

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique



Mémoire De Fin de cycle

En vue d'obtention du diplôme de master en informatique.
Spécialité : Administration et Sécurité des Réseaux.

Thème

Réalisation d'une solution VoIP avec le serveur FreePBX

Réalisé par :

M. HADJ ALI Mehdi et M. DJENAOUCINE Anis .

Évalué le 04/07/2022 à 12H devant le jury composé de :

Examineur 1	M. AMROUN kamal	U. A/Mira Béjaïa.
Examineur 2	M. KHANOUCHE Mohamed Essaid	U. A/Mira Béjaïa.
Encadrante	Mme. GADOUCHE Hania	U. A/Mira Béjaïa.

Année universitaire 2021/2022

Remerciements

À travers ce modeste travail, Nous tenons à remercier notre encadrante pour ses conseils, son orientation et son aide le long de notre projet de fin d'études.

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 ont aidé 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.

Nous remercions aussi l'entreprise EXSON TELECOM, pour leurs accueils en stage pratique.

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

Résumé

La téléphonie IP a de nos jours pris beaucoup d'ampleur dans le monde des télécommunications en particulier pour les entreprises qui utilisent des services de centres d'appels. En effet, l'adoption de cette technologie a pour avantage d'offrir des services de voix, images ou vidéos tout en minimisant les coûts de communication.

Dans le cadre de notre projet, nous avons réalisé une solution VoIP en utilisant le serveur FreePBX. Cette solution est une alternative intéressante pour l'utilisation personnelle et professionnelle qui permet de mettre en place un système téléphonique complet et d'établir un centre d'appels pour n'importe quel organisme en utilisant le protocole SIP.

L'implémentation de cette architecture a été faite avec des outils open source dont les softphones, le serveur FreePBX et VMware Workstation.

Mots clés : VOIP, FreePBX, SIP, VMware workstation, softphones.

Abstract

IP telephony has nowadays taken a lot of importance in the world of telecommunications, especially for companies that use call center services. Indeed, the adoption of this technology has the advantage of offering voice, image or video services while minimizing communication costs.

In the framework of our project, we have implemented a VoIP solution using the FreePBX server. This solution is an interesting alternative for personal and professional use that allows to set up a complete telephone system and to establish a call center for any organization using the SIP protocol.

The implementation of this architecture was made with open source tools including softphones, FreePBX server and VMware Workstation. **Keywords :** VOIP, FreePBX, SIP, VMware workstation, softphones.

Keywords : VOIP, FreePBX, SIP, VMware workstation, softphones.

Table des matières

Introduction générale	1
1 Généralités sur les réseaux informatiques	4
1.1 Introduction	5
1.2 Définition d'un réseau informatique	5
1.3 Objectifs d'un réseau informatique	5
1.4 Les types de réseaux	6
1.4.1 Les modes de transmission	6
1.4.2 La portée	6
1.5 Les topologies des réseaux	7
1.6 Les architectures des réseaux informatiques	11
1.6.1 Architecture poste-à-poste	11
1.7 Composants matériels d'un réseau	12
1.7.1 Equipements d'interconnexion	12
1.7.2 Les supports de transmissions	13
1.7.3 Les périphériques finaux	15
1.8 Le modèle de référence OSI	15
1.8.1 Définition	15
1.8.2 Les différentes couches	15
1.9 Conclusion	17
2 Les réseaux IP	18
2.1 Introduction	19
2.2 Définition	19
2.3 Le modèle TCP/IP	19
2.3.1 Les différentes couches du modèle TCP/IP	20
2.3.2 Les protocoles de chaque couche	21
2.4 L'adressage IP	23
2.4.1 Composition d'une adresse ipv4	24
2.5 Les classes d'adresses	24

Table des matières

2.5.1	Les sous-réseaux	25
2.5.2	Le masque sous-réseau	26
2.5.3	L'adresse de diffusion (Broadcast)	27
2.6	Le routage	27
2.6.1	Types de routage	27
2.7	Le network address translation (NAT)	28
2.8	Le DNS (domain name system)	29
2.8.1	Types de service DNS	29
2.9	Le DHCP (dynamics host configuration protocol)	30
2.9.1	Fonctionnement de DHCP	30
2.10	Conclusion	32
3	La voix sur les réseaux IP	33
3.1	Introduction	34
3.2	Définition	34
3.3	Téléphonie classique vs Téléphonie sur IP	34
3.4	Principes et fonctionnement de la VoIP	35
3.5	Les protocoles utilisés par la VoIP	37
3.5.1	Les protocoles de transport	37
3.5.1.1	Le protocole RTP (Real-time Transport Protocol)	37
3.5.1.2	Le protocole RTCP	38
3.5.1.3	Le protocoles SRTP	40
3.5.2	Les protocoles de Signalisation	40
3.5.2.1	Le protocole H323	41
3.5.2.2	Le protocole SIP	42
3.6	Points forts et limites de la voix sur IP	48
3.6.1	Les points forts	48
3.6.2	Les limies	48
3.7	Conclusion	49
4	Présentation du serveur FreePBX	50
4.1	Introduction	51
4.2	Définition	51
4.3	Le standard téléphonique traditionnel (PABX)	51
4.4	Le standard téléphonique IP (IP-PBX)	52
4.5	Standard PABX analogique vs standard IPBX	53
4.6	Pourquoi utiliser FreePBX?	53
4.7	Les principales fonctionnalités de FreePBX	54

Table des matières

4.8	Matériels installés avec FreePBX	54
4.9	Installation de FreePBX	56
4.10	Connexion a l'interface graphique	59
4.11	Conclusion	60
5	Réalisation	61
5.1	Introduction	62
5.2	Architecture réseau de la réalisation	62
5.2.1	Adressage	63
5.3	Configuration	63
5.3.1	Configuration des extensions (postes)	63
5.3.2	Configuration des files d'attentes (queues)	67
5.3.3	Configuration de la réponse vocale interactive (IVR)	71
5.3.4	Configuration des appels sortants	75
5.3.5	Conclusion	78
	Conclusion générale	78

Table des figures

1.1	Classification des réseaux selon la portée	7
1.2	Topologie en bus	8
1.3	Topologie en anneau	8
1.4	Topologie en étoile	9
1.5	Topologie maillée	10
1.6	Topologie hybride	10
1.7	Architecture poste-à-poste	11
1.8	Câble coaxial	13
1.9	Câbles à paires torsadées	14
1.10	Câble fibre optique	14
1.11	Le modèle de référence OSI	17
2.1	Exemple d'un sous-réseaux	26
2.2	Le NAT	29
2.3	DHCP discover	30
2.4	DHCP offer	31
2.5	DHCP request	31
2.6	DHCP ACK	32
3.1	Réseau téléphonique comuté	35
3.2	Fonctionnement de la VoIP	37
3.3	Enregistrement d'un terminal	47
3.4	Communication directe	47
4.1	PABX Alcatel 4200	52
4.2	Standard téléphonique IP (IP-PBX)	52
4.3	Softphone mizu droid sur PC	55
4.4	Téléphone SIP Sangoma	55
4.5	Softphone Zoiper sur Android	56
4.6	Étape 1	57

Table des figures

4.7	Étape 2	57
4.8	Étape 3	58
4.9	Étape 4	58
4.10	Interface de FreePBX sur VMware	59
4.11	Création d'un utilisateur avec des privilèges d'administrateur	60
4.12	L'interface graphique de FreePBX	60
5.1	Architecture réseau de la réalisation	62
5.2	Création d'une extension	64
5.3	Liste des extensions créées	65
5.4	Enregistrement du poste 100	66
5.5	Enregistrement du poste 200	66
5.6	Postes (100 et 200) en ligne	66
5.7	Poste 100 (appellant)	67
5.8	poste 200 (appelé)	67
5.9	Importation d'un enregistrement vocal	68
5.10	Création d'une file d'attente	69
5.11	Création d'une file d'attente - suite	70
5.12	Liste de files d'attentes créée	70
5.13	Service de réception	71
5.14	Service d'administration	71
5.15	Shéma de l'IVR	72
5.16	Création de l'IVR	73
5.17	Création de l'IVR - suite	73
5.18	Création de la route entrante	74
5.19	Poste 200 (service d'administration)	75
5.20	Poste 100 (service de réception)	75
5.21	Création d'un trunk	76
5.22	Création d'une route sortante	77

Liste des tableaux

2.1	Les couches du modèle TCP/IP	21
2.2	IPV4 VS IPV6	23
2.3	Structure d'adresses de classe A	24
2.4	Structure d'adresses de classe B	24
2.5	Structure d'adresses de classe C	25
2.6	Structure d'adresses de classe D	25
5.1	Adressage et affectation des numéros	63
5.2	la téléphonie analogique VS la solution proposée	78

Liste des abréviations

ACK	ACKnowledged
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPBX	Internet Protocol Private Branch eXchange
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
NAT	Network Address Translation
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PABX	Private Automated Branch Exchange
PBX	Private Branch eXchange
RIP	Routing Information Protocol
RTC	Réseau téléphonique commuté
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SRTP	Secure Real-time Transport Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTP	UNSHIELDED TWISTED PAIRS
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

Introduction générale

Le développement des technologies de transmission de la voix basée sur le protocole IP représente actuellement 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 a rendue possible grâce à la baisse des coûts d'accès et de communication, et les efforts fournis pour le développement de la technique dans le domaine des réseaux IP et RTC a permis de donner naissance à la téléphonie sur IP, mieux connue sous le nom voix sur IP (VoIP, voice over internet protocol), c'est une nouvelle technologie qui s'impose rapidement dans le domaine de la communication vocale. Elle utilise les réseaux Internet pour communiquer dans le monde entier et dans un grand nombre d'entreprises.

la téléphonie sur IP propose des différents services basés sur plusieurs scénarios de communication (PC à PC, téléphonie entre un PC et un poste ...). De plus, cette technologie est devenue un outil de communication sur le réseau internet, en intégrant des outils d'interfaces avec les réseaux téléphoniques traditionnels, elle utilise des protocoles spéciaux dédiés à ce genre d'applications, comme le protocole de transport en temps réel RTP utilisé en parallèle avec des protocoles de signalisation, le standard H323 et le protocole d'Initiation de sessions (SIP).

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. Toutefois, les aspects techniques de 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.

Problématique

La plupart des entreprises aujourd'hui utilisent encore la téléphonie classique basée sur le réseau téléphonique commuté (RTC) dans leurs communications quoiqu' soient dotées de réseaux informatiques qui parcourent presque leurs infrastructures.

Ce type de réseau existe depuis près d'un demi-siècle maintenant donc les pannes se multiplient en raison de l'ancienneté de la technologie, et les équipements nécessaires au fonctionnement du réseau RTC sont plus difficiles d'accès qu'auparavant. De plus l'équipement, l'installation et la maintenance de ces réseaux entraînant un coût d'installation et d'exploitation très élevé, cette situation que semblent minimiser plusieurs managers diminue le budget de fonctionnement de ces entreprises. Le problème de la cherté des coûts de communication est d'autant plus important que le transport des données en entreprise est vital pour cette dernière.

Le but est de rechercher la meilleure solution qui permettrait une réduction des coûts de communication en entreprise. L'idéal serait de fusionner tous ces moyens de communication dans une solution intégrée qui offrirait toutes les garanties des services communicationnels ci-dessus cités. Pour y parvenir, la communication sur IP apparaît comme une solution prometteuse qu'il conviendrait d'explorer.

Objet de l'étude

L'objectif de notre étude est de savoir comment utiliser la téléphonie sur IP pour minimiser les coûts d'installation et d'exploitation tout en optimisant la communication en entreprise. S'interroger sur les mécanismes d'une telle optimisation revient à examiner les voies et moyens pour rendre attractive la communication sur IP en vue d'amener les entreprises à se l'approprier.

Structure de mémoire

Ce mémoire est composé en cinq chapitres :

Dans le premier chapitre intitulé " Généralités sur les réseaux informatiques " nous permet d'avoir une idée sur les réseaux informatiques, et comprendre les architectures d'un réseau, les différents équipements et les techniques de transmission sur ces réseaux.

Le deuxième chapitre intitulé " Les réseaux IP " 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 classes d'adresses IP.

Le chapitre 3 " La voix sur les réseaux IP " illustre les principes de base de la VoIP, des définitions importantes, l'adressage IP, ainsi que les différents protocoles utilisé dans la VoIP (H323 et SIP).

Le chapitre 4 " Présentation du serveur FreePBX " introduit des notions générales sur le serveur FreePBX, ses versions, ses principaux services aisi que les différents matériels qui l'utilisent.

Le dernier chapitre présente une étude technique et mise en place d'une solution VoIP basée sur le serveur FreePBX avec le protocole SIP.

Chapitre 1

Généralités sur les réseaux informatiques

1.1 Introduction

Les réseaux informatiques ont objectif de permettre l'exploitation à distance de systèmes informatiques et établir une transmission rapide et fiable d'informations entre les utilisateurs du système information.

Dans ce premier chapitre, nous allons voir quelques notions de base, pour une meilleure compréhension de l'avancement du sujet posé.

1.2 Définition d'un réseau informatique

Un réseau informatique est l'interconnexion de deux ou plusieurs ordinateurs ou autres appareils électroniques, grâce à des liens physiques, permettant l'échange de données et le partage de ressources communes.

1.3 Objectifs d'un réseau informatique

a) Le partage de ressources :

C'est le fait de rendre des ressources tels que les données, les périphériques, les programmes accessibles dans un réseau informatique.

b) La fiabilité :

Dans un réseau informatique la fiabilité c'est l'assurance que toutes les données envoyées sont arrivées au bon destinataire, sans aucune perte ou modification.

c) La réduction des coûts :

Consiste à trouver le meilleur rapport performance/prix dans l'architecture réseau. Elle permet de réaliser des économies dans le budget investi dans de nouvelles technologies pour le développement de l'entreprise.

1.4 Les types de réseaux

Généralement, les réseaux sont catégorisés en différents types, en fonction du mode de transmission des données et de leur portée.

1.4.1 Les modes de transmission

Concernant les modes de transmission, on distingue les réseaux filaires et les réseaux sans fil :

- a) **Réseaux filaires** : Ce type de réseaux utilise des câbles Ethernet pour relier des ordinateurs et des périphériques grâce à un routeur ou à un commutateur. On qualifie souvent ce réseau de rapide, fiable et sécurisé. [1]
- b) **Réseaux sans fil** : Les différents postes de ce type de réseau sont interconnectés entre eux par des ondes radio, ils utilisent la norme IEEE 802.11, mieux connue sous le nom de Wi-Fi, par contre les réseaux sans fil sont peu fiables et moins sécurisés, et la vitesse de transmission de données entre les équipements est faible. [1]

1.4.2 La portée

Il existe différents types de réseaux, selon leur portée et leur vitesse de transfert de données, On peut distinguer trois types de réseaux selon portée :

- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

- a) **LAN : Local Area Network** C'est un réseau local permettant de relier des ordinateurs et des périphériques situés à proximité les uns des autres, Il est dans un espace limité, son taux de transmission des données est élevé, Il est au minimum de 10 Mbits/s. [1]

- b) **MAN : Metropolitan Area Network** Un réseau métropolitain (MAN) est similaire à un réseau local (LAN) mais couvre une ville ou un campus entier. C'est une série de réseaux locaux permettant de relier plusieurs LAN géographiquement à proximité. Donc, ils sont plus grands que les LAN mais plus petits que les réseaux étendus (WAN). [1]
- c) **WAN : Wide Area Network** Un réseau est dit WAN lorsque la distance entre deux stations situées dans des lieux différents atteint au maximum quelques centaines de kilomètres, la vitesse de transmission d'un réseau étendu est généralement moins grande que celle d'un réseau local. [1]



FIGURE 1.1 – Classification des réseaux selon la portée

1.5 Les topologies des réseaux

1. **Topologie en bus :** C'est la topologie physique la plus simple, dans cette topologie, tous les nœuds sont connectés via un seul câble. Le support de transmission utilisé dans ce cas est le câble coaxial ou le câble RJ 45. [2]

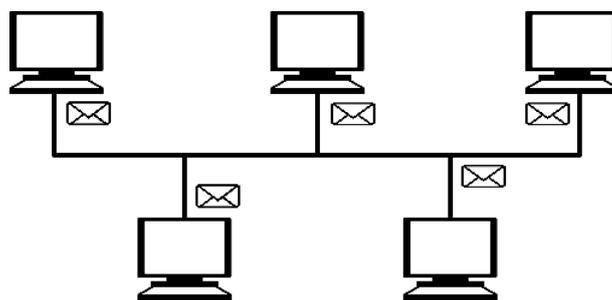


FIGURE 1.2 – Topologie en bus

les avantages :

- Facile à mettre en œuvre.
- Economique en câble.
- La panne d'une station est sans conséquence.

les inconvénients :

- Un seul ordinateur peut envoyer un signal à la fois.
- Défaillance du réseau en cas de panne du support.
- Sécurité faible.

2. **Topologie en anneau :** Dans cette topologie chaque appareil est connecté à ses deux appareils voisins exactement, comme des points sur un cercle qui forme une structure en anneau. Cette configuration est moins exigeante en câblage, elle est donc plus facile à mettre en œuvre et pour un coût inférieur. [2]

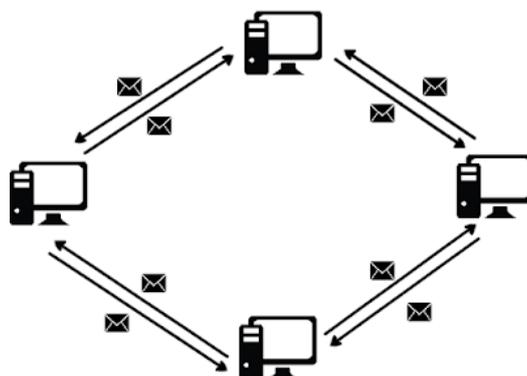


FIGURE 1.3 – Topologie en anneau

les avantages :

- Evite la gestion des collisions.
- Facile à installer.

les inconvénients :

- Performance réduite pour chaque nœud supplémentaire.
- Le retrait ou la panne d'une unité active paralyse le trafic du réseau.

3. **Topologie en étoile :** Une topologie en étoile est une topologie dans laquelle tous les nœuds sont connectés à un périphérique central (Hub ou Switch), formant ainsi une étoile. [2]

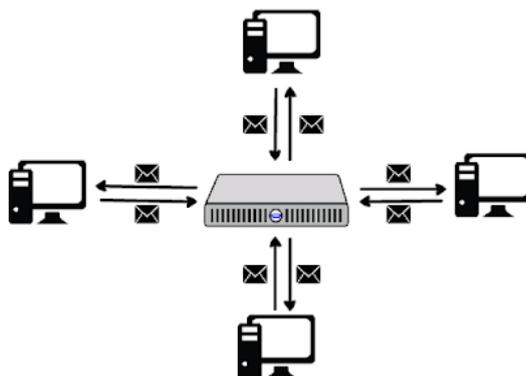


FIGURE 1.4 – Topologie en étoile

les avantages :

- Localisation facile des pannes.
- Le débranchement d'une connexion ne paralyse pas le reste du réseau.
- Les performances sont en fonction du terminal ou du nœud central.

les inconvénients :

- Repose entièrement sur le nœud central.
- Coût élevé pour les réseaux étendus.

4. **Topologie maillée :** Une topologie maillée est une topologie de réseau dans laquelle tous les nœuds de réseau sont connectés les uns avec les autres, dans cette topologie la sécurité et la confidentialité sont assurés. [2]

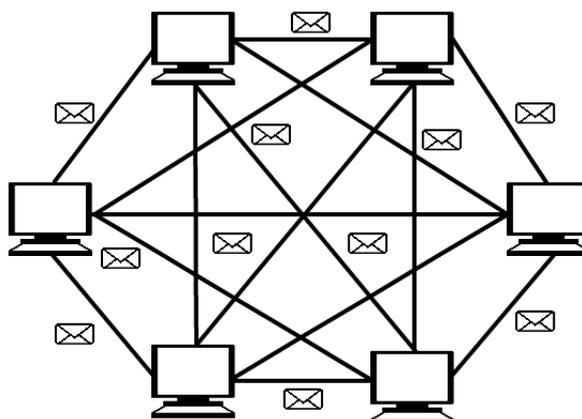


FIGURE 1.5 – Topologie maillée

5. **Topologie hybride :** C'est le regroupement de plusieurs topologies différentes, par exemple, Internet est un réseau hybride car il relie des réseaux en anneau avec des réseaux en bus, avec des réseaux en étoile. [2]

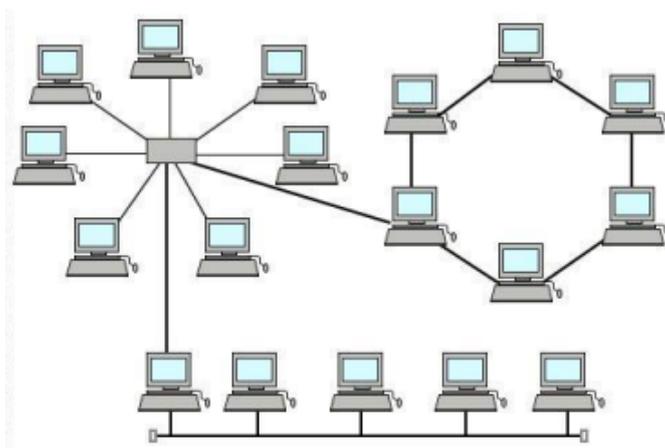


FIGURE 1.6 – Topologie hybride

1.6 Les architectures des réseaux informatiques

1.6.1 Architecture poste-à-poste

L'architecture poste-à-poste permet de mettre en place un réseau avec un coût minimal, son principe est de relier les postes entre eux en utilisant une topologie physique, tel que chaque utilisateur du réseau est libre de partager ses ressources. [1]

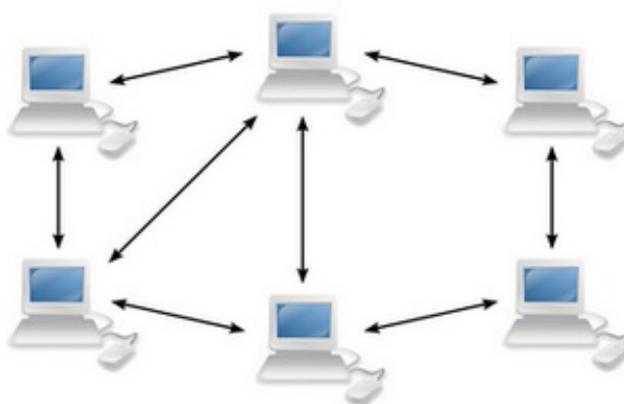


FIGURE 1.7 – Architecture poste-à-poste

L'architecture poste-à-poste a tout de même quelques avantages :

- C'est une architecture très simple.
- Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.

Le réseau poste à poste a énormément d'inconvénients :

- Si un poste est éteint ou il se plante, ses ressources ne sont plus accessibles.
- La sécurité est peu présentée.

1.7 Composants matériels d'un réseau

1.7.1 Equipements d'interconnexion

Voici les équipements qui peuvent entrer dans la composition d'un réseau d'entreprise : [3]

- **La carte réseau :** La carte réseau constitue l'interface physique entre l'ordinateur et le support de communication. Pour qu'un ordinateur soit mis en réseau, il doit être muni d'une carte réseau.
- **Le concentrateur :** Le concentrateur (appelé Hub en anglais) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Son rôle c'est de diffuser la donnée sur l'ensemble des ports.
- **Le répéteur :** Le répéteur est un équipement utilisé pour régénérer le signal entre deux nœuds du réseau, pour étendre la distance du réseau. On peut l'utiliser aussi pour relier des câbles de même type et de types différents.
- **Les ponts :** Le pont (bridge) est un équipement matériel qui permet de relier des réseaux qui utilisent le même protocole, il sert généralement à faire transférer des paquets entre deux réseaux de même type.
- **Le commutateur :** Comme le concentrateur, le commutateur (en anglais Switch) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Sa seule différence avec le Hub, c'est qu'il est capable de connaître l'adresse physique des machines qui lui sont connectées et d'analyser les trames reçues pour les diriger vers la machine de destination.
- **La passerelle :** La passerelle permet à des architectures réseau différentes de communiquer entre elles. La passerelle la plus connue est la « box Internet » qui relie un réseau local privé à Internet.
- **Le routeur :** Un routeur est un équipement matériel informatique dont la fonction principale consiste à orienter les données à travers un réseau, il permet de faciliter

l'accès aux ressources disponibles sur le réseau pour les utilisateurs et de faire circuler des données entre deux interfaces réseau.

- **Le modem** : Le modem est un périphérique qui permet de transmettre et de recevoir les données sous forme de signal. Il transforme les signaux analogiques et numériques et inversement, ces signaux sont acheminés par une ligne téléphonique.

1.7.2 Les supports de transmissions

- a) **Le câble coaxial** : Le câble coaxial est composé d'un fil de cuivre entouré successivement d'une gaine d'isolation, d'un blindage métallique et d'une gaine extérieure.
- Vitesse et débit : 10 à 100Mbit/s.
 - Longueur de câble maximale : 500 m.
 - Coût : économique. [4]

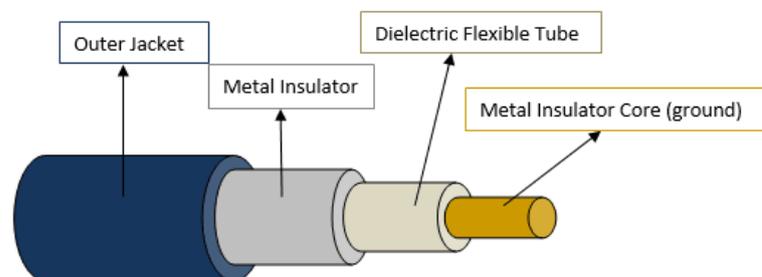


FIGURE 1.8 – Câble coaxial

b) **Le câble à paires torsadées** : il s'agit d'un câble constitué au moins de deux brins de cuivres attachés en torsade (le cas d'une paire torsadée) et recouverts d'isolants.

En réseau informatique, on distingue deux types de câbles à paires torsadées STP et UTP. [4]

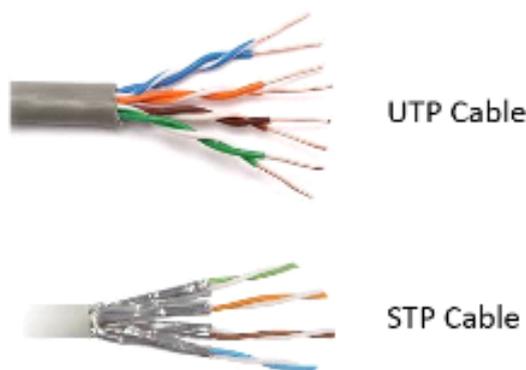


FIGURE 1.9 – Câbles à paires torsadées

c) **Le câble fibre optique** : C'est un câble qui permet de transmettre des données sous forme de signal lumineux avec un débit nettement supérieur à celui des autres supports de transmissions filaires. La fibre optique est constituée du cœur, d'une gaine optique et d'une enveloppe protectrice. [4]

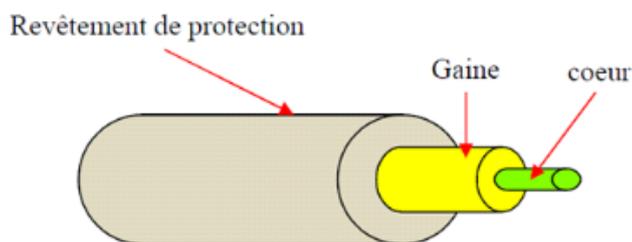


FIGURE 1.10 – Câble fibre optique

1.7.3 Les périphériques finaux

Dans un réseau informatique, les périphériques finaux sont appelés hôtes. Parmi ces périphériques on retrouve :

- Les Ordinateurs.
- Les Imprimantes réseau.
- Les Téléphones VoIP.
- Les Caméras de surveillance.
- Les Appareils mobiles.
- Les Serveur (physique ou virtuel).

1.8 Le modèle de référence OSI

1.8.1 Définition

Le modèle OSI (Open System Interconnexion) ou Interconnexion des Systèmes Ouverts est un modèle mis en place par l'ISO (International Standard Organisation) qui communique entre applications d'un réseau.

Il a été mis au point pour aider les fournisseurs et les développeurs à créer des solutions de communication numériques et pour faciliter les comparaisons entre les outils de communication. [5]

1.8.2 Les différentes couches

L'architecture de modèle OSI est défini sur 7 couches : [5]

- **La couche physique** : C'est la première couche du modèle OSI, elle est chargée de la transmission des bits sur le réseau au niveau électrique, optique ou radio.

- **La couche liaison de données :** c'est la deuxième couche du modèle OSI, elle permet de gérer les liaisons sur le réseau physique. Elle est divisée en deux sous-couches : contrôle de la liaison logique, ou LLC et contrôle d'accès au support, ou MAC, la couche de liaison de données est également responsable du contrôle de flux et du contrôle d'erreur dans les communications réseau.
- **La couche réseau :** c'est la couche 3 du module OSI son rôle principal est de faciliter le transfert de données entre deux réseaux différents, cette couche décompose les segments de la couche transport en unités plus petites, appelées paquets, et ensuite les réassemble. Elle trouve également le meilleur chemin physique pour que les données atteignent leur destination : c'est ce qu'on appelle le routage.
- **La couche transport :** cette couche est responsable de la communication de bout en bout entre les deux appareils, en récupérant les données de la couche session et les découper en morceaux appelés segments avant de les envoyer à la couche réseau. La couche de transport est également responsable du contrôle de flux et du contrôle d'erreur.
- **La couche de session :** C'est la couche responsable de l'ouverture et de la fermeture de la communication entre les deux appareils, elle synchronise également le transfert de données avec les points de contrôle.
- **La couche de présentation :** Cette couche est principalement responsable de la préparation des données pour les utiliser par la couche applicative, elle est responsable de la traduction, du chiffrement et de la compression des données.
- **La couche applicative :** C'est la dernière couche du modèle OSI, elle est la seule couche qui interagit directement avec les données de l'utilisateur. Les protocoles de la couche applicative incluent HTTP et SMTP.

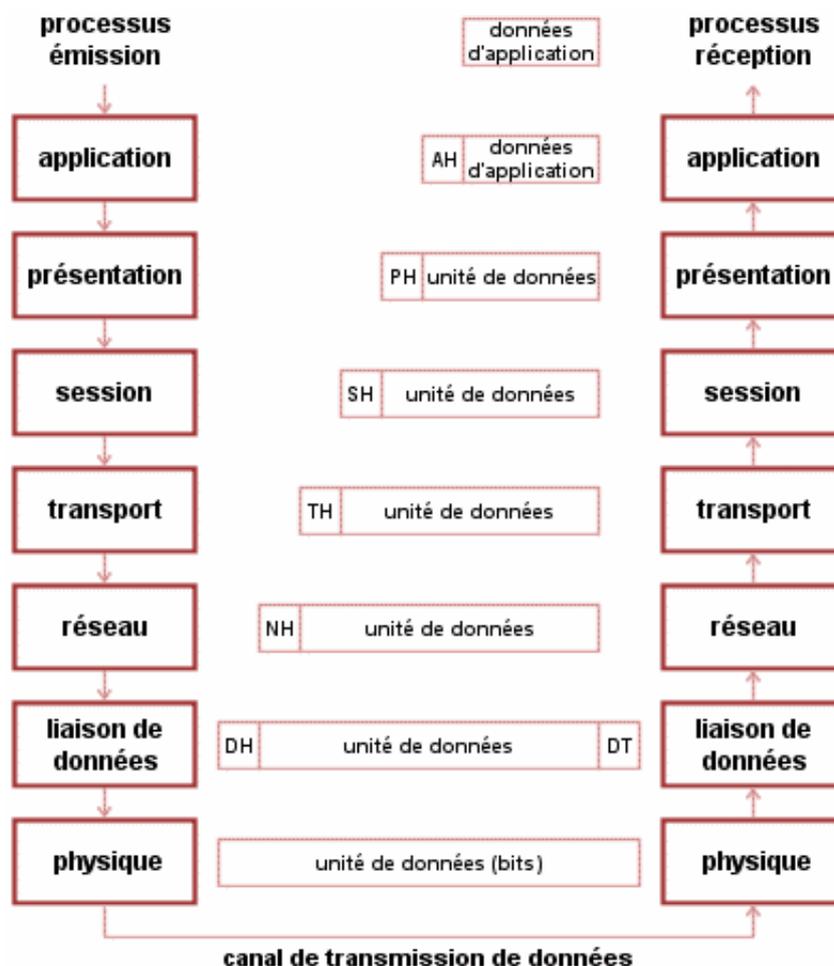


FIGURE 1.11 – Le modèle de référence OSI

1.9 Conclusion

Au cours de ce chapitre, nous avons parcouru des généralités sur les réseaux informatiques, leurs notions et leurs aspects élémentaires, à savoir les outils d'interconnexion, les classifications des réseaux. Aussi, il nous a permis de voir quelques notions sur le modèle de référence OSI.

Le prochain chapitre, sera consacré aux réseaux IP.

Chapitre 2

Les réseaux IP

2.1 Introduction

Internet est un regroupement de réseaux formé de milliers d'ordinateurs, c'est le plus grand réseau d'informations dans le monde, internet fonctionne selon plusieurs lois appelées protocoles, TCP/IP est le plus connue et la plus utilisée.

Dans ce chapitre nous allons voir quelques notions sur les réseaux IP.

2.2 Définition

Un réseau IP est un groupe d'ordinateurs connectés via leurs adresses Internet Protocol (IP), il permet à un ordinateur d'utiliser Internet pour communiquer avec un autre ordinateur en recueillant des informations et en les envoyant directement à l'autre. Il est implémenté dans les réseaux Internet, les réseaux locaux (LAN) et les réseaux d'entreprise.

Tous les hôtes ou nœuds du réseau doivent utiliser le protocole TCP/IP pour fonctionner, chaque ordinateur connecté au réseau possède sa propre adresse IP permettant l'envoi des informations directement vers leurs destination.

2.3 Le modèle TCP/IP

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

TCP/IP est un protocole de 4 couches qui permet à une machine de communiquer avec une autre machine via Internet. Chacune de ces couches fournit des services bien précis aux couches supérieures, son rôle consiste à compiler des paquets de données et à les envoyer au bon destinataire. [6]

2.3.1 Les différentes couches du modèle TCP/IP

Le modèle TCP/IP, est construit sur un modèle en couches moins complet que le modèle OSI. Quatre couches sont suffisantes pour définir l'architecture de ce modèle :

- **La couche d'application** : La couche application regroupe les 3 couches application, présentation et session du modèle OSI. 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. [6]
- **La couche transport** : Ses 2 principaux protocoles sont UDP, le protocole de base de la couche transport et TCP qui assure le contrôle et le transport des données, ces protocoles peuvent résoudre des problèmes comme la fiabilité des échanges et assurer que les données arrivent dans l'ordre correct. [6]
- **La couche internet** : cette couche s'occupe de l'acheminement de données à travers un seul réseau ou entre 2 réseaux. C'est la couche qui définit et établit internet. Le principal protocole de cette couche est le protocole Internet, ou IP, qui définit les adresses IP propres à chaque ordinateur. La version la plus récente est IPv6. [6]
- **La couche accès réseau** : La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, elle contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau. [6]

APPLICATION HTTP, FTP, DNS, ...
TRANSPORT TCP, UDP
INTERNET IP
ACCÈS RÉSEAU WIFI, ATM, PPP, ...

TABLE 2.1 – Les couches du modèle TCP/IP

2.3.2 Les protocoles de chaque couche

a) Les protocoles de la couche application :

La couche application utilise plusieurs protocoles, parmi ces protocoles on retrouve :

- **Le protocole http** : HTTP (HyperText Transfer Protocol) est un protocole de communication entre client et serveur développé pour le web.
- **Le protocole FTP** : Le protocole FTP (File Transfer Protocol) permet d'assurer le transfert de fichiers de façon indépendante des spécificités des OS (Operating System).
- **Le protocole SMTP (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.

b) Les protocoles de la couche transport :

- **Le protocole UDP (User Datagram Protocol) :** défini en 1980, est un protocole permettant l'envoi sans connexion de données dans des réseaux basés sur le protocole IP, il n'effectue pas de contrôle d'erreur, il est alors appelé mode non connecté, il est donc peu fiable, les domaines d'application typiques de l'UDP sont donc les requêtes DNS, les connexions VPN et le streaming audio et vidéo.
- **Le protocole TCP (Transfert Control Protocol) :** adopté en 1983, est un protocole orienté connexion qui garantit que les données sont remises de façon fiable en effectuant un contrôle des données et en effectuant une réémission pour les données qui n'ont pas pu être transférées, il gère aussi le multiplexage, c'est à dire que plusieurs applications peuvent utiliser simultanément les services du protocole TCP.

c) Les protocoles de la couche Internet : La couche internet utilise plusieurs protocoles, parmi ces protocoles on retrouve :

- **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, cette technique est appelée commutation de paquets.
- **Le protocole ARP (Adresse Resolution Protocol) :** est un protocole de résolution d'adresses, son objectif est de résoudre une adresse physique (MAC) par l'intermédiaire de l'adresse IP correspondante d'un host distant.
- **Le protocole ICMP (Internet Control Message Protocol) :** est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées. Il ne permet pas de corriger ces erreurs mais d'en informer les différents émetteurs des Datagrammes en erreurs.

d) Les protocoles de la couche accès réseaux :

- **Le protocole Ethernet :** Ethernet est une technologie et protocole de connexion et de communication pour les réseaux locaux et les réseaux étendus. C'est une mise en réseau filaire avec des câbles RJ45 qui relie des équipements.
- **Le protocole WIFI :** c'est un ensemble de protocoles de communication sans fil créée par les normes du groupe IEEE 802.11. Un réseau Wi-Fi permet de relier sans fil plusieurs appareils informatiques au sein d'un réseau informatique.

2.4 L'adressage IP

Une adresse IP (Internet Protocol) est une représentation numérique qui identifie de façon unique un hôte donnée sur le réseau auquel il appartient, chaque adresse IP contient donc deux informations élémentaires, une adresse de réseau et une adresse d'hôte, deux versions d'IP sont utilisées à l'heure actuelle : IPv4 (32 Bits) et IPv6 (128 Bits). [7]

	IPV4	IPV6
Espace d'adressage	Une adresse sur 32 bits	Une adresse sur 64 bits
Structure de l'adresse	4 mots (X.X.X.X)	8 mots (X.X.X.X.X.X.X.X)
Notation	Décimale pointée	Hexadécimale pointée
Définition d'un mot	1 mot= 1 octect= 8 bits	1 mot= 2 octect= 16 bits
Possibilité par mot	2 puissance 8 = 256	16 puissance 4 = 65536

TABLE 2.2 – IPV4 VS IPV6

On distingue deux types d'adresse IP :

- **Les adresses privées :** que tout administrateur de réseau peut s'attribuer librement pourvu qu'il ne cherche pas à les router sur Internet.
- **Les adresses publiques :** délivrées par une structure mondiale qui en assurent l'unicité.

2.4.1 Composition d'une adresse ipv4

À la différence des adresses physiques, les adresses réseaux ou adresses IP sont attribuées par les administrateurs réseau et sont configurées logiquement.

L'adresse IP comporte pour commencer deux parties principales :

Une partie réseau (net ID) qui est l'adresse réseau logique du sous réseau auquel l'ordinateur sera attaché.

Une partie hôte (host ID) qui est l'adresse logique du périphérique logique identifiant un ordinateur donné sur un sous réseau. [7]

2.5 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. [7]

Partie réseau	Partie hôte		
0xxxxxxx	Xxxxxxxx	Xxxxxxxx	Xxxxxxxx

TABLE 2.3 – Structure d'adresses de 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. [7]

Partie réseau		Partie hôte	
10xxxxxx	Xxxxxxxx	Xxxxxxxx	Xxxxxxxx

TABLE 2.4 – Structure d'adresses de 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. [7]

Partie réseau			Partie hôte
110xxxxx	xxxxxxx	xxxxxxx	xxxxxxx

TABLE 2.5 – Structure d'adresses de 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). [7]

Adresse multidiffusion			
111xxxxx	xxxxxxx	xxxxxxx	xxxxxxx

TABLE 2.6 – Structure d'adresses de 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. [7]

2.5.1 Les sous-réseaux

Un sous-réseau est un sous-ensemble d'un réseau de classe, son utilisation dans un réseau IP permet de diviser un grand réseau en plusieurs sous-réseaux, ils sont utilisés lorsque la charge du réseau doit être réduite et mieux distribuée, dans ce cas, plusieurs adresses IP sont regroupées au sein d'un sous-réseau. [7]

La figure ci-dessous représente une décomposition d'un réseau en sous-réseaux :

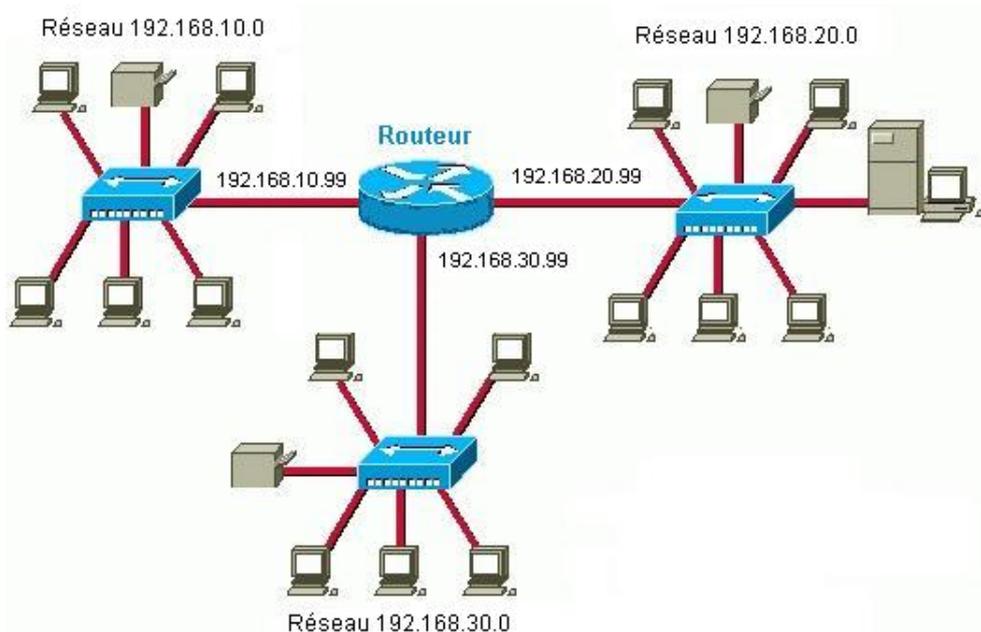


FIGURE 2.1 – Exemple d'un sous-réseaux

2.5.2 Le masque sous-réseau

Le masque de sous réseau permet de savoir qu'elle est la partie de 32 bits qui est utilisé pour identifier le réseau, les bits du masque de sous réseau sont à 1 pour indiquer « la partie réseau » et sont à 0 pour indiquer la partie station. [7]

Pour identifier une station sur le réseau Internet, il faut connaître deux adresses :

- Le masque de sous réseau.
- L'adresse IP.

Exemple :

- L'adresse IP : 192.168.20.7
- Le masque de sous réseau : 255.255.255.0
- La partie réseau : 192.168.20.0
- La partie station : 0.0.0.7

2.5.3 L'adresse de diffusion (Broadcast)

Une adresse de diffusion est une adresse IP (Internet Protocol) spéciale utilisée pour transmettre des messages et des paquets de données aux systèmes de réseau, les administrateurs réseau vérifient la transmission réussie des paquets de données via les adresses de diffusion.

[7]

2.6 Le routage

Le routage est le processus qui permet d'acheminer un datagramme IP de son hôte émetteur jusqu'à son hôte destinataire, chaque datagramme est routé indépendamment des autres.

Les routeurs se réfèrent à des tables de routage internes pour prendre des décisions d'acheminement des paquets dans le réseau. Une table de routage enregistre les chemins que les paquets doivent emprunter pour atteindre chaque destination dont le routeur est responsable. [8]

2.6.1 Types de routage

Il existe trois types de routage :

- a) **Le routage statique** : Le routage statique est également connu sous le nom de routage non adaptatif. C'est une technique dans laquelle l'administrateur ajoute manuellement les routes dans une table de routage. [8]

— **Avantage** : Aucune surcharge de routage pour le processeur du routeur.

— **Désavantage** : difficulté de l'ajout manuel de route pour le réseau dans la table de routage.

b) Le routage dynamique : Également connu sous le nom de routage adaptatif, le routage dynamique effectue un ajustement automatique des routes en fonction de l'état actuel de la route dans la table de routage, il utilise des protocoles pour découvrir les destinations du réseau et les routes pour l'atteindre. RIP, OSPF et EIGRP sont les meilleurs exemples de protocole de routage dynamique. [8]

— **Avantage :**

- Facile à configurer.
- Plus efficace pour sélectionner le meilleur itinéraire vers un réseau distant de destination et également pour découvrir un réseau distant.

— **Désavantage :**

- Consomme plus de bande passante pour communiquer avec d'autres voisins.
- Moins sécurisé que le routage statique.

c) Le routage par défaut : La route par défaut est utilisée quand la table de routage ne dispose pas d'une entrée correspondant au réseau de destination recherché. Le concept de route par défaut est très utile pour les routeurs qui ne disposent que d'un seul choix pour expédier les paquets. [8]

2.7 Le network address translation (NAT)

NAT (network adresse translation) est un processus de modification des adresses IP et des ports source et de destination, ce processus est généralement effectué par des routeurs ou des pare-feu. Il existe trois types de traduction d'adresses : [9]

- **NAT statique :** traduit une adresse IP privée en une adresse publique. L'adresse IP publique est toujours la même. [9]
- **NAT dynamique :** traduit une adresse IP privée en un ensemble d'adresses publiques. [9]
- **Traduction d'adresse de port (PAT) :** une adresse IP publique est utilisée pour tous les

périphériques internes, mais un port différent est attribué à chaque adresse IP privée, il est également connu sous le nom de surcharge NAT. [9]

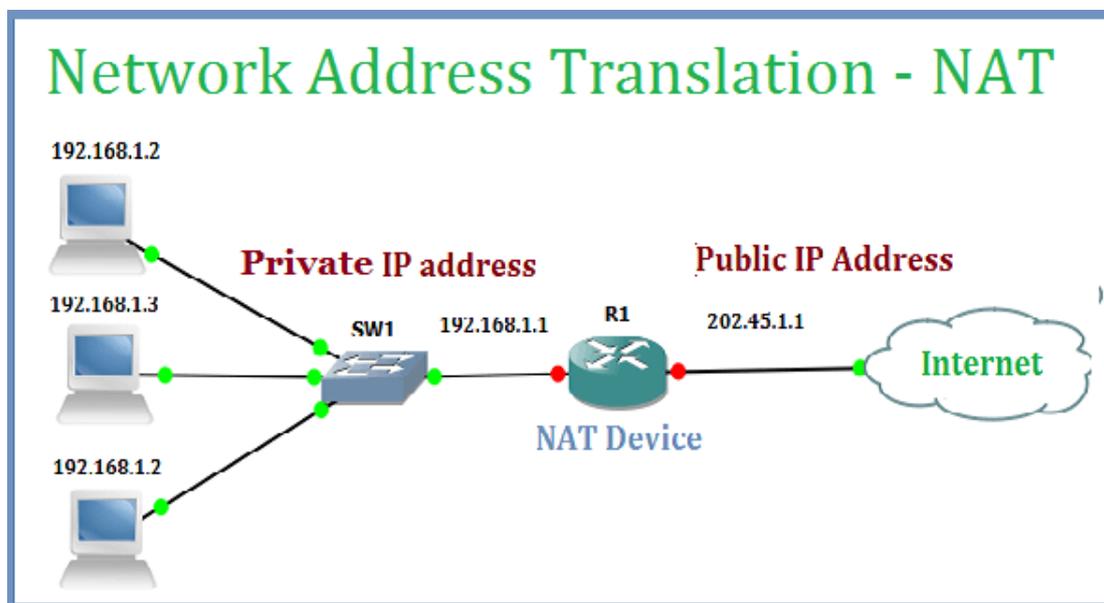


FIGURE 2.2 – Le NAT

2.8 Le DNS (domain name system)

Le serveur DNS (Domain Name System) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Le serveur DNS permet d'associer à site web (ou un ordinateur connecté ou un serveur) une adresse IP, la plupart des autres activités sur Internet s'appuient sur DNS pour disposer rapidement des informations nécessaires permettant aux utilisateurs d'accéder aux hôtes distants.

2.8.1 Types de service DNS

On retrouve deux types de service DNS différents sur Internet, chacun de ces services traite différemment les requêtes DNS, selon leurs fonctions :

- **DNS récursif** : un serveur DNS récursif est un serveur de système de noms de domaine qui prend les demandes de nom de site Web des utilisateurs et vérifie les enregistre-

ments obtenus à partir des serveurs DNS faisant autorité pour l'adresse IP associée.

- **Serveur DNS faisant autorité** : un serveur DNS faisant autorité contient le résultat de la requête DNS, celui-ci n'a pas besoin d'interroger un autre serveur.

2.9 Le DHCP (dynamics host configuration protocol)

dynamic host configuration protocol (DHCP) est un protocole de gestion de réseau utilisé pour automatiser le processus de configuration des périphériques sur les réseaux IP, leur permettant ainsi d'utiliser des services réseau tels que DNS, NTP et tout protocole de communication basé sur UDP ou TCP. Un serveur DHCP attribue dynamiquement une adresse IP et d'autres paramètres de configuration réseau à chaque périphérique sur un réseau pour qu'ils puissent communiquer avec d'autres réseaux IP. [10]

2.9.1 Fonctionnement de DHCP

DHCP fonctionne au niveau de la couche application, son rôle est d'attribuer dynamiquement l'adresse IP au client et cela se produit par l'échange d'une série de messages appelés transactions DHCP ou conversation DHCP :

- **DHCP discovery** : Le client DHCP diffuse des messages pour découvrir les serveurs DHCP et l'ordinateur client envoie un paquet ensuite avec la destination de diffusion par défaut. [10]

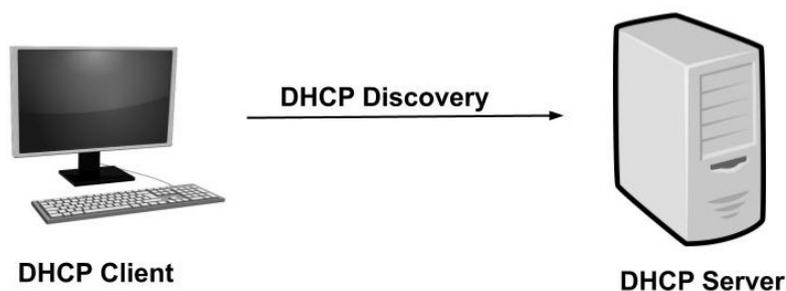


FIGURE 2.3 – DHCP discover

- **DHCP Offer** : Lorsque le serveur DHCP reçoit le message DHCP Discover, il propose une adresse IP au client en envoyant un message d'offre DHCP au client, Ce message d'offre DHCP contient l'adresse IP proposée pour le client DHCP, l'adresse IP du serveur, l'adresse MAC du client, le masque de sous-réseau, la passerelle par défaut, l'adresse DNS. [10]

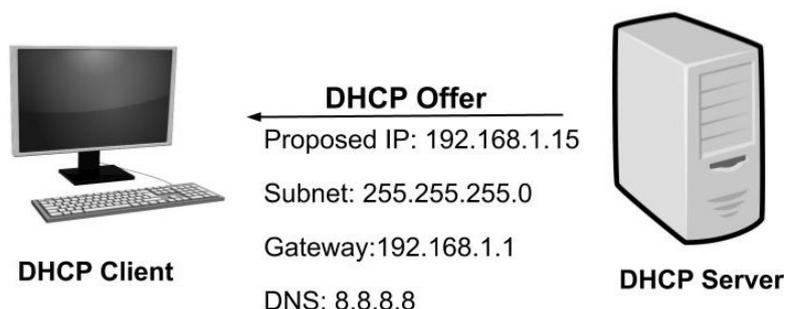


FIGURE 2.4 – DHCP offer

- **DHCP request** : Dans la plupart des cas, le client peut recevoir plusieurs offres DHCP, en réponse à l'offre, le client envoie une requête DHCP demandant l'adresse offerte à l'un des serveurs DHCP, toutes les autres adresses IP proposées par les serveurs DHCP restants sont retirées. [10]

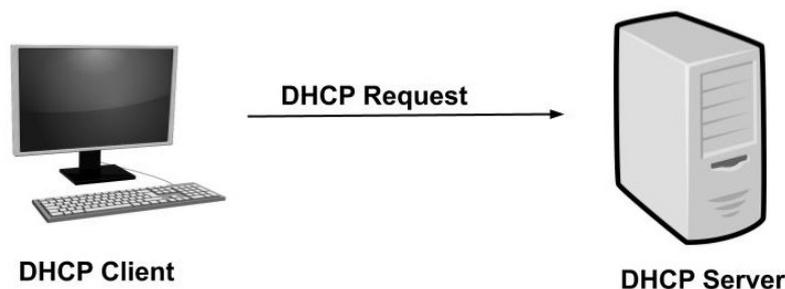


FIGURE 2.5 – DHCP request

- **DHCP ACK** : Le serveur envoie ensuite un accusé de réception au client qui confirme le bail DHCP au client. À cette étape, la configuration IP est terminée et le client peut utiliser les nouveaux paramètres IP. [10]

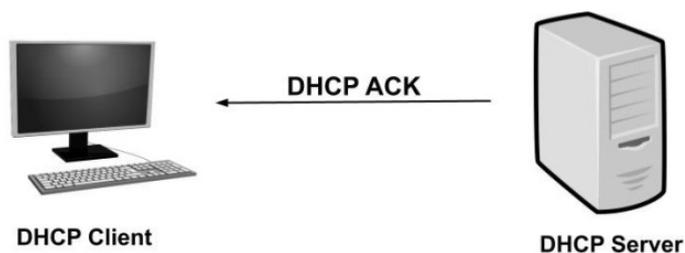


FIGURE 2.6 – DHCP ACK

2.10 Conclusion

Nous avons présenté de manière générale les réseaux IP, ainsi que le modèle TCP/IP, 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 3

La voix sur les réseaux IP

3.1 Introduction

La voix sur les réseaux IP est un ensemble de technologies qui révolutionne depuis une vingtaine d'année les communications entre individus et au sein des entreprises. Dans ce chapitre nous allons aborder en détail le fonctionnement de la VoIP, ainsi que les différents protocoles qu'elle utilise.

3.2 Définition

La VoIP (Voice Over Internet Protocol), veut dire transmission de la voix par Internet, c'est une technologie qui permet la communication par voix via le réseau Internet (IP).

On distingue :

- **La voix sur IP** : transmission de la parole sur un réseau internet IP.
- **La téléphonie sur IP** : en plus de la parole, les fonctions téléphoniques (signalisation, fax, multi appel) sur un réseau internet IP.

La VoIP n'offre pas que le service de la transmission de la voix, mais, grâce à la VoIP, il est possible d'émettre et de recevoir aussi des messages vocaux, des emails, un fax, de créer un répondeur automatique, d'assister à une conférence audio et vidéo.

3.3 Téléphonie classique vs Téléphonie sur IP

- **La Téléphonie classique** La téléphonie classique utilise le réseau à commutation de circuits ou le réseau téléphonique commuté (RTC), pour chaque communication il faut réserver un circuit logique entre les deux correspondants. Les informations de la session de communication empruntent le même chemin pour atteindre la destination. Aussi, les tarifs des communications sont assez élevés, la figure (3.1) illustre un réseau téléphonique comuté. [11]

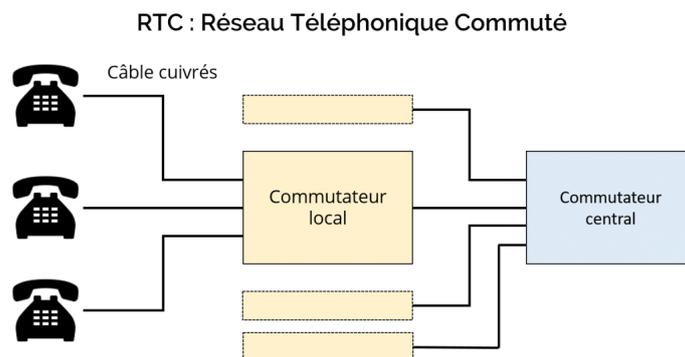


FIGURE 3.1 – Réseau téléphonique comuté

— **La téléphonie sur IP** La téléphonie sur IP utilise, par contre, les réseaux à commutation de paquets ou réseaux IP, les messages ou les informations à transporter sont alors découpés en fragments de petite taille, appelés paquets. Chaque paquet est transporté dans le réseau indépendamment des autres.

Les paquets provenant de différentes sources sont envoyés sur un même circuit, ce qui permet d’optimiser l’utilisation des ressources. En ce qui concerne ce type de communications, les coûts ne sont pas élevés. [11]

3.4 Principes et fonctionnement de la VoIP

Le principe consiste à numériser la voix analogique et l’acheminer dans des paquets IP sur Internet ou n’importe quel autre réseau IP. Le processus de communication VoIP est illustré dans la figure 3.2 : [12]

— **Acquisition du signal** : La première étape consiste naturellement à capter la voix à l’aide d’un micro, qu’il s’agisse de celui d’un téléphone ou d’un micro casque, la voix qui est un signal analogique utilise une bande de fréquence moyenne d’environ 200 Hz. [12]

— **Numérisation** : La voix ou la parole téléphonique est un signal analogique. Pour être acheminée sur un réseau IP, il faut donc la convertir en un signal ou données numériques (binaire) à l’aide d’un Codec (codeur /décodeur). Pour ce faire, le signal est

d'abord échantillonné à une vitesse ou rythme très élevé (au moins 8000 fois par seconde), puis transformé en un signal numérique par un convertisseur A/D (Analogique/Digital), le temps de numérisation est généralement négligeable. [12]

- **Compression** : Les données numériques sont ensuite traitées par un DSP (Digital Signal Processor) afin de réduire leur taille selon une certaine norme de compression. Ceci a pour avantage d'optimiser la bande passante nécessaire à leur transfert sur un réseau IP.[12]
- **habillage des en-têtes** : Elle consiste en la mise en paquet des éléments binaires issus de la numérisation du signal analogique (la voix). Dès qu'un paquet est plein, il est émis à son destinataire. [12]
- **Emission et transport** : Les paquets IP qui encapsulent des données vocales sont alors acheminés à travers Internet ou n'importe quel autre réseau IP, les données arrivent à destination après un temps qui dépend de la quantité de données émises et du débit auquel fonctionnent les liens entre l'émetteur et le récepteur.[12]
- **Réception** : Lorsque les paquets arrivent à destination, ils sont remis dans le bon ordre (l'ordre initial) assez rapidement pour éviter la dégradation de la voix.[12]
- **Conversion D/A** : C'est l'inverse de l'étape de numérisation, c'est-à-dire le flux de données digitales est à nouveau reconverti en un signal analogique.[12]
- **Restitution** : La voix peut être retranscrite par les hauts parleurs d'un combiné téléphonique ou de l'ordinateur par exemple.

[12]

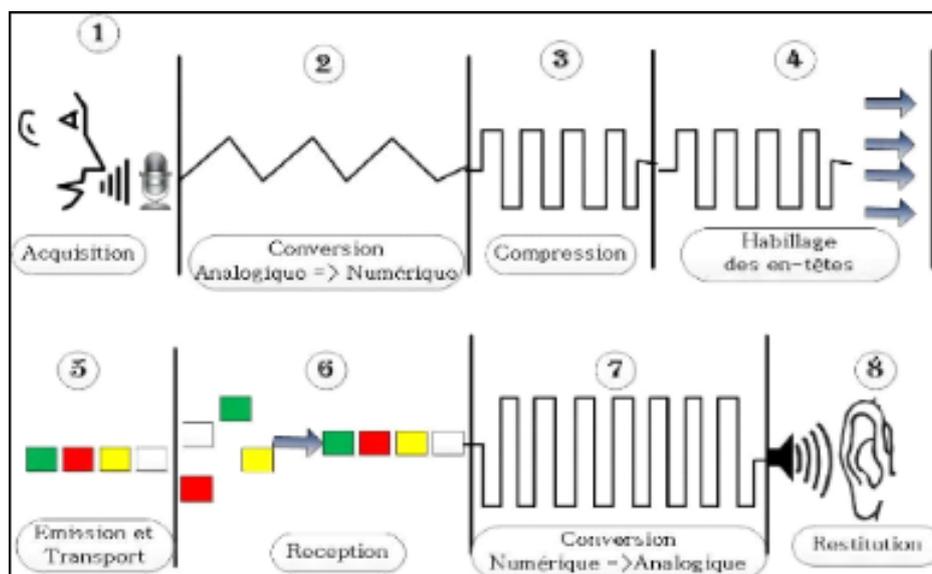


FIGURE 3.2 – Fonctionnement de la VoIP

3.5 Les protocoles utilisés par la VoIP

3.5.1 Les protocoles de transport

Le protocole TCP exige de nombreuses procédures de contrôle, ce qui le rend peu adapté au transport des données multimédias ayant de fortes contraintes de délai. À l'inverse, le protocole UDP ne propose aucun mécanisme de contrôle, mais la séquence temporelle originale ne peut être reconstituée au niveau du récepteur.

3.5.1.1 Le protocole RTP (Real-time Transport Protocol)

Le protocole RTP est un protocole de communication, il est utilisé pour transporter les données qui ont généralement de fortes contraintes temporelles, comme la voix ou la vidéo dans la VoIP, il assure que les paquets IP qui seront transmis sont correctement reconstitués chez le destinataire de la communication, le protocole RTP est utilisé sur UDP, il a été développé et standardisé par l'IETF en 1996 dans la RFC 1889, qui est aujourd'hui remplacée par la RFC 3550. [13]

a) Fonctionnalités du protocole RTP :

RTP est un protocole de communication qui a été proposé principalement pour enrichir les fonctions du protocole UDP de telle sorte qu'il puisse assurer la reconstitution de l'ordre de flux d'origine, ses principales fonctionnalités sont :

- **Synchronisation des flux :** RTP ajoute aux paquets une estampille (l'horodatage) pour indiquer le moment d'envoi du paquet, si l'audio et la vidéo sont transmis séparément dans des paquets différents, car la lecture par le destinataire de la séquence audio doit impérativement coïncider avec la séquence de la vidéo. [13]
- **Reconstitution de l'ordre et détection des pertes de paquets :** Les paquets IP sont émis indépendamment les uns des autres. Par conséquent, leur ordre de réception n'est pas forcément le même avec l'ordre d'émission. Afin d'obtenir le même ordre, un numéro de séquence qui s'incrémente progressivement est affecté à chaque paquet lors de son envoi, ce numéro permet d'un côté d'ordonner les paquets et de détecter les pertes de paquets de l'autre. [13]

b) Point fort et limite du protocole RTP :

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.), de détecter les pertes de paquet et d'identifier le contenu des paquets.

Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi, il ne garantit pas le délai de livraison. [13]

3.5.1.2 Le protocole RTCP

Le protocole RTCP (Real-time Transport Control Protocol) est un protocole de contrôle et de supervision du réseau. Il a pour objectif d'offrir aux participants d'une session une vision sur l'état du réseau et de s'y adapter de façon dynamique. Il fournit périodiquement des informations ou un rapport sur la qualité de service dans le réseau. [13]

a) Fonctionnalités du protocole RTCP :

- **L'identification des participants à une session :** en effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique. [13]
- **Le contrôle de la session :** en effet, le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement. [13]

b) Les paquets RTCP :

- **Sender Report (SR) :** Ce type de paquets véhicule un rapport de l'émetteur sous forme d'un ensemble de statistiques relatives à la qualité de service concernant l'émetteur. Parmi ces informations, on trouve le nombre de paquets perdus. [13]
- **Receiver Report (RR) :** Le paquet RR est semblable au précédent mais véhicule plutôt un rapport du récepteur. [13]
- **Source Description (SDS) :** Le paquet SDS décrit une source avec un ensemble de paramètres spécifiques tels que le nom permanent de la source, le nom du participant (NAME), son adresse e-mail (EMAIL), son numéro de téléphone (PHONE), sa localisation (LOC), ainsi que des informations sur l'application qu'il utilise. [13]
- **BYE :** Ce type de paquets est envoyé pour indiquer que l'émetteur quitte une session multimédia. [13]
- **Application (APP) :** Ce type de paquets est réservé pour transporter des paramètres spécifiques d'une application. [13]

c) Point fort et limite du protocole RTCP : Le protocole de RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanent sur une session et ses participants.

Par contre, il n'est pas proposé pour garantir une qualité de service. Donc Il ne supporte pas notamment le service : « Fiabilisation des échanges ».

Une perte de paquets est équivalente au niveau du récepteur à un silence et la garantie des délais de transit dans le réseau. [13]

3.5.1.3 Le protocoles SRTP

Le transport de la voix sur un réseau IP peut être protégé soit par des mécanismes de transport généraux tels qu'IPsec, soit par des mécanismes spécifiques comme SRTP (Secure real-time transport protocol). Ce dernier est une extension du protocole RTP qui ajoute davantage de fonctions de sécurité, comme le message d'authentification, la confidentialité et la protection anti-replay.

a) Fonctionnalités du Secure RTP : SRTP fournit des fonctionnalités de protocole RTP tout en renforçant la sécurité de la messagerie unicast et multicast, y compris les messages multimédias et la communication, comme la téléphonie Internet et la vidéoconférence. SRTP applique un algorithme AES (Advanced Encryption Standard) pour crypter et décrypter tous les messages entrants et sortants.

3.5.2 Les protocoles de Signalisation

Un protocole de signalisation permet d'établir, maintenir et fermer une communication entre deux postes (téléphoniques) terminaux. La communication téléphonique est décomposée en trois phases : la première phase permet d'avertir le destinataire, la seconde correspond au transport de la parole proprement dite, et la troisième phase consiste en la finalisation de la communication lorsqu'un des deux terminaux raccroche. Cette dernière phase utilise le même type de protocole que la première : un protocole de signalisation. Parmi ces protocoles, nous citons H.323 et SIP.

3.5.2.1 Le protocole H323

a) **Définition :** Le standard H.323 fournit, depuis son approbation en 1996, un cadre pour les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (pour International Télécommunication Union), Le protocole H.323 fait partie de la série H.23x qui traite de la vidéoconférence à travers différents réseaux.

Son architecture est constituée de quatre entités qui sont les terminaux, la passerelle, la Gatekeeper, (ou garde-barrière) et le MCU (Multipoint Control Unit). Sa gestion demeure difficile et reste peu adaptée au monde Internet. [14]

b) Le rôle de ses composants :

- **Les terminaux H.323 :** Le terminal peut être un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet.[14]
- **la passerelle :** Les passerelles H.323 assurent l'interconnexion avec les autres réseaux. Cette connectivité est établie en traduisant les protocoles destinés à l'établissement et à la libération des appels, en transformant les formats multimédias entre les différents réseaux.[14]
- **Les Gatekeeper :** Il est considéré comme le composant H.323 le plus important , le gatekeeper sert de point central pour chaque appel à l'intérieur de sa zone, tout en fournissant aux terminaux H.323 enregistrés des services de contrôle d'appel.[14]
- **La MCU :** elle offre aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus. Chaque terminal participant à une conférence établit une connexion MCU. [14]

c) Les avantages de la technologie H.323

- H.323 supporte des conférences entre trois terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée.
- H.323 n'est lié à aucun équipement ou système d'exploitation donc il est indépendant vis à vis des plates-formes et des applications.
- H.323 permet une bonne gestion de la bande passante, afin d'éviter que ces flux ne congestionnent le réseau car le trafic audio et vidéo est un grand consommateur de ressources réseau. [14]

d) Les limites de la technologie H.323

- Comprend de nombreuses options susceptibles d'être implémentées de façons différentes par les constructeurs et donc de poser des problèmes d'interopérabilité.
- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence des services de téléphonie et d'Internet, ainsi qu'un manque de modularité et de souplesse. [14]

3.5.2.2 Le protocole SIP

SIP (Session Initiation Protocol) est un protocole de communication de la couche applicative du modèle, c'est un protocole normalisé et standardisé par l'IETF qui a été conçu pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification et de la localisation des multiples participants, mais aussi de la négociation sur les types de média utilisables par les différents participants. SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo, autrement dit, il ne véhicule pas la voix, ni la vidéo, mais assure simplement la signalisation. [15]

1. Les caractéristiques du protocole SIP : Ce protocole se caractérise essentiellement par la :

- **Compatibilité :** Il est prévu pour fonctionner avec différentes applications, telles

que la téléphonie, la messagerie instantanée, la vidéoconférence, la réalité virtuelle ou même les jeux vidéo. Il a la capacité à s'intégrer à d'autres protocoles tels que RTP, RTCP, HTTP, etc.

- **Modularité** : Il a été conçu d'une manière indépendante de la couche de transport. Les protocoles TCP et UDP sont donc tous deux supportés pour l'envoi de messages SIP.
- **Simplicité** : Il utilise un langage textuel très proche des protocoles HTTP et SMTP, ce qui facilite son intégration à Internet. Son implémentation est peu gourmande en ressources de traitement.

2. **L'architecture de SIP** : Le protocole SIP s'appuie sur une architecture purement logicielle. Elle repose sur des serveurs distincts qui communiquent entre eux et distribuent la charge du réseau. Elle s'articule autour de cinq entités :

- **Terminal utilisateur** : Le terminal, appelé UA (User Agent) est l'élément qui permet aux utilisateurs d'appeler et d'être appelés. Il peut se présenter sous la forme d'un composant matériel (un téléphone) ou d'un composant logiciel (un programme lancé à partir d'un ordinateur). [15]
- **Serveur d'enregistrement** : Le serveur d'enregistrement (Registrar Server) permet de localiser un correspondant, de gérer la mobilité d'un utilisateur et de supporter l'authentification des abonnés. L'enregistrement d'un utilisateur est constitué par l'association de son identifiant et de son adresse IP, un utilisateur peut s'enregistrer sur plusieurs serveurs d'enregistrement en même temps. Dans la pratique, la première action initiée par un terminal dans un réseau consiste à transmettre une requête d'enregistrement, appelée REGISTER auprès du serveur d'enregistrement afin de lui indiquer sa présence et sa position actuelle. [15]
- **Serveur de localisation** : Le serveur de localisation (Location Server) joue un rôle complémentaire par rapport au serveur d'enregistrement en permettant la localisation des abonnés. Ce serveur dispose de la base de données de l'ensemble des abonnés qu'il gère, et qui a été renseignée par le serveur d'enregistrement.

A chaque fois qu'un utilisateur s'enregistre auprès du serveur d'enregistrement, celui-ci en informe le serveur de localisation. [15]

- **Serveur de redirection :** Le serveur de redirection sert d'intermédiaire entre le terminal client et le serveur de localisation, le terminal client le sollicite pour contacter le serveur de localisation afin de déterminer la position actuelle d'un utilisateur. L'utilisateur n'a pas besoin de connaître l'adresse du serveur de localisation. En effet, l'appelant envoie une requête de localisation d'un correspondant au serveur de redirection, ce dernier contacte le serveur de localisation qui traite cette requête puis renvoie une réponse. Enfin, le serveur de redirection informe l'appelant en lui communiquant la localisation trouvée. [15]
- **Serveur proxy :** Le serveur proxy (parfois appelé serveur mandataire) permet d'initier une communication à la place de l'appelant. Il joue le rôle d'intermédiaire entre les terminaux des interlocuteurs, Ce serveur assure différentes fonctions notamment, la localisation d'un correspondant et l'initialisation, le maintien et la terminaison d'une session. [15]

3. **Adressage SIP :** L'adressage est une des étapes indispensables qui a pour objectif de localiser les utilisateurs dans un réseau. Pour localiser les utilisateurs, il faut pouvoir les identifier de façon unique.

Le format d'une adresse SIP se présente sous la forme suivante :

sip : identifiant[:mot-de-passe]@serveur[?paramètres] [15]

- **sip :** mot clé qui spécifie le protocole à utiliser pour la communication.
- **Identifiant :** définit le nom ou le numéro de l'utilisateur, il doit être unique.
- **mot-de-passe :** cette partie est facultative et permet l'authentification auprès du serveur.
- **Serveur :** spécifie le serveur chargé du compte SIP dont l'identifiant précède l'arobase. Le serveur est indiqué par son adresse IP ou par un nom qui sera résolu par DNS.

- **Paramètres** : cette partie est aussi facultative qui permet de modifier le comportement par défaut.

Voici un exemple d'adresse SIP : **sip :islam@192.20.2.23**.

4. **Les messages SIP** : Les messages échangés dans le protocole SIP sont soit des requêtes, soit des réponses. Dans les deux cas, les messages sont de type texte, ce qui permet une mise en œuvre facile :

(a) **Les requêtes SIP** : SIP n'utilise que six méthodes fondamentales pour formuler ses requêtes qui sont : [15]

- **INVITE** : permet d'initier une session de communication en invitant un correspondant à y participer.
- **ACK** : peut être utilisée suite à l'acceptation d'un appel par l'appelé, et utilisée pour confirmer les paramètres qui seront utilisés lors de la session.
- **OPTIONS** : permet d'interroger un serveur SIP, par exemple, cette méthode offre la possibilité de savoir si un utilisateur que l'on souhaite appeler est présent.
- **BYE** : permet de libérer une communication ou terminer une session.
- **CANCEL** : annule une requête dont la réponse n'est pas encore parvenue au demandeur, elle est nécessairement acquittée par un message ACK pour signifier que l'annulation est prise en compte.
- **REGISTER** : permet d'enregistrer son adresse IP auprès d'un serveur d'enregistrement. Elle permet donc d'assurer le service de localisation.

(b) **Les réponses SIP** : Les principaux codes d'une réponse SIP sont : [15]

- **1xx** : Messages d'information. La requête est en cours de traitement.

Exemple :

-**100 TRYING** : Tentative d'appel en cours.

-**180 RINGING** : Le poste de l'appelé est en train de sonner.

- **2xx** : Messages de succès. La requête a été reçue et acceptée par le serveur.

Exemple :

-**200 ok** : La requête a été exécutée avec succès.

- **3xx** : Messages de redirection. Il décrit une autre action à effectuer avant de finaliser la requête.

Exemple :

-**301 moved permanently** : L'appelé n'est plus disponible à la localisation demandée.

-**302 moved temporarily** : L'appelé est temporairement indisponible à l'adresse spécifiée.

- **4xx** : Messages d'erreurs. Les erreurs du client ou requêtes ne pouvant être prises en charge.

Exemple :

-**400 BAD REQUEST** : Le format de la requête est incorrect et ne peut être compris.

-**404 NOT FOUND** : L'appelé n'a pas été trouvé.

- **5xx** : Messages d'erreurs : erreur du serveur La requête est correcte, mais le serveur n'a pas réussi à la traiter, car le service n'est plus disponible sur le serveur sollicité.

Exemple :

-**503 SERVICE UNAVAILABLE** : Le service n'est pas disponible pour le moment, à cause de la surcharge du serveur.

- **6xx** : Messages d'erreurs, échec général, aucun serveur ne peut traiter cette requête, car ils sont occupés, inaccessibles ou refusent l'appel.

Exemple :

-**603 DECLINE** : L'appelé a été joint, mais il a refusé la communication.

5. Scénarios de communication

- **Enregistrement d'un terminal** : La première action effectuée par un terminal lorsqu'il est activé dans un réseau, consiste à se déclarer auprès d'un serveur d'enregistrement en lui envoyant une requête "Register", le serveur de localisation maintient dans sa base de données une entrée associant l'identifiant d'un utilisateur avec sa position dans le réseau. [15]

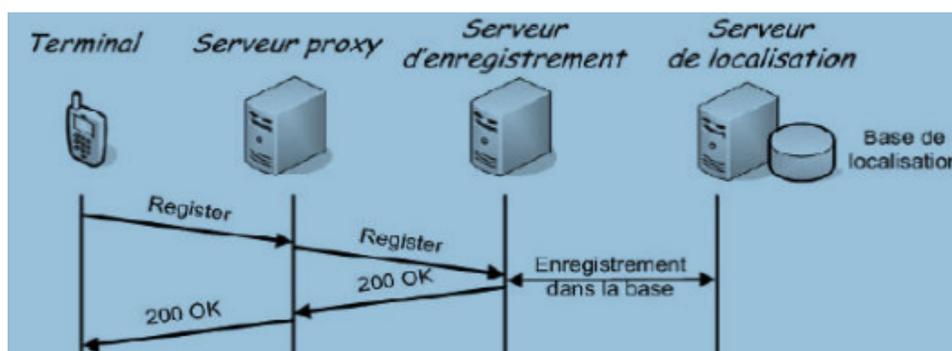


FIGURE 3.3 – Enregistrement d'un terminal

- **Initialisation d'une communication directe** : Une communication peut s'effectuer directement entre deux correspondants, sans faire intervenir d'autres entités si l'appelant connaît la localisation (l'adresse IP) de la personne qu'il souhaite contacter : [15]

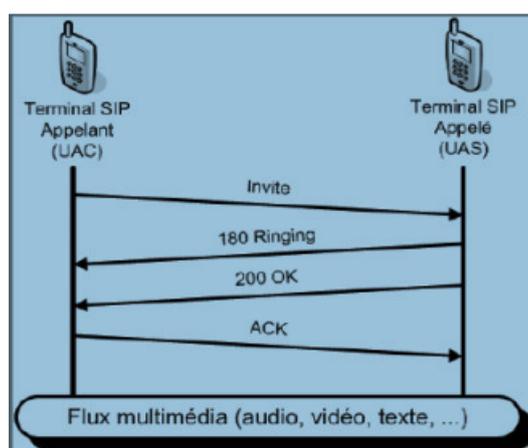


FIGURE 3.4 – Communication directe

- L'appelant (UAC) envoie la requête INVITE proposant à son correspondant (UAS) d'initier une communication.

- Dès que l'UAS reçoit ce message, il indique à l'appelant (par une réponse provisoire 180 RINGING) que l'appelé est en train d'être averti de l'appel.
- Dès que l'appelé accepte l'appel (en décrochant), l'UAS informe l'appelant (par une réponse définitive 200 OK) que l'appel peut débuter.
- L'UAC retourne à l'UAS un message d'acquiescement ACK lui indiquant qu'il a pris note que l'appel peut débuter.

3.6 Points forts et limites de la voix sur IP

3.6.1 Les points forts

- **Réduction des coûts :** Il est possible de téléphoner d'un ordinateur à un autre, sans frais additionnels, dans le monde entier. Les frais d'appel vers un téléphone seront aussi beaucoup plus bas en utilisant la téléphonie.
- **Utilisation hors bureau :** les employés peuvent s'y connecter de la maison, de leur voiture, ou tout autre endroit où il y a un accès au réseau. [15]

3.6.2 Les limites

- **Fiabilité et qualité de la voix :** un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale, il se peut que des morceaux de la conversation manquent (des paquets perdus pendant le transfert).
- **La sécurité :** si un serveur VoIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au réseau téléphonique. Le virus peut également infecter d'autres Ordinateurs connectés au système. [15]

3.7 Conclusion

Au cours de ce chapitre, on a expliqué le principe de fonctionnement de la voix et les différents protocoles utilisés dans cette technologie, ceci est très important pour entamer le prochain chapitre, dans lequel on va faire une présentation du serveur FreePBX.

Chapitre 4

Présentation du serveur FreePBX

4.1 Introduction

Ce chapitre sera consacré à l'installation et configuration du serveur FreePBX, on montrera toutes les étapes nécessaires pour son fonctionnement.

nous allons faire une comparaison entre la téléphonie classique et la VoIP, nous démontrons les avantages de cette dernière par rapport à la téléphonie classique.

4.2 Définition

FreePBX est la solution de téléphonie (IPBX) open-source, la plus utilisée au monde. Elle permet de construire un système téléphonique complet pour des entreprises de toutes tailles ainsi que pour des centres d'appels(call center). La première version de FreePBX a été développée par la société Sangoma et publiée en 2004.

FreePBX peut être installé sous forme de distribution GNU/Linux incorporant le logiciel Asterisk et l'environnement graphique de configuration et d'administration FreePBX (qui est donc une surcouche graphique à Asterisk apportant plusieurs fonctionnalités).

4.3 Le standard téléphonique traditionnel (PABX)

Un PABX (Private Automatic Branch eXchange) est un commutateur électronique, qui permet des installations privées de téléphonie dans le secteur professionnel. Sa tâche principale est d'interconnecter des équipements qui appartiennent à la même entreprise par la commutation de circuits ou de paquets, tout en réduisant le coût de la communication. L'un des plus importants rôles de PABX est l'interconnexion avec l'extérieur, viennent ensuite les différents services demandés par les organisations, selon leurs besoins qui ne cessent d'évoluer.

[16]



FIGURE 4.1 – PABX Alcatel 4200

4.4 Le standard téléphonique IP (IP-PBX)

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

L'IPBX est conçu pour véhiculer de la voix sur IP, ses fonctionnalités sont 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 moins chers que les opérateurs classiques. [16]



FIGURE 4.2 – Standard téléphonique IP (IP-PBX)

4.5 Standard PABX analogique vs standard IPBX

- L'IPBX qui utilise la technologie IP passe donc par Internet, par contre, le PABX fonctionne avec des lignes de téléphones analogiques traditionnelles.
- Le standard IPBX est un peu plus cher que le PABX, par contre l'installation et la maintenance de ce dernier sont beaucoup plus compliquées.
- Les standards PABX et IPBX offrent les mêmes fonctionnalités, telles que le serveur vocal interactif, la messagerie vocale ou encore le journal d'appel. [16]

4.6 Pourquoi utiliser FreePBX?

- **Fiable et sécurisé :** FreePBX propose des mises à jour très régulières ce qui permet d'avoir un système à jour et sécurisé, il est utilisé par plus d'un million d'entreprises à travers le monde.
- **Une interface web complète :** FreePBX propose une interface d'administration complète et facilement utilisable, ce qui permet la gestion de la téléphonie au quotidien ou à distance (consulter l'historique d'appel, appel en un clic, chat, consultation des messages vocaux, ...).
- **Pas de limitation de licence :** FreePBX est offert sans aucune limitation sur les fonctionnalités intégrées (le nombre d'utilisateurs, d'extensions, de numéros de téléphone, de messageries vocales).
- **Flexible et évolutif :** FreePBX peut être installé facilement sur n'importe quelle machine virtuelle ou physique compatible GNU/Linux, il est compatible avec la plupart des téléphones SIP du marché et des opérateurs offrant des trunk SIP.

4.7 Les principales fonctionnalités de FreePBX

- **Toutes les fonctionnalités classiques de la téléphonie** : gestion des appels entrants et sortants, messageries vocales, appels internes, filtrage patron-secrétaire, mode « ne pas déranger », renvoi et transfert des appels, historique des appels, etc. [17]
- **Serveur vocal interactif** : possibilité de mettre en place un ou plusieurs serveurs vocaux interactifs pour l'accueil téléphonique de ses clients.
- **Calendrier d'appels** : configuration d'un routage des appels entrants différenciés en fonction du jour et de l'heure. [17]
- **Musique d'attente personnalisée** : plusieurs musiques d'attente libre de droit sont fournies avec FreePBX. Il est possible d'ajouter musiques personnalisées. [17]
- **Couplage téléphonie-informatique** : possibilité de coupler FreePBX avec sa boîte e-mail, ses contacts, son agenda ou son CRM. [17]
- **Gestion centralisée** : toute la gestion s'effectue de façon simple et rapide depuis l'interface web et ne nécessite pas de connaissances approfondies en téléphonie pour configurer le système téléphonique. [17]
- **Administration complète** : sauvegarde, restauration, supervision, mise en haute-disponibilité, ... toutes ces fonctionnalités sont possibles avec FreePBX. [17]

4.8 Matériels installés avec FreePBX

1. **Téléphones SIP** : Un système téléphonique VoIP nécessite l'utilisation de téléphones SIP. Ces téléphones se basent sur le protocole SIP (Session Initiation Protocol), un standard industriel auquel adhèrent la plupart des PBX IP récents.

Les téléphones SIP sont disponibles dans plusieurs versions / types :

- **Téléphones SIP logiciels** : Un téléphone SIP logiciel est un programme permettant d'utiliser le microphone et les haut-parleurs de l'ordinateur, ou un casque micro

pour téléphoner.

Exemples : Zoiper, X-lite, MizuPhone.

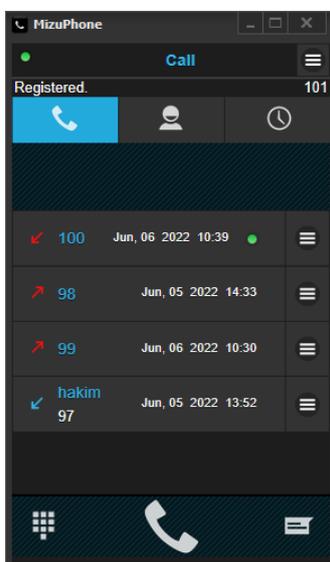


FIGURE 4.3 – Softphone mizu droid sur PC

- **Téléphones SIP matériels :** Un téléphone SIP ressemble et se comporte comme un téléphone classique. Il s'agit en réalité d'un mini-ordinateur qui se connecte directement au réseau informatique. Comme il possède un mini hub, il peut partager une prise réseau avec un ordinateur, supprimant la nécessité d'une prise supplémentaire pour le téléphone.



FIGURE 4.4 – Téléphone SIP Sangoma

- **Smartphones (iPhone et Android) :** Les smartphones iPhone et Android peuvent

être utilisés en tant que clients de FreePBX System via différents application (Zoiper, MizuDroid..), vous pouvez utiliser votre smartphone au bureau, et recevoir des appels professionnels pendant vos déplacements via le Wifi ou la 4G.

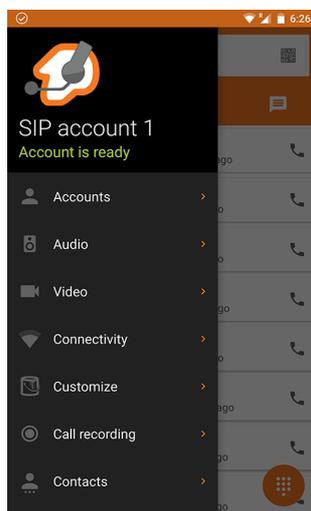


FIGURE 4.5 – Softphone Zoiper sur Android

2. **Passerelle VoIP ou une carte de Voix sur IP :** Une passerelle VoIP est un périphérique permettant de convertir le trafic téléphonique en données, pour qu'il puisse être transmis sur un réseau informatique. De cette manière, les lignes téléphoniques RTC sont converties en extensions SIP, ce qui permet de recevoir et passer des appels via le réseau de téléphonie traditionnel. Les cartes VoIP s'installent sur un PC existant, Il existe aujourd'hui beaucoup de passerelles VoIP ou cartes VoIP disponibles à des prix compétitifs.

4.9 Installation de FreePBX

Nous allons installer FreePBX sur une machine virtuelle (Vmware Worstation), c'est une machine très légère puisque Asterisk ne consomme pas beaucoup de ressources.

Les étapes de l'installation sont les suivantes :

- Nous téléchargeons l'image ISO à partir du site web de FreePBX. Nous allons ensuite introduire l'image ISO (DVD) dans la machine virtuelle.

- Nous lançons l'installation puis nous sélectionnons l'option recommandée (FreePBX 16 Installation (Asterisk 16)).

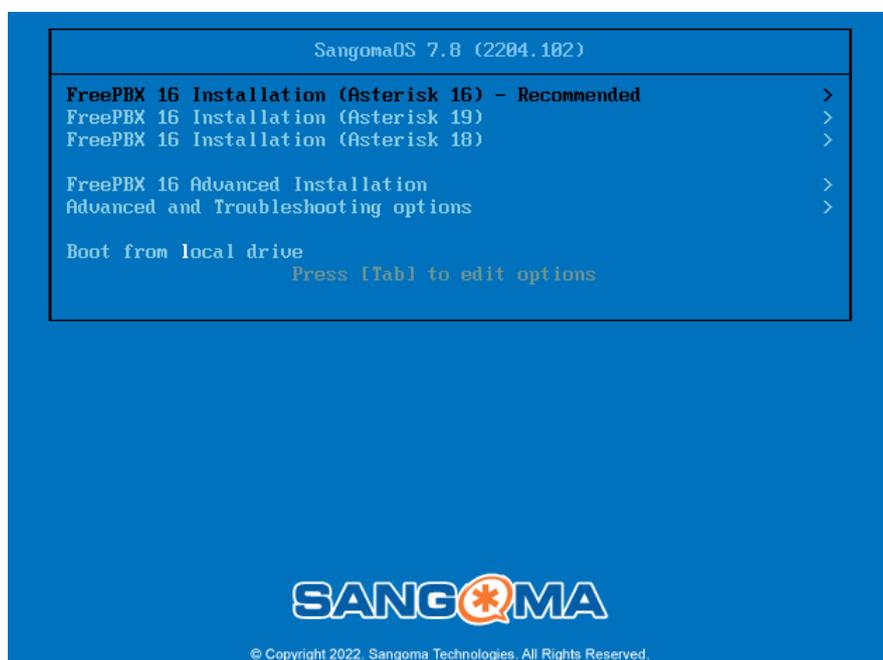


FIGURE 4.6 – Étape 1

- Nous allons sélectionner “Graphical Installation – Output to VGA”.

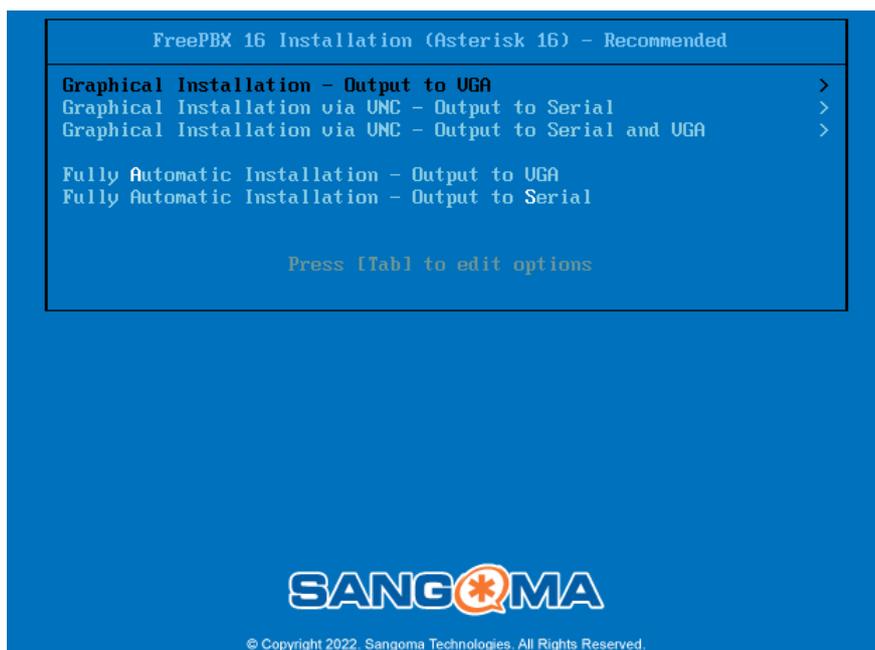


FIGURE 4.7 – Étape 2

— Après, on sélectionne “FreePBX Standard”.

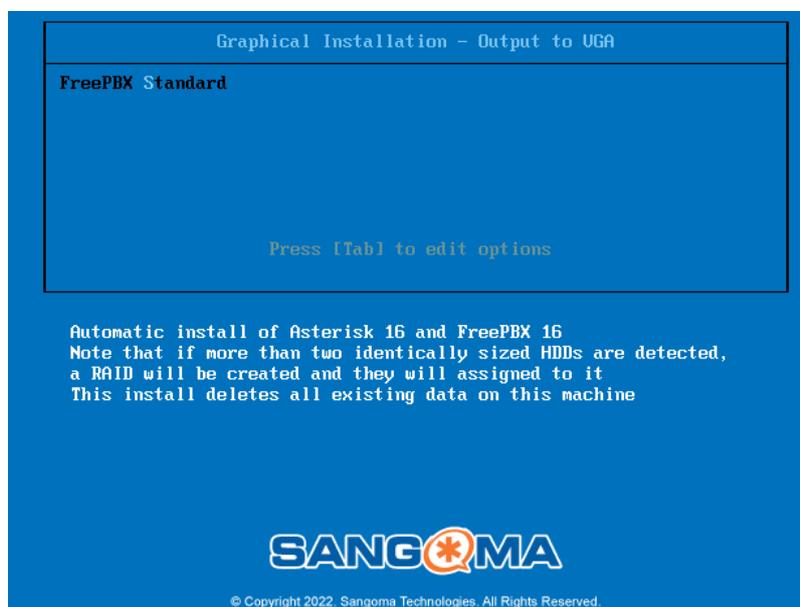


FIGURE 4.8 – Étape 3

— Nous choisissons ensuite un mot de passe pour l'utilisateur "root" dans le champ “Root password”.

— Enfin, on clique sur Begin Installation.

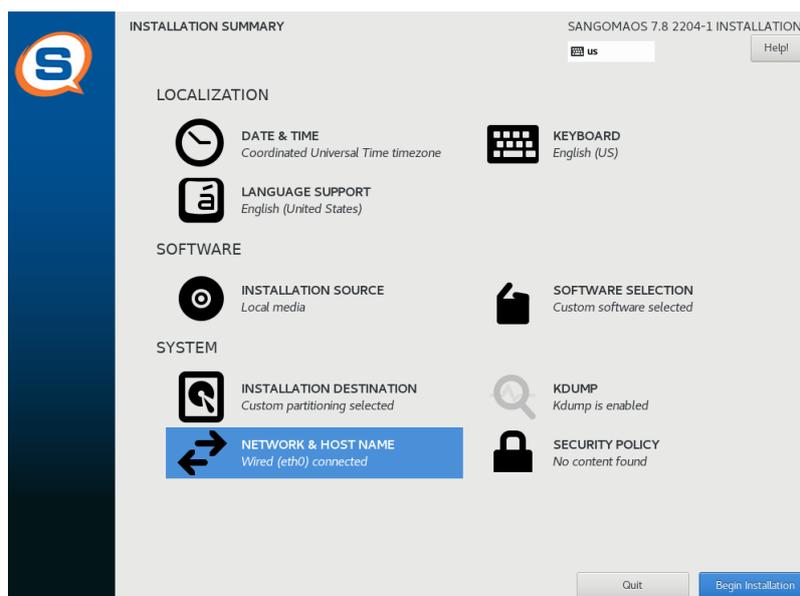


FIGURE 4.9 – Étape 4

Après l'installation, nous allons avoir cette interface.

- Nous allons introduire le login : root, et le password, nous obtenons ensuite la configuration réseau, (l'adresse IP, adresse MAC, interface).

```
Sangoma Linux 7 (Core) (x86_64)
Kernel version 3.10.0-1127.19.1.el7.x86_64

freepbx login: root
Password:
Last login: Fri Jun 10 13:05:04 on tty1

FreePBX

NOTICE! You have 2 notifications! Please log into the UI to see them!
Current Network Configuration
+-----+-----+-----+
| Interface | MAC Address | IP Addresses |
+-----+-----+-----+
| eth0      | 00:0C:29:24:75:6C | 192.168.130.58 |
|           |                | fe80::20c:29ff:fe24:756c |
+-----+-----+-----+

Please note most tasks should be handled through the GUI.
You can access the GUI by typing one of the above IPs in to your web browser.
For support please visit:
  http://www.freepbx.org/support-and-professional-services

[root@freepbx ~]#
```

FIGURE 4.10 – Interface de FreePBX sur VMware

4.10 Connexion a l'interface graphique

- Sur une autre machine de notre réseau, on accède à l'interface web de configuration de FreePBX en entrant l'adresse du serveur dans un navigateur internet.
- On va créer un utilisateur qui aura des privilèges d'administrateur.
- Nous choisissons un mot de passe et une adresse de courriel pour le compte.

Chapitre 4 : Présentation du serveur FreePBX

Welcome to FreePBX Administration!

Initial Setup

Please provide the core settings that will be used to administer and update your system

Administrator User

Username: Admin

Password:

Confirm Password:

System Notifications Email: admin@freepbx.com

System Identification: VoIP Server

FIGURE 4.11 – Création d'un utilisateur avec des privilèges d'administrateur

— Voici l'interface graphique de FreePBX.

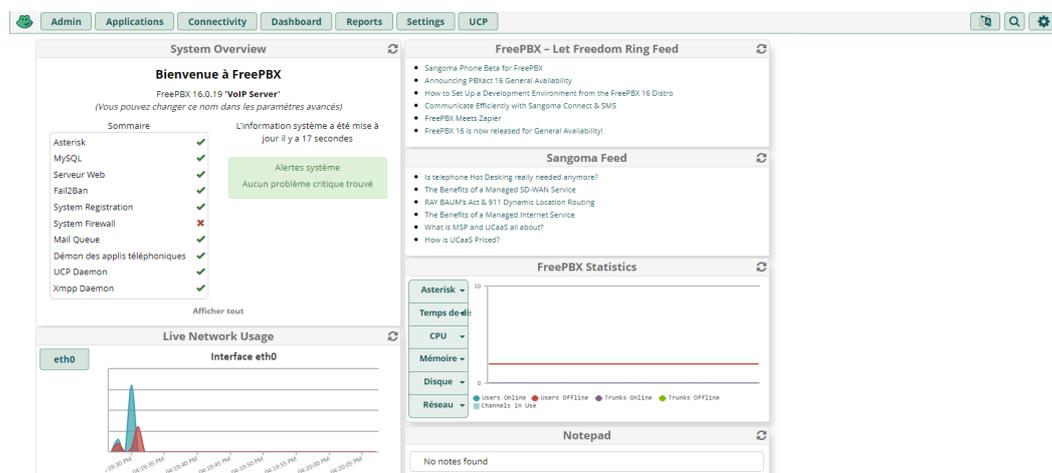


FIGURE 4.12 – L'interface graphique de FreePBX

4.11 Conclusion

Dans ce chapitre, nous avons présenté d'une manière générale le serveur FreePBX, ainsi que ses différentes fonctionnalités et les équipements indispensables à son fonctionnement. Nous avons également détaillé l'installation et la configuration initiale de ce serveur. Une fois les étapes initiales achevées, nous passons à la mise en service illustrée par le prochain chapitre.

Chapitre 5

Réalisation

5.1 Introduction

Ce chapitre est consacré à la mise en œuvre du serveur VoIP FreePBX. Dans le vif de ce chapitre, nous allons mettre en service un centre d'appel complet en utilisant différentes fonctionnalités de FreePBX, et on testera les connectivités.

5.2 Architecture réseau de la réalisation

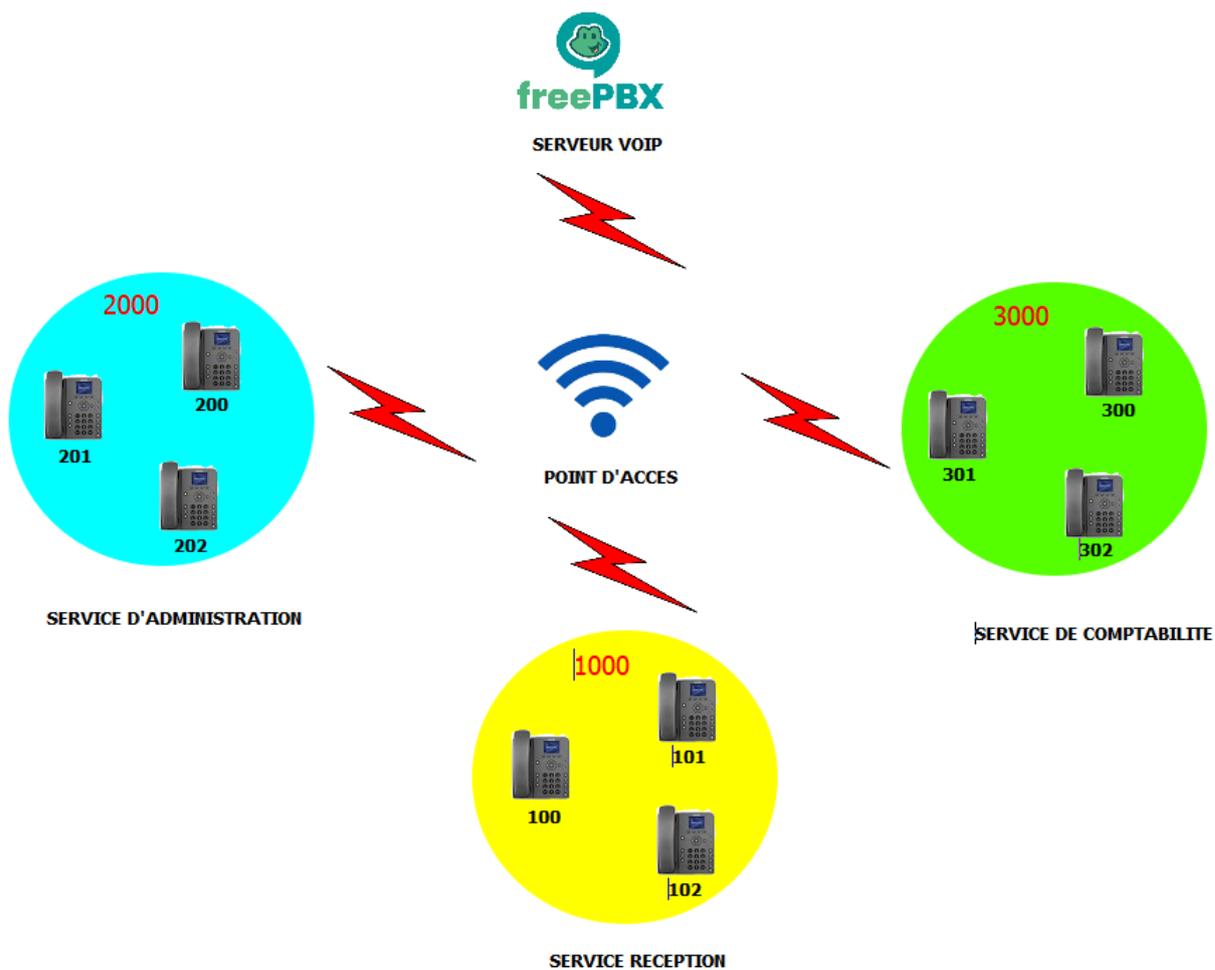


FIGURE 5.1 – Architecture réseau de la réalisation

5.2.1 Adressage

Le tableau suivant représente un tableau qui contient l'adresse du serveur et les numéros de chaque poste :

Serveur VOIP	ADRESSE IP		
	192.168.43.21		
Service de réception	Poste	Adresse	Numéro
	100	192.168.43.62	
	101	192.168.43.63	
	102	192.168.43.64	
Service d'administration	200	192.168.43.65	2000
	201	192.168.43.66	
	202	192.168.43.67	
Service de comptabilité	300	192.168.43.68	3000
	301	192.168.43.69	
	302	192.168.43.70	

TABLE 5.1 – Adressage et affectation des numéros

5.3 Configuration

5.3.1 Configuration des extensions (postes)

1. Création des extensions

La première étape consiste à créer des extensions, pour que les clients puissent s'enregistrer dans le serveur , en s'introduisant dans le menu **Application** puis **Extensions**.

(Figure 5.3)

- Nous cliquons sur **Add Extension** ensuite **Add New SIP Extension**.
- Nous remplissons les champs suivants :
 - **User Extension** : le numéro du poste.
 - **Display Name** : le nom affiché au destinataire lorsque ce poste effectue un apelle.
 - **Secret** : un mot de passe pour enregistrer le poste dans un softphone.
- Les autres champs sont facultatifs.
- Enfin nous cliquons sur **Submit**.

User Extension ?	100
Display Name ?	Réception 1
Outbound CID ?	
Emergency CID ?	
Secret ?	reception1 Really Weak

FIGURE 5.2 – Création d'une extension

- Nous suivons les mêmes étapes pour créer les autres extensions.
- La figure suivante représente tous les extensions qu'on as crée.

Extension	Name
100	Réception 1
101	Réception 2
102	Réception 3
200	Administration 1
201	Administration 2
202	Administration 3
300	Comptabilité 1
301	Comptabilité 2
302	Comptabilité 3

FIGURE 5.3 – Liste des extensions créés

2. Enregistrement des extension

Avant de tester les appels entres les extension, il faut dabord les enregistrer sur les softphone, et pour cela nous utilisons 2 softphones, MizuPhone (windows) et Mizu-Droid (android).

Les deux figures (**Figure 5.5**) et (**Figure 5.6**), représente comment enregistrer une extension sur un softphone sur Windows et android.

- Nous lançons les deux softphones, ensuit nous introduisant dans leurs **Menus** puis sur **Settings**.
- Nous remplissons les champs suivants :
 - **Server** : l'adress du serveur FreePBX.
 - **Username** : le numéro de l'extension.
 - **Password** : le mot de passe de l'externsion.
- Nous cliquons sur **Login**.

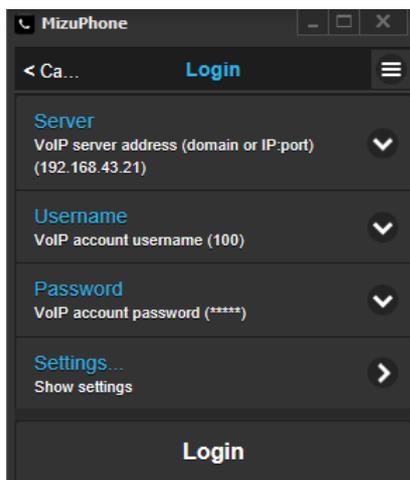


FIGURE 5.4 – Enregistrement du poste 100

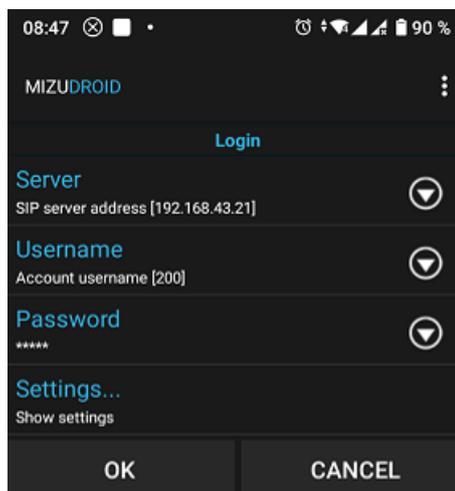


FIGURE 5.5 – Enregistrement du poste 200

- Maintenant les deux postes sont en ligne et ils peuvent passer et recevoir des appels.
- La figure (**Figure 5.7**), montre que les deux poste **100** (Réception 1) et **200** (Administration 1) sont en ligne.

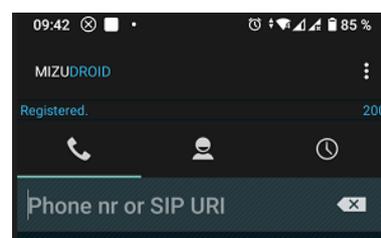
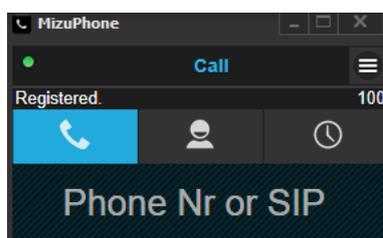


FIGURE 5.6 – Postes (100 et 200) en ligne

3. Tester les appels entre les extensions :

- Maintenant nous allons effectuer un appel entre les deux postes.
- Nous composons le numéro du poste qu'on veut appeler et nous cliquons ensuite sur Initiate Call.
- Les figures (**Figure 5.8**) et (**Figure 5.9**), représente le test d'appel du poste **100** (Réception 1) vers le poste **200** (Administration 1).

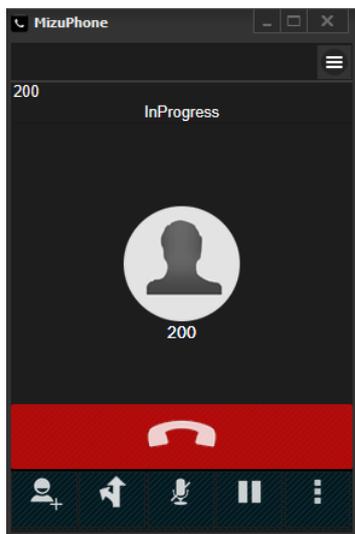


FIGURE 5.7 – Poste 100 (appellant)

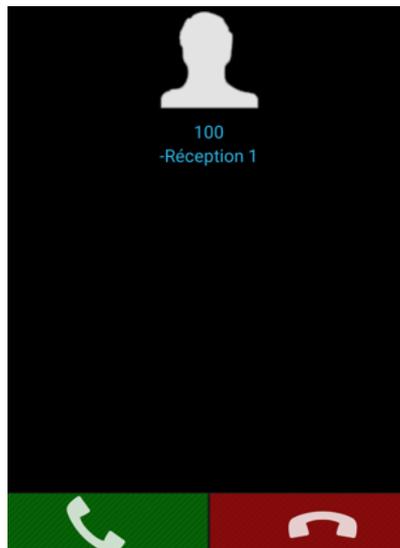


FIGURE 5.8 – poste 200 (appelé)

5.3.2 Configuration des files d'attentes (queues)

La fonctionnalité file d'attente permet de créer un numéro globale qui est utilisé pour appeler un ensemble de postes.

Elle est généralement utilisée pour gérer les appels simultanés et avoir une meilleure performance du serveur.

Par conséquent, nous avons mis chaque service de notre réseau dans une file d'attente.

1. Importation de l'enregistrement vocal :

D'abord nous allons importer l'enregistrement vocal de la file d'attente, afin de l'utiliser dans la création.

Pour le faire nous allons suivre les étapes suivantes :

- Nous nous introduisons dans le menu **Admin** puis **System Recordings**.
- Nous cliquons sur **Add Recording**.
- Nous affectons un nom pour l'enregistrement vocal puis nous importons l'enregistrement vers le serveur.

— La figure suivante montre comment importer un enregistrement.

The screenshot shows a web form for importing a voice recording. It consists of the following elements:

- Name**: A text input field containing the word "ATTENDRE".
- Description**: A text input field containing the word "ATTENDRE".
- File List for English**: A section containing a dropdown menu with "English" selected, and a file named "custom/wait" with a play icon. Below this is a green message box that reads: "You can click any file above to replace it with a recording option below."
- Upload Recording**: A section with a "Browse" button.

FIGURE 5.9 – Importation d'un enregistrement vocal

2. Création des queues :

- Nous s'introduisons dans le menu **Application** puis **Queues**.
- Nous cliquons sur **Add Queue**.
- Dans l'onglet **General Settings**, nous remplissons les champs suivants :
 - **Queue Number** : le numéro de la file d'attente.
 - **Queue Name** : le nom de la file d'attente.
- Nous configurons ensuite les champs suivants comme suit :
 - - **Ring Strategy** : rmemory, appeler les postes à tour de rôle.
 - **Autofill** : Yes, pour une meilleur gestion des appels simultanés.
 - **Skip Busy Agents** : Yes, ne pas appeler un poste s'il est occupé.
 - **Join Announcement** : ici nous selectionons l'enregistrement vocal de la file d'attente.
 - **Fail Over Destination** : Terminate Call, terminer l'appel s'il ya une erreur.
- Dans l'onglet **Queue Agents**, nous ajoutons les postes dans la file d'attente.

— Les figures (Figure 5.11) et (Figure 5.12), montrent la méthode de création d'une file d'attente.

General Settings	Queue Agents	Timing & Agent Options	Capacity Options	Caller Announcements	Advanced Options
Queue Number	1000				
Queue Name	Service de réception				
Queue No Answer	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Call Confirm	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Call Confirm Announce	Default				
CID Name Prefix					
Wait Time Prefix	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Alert Info	None				
Ringer Volume Override	None				
Ringer Volume Override Mode	<input type="radio"/> Force <input type="radio"/> Yes <input checked="" type="radio"/> Don't Care <input type="radio"/> No <input type="radio"/> Never				
Restrict Dynamic Agents	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Agent Restrictions	<input checked="" type="radio"/> Call as Dialed <input type="radio"/> No Follow-Me or Call Forward <input type="radio"/> Extensions Only				
Ring Strategy	rrmemory				
Autofill	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Skip Busy Agents	<input type="radio"/> No <input checked="" type="radio"/> Yes <input type="radio"/> Yes + (ringinuse=no) <input type="radio"/> Queue calls only (ringinuse=no)				
Queue Weight	0				
Music on Hold Class	inherit				
	<input checked="" type="radio"/> MoH Only <input type="radio"/> Agent Ringing <input type="radio"/> Ring Only				
Join Announcement	ATTENDRE				
	<input checked="" type="radio"/> Always <input type="radio"/> When No Free Agents <input type="radio"/> When No Ready Agents				
Call Recording	<input type="radio"/> Force <input type="radio"/> Yes <input checked="" type="radio"/> Don't Care <input type="radio"/> No <input type="radio"/> Never				
Mark calls answered elsewhere	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Fail Over Destination	Terminate Call				
	Hangup				

FIGURE 5.10 – Création d'une file d'attente

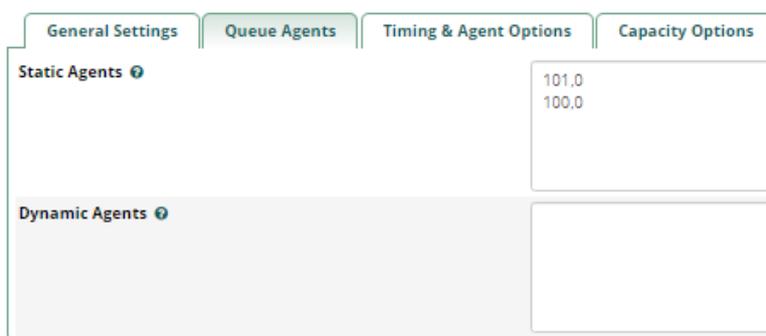


FIGURE 5.11 – Création d'une file d'attente - suite

— La figure suivante représente la liste de files d'attentes q'on as crée.

Queue	Description
1000	Service de réception
2000	Service d'administration
3000	Service de comptabilité

FIGURE 5.12 – Liste de files d'attentes crée

3. **Teste d'appels :** Maintenant nous allons tester d'effectuer un appel du service réception **1000** vers le service d'adminstration **2000**.

— Nous composons sur un poste du service réception le numéro du service d'administration **2000**.

— Ensuite nous cliquons sur **Initiate Call**.

— Les figures (**Figure 5.14**) et (**Figure 5.15**), montrent l'appel entre un poste du service de réception et un poste du service d'administration.

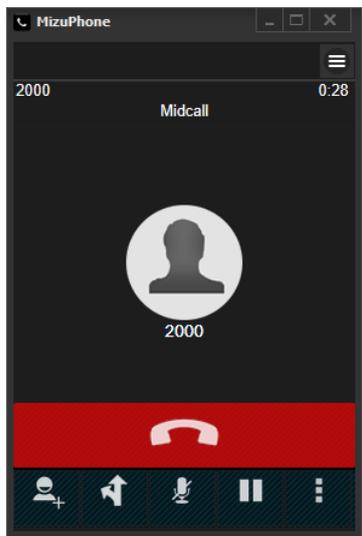


FIGURE 5.13 – Service de réception

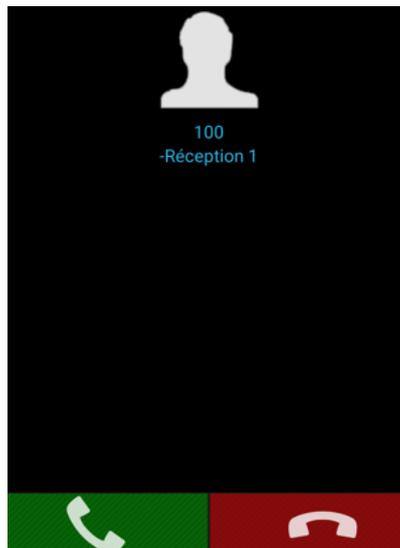


FIGURE 5.14 – Service d'administration

5.3.3 Configuration de la réponse vocale interactive (IVR)

IVR signifie Interactive Voice Response, une technologie qui automatise les interactions de routine avec le service client en permettant aux appelants d'interagir à l'aide de chiffres à clavier ou de leur voix.

Elle permet aux appelants entrants d'accéder aux informations via un système de réponse vocale de messages préenregistrés sans avoir à parler à un agent, ainsi que d'utiliser les options de menu via la sélection du clavier à touches ou la parole.

La figure suivante explique notre menu IVR :

- Lorsque l'appelant tape **1** sur son clavier, son appel sera réorienté vers le service de réception.
- Lorsque il tape **2**, son appel sera réorienté vers le service d'administration.
- Lorsque il tape **3**, son appel sera réorienté vers le service de comptabilité.

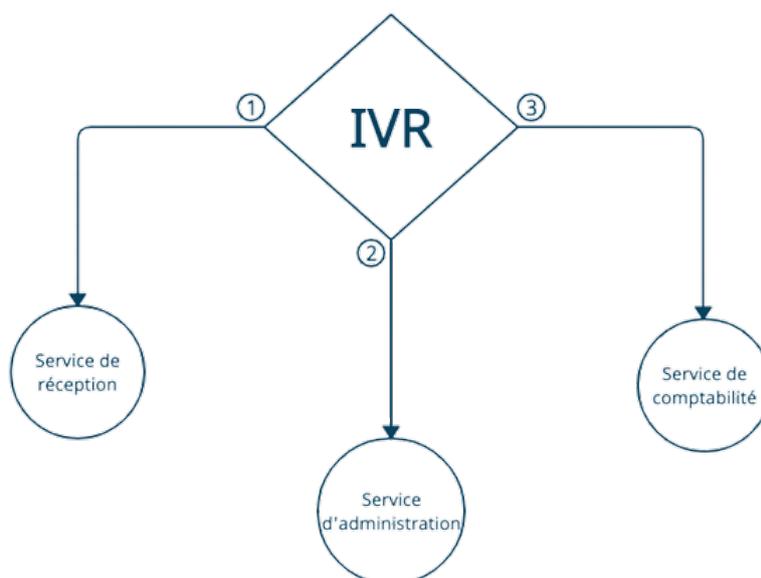


FIGURE 5.15 – Schéma de l'IVR

1. Importation des enregistrements vocaux :

Nous allons tout d'abord importer des enregistrements vocaux, un pour le menu de l'IVR et l'autre au cas où le serveur trouve une erreur dans l'IVR.

Nous suivons les mêmes étapes cités dans la configuration des files d'attente.

2. Création de l'IVR :

- Nous nous introduisons dans le menu **Application** puis **IVR**.
- Nous cliquons sur **Add IVR**.
- Nous remplissons les champs suivants :
 - **IVR Name** : le nom de l'IVR.
 - **Announcement** : nous sélectionnons l'enregistrement vocal de l'IVR.
 - **Invalid Retry Recording** : si l'appelant entre une valeur incorrecte, cet enregistrement lui demande d'entrer une valeur correcte.
 - **IVR Entries** : dans ce champ nous ajoutons nos valeurs et leurs destinations.
- Par exemple** : si l'appelant tape **1**, la destination sera la file d'attente du service de réception.
- Nous laissons les autres champs par défaut.

— Les figures (Figure 5.17) et (Figure 5.18), montrent la création de l'IVR.

— IVR General Options

IVR Name	Interactive Voice Response
IVR Description	IVR

— IVR DTMF Options

Announcement	IVR
Enable Direct Dial	Disabled
Force Strict Dial Timeout	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> No - Legacy
Timeout	10
Alert Info	None
Ringer Volume Override	None
Invalid Retries	3
Invalid Retry Recording	IVR INCORRECT ENTRY
Append Announcement to Invalid	<input type="radio"/> Yes <input checked="" type="radio"/> No
Return on Invalid	<input type="radio"/> Yes <input checked="" type="radio"/> No
Invalid Recording	Default
Invalid Destination	None
Timeout Retries	3
Timeout Retry Recording	Default
Append Announcement on Timeout	<input type="radio"/> Yes <input checked="" type="radio"/> No
Return on Timeout	<input type="radio"/> Yes <input checked="" type="radio"/> No
Timeout Recording	Default
Timeout Destination	<input type="radio"/> Terminate Call <input type="radio"/> Hangup

FIGURE 5.16 – Création de l'IVR

— IVR Entries

Digits	Destination
1	Queues 1000 Service de réception
2	Queues 2000 Service d'administration
3	Queues 3000 Service de comptabilité

FIGURE 5.17 – Création de l'IVR - suite

3. Configuration des appels entrants :

On va maintenant permettre aux appels entrants d'être dirigés vers la bonne destination.

Pour faire ça, nous allons ajouter une route entrante qui va réorienter tous les appels entrants vers l'IVR.

Nous allons suivre les étapes suivantes :

- Nous s'introduisons dans le menu **Connectivity** puis **Inbound Routes**.
- Nous cliquons sur **Add Inbound Route**.
- Nous remplissons les champs suivants :
 - **Description** : décrire le nom de la route.
 - **Set Destination** : choisir la destination, dans notre cas on va choisir l'IVR.
- Nous laissons les autres champs par défaut.
- La figure (**Figure 5.19**), montre la configuration de la route entrante.

General	Advanced	Privacy	Fax	Other	
Description					IVR
DID Number					ANY
CallerID Number					ANY
CID Priority Route					<input type="radio"/> Yes <input checked="" type="radio"/> No
Alert Info					None
Ringer Volume Override					None
CID name prefix					
Music On Hold					Default
Set Destination					IVR
					IVR

FIGURE 5.18 – Création de la route entrante

4. Teste de l'IVR :

Nous allons maintenant tester notre IVR, pour faire ça nous allons simuler un appel

entrant sur un poste, en tapons **534** sur le clavier.

- Sur le poste **200** (service d'administration), nous composons **534** pour simuler un appel entrant.
- L'enregistrement de l'IVR nous demande de choisir un service qu'on veut appeler.
- Nous tapons sur **1**, pour c le service de réception.
- Si nous tapons une valeur incorrecte, l'enregistrement nous demande de rentrer une valeur correcte.
- Les figures (**Figure 5.20**) et (**Figure 5.21**) montrent le test d'appel.

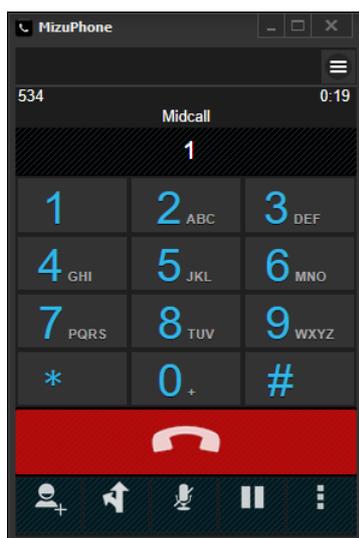


FIGURE 5.19 – Poste 200 (service d'administration)

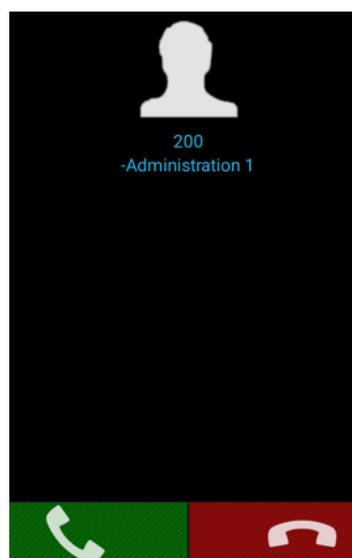


FIGURE 5.20 – Poste 100 (service de réception)

5.3.4 Configuration des appels sortants

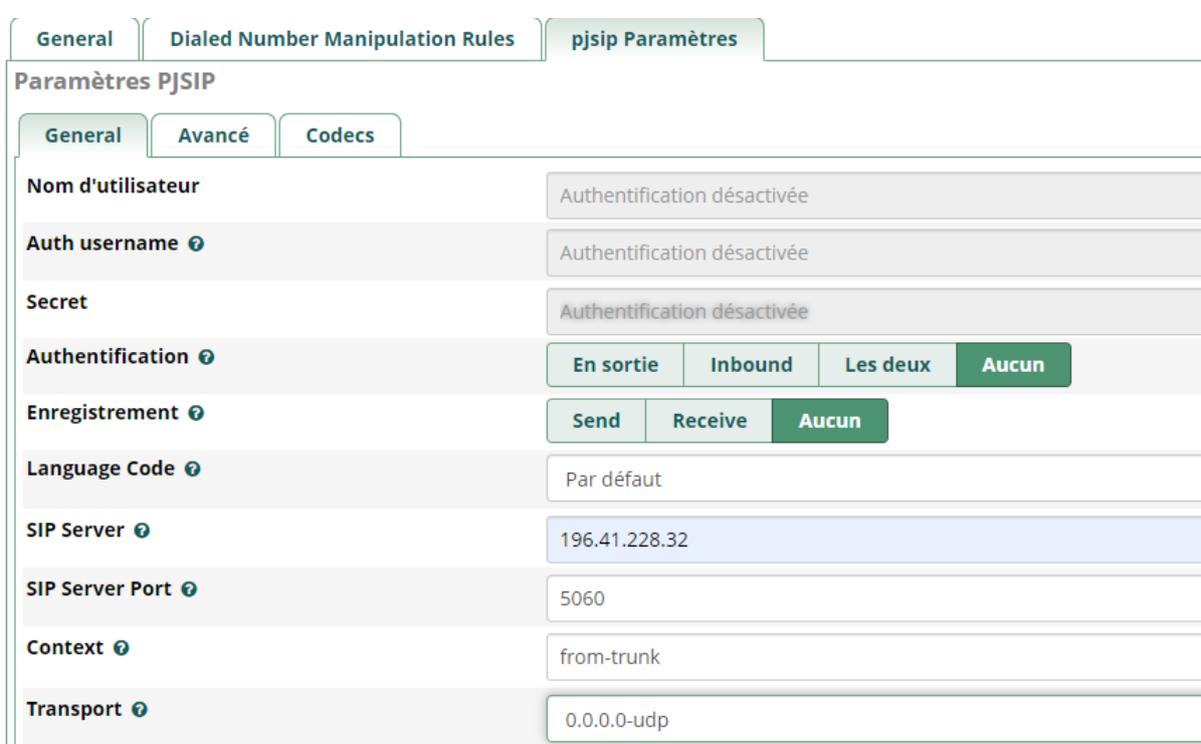
1. Les trunks :

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.

Pour créer un trunk, nous suivons les étapes suivantes :

- Nous nous introduisons dans le menu **Connectivity** puis **Trunks**.

- Sur l'onglet **PJSIP Settings**, nous remplissons les champs suivants :
 - **SIP Server** : l'adresse du serveur avec lequel on veut communiquer.
 - **SIP Server Port** : le port.
 - Transport** : nous choisissons le protocole UDP.
- Nous laissons les autres champs par défaut.
- La figure (**Figure 5.22**) présente la configuration d'un trunk.



The screenshot shows the 'pjsip Paramètres' configuration window. It has three tabs: 'General', 'Avancé', and 'Codecs'. The 'General' tab is active. The settings are as follows:

Field	Value
Nom d'utilisateur	Authentification désactivée
Auth username	Authentification désactivée
Secret	Authentification désactivée
Authentification	En sortie, Inbound, Les deux, Aucun
Enregistrement	Send, Receive, Aucun
Language Code	Par défaut
SIP Server	196.41.228.32
SIP Server Port	5060
Context	from-trunk
Transport	0.0.0.0-udp

FIGURE 5.21 – Création d'un trunk

2. Les routes sortantes :

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 que nous avons créé si le numéro appelé est préfixé d'un 4.

- Nous s'introduisons dans le menu **Connectivity** puis **Outband Routes**
- Nous cliquons sur **Add Route**
- Sur l'onglet **General Settings**, nous remplissons les champs suivants :
 - Route Name** : nom de la route.
 - Trunk Sequence for Matched Routes** : redirige l'appel vers le trunk qui nous avons créé.
- Nous laissons les autres champs par défaut.
- La figure (**Figure 5.23**) présente la configuration d'une route sortante.

Route Settings	Dial Patterns	Import/Export Patterns	Notifications	Additional Settings
Route Name ⓘ	outband			
Route CID ⓘ				
Override Extension ⓘ	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>			
Route Password ⓘ				
Route Type ⓘ	<input checked="" type="button" value="Emergency"/> <input type="button" value="Intra-Company"/>			
Music On Hold? ⓘ	default			
Time Match Time Zone: ⓘ	Use System Timezone			
Time Match Time Group ⓘ	---Permanent Route---			
Trunk Sequence for Matched Routes ⓘ	+ sip1			

FIGURE 5.22 – Création d'une route sortante

Le tableau suivant représente la comparaison entre la téléphonie analogique et la solution proposée :

Considérations	Analogique	La solution proposée
Configuration de la ligne	Élevé. L'installation d'une ligne fixe est généralement facturée entre 50 et 100 dollars par ligne.	Faible. La ligne téléphonique VoIP peut être installée en quelques minutes avec peu ou pas de frais d'installation.
Coût de la maintenance	Élevé. La maintenance doit être effectuée par un technicien sur place, ce qui est coûteux.	Faible. Avec une solution VoIP hébergée, votre fournisseur se charge de toute la maintenance et des mises à jour.
Prix d'appel	Des frais de service mensuels et des tarifs d'appel plus élevés.	Les appels internationaux et mobiles sont généralement facturés à un tarif beaucoup plus bas. avec Une réduction potentielle de 60
Mobilité	Fixe, limite le numéro de bureau à un endroit fixe.	Mobile, permet d'amener le téléphone de bureau partout, et d'ainsi travailler à partir de n'importe où.
Compléments	Options limitées pour les ajouts. La plupart des fonctions avancées coûtent plus cher ou nécessitent du matériel supplémentaire.	Riches fonctionnalités avancées disponibles sans coût supplémentaire Considérations sur la VoIP analogique.

TABLE 5.2 – la téléphonie analogique VS la solution proposée

5.3.5 Conclusion

Durant ce chapitre nous avons procédé à la mise en place d'une solution VoIP pour un LAN, nous avons expliqué la configuration des extensions, files d'attente et IVR, ensuite nous avons testé les appels entre les différents services. Enfin, nous avons expliqué la configuration des communications internes et externes au réseau.

Conclusion générale

La téléphonie sur IP est un marché qui attire de plus en plus l'attention, permettant de regrouper accès, gestion et administration sur un seul système, elle représente une très forte potentialité de gains fondés sur de réelles économies de coûts. Elle assure l'intégration des différents sites des entreprises en un seul système de communication.

Si notre solution VoIP possède de nombreux avantages, elle présente aussi de nombreux inconvénients techniques, notamment en sécurité et en normes et de qualité de voix, La difficulté de la téléphonie IP réside aussi dans la très forte contrainte temporelle due à l'interaction entre individus.

Un cas encore plus complexe se produit lorsqu'il y a un écho, c'est-à-dire un signal qui revient dans l'oreille de l'émetteur. L'écho se produit lorsque le signal rencontre un obstacle, comme l'arrivée sur le combiné téléphonique. L'écho qui repart en sens inverse, Il faut donc que, dans les équipements terminaux, les logiciels extrémité soient capables de gérer les retards et de resynchroniser les octets qui arrivent.

Dans le cadre de l'étude de leurs besoins, les entreprises doivent tenir compte de plusieurs points : le nombre et le type d'utilisateurs distants ou internes, la téléphonie sur IP globale ou locale, les coûts liés à l'utilisation et au remplacement de l'équipement existant par un système de téléphonie sur IP, la qualité de la voix, les mesures de protection contre les attaques de l'extérieur et enfin, le type de fonctionnalités souhaité comme services intégrés de types messagerie électronique, messagerie vocale, vidéoconférences.

Afin de choisir le système de téléphonie sur IP le mieux adapté à leurs besoin, et qui n'est pas forcément le plus développé, les entreprises doivent prendre en considération les coûts d'installation, de maintenance, au retour sur investissement et à la sécurité.

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

Bibliographie

- [1] IONOS , <https://www.ionos.fr/digitalguide/serveur/know-how/reseau-informatique-definition/>, Qu'est-ce qu'un réseau informatique? Définition et exemples , 2020.
- [2] Waytolearnx, Topologie du Réseau Informatique, <https://waytolearnx.com/2019/06/topologie-du-reseau-informatique.html>, 2019.
- [3] Samomoi, <https://www.samomoi.com/reseauxinformatiques/lesprincipauxcomposantdinterconnexi.php>, Les principaux composants d'interconnexion, 2018.
- [4] Samomoi, Les supports de transmission, <https://www.samomoi.com/reseauxinformatiques/les-supports-de-transmission.php>, 2018.
- [5] Cloudflare, Qu'est-ce que le modèle OSI?, <https://www.cloudflare.com/fr-fr/learning/ddos/glossary/open-systems-interconnection-model-osi/>, 2017.
- [6] Futura Tech, TCP/IP : qu'est-ce que c'est?, <https://www.futura-sciences.com/tech/definitions/internet-tcp-ip-1961/>, 2016.
- [7] InetDoc, Les classes d'adresses, <https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html>, 2006.
- [8] Java T Point, Routing, <https://www.javatpoint.com/computer-network-routing>, 2012.
- [9] Comptia, What-Is-Network-Address-Translation?, <https://www.comptia.org/content/guides/what-is-network-address-translation>, 2018.
- [10] Geeksforgeeks, Dynamic Host Configuration Protocol (DHCP), <https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/>, 2022.
- [11] impro-solutions, La Voix sur IP : l'avenir de vos télécommunications, <https://impro-solutions.fr/telephonie/fin-du-telephone-classique>, 2021.
- [12] docplayer, LA VoIP LES PRINCIPES, <https://docplayer.fr/3134961-La-voip-les-principes.html>, 2016.
- [13] frameip, Transport RTP et RTCP, <https://www.frameip.com/voip/>, 2015.
- [14] wikimemoires, Protocole H.323 : équipements, avantages et inconvénients , <https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/>, 2016.
- [15] O.Hersent,D.Gurle ,J.P.Petit, La Voix Sur IP, <https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/>, 2006.
- [16] Wazo, IPBX PABX, <https://wazo.io/fr/guide-voip-webrtc/ipbx/pabx-definition/>, 2020.
- [17] Boxip,FreePBX, c'est quoi?, <https://boxip.fr/doc/freepbx-quest-ce-que-cest/>, 2022.