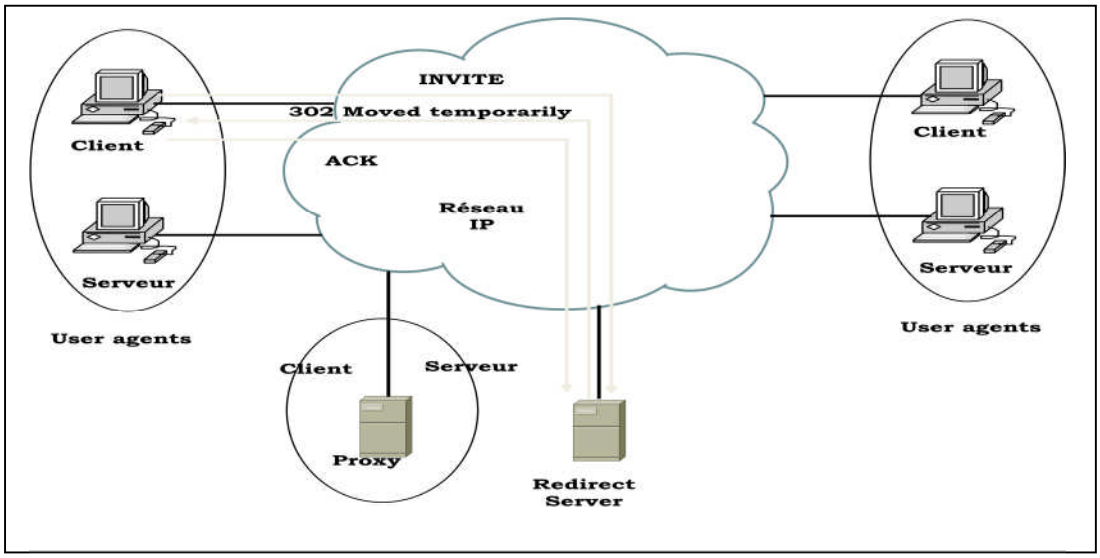


Figure III.10 : Requête SIP à travers un Redirect Server

L'appelant transmet la requête à l'équipement indiqué dans l'information de redirection (qui peut être la partie appelée ou un autre serveur qui achemine la requête).

Une fois que la requête atteint la partie appelée, celle-ci une réponse et l'appelant acquitte cette réponse. RTP (Real-time Transfer Protocol) est utilisé pour la communication entre les parties appelante et appelée.

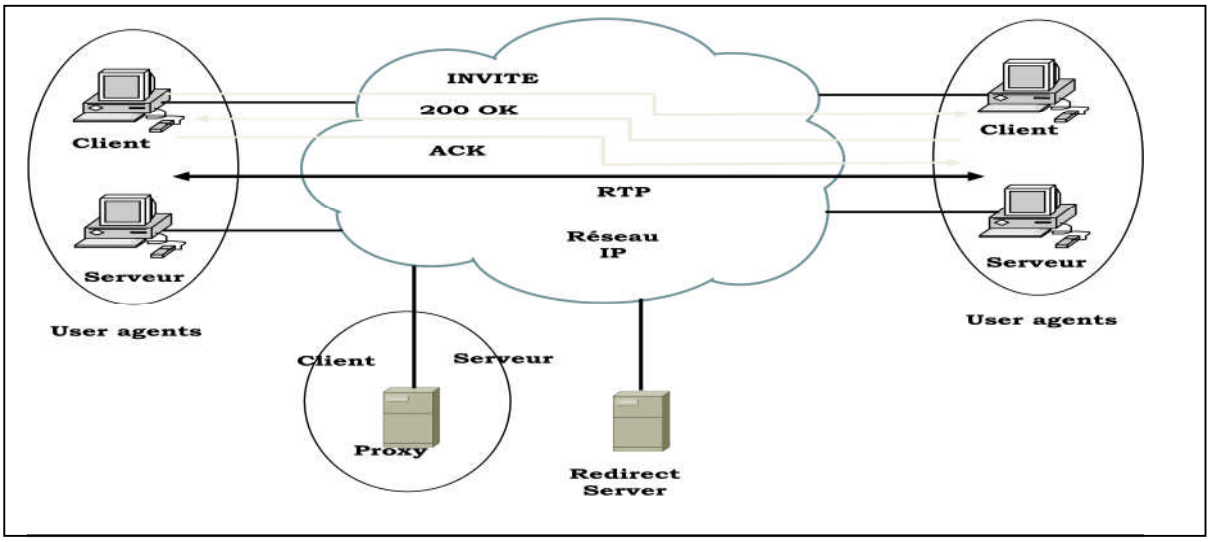


Figure III.11 : Requête SIP à travers un Redirect Server

2.2.4-Communications SIP :

Cette section décrit les communications pour les scénarios suivants qui illustrent des communications réussies:

- SIP Gateway vers SIP Gateway - Call Setup ET Disconnect
- SIP Gateway vers SIP Gateway - Appel via Redirect Server SIP
- SIP Gateway vers SIP Gateway - Appel via Proxy Server SIP

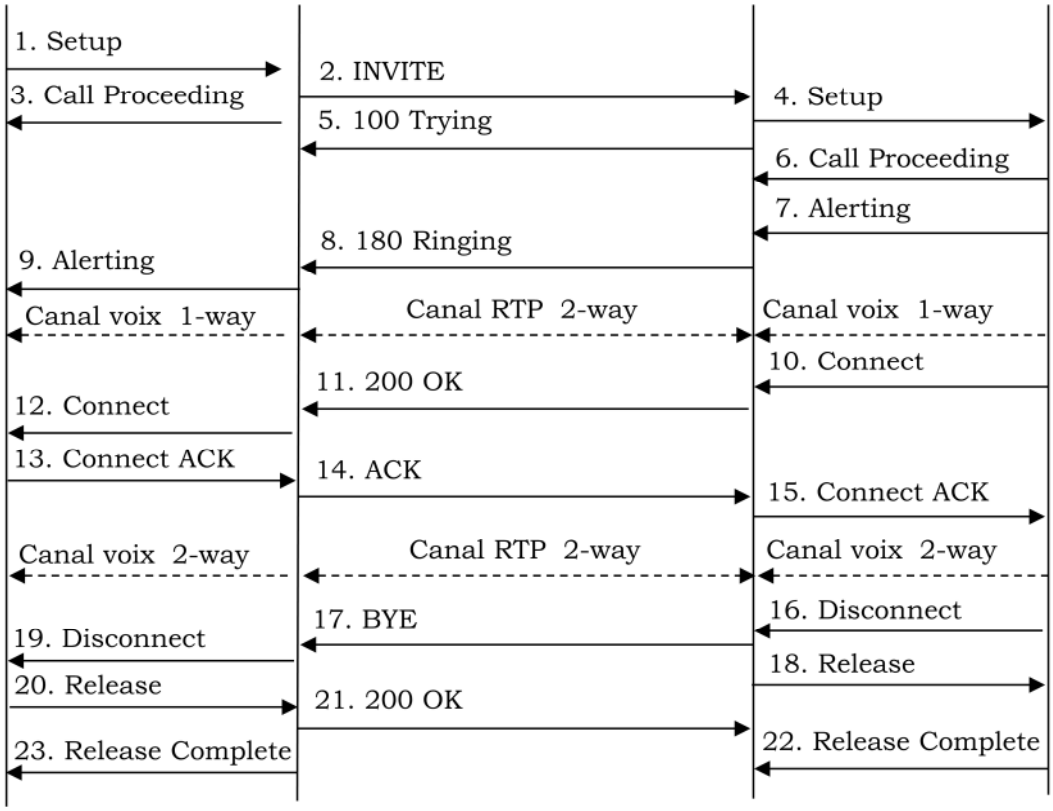
➢ SIP Gateway vers SIP Gateway - Call Setup ET Disconnect

La figure suivante montre un établissement d'appel et une déconnexion Gateway vers Gateway réussis. Les deux utilisateurs d'extrémités sont User A et User B. User A est localisé sur PBX A qui est connecté à une passerelle SIP(GW1) via une liaison. User B est situé sur PBX B qui est connecté à une passerelle SIP (GW2) via une liaison. Le numéro de téléphone d'USER B est 555 0100. La passerelle SIP GW1 est connectée à la passerelle GW2 par un réseau IP. Le scénario de la communication est le suivant:

1. User A appelle User B

2. User B répond à l'appel

3. User B termine la communication



Message	**Description**
1. Setup	Le message Setup comprend les transactions standards effectuées lorsqu'User A tente d'appeler User B.
2. INVITE	La passerelle SIP GW1 transmet une requête INVITE à la passerelle SIP GW2. La requête invite est une demande faite à User B de participer à une session de communication.
3.Call Proceeding	La passerelle SIP GW1 transmet un message Call Proceeding vers PBX A pour acquitter la requête Setup.
4. Setup	La passerelle SIP GW2 reçoit la requête INVITE de la passerelle SIP GW1 et initie un message Setup vers User B via PBX B.
5. 100 Trying	La passerelle SIP GW2 transmet une réponse 100 String à la requête INVITE transmise par la passerelle SIP GW1. La réponse 100 Trying indique que la requête INVITE a bien été reçue par la passerelle SIP GW2 mais qu'User B n'a pas été encore localisé et qu'une action non spécifiée est en cours.
6. Call Proceeding	PBX B transmet un message Call Proceding vers la passerelle SIP GW2 pour acquitter la requête Setup.
7. Alerting	PBX B localise User B et transmet un message Alert vers la passerelle SIP GW2. Le téléphone d'User B commence à sonner.

8. 180 Ringing	La passerelle SIP GW2 transmet un message 180 Ringing vers la passerelle SIP GW1. La réponse 180 Ringing indique que la passerelle SIP GW2 a localisé User B et tente d'alerter User B.
9. Alerting	La passerelle SIP GW1 transmet un message Alert vers User A via PBX A. Le message Alert indique que la passerelle SIP GW1 a reçu une réponse 180 Ringing de la passerelle SIP GW2. User A entend la tonalité de retour d'appel qui indique qu'User B est alerté
10. Connect	User B répond à l'appel. PBX B transmet un message Connect vers la passerelle SIP GW2. Le message Connect notifie à la passerelle GW2 que la connexion a été faite.
11. 200 OK	La passerelle SIP GW2 transmet un message 200 OK vers passerelle SIP GW1 que la connexion a été faite.
12. Connect	La passerelle SIP GW1 transmet un message connecte vers PBX A. Le message Connecte notifie à PBX A que la connexion a été faite.
13. Connect	PBX A acquitte le message Connect de la passerelle SIP GW1.
14. ACK	La passerelle SIP GW1 transmet un message ACK vers la passerelle SIP GW2. Le message ACK confirme que la passerelle SIP GW1 a reçu le message de réponse 200 OK de la passerelle GW2.

15. Connect ACK	La passerelle SIP GW2 acquitte le message Connect de PBX B.
16. Disconnect	Lorsqu'User B raccroche son téléphone, PBX B transmet un message Disconnect vers la passerelle SIP-GW2. Le message Disconnect démarre le processus de libération de la session de communication.
17. BYE	La passerelle SIP GW2 transmet une requête BYE vers la passerelle SIP GW1. La requête BYE indique qu'User B veut terminer la communication.
18. Release	La passerelle SIP GW2 transmet un message Release vers PBX B.
19. Disconnect	La passerelle SIP GW1 transmet un message Disconnect vers PBX A.
20. Release	PBX A transmet un message Release vers la passerelle SIP GW1.
21. 200 OK	La passerelle SIP GW1 transmet un message 200 OK en réponse à la passerelle SIP GW2. Le message 200 OK notifie à la passerelle SIP GW2 que la passerelle SIP GW1 a reçue la requête BYE.
22. Release Complete	PBX B transmet un message Release Complete vers la passerelle SIP GW2.
23. Release Complete	La passerelle SIP GW1 transmet un message Release Complete vers PBX A et la session est terminée

Conclusion

La voix et la vidéo sur IP procurent des avantages certains aux entreprises et aux utilisateurs. Un seul réseau est utilisé pour la voix, la vidéo et les données, ce qui a pour conséquence de réduire les frais d'exploitations. D'autre part, les utilisateurs peuvent éviter les frais dus aux appels interurbains et payer uniquement les frais de connexions locales. D'autres applications de la voix et la vidéo sur IP permettent la tenue de réunions et de conférences multimédia.

Dans ce chapitre, nous avons présenté le principe de la téléphonie sur IP et des modes de communications des téléconférences multimédia. Nous avons également étudié les protocoles qui permettent ce genre d'applications. Parmi ces protocoles, nous avons présenté les protocoles de transports et de contrôles en temps réel RTP et RTCP qui utilisent le protocole UDP pour le transport de la voix et de la vidéo.

Nous avons étudié le standard H.323 et SIP qui permet entre autre la signalisation des appels.

Dans ce travail, nous parlerons de la simulation par packet tracer d'un réseau de deux stations différentes, la station de Tizi-Ouzou et la station de Boumerdes.

Par la suite nous discuterons de résultat obtenu de logiciel traceur d'appels pour les messages de protocole SIP qui déterminent, la nature d'appel puis déduire les différentes étapes pour chaque message.

1- Simulation par le logiciel Packet Tracer :

Dans notre travail nous avons réalisé une connexion entre deux réseaux, de stations déférentes, le réseau de la station de Boumerdes et le réseau de la station de Tizi ouzou, ces stations sont représentées par des routeurs et chacune d'elles est reliée à un réseau local LAN par un Switch vers les serveurs et chaque réseau local relié à l'autre formant un réseau WAN.

Tous les media Gateway de Boumerdes, Bouira et Bejaia sont commandé par le softeswitch de Tizi-Ouzou.

Pour suivre le chemin du message une topologie de réseau est établie à l'aide du simulateur de logiciel packet tracer, la figure suivante représente la topologie du réseau. Le Softswitch de Tizi-Ouzou qui commande par distance le Media-Gateways de Boumerdes.

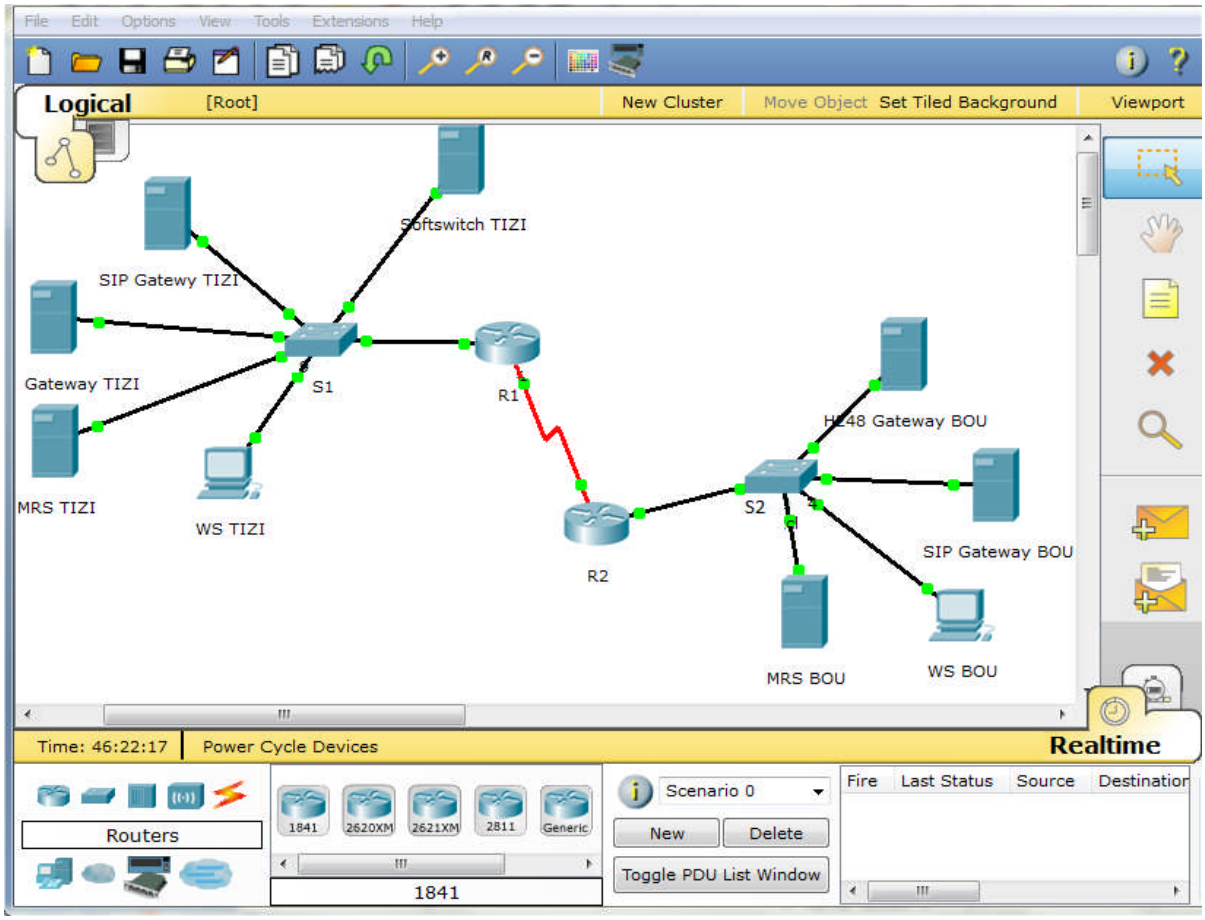


Figure IV.1 : Simulation d'un réseau par packet tracer.

Nous avons utilisé le logiciel packet tracer pour réaliser ce réseau et mise on marche

1.1-Représentation de logiciel packet tracer :

Le logiciel Packet Tracer version 5.0, permet aux utilisateurs de construire leur propre modèle ou des Réseaux virtuels, obtenir l'accès à des représentations graphiques de ces réseaux, d'animer ces réseaux en ajoutant leurs propres paquets de données, poser des questions sur ces réseaux et enfin, mettre leurs création.

IL fournit un environnement de simulation pour la formation de réseaux, il offre une combinaison unique d'outils de visualisation, l'évaluation des complexes et des capacités de création d'activité, et les possibilités de collaboration multi utilisateur et de la concurrence.

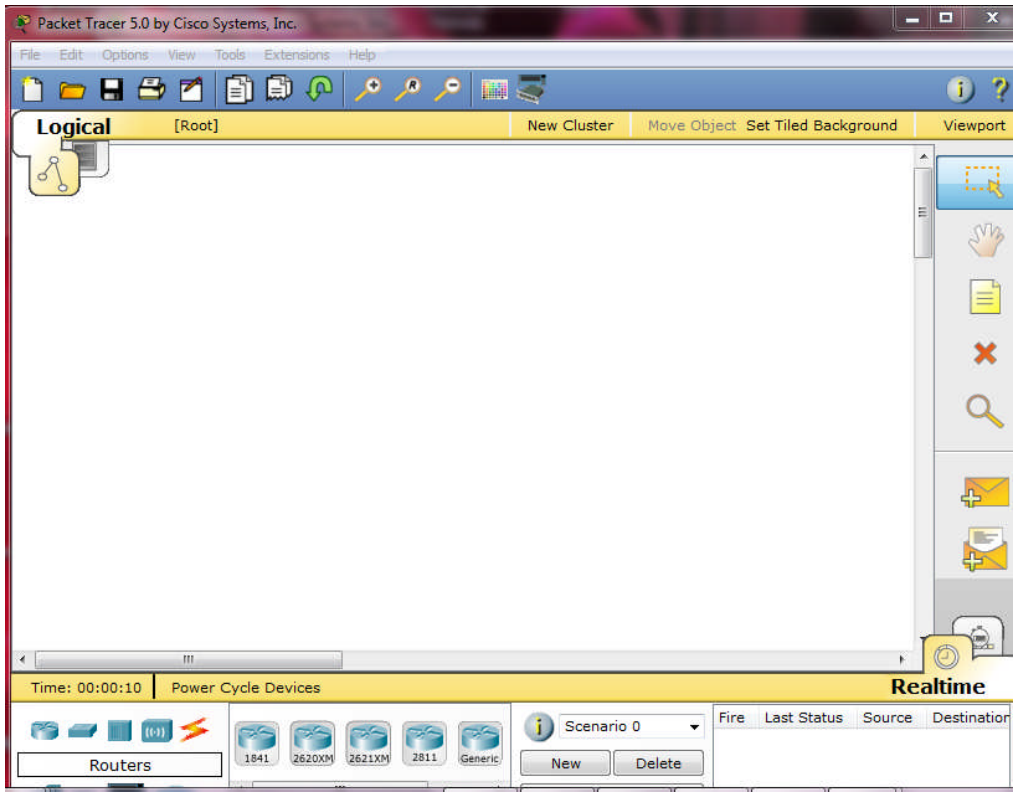
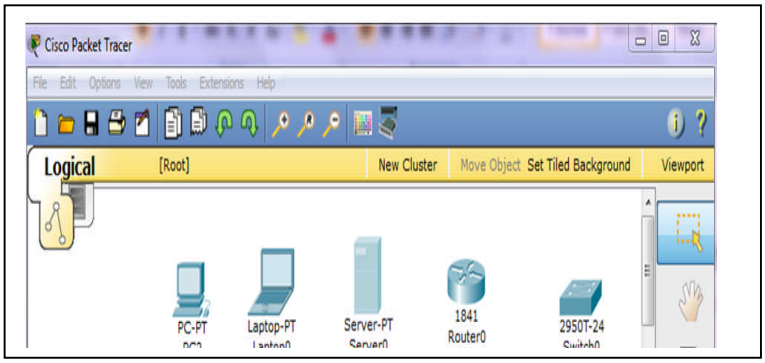


Figure IV.2 : Représentation de packet tracer version 5.0.

1.1.1-Les étapes à suivre :

- La première chose à faire est de sélectionner les périphériques besoin de la barre d'outils de packet tracer comme la montre la figure ci-dessous.
- On place les équipements choisis dans l'espace de travail on cliquant sur son icone et le faisant glisser dans l'espace de travail.



- Pour interconnecter les périphériques choisis entre eux il faut choisir les types de câblage approprié aux interfaces présentes sur notre matériel.
- Arriver à ce stade il pouvoir distinguer les routeurs les uns des autres, en attribuant l'adresse IP de chacun. Le masque de sous réseau sera ajouter par

défaut de même pour les pc et les Switch.

La figure IV.1représente un réseau qui regroupe deux stations de région différente Tizi-Ouzou et Boumerdes qui sont reliés avec un lien périodique de deux Routeurs R1 et R2.
Le réseau porte quatre types de signaux: Signal de protocole (SIP), signal de management, signal de trunk, Signal de Ressource de Médias.

Il est dans les habitudes courantes de séparer ces signaux pour cela, on a crée des VLANs dans chaque commutateur. Un VLAN est un sous-réseau logiquement séparé d'IP, ils permettent aux réseaux multiples d'IP d'exister sur le même réseau commuté.

Les commutateurs (S1, S2) contiennent les quatre VlANS configurés. Une gamme d'interfaces est assignée pour chaque VLAN, les interfaces sont configurées en mode d'accès pour les types de VlANS qui soutiennent l'écoulement de ces quatre signaux (Protocol, management, ressource média et le signal trunk).
Les VLANS sont appelés comme suivent:

VLAN 99: nommé Trunck (multimédia)
VLAN 10: nommé protocole
VLAN 20: nommé management.
VLAN 30: nommé medias (voix)

La passerelle par défaut d'IP est configurée dans chaque commutateur (S1, S2) pour rendre le commutateur capable à expédier le paquet hors du secteur local.

Les Routeurs sont les dispositifs responsables du transfert des paquets à partir d'un réseau au prochain.

Nous avons configuré les routeurs et mis en place l'interface faste Ethernet pour chacun en suite nous avons configuré les commutateurs (switch).

L'interface fastethernet0/0 de Routeur est configurée pour fonctionner comme lien de truck et est reliée à un port de commutateur configuré en mode de trunk. Le routeur exécute l'acheminement d'inter-VLAN en acceptant le trafic étiqueté par VLAN sur l'interface de truck venant du commutateur adjacent et conduisant intérieurement le Vlan.

1.1.2-Procédure de configuration du routeur R1 :

-L'interface fastethernet0/0 est permise.

-Subinterface fa0/0.99 assigné VLAN 99 a l'adresse IP 172.17.1.1, et le masque de sous réseau 255.255.255.0.

-Subinterface fa0/0.10 assigné pour VLAN10 à l'adresse IP 172.17.2.1, et le masque de sous réseau 255.255.255.0.

-Subinterface fa0/0.20 assigné pour VLAN20 à l'adresse IP 172.17.3.1 et le masque de sous réseau 255.255.255.0.

-Subinterface fa0/0.30 assigné pour VLAN10 à l'adresse IP 172.17.4.1, et le masque de sous réseau 255.255.255.0.

-L'interface Serial0/0/0 à l'adresse IP 172.17.5.2 et le masque de sous réseau 255.255.255.0.

-Un itinéraire statique à l'adresse IP 172.18.0.0 et masque de sous réseau 255.255.248.0 est ajouté à la table d'acheminement de R1

1.1.3-Procédure de configuration du routeurR2 :

-L'interface fastethernet0/0 EST permise.

-Subinterface fa0/0.99 assigné VLAN 99 à l'adresse IP 172.18.1.1, le masque de sous réseau 255.255.255.0.

-Subinterface fa0/0.10 assigné pour VLAN10 à l'adresse IP 172.18.2.1, le masque de sous réseau 255.255.255.0.

-Subinterface fa0/0.20 assigné pour VLAN20 à l'adresse IP 172.18.3.1, et le masque de sous réseau 255, 255, 255,0.

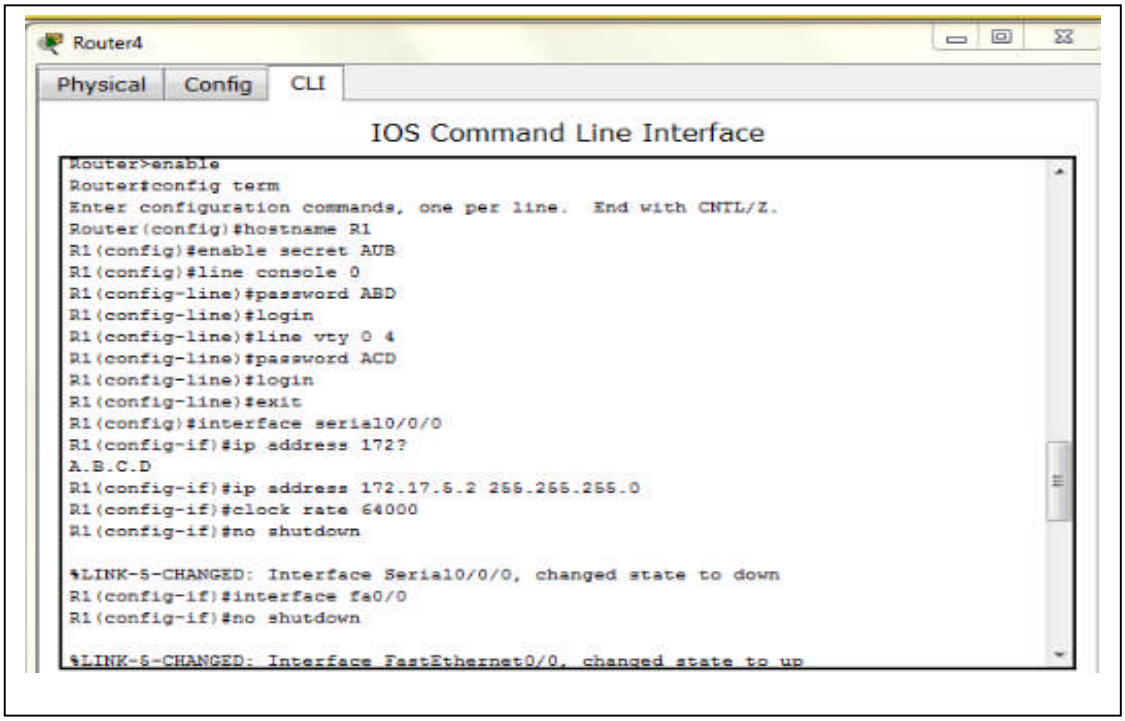
-Subinterface fa0/0.30 assigné pour VLAN10 à l'adresse IP 172.18.4.1 le masque de sous réseau 255.255.255.0.

-L'interface Serial0/0/0 à l'adresse IP 172.17.5.4, et le masque de sous réseau 255.255.255.0.

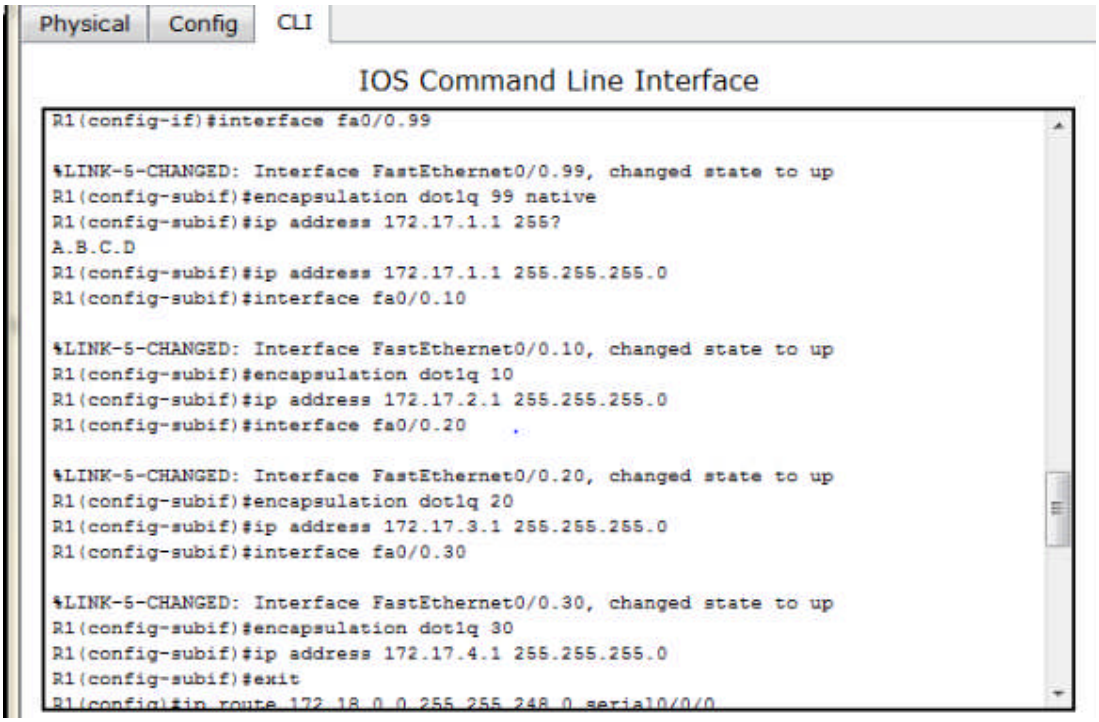
-Un itinéraire statique à l'adresse IP 172.18.0.0 et 255.255.248.0 est ajouté à la table d'acheminement de R1.

1.1.4-Résultats Obtenus De Configuration Des Routeurs et les swicth :

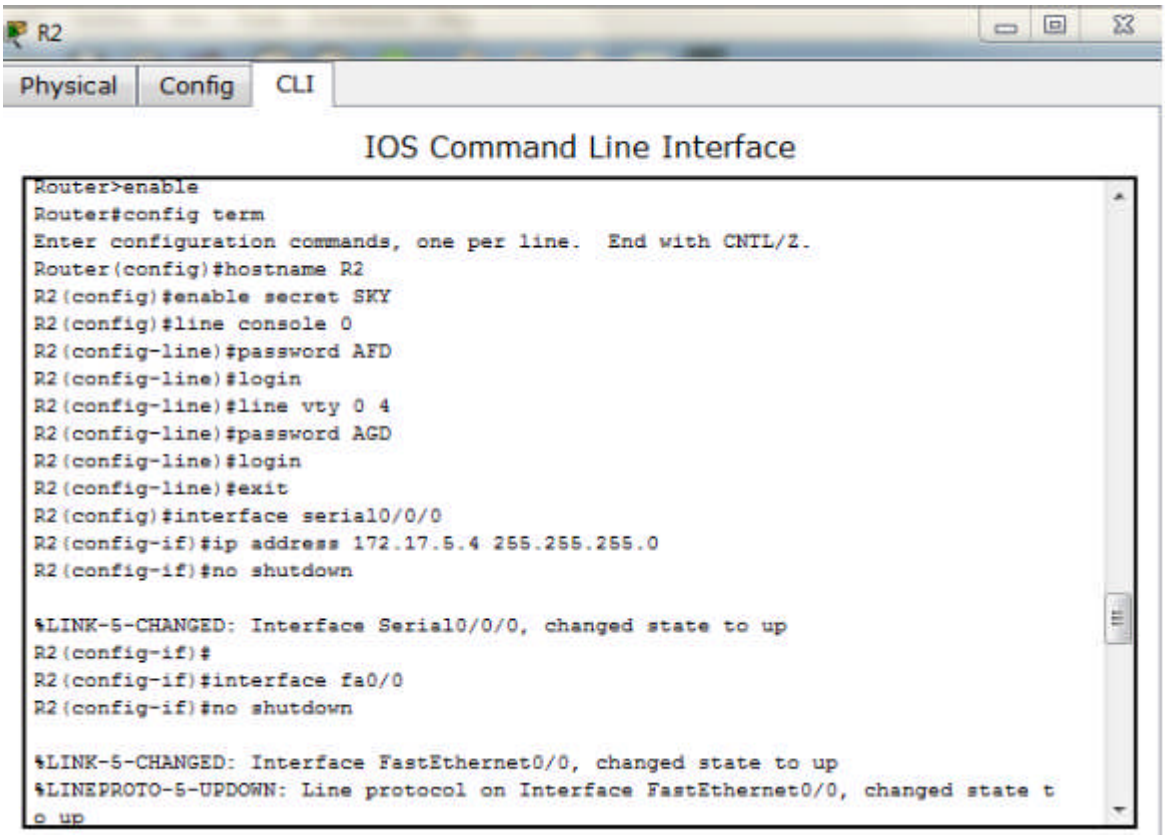
-Configuration de Routeur de Tizi-Ouzou :

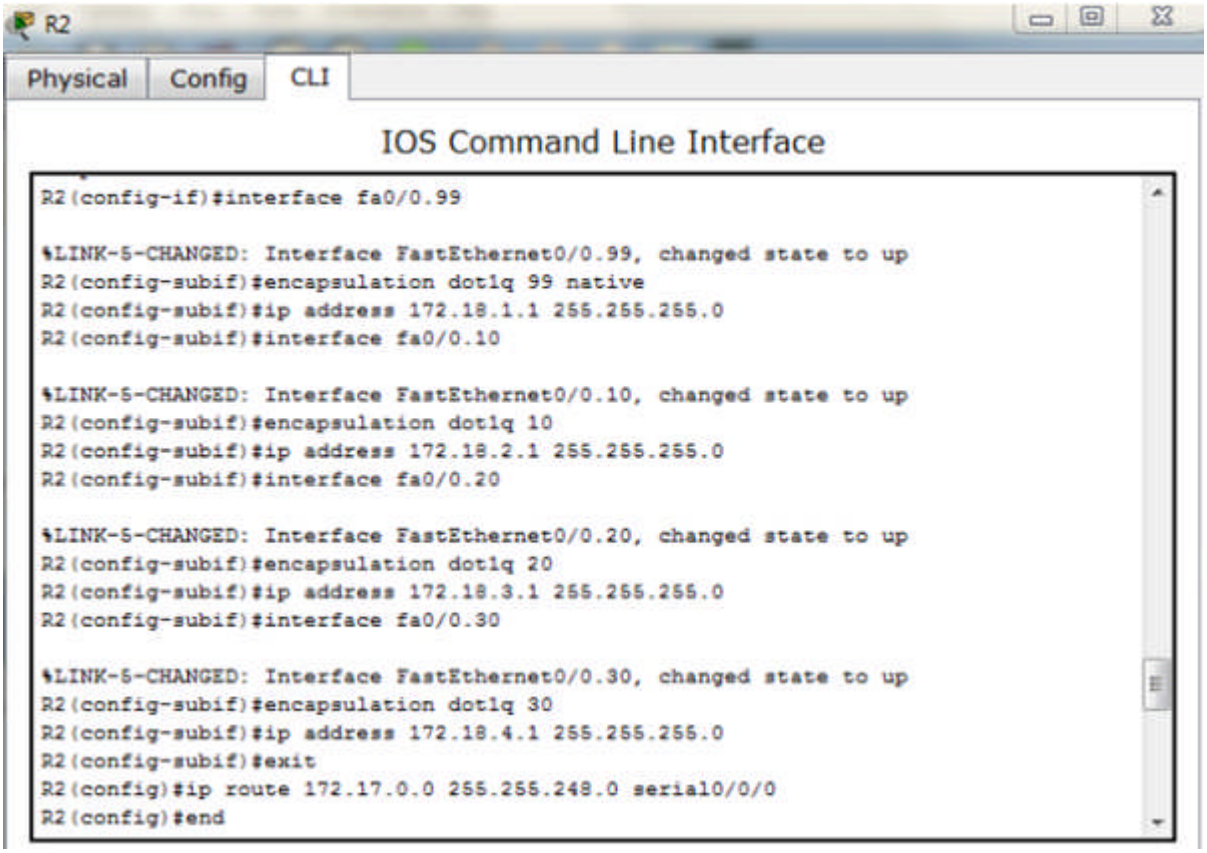


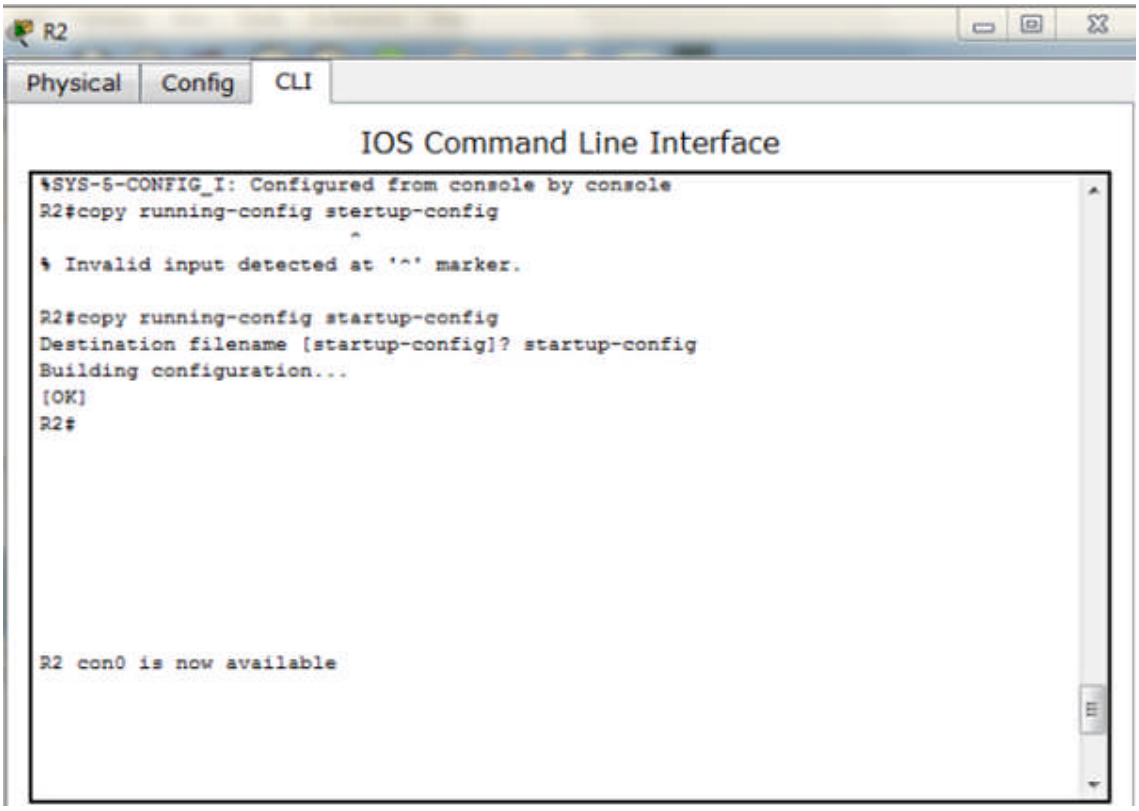
Suit



-Configuration des routeurs de Boumerdes :

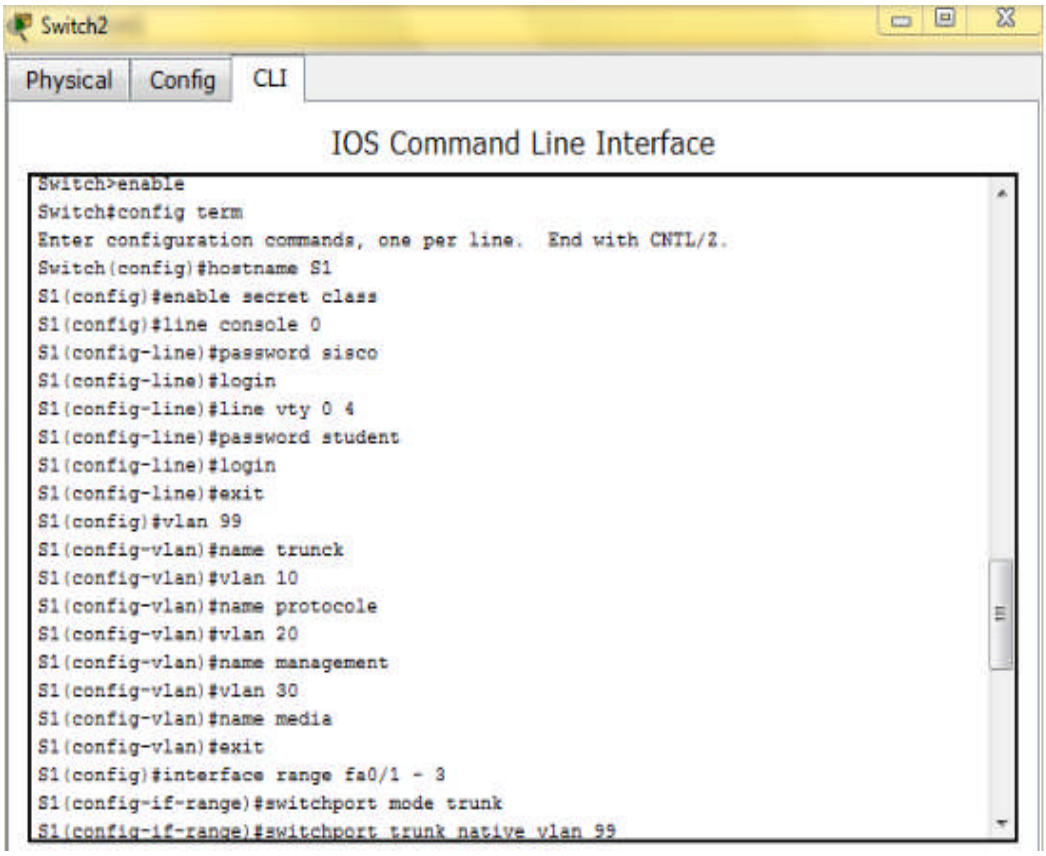


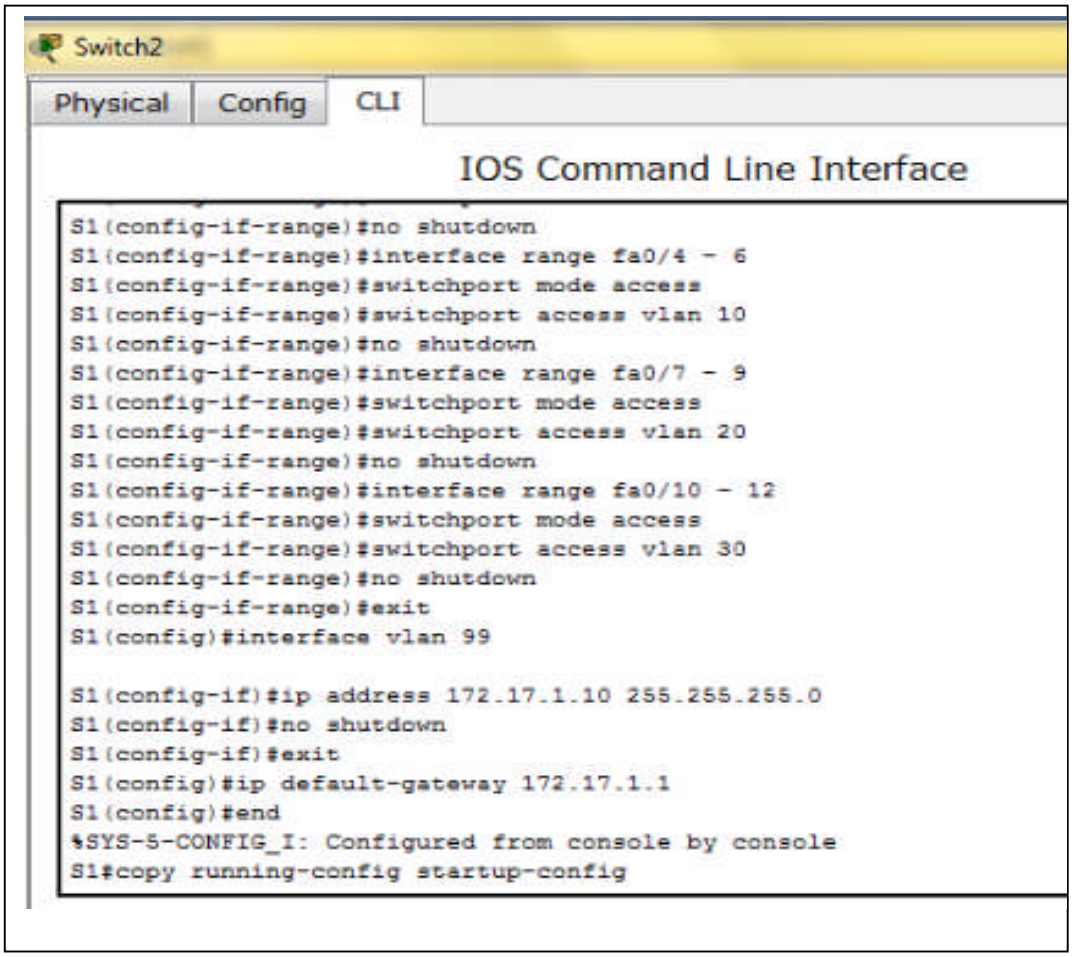




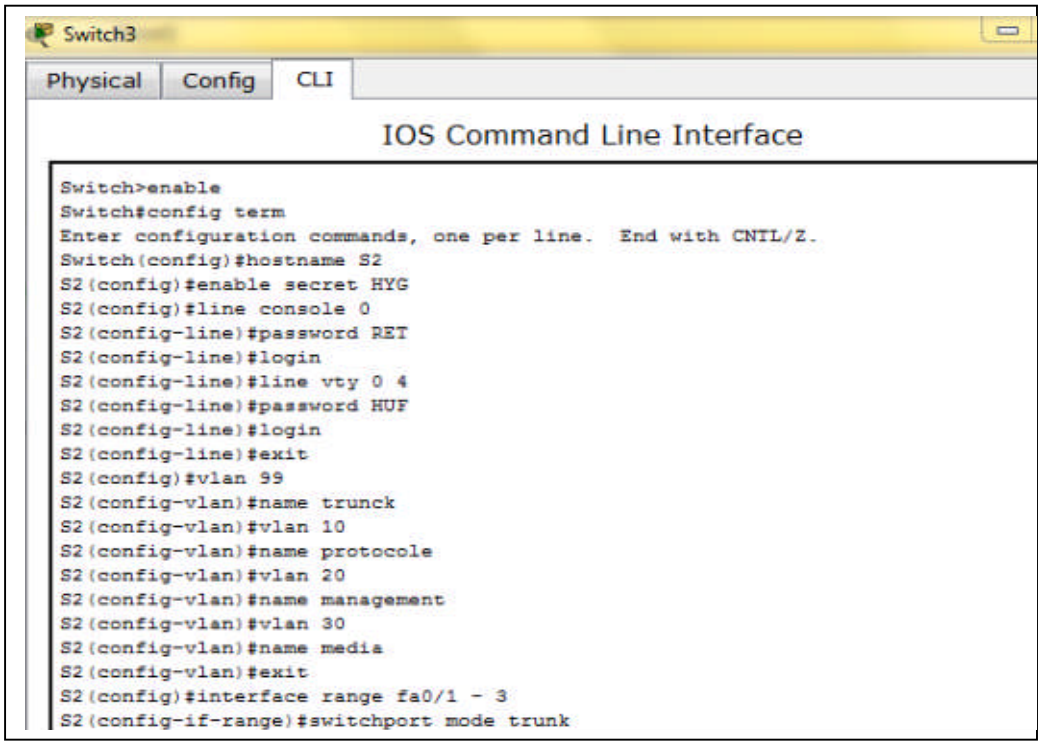
Configuration des Switch :

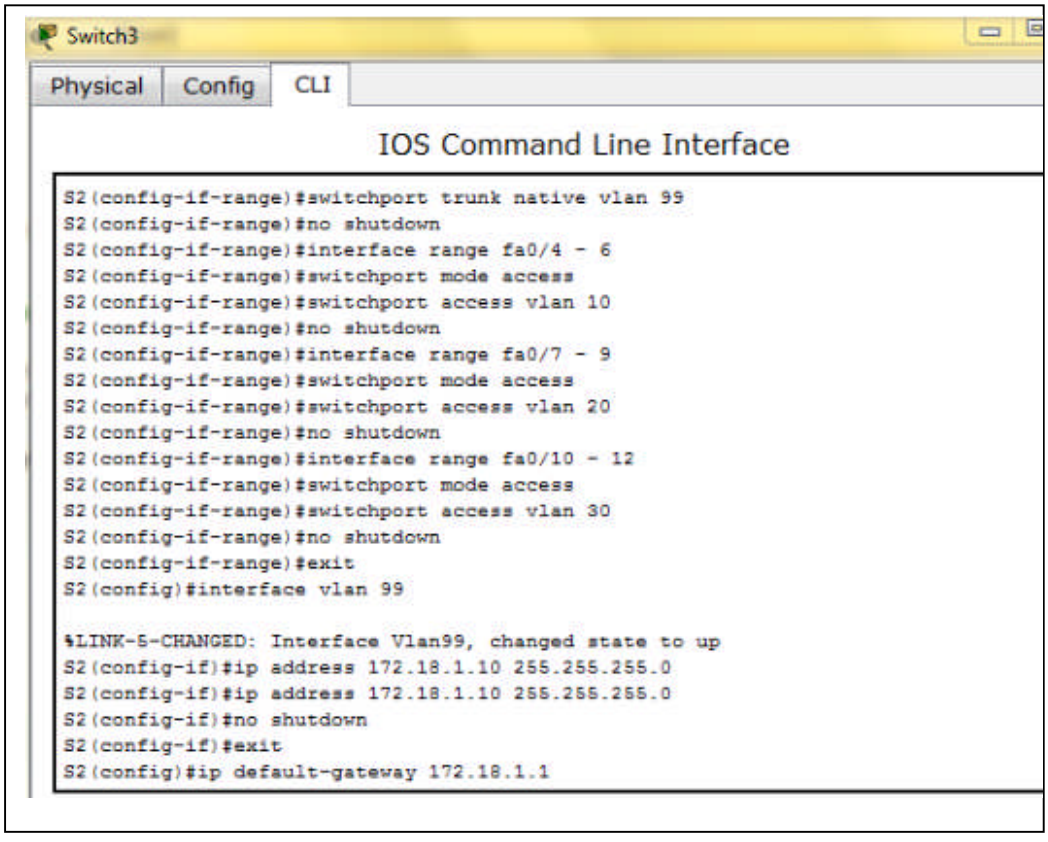
- Configuration des Switch de Tizi-Ouzou :

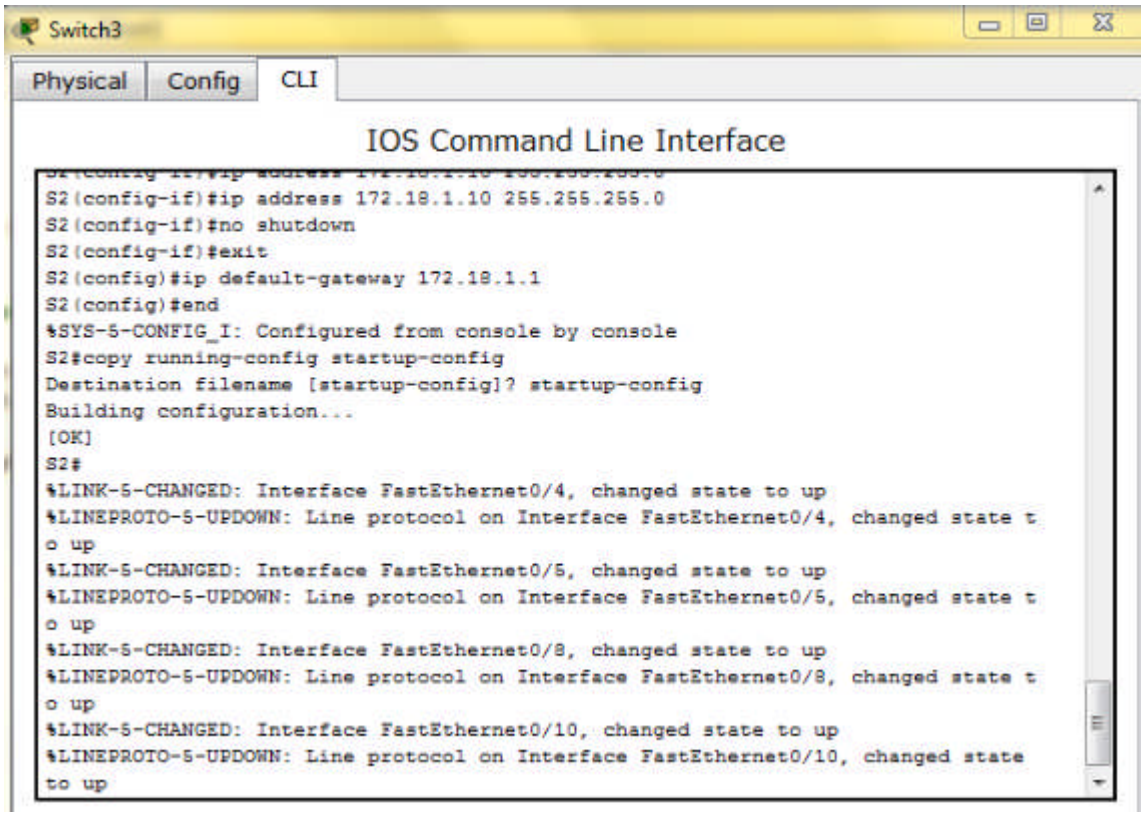

Switch2
Physical
Config
CLI
IOS Command Line Interface
Switch>enable
Switch#config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password sisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password student
S1(config-line)#login
S1(config-line)#exit
S1(config)#vlan 99
S1(config-vlan)#name trunck
S1(config-vlan)#vlan 10
S1(config-vlan)#name protocole
S1(config-vlan)#vlan 20
S1(config-vlan)#name management
S1(config-vlan)#vlan 30
S1(config-vlan)#name media
S1(config-vlan)#exit
S1(config)#interface range fa0/1 - 3
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99


Switch2
Physical
Config
CLI
IOS Command Line Interface
S1(config-if-range)#no shutdown
S1(config-if-range)#interface range fa0/4 - 6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#no shutdown
S1(config-if-range)#interface range fa0/7 - 9
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 20
S1(config-if-range)#no shutdown
S1(config-if-range)#interface range fa0/10 - 12
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 30
S1(config-if-range)#no shutdown
S1(config-if-range)#exit
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.1.10 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 172.17.1.1
S1(config)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config

-Configuration de Switch de Boumerdes :







2- L'architecture de système du traceur d'appels:

Ce système se compose d'architecture logique, et d'architecture matérielle.

2.1 Architecture logique:

Les éléments de participation sont:

1- La base de données : pour le stockage des données.

2- Le système logiciel traceur d'appel "pour détecter le type de message.

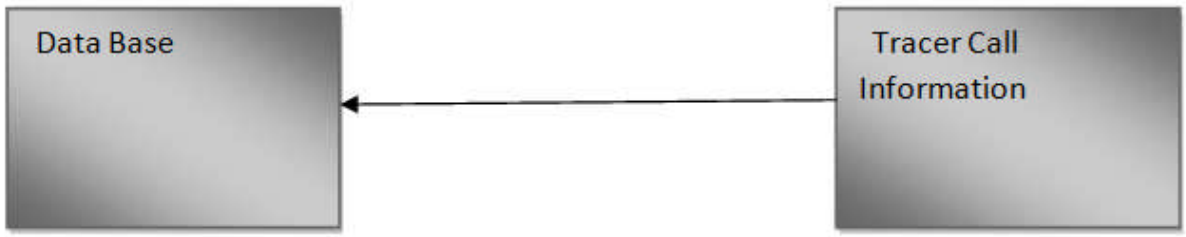


Figure IV.3 : Architecture de logiciel traceur d'appel

2.2 Architecture matériel :

Dans notre application nous avons utilisé un ordinateur équipé d'un logiciel « tracer d'appel », un softswitch qui porte tous les événements passif pendant l'application, relié à cet ordinateur. Dés qu'un appel est effectué, le softswitch envoie tous les événements au poste de travail pour que ce logiciel puisse détecter l'événement ou l'information qui a besoin, puis il affichera sur l'écran de l'ordinateur.

2.3-Partie pratique :

Différents appels ont été effectués dans des différents endroits, le Softswitch de Tizi-Ouzou envoie les événements au poste de travail, et celui-ci stocke les informations dans un dossier. Afin que le logiciel (traceur d'appel) puisse choisi l'information qu'il veut détecter puis il affichera sur l'écran. Dans notre travail nous avons basé sur le message SIP qui a été échangés entre le passage de médias Gateway de Boumerdes et le Softswitsh, et entre le softswitch et le Média Gateway de Tizi- Ouzou durant l'appel.

2.3.1-Résultats de traceur d'appel de protocole SIP:

Un appel est déroulé entre deux abonnés, abonné A est situé à Boumerdes, et l'abonné B est situé à Tizi-Ouzou.

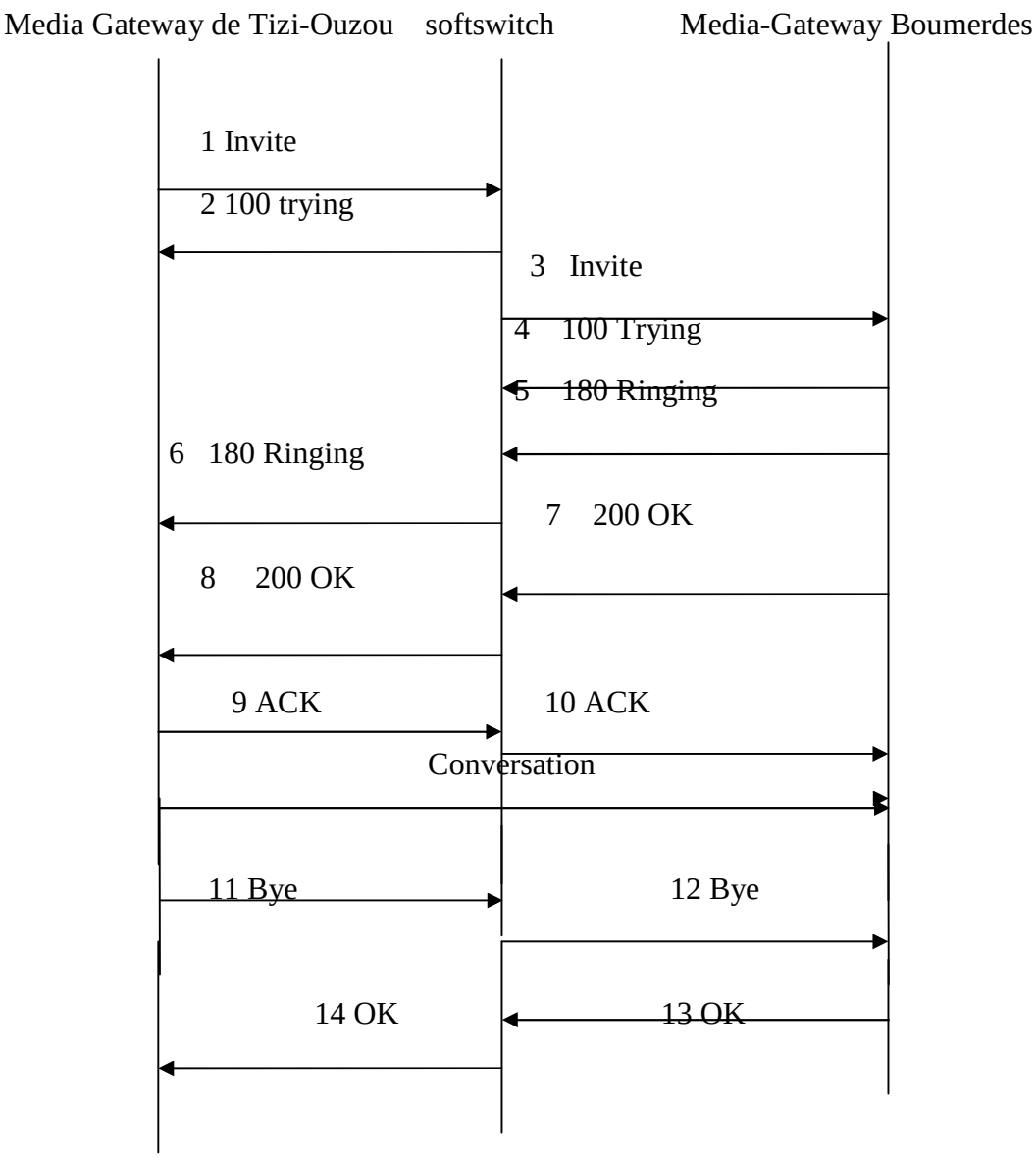
Le tableau suivant montre le type de message SIP qui à été échangés entre le média Gateway de Boumerdes et le Softswitch.

Direction	Msg Name	Module No	Local Address	Remote Address	Hex Msg
RECV	INVITE	211	172.17.1.2:500	172.18.2.8:500	49 4E 56 49 54 45 20 73 69 70 3A 30 33 36 36 30...
SEND	100	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 31 30 30 20 54 72 79 69 6E...
SEND	180	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 31 38 30 20 52 69 6E 67 69...
RECV	ACK	211	172.17.1.2:500	172.18.2.8:500	41 43 4B 20 73 69 70 3A 30 33 36 36 36 30 31 30 35...
RECV	BYE	211	172.17.1.2:500	172.18.2.8:500	42 59 45 20 73 69 70 3A 30 33 36 36 36 30 31 30 35...
SEND	200	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 32 30 30 20 4F 4B 0D 0A 5...
SEND	487	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 34 38 37 20 52 65 71 75 65...

Le 2éme tableau montre le type de message SIP qui à été échangés entre le Softswitch et le média gateway de Tizi-Ouzou.

Direction	Msg Name	Module No	Local Address	Remote Address	Hex Msg
SEND	INVITE	211	172.17.1.2:500	172.17.2.2:500	49 4E 56 49 54 45 20 73 69 70 3A 30 33 36 37 32 34...
RECV	100	211	172.17.1.2:500	172.17.2.2:500	53 49 50 2F 32 2E 30 20 31 30 30 20 54 72 79 69 6E...
RECV	180	211	172.17.1.2:500	172.17.2.2:500	53 49 50 2F 32 2E 30 20 31 38 30 20 52 69 6E 67 69...
SEND	ACK	211	172.17.1.2:500	172.17.2.2:500	41 43 4B 20 73 69 70 3A 30 33 36 37 32 34 30 30 30...
SEND	BYE	211	172.17.1.2:500	172.17.2.2:500	43 41 4E 43 45 4C 20 73 69 70 3A 30 33 36 37 32 3...
RECV	200	211	172.17.1.2:500	172.17.2.2:500	53 49 50 2F 32 2E 30 20 32 30 30 20 4F 4B 0D 0A 5...
RECV	487	211	172.17.1.2:500	172.17.2.2:500	53 49 50 2F 32 2E 30 20 34 38 37 20 52 65 71 75 65...

Le diagramme suivant représente l'écoulement des messages entre le Media-Gateway de boumerdes et le Softswitch, et entre Softswitch et Media-Gateway de Tizi-Ouzou.



1) Invite : Media-Gateway de Boumerdes envoie une demande d'INVITATION au Softswitch, pour inviter l'abonné B à une session. La description de la session du message d'invitation porte l'adresse IP de Media-Gateway (172.18.2.8) de Boumerdes, avec le nombre de port (500) à gauche

2) Trying: Softswitch renvoie une réponse 100 trying au Média Gateway de Boumerdes, informant la réception de la demande au même temps il la traite.

3) Invite: Softswitch envoie une demande d'invitation au media-Gateway de Tizi-Ouzou

pour participer à la session, ce message porte l'adresse IP du média Gateway de Boumerdes.

4) 100 Trying: Le média Gateway de Tizi - Ouzou envoie une réponse 100 trying au Softswitch, et lui informe la réception de la demande, au même temps il la traite.

5)180 Ringing (sonner) : Le Media-Gateway de Tizi-Ouzou informe au softswitch que le phone B est en train de sonner

6) 180 Ringing (sonner) : Le Softswitch envoie une réponse 180 Ringing au média Gateway de Boumerdes, lui informer que le phone B est en train de sonner.

7)200 OK : Le média Gateway de Tizi-Ouzou envoie une réponse de 200 OKS au Softswitch.

8) 200OK : Softswitch envoie une réponse de 200 OKS au média gateway de Boumerdes, annonçant qu'il a reçu la demande d'invitation.

9) ACK : Le média Gateway de Boumerdes envoie un message de ACK au Softswitch, accusé de réception de la réponse finale à la demande d'invitation.

10) ACK : le Softswitch envoie un message d'ACK au média gateway de Tizi-Ouzou, accusé de réception de la réponse finale à la demande d'invitation.

11) Bye : le phone A raccroche, le média **G**ateway de Boumerdes détecte l'événement et envoie un message au Softswitch, lui demandé de terminer la session.

12) Bye: Le Softswitch reçoit le BYE de média gateway de Boumerdes, il sait que l'abonné A est raccroché. Le Softswitch envoie un message au Média Gateway de Tizi-Ouzou demandant de terminer la session.

13) 200OK : Le phone B raccroche, le média Gateway Tizi-Ouzou envoie une réponse de 200 OKS au Softswitch, indiquant que la session est terminée.

14) 200OK : Softswitch envoie une réponse de 200 OKS au média Gateway de Boumerdes, indiquant que la session est terminée.

Conclusion:

Ce traceur d'appel représente un appel réussi puisque l'extrémité appelée reçoit l'appel et répond.

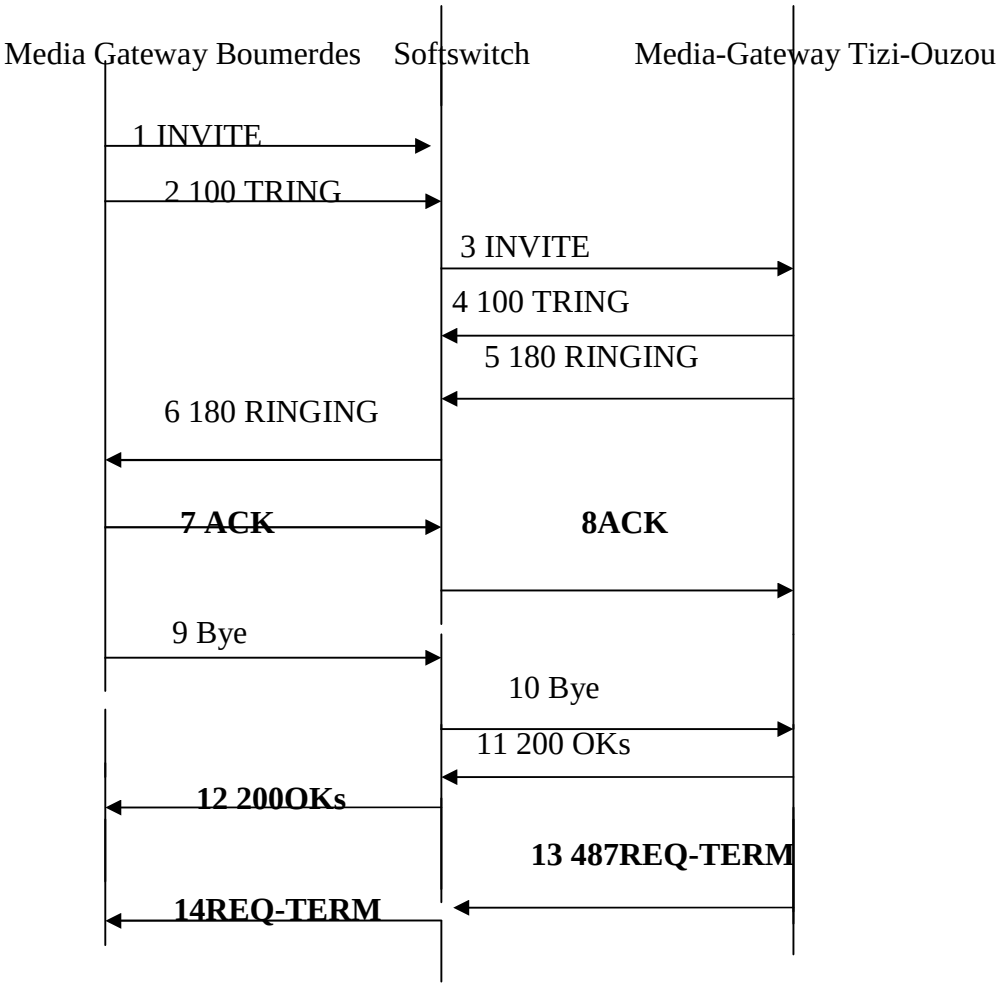
Un autre appel est déroulé, le tableau suivant d'écrit le type de message qui à été échangé entre Media-Gateway de Boumerdes et Softswitch.

Direction	Msg Name	Module No	Local Address	Remote Address	Hex Msg
RECV	INVITE	211	172.17.1.2:500	172.18.2.8:500	49 4E 56 49 54 45 20 73 69 70 3A 30 33 36 36 36 30...
SEND	100	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 31 30 30 20 54 72 79 69 6E...
SEND	180	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 31 38 30 20 52 69 6E 67 69...
RECV	ACK	211	172.17.1.2:500	172.18.2.8:500	41 43 4B 20 73 69 70 3A 30 33 36 36 36 30 31 30 35...
RECV	BYE	211	172.17.1.2:500	172.18.2.8:500	42 59 45 20 73 69 70 3A 30 33 36 36 36 30 31 30 35...
SEND	200	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 32 30 30 20 4F 4B 0D 0A 5...
SEND	487	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 34 38 37 20 52 65 71 75 65...

-Le tableau suivant d'écrit le type de message SIP qui à été échangé entre le Softswitch et le media Gateway de Tizi-Ouzou.

Direction	Msg Name	Module No	Local Address	Remote Address	Hex Msg
SEND	INVITE	211	172.17.1.2:500	172.17.2.2:500	49 4E 56 49 54 45 20 73 69 70 3A 30 33 36 37 32 34...
RECV	100	211	172.17.1.2:500	172.17.2.2:500	53 49 50 2F 32 2E 30 20 31 30 30 20 54 72 79 69 6E...
RECV	180	211	172.17.1.2:500	172.17.2.2:500	53 49 50 2F 32 2E 30 20 31 38 30 20 52 69 6E 67 69...
SEND	ACK	211	172.17.1.2:500	172.17.2.2:500	41 43 4B 20 73 69 70 3A 30 33 36 37 32 34 30 30 30...
SEND	BYE	211	172.17.1.2:500	172.17.2.2:500	43 41 4E 43 45 4C 20 73 69 70 3A 30 33 36 37 32 3...
RECV	200	211	172.17.1.2:500	172.17.2.2:500	53 49 50 2F 32 2E 30 20 32 30 30 20 4F 4B 0D 0A 5...
RECV	487	211	172.17.1.2:500	172.17.2.2:500	53 49 50 2F 32 2E 30 20 34 38 37 20 52 65 71 75 65...

Ainsi le diagramme suivant représente l'écoulement des messages entre le Media gateway de Boumerdes et le Softswitch, et entre Softswitch et Media-Gateway de Tizi-Ouzou.



L'événement1 : Media-Gateway de Boumerdes envoie une demande d'invitation au Softswitch, pour inviter le phone B à une session. La description de session du message d'invitation porte l'adresse IP de Media-Gateway (172.18.2.8) de Boumerdes, le numéro port (500).

Événement 2: le Softswitch envoie une réponse 100 tying au Media-Gateway de Boumerdes, informant la réception de la demande et également ce Softswitch traite la demande.

L'événement 3 : le Softswitch envoie une demande d'invitation au media-Gateway de Tizi-ouzou pour participer à la session, et porte l'adresse IP du media Gateway de Boumerdes et le numéro du port 500.

Événement 4 : Media Gateway de Tizi-Ouzou renvoie 100 tying au Softswitch lui informe la réception de la demande.

Événement 5 : Media-Gateway de Tizi-Ouzou reçoit la tonalité sonnante et renvoie une réponse 180 sonnante au Softswitch.

Événement 6 : le Softswitch envoie une réponse 180 sonnante au Media-Gateway de Boumerdes lui informant que le phone B est entrain de sonner.

Événement 7: Media-Gateway de Boumerdes envoie un message de ACK au softswitch, informe la réception de la réponse finale à la demande d'invitation de Media-Gateway de Tizi-Ouzou.

Événement 8: Le Softswitch envoie un message d'ACK au Media-Gateway de Tizi-Ouzou, accusé de réception de la réponse finale à la demande d'invitation du Media-Gateway de Boumerdes.

Événement 9 : Le phone A raccroche, le Media-Gateway de Boumerdes détecte l'événement, envoie alors un message Bye au Softswitch demandant de terminer la session.

Événement 10 : Le Softswitch reçoit le BYE, sachant que le phone A est raccroché, alors il envoie une demande secondaire au Media-Gateway de Tizi-Ouzou demandant de terminer la session.

Événement 11 : Media-Gateway de Tizi-Ouzou' envoie une réponse de 200 OKS au Softswitch, indiquant que la session est terminée.

Événement12 : Le Softswitch envoie une réponse de 200 OKS au Media-Gayeway de Boumerdes, indiquant que la session est terminée.

L'événement13: Le Media-Gateway de Tizi-Ouzou envoie une réponse 487 au softswitch, indiquant la terminaison de la session.

Événement 14 : Le Softswitch envoie une réponse 487 au Media-Gateway de Boumerdes,

indiquant la terminaison de la session

Conclusion

Le Softswich reçoit la forme sonnante de la réponse 180 le Media-Gateway de Tizi-Ouzou, mais il n'a pas reçu la réponse de 200 OKS de la demande d'invitation, qui signifie que l'extrémité d'appeler reçoit l'appel, mais ne répond pas.

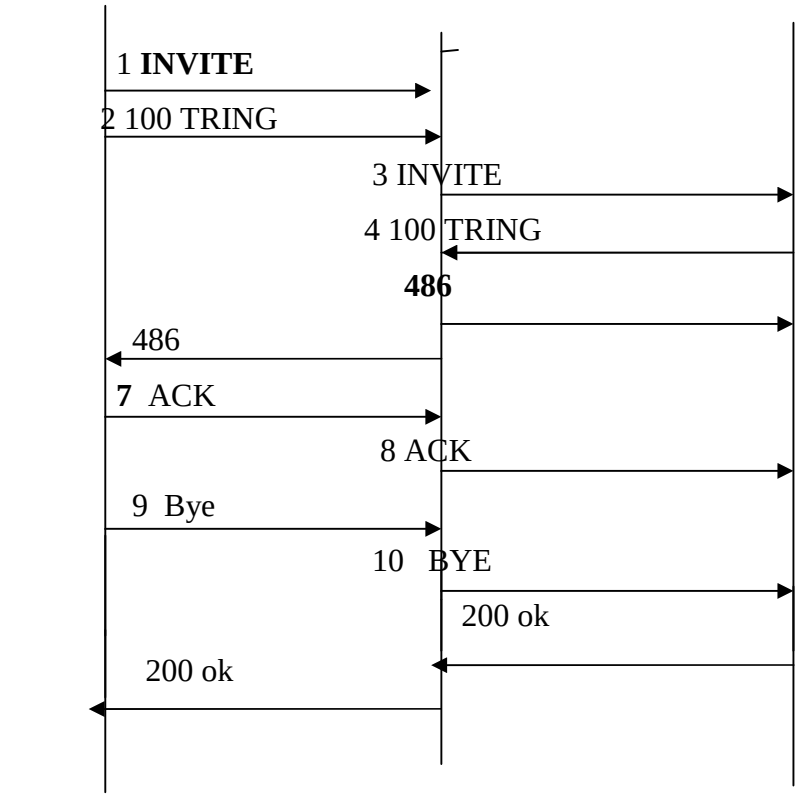
Un autre appel est déroulé et le tableau suivant d'écrit le type de message SIP qui à été échange entre le Media-Gateway de Boumerdes et le Softswitch.

Direction	Msg Name	Module No	Local Address	Remote Address	Hex Msg
SEND	INVITE	211	172.17.2.1:500	172.18.2.8:500	49 4E 56 49 54 45 20 73 69 70 3A 30 33 36 37 32 34...
RECV	100	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 31 30 30 20 54 72 79 69 6E...
RECV	486	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 34 38 36 20 42 75 73 79 20...
SEND	ACK	211	172.17.1.2:500	172.18.2.8:500	41 43 4B 20 73 69 70 3A 30 33 36 37 32 34 30 30 30...
RECV	BYE	211	172.17.1.2:500	172.18.2.8:500	42 59 45 20 73 69 70 3A 30 33 36 36 36 30 31 30 35...
SEND	200	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 32 30 30 20 4F 4B 0D 0A 5...

Le tableau suivant d'écrit le type de message SIP qui à été échange entre le Softswitch et le media Gateway de Tizi-Ouzou.

Direction	Msg Name	Module No	Local Address	Remote Address	Hex Msg
RECV	INVITE	211	172.17.1.2:500	172.18.2.8:500	49 4E 56 49 54 45 20 73 69 70 3A 30 33 36 36 36 30..
SEND	100	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 31 30 30 20 54 72 79 69 6E..
SEND	486	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 34 38 36 20 42 75 73 79 20..
RECV	ACK	211	172.17.1.2:500	172.18.2.8:500	41 43 4B 20 73 69 70 3A 30 33 36 36 36 30 31 30 35..
RECV	BYE	211	172.17.1.2:500	172.18.2.8:500	42 59 45 20 73 69 70 3A 30 33 36 36 36 30 31 30 35..
SEND	200	211	172.17.1.2:500	172.18.2.8:500	53 49 50 2F 32 2E 30 20 32 30 30 20 4F 4B 0D 0A 5...

Ainsi le diagramme suivant représente l'écoulement des messages entre le Media gateway de Boumerdes et le Softswitch, et entre Softswitch et le Media-Gateway de Tizi-Ouzou.



1) Invite : Media-Gateway de Boumerdes envoie une demande d'invitation au Softswitch, pour inviter le téléphone B à une session. La description de la session du message d'invitation porte l'adresse IP de Media-Gateway (172. 18.2.8) de Boumerdes, avec le nombre de port (500) à gauche

2) Trying: Le Softswitch renvoie une réponse 100 trying au Média Gateway de Boumerdes, informant la réception de la demande au même temps il la traite.

3) Invite: Le Softswitch envoie une demande d'invitation au media-Gateway de Tizi-ouzou pour participer à la session.

4) 100 Trying: Le média Gateway de Tizi-Ouzou envoie une réponse100 tying au softswitch, lui informe qui a la reçu la demande

***5)* 486 BUSY HERE** : Le media Gateway de Tizi -ouzou envoie une repense au softswitch lui informe que l'appelé a été contacté, mais il est occupé et ne peut prendre la communication.

6) ACK : Le média Gateway de Boumerdes envoie un message de ACK au Softswitch, accusé de réception de la réponse finale à la demande d'invitation

7) ACK : Le Softswitch envoie un message d'ACK au média Gateway de Tizi-Ouzou, accusé de réception de la réponse finale à la demande d'invitation.

8) Bye : Le phone A raccroche, le média **G**ateway de Boumerdes détecte l'événement et envoie un message au Softswitch, demandant de terminer la session.

9) Bye: Le Softswitch reçoit le BYE de média gateway de Boumerdes sachant que le phone A est raccroché, il envoie un message au Média Gateway de Tizi-Ouzou demandant de terminer la session.

10) 200OK : Le phone B raccroche, le média Gateway Tizi-Ouzou envoie une réponse de 200 OKS au Softswitch, indiquant que la session est terminée.

11) 200OK : Le Softswitch envoie une réponse de 200 OKS au média gateway de Boumerdes, indiquant que la session est terminée.

Conclusion :

Le phone B à été contacté, le softtswitch reçoit la repense 486 (BUSY HERE) pour lui informe que le phone B est en dérangement, il ne peut pas rependre à la communication.

La voix et la vidéo sur IP prennent des dimensions de plus en plus importantes depuis quelques années. D'autre part, la téléphonie entre PCs via l'Internet commence à prendre une part importante dans le monde des télécommunications. Dans un avenir proche, l'utilisation coûteuse du réseau de téléphonie fixe ne sera plus nécessaire, surtout avec la possibilité de transférer la voix, la vidéo et les données sur le même support via l'internet. D'où la nécessité d'évoluer vers des solutions IP ce qui provoque l'émergence de nouveaux standards.

Pour certains, actuellement le seul frein à l'essor de la téléphonie sur IP serai la qualité.

Or, comme celle-ci s'améliore de plus en plus grâce à l'augmentation conjointe de la bande passante d'Internet, de la vitesse de commutation, de la performance des CPU et enfin des algorithmes de compression, la téléphonie sur IP ne peut que se développer.

A l'heure actuelle, SIP se présente comme le protocole de signalisation le plus adéquat aux applications de voix et vidéo sur IP. Sa simplicité relative par rapport au standard H323, le rend de plus en plus populaire dans ce domaine. En effet, des études comparatives de ces deux protocoles, ont fait ressortir les forces de chacun des deux standards et ont montré que SIP se présente comme concurrent principal du standard H323 dans ce domaine de la voix et de la vidéo sur IP.

Dans le contexte de notre travail, nous avons introduit les concepts de la téléphonie sur IP et nous avons défini les protocoles et concepts de mise en œuvre et de signalisation.

Nous avons opté pour le protocole SIP. Notre application est une application client-serveur. Le serveur est un proxy, il traite toute les requêtes provenant des clients et les achemine selon le contexte. Il inclut aussi le registra, qui est un serveur qui s'occupe de l'enregistrement des clients et fournit à chaque fois au proxy le non, l'adresse IP et le numéro de port du destinataire. Notre cas d'application est un cas simple d'utilisation du protocole SIP vu que la présence des autres serveurs de localisation et de redirection n'est pas nécessaire. On n'espère que ce modeste travail puisse servir à des travaux futurs pour élargir le domaine d'application.

Bibliographie

1- B. HERNANDEZ, « La téléphonie sur IP », Centre d'Expertise des Grands Organismes, Février 2007.

2- Bill Douskalis (1999). *IP Telephony : The integration of robust VoIP Services.* Prentice Hall.

3- J. Delacroix, « Comment trouver sa voix sur IP ? », Publication coordonnée par la Direction de la Communication de Completel et l'EBG, Janvier 2006.

4- J. L. Mélin, « Qualité de service sur IP », édition Eyrolle, 2000.

5- K. Bakhti (2000). La voix sur Internet dans le contexte du Standard H.323, Thèse de maîtrise, UQAM.

6- K. JABRI, Rapport de projet de finn d'études : "Evaluation de performances du protocole SIP dans un contexte voix sur IP", ENIT. Juin 2007.

7- Télécoms 1 de la transmission à l'architecture des réseaux par Claude Servin (2ème édition 2001).

L'ouvrage :

1- (S.I.R) Présenté par Bassirou KASSE en décembre2006.

2- Etude et mise en place d un système de communication de VOIP : APPLIQUE A UN PABX IP OPEN SOURCE

3- G. Pujolle (1998). Les réseaux, 2ème édition, Eyrolles.

4- Master II professionnel Système d'Information Reparties.

5- Projet de Fin d'étude Ben Ammar Rajaa- 2006 G1.

GLOSSAIRE

« A »

ALG: Application Layer Gateway

ATM: Asynchronous Transfer Protocol

ARP: Address Resolution Protocol

ASCII : American Standard Code for Information Interchange Alphabet define

« D »

DNS: Domain Name System

DHCP: Dynamic Host Configuration Protocol

« E »

ENUM: TElephone NUmber Mapping

« F »

FTP: File Transfert Protocol.

« G »

GK: Gatekeeper.

« H »

HTTP: Hypertext Transfer Protocol.

« I »

IP: Internet Protocol.

IPX: Internetwork Packet Exchange.

ITU: International Telecommunication Union.

IETF: Internet Engineering Take Force.

IFS: Inter Frame Space.

ISDN : Union International de télécommunication

ICMP : Internet Control Message Protocol

IGMP: Internet group Message Protocol

GLOSSAIRE

IPv6: IP version 6

« L »

LAN: Local Area Network.

« M »

MAC: Media Access Control.

MAN: Metropolitan Area Network.

MOS: Mean Operational Score.

MCU: Multipoint Control Unit.

MMUSIC: Multiparty Multimedia Session Control.

MGC: Media Gateway Controller.

MGCP: Media Gateway Control Protocol.

« N »

NAT: Network Address Translation

NGN: Next Generation Network

« O »

OSI: Open Interconnection System.

« P »

PABX IP: Private Automatic Branch Exchange IP.

PCM: Pulse Code Modulation.

PSTN: Public Switched Telephone Network.

PPP: Point to Point Protocol.

PABX: Private Automatic Branch eXchange.

PBX: Private branch exchange.

« Q »

QoS: Quality of Service.

« R »

RFC: Request for Comment

GLOSSAIRE

RTC: Réseau Téléphonique Commuté

RTCP: Real-Time Control Protocol

RTP: Real-Time transport Protocol

RTP: Real Time Transport Protocol.

RTPC : Réseau Téléphonique Public Commuté.

RAS : Protocole de signalisation (Registration Admission and Status).

RNIS : Réseau Numérique avec Intégration de Service.

RSVP : Resource Réservation Protocol.

RG: Registrar

RS: Redirect Server

RARP: Reverse Address Resolution Protocol

RIP2: Routing Information Protocol v2

« S »

SIP: Session Initiation Protocol.

SS7: Signalling System 7.

SMTP: Simple Mail Transfer Protocol.

SG: Signalling Gateway.

SIGTRAN: Signalling Transport, Informational: RFC 2719.

SCTP: Stream Control Transmission Protocol.

SLIP: (serial Line Internet Protocol)

Protocole standard permettant de véhiculer des paquets IP sur une liaison série via un modem.

« T »

ToIP: Telephony over Internet Protocol

TURN: Traversal Using Relay NAT Telecommunications

TCP: Transmission Control Protocol.

TDM: Time Division Multiplexing.

GLOSSAIRE

« U »

UDP: User Datagramme Protocol.

URI: Uniform Resource Identi_er.

URL: Uniform Resource Locator.

UA: User Agent.

UAS: User Agent Server.

UE: User Equipement

« V »

VoIP: Voice Over IP.

« W »

WAN: Wide Area Network.

Wi-Fi : Wireless Fidelity.

WLAN: Réseau Local sans _l (Wireless Local Area Network).

WSDL: Web Services Description Language.