

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE  
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

Présenté en vue de l'obtention  
du diplôme de Master en Électronique

*Option : Réseaux et Télécommunications*

*Thème:*

**Mise en place d'une solution VoIP à base de  
serveur Asterisk**

**Proposé et dirigé par:**

Mr: LAHDIR. M

**Étudié et réalisé par:**

Mr : GADOUM Karim

Mr : AZOUAOUI Sofiane

Année universitaire **2011/2012**

## **Remerciements**

*Louange à notre Seigneur "ALLAH" qui nous a doté de la merveilleuse faculté de raisonnement. Louange à notre Créateur qui nous a incité à acquérir le savoir. C'est à lui que nous adressons toute notre gratitude en premier lieu.*

*A travers ce modeste travail, Nous tenons à remercier nos parents, notre encadreur pour ses conseils, son orientation et son aide le long de notre projet de fin d'étude.*

*Nos remerciements s'adressent aussi aux messieurs le président et les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.*

*Nous exprimons également notre gratitude à tous les professeurs et enseignants qui nous aide à réaliser ce travail, sans omettre bien-sûr de remercier profondément tous ceux qui ont contribué de près ou de loin à la réalisation de ce présent travail.*

*Et enfin, que nos chers parents et familles, et bien avant tout, trouvent ici l'expression de nos remerciement les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation dans les meilleurs conditions.*

## *Résumé*

---

*Ce travail a pour objectif la présentation générale de la VoIP, comme une solution alternative intéressante pour l'utilisation personnelle et professionnelle.*

*Les trois premiers chapitres constituent la partie étude théorique, elle représente des généralités sur les réseaux informatiques. Par la suite, le modèle TCP/IP comme support de base de La VoIP. Plus loin dans cette partie, l'étude des divers Protocoles et mécanismes qui font fonctionner une infrastructure VoIP, dans des réseaux LAN et sur des réseaux étendus.*

*Comme partie pratique, une mise en place d'une solution VoIP basée sur des outils open source, précisément le serveur Asterisk et le protocole SIP.*

*Nous finirons ce mémoire par une conclusion général qui résume les points essentiels de ce travail et présente les perspectives de recherches suggérées.*

---

# SOMMAIRE

Introduction.....	1
CHAPITRE - I	
1 Préambule.....	3
2. Notion de réseau .....	3
2.1. Qu'est ce qu'un réseau ?.....	3
2.2. L'intérêt des réseaux .....	4
2.3. Les différents types des réseaux .....	4
2.3.1. La classification géographique.....	5
2.3.2. La classification fonctionnelle .....	6
2.3.3. Les réseaux homogènes et les réseaux hétérogènes .....	6
2.3.4. Les différentes catégories des réseaux .....	6
2.4. Les topologies des réseaux .....	7
2.4.1. La Topologie physique .....	7
2.4.2. La topologie logique .....	9
3. Le modèle de référence OSI .....	11
3.1. Définition .....	11
3.2. Les différentes couches .....	11
3.3. La transmission de données au travers du modèle OSI.....	12
4. La transmission dans les réseaux .....	13
4.1. Les techniques de transmission .....	13
4.1.1. La transmission en Bande de base .....	13
4.1.2. La transmission par transposition de base.....	13
4.2. Le sens de transmission.....	14
4.3. Les types de transmission.....	15
4.3.1. La transmission parallèle.....	15
4.3.2. La transmission série .....	15
4.4. Les techniques de Communication .....	16
4.4.1. La commutation de circuits .....	16
4.4.2. La commutation de messages .....	16
4.4.3. La commutation de paquets .....	16
4.4.4. La commutation de cellules.....	16
4.5. Les modes de communication .....	17
4.5.1. Mode avec/sans connexion .....	17
4.5.2. Le mode d'envoi des informations .....	17
5. Les supports de transmission .....	17
5.1. Les caractéristiques des supports de transmission .....	17
5.2. Les types de supports de transmission .....	18
5.2.1. Les paires torsadées .....	18
5.2.2. Le câble coaxial .....	18
5.2.3. La fibres optiques .....	19

5.2.4. Les canaux hertziens .....	19
5.2.5. La liaisons satellite .....	20
6. Les équipements réseau .....	20
6.1. Les concentrateurs (Hubs) .....	20
6.2. Les commutateurs (Switch) .....	20
6.3. Les répéteur (Repeater) .....	20
6.4. Les ponts (Bridge) .....	20
6.5. Les passerelles (Gateway) .....	20
6.6. LES Routeur.....	21
7. Discussion .....	21

## CHAPITRE – II

1. Préambule.....	22
2. Le modèle TCP/IP.....	22
2.1. Les différentes couches.....	22
2.1.1. Couche application.....	22
2.1.2. Couche transport .....	23
2.1.3. Couche Internet .....	23
2.1.4. Couche physique.....	23
2.2. Concept des réseaux IP.....	23
2.3. Les protocoles de chaque couche .....	23
2.3.1. Les protocoles de la couche application .....	24
2.3.2. Les protocoles de la couche transport .....	25
2.3.3. Les protocoles de la couche Internet.....	26
3. L'adressage dans les réseaux IP.....	27
3.1. Structure de l'adresse IP.....	27
3.2. L'espace d'adressage.....	28
3.3. Sous réseaux .....	29
3.4. Le masque sous réseau .....	29
3.5. L'adresse de diffusion (broadcast).....	30
3.6. Les classes d'adresses.....	30
4. Le routage.....	32
4.1. Type de routage.....	32
4.1.1. Le routage direct.....	32
4.1.2. Routage Indirect .....	33
4.2. Les protocoles de routage.....	34
6. Le Network Address Translation .....	35
7. Le DNS .....	36
8. Le DHCP .....	36
9. Discussion .....	37

## CHAPITRE –III

1. Préambule .....	38
2. Téléphonie conventionnelle et Téléphonie IP.....	38
3. Les différentes architectures d'un réseau VoIP.....	38
3.1. Ordinateur à Ordinateur (PC to PC).....	38
3.2. Ordinateur à Téléphone (Pc to Phone).....	40
3.3. Téléphone à Téléphone (Phone to Phone).....	40
4. Les différents éléments pouvant composés un réseau VoIP .....	40
4.1. Le PABX-IP .....	40
4.2. Le serveur de communications : .....	40
4.3. La passerelle (Gateway).....	41
4.4. Le routeur .....	41
4.5. Le switch .....	41
4.6. Le Gatekeeper .....	41
4.7. Le MCU .....	41
4.8. L'IP-Phone .....	41
5. Fonctionnement de la téléphonie sur IP.....	42
5.1. Concept .....	42
5.2. Principe de la transmission .....	43
5.2.1. Codage de la voix .....	43
5.2.2. Les modes de diffusion dans la VoIP :.....	44
6. Standards de la VoIP .....	45
6.1. Protocole H323 :.....	45
6.1.1. Fonctionnement.....	45
6.1.2. Eléments de réseaux H.323.....	45
6.1.3. La signalisation .....	46
6.1.3.1. Objectifs de la signalisation .....	46
6.1.3.2. Les protocoles de signalisation dans le cadre de H.323...46	
6.1.4. Déroulement d'une communication H.323.....	47
6.1.5. Empilement de H.323 .....	48
6.1.6. Avantages et inconvénients .....	48
6.1.7. Conclusion sur H.323.....	49
6.2. Le protocole SIP .....	49
6.2.1. Définition de SIP .....	49
6.2.3. Principe.....	49
6.2.4. Eléments d'une architecture SIP .....	49
6.2.5. Les messages SIP .....	51
6.2.5.1. L'entête .....	51
6.2.5.2. Les méthodes .....	52
6.2.6. Le fonctionnement .....	53
6.2.6.1. Enregistrement d'un UA .....	53

6.2.6.2. Etablissement d'une connexion :	53
6.2.6.3. Modes de communication	54
6.2.7. Conclusion sur SIP	54
6.3. Les protocoles de transport:	55
6.3.1. Le protocole TCP	55
6.3.2. Le protocole UDP	55
6.3.3. Le protocole RTP	55
6.3.4. Le protocole RTCP V	56
6.4. Les protocoles secondaires	56
7. Qualité de service (QoS)	56
7.1. Gestion de la qualité de service	56
7.2. Problèmes liés à la qualité de service :	57
7.2.1. Gestion de la bande passante	57
7.2.2. Réduction de la latence	57
7.2.3. Réduction de la Gigue	57
7.2.4. Réduction du nombre de paquets perdus	58
7.2.5. Applications agressives	58
7.3. Politique de mise en place d'une qualité de service	58
8. Discussion	59

## CHAPITRE –IV

1. Préambule :	60
2. Le standard téléphonique traditionnel – PABX	60
2.1. Les fonctionnalités:	60
3. Le standard téléphonique IP – PBX-IP	61
3.1. Fonctionnalités IPBX .59	61
3.2. Les avantages	63
4. Installation de la solution VoIP	64
4.1. Identification des besoins	64
4.2. Asterisk :	64
4.3. Eléments nécessaires	65
4.4. Installation de serveur	66
4.4.1 Lancement de l'installation de trixbox	66
4.4.2. Premier démarrage	67
4.4.3. Connexion a l'interface graphique	69
4.5. Création des comptes SIP (Extension)	70
4.6. Installation des postes clients (Softphone)	72
4.7. Configurer les appels sortants	74
4.7.1. Le Trunks	74
4.7.2. La Routes	74
4.8. Configuration des appels entrants	74

5. Evaluation des performances avec Wireshark .....	76
6. Discussion.....	77
Conclusion.....	78
Bibliographie.....	80

## Table des figures

### CHAPITRE I

Figure 1.1 : Classification géographique des réseaux.....	5
Figure 1.2 : Exemple d'architecture Client/Serveur.....	7
Figure1.3 : Exemple d'architecture Pair à Pair (P2P).....	7
Figure1.4 : Topologie en bus.....	8
Figure 1.5 : Topologie en étoile .....	9
Figure 1.6 : Topologie en anneau .....	9
Figure 1.7 : Principe de transmission de donnée dans le modèle OSI.....	12
Figure 1.8 : différents types de modulation.....	14
Figure 1.9 : Sens de transmission.....	14
Figure 1.10 : Transmission parallèle.....	15
Figure 1.11 : Transmission série.....	15
Figure 1.12 : La bande passante .....	18
Figure 1.13: Câble paires torsadées.....	18
Figure 1.14 : Câble coaxial.....	19
Figure 1.15 : Fibre optique- guide de lumière.....	19

## CHAPITRE II

Figure 2.1 : Structure d'une adresse IP.....	25
Figure 2.2 : Adresses d'un routeur.....	26
Figure 2.3 : Décomposition d'un réseau en sous réseaux.....	27
Figure 2.4: format d'adressage classe A.....	28
Figure 2.5: format d'adressage classe B.....	29
Figure 2.6 : format d'adressage classe C.....	29
Figure 2.7: forma d'adressage classe D.....	29
Figure 2.8 : Exemple de routage direct.....	31
Figure 2.9: Exemple de routage indirect.....	31
Figure 2.10: Exemple de routage par défaut.....	32
Figure 2.11: La translation d'adresses réseaux.....	33
Figure 2.12 : Fonctionnement de DNS.....	34
Figure 2.13 : Le serveur DHCP.....	34

## CHAPITRE III

Figure 3.1 : Le réseau RTC.....	37
Figure 3.2 : Architecture PC to PC.....	37

Figure 3.3 : Architecture PC to Phone.....	38
Figure 3.4 : Architecture Phone to Phone.....	38
Figure 3.5 : Schéma général de l'utilisation de la VoIP.....	40
Figure 3.6 : Echantillonnage et quantification.....	42
Figure 3.7 : Envoi de données et codage.....	42
Figure 3.8 : Eléments d'une architecture H.323.....	44
Figure 3.9 : Déroulement d'une communication H.323.....	45
Figure 3.10 : Pile de protocole H323.....	46
Figure 3.11 : Eléments d'un réseau SIP.....	48
Figure 3.12: Syntaxe de base d'un message SIP.....	49
Figure 3.13 : Exemple d'entête SIP.....	49
Figure 3.14 : Enregistrement d'un UA auprès de son Registrar.....	51
Figure 3.15: Initialisation et fermeture d'une session SIP.....	51

## Introduction générale

Le développement des technologies de transfert de la voix fondées sur le protocole IP constitue potentiellement un élément majeur de l'évolution du monde des télécommunications. Il y a quelques années, la téléphonie classique ou RTC constituait l'exclusivité des télécommunications et les offres des opérateurs étaient guidées uniquement par la concurrence dans le domaine. De nos jours la donne a changé. La popularité de l'Internet, rendue possible grâce à la baisse des tarifs d'accès et des coûts de communication, conjuguée à l'innovation de la technique dans le domaine des réseaux IP et RTC a permis de donner naissance à la téléphonie sur IP. Au delà de la nouveauté technique, la téléphonie sur IP constitue un véritable eldorado financier du fait des économies substantielles qu'elle engrange. La possibilité de fusion des réseaux informatiques et téléphoniques entraîne non seulement une diminution de la logistique nécessaire à la gestion des deux réseaux, mais aussi une baisse importante des coûts de communication.

Côté services, cette intégration peut aussi permettre d'ajouter des fonctions de communications nouvelles aux équipements utilisés actuellement :

- Un poste téléphonique va pouvoir communiquer avec n'importe quel ordinateur de l'Internet ;
- Un ordinateur intégrera toutes les fonctions d'un téléphone ;
- Le transport de la vidéo entre ordinateurs sera plus facilement généralisable;
- L'intégration des messageries vocales et Internet sera très facile ;
- De nouveaux services d'annuaires, de communications de groupe (« multicast téléphonique ») seront facilement réalisables, etc.

Toutefois, les aspects techniques sous-jacents à cette nouvelle technologie ne sont pas toujours bien maîtrisés. Les problèmes dus à la gestion de la bande passante sur Internet, la qualité audio, l'écho, etc. sont tant de contraintes qui restent encore à dominer.

Après une introduction, sommaire et des objectifs le plan de notre travail est comme suit :

Le chapitre I présente des généralités sur les réseaux. Dans ce chapitre,

nous donnons un petit aperçu sur les types de réseaux et les différentes topologies physiques et logiques. Nous donnons également des définitions des différentes techniques de communication et des supports de transmission.

Le chapitre II est consacré à une brève étude sur les réseaux IP et des protocoles qu'ils enveloppent. On présentera également le model TCP/IP et les différents class d'adresses IP.

Le chapitre III concerne la voix sur IP, des définitions importantes et les différentes architecture et standards du VoIP.

Le chapitre IV presente une étude technique et mise en place d'une solution VoIP basé sur le serveur Asterisk avec le protocole SIP.

Nous finirons ce mémoire par une conclusion générale et quelques perspectives.

# CHAPITRE I

---

## *Généralités sur les réseaux informatiques*

## 1. Préambule

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que des stations de travail ou des serveurs.

Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo sur ces réseaux informatiques devient naturelle même si cela ne va pas sans difficulté.

Les réseaux peuvent être classés en trois catégories principales, selon le type et l'origine des informations :

- Réseaux téléphoniques des opérateurs de télécommunications.
- Réseaux informatiques nés de posemètre de communique des ordinateurs.
- Réseaux de diffusion acheminant les programmes audiovisuels.

Chacune de ces catégories présente des caractéristiques, liées aux applications téléphone, informatique, et de vidéo transportées par les différents réseaux.

## 2. Notion de réseau [1]

### 2.1. Qu'est ce qu'un réseau ?

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

• **Réseau (Network)** : Ensemble des ordinateurs et périphériques connectés les uns aux autres.

• **Mise en réseau (Networking)** : Mise en œuvre des outils et des tâches permettant de relier des ordinateurs afin qu'ils puissent partager des ressources.

Selon le type d'objet, on parlera parfois de :

• **Réseau téléphonique**: Qui permet de faire circuler la voix entre plusieurs postes téléphoniques.

• **Réseau de neurones**: Ensembles de cellules interconnectées entre elles.

• **Réseau informatique:** ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données binaires.

### **2.2. L'intérêt des réseaux**

Un ordinateur est une machine permettant de manipuler des données. L'homme, un être de communication, a vite compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations. Voici un certain nombre de raisons pour lesquelles un réseau est utile, un réseau permet:

- Le partage de fichiers, d'applications.
- La communication entre personnes.
- La communication entre processus.
- La garantie de l'unicité de l'information (bases de données).
- Le jeu à plusieurs.
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).

Les réseaux permettent aussi de standardiser les applications, on parle généralement de groupware. Par exemple la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement.

Avantages de tels systèmes :

- Diminution des coûts grâce aux partages des données et des périphériques.
- Standardisation des applications.
- Accès aux données en temps utile.
- Communication et organisation plus efficace.

### **2.3. Les différents types des réseaux**

Les réseaux ont des capacités différentes. Le type de réseau dépend des critères suivants :

- Taille de l'entreprise.
- Niveau de sécurité nécessaire.

- Type d'activité.
- Niveau de compétence d'administration disponible.
- Volume du trafic sur le réseau.
- Besoins des utilisateurs du réseau.
- Budget alloué au fonctionnement du réseau.

On peut faire une classification des réseaux à l'aide de leur taille et la fonction qu'ils accomplissent.

### 2.3.1. La classification géographique [1], [2]

- **PAN (Personal Area Network):** La plus petite taille de réseau. Ces réseaux personnels interconnectent sur quelques mètres les équipements personnels tels que GSM, portable, organiseur, clé USB... d'un même utilisateur.

- **LAN (Local Area Network):** Peut s'étendre de quelques mètres à un kilomètre et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.

- **MAN (Metropolitan Area Network):** Interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.

- **WAN (Wide Area Network) :** Permet de communiquer à l'échelle d'un pays ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications. Exemple : Internet.

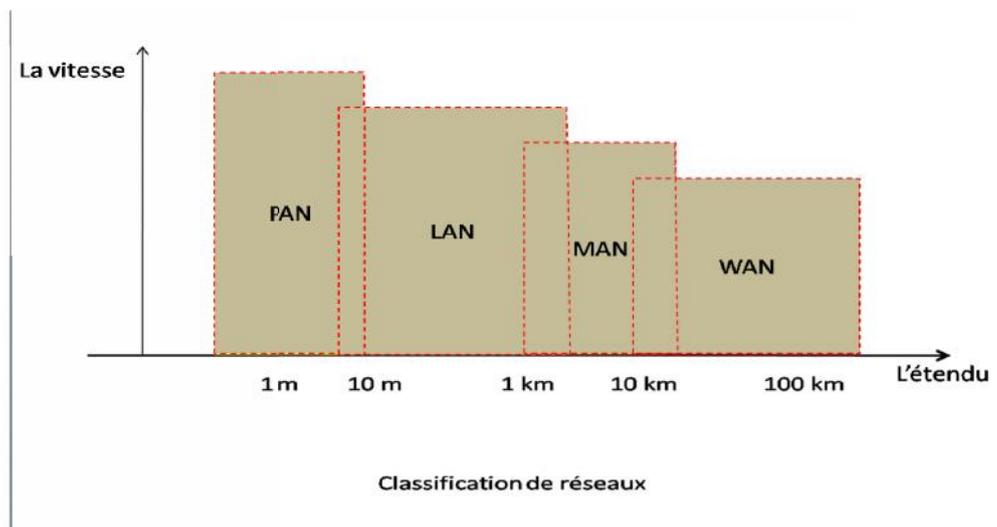


Figure 1.1 : Classification géographique des réseaux

### 2.3.2. La classification fonctionnelle [3]

Certains réseaux sont classés en fonction des tâches qu'ils accomplissent :

- **Intranet** : Est un réseau informatique utilisé à l'intérieur d'une entreprise ou de toute autre entité organisationnelle utilisant les techniques de communication d'Internet.

- **Extranet** : En extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'extranet se fait via Internet, par une connexion sécurisée.

- **Internet** : Internet constitue un réseau informatique mondial, utilisant un ensemble standardisé de protocoles de transfert de données. C'est donc un réseau composé de millions de réseaux publics et privés.

### 2.3.3. Les réseaux homogènes et les réseaux hétérogènes

- **Homogènes** : Tous les ordinateurs sont du même constructeurs.

- **Hétérogènes** : Les ordinateurs reliés au réseau sont de constructeurs divers.

### 2.3.4. Les différentes catégories des réseaux [4]

On distingue également deux catégories de réseaux :

- **Le réseau Client/Serveur** :

Un environnement client/serveur désigne un mode de communication à travers un réseau entre plusieurs programmes. Des programmes qualifié de clients, envoient des requêtes, les autres, qualifiés de serveurs, attendent les requêtes des clients et y répondent.

Un client désigne également l'ordinateur sur lequel est exécuté le logiciel client, et le serveur, l'ordinateur sur lequel est exécuté le logiciel serveur.

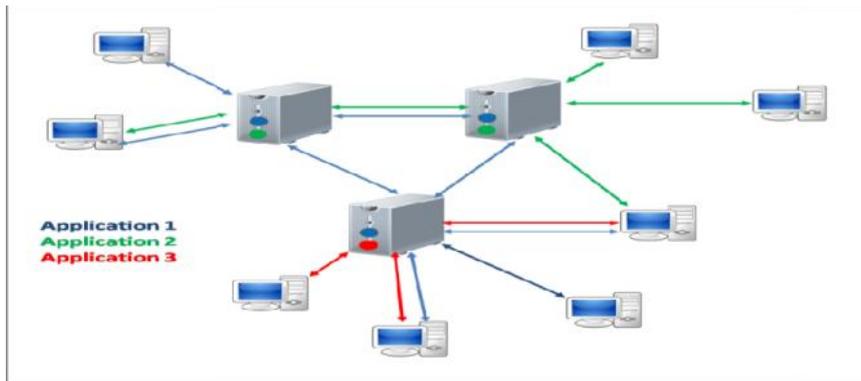


Figure 1.2 : Exemple d'architecture Client/Serveur

- **Le réseau Peer to Peer (P2P) :**

Le Peer to Peer ou pair à pair (P2P) est un modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur.

Le pair à pair peut être centralisé ou décentralisé. Il peut servir au partage de fichiers en pair à pair, au calcul scientifique ou à la communication.

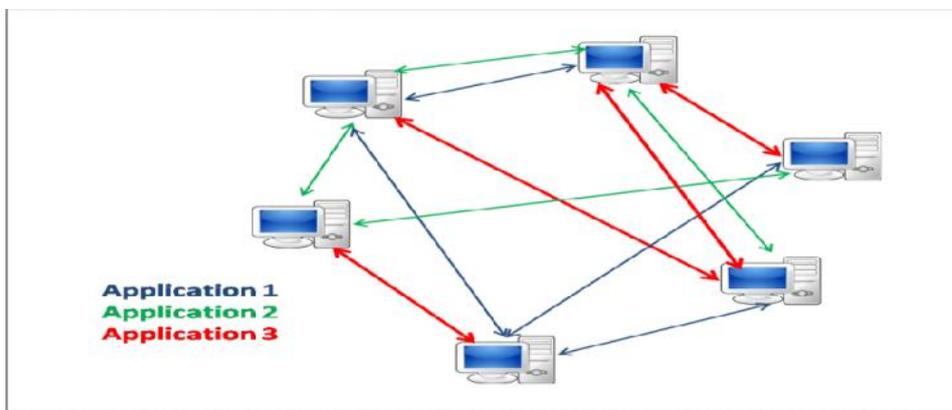


Figure1.3 : Exemple d'architecture Pair à Pair (P2P)

## **2.4. Les topologies des réseaux [2], [4], [6]**

Il faut distinguer deux topologies: La topologie physique et la topologie logique (électrique).

### **2.4.1. La Topologie physique**

La topologie physique c'est la configuration spatiale, visible, du réseau. Il en existe trois types : En bus, en étoile et en anneau. Ces éléments de base sont combinés pour former des réseaux complexes.

## CHAPITRE I Généralités sur les réseaux informatiques

- **La topologie en bus :** La voie est constituée d'un support linéaire ou d'un ensemble de segments reliés par des répéteurs. Les nœuds sont reliés de part et d'autre de ce câble.

Si ce câble unique vient à être défaillant, c'est l'ensemble du réseau qui tombe en panne mais si un hôte tombe en panne, le réseau n'est pas affecté.

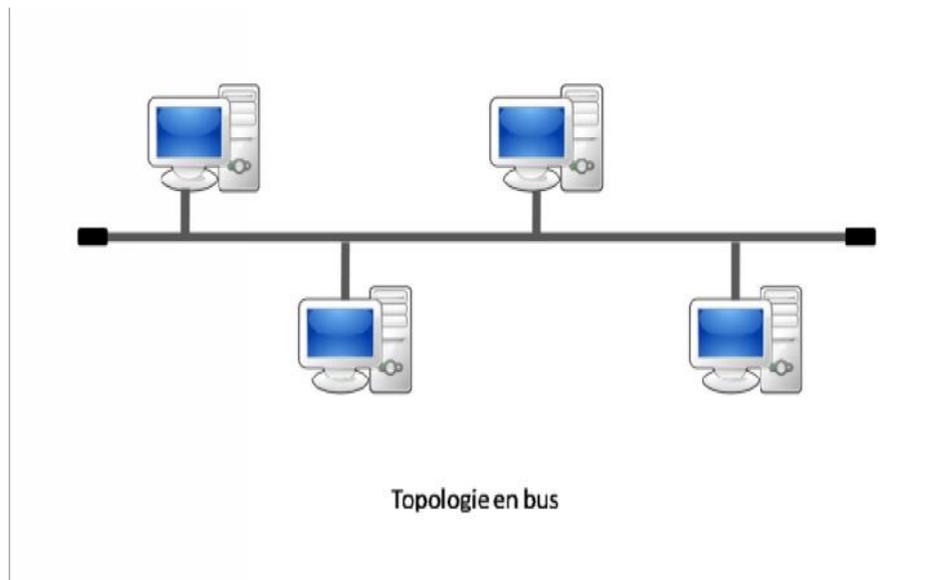


Figure1.4 : Topologie en bus

- **La topologie en étoile :** Les nœuds sont tous connectés à un concentrateur central par lequel transitent toutes les transmissions (Hub ou Switch).

Si un câble ou un nœud est défaillant, cela ne touche que cette station, et le reste du réseau n'est pas affecté alors que la panne du concentrateur central immobilise tout le réseau.

- **La topologie en étoile répartie:** C'est une méthode dérivée de la topologie en étoile. On peut relier plusieurs concentrateurs sur un seul câble.

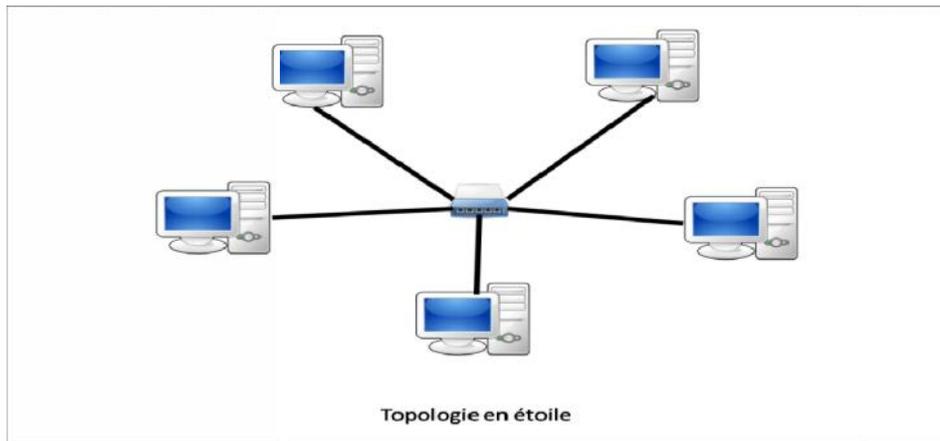


Figure 1.5 : Topologie en étoile

- **La topologie en anneau :** Les machines sont reliées en anneau unidirectionnel ou bidirectionnel formant une succession de liaisons point à point circulaire.

Tous les coupleurs doivent être en état de fonctionnement sinon tout le réseau est bloqué. L'utilisation d'un double anneau augmente la sécurité.

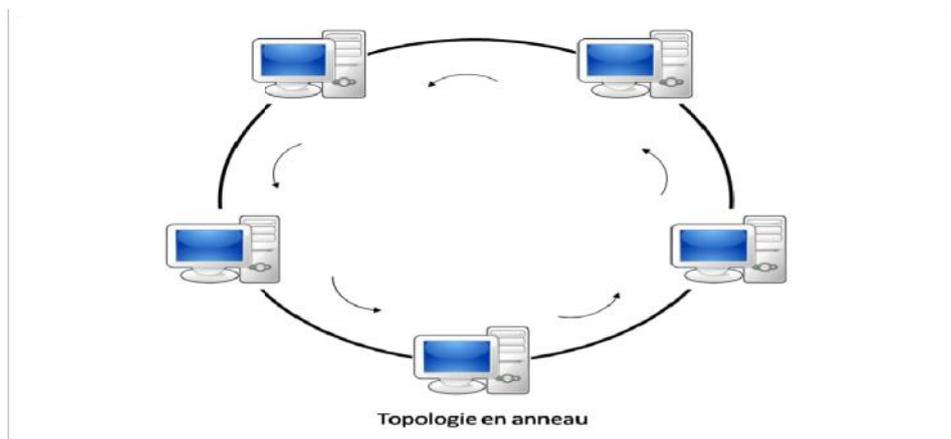


Figure 1.6 : Topologie en anneau

### 2.4.2. La topologie logique

La topologie logique représente la façon selon laquelle les données transitent dans les câbles.

- **En bus :**

Cette topologie désigne le fait que lors de l'émission de données sur le bus par une station de travail, l'ensemble des stations de travail connectées sur le bus la reçoivent. Seule la station de travail à qui le message est destiné la recopie.

**a) La topologie en bus unidirectionnel :**

Cette topologie nécessite deux bus séparés, il en existe deux types:

- Les stations émettent et reçoivent dans un sens sur un des deux bus et dans l'autre sur le second bus.
- Les stations émettent et reçoivent les données sur les deux bus grâce à deux fréquences séparées, une par bus : Fréquence 1, Fréquence 2 .

**b) La topologie en bus bidirectionnel :**

L'émission et la réception se font sur un bus unique, mais non simultanément. Lorsqu'une station émet le signal se propage dans les deux sens. Cette technologie est utilisée par les réseaux Ethernet, Appletalk, et Token Bus d'IBM.

- **En anneau :**

L'information circule le long de l'anneau dans un seul sens. A chaque passage d'un message au niveau d'une station de travail, celle-ci regarde si le message lui est destiné, si c'est le cas elle le recopie.

Cette technologie est utilisée par les réseaux Token Ring et FFDI ( FiberDistributed Data Interface, réseau double anneaux ).

- **En étoile :**

L'ensemble des stations de travail est connecté à un concentrateur qui examine le contenu du message, qui le régénère, et qui le transmet qu'à son destinataire. C'est en réalité un réseau de "n" liaisons point par point, car il établit un circuit entre une paire d'utilisateurs. Concentrateur

Cette technologie est utilisée pour les réseaux téléphoniques privée ( PABX ), et les réseaux Starlan et Arcnet.

**Remarque :**Un réseau ayant une topologie physique en étoile peut très bien avoir une topologie logique en bus.

### **3. Lemodèle de référence OSI[4], [5]**

#### **3.1. Définition**

OSI (Open SystemsInterconnection) ou Interconnexion des SystèmesOuverts est un modèle mis en place par l'ISO (International Standard Organization) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs. En effet, aux origines des réseaux chaque constructeur avait un système propre à lui.

Ainsi de nombreux réseaux incompatibles coexistaient. C'est la raison pour laquelle l'établissement d'une norme a été nécessaire. Le rôle du modèle OSI consiste à normaliser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits compatibles.

#### **3.2. Les différentes couches**

L'architecture de modèle OSI est défini sur 7 couches :

- **La couche physique** : Est chargée de la transmission effective des signaux entre les interlocuteurs. Son service est limité à l'émission et la réception d'un bit ou d'un train de bit continu.
- **La couche liaison de données** : Gère les communications entre 2 machines adjacentes, directement reliées entre elles par un support physique.
- **La couche réseau** : Gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets.
- **La couche transport** : Gère les communications de bout en bout entre processus.
- **La couche session** : Gère la synchronisation des échanges et les transactions, elle permet l'ouverture et la fermeture de session.
- **La couche présentation** : Est chargée du codage des données applicatives, précisément de la conversion entre données manipulées au niveau applicatif et chaînes d'octets effectivement transmises.

- **La couche application** : Est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme.

### 3.3. La transmission de données dans le modèle OSI

Le processus émetteur remet les données à envoyer au processus récepteur à la couche application qui leur ajoute un entête application. Le résultat est alors transmis à la couche présentation.

La couche présentation transforme alors ce message et lui ajoute un nouvel entête. Pour la couche présentation, l'entête application (AH) fait partie des données utilisateur. Une fois le traitement terminé, la couche présentation envoie le nouveau message à la couche session et le même processus recommence.

Les données atteignent alors la couche physique qui va effectivement transmettre les données au destinataire. A la réception, le message va remonter les couches et les en-têtes sont progressivement retirés jusqu'à atteindre le processus récepteur.

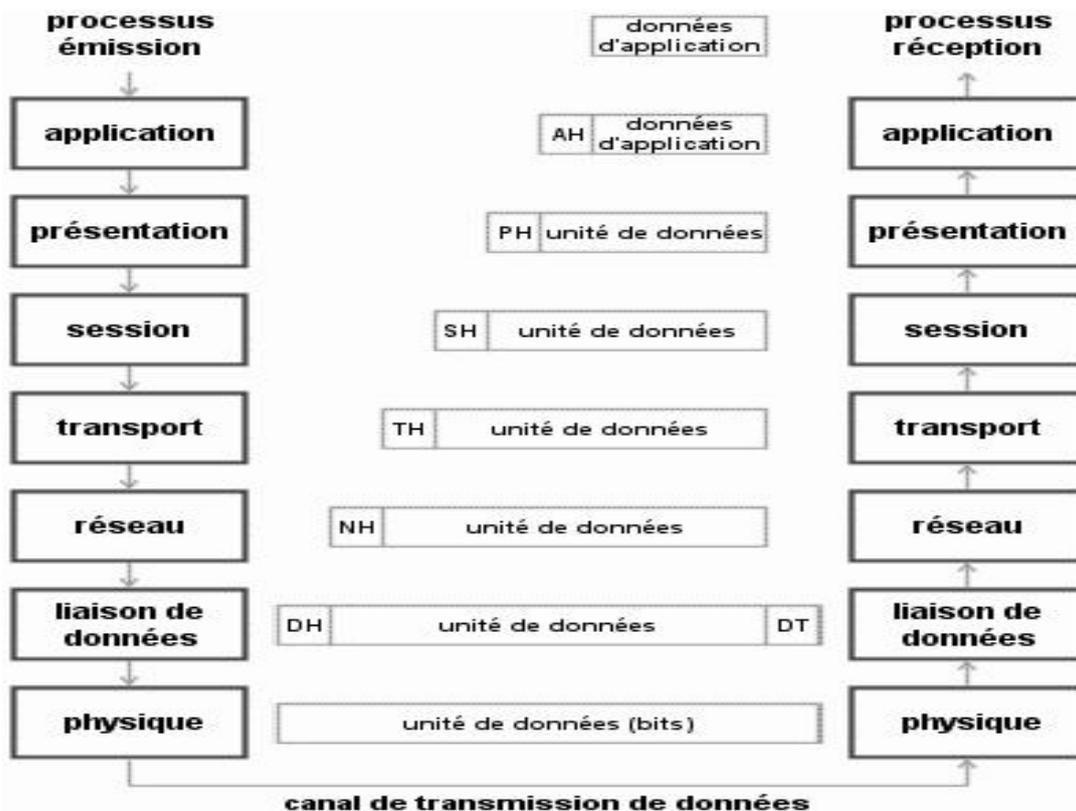


Figure 1.8 : Principe de transmission de donnée dans le modèle OSI

Le concept important est le suivant : il faut considérer que chaque couche est programmée comme si elle dialoguait directement avec sa couche paire réceptrice. Au moment de dialoguer avec sa couche paire, chaque couche rajoute un entête et l'envoi virtuellement, grâce à la couche sous-jacente, à sa couche paire.

### **4. La transmission dans les réseaux [6], [7], [8]**

#### **4.1. Les techniques de transmission**

Dans l'ordinateur, le signal est numérique et utilise deux tensions pour représenter le bit. Le signal correspondant à la séquence binaire et circulant sur le support de transmission est soit un signal analogique soit un signal numérique. Le choix est fait selon les caractéristiques du support et ceux du signal à transmettre.

La technique de transmission numérique est appelée Transmission en Bande de Base tandis que la transmission analogique est appelée Transmission par Transposition de Fréquence.

L'équipement mettant en œuvre une technique de transmission est l'ETCD.

Dans le cas où nous désirons transmettre l'information analogique par un signal numérique, il faut au préalable la numériser. Ceci est effectué par un Codec.

##### **4.1.1. La transmission en Bande de base**

Dans cette technique, l'information est directement codée par des tensions et le signal généré est transmis sur la ligne. Cette transmission est celle effectuée au sein de l'ordinateur. La transmission directe de ce signal sur un support de transmission peut être envisagée mais différents éventuels problèmes de transmission conduisent à considérer d'autres solutions de codage.

Différents codages ont été proposés, par exemple: le codage NRZ et le codage biphase.

##### **4.1.2. La transmission par transposition de base**

## CHAPITRE I Généralités sur les réseaux informatiques

La transmission par transposition de base consiste à utiliser un signal sinusoïdal de base dont les caractéristiques, amplitude, fréquence, phase sont modifiées en fonction de l'information à transmettre. C'est le codage par modulation.

Cette technique est utilisée lorsque la Bande Passante du support ne permet pas de transmettre directement le signal d'origine. Elle est aussi utilisée pour des supports large bande dans le cas de partage de la bande passante.

Plusieurs codages sont possibles: modulation d'amplitude, de fréquence, de phase ou d'une combinaison de ces paramètres. Il est possible de coder le bit comme le dibit ou le tribit. Cette multivalence permet d'augmenter le débit.

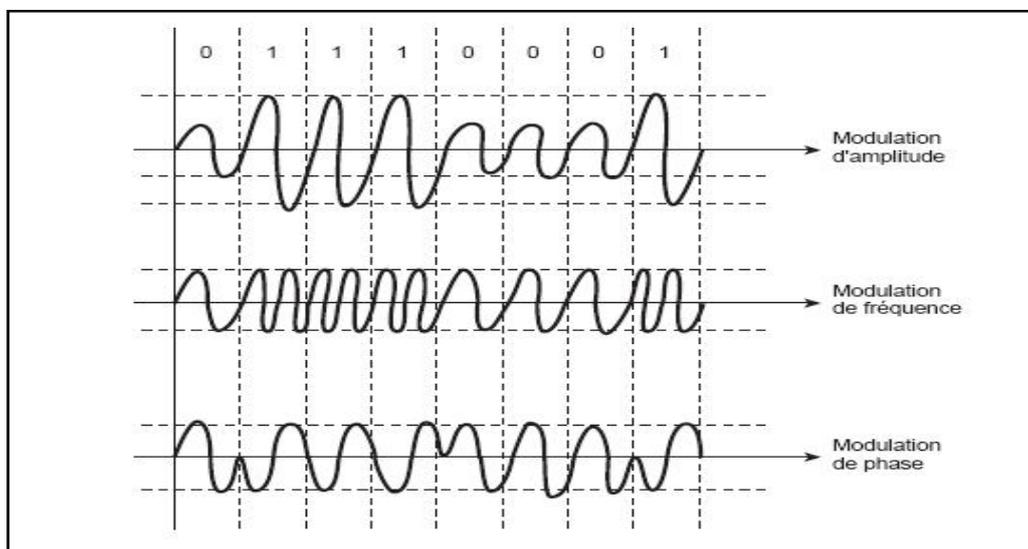


Figure 1.9 : différents types de modulation

### 4.2. Le sens de transmission

Désigne le mode d'exploitation de la liaison, il dépend du choix fait par le protocole de liaison.

- **Simplex** : Dans ce mode simplex, l'échange de données se fait dans un seul sens.
- **Half-Duplex** : l'échange se fait alternativement dans les deux sens.
- **Full-Duplex** : dans ce troisième type les stations peuvent émettre simultanément sans aucune contrainte.

Les schémas suivants, montrent les modes d'exploitation d'une liaison entre deux points A et B.

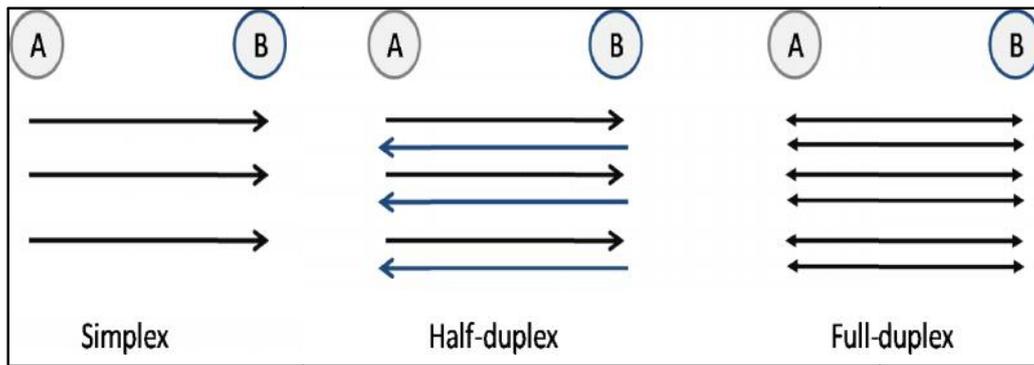


Figure 1.10 : Sens de transmission

### 4.3. Les types de transmission

#### 4.3.1. La transmission parallèle

La transmission parallèle est caractérisée par un transfert simultané de tous les bits d'un même mot. Elle nécessite autant de conducteurs qu'il y a de bits à transmettre.

Ce type de transmission est très performant en terme de débit. Elle est utilisée pour des liaisons entre un ordinateur, ses périphériques et ses unités de calcul esclaves.

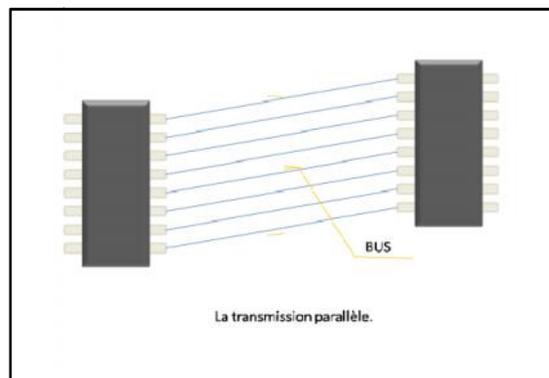


Figure 1.11: Transmission parallèle

#### 4.3.2. La transmission série

En transmission série, tous les bits d'un mot ou d'un message sont transmis successivement sur une même ligne.

La transmission série nécessite une interface de conversion pour sérialiser les bits en émission (conversion parallèle/série) et les désérialiser en réception (conversion série/parallèle).

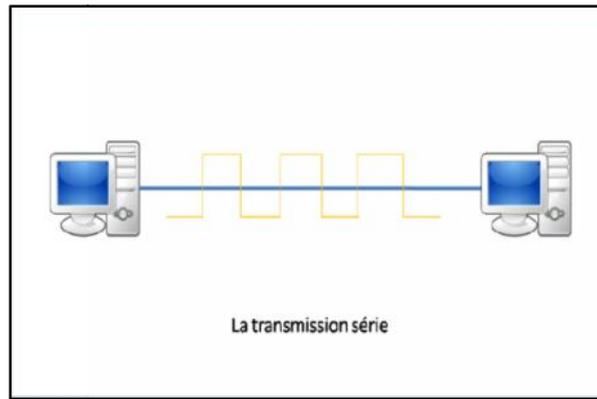


Figure 1.12 : Transmission série

#### **4.4. Les techniques de Commutation[1]**

La commutation dans ce contexte, c'est la manière de faire passer l'information de l'émetteur au récepteur.

##### **4.4.1. La commutation de circuits**

Utilisée sur le réseau téléphonique, RNIS, GSM, par la création d'un circuit physique reliant les deux extrémités lors de l'établissement de la connexion.

- Elle est adaptée au transport de la voix
- Contrainte de temps de transmission (téléphonie : isochronie et écho)
- **Inconvénient** : le circuit est occupé pendant la communication, qu'il soit utilisé ou non.

##### **4.4.2. La commutation de messages**

La commutation de message consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de nœud de commutation à un nœud de commutation. Chaque nœud de commutation attend d'avoir reçu complètement le message avant de le réexpédier au nœud suivant.

##### **4.4.3. La commutation de paquets**

L'information est découpée en paquets qui sont transportés de point en point à l'autre extrémité du réseau, une reconstitution est nécessaire une fois l'information arrive au destinataire.

La commutation de paquets est utilisée sur les réseaux locaux, Internet, Frame Relay, GPRS.

### 4.4.4. La commutation de cellules

Utilisée par ATM (Asynchronous Transfer Mode) Cellule de taille fixe : 53 octets (5 d'en-tête + 48 de données)

- Temps de commutation très faible par rapport au temps de propagation du signal.
- Permet d'introduire des notions de qualité de service
- Utilisée principalement sur les liens d'interconnexion ou dans des applications multimédia.

### 4.5. Les modes de communication [9]

#### 4.5.1. Mode avec/sans connexion

Ñ **Mode connecté** : toute transmission doit être précédée d'une demande de connexion réussie

- **Permet de contrôler proprement la transmission** : authentification des intervenants, contrôle de flux
- **Trois phases** : établissement de la connexion, transfert des données, coupure de la connexion
- Les ressources mobilisées ne sont pas forcément utilisées.

Ñ **Mode non connecté** : pas de négociation entre les intervenants, ni contrôle de flux ou d'erreur. Il est bon pour des envois de messages courts ; similaire à l'envoi d'une lettre à la Poste.

#### 4.5.2. Le mode d'envoi des informations

Ñ **Unicast** : point à point, c'est le cas général une source, une destination.

Ñ **Multicast** : multidiffusion, une source, des destinations multiples. Permet d'atteindre plusieurs correspondants à la fois, utilisé dans certaines applications.

Ñ **Broadcast**: multidiffusion, une source, toutes les cibles possibles, en général, toutes les machines d'un réseau local.

### 5. Les supports de transmission [7], [8]

L'infrastructure d'un réseau, la qualité de service offerte, les solutions logicielles à mettre en œuvre dépendent largement des supports de transmission utilisés. Les supports de transmission exploitent les propriétés de conductibilité des métaux, et

aussi celles des ondes électromagnétiques ou encore celles du spectre visible de la lumière.

Généralement on classe les supports en deux catégories :

- **les supports guidés** : supports cuivre et supports optiques.
- **les supports libres** : faisceaux hertziens et liaisons satellites.

### 5.1. Les caractéristiques des supports de transmission

Le système de transmission devra réaliser l'adaptation du signal à transmettre au support utilisé. Les caractéristiques des supports diffèrent selon la nature physique du support et le mode de propagation choisi. Cependant, certaines caractéristiques sont communes à tous les types de support comme la bande passante, et d'autres sont spécifiques à chaque type de support. En général les caractéristiques les plus considérées sont : la bande passante, l'impédance caractéristique et le coefficient de vélocité.

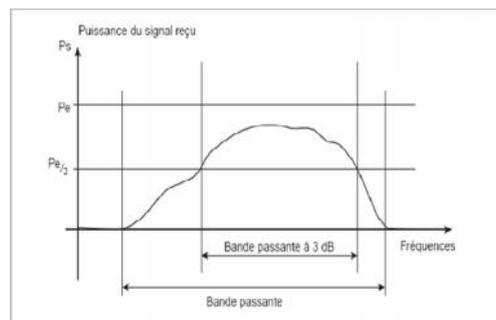


Figure 1.13 : La bande passante

### 5.2. Les types de supports de transmission

#### 5.2.1. Les paires torsadées

Est un câble l'origine de deux fils de cuivre isolés et enroulés l'un sur l'autre. Actuellement on utilise plutôt des câbles constitués de 2 ou 4 paires torsadées. Elle est très répandue, de connexion facile et d'un faible coût mais elle possède une faible immunité aux bruits. Il en existe les deux types suivants :

- **Blindées (STP: Shielded Twisted Pair).**
- **Non blindées (UTP: Unshielded Twisted Pair).**

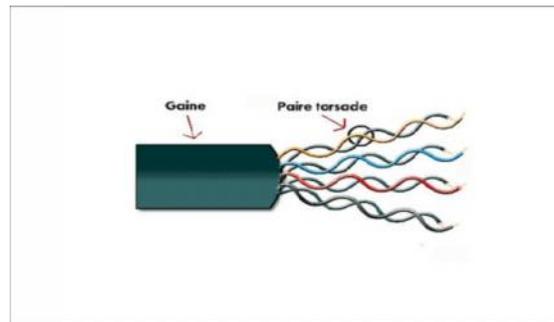


Figure 1.14: Câble paires torsadées

### **5.2.2. Le câble coaxial**

Une paire coaxiale ou câble coaxial est constituée de deux conducteurs concentriques maintenus à distance constante par un diélectrique. Le conducteur extérieur, tresse métallique en cuivre recuit appelée blindage, est mis à la terre. L'ensemble est protégé par une gaine isolante.

Le câble coaxial possède des caractéristiques électriques supérieures à celles de la paire torsadée. Il autorise des débits plus élevés et est peu sensible aux perturbations électromagnétiques extérieures.

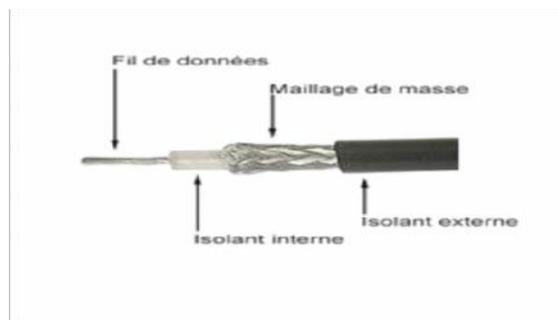


Figure 1.15 : Câble coaxial

### **5.2.3. La fibres optiques**

Ce type de câble, léger, possède une immunité parfaite au bruit et présente une très faible atténuation. Il tolère sans problème des débits de 100 Mb/s et plus. La largeur de bande atteint quelques dizaines de Mhz dans le cas des fibres multimodes et quelques GHz dans celui des fibres monomodes.

Toutefois, malgré sa flexibilité mécanique, ce type de câble ne convient pas pour des connexions dans un réseau local car son installation est problématique et son coût est élevé.

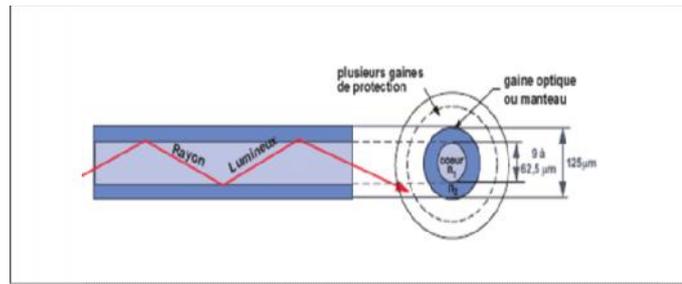


Figure 1.16 : Fibre optique- guide de lumière.

### 5.2.4. Les canaux hertziens

Elles supportent de grandes distances et de grandes capacités pour une propagation en visibilité directe (entre 50 et 80 Km). Les débits sont très élevés mais les transmissions sont sensibles aux perturbations et les possibilités d'écoute sont nombreuses.

### 5.2.5. Liaisons satellite

Les liaisons satellites sont très rapides, cependant elles sont dans un seul sens, ainsi lorsque l'on veut aller sur un site on ne peut pas en donner l'ordre.

## 6. Les équipements réseau [2]

### 6.1. Les concentrateurs (Hubs)

Servent à relier toutes les parties d'un même réseau physique, généralement tous les ordinateurs sont reliés à un Hub, sauf dans le cas d'un câblage coaxial. Lorsqu'une information arrive sur un Hub, elle est rediffusée vers toutes les destinations possibles à partir de celui-ci.

### 6.2. Les commutateurs (Switch)

Comme les Hubs, ils servent à relier toutes les parties d'un même réseau physique, mais d'une façon intelligente. A un instant donné, ils ne laissent passer les informations que vers la destination voulue.

### 6.3. Les répéteur (Repeater)

Sont des dispositifs permettant d'étendre la distance de câblage d'un réseau local. Leur rôle consiste à amplifier et à répéter les signaux qui leur parviennent. Ceci réduit le bruit et la distorsion. Le répéteur intervient au niveau 1 du modèle OSI.

#### **6.4. Les ponts (Bridge)**

Ils servent à relier entre eux deux réseaux différents d'un point de vue physique. De plus ils filtrent les informations et ne laissent passer que celles qui doivent effectivement aller d'un réseau vers l'autre. Ils peuvent être utilisés pour augmenter les distances de câblage en cas d'affaiblissement prématuré du signal.

#### **6.5. Les passerelles (Gateway)**

Sont des dispositifs permettant d'interconnecter des architectures de réseaux différentes. Elles offrent donc la conversion de tous les protocoles, au travers des 7 couches du modèle OSI. L'objectif étant de disposer d'une architecture de réseau évolutive.

#### **6.6. Les routeurs (Router)**

Ils relient des réseaux physiques et/ou logiques différents, généralement distants. Leur fonction principale est d'acheminer les informations au point suivant, ils filtrent aussi les informations mais à un niveau beaucoup plus fin, et l'on peut même s'en servir pour protéger un réseau de l'extérieur tout en laissant des réseaux amis accéder au réseau local.

### **7. Discussion**

Le choix d'une topologie adéquate, un bon système de câblage, une technique de transmission et de commutation efficace ainsi qu'une architecture conforme aux organismes de normalisation pour les réseaux est devenu aujourd'hui une préoccupation économique et technologique de première importance.

Les besoins sans cesse croissants en matière de communication qui converge de plus en plus vers le multimédia (voix, son, image, vidéo) ne seront supportés par les réseaux que si ces derniers évoluent vers les hauts débits alliant performance, qualité de service, rapidité et adaptabilité.

# CHAPITRE II

---

## *Les réseaux IP*

## 1. Préambule

Dans les années 1970, suite au foisonnement des systèmes utilisant des protocoles différents et incompatibles, le département américain de la défense décide de définir son propre architecture.

Cette architecture dite TCP/IP, est née de besoin industriel, donc plus pratique contrairement au modèle OSI.

TCP/IP est la source de réseau Internet, elle est rapidement adoptée par plusieurs constructeurs.

## 2. Le modèle TCP/IP [4], [14]

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait deux protocoles étroitement liés: un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise par-dessus un protocole réseau, IP (Internet Protocol).

Ce qu'on entend par modèle TCP/IP, c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le modèle Internet a été créé afin de répondre à un problème pratique, alors que le modèle OSI correspond à une approche plus théorique, et a été développé plus tôt dans l'histoire des réseaux. Le modèle OSI est donc plus facile à comprendre, mais le modèle TCP/IP est le plus utilisé en pratique.

### 2.1. Les différentes couches

La suite de protocoles désignée par TCP/IP, est construite sur un modèle en couches moins complet que le modèle OSI. Quatre couches sont suffisantes pour définir l'architecture de ce modèle.

#### 2.1.1. Couche application

C'est dans cette couche que se situent la plupart des programmes réseau et les protocoles qu'ils utilisent ( HTTP, FTP, DNS ,...).

Les applications fonctionnent généralement au-dessus de TCP ou d'UDP, et sont souvent associées à un port bien connu (HTTP port TCP 80, SSH port TCP 22, RIP port UDP 520, FTP port TCP 21)

**2.1.2. Couche transport**

Les protocoles de la couche de transport peuvent résoudre des problèmes comme la fiabilité des échanges et assurer que les données arrivent dans l'ordre correct. Dans la suite de protocoles TCP/IP, les protocoles de transport déterminent aussi à quelle application chaque paquet de données doit être délivré

**2.1.3. Couche Internet**

Cette couche reçoit des datagrammes en provenance de la couche réseau, qu'elle doit analyser pour déterminer s'ils lui sont adressés ou pas. Dans le premier cas elle doit décapsuler son entête du datagramme pour transmettre les données à la couche de transport et au bon protocole (TCP, UDP...), dans le deuxième cas elle les ignore.

Cette couche prend aussi en charge la communication de machine à machine.

**2.1.4. Couche physique**

La couche physique décrit les caractéristiques physiques de la communication, comme la nature du média utilisé (les câbles, les liens par fibre optique,...) et tous les détails associés comme les connecteurs, les types de codage ou de modulation, le niveau des signaux, les longueurs d'ondes, la synchronisation et les distances maximales.

**2.2. Concept des réseaux IP**

La plupart des réseaux sont des entités indépendantes, mises en place pour rendre un service à une population restreinte. Donc, il est impossible de trouver une technologie satisfaisant tous les types de besoin.

Dans cet environnement de base, les utilisateurs qui utilisent différents réseaux rencontrent généralement des difficultés pour se communiquer. L'Internet est le résultat de l'interconnexion de ces différents réseaux physiques par des routeurs.

Pour obtenir l'interfonctionnement des différents réseaux, la présence du protocole IP est obligatoire dans les nœuds qui vont faire le routage entre les réseaux. Globalement, l'Internet est donc un réseau à transfert de paquets. Ces paquets traversent un ou plusieurs sous-réseaux pour atteindre leur destination, sauf si l'émetteur se trouve dans le même sous-réseau que le récepteur.

**2.3. Les protocoles de chaque couche [2], [4]****2.3.1. Les protocoles de la couche application**

Les protocoles d'application sont des protocoles de haut niveau, adaptés aux besoins d'applications spécifiques.

- **Le protocole HTTP** : Ce protocole est utilisé pour la navigation web entre un serveur HTTP et un butineur. Le protocole assure qu'un logiciel client peut envoyer des requêtes et recevoir les réponses de serveurs HTTP sans problèmes particuliers.
- **Le protocole FTP** : Il permet d'assurer le transfert de fichiers de façon indépendante des spécificités des OS (Operating System).
- **Le protocole SMPT (Simple Mail Transfert Protocol)** : Le protocole qui permet d'acheminer le courrier depuis le serveur SMTP de l'émetteur, jusqu'au serveur SMTP du destinataire, qui le classe dans les Boîtes aux lettres de ses clients.
- **Le protocole POP3 (Post Office Protocol version 3)** : Le protocole qui permet au client de relever à distance le courrier classé dans sa boîte aux lettres.
- **Le protocole TELNET (Tele Network)** : Un client TELNET est une console en mode texte, capable de se connecter sur la plupart des serveurs, comme POP3 ou SMTP. Il devient alors possible d'envoyer et de lire des messages, si l'on connaît les commandes inhérentes aux protocoles SMTP et POP3.

Un serveur TELNET permet cependant des choses bien plus puissantes puisqu'il devient possible de prendre à distance le contrôle d'un hôte. C'est un outil qui permet l'administration distante d'une machine, du moment que l'on est capable d'ouvrir une session et d'acquérir les droits de super utilisateur.

**2.3.2. Les protocoles de la couche transport**

- **Le Protocole UDP (USER DATAGRAM PROTOCOL)** : Le protocole UDP est basé en couche 4. Il n'ouvre pas de session et n'effectue pas de control d'erreur. Il est alors appelé mode non connecté. Il est donc peut

fiable, cependant, il permet aux applications d'accéder directement à un service de transmission de Datagrammes rapide.

UDP est utilisé pour transmettre de faibles quantités de données où le coût de la création de connexions et du maintien de transmissions fiables s'avèrent supérieur aux données à émettre. UDP peut également être utilisé pour les applications satisfaisant à un modèle de type interrogation réponse. La réponse étant utilisée comme un accusé de réception à l'interrogation. On y trouve classiquement SNMP et DNS. UDP est aussi utilisé dans un second cas, tel que la voix sur IP.

L'envoi en temps réel est primordial, donc si une trame n'arrivait pas, la retransmission serait inutile. Chaque machine contient un ensemble de points de destination abstraits appelés protocole ports, identifiés par un entier positif codé sur deux octets. Une application qui souhaite communiquer sur le réseau avec une autre application doit se raccorder à un port. Une application est donc identifiée sur le réseau par :

- L'adresse IP de la station sur laquelle elle se trouve.
- Le protocole TCP ou UDP.
- Le port number auquel elle s'est raccordée.

Cette connexion logique entre deux ports est appelée : **Socket**. UDP est un protocole de transport utilisant directement IP ce qui entraîne qu'il offre un service de transport :

- Non fiable (sans acquittement).
  - Sans connexion.
  - Sans contrôle de flux.
- **Le protocole TCP (Transfert Control Protocol) :** Le protocole TCP est basé en couche 4. Il ouvre une session et effectue lui-même le contrôle d'erreur. Il est alors appelé mode connecté.

TCP fournit un service :

- Fiable (canal sans erreurs).
- Avec contrôle de flux.
- Ordonné.
- En mode full duplex et en mode connecté

**2.3.3. Les protocoles de la couche Internet**

- **Le protocole IP (Internet Protocol) :** IP représente le protocole réseau le plus répandu. Il permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée. Ce protocole utilise ainsi une technique dite de commutation de paquets.

Au niveau IP, les données des utilisateurs ou des applications sont encapsulées à l'intérieur d'unités de transfert appelées datagrammes IP. Le protocole IP fournit un service d'acheminement des datagrammes IP sans connexion et non fiable.

- **Le protocole ARP (Address Resolution Protocol) :** L'objectif d'ARP est de résoudre une adresse physique par l'intermédiaire de l'adresse IP correspondante d'un host distant.

Il permet d'obtenir l'adresse physique (MAC) d'une machine connaissant son adresse IP (logique).

- **Le protocole ICMP (Internet Control Message Protocol) :** Le protocole ICMP (Internet Control Message Protocol) permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des Datagrammes en erreurs.
- **Le protocole IGMP (Internet Group Management Protocol) :** Le protocole IGMP (Internet Group Management Protocol) permet de gérer les déclarations d'appartenance à un ou plusieurs groupes auprès des routeurs Multicast. Les inscriptions sont soit spontanées soit après requête du routeur. Pour cela, l'hôte envoie une trame IGMP destinées à ce ou ces groupes.

**3. L'adressage dans les réseaux IP [1], [2], [4]**

Comme le réseau Internet est un ensemble de réseaux différents, l'adressage est particulièrement important. Les adresses IP ont été définies pour être traitées rapidement. Les routeurs qui effectuent le routage en se basant sur

le numéro de réseau sont dépendants de cette structure.

### 3.1. Structure de l'adresse 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.



Figure 2.1 : Structure d'une adresse IP

Toutes les machines sur le même réseau auront la même partie réseau. En réalité, c'est l'adresse du point d'accès d'une machine sur un réseau donc, si un ordinateur change de réseau, il change d'adresse. Ainsi, si une station connectée à un réseau a normalement qu'une adresse IP, le routeur aura autant d'adresses IP que de réseaux qu'il interconnecte.

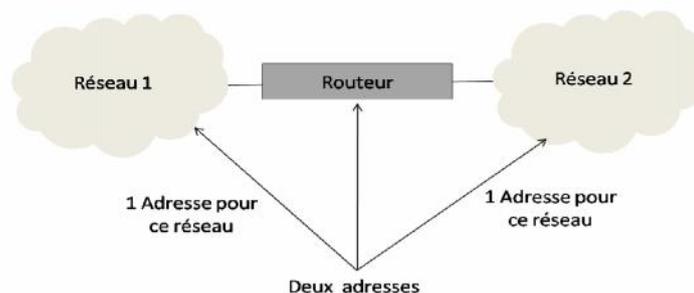


Figure 2.2 : Adresses d'un routeur

**3.2. 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 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 la possibilité d'adressage est donc 4294967296.

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

	IPV4	IPV6
Espace d'adressage	Une adresse sur 32 bits	Une adresse sur 128 bits
Structure de l'adresse	<b>4 mots</b> (x.x.x.x)	<b>8 mots</b> (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 puissance 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

TAB -1: L'espace d'adressage IP

**3.3. Sous réseaux**

Dans un réseau d'adresse par exemple 190.120.0.0 (classe B), on aura la possibilité de mettre 65000 machines sur un seul réseau. Mais ce n'est pas le cas en pratique, on crée donc des sous réseaux.

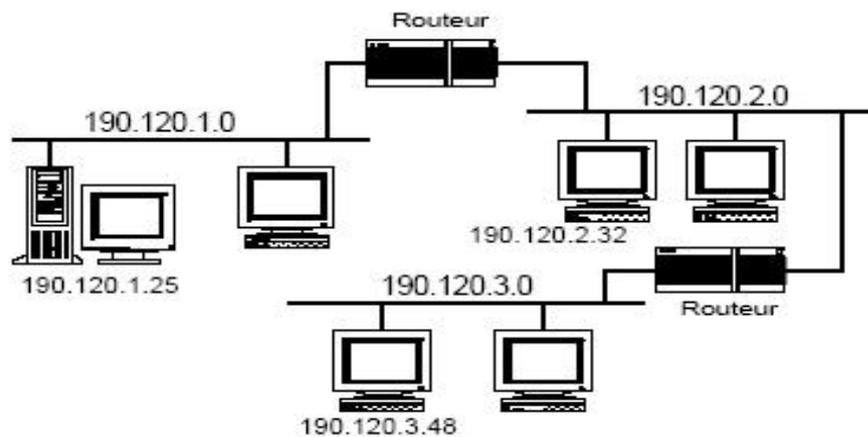


Figure 2.3 : Décomposition d'un réseau en sous réseaux

### 3.4. Le masque sous réseau

Une adresse IP est constituée d'une partie sera utilisée pour identifier le réseau et une autre partie (le reste) sera utilisée pour identifier la station à l'intérieur de 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, 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 sur Internet est 192.168.100.0 et l'adresse de la première station à l'intérieur de ce réseau est 192.168.100.1 .

### 3.5. 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

### 3.6. Les classes d'adresses

La partie réseau de l'espace d'adressage est divisée en classes A, B, C, D et 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.

<i>Partie réseau</i>	<i>Partie hôte</i>		
0xxxxxxx	Xxxxxxxx	Xxxxxxxx	Xxxxxxxx

Figure 2.4: Format 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.

<i>Partie réseau</i>	<i>Partie hôte</i>		
10xxxxxx	Xxxxxxxx	Xxxxxxxx	Xxxxxxxx

Figure 2.5: Format 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.

<i>Partie réseau</i>			<i>Partie hôte</i>
110xxxxx	Xxxxxxxx	Xxxxxxxx	Xxxxxxxx

Figure 2.6 : Format 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*).

<i>Adresse multidiffusion</i>			
111xxxxx	Xxxxxxxxxx	Xxxxxxxxxx	Xxxxxxxxxx

Figure 2.7: Format 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 un nombre maximum de stations pouvant bénéficier d'une adresse fixe à l'intérieur de chaque réseau.

Le tableau suivant représente les propriétés des différentes classes :

	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 1 <sup>er</sup> octet en binaire	00000001 à 01111110	10000000 à 10111111	11000000 à 11011111		
Nombre de machines par réseau	16 777 214	65 534	254		

**Tab 1:** Propriétés des classes d'adressage

4. Le routage [1], [2], [13]

Le routage est le processus permettant d'acheminer un datagramme IP de son hôte émetteur jusqu'à son hôte destinataire. Chaque datagramme est routé indépendamment des autres.

Le routage est une tâche exécutée dans de nombreux réseaux, tels que les réseaux de données électroniques comme l'Internet, et les réseaux de transports. Sa performance est importante dans les réseaux décentralisés. c'est-à-dire où l'information n'est pas envoyée à une source qui va les redistribuer mais échangée entre des agents indépendants.

4.1. Type de routage

Il existe deux types de routage appliqués selon la position de la machine de destinataire par rapport à la machine émettrice.

4.1.1. Le routage direct

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

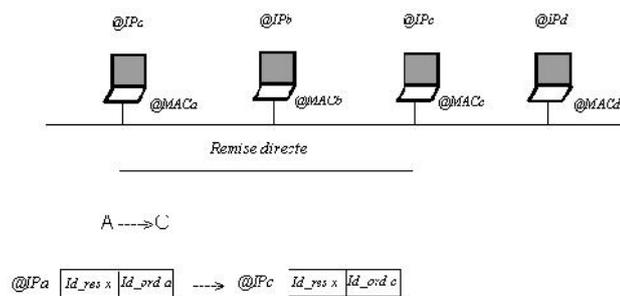


Figure 2.8 : Exemple de routage direct.

4.1.2. Routage Indirect

Si la machine de destination du datagramme ne se trouve pas sur le même réseau que la machine émettrice, il faut passer par un routeur (aussi appelé passerelle, dans un sens plus large et dans le cas de TCP/IP). L'adresse de la première passerelle par laquelle il faut passer pour atteindre la destination est appelée la route indirecte.

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

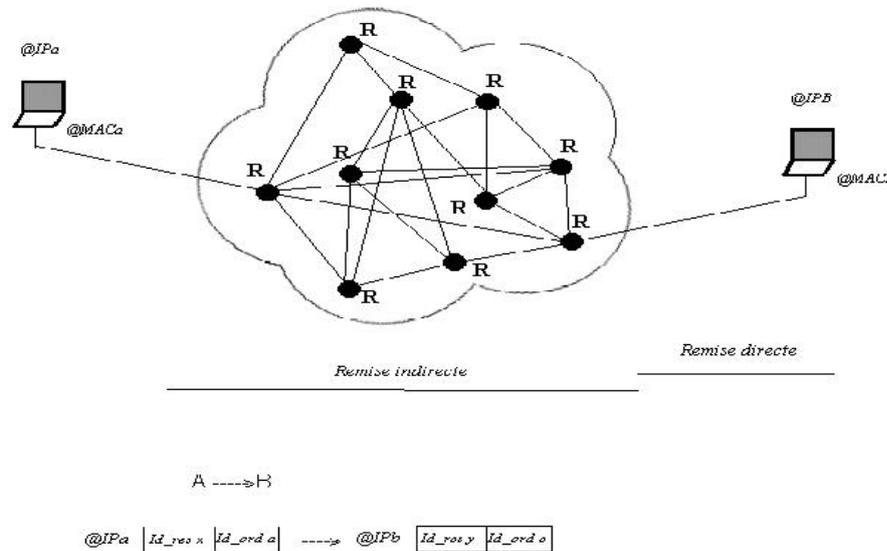


Figure 2.9: Exemple de routage indirect.

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

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

- **Routage par tables:** Les machines communiquant avec TCP/IP possèdent une table de routage IP. Il s'agit d'un ensemble de correspondances entre une adresse de réseau IP et l'adresse de la première passerelle à emprunter. Quand une machine émet un datagramme, elle vérifie d'abord si l'adresse du réseau de destination est reprise dans cette table. Si c'est le cas, elle peut y lire l'adresse de la passerelle vers laquelle il faut envoyer le datagramme.
- **Routage par défaut :** si la table de routage IP ne contient aucune entrée faisant référence à la destination du datagramme, celui-ci est alors envoyé vers une passerelle dite passerelle par défaut (default Gateway), dont l'adresse est généralement stockée dans la table de routage.

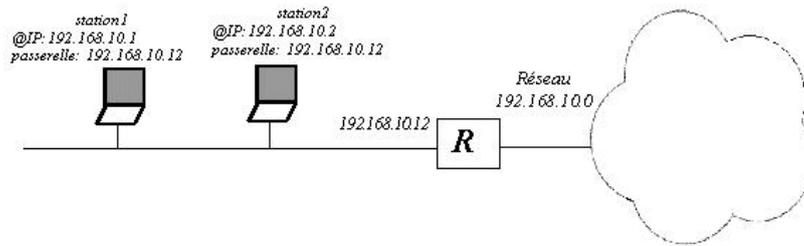


Figure 2.10: Exemple de routage par défaut.

## 4.2. Les protocoles de routage

- **Le protocole RIP (Routing Information Protocol)**

RIP est un protocole de routage IP de type vecteur de distances. Il permet à chaque routeur de communiquer aux routeurs voisins en utilisant le nombre de sauts comme métrique de sélection de chemin. Pour éviter les boucles de routage, le nombre de sauts maximum autorisé est égal à 15 et les mises à jour du routage sont diffusées par défaut toutes les 30 secondes.

Les limites de ce protocole entraînent le développement d'autres protocoles. En effet, le nombre de sauts est limité à 15, au delà, les paquets sont supprimés. Et aussi, RIP ne prend en compte que la distance entre deux machines en termes de saut, mais il ne considère pas l'état de la liaison afin de choisir la meilleure bande passante possible.

- **Le protocole IGRP (Interior Gateway Routing Protocol)**

Le protocole IGRP est un protocole de routage à vecteur de distance mis au point par Cisco. Il envoie les mises à jour de routage toutes les 90 secondes et donne aux réseaux des informations sur un système autonome particulier.

## 5. Le Network Address Translation [4], [12]

Un routeur fait du NAT (traduction d'adresse réseau) lorsqu'il fait correspondre les adresses IP internes non uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.

Avec une plage d'adresse IP codée sur 4 octets il est possible d'avoir  $256 \times 256 \times 256 \times 256 = 4\,294\,967\,296$  adresses IP différentes. 4 milliards

d'adresses IP ne suffisent plus pour affecter des adresses IP à toutes les stations existantes.

Pour remédier en partie à ce problème les plages d'adresses privées ont été créées.

NAT utilise l'adresse IP et le numéro de port d'une station et les transforme en une adresse IP et un numéro de port qui n'est pas attribué à une application standard.

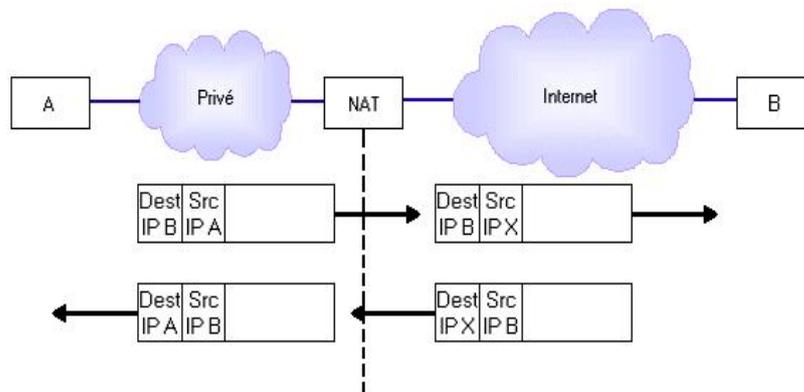


Figure 2.11: La translation d'adresses réseaux

## 6. Le DNS [2], [10]

Le DNS permet la mise en correspondance des adresses physiques dans le réseau et des adresses logiques. La structure logique est hiérarchique et utilise au plus haut niveau des domaines caractérisant principalement les pays, qui sont indiqués par deux lettres, comme dz pour l'Algérie, sn pour le Sénégal, ml pour le mali et des domaines fonctionnels comme : **.com**, **.edu**, **.org**, ...

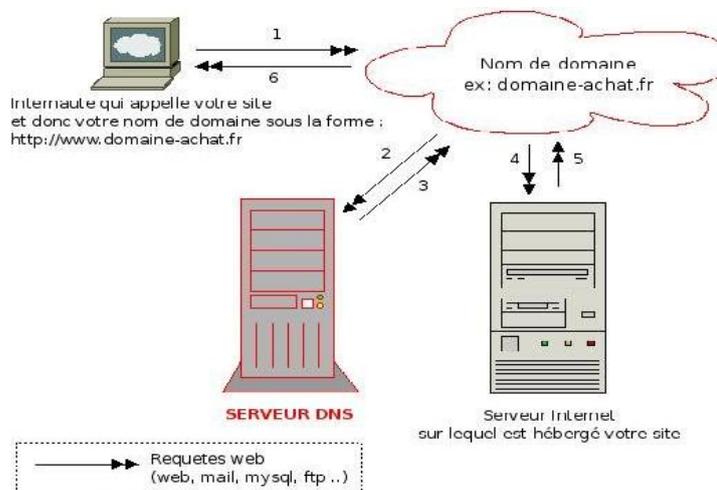


Figure 2.12 : Fonctionnement de DNS

## 7. Le DHCP [2], [11]

Il s'agit d'un système qui permet dynamiquement d'attribuer une adresse IP à un poste qui se connecte au réseau.

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

Ce système est bien pratique, lorsque il fonctionne correctement, il évite à l'utilisateur d'avoir à configurer manuellement sa pile IP. Il permet également à l'administrateur de réseau de modifier son architecture sans avoir à prévenir tous ses clients.

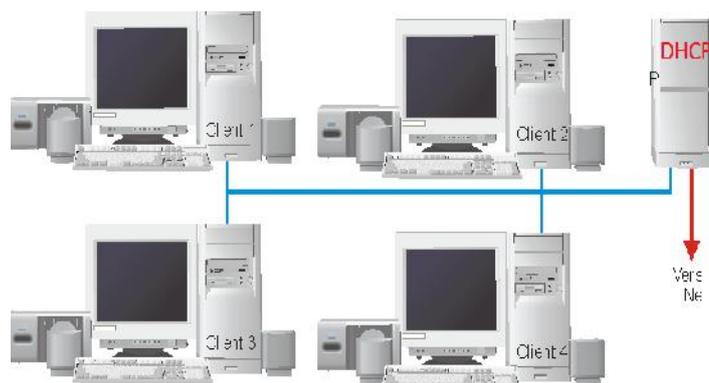


Figure 2.13 : Le serveur DHCP

## 8. Discussion

Nous avons présenté de manière générale le modèle TCP/IP, le plus largement répandu puisqu'il est plus pratique et plus utilisé. On a expliqué l'architecture en couches, le fonctionnement et les protocoles de chacune de ces couches. On a parlé aussi de système d'adressage IP et le principe d'acheminement de données par les différentes techniques de routage.

Comprendre les principes de TCP/IP est très important pour entamer une étude de la voix sur IP, puisque cette dernière se base essentiellement sur les réseaux IP.

## CHAPITRE III

---

### *La voix sur les réseaux IP*

## 1. Préambule

L'émergence de nouvelles technologies peut parfois être effrayante pour les entreprises qui ne savent pas toujours déterminer la voie à suivre. Bien souvent, elles sont en retard dans l'évolution de leurs réseaux ou de leur matériel informatique.

Aujourd'hui, des standards sont en train d'émerger et des entreprises commencent à satisfaire le marché en fournissant des passerelles faisant le lien entre le monde IP et le monde RTCP.

Le but de la téléphonie sur IP est de finaliser la convergence voix/données autour d'un protocole unique, IP. En effet, la téléphonie IP se base sur la même architecture que l'Internet et utilise les mêmes infrastructures. De plus en plus d'entreprises sont équipées de réseaux LAN (Local Area Network) et peuvent donc tirer profit de la voix sur IP à moindre coût. En intégrant voix et données, la téléphonie IP simplifie l'administration du réseau car tout est centralisé dans un unique réseau. Elle procure aussi des facilités pour le développement d'applications utilisant de la voix et des données, en téléphonie tout est basé sur le matériel alors que la téléphonie IP tire avantage d'une architecture basée sur du logiciel.

Afin d'éviter toute confusion on utilise les termes suivants :

- **Voice over Internet Protocol (VoIP)** : est un nom définissant le transport de trafic vocal par paquets sur le protocole Internet IP.
- **Telephone over Internet Protocol (ToIP)** : est un service spécifique de VoIP.

## 2. Téléphonie conventionnelle et Téléphonie IP [2], [15]

Le RTC est tout simplement le réseau téléphonique que nous utilisons dans notre vie tous les jours et qui nous donne accès à de multiples fonctions. En effet outre le fait de pouvoir téléphoner, le RTC nous permet d'utiliser de multiples services tel que la transmission et réception de fax, l'utilisation d'un minitel, accéder à Internet etc.... Il représente donc l'un des protocoles de discussion utilisé sur la paire de cuivre boucle locale.

Le réseau téléphonique public (RTPC, Réseau Téléphonique Public Commuté ou simplement RTC) a essentiellement pour objet le transfert de la voix. Utilisant le principe de la commutation de circuits, il met en relation deux abonnés à travers une liaison dédiée pendant tout l'échange.

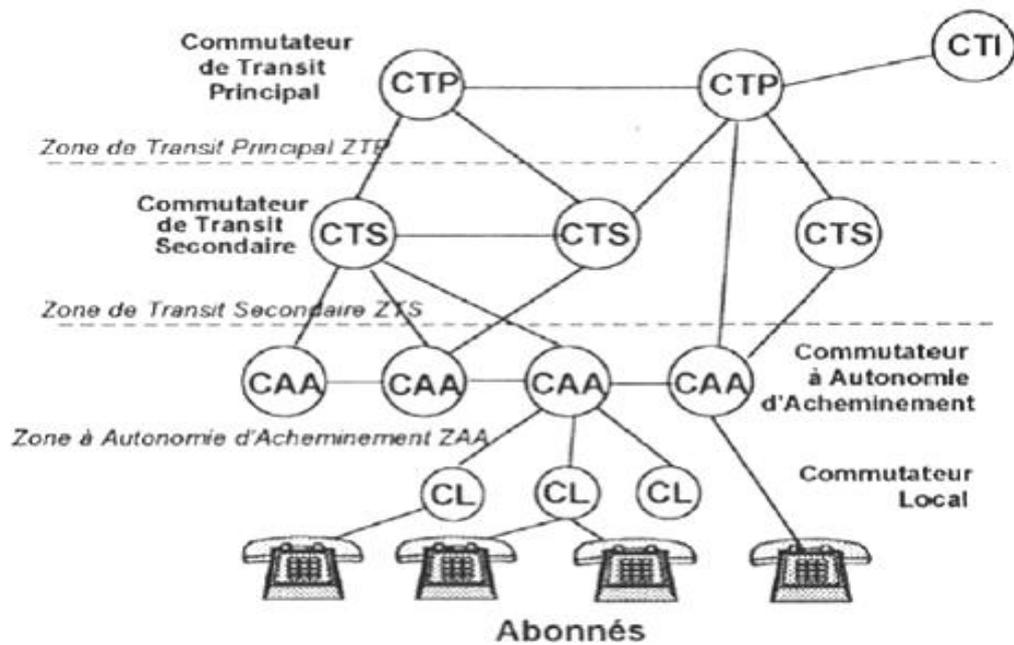


Figure 3.1 : Le réseau RTC

La téléphonie IP fait référence aux communications téléphoniques sur des réseaux TCP/IP. A la différence du réseau RTC qui fonctionne par transmission de signaux analogiques et numériques sur un réseau de commutation de circuits, la téléphonie IP fonctionne par commutation de paquets.

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.

Dans la téléphonie IP les paquets de données partagent un circuit avec d'autres transmissions.

### 3. Les différentes architectures d'un réseau VoIP [1], [16]

#### 3.1. Ordinateur à Ordinateur (PC to PC)

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.



Figure 3.2 : Architecture PC to PC

### 3.2. Ordinateur à Téléphone (Pc to Phone)

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 entre les deux réseaux pour rendre possible cette technique et faire la conversion entre réseaux.

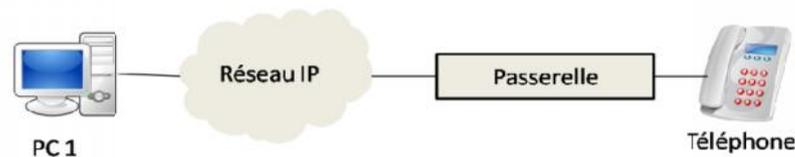


Figure 3.3 : Architecture PC to Phone

### 3.3. Téléphone à Téléphone (Phone to Phone)

Chacun des deux téléphones doit être raccordé à une passerelle pour leur permettre de communiquer sur un réseau IP.



Figure 3.4 : Architecture Phone to Phone

## 4. Les différents éléments pouvant composés un réseau VoIP [2], [16]

### 4.1. Le PABX-IP

C'est lui qui assure la commutation des appels et leurs autorisations, il peut servir aussi de routeur ou de Switch dans certains modèles, ainsi que de serveur DHCP. Il peut posséder des interfaces de type analogiques (fax), numériques (postes), numériques (RNIS) ou opérateurs (RTC- PSTN ou RNIS). Il peut se gérer par IP en Intranet ou par un logiciel serveur spécialisé que ce soit en interne ou depuis l'extérieur.

Il peut s'interconnecter avec d'autres PABX-IP ou PABX non IP de la même marque (réseau homogène) ou d'autres PABX d'autres marques (réseau hétérogène).

#### **4.2. Le serveur de communications**

Il gère les autorisations d'appels entre les terminaux IP ou soft phones et les différentes signalisations du réseau. Il peut posséder des interfaces réseaux opérateurs (RTC-PSTN ou RNIS), sinon les appels externes passeront par la passerelle dédiée à cela (Gateway).

#### **4.3. La passerelle (Gateway)**

C'est un élément de routage équipé de cartes d'interfaces analogiques et/ou numériques pour s'interconnecter avec soit d'autres PABX, soit des opérateurs de télécommunications local, national ou international. Plusieurs passerelles peuvent faire partie d'un seul et même réseau, ou l'on peut également avoir une passerelle par réseau local (LAN).

La passerelle peut également assurer l'interface de postes analogiques classiques qui pourront utiliser toutes les ressources du réseau téléphonique IP (appels internes et externes, entrants et sortants).

#### **4.4. Le routeur**

Il assure l'acheminement des paquets d'un réseau vers un autre réseau.

#### **4.5. Le switch**

Il assure la distribution et la commutation de dizaines de port Ethernet à 10/100 voire 1000 Mbits/s. Suivant les modèles, il peut intégrer la télé alimentation des ports Ethernet à la norme 802.3af pour l'alimentation des IP-phones ou des bornes WIFI en 48V.

#### **4.6. Le Gatekeeper**

Il effectue les translations d'adresses et gère la bande passante et les droits d'accès. C'est le point de passage obligé pour tous les équipements de sa zone d'action.

#### **4.7. Le MCU**

Le MCU (multi conferences unit) est un élément optionnel et gère les conférences audio vidéo.

#### **4.8. L'IP-Phone**

C'est un terminal téléphonique fonctionnant sur le réseau LAN IP Avec une norme soit propriétaire, soit SIP, soit H.323. Il peut y avoir plusieurs codecs pour l'audio, et il peut disposer d'un écran monochrome ou couleur, et d'une ou plusieurs touches soit programmables, soit préprogrammées.

Il est en général doté d'un hub passif à un seul port pour pouvoir alimenter le PC de l'utilisateur (l'IP PHONE se raccorde sur la seule prise Ethernet mural et le PC se raccorde derrière l'IP PHONE).

On peut utiliser un Soft-Phone qui est un logiciel qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. Il est géré soit par le Call Manager, soit par le PABX-IP.

Voici dans la figure suivante, le schéma général de l'utilisation de la VoIP.

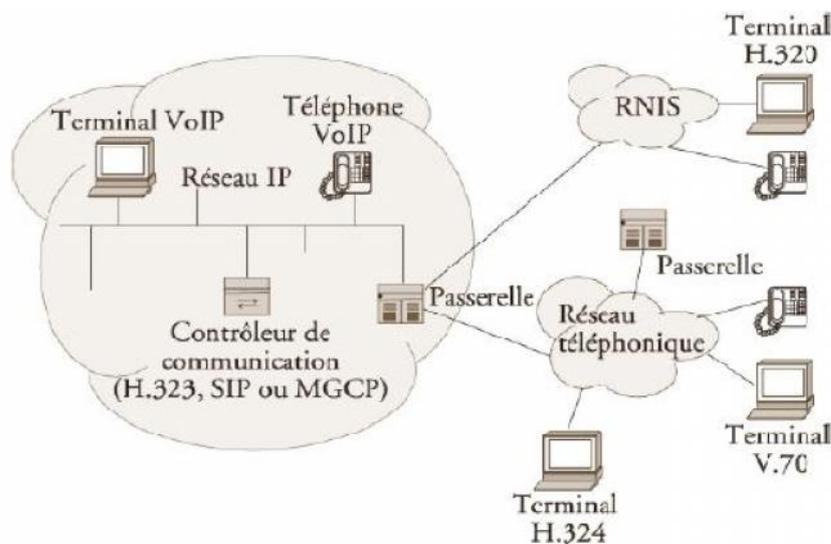


Figure 3.5 : Schéma général de l'utilisation de la VoIP

## 5. Fonctionnement de la téléphonie sur IP [16], [17]

### 5.1. Concept

De manière générale, le principe de la téléphonie sur réseau de données par paquets consiste à numériser la voix, à comprimer ensuite éventuellement le signal numérique correspondant, à découper le signal obtenu en paquets de données, enfin à transmettre ces paquets sur un réseau de données utilisant la même technologie.

A l'arrivée, les paquets transmis sont réassemblés, le signal de données ainsi obtenu est décomprimé puis converti en signal analogique pour restitution sonore à l'utilisateur.

Dans un système de téléphonie sur un réseau de données par paquets, deux cas peuvent être distingués :

- Le premier consiste à utiliser un réseau de paquets à liaison permanente de type X25, ce qui permet de garantir la transmission de bout en bout de l'intégralité des paquets.
- Le deuxième consiste à utiliser un réseau de type Internet, basé sur le protocole IP, dans lequel les paquets sont acheminés par les nœuds du réseau

qui comportent des routeurs.

Dans une communication téléphonique, le problème du transport de la voix est une chose, l'établissement ou la rupture de la communication est une autre chose. Il faut que l'utilisateur appelant puisse indiquer les coordonnées du correspondant, que ce dernier soit prévenu de l'appel, qu'il accepte l'appel, que les lignes des deux correspondants soient considérées comme occupées pendant toute la durée de la communication, enfin que les lignes des deux correspondants soient à nouveau réputées libres lorsque les correspondants mettent fin à la communication.

Toutes ces opérations sont rendues possibles par le biais des signaux de service que s'échangent les différents équipements traversés par la communication. C'est ce qu'on appelle la signalisation, qui est acheminée par le réseau en plus de la conversation.

Donc pour établir une communication il faut avoir en plus de transport un système de signalisation.

## 5.2. Principe de la transmission [1], [18], [19]

### 5.2.1. Codage de la voix

La voix produit lorsqu'on parle des fréquences à changements permanents. Grâce à ce changement de fréquence constant, nous pouvons laisser percevoir des émotions et des intonations. Cette multitude de fréquence provoquerait un affichage sinusoïdal.

La voix provoque donc un signal sinusoïdal, c'est-à-dire analogique. Pour le passer sur un réseau TCP/IP, il va falloir convertir ce signal analogique en un signal numérique.

Une fois convertie, il faut compresser la voix ainsi numérisée par le biais d'un codec (Compresseur/Décompresseur) pour l'insérer dans un paquet IP. Le codage doit offrir une qualité de voix la meilleure possible pour un débit et un délai de compression les plus faibles possibles.

Il existe plusieurs techniques de codage, voici dans le tableau suivant un classement des principaux codecs, effectué d'une façon subjective par une masse de population prise au hasard.

Nom du Codec	Débit du Codec	Note du Codec
G.711 (PCM)	~64Ko/s	4.1
G.723.1	~6.4Ko/s	3.9
G.726	~32Ko/s	3.85
G.729	~8Ko/s	3.92

**Tab 1:** Tableau de classification de codecs

Les trois opérations successives nécessaires à la numérisation de la parole sont, l'échantillonnage, la quantification et le codage.

- **L'échantillonnage** : cette opération consiste à prendre des points du signal analogique au fur et à mesure qu'il se déroule avec une certaine précision qui est caractérisée par le nombre de bits utilisés pour coder l'amplitude de chaque échantillon. Le choix de la fréquence et le nombre de bit utiliser répond à un compromis débit/qualité du signal codé.
- **La quantification** : consiste à attribuer à chaque échantillon une valeur numérique au moyen d'une loi de correspondance. Cette phase consiste à déterminer la loi de correspondance de telle sorte que la valeur des signaux aura plus de signification possible.

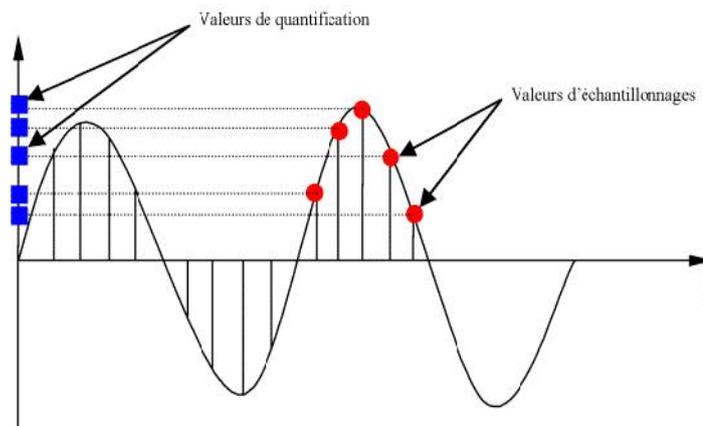


Figure 3.6 : Echantillonnage et quantification

- **Le codage** : traduit les nombres obtenus après quantification, en séquence de nombres binaires qui seront transmis au décodeur. A la fin on aura une diminution de débit binaire et une résistance plus forte aux erreurs de transmission.



Figure 3.7 : Envoi de données et codage

### 5.2.2. Les modes de diffusion dans la VoIP :

La VoIP est en général utilisée pour décrire des communications point à point. On parlera de streaming pour une diffusion de son ou de vidéos sur IP en simple

diffusion pour plusieurs utilisateurs (exemple: Web Radio). Le terme multipoints sera réservé à des visioconférences dont le nombre de participants est plus grand que deux.

La voix ou le son sur IP peut se faire en mode point à point, en mode une émission et plusieurs réceptions et en mode une émission pour plusieurs réceptions dont le signal n'est routé que s'il y a des récepteurs comme les radios Web.

## **6. Standards de la VoIP [4], [18], [20]**

### **6.1. Protocole H323**

H.323 est un protocole de communication englobant un ensemble de normes utilisées pour l'envoi de données audio et vidéo sur Internet. Il existe depuis 1996 et a été initié par l'ITU.

#### **6.1.1. Fonctionnement**

Le protocole H.323 est utilisé pour l'interactivité en temps réel, notamment la visioconférence (signalisation, enregistrement, contrôle d'admission, transport et encodage).

Il s'inspire du protocole H.320 qui proposait une solution pour la visioconférence sur un réseau RNIS, donc H.323 est une adaptation de H.320 pour les réseaux IP.

#### **6.1.2. Eléments de réseaux H.323**

- **Les terminaux H.323:**

Un poste téléphonique IP raccordés directement au réseau Ethernet de l'entreprise ou un PC sur lequel est installé une application compatible H.323.

- **Les passerelles (Gateway):**

Elles assurent l'interconnexion entre un réseau IP et le réseau téléphonique. Elles assurent la correspondance de la signalisation et des signaux de contrôle et la cohésion entre les médias. Pour ce faire, elles implémentent les fonctions suivantes de transcodage audio, de modulation, démodulation, de suppression d'échos, de suppression des silences et de contrôle d'appels.

Les passerelles sont le plus souvent basées sur des serveurs informatiques standards (Windows NT, Linux) équipés d'interfaces particulières pour la téléphonie et d'interfaces réseau.

- **Les portiers (Gatekeeper):**

Ils ont pour rôle de réaliser la traduction numéro de téléphone vers adresse IP et la gestion des autorisations, de limiter la bande passante si besoin et de gérer le trafic sur le LAN. Les gardes-barrière permettent également de gérer les téléphones classiques et la signalisation permettant de router les appels afin

d'offrir des services supplémentaires. Ils peuvent enfin offrir des services d'annuaires.

- **Les unités de contrôle multipoint (MCU) :**

Référence au protocole T.120 qui permet aux clients de se connecter aux sessions de conférence de données. Les unités de contrôle multipoint peuvent communiquer entre elles pour échanger des informations de conférence.

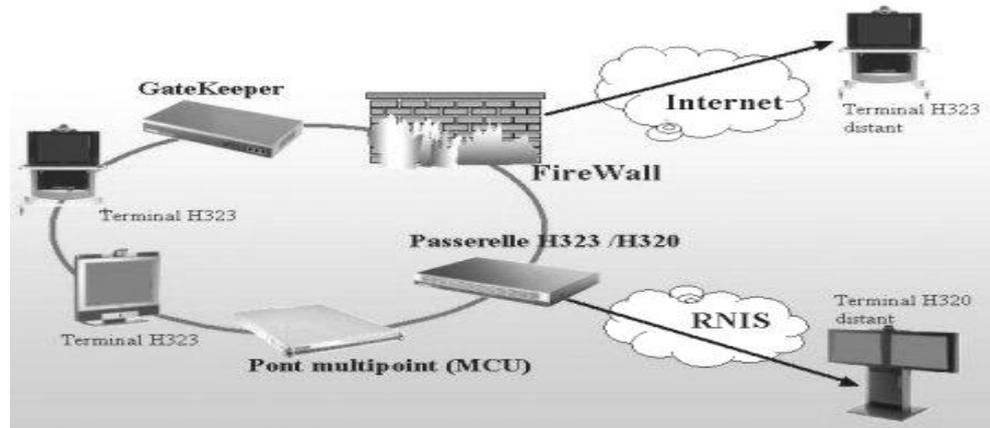


Figure 3.8 : Eléments d'une architecture H.323

### 6.1.3. La signalisation

#### 6.1.3.1. Objectifs de la signalisation

La signalisation a pour objectif de réaliser les fonctions suivantes :

- **Recherche et traduction d'adresses :**

Sur la base du numéro de téléphone du destinataire, il s'agit de trouver son adresse IP ou l'adresse IP de la passerelle desservant le destinataire. Cette fonction est prise en charge par le Gatekeeper. Elle est effectuée soit localement soit par requête vers un annuaire centralisé.

- **Contrôle d'appel :**

L'équipement terminal (ou une passerelle) situé à l'origine de l'appel établit une connexion avec l'équipement de destination et échange avec lui les informations nécessaires à l'établissement de l'appel. Dans le cas d'une passerelle, cette fonction implique également de supporter la signalisation propre à l'équipement téléphonique à laquelle elle est raccordée et de traduire cette signalisation dans le format défini dans H.323. Le contrôle d'appel est pris en charge soit par les équipements terminaux soit par le Gatekeeper. Dans ce cas, tous les messages de signalisation sont routés via le Gatekeeper.

#### 6.1.3.1.2. Les protocoles de signalisation dans le cadre de H.323

Trois protocoles de signalisation sont spécifiés dans le cadre de H.323 à savoir :

- **RAS (Registration, Admission and Status)**

Ce protocole est utilisé pour communiquer avec un Gatekeeper. Il sert notamment aux équipements terminaux pour découvrir l'existence d'un Gatekeeper et s'enregistrer auprès de ce dernier ainsi que pour les demandes de traduction d'adresses. La signalisation RAS utilise des messages H.225.0 6 transmis sur un protocole de transport non fiable comme UDP.

- **Q.931**

H.323 utilise Q.931 (version simplifiée de signalisation RNIS) pour l'établissement et le contrôle d'appels téléphoniques sur IP.

- **H.245**

Ce protocole est utilisé pour l'échange de capacités entre deux équipements terminaux. Par exemple le type de codec à activer. Il peut également servir à mesurer le RTD (Round Trip Delay) d'une communication.

#### 6.1.4. Déroulement d'une communication H.323

Une communication H.323 se déroule en cinq phases :

1. Établissement d'appel
2. Échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource ReserVation Protocol)
3. Établissement de la communication audio-visuelle
4. Invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.)
5. Libération de l'appel.

Dans l'image suivante, un exemple d'initiation d'une communication avec H.323.

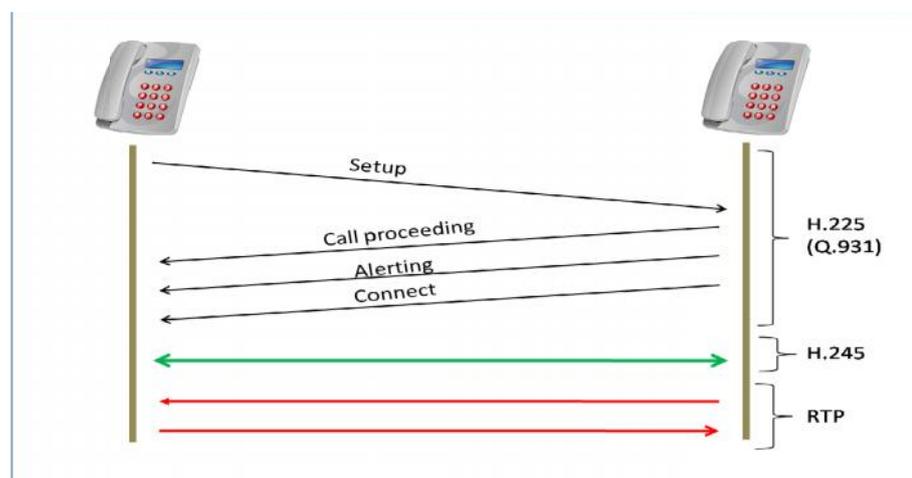


Figure 3.9 : Déroulement d'une communication H.323

### 6.1.5. Empilement de H.323

La pile protocolaire de H.323 est représentés dans le schéma suivant:

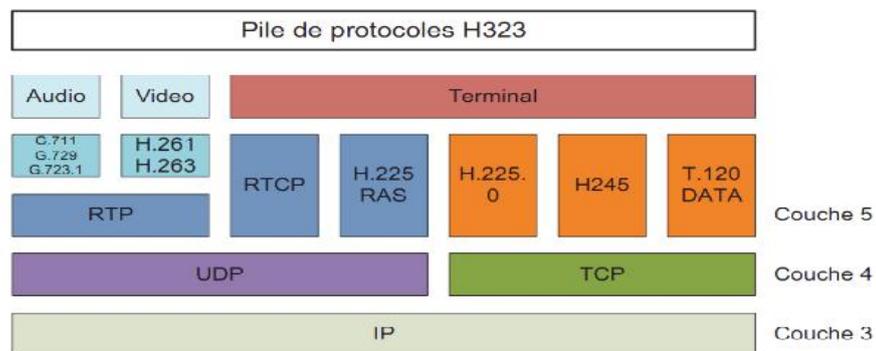


Figure 3.10 : Pile de protocole H323

### 6.1.6. Avantages et inconvénients

Les débits des réseaux IP doivent être adaptés en fonction du trafic afin d'éviter tout risque de coupure du son et de la vidéo. Plus le débit sera élevé et plus le risque de coupure sera faible.

Par ailleurs, tant que la QoS n'existera pas dans les réseaux IP, la fiabilité d'une application VoIP sur des réseaux à faible débit sera faible.

Voici les principaux bénéfices qu'apporte la norme H.323:

- **Codec standards** : H.323 établit des standards pour la compression et la décompression des flux audio et vidéo.
- **Interopérabilité** : pouvoir de dialoguer sans avoir à se soucier de la compatibilité du terminal destinataire.
- **Indépendance vis à vis du réseau** : H.323 est conçu pour fonctionner sur tout type d'architecture réseau.
- **Indépendance vis à vis des plates formes et des applications** : H.323 n'est lié à aucun équipement ou système d'exploitation.
- **Support multipoint** : H.323 supporte des conférences entre trois points terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée.
- **Gestion de la bande passante** : afin d'éviter des flux qui alourdissent le réseau, H.323 permet une gestion de la bande passante à disposition.
- **Support multicast** : H.323 supporte le multicast dans les conférences multipoint.

H.323 présente toutefois les inconvénients suivants :

- **Protocole complexe** : créé initialement pour les conférences multimédia et qui

incorpore des mécanismes superflus dans un contexte purement téléphonique.

- **Nombreuses options susceptibles d'être implémentées** : par différents constructeurs et donc de poser des problèmes d'interopérabilité.

### 6.1.7. Conclusion sur H.323

Le protocole H.323 est une des normes envisageables pour la VoIP. Cependant, elle est pour l'instant surtout employé par des programmes propriétaires. La documentation est difficile d'accès en dehors des efforts faits par le projet Open H.323 pour rendre cette technologie accessible à tous.

## 6.2. Le protocole SIP [21], [22]

### 6.2.1. Définition de SIP

Le protocole SIP est un protocole de signalisation largement utilisé, essentiellement pour des applications de type téléphonie sur IP. Il fournit les mécanismes nécessaires à l'ouverture et à la fermeture d'une session.

### 6.2.3. Principe

SIP est un protocole de signalisation conçu pour établir et contrôler des sessions multimédia. Pour cela, SIP associe une session avec des supports de type audio, vidéo et données.

Ce protocole peut fonctionner au dessus de TCP ou d'UDP. Afin de palier aux pertes éventuelles de messages possibles si UDP est utilisé, SIP doit donc avoir ses propres mécanismes de retransmissions.

Ses caractéristiques principales qui le rendent si pratique sont:

- SIP utilise le système d'adressage URL. L'adressage peut être un nombre de téléphone, une adresse IP ou une adresse email. Les messages sont très semblables à ceux employés par l'Internet HTTP1.1, constituée d'un utilisateur et d'un domaine séparés par un @ :  
user@domaine | user@machine | user@ip\_adresse Numéro | telephone@passerelle
- Le protocole SIP peut avoir des sessions multiples de média pendant un appel. Le protocole SIP étant indépendant de la transmission des données, tout type de données et de protocoles peut être utilisé pour cet échange.
- SIP est un protocole léger qui nécessite peu de ressource physique et peu de temps de développement.

### 6.2.4. Eléments d'une architecture SIP

SIP définit deux types d'entités: les clients et les serveurs. Plus précisément les entités définies par SIP sont :

- **Le serveur proxy (Proxy server) :** Il reçoit des requêtes de clients qu'il traite lui même ou qu'il achemine à d'autres serveurs après avoir éventuellement réalisé certaines modifications sur ces requêtes.
- **Le serveur de redirection (Redirect server) :** Il s'agit d'un serveur qui accepte des requêtes SIP, traduit l'adresse de destination en une ou plusieurs adresses réseau et les retourne au client. Contrairement au Proxy server, le Redirect server n'achemine pas de requêtes SIP. Dans le cas d'un renvoi d'appel, le Proxy server a la capacité de traduire le numéro de l'appelé dans le message SIP reçu, en un numéro de renvoi d'appel et d'acheminer l'appel à cette nouvelle destination, et ce, de façon transparente pour le client origine ; pour le même service, le Redirect server retourne le nouveau numéro (numéro de renvoi) au client origine qui se charge d'établir un appel vers cette nouvelle destination.
- **L'agent utilisateur (UA) :** Il s'agit d'une application sur un équipement de l'utilisateur qui émet et reçoit des requêtes SIP. Il se matérialise par un logiciel installé sur un PC, sur un téléphone IP.
- **L'enregistreur (Registrar) :** Il s'agit d'un serveur qui accepte les requêtes SIP de type REGISTER. L'utilisateur indique par un message REGISTER émis au Registrar, l'adresse où il est joignable (exemple : adresse IP).

Le Registrar met alors à jour une base de données de localisation. L'enregistrement est une fonction associée à un Proxy Server ou à un Redirect Server. Un utilisateur peut s'enregistrer sur différents UAs SIP, dans ce cas, l'appel lui sera délivré sur l'ensemble de ces UAs.

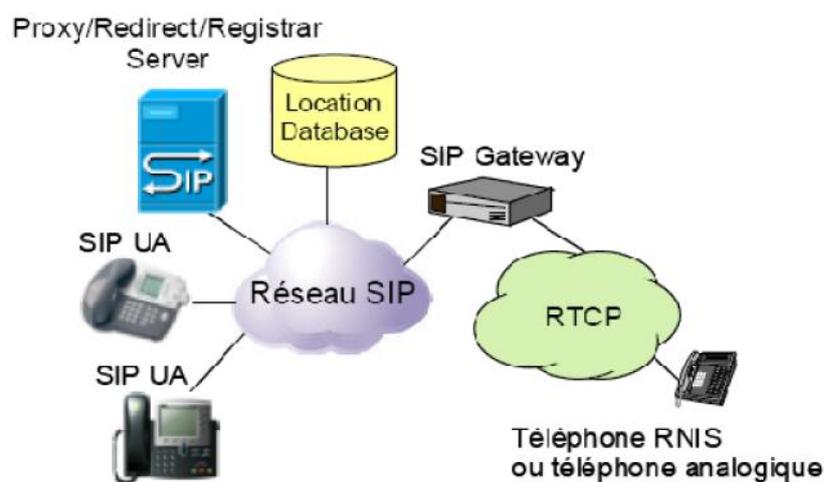


Figure 3.11 : Eléments d'un réseau SIP

### 6.2.5. Les messages SIP

Les messages du protocole SIP sont codés en utilisant la syntaxe de message semblable au protocole HTTP.

Un message SIP est composé de deux rubriques principales qui sont la méthode et l'entête. La ligne vide représente la possibilité d'utiliser d'autres protocoles multimédia tel que SDP.



Figure 3.12: Syntaxe de base d'un message SIP

#### 6.2.5.1. L'entête

Voici un exemple d'entête SIP avec la méthode INVITE :

```
INVITE sip:personnel@domaine.fr SIP/2.0
Via: SIP/2.0/UDP pc5.domaine.fr ;branch=z9h4K76shds
Max-Forwards: 70
To: personne2 <sip:personne2@domaine.fr>
From: Pascal <sip:personnel@domaine.fr>;tag=1928301774
Call-ID: a844c7670@pc5.domaine.fr
CSeq: 314159 INVITE
Contact: <sip:personnel@pc5.domaine.fr>
Content-Type: application/sdp
Content-Length: 142
```

Figure 3.13 : Exemple d'entête SIP

La première ligne contient le type de message.

- **Via** : ce champ représente le chemin parcouru par la requête, lors de l'envoi de la requête il contient initialement l'URI de l'émetteur de cette requête. Ensuite, à chaque fois qu'un UA fait suivre la requête celui-ci rajoute sa propre URI dans ce champ.
- **Max-Forwards** : nombre maximum de sauts.
- **To** : URI du destinataire du message.

- **From** : URI de l'expéditeur du message.
- **Call-ID** : identifiant unique représentant la session SIP.
- **Cseq** : contient un entier et un nom de méthode, l'entier est généré d'une façon aléatoire une première fois puis est ensuite incrémenté à chaque message.
- **Contact** : contient une ou plusieurs URI représentant une route directe pour contacter l'UA de l'expéditeur.
- **Content-Type** : description du corps du message
- **Content-Length** : taille en octet du corps du message
- **Branchtag** : utilisés pour des raisons d'identification

#### 6.2.5.2. Les méthodes

- **Les principales requêtes**

Le client envoie des requêtes au serveur. Les méthodes de base sont :

- **INVITE** : permet à un client de demander une nouvelle session
- **ACK** : confirme l'établissement de la session
- **CANCEL** : annule un INVITE en suspens
- **BYE** : termine une session en cours
- **OPTIONS** : pour récupérer les capacités de gestion des usagers, sans ouvrir de session
- **REGISTER** : enregistrement auprès d'un serveur d'enregistrement.

- **Les principales réponses :**

Les codes de réponse sont similaires à HTTP.

- **100 Trying**
- **200 OK**
- **404 Not Found**

Les codes supérieurs ou égaux à x80 sont spécifiques à SIP.

- **180 Ringing**
- **486 Busy**

SIP diffère de HTTP du fait qu'un agent SIP (UA) joue habituellement à la fois les rôles de client et de serveur. C'est-à-dire qu'il peut aussi bien envoyer des requêtes, que répondre à celles qu'il reçoit.

6.2.6. Le fonctionnement

6.2.6.1. Enregistrement d'un UA

Dans la figure suivante une représentation de l'enregistrement d'un UA à son Registrar. Les flèches de l'AE vers le REGISTRAR représentant les requêtes et de droite à gauche représentant les réponses.

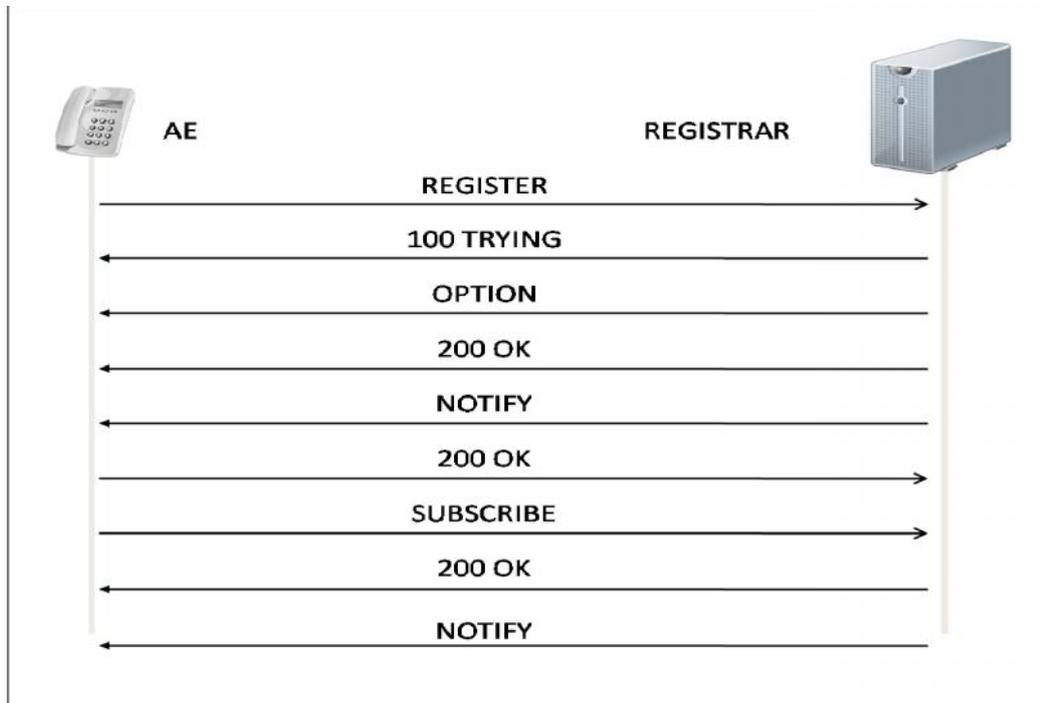


Figure 3.14 : Enregistrement d'un UA auprès de son Registrar

6.2.6.2. Etablissement d'une connexion

Ce mécanisme d'établissement d'une connexion entre deux UAs depuis l'invitation jusqu'à la clôture de la session, peut être décrit en 8 étapes :

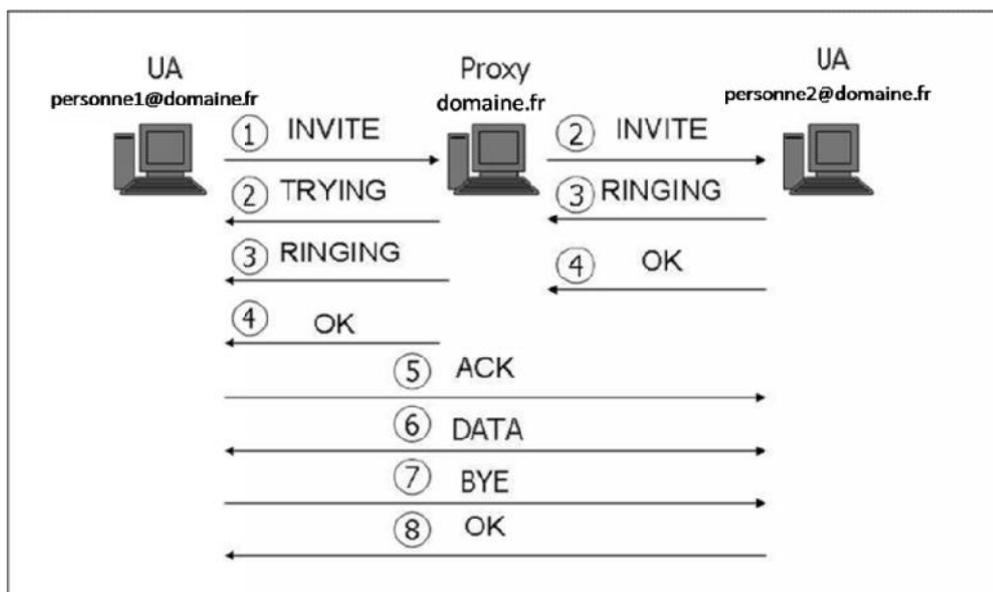


Figure 3.15: Initialisation et fermeture d'une session SIP

1. L'UA identifié par l'URI sip:personnel@domaine.fr souhaite contacter l'UA d'URI sip:personne2@domaine.fr. Pour cela il envoie une requête de type INVITE à destination de cette URI.
2. Le proxy du domaine domaine.fr fait suivre la requête INVITE et le signale à l'UA de l'appelant en lui retournant le code d'état 100 TRYING.
3. L'UA de l'appelé a reçu le message mais la communication n'est pas encore acceptée en effet, dans une application téléphonique on se retrouve dans la situation où le téléphone sonne et où l'on attend que la personne décroche. L'UA de l'appelé signale cela en renvoyant le code d'état 180 RINGING au proxy qui va l'envoyer à l'UA de l'appelant.
4. L'UA de l'appelé accepte la communication et retourne le code d'état 200 OK au proxy qui le relaye à l'UA de l'appelant.
5. L'UA de l'appelant envoie un message d'acquiescement. A partir de ce moment, la connexion entre les deux UA est initialisée et plus aucun message ne passe par le proxy.
6. Les deux UA à présent peuvent s'envoyer des données via la connexion qui a été décrite dans le message INVITE (UDP ou TCP). Cette connexion utilisée pour l'échange de données est totalement indépendante de la connexion utilisée pour la signalisation SIP.
7. Si, un UA souhaite fermer la connexion, il envoie un message BYE.
8. Le message BYE est acquitté via un code d'état 200 OK. La connexion entre les deux UA est close.

#### **6.2.6.3. Modes de communication**

- **Mode direct**

Les entités utilisatrices communiquent directement. SIP est un protocole de signalisation de bout en bout. Dans ce cas les serveurs ne sont pas nécessaires si les entités utilisatrices connaissent leurs adresses IP.

- **Mode indirect**

Les entités réseaux relaient les messages échangés, il est utilisé quand l'appelant ne connaît pas l'adresse IP de l'appelé.

#### **6.2.7. Conclusion sur SIP**

La simplicité, la rapidité et la légèreté d'utilisation, tout en étant très complet, sont autant d'arguments qui pourraient permettre à SIP de convaincre les investisseurs. De plus, ses avancées en matière de sécurité des messages sont un atout important par rapport à ses concurrents.

**6.3. Les protocoles de transport** [4], [23]

Les protocoles de transport utilisés dans la VoIP sont: TCP, UDP, RTP, RTCP.

**6.3.1. Le protocole TCP**

Le protocole TCP (Transmission Control Protocol) permet, au niveau des applications, de gérer les données en provenance de la couche inférieure du modèle (protocole IP).

Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP. Le protocole TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission. Le protocole TCP permet principalement de:

- Remettre en ordre les datagrammes en provenance du protocole IP.
- Vérifier le flux de données afin d'éviter une saturation du réseau.
- Formater les données en segments de longueur variable afin de les remettre au protocole IP.
- Permet aussi de multiplexer les données.

**6.3.2. Le protocole UDP**

Contrairement aux données où seul le débit global compte, il faut garantir pour la voix un flux le plus régulier possible. Pour ne pas ralentir le trafic, il faudrait utiliser des protocoles de transport simplifié, quitte à ne pas prendre en compte la gestion des erreurs, mais la qualité perçue est très dépendante des fluctuations de délais dues aux congestions dans le réseau.

Ainsi le protocole UDP basé sur la même couche que TCP. Cependant, il présente des performances moyennes par rapport à TCP, car il permet l'envoi de paquets sans contrôle de réception.

**6.3.3. Le protocole RTP**

C'est le protocole qui a été développé par l'IETF, afin de faciliter le transport réel, de bout en bout, des flots de données audio et vidéo sur les réseaux IP. Le protocole RTP n'est pas un protocole réel de transfert, puisque son utilisation se fait généralement sur UDP ce qui permet d'atteindre plus facilement le temps réel.

Les applications temps réel constitue un véritable problème pour le réseau Internet. Plus généralement RTP permet:

- D'identifier le type d'information transporté.
- D'ajouter des marqueurs temporels et des numéros de séquence à l'information transportée.
- De contrôler l'arrivée à destination de paquets.

#### **6.3.4. Le protocole RTCP**

Le protocole RTCP est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. L'objectif de RTCP est de fournir différents types d'informations et un retour quant à la qualité de réception. Le protocole RTCP est un protocole de contrôle associé à RTP, il mesure les performances, il n'offre pas de garantie par contre. Pour cela, il faut, employer un protocole de réservation de type RSVP ou bien s'assurer que les liens de communication utilisés sont correctement dimensionnés par rapport à l'utilisation qui en est fait. Trois principales fonctions de RTCP:

- Fournir des informations sur la qualité de session.
- Contrôler le débit auquel les participants à une session RTP transmettent leurs paquets RTCP.
- Transmettre des informations de contrôle de session.

#### **6.4. Les protocoles secondaires**

Les protocoles secondaires utilisés pour le fonctionnement de la VoIP sont :

- **DHCP** : pour les attributions d'adresses IP, de DNS...
- **TFTP** : pour la configuration et la mise à jour .
- **DNS** : pour les services d'annuaire et de localisation ;
- **HTTP** : pour l'administration.
- **ENUM** : concernant SIP, pour la correspondance des adresses SIP et numéros E.164 (RTC) en utilisant DNS.

### **7. Qualité de service (QoS) [24]**

#### **7.1. Gestion de la qualité de service**

Il y a quelques années chaque type de trafic, voix, données, etc., avait son propre réseau, dédié et taillé sur mesure. Aujourd'hui les différents flux sont regroupés sur un seul et même support que constituent les réseaux IP. Les débits ne cessent donc de grimper et les réseaux sont désormais multiservices.

Cette centralisation simplifie grandement les tâches des administrateurs et

utilisateurs car il n'y a plus qu'une seule infrastructure à gérer.

Cependant, sans régulation du trafic, les réseaux IP se retrouvent vite saturés. La multiplication des flux provoque l'engorgement des liaisons. Afin de pouvoir assurer un niveau de service satisfaisant pour les utilisateurs et améliorer les performances d'un réseau, il convient d'envisager la notion de qualité de service (QoS).

## **7.2. Problèmes liés à la qualité de service :**

### **7.2.1. Gestion de la bande passante :**

Sur le réseau WAN, la ressource en bande passante est bien plus contrainte que sur le LAN. Une application gourmande en bande passante, telle qu'une application de messagerie ou de transfert de fichiers, peut donc rapidement compromettre la qualité de service (QoS) des applications critiques, comme les progiciels de gestion intégrés ou les bases de données.

### **7.2.2. Réduction de la latence**

La latence est le temps mis par un paquet pour parcourir le trajet source – destination. La latence peut être réduite en donnant aux paquets appartenant aux clients les plus importants la priorité dans les files d'attente des routeurs.

Cependant ce procédé oblige les paquets avec une priorité moindre à une attente un peu plus longue, et de ce fait leur latence est plus grande

Les applications interactives sont sensibles à la latence du réseau, car une latence trop grande génère un retard de livraison des paquets.

### **7.2.3. Réduction de la Gigue**

La Gigue (ou Jitter) est définie de la façon suivante:

$$\text{Gigue} = \text{Latence (Pi)} - \text{Latence (Pi-1)}$$

Où Latence (Pi) est la latence du paquet numéro i, à son arrivée au destinataire. En d'autres termes la gigue est la variation de latence constatée par le récepteur des paquets.

Pour beaucoup d'applications une gigue élevée est encore pire qu'une latence même très forte, car cela introduit un facteur d'incertitude dans le flux de données.

#### **7.2.4. Réduction du nombre de paquets perdus**

La perte de paquets force beaucoup d'applications et de protocoles à renvoyer des paquets qui ont été déjà envoyés. Ceci retarde bien sur les transmissions, d'autant plus qu'un certain temps est nécessaire avant que la perte de paquets ne soit décelée.

Ainsi la perte de paquets est quelque chose dont personne ne veut mais qui est une réalité due aux tailles limitées des buffers sur le réseau. Pendant les pics de transmission, certains nœuds sont obligés de rejeter des paquets si leurs buffers sont pleins.

Une méthode pour éviter la perte de paquets serait de s'assurer qu'un nœud du réseau a la capacité d'envoyer des données plus rapidement qu'il ne les reçoit.

#### **7.2.5. Applications agressives**

En effet, quel que soit le réseau considéré, il existera toujours des applications au comportement plus agressif, à savoir occupant une grande partie de la bande passante, voire la totalité, en fonction de leurs besoins. Généralement, même si elles sont importantes, ces applications ne sont pas urgentes (par exemple la réplication de base de données et la messagerie). La majorité des applications des réseaux IP d'entreprise utilisent le protocole TCP (Transport Control Protocol) conçu pour octroyer un accès équitable à la bande passante du réseau.

### **7.3. Politique de mise en place d'une qualité de service**

De la préparation au déploiement, on distingue trois étapes:

- **Caractériser le trafic** Pour que l'administrateur ait une vue des flux circulant sur son réseau, un audit est indispensable. Il peut être réalisé sur la totalité ou sur un sous-ensemble représentatif des liaisons du réseau.

- **Classifier les flux** Selon les impératifs de l'entreprise, le responsable réseau définira une classification des divers flux et leur attribuera des niveaux de priorité. Cette phase doit impérativement être menée en concertation avec les différents utilisateurs du système d'information.
- **Définir les règles de traitement des flux** : Selon la classification auparavant établie, le responsable réseau doit définir les règles de traitement des flux selon leur classe. Il s'agit, par exemple, de déterminer les priorités de routage ou des niveaux de bande passante minimale pour certaines applications.

## **8. Discussion**

Dès à présent, il est possible de prévoir qu'un développement substantiel devrait se faire dans le domaine des télécommunications d'entreprises car c'est là que la notion d'intégration complète voix-données pourra prendre toute sa dimension économique.

Le développement de la téléphonie entre passerelles, de poste ordinaire à poste ordinaire, est quant à lui vraisemblablement voué, dans un premier temps, à un écrémage du trafic sur des zones géographiques où une telle implantation s'avérerait rapidement rentable. Le déploiement ira ensuite sans doute plus loin, ne serait-ce que lorsque les opérateurs traditionnels eux-mêmes adopteront la norme IP pour l'ensemble de leurs transmissions d'informations.

Sur le plan commercial, au-delà de la dimension concurrentielle déjà présente avec la fin des monopoles de télécommunications, la voix sur IP introduit une nouvelle dimension : celle du choix du rapport qualité / prix par l'utilisateur lui-même. Là aussi, voilà un nouveau défi pour les opérateurs de télécommunications, qu'ils soient traditionnels ou nouveaux venus, car jusqu'à présent le niveau de qualité de service a toujours été défini par l'opérateur lui-même sans discussion avec l'utilisateur.

Sur le plan industriel, l'avenir sera aux entreprises qui auront anticipé suffisamment la généralisation de la norme IP et de ses évolutions, ce qui conduit à l'évidence à inciter vivement l'industrie dans ce sens.



## CHAPITRE IV

---

### *Mise en place d'une solution VoIP*

## 1. Préambule

A l'heure des télécommunications ouvertes a différents opérateurs, ou l'on se voit noyés sous les offres ou l'appel devient gratuit, comprenons comment est-il possible de traiter des appels sans moyens immenses et installons un serveur de téléphonie pour un usage local et le plus répandu reste Asterisk. Le but n'est pas de faire un opérateur téléphonique, mais simplement pour comprendre ou tenter le challenge et pourquoi installer un système de téléphonie au sein d'une entreprise petite ou moyenne.

## 2. Le standard téléphonique traditionnel – PABX

Un PABX est un interface privée entre le réseau téléphonique et les utilisateurs de celui-ci. Sa fonction essentielle consiste à mettre, temporairement deux usagers en relation. Cette relation peut être locale ou établie à travers le réseau téléphonique public ou privé.

### 2.1. Les fonctionnalités

On considère les PABX comme offrant quatre types de fonction :

- **Les fonctions de raccordements** : On distingue les différents raccordements suivants :
  - Raccordement de ligne d'abonné analogique.
  - Raccordement de ligne d'abonné numérique.
  - Raccordement de circuits analogiques individuels.
  - Raccordement de circuits multiplexés numériques.
  - Raccordement sans fil (CT2, DECT,...).
- **Les fonctions de commutation** : Qui consistent à diriger en transparence les signaux acheminés par le système en fonction des demandes d'utilisateurs : demandeur et demandé.
- **Les fonctions de signalisation et d'adressage** : Qui consistent à élaborer et à échanger les informations nécessaires à l'invocation et à la fourniture des services, entre le système et les utilisateurs, les réseaux extérieurs et entre les nœuds du système lui-même.
- **Les fonctions de commande** : Qui incluent d'une part la commande des fonctions de commutation à partir de traitement des signalisations échangés et, d'autre part, les opérations de gestion, d'administration, de maintenance et d'exploitation.

### 3. Le standard téléphonique IP – PBX-IP

IPBX signifie Internet Protocol Branch eXchange (autocommutateur téléphonique privé par Internet).

L'IPBX est directement conçu pour véhiculer de la voix sur IP. Ses fonctionnalités sont généralement les mêmes que pour un standard téléphonique PABX. Seul le réseau utilisé pour acheminer les données est différent : réseau téléphonique traditionnel pour le PABX et Internet pour l'IPBX.

Les tarifs des opérateurs de VoIP sont avantageux (certaines destinations en illimité) et souvent moins chers que les opérateurs classiques. Cependant, ils sont tout de même payants et même des appels locaux peuvent l'être.

L'avantage principal du standard téléphonique IPBX est la réduction des coûts due à l'utilisation de la téléphonie sur IP :

- Le standard téléphonique IPBX est généralement moins cher à l'utilisation (appels téléphoniques) qu'un standard PABX.
- L'IPBX permet une réduction des coûts d'exploitation (maintenance et communications) de 25 à 50 %.

#### 3.1. Fonctionnalités IPBX

Voici un tableau vous présentant les principales fonctionnalités pour un standard téléphonique IPBX :

Fonctionnalités		Description
Messagerie	Vocale	<ul style="list-style-type: none"> <li>• Chaque poste téléphonique a sa propre messagerie vocale et a la possibilité de stocker les messages vocaux.</li> <li>• La boîte vocale est consultable en externe (à l'aide de la SDA*).</li> </ul>
	Unifiée	<ul style="list-style-type: none"> <li>• Elle joue le même rôle que la messagerie vocale, mais avec des mails.</li> <li>• Vos messages vocaux ou fax atterrissent directement dans</li> </ul>

		<p>vosre boîte mail de réception ou téléphone portable.</p>
<b>Numérotation</b>	Numérotation abrégée collective	<ul style="list-style-type: none"> <li>• Possibilité d'appeler en externe (fixe ou mobile) en tapant un préfixe spécifique sur tous les postes raccordés au standard téléphonique. Exemple : le 588 pour contacter la société de maintenance.</li> </ul>
	Numérotation abrégée individuelle	<ul style="list-style-type: none"> <li>• Possibilité d'appeler en externe (fixe ou mobile) à l'aide d'un préfixe spécifique par poste. Il s'agit généralement d'une manipulation de l'utilisateur.</li> </ul>
	Plan de numérotation	<ul style="list-style-type: none"> <li>• Préfixes à taper pour différentes fonctionnalités voulues avant un appel.</li> <li>• Exemple : <ul style="list-style-type: none"> <li>– Le 5, afin de consulter sa messagerie vocale.</li> <li>– Le 0, pour les appels vers l'extérieur.</li> <li>– Entre le 500 et 999 si vous souhaitez appeler un poste précis dans l'entreprise.</li> </ul> </li> </ul>
	Plan de suffixe	<ul style="list-style-type: none"> <li>• Préfixes que vous composez pour obtenir différentes fonctionnalités voulues pendant un appel.</li> <li>• Exemple : <ul style="list-style-type: none"> <li>◦ Le 3, une conférence à 3.</li> </ul> </li> </ul>
<b>Identification de l'appelant (ANI)</b>		<ul style="list-style-type: none"> <li>• Sur votre ordinateur, <b>les données de la personne appelant apparaissent juste avant son appel</b> grâce à une base de données.</li> </ul>
<b>Sélection Directe à l'Arrivée (SDA)</b>		<ul style="list-style-type: none"> <li>• Un appel peut être orienté vers un poste interne sans avoir besoin de passer par l'accueil téléphonique de l'entreprise.</li> <li>• Exemple : composer le 588 pour le poste 01.02.03.04.05.</li> </ul>

<b>Attente téléphonique</b>	<ul style="list-style-type: none"> <li>• La personne qui appelle est mise en attente de façon automatique (messages d'accueil) avant d'entrer en contact avec son correspondant.</li> </ul>
<b>Least Cost Routine (LCR)</b>	<ul style="list-style-type: none"> <li>• <b>Vous gérez dynamiquement différents opérateurs</b> : suivant la destination et l'heure, l'IPBX utilise les liaisons qui coûtent le moins cher.</li> </ul>
<b>Serveur vocal interactif</b>	<ul style="list-style-type: none"> <li>• La personne qui appelle est dirigée vers une sorte de standard automatique qui lui demande de composer un chiffre ou de parler pour identifier le poste vers lequel il veut être redirigé.</li> </ul>
<b>Taxation (accès aux statistiques)</b>	<ul style="list-style-type: none"> <li>• Analyse de différentes données : <ul style="list-style-type: none"> <li>– Trafic appel entrant/sortant.</li> <li>– Facturation par poste.</li> </ul> </li> </ul>

### 3.2. Les avantages

Nous listons ici les principaux avantages de la VOIP pour permettre à chacun d'y voir les applications potentielles:

- **Gains importants au niveau du câblage** : Capacité à utiliser un seul port pour le téléphone et le PC qui génère :
  - Un besoin réduit de l'espace de brassage.
  - La réduction des taches de brassage.
- **Gains d'administration et d'interlocuteur gestionnaire** : On ne gère plus qu'un réseau unique : le réseau IP, plus de réseau spécifique à la téléphonie.
- **Mobilité des postes/utilisateurs** : Le poste téléphonique n'est plus attaché à une prise.
- **Economies télécoms** : Lorsque la solution est multi site, l'utilisation des liens DATA existant comme transport de la voix inter site constitue de très

importantes économies sans avoir à avoir des liens spécifiques pour la téléphonie.

- **Pérennité** : Les postes IP répondent à une norme H323 ou SIP et sont donc réutilisables avec d'autres IPBX indépendant du constructeur pour les fonctions standards.

#### 4. Installation de la solution VoIP

Notre projet consiste à la réalisation d'une solution assurant la transmission de la voix sur le protocole IP. Il est composé de deux phases : Une phase d'identification des besoins techniques, des services, des protocoles et des outils nécessaires pour l'implémentation d'une solution VOIP. Ensuite, une phase d'installation, de configuration et d'administration d'une plateforme, des serveurs et des clients d'une manière cohérente et adaptée à la solution proposée.

##### 4.1. Identification des besoins

Dans cette partie on va étudier les fonctionnalités offertes par un IPBX. Il s'agit uniquement de traiter les possibilités d'un serveur VoIP dans le cadre d'un réseau local. Donc toute la partie concernant la connexion de l'IPBX avec le réseau téléphonique classique est peu abordée. Nous avons à notre disposition des ordinateurs, un jouera le rôle du PBX et les autres les clients.

Le protocole de VoIP utilisé sera SIP, car il a l'avantage d'être celui qui est le plus utilisé sur les équipements VoIP et ses spécifications sont libres d'accès.

Pour notre application on a choisi Asterisk pour jouer le rôle d'un PABX, qui sera installé sur le serveur.

##### 4.2. Asterisk

Asterisk est né en 1999, créé par un étudiant de l'université d'Auburn (États-Unis - Alabama). A la recherche d'un commutateur téléphonique privé pour créer un centre de support technique sur Linux, il est dissuadé par les tarifs trop élevés des solutions existantes, et décide de se créer son propre routeur d'appels sous Linux, le PBX Asterisk.

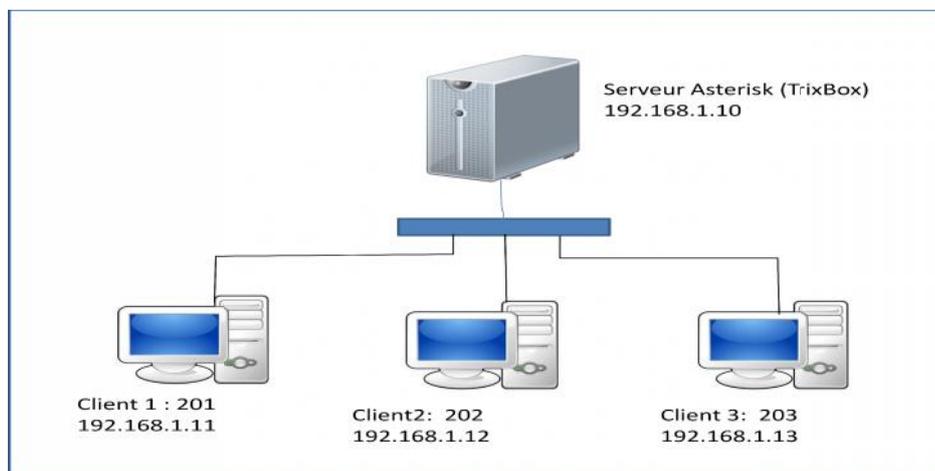
Asterisk est un logiciel libre qui permet d'utiliser un ordinateur en tant que commutateur téléphonique privé. Il interconnecte en temps réel des réseaux de voix sur IP via plusieurs protocoles (SIP, H323,...) et des réseaux de téléphonies classiques via des cartes d'interface téléphonique et tout ceci à moindre coût. Asterisk offre toutes les fonctions d'un PBX et ses services associés comme de la conférence

téléphonique, des répondeurs interactifs, de la mise en attente d'appels, des mails vocaux, de la musique d'attente, de la génération d'enregistrement d'appels pour l'intégration avec des systèmes de facturation, etc....

### 4.3. Eléments nécessaires

- **Le serveur VoIP** : il peut être une machine virtuelle ou une machine dédiée.
- **Le Switch** : il assure la distribution et commutation des ports Ethernet.
- **Le softphone** : c'est un logiciel installé sur les ordinateur clients et qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC.

Voici le plan de câblage qu'on va réaliser avec l'adressage suivant :



#### Serveur Asterisk :

Adresse IP : 192.168.1.10

Masque de sous réseau : 255.255.255.0

#### Client 1 :

Adresse IP : 192.168.1.11

Masque de sous réseau : 255.255.255.0

#### Client 2 :

Adresse IP : 192.168.1.12

Masque de sous réseau : 255.255.255.0

#### Client 3 :

Adresse IP : 192.168.1.13

Masque de sous réseau : 255.255.255.0

#### 4.4. Installation de serveur

Asterisk est compatible avec n'importe quelle distribution Linux dont la version du kernel est au moins 2.4.5. Pour installer asterisk dans notre cas on utilise une distribution très répandue appelée TrixBOS.

Le système TrixBOS est un ensemble de logiciels open source qui permettent de compléter le logiciel Asterisk, pour fournir l'ensemble des fonctions nécessaires à un central téléphonique haut de gamme.

C'est une distribution GNU/Linux basée sur Cent OS . Voici quelques fonctionnalités incluses avec trixbos:

- \_ **Linux CentOS:** Système d'exploitation
- \_ **MySQL:** serveur de base de données
- \_ **Apache:** Serveur Internet
- \_ **PHP:** Langage de script orienté serveur
- \_ **Asterisk:** PBX voix-sur-IP
- \_ **FreePBX:** Interface graphique pour Asterisk
- \_ **SugarCRM:** Outil de gestion de la relation client.

##### 4.4.1 Lancement de l'installation de trixbos

*L'installation est extrêmement simple : il suffit d'insérer le CD d'installation gravé sous forme d'une image .ISO et suivre les étapes suivantes :*

- **choix du langage :** Quand demandé, on sélectionne le bon type de clavier:



- **Choix du fuseau horaire** : on choisi la localisation, pour régler les paramètres de l'heure.



- **Configuration du mot de passe root** : il faut maintenant choisir le mot de passe root, on le tape deux fois.

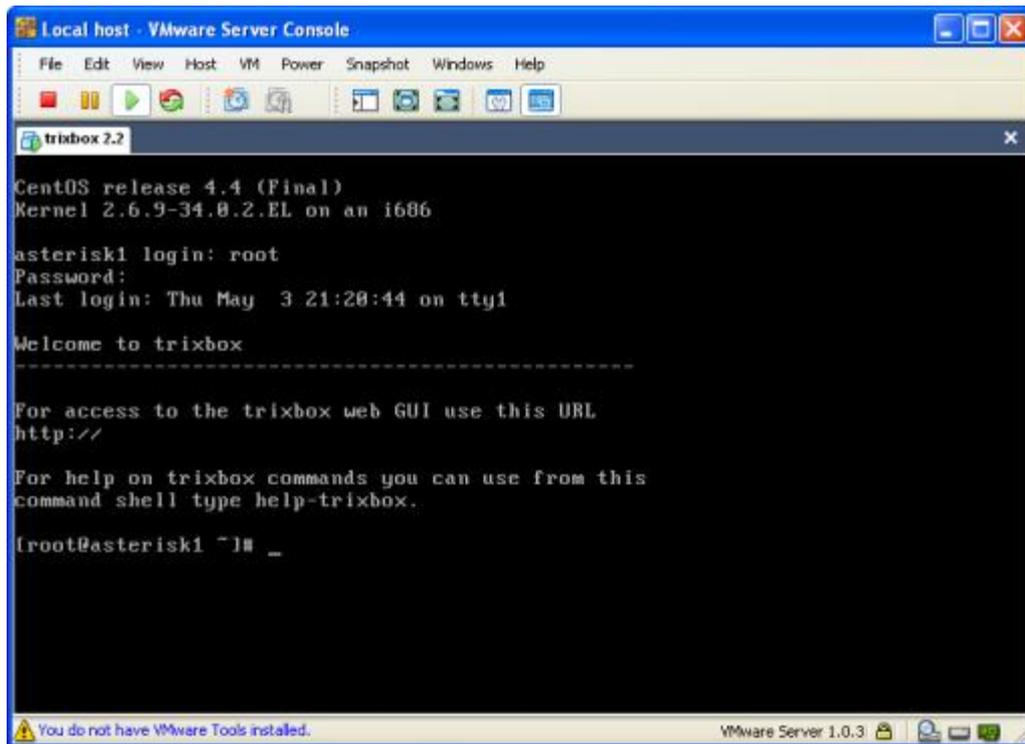


L'installation se déroule ensuite automatiquement et plusieurs redémarrages seront nécessaires. le CDROM s'éjecte automatiquement au premier redémarrage, donc on doit le retirer dès le premier redémarrage.

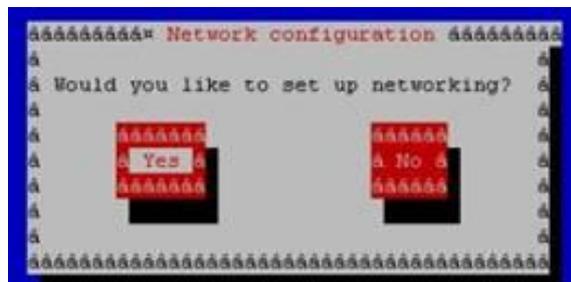
Par défaut, le système s'installe sur le disque dur entier sans demander de partitionnement.

#### 4.4.2. Premier démarrage

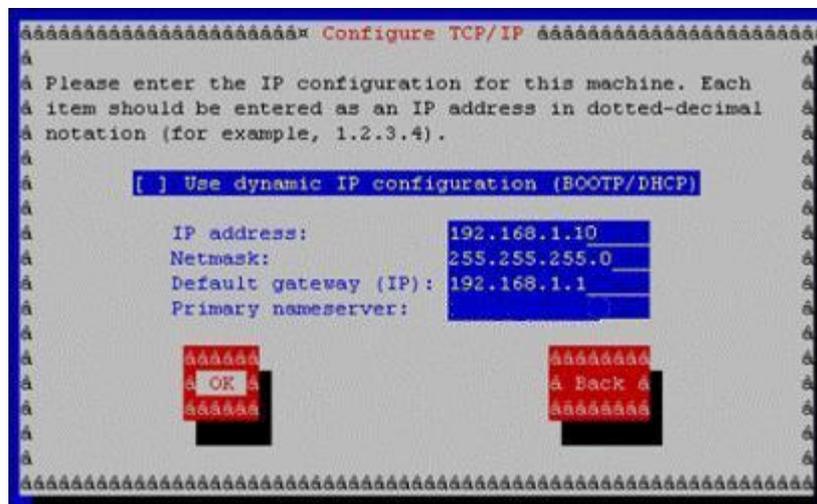
Maintenant on doit paramétrer le réseau pour un serveur statique car la configuration par défaut est en DHCP. Une fois la machine est redémarrée on se connecte avec le compte root, et le mot de passe choisis.



Une fois connecté, on tape la commande **system-config-network** pour définir les nouveaux paramètres de la carte. Cette opération va complètement effacer les valeurs précédentes.



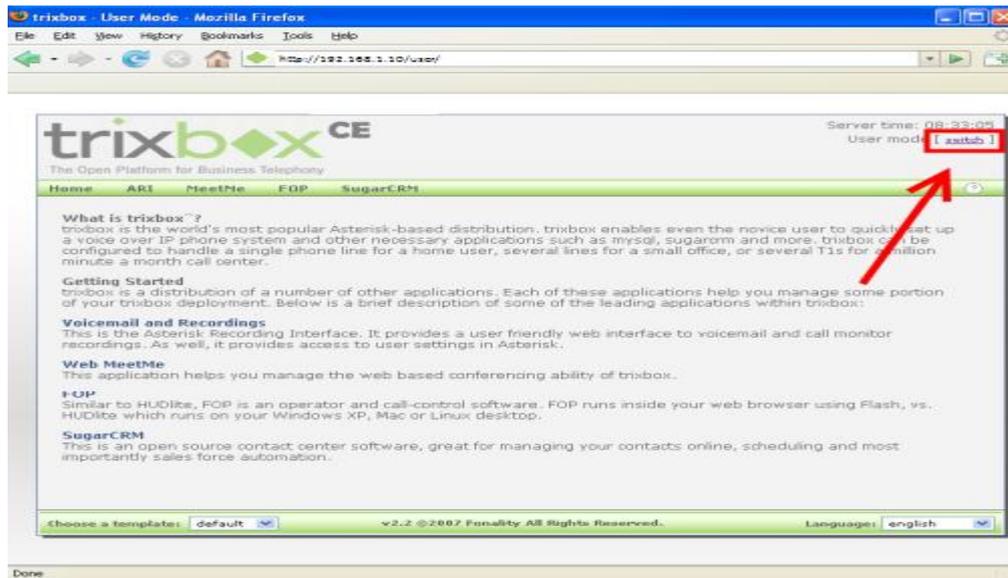
On configure l'adresse IP, masque de réseau, passerelle, avec les paramètres choisis on clique sur Yes.



Maintenant il faut redémarrer l'interface réseau avec la commande **service network restart** et notre serveur est fonctionnel et prêt à être configuré.

#### 4.4.3. Connexion a l'interface graphique

Sur une autre machine de notre réseau, on accède à l'interface web de configuration de Trixbox en entrant l'adresse du serveur dans un navigateur internet :

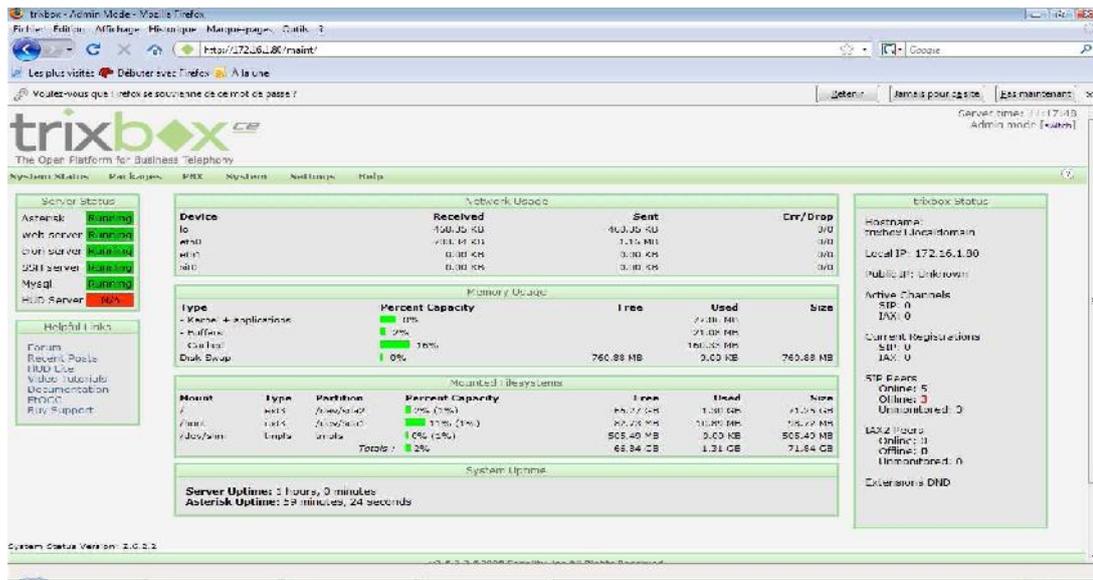


On clique sur **switch** pour entrer dans le mode administration: Un pop-up apparait pour entrer l'identifiant et le mot de passe. Par défaut c'est :

- login : **maint**
- password : **password**



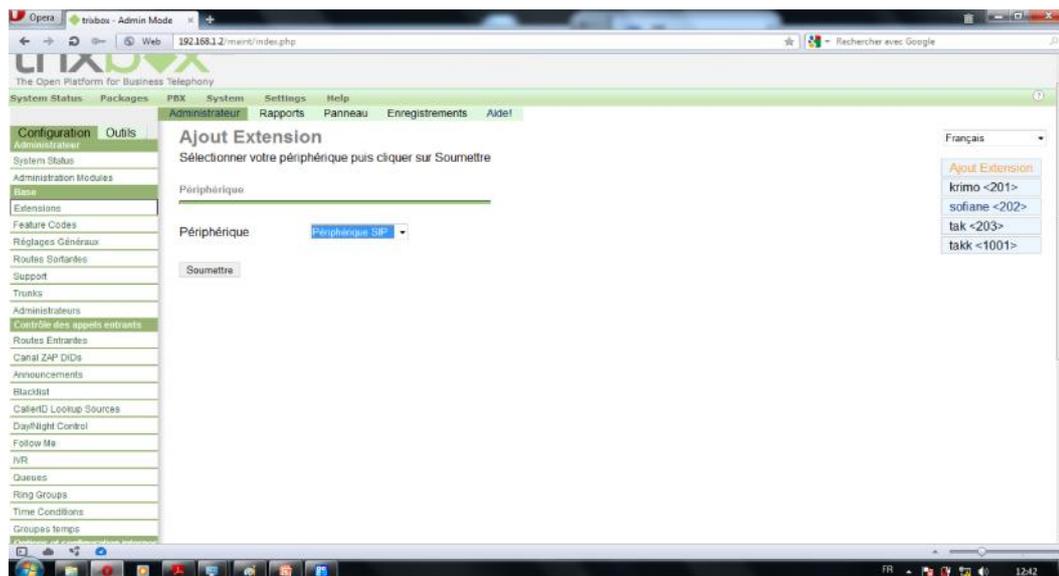
La page suivante s'affichera et on remarque qu'Asterisk et autres serveurs en état de marche.



#### 4.5. Création des comptes SIP (Extension)

Pour créer des extensions, on entre dans **PBX > PBX setting**. Dans le menu vertical on sélectionne **Extensions**. C'est ici que nous allons pouvoir créer les différentes lignes pour les téléphones. Nous avons le choix entre trois types de ligne différente.

- **Generic SIP Device** : vous permet de créer une ligne SIP.
- **Generic IAX2 Device** : vous permet de créer une ligne spécifique entre deux Asterisk.
- **Generic ZAP Device** : vous permet de créer une ligne pour l'extérieur (ligne RTC).



Pour une ligne SIP, il faut choisir **Périphérique SIP**. Une fois le type choisi cliquer sur **Submit**.

Les champs de base à remplir sont :

- **User Extension** : Numéro de la ligne.
- **Display Name** : Nom de la ligne SIP.
- **Secret** : mot de passe de la ligne.

Une fois la configuration terminée cliquer sur **Submit**.

Pour enregistrer les modifications, il faut cliquer sur **Submit** puis **Activer les nouvelles modifications** puis **Activer**.



Pour chaque modification, on remarque des feedbacks sur l'écran du serveur.

Les comptes à configurer sont :

**Compte 1 :**

Numéro de téléphone : 201  
 Nom : Personne 1  
 Mot de passe : 12345

**Compte 2 :**

Numéro de téléphone : 202  
 Nom : Personne 2  
 Mot de passe : 12345

**Compte 3 :**

Numéro de téléphone : 203  
 Nom : Personne 3  
 Mot de passe: 12345

#### 4.6. Installation des postes clients (Softphone)

Notre serveur Trixbox est maintenant configuré avec trois extensions ou numéros de téléphone. Des téléphones logiciels (softphones) SIP sont utilisés sur trois ordinateurs.

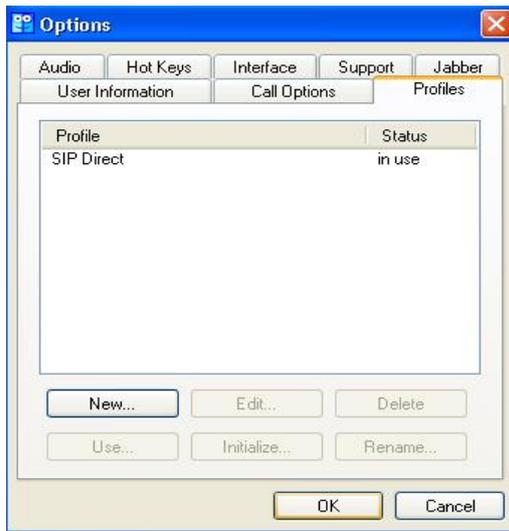
Un téléphone logiciel (softphone) est un téléphone installé sur un ordinateur pendant qu'un téléphone matériel (hardphone) est un téléphone physique semblable à un téléphone traditionnel. Dépendant de leurs capacités, les deux types de téléphones peuvent être capables d'utiliser la voix-sur-IP.

On a choisit le logiciel SJPhone. Voici les étapes de configuration des softphones pour s'identifier auprès de notre serveur.



Cliquer sur le bouton **Menu**, puis sur **Option**.

Cliquer sur **New** pour créer un nouveau profil.



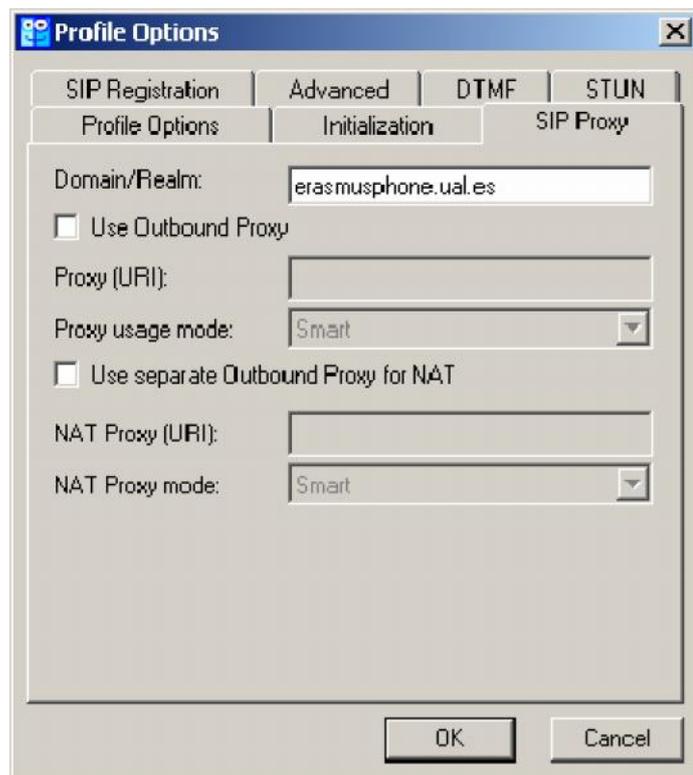
On introduit le nom de profil, ici personne 1.

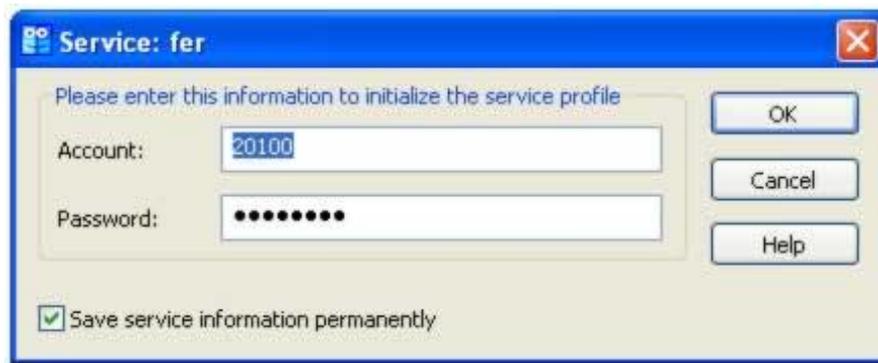


A présent, on doit configurer les paramètres IP et proxy . Dans l'onglet **SIP Proxy**, on introduit les valeurs suivantes.

- **Domaine/Realm** : adresse réseau de la machine ex : 192.168.1.11.
- **Use Outbound proxy** : adresse de notre serveur ex : 192.168.1.10.

Puis la validation par OK.





Sur l'écran de serveur, on remarque un message qui indique que les compte sont bien enregistrés et sont prêts pour se communiquer.

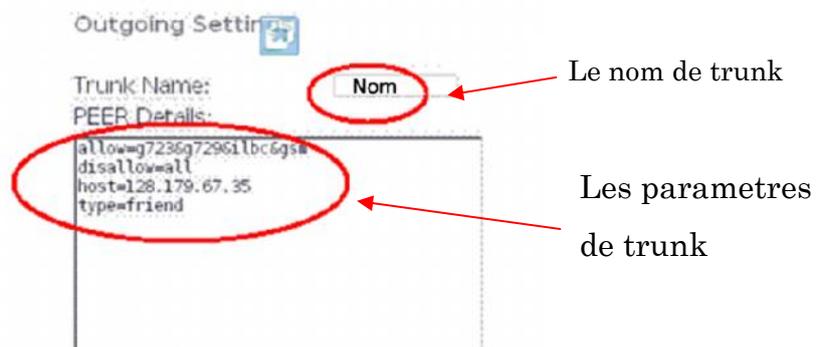
## 4.7. Configurer les appels sortants

### 4.7.1. Le Trunks

Un trunk représente un accès du serveur vers l'extérieur. Par exemple vers un serveur spécifique, un routeur... Tous les trunks que nous utilisons ici sont des trunks SIP.

Dans la configuration du trunk, on donne l'adresse du serveur externe auquel on veut se connecter, la liste des codecs autorisés dans l'ordre de préférence et le type du serveur externe (peer ou friend).

Dans notre cas on configure un trunk pour un serveur SIP de type **friend**. Cette méthode de connexion est la plus simple, mais aussi la moins sûre.



On déclare un trunk différent pour chaque serveur sortant.

### 4.7.2. La Routes

Une route va permettre de diriger un appel sortant vers une destination particulière, par exemple en fonction du numéro composé.

Par exemple ici, on crée une route qui redirige l'appel vers le trunk qui nous avons créé si le numéro appelé est préfixé d'un 4.

Basic

- Administrators
- Extensions
- General Settings
- Outbound Routes
- Trunks
- Inbound Call Control
- Inbound Routes

### Add Route

Route Name:

Route Password:

Emergency Dialing:

Intra Company Route:

Dial Patterns

Insert:

Trunk Sequence

Nom de route

Préfixe

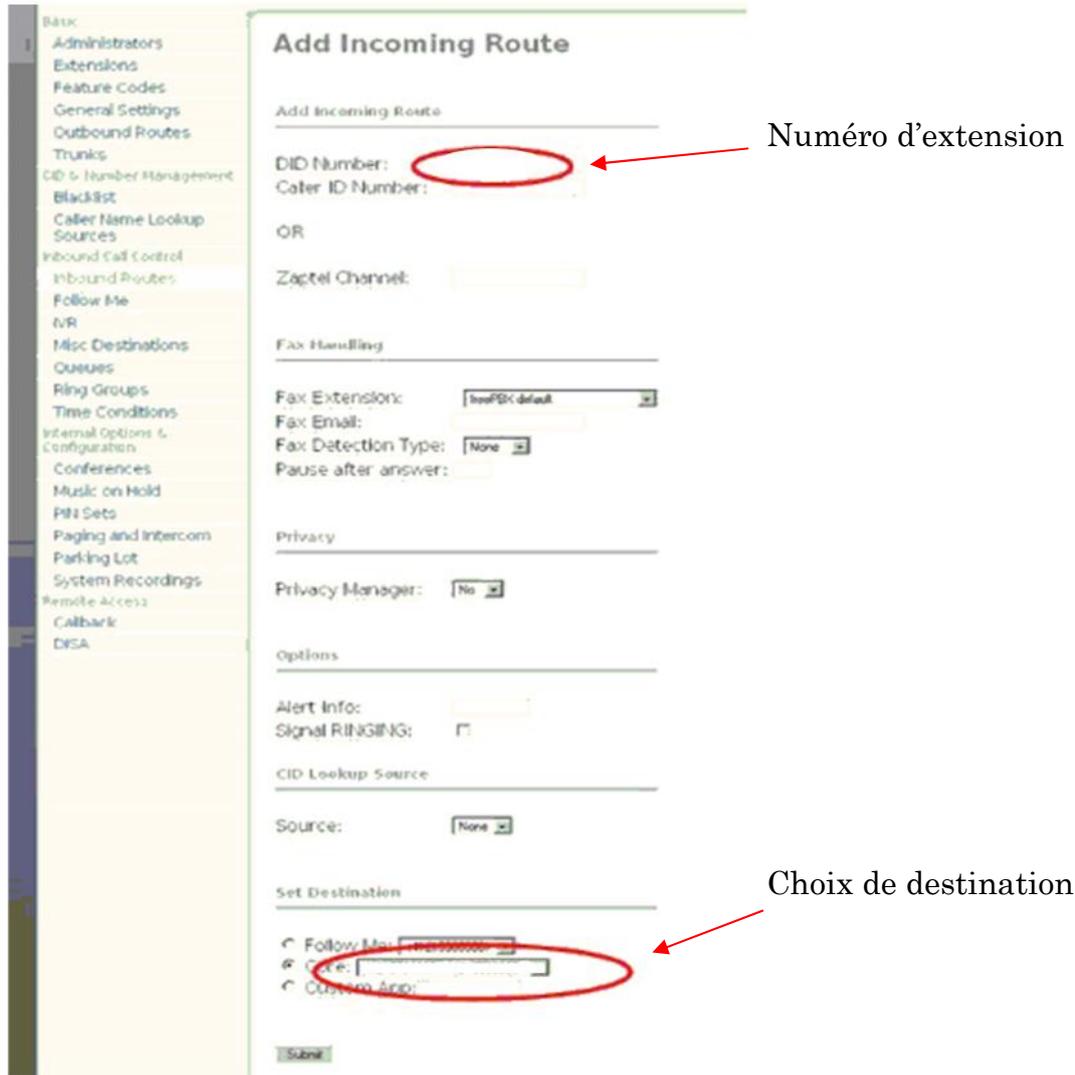
Type de trunk

A ce stade, le serveur sera capable d'appeler des appareils externes suivant les trunks définis.

#### 4.8. Configuration des appels entrants

On va maintenant permettre aux appels entrants d'être dirigés sur le bon appareil. On ajoute une route entrante pour chaque extension qui doit être atteignable de l'extérieur.

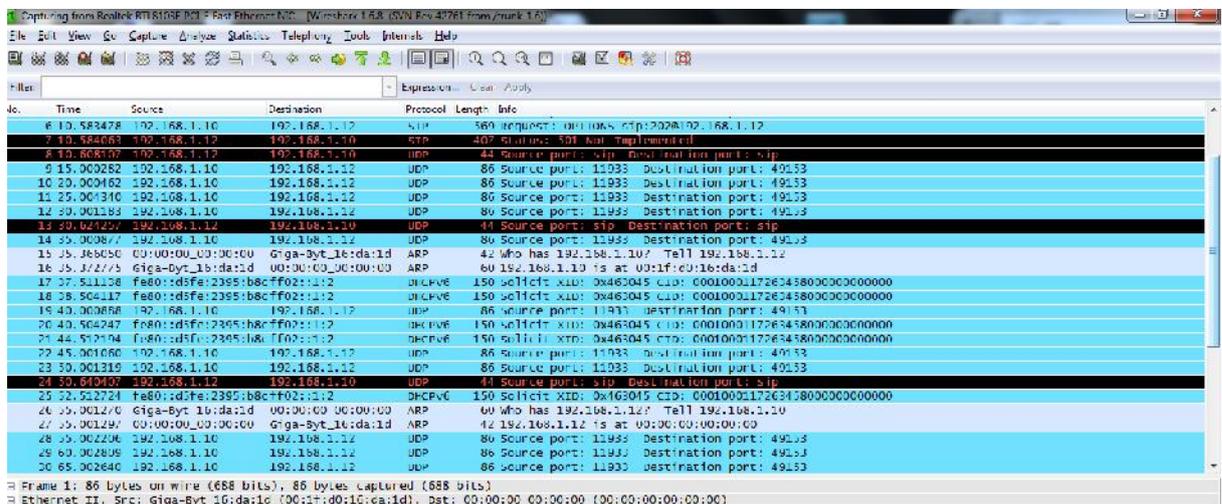
On entre le numéro SIP comme identifiant de la route, et on indique quoi faire de l'appel entrant. Ici, il est simplement redirigé vers l'appareil concerné.



### 5. Evaluation des performances avec Wireshark

Nous avons réalisé quelques études concernant les performances de la mise en place de notre solution VoIP. Pour cela nous avons utilisé l'application Wireshark.

La capture suivante montre les paquets interceptés par Wireshark.



Suite à cette interception nous avons procédé à l'évaluation des critères de performance d'une communication: Taux de perte, Le Max Delta, Max Jitter et le Mean Jitter. La figure ci-dessous que la valeur de la perte des paquets est de 0%, et que la valeur de Jitter moyenne est de 20 ms ce qui indique une qualité de son acceptable.

Src IP addr	Src port	Dst IP addr	Dst port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)
192.168.1.10	13060	192.168.1.12	49156	0x789FF0DC	g711U	2344	0 (0,0%)	144,73	23,35
192.168.1.10	10156	192.168.1.12	49158	0x2673C700	g711U	1125	0 (0,0%)	99,71	18,01
192.168.1.10	11124	192.168.1.12	49160	0x60C459E5	g711U	391	0 (0,0%)	122,99	20,57
192.168.1.10	17014	192.168.1.12	49162	0x23D2D4F9	g711U	2087	0 (0,0%)	166,12	23,91

## 6. Discussion

Durant ce chapitre nous avons procédé à la mise en place d'une solution VoIP pour un LAN, sur les différentes plateformes Linux comme serveur et Windows comme des clients. Nous avons expliqué la configuration des communications internes et externes au réseau.

Enfin, une évaluation des performances de cette solution. Les résultats que nous avons obtenus concernant la QoS sont intéressants.



## Conclusion générale

La téléphonie sur IP constitue un marché qui attire de plus en plus l'attention, permettant de concentrer accès, gestion et administration sur un seul système, elle génère ainsi une très forte potentialité de gains fondés sur de réelles économies de coûts. Elle autorise l'intégration des différents sites des grandes entreprises en un seul système de téléphonie, à la fois synonyme d'économies pour les employés en déplacement comme pour les télétravailleurs, et optimisant les applications informatiques des systèmes de téléphonie.

Si la téléphonie sur IP présente de nombreux avantages, elle doit néanmoins relever de nombreux défis, et pallier certains inconvénients techniques, notamment en matière de sécurité, de normes et de qualité de voix. Les entreprises doivent affronter une hétérogénéité de l'offre au moment même d'un certain ralentissement économique. Pour fonder au mieux leur prise de décision, les entreprises doivent évaluer leurs besoins, établir un plan et procéder à l'investissement qui s'impose en conséquence.

Dans le cadre de l'étude de leurs besoins, les entreprises doivent tenir compte de plusieurs facteurs : le nombre et le type d'utilisateurs à savoir distants ou internes, la téléphonie sur IP globale et locale, les coûts liés à l'utilisation ou au remplacement de l'équipement existant par un système de téléphonie sur IP, le niveau acceptable de la qualité de la voix, les mesures de protection contre les atteintes à la sécurité et enfin, le type de convergence souhaité comme services intégrés de types messagerie électronique, messagerie vocale, click-to-dial, vidéoconférences basée sur le Web.

Pour choisir le système de téléphonie sur IP le mieux adapté à leurs besoin, et qui n'est pas nécessairement le plus évolué ou le plus onéreux, les entreprises doivent prendre en considération les questions relatives aux coûts d'installation et de maintenance, au retour sur investissement, à la sécurité et aux normes.

Autre point important à considérer, ce sont les contrats de niveau de service relatifs, par exemple, à la disponibilité du réseau, le temps d'attente, la

perte de paquets, la prestation de services, le temps moyen de réparation et l'indice de qualité de la voix / l'indice des appels. Les questions de sécurité vont être de plus en plus importantes à court terme et cela, jusqu'à ce que les systèmes de téléphonie s'appuyant sur les réseaux locaux soient plus aboutis.

La technologie VoIP permet une grande mobilité en le combinant avec des technologies comme wireless, bluetooth, WIFI. Nous ne pouvons que nous réjouir de vivre l'essor de ses différentes technologies.

Nous pouvons donc vraisemblablement penser que le protocole IP deviendra un standard unique permettant l'interopérabilité des réseaux mondialisés. C'est pourquoi l'intégration de la voix sur IP n'est qu'une étape vers EoIP : Everything over IP.

# Glossaire

**ARP:** Address Resolution Protocol.  
**ADM:** Adaptive Delta Modulation.  
**ADPCM:** Adaptive Differential Pulse Code Modulation.  
**ATM:** Asynchronous Transfert Mode.  
**CSMA/CD :** Carrier Sense Multiple Access/Collision Detection.  
**CODEC :** COder DECoder.  
**DCME:** Digital Circuit Multiplication Equipment.  
**PCM:** Pulse Code Modulation.  
**DHCP :** Dynamic Host Configuration Protocol.  
**DNS :** Domain Name Server.  
**DiffServ :** Diffetiel Service.  
**FDDI:** Fiber Distributed Data Interface.  
**FTP :** File Transfert Protocol.  
**HTTP:** Hyper Text Transport Protocol.  
**IGMP :** Internet Group Management Protocol.  
**ICMP :** Internet Control Message Protocol.  
**IGRP :** Interior Gateway Routing Protocol.  
**LPC:** Linear Predictive Coding.  
**LAN :** Local Area Network.  
**LS :** Location Server.  
**MAN :** Metropolitan Area Network.  
**MAU :** Multi station Access Unit.  
**MAC:** Media Access Control.  
**MGCP :** Media Gatway Control Protocol.  
**MPLS :** Multi-Protocol Label Switching.  
**MMUSIC :** Multiparti Multimedia Session Control.  
**NAT :** Network Address Translation.  
**OSI :** open system inteconnection.  
**PABX :** Private Automatic Branch eXchange.  
**PSTN:** Public Switched Telephone Network.  
**PCM:** Pulse Code Modulation.  
**POP3 :** Post Office Protocol version 3.  
**QoS:** Quality of Service.  
**QSIG:** an ISDN based signalling protocol.  
**RAS :** registration admission status.  
**RPE-LTP:** Regular Pulse Excited-Long Term Predictor.  
**RSVP:** Resource ReSerVation Protocol.  
**RTCP :** Real Time Control Protocol.  
**RTP:** Real Time Protocol.  
**RTPC :** Réseau téléphonique public commuté.  
**RNIS :** Réseau Numérique à Intégration de Services (ISDN).  
**RIP :** Routing Information Protocol.  
**RSVP :** ReSerVation Protocol.  
**RS :** Redirect Server.  
**SDP :** Session Description Protocol.  
**SIP :** Session Initiation Protocol.  
**SIP:** Session Internet Protocol.  
**SMTP :** Simple Mail Transfert Protocol.  
**ToIP :** Telephony over Internet Protocol.  
**TCP/IP :** Transmission Control Protocol/Internet Protocol.  
**UDP :** User Datagram Protocol.  
**UAS :** User Agent Server.  
**UAC :** User Agent Client.  
**VoIP:** Voice over IP.  
**VPN:** Virtual Private Network.  
**VoDSL:** Voice over DSL.  
**WAN :** Wide Area Network.



## Bibliographie

- [1] – Mémoire : La téléphonie sur IP – Mr : MAIGA Malik et Mr : FAYE Modou – ITAB-Oran 2004
- [2] – Mémoire : La voix sur IP – Mr : ABED Amine et Mr : GUENOVA Abdelwahab – ITAB-Oran 2005
- [3] – <http://www.ietf.org/rfc/rfc2705.txt?number=2705>
- [4] – Wikipedia.org
- [5] – [www.lejura.fr/telephonie/normes/documents/modele%20osi.pdf](http://www.lejura.fr/telephonie/normes/documents/modele%20osi.pdf)
- [6] – Danièle DROMARD et Dominique SERET : Architecture des réseaux – Edition: Pearson Education France 2009 – Pages : 248
- [7] – Claude Servin: Réseaux et télécoms cours et exercices corrigés – Edition: DUNOD 2003 – Pages : 811 (Nouvelle édition corrigée)
- [8] – <http://www.htrr.ups-tlse.fr/pedagogie/cours/trans/techniques.html#S1>
- [9] – [www.pasteur.fr/formation/infobio/arch/archi-reseaux.pdf](http://www.pasteur.fr/formation/infobio/arch/archi-reseaux.pdf)
- [10] – <http://faq.domaine-achat.fr/content/3/48/fr/serveur-dns-definition-.html>
- [11] – [http://irp.nain-t.net/doku.php/165dhcp:20-serveur\\_dhcp](http://irp.nain-t.net/doku.php/165dhcp:20-serveur_dhcp)
- [12] – <http://www.commentcamarche.net/contents/internet/nat.php3#principe-du-nat>
- [13] – [http://ipcreator.free.fr/technique/reseau/protocoles/tcpip/routage\\_ip.htm](http://ipcreator.free.fr/technique/reseau/protocoles/tcpip/routage_ip.htm)
- [14] – [www.laissus.fr/pub/cours/cours.pdf](http://www.laissus.fr/pub/cours/cours.pdf) cours tcp/ip
- [15] – [www.frameip.com/voip/](http://www.frameip.com/voip/)
- [16] – <http://www.blog.saeed.com/2011/03/architecture-et-mode-access-de-la-telephonie-sur-ip/>
- [17] – [iutsa.unice.fr/~frat/PT/Telephonie/CallManager/TP001.4.doc](http://iutsa.unice.fr/~frat/PT/Telephonie/CallManager/TP001.4.doc)
- [18] – Mémoire: Conception d'une application VoIP Pc vers PC – Mr: DAF Karim et Mr: IBOUCHICHENE Mourad – UMMTO 2010
- [19] – [belpois.perso.libertysurf.fr/dossiers/gsm/index.php](http://belpois.perso.libertysurf.fr/dossiers/gsm/index.php)
- [20] – [www.efort.com/r\\_tutoriels/H323\\_EFORT.pdf](http://www.efort.com/r_tutoriels/H323_EFORT.pdf)
- [21] – [www.architoip.com/entete-sip/](http://www.architoip.com/entete-sip/)
- [22] – [www.telephonie-ip.com/ipsolutions/docs/technologie\\_sip\\_fr.pdf](http://www.telephonie-ip.com/ipsolutions/docs/technologie_sip_fr.pdf)
- [23] – Mémoire: Mesure des paramètres de qualité de service pour les applications voix sur IP – Mlle LOUHICHI Zineb – Ecole Supérieure de Télécommunication de Tunis – 2005/2006
- [24] – <http://www.blog.saeed.com/2011/03/codes-et-gestion-de-qualite-de-service-telephonie-ip/>
- [25] – <http://www.frameip.com/telephonietraditionnelle>
- [26] – <http://standard-telephonique.comprendrechoisir.com/comprendre/centex>
- [27] – Mémoire: La VoIP – Mr: RIMEH Salhi – A-U – 2008/2009