

الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة عين تموشنت بلحاج بوشعيب
Université –Ain Temouchent- Belhadj Bouchaib
Faculté des Sciences et de Technologie
Département d'Électronique et des Télécommunications



Projet de Fin d'Etudes
Pour l'obtention du diplôme de Master en :
Domaine : Sciences et Technologie
Filière : TELECOMMUNICATIONS
Spécialité : Réseaux et Télécommunications
Thème

Développement d'un Serveur SIP pour les Réseaux Multimédia

Présenté Par :

1) Mr Younes MAREF

Devant le jury composé de :

Mr DEBBAL Mohammed	Pr	UAT.B. B (Ain Témouchent)	Président
Mme SOUIKI Sihem	MCA	UAT.B. B (Ain Témouchent)	Examineur
Mme MEKAMI Hayat	M C B	UAT.B. B (Ain Témouchent)	Encadrant
Dr Nour el Houda YAHY		UAT.B. B (Ain Témouchent)	Co-Encadrante

Année Universitaire 2026/2027

Dédicaces

Avant tout, je rends grâce à Allah, Le Tout-Puissant, pour m'avoir accordé la santé, la volonté, le courage et la patience nécessaires afin de mener à bien ce modeste travail.

Je dédie ce mémoire avec un immense respect et une profonde reconnaissance :

À mon très cher père,

qui a toujours été un exemple de sacrifice, de générosité et de sagesse.

Merci pour tous vos efforts, vos conseils précieux, votre confiance et votre soutien inconditionnel tout au long de mes études.

À ma très chère mère,

source infinie d'amour, de tendresse et de patience.

Merci pour toutes vos prières, votre affection, votre présence constante et tous les sacrifices que vous avez accomplis pour mon bonheur et ma réussite.

Votre soutien moral m'a donné la force d'avancer et de croire en moi dans les moments les plus difficiles.

À mes chères sœurs,

pour leur amour, leurs encouragements et leur présence précieuse dans ma vie.

Merci pour tous les moments de joie et de soutien partagés ensemble.

Je vous souhaite un avenir rempli de réussite, de bonheur et de prospérité.

*Je dédie également ce travail à toute **ma famille**,*

pour leur affection, leurs encouragements et leurs prières qui m'ont accompagnée tout au long de mon parcours universitaire.

Enfin, à toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce mémoire, je leur adresse mes plus sincères remerciements et ma profonde gratitude.

Younes.

Remerciements

Avant tout, je rends grâce à Allah, Le Tout-Puissant, qui m'a accordé la force, le courage et la patience nécessaires pour accomplir ce travail.

Je tiens à exprimer mes sincères remerciements à notre encadrante, Dr MEKAMI.H, pour son accompagnement, ses précieux conseils, sa disponibilité et son soutien tout au long de la réalisation de ce mémoire.

Mes remerciements vont également à notre Co-encadrante, Dr YAHI.N, pour son aide, ses orientations et ses encouragements qui ont grandement contribué à l'aboutissement de ce travail.

J'adresse aussi mes remerciements aux membres du jury pour l'honneur qu'ils nous font en acceptant d'évaluer ce mémoire.

Je remercie également tous les enseignants qui ont contribué à notre formation universitaire.

Enfin, je tiens à remercier chaleureusement ma famille, ainsi que toutes les personnes ayant participé de près ou de loin à la réalisation de ce mémoire.

Résumé

Dans le cadre de notre projet de fin d'études, nous avons réalisé une solution de téléphonie sur IP (VoIP) basée sur le serveur Asterisk sous Debian 12.

Nous avons tout d'abord étudié les concepts fondamentaux de la VoIP ainsi que les principaux protocoles utilisés dans les communications vocales sur IP, notamment SIP, H.323, RTP et RTCP. Cette étude nous a permis de mieux comprendre le fonctionnement des réseaux de téléphonie IP et les mécanismes de transport et de signalisation des communications.

Pour la partie pratique, nous avons utilisé VMware Workstation afin de créer une machine virtuelle sous Debian 12. Sur cet environnement, nous avons installé et configuré le serveur Asterisk, puis créé des comptes SIP permettant d'établir des communications entre différents utilisateurs à l'aide du logiciel MicroSIP.

Nous avons ensuite assuré l'interconnexion entre le réseau VoIP et le réseau téléphonique commuté (RTC). Par la suite, des mécanismes de sécurisation ont été déployés afin de garantir la protection de l'infrastructure mise en place. Enfin, une série de tests a été réalisée pour vérifier le bon fonctionnement du système et valider les différentes configurations effectuées.

Les résultats obtenus montrent qu'une solution VoIP basée sur Asterisk constitue une alternative fiable, flexible et économique aux systèmes de téléphonie traditionnels, tout en offrant de nombreuses possibilités d'évolution et d'intégration.

Mots-clés: VoIP, Asterisk, SIP, H.323, RTP, RTCP, Debian 12, VMware Workstation, Machine virtuelle, MicroSIP, Sécurité, RTC.

Abstract

As part of our final-year project, we developed a Voice over IP (VoIP) telephony solution based on the Asterisk server running on Debian 12.

First, we studied the fundamental concepts of VoIP and the main protocols used in IP voice communications, including SIP, H.323, RTP, and RTCP. This theoretical study enabled us to gain a better understanding of IP telephony networks and the signaling and media transport mechanisms involved in voice communications.

For the practical implementation, VMware Workstation was used to create a virtual machine running Debian 12. Within this environment, the Asterisk server was installed and configured, and several SIP accounts were created to establish voice communications between users through the MicroSIP softphone.

In addition, security mechanisms were implemented to enhance the reliability of the solution, and an interconnection between the VoIP network and the Public Switched Telephone Network (PSTN) was established. Finally, a series of tests was conducted to verify the proper operation of the system and validate the different configurations performed.

The results demonstrate that an Asterisk-based VoIP solution represents a reliable, flexible, and cost-effective alternative to traditional telephony systems while providing significant opportunities for scalability and integration.

Keywords : VoIP, Asterisk, SIP, H.323, RTP, RTCP, Debian 12, VMware Workstation, Virtual Machine, MicroSIP, Security, PSTN.

الملخص

في إطار مشروع التخرج الخاص بنا، قمنا بإنجاز حل للاتصالات الهاتفية عبر بروتوكول الإنترنت (VoIP) اعتمادًا على خادم Asterisk المثبت على نظام Debian 12.

في البداية، قمنا بدراسة المفاهيم الأساسية لتقنية VoIP ، بالإضافة إلى أهم البروتوكولات المستخدمة في الاتصالات الصوتية عبر الشبكات المعتمدة على بروتوكول الإنترنت، لاسيما SIP و H.323 و RTP و RTCP. وقد مكنتنا هذه الدراسة من فهم أفضل لكيفية عمل شبكات الهاتف عبر IP وآليات الإشارة ونقل الوسائط المستخدمة في الاتصالات الصوتية.

أما في الجانب التطبيقي، فقد استخدمنا VMware Workstation لإنشاء آلة افتراضية تعمل بنظام Debian 12 وفي هذه البيئة قمنا بتثبيت خادم Asterisk وإعداداته، ثم أنشأنا حسابات SIP تسمح بإجراء الاتصالات بين مختلف المستخدمين باستخدام برنامج MicroSIP.

كما قمنا بتطبيق آليات أمنية لتأمين الحل المنجز، وإنجاز الربط البيني بين شبكة VoIP والشبكة الهاتفية العمومية المبدلة (RTC). وأخيرًا، أجرينا مجموعة من الاختبارات للتحقق من حسن سير عمل النظام ككل والتأكد من صحة مختلف الإعدادات المنجزة.

أظهرت النتائج المتحصل عليها أن الحل المعتمد على Asterisk يمثل بديلاً موثوقاً ومرناً واقتصادياً لأنظمة الهاتف التقليدية، مع توفير إمكانيات واسعة للتطوير والتكامل مستقبلاً.

الكلمات المفتاحية: VoIP، Asterisk، SIP، H.323، RTP، RTCP، Debian 12، VMware Workstation ، آلة افتراضية، MicroSIP ، الأمن،

Table des matières

Dédicaces	i
Remerciements.....	ii
Résumé.....	iii
Abstract.....	iv
المخلص.....	v
Table des matières.....	vi
Liste des figures.....	ix
Liste des tableaux.....	xii
Liste des acronymes.....	xiii

INTRODUCTION GÉNÉRALE.....	1
----------------------------	---

CHAPITRE I : GÉNÉRALITÉS ET FONDEMENTS DE BASE DE LA VOIX SUR IP.

1. Introduction.....	3
2. Définition.....	3
3. Téléphonie classique.....	3
3.1 Principe de la téléphonie analogique.....	3
3.2 Structure générale du Réseau Téléphonique Commuté (RTC).....	4
3.3 Hiérarchie du RTC.....	5
3.4 Avantages.....	6
3.5 Inconvénients.....	6
4. Téléphonie numérique.....	7
4.1 Échantillonnage.....	7
4.2 Quantification.....	7
4.3 Codage.....	7
5. Compression numérique.....	7
6. Décompression.....	8
7. Les différents types de communications sur IP.....	8
7.1 Communication PC à PC.....	8
7.2 Communication PC à Téléphone.....	9
7.3 Communication Téléphone à Téléphone.....	9
8. Migration vers la téléphonie sur IP.....	9
9. Les différents éléments composant un réseau.....	9
10. Le concept de la VoIP.....	11
11. Qualité de service de la VoIP.....	12
12. Les avantages et les inconvénients de la VoIP.....	12
13. Conclusion.....	13

CHAPITRE II: LES PROTOCOLES DE LA VOIX SUR IP.

1. Introduction.....	14
2. Les protocoles de la VoIP.....	14
2.1 Les protocoles de signalisation.....	14
2.1.1. Protocole H.323.....	14

2.1.1.1 Description générale du protocole H.323.....	14
2.1.1.2 Les protocoles de signalisation dans le cadre H.323.....	14
2.1.1.3 Déroulement d'une communication H.323.....	15
2.1.1.4 Avantages et inconvénients du protocole H.323.....	15
2.1.2. Protocole SIP.....	16
2.1.2.1 Définition du protocole SIP.....	16
2.1.2.2 Principes.....	16
2.1.2.3 Architecture du protocole SIP.....	17
2.1.2.4 Structure des messages SIP.....	18
2.1.2.5 Les requêtes SIP (messages) et les réponses.....	19
2.1.2.6 Le fonctionnement	23
2.1.2.7 Modes de communication.....	24
2.1.2.8 Les serveurs.....	26
2.1.2.9 Avantages et inconvénients du protocole SIP.....	27
2.1.3. Comparaison entre H.323 et SIP.....	29
2.2 Protocoles de transport.....	29
2.2.1. Protocole RTP.....	29
2.2.1.1 Format des paquets RTP.....	30
2.2.2. Protocole RTCP.....	30
2.2.3. Protocole UDP.....	30
2.2.4. Protocole SRTP.....	30
3. Conclusion.....	31

CHAPITRE III : MISE EN ŒUVRE D'UNE SOLUTION VoIP BASÉE SUR ASTERISK : CONFIGURATION, SÉCURISATION ET INTERCONNEXION RTC.

1. Introduction.....	32
2. Définitions des concepts clés.....	32
2.1 Définition d'Asterisk.....	32
2.2 Définition de Linux.....	32
2.3 Définition de Debian 12	32
2.4 Définition de la machine virtuelle.....	33
3. Architecture de la solution VoIP.....	33
4. Installation d'Asterisk sous Debian 12.....	34
4.1 Mise à jour du système.....	34
4.2 Installation des dépendances.....	34
4.3 Création d'un dossier pour les sources.....	35
4.4 Téléchargement et décompresser es sources d'Asterisk.....	35
4.5 Compilation et installation.....	36
4.6 Démarrage du service.....	40
5. Configuration et création des comptes utilisateurs.....	40
5.1 Identification des fichiers de configuration.....	40
5.2 Configuration des comptes utilisateurs.....	41
5.3 Configuration du Dialplan (extensions).....	42
6. Configuration de MicroSIP avec Asterisk.....	43
6.1 MicroSIP.....	43
6.2 Configuration de MicroSIP.....	43
6.3 Test de communication.....	46

7. Capture du trafic en utilisant Wireshark.....	48
7.1 Capture du trafic.....	50
7.2 Visualisation et analyse du processus d'établissement d'un appel SIP.....	54
7.2.1. Analyse du scénario.....	55
8. Sécurisation des appels VoIP entre clients via SRTP.....	55
8.1 Étapes de sécurisation du trafic RTP par SRTP.....	55
8.1.1. Activation de la sécurité SRTP.....	55
8.1.2. Configuration du client MicroSIP et de l'application MizuDroid	56
8.1.3. Rechargement de la configuration.....	57
8.1.4. Test après sécurisation.....	58
9. Architecture de liaison entre RTC et voix IP.....	59
9.1 Éléments de l'architecture.....	60
9.1.1. Réseau RTC.....	60
9.1.2. Passerelle VoIP (Gateway) – Interface FXO.....	61
9.1.3. Routeur Cisco CME.....	61
10. Conclusion.....	64
CONCLUSION GÉNÉRALE.....	65
RÉFÉRENCES BIBLIOGRAPHIQUES.....	67

Listes des figures

Figure I.1 : Liaison téléphonique élémentaire.

Figure I.2 : Principe du RTC.

Figure I.3 : Synoptique d'un RTC.

Figure I.4 : Hiérarchie du RTC.

Figure I.5 : Architecture d'un réseau VOIP.

Figure I.6 : Le principe de fonctionnement de la VoIP.

Figure II.1 : Déroulement d'une communication H.323

Figure II.2 : Architecture du protocole SIP.

Figure II.3 : Exemple de message SIP.

Figure II.4 : structure des en-têtes d'un message SIP.

Figure II.5 : Entête de réponse SIP.

Figure II.6 : Initialisation et fermeture d'une session SIP

Figure II.7 : Mode point à point.

Figure II.8 : Les paquets de Mode point à point.

Figure II.9 : mode diffusif.

Figure II.10 : Les paquets de Mode diffusif.

Figure II.11 : Un appel SIP en utilisant un serveur proxy

Figure II.12 : Un appel SIP en utilisant un serveur de redirection

Figure III.1 : Architecture de communication SIP sous Asterisk.

Figure III.2 : configuration d'Asterisk réussie

Figure III.3 : Ajout et configuration des packages sonores français dans le serveur Asterisk.

Figure III.4 : Sélection des packages audio supplémentaires (Extras Sound Packages).

Figure III.5 : Sélection des fichiers de musique d'attente (Music On Hold).

Figure III.6 : Compilation réussie d'Asterisk avant son installation.

Figure III.7 : Validation de l'installation d'Asterisk après make install.

Figure III.8 : Vérification du bon fonctionnement d'Asterisk via la commande asterisk – rvvv.

Figure III.9 : Utilisateur 1000

Figure III.10 : Utilisateur 2000.

Figure III.11 : la rubrique extensions.

Figure III.12 : l'adresse IP d'Asterisk.

Figure III.13 : configuration de l'utilisateur 1000.

Figure III.14 : configuration de l'utilisateur 2000.

Figure III.15 : État « Disponible » des postes SIP après l'enregistrement.

Figure III.16 : Démarrage du service Asterisk utilisant la commande `/usr/sbin/asterisk -cvvv`

Figure III.17 : Connexion à l'interface de commande d'Asterisk avec `asterisk -rvvv`

Figure III.18 : Résultat de la vérification de l'enregistrement des extensions SIP dans Asterisk.

Figure III.19 : Test d'un appel de 1000 vers 2000.

Figure III.20 : lancement de l'appel 1.

Figure III.21 : Utilisateur 2000 accepter l'appel de l'utilisateur 1000.

Figure III.22 : Test d'un appel de 2000 vers 1000.

Figure III.23 : lancement de l'appel 2.

Figure III.24 : Utilisateur 1000 accepter l'appel de l'utilisateur 2000.

Figure III.25 : ouverture de Wireshark.

Figure III.26 : Test d'appel VoIP entre un client sur PC (MicroSIP) (**1000**) et un client sur téléphone (MizuDroid) (**2000**).

Figure III.27 : écran de Wireshark (sip).

Figure III.28 : Exemple de paquet contenant une requête INVITE.

Figure III.29 : écran de Wireshark (rtp).

Figure III.30 : accéder au décodage d'appel

Figure III.31 : Communication téléphonique détectée.

Figure III.32 : Communication décodée (RTP Player).

Figure III.33 : Capture du flux SIP entre les extensions 1000 et 2000.

Figure III.34 : Configuration du chiffrement des médias (SRTP) dans le fichier `pjsip.conf` du serveur Asterisk.

Figure III.35 : Activation du protocole SRTP dans les paramètres de MicroSIP.

Figure III.36 : Activation du protocole SRTP dans les paramètres de MizuDroid.

Figure III.37 : Ouverture de la console Asterisk.

Figure III.38 : Rechargement de la configuration PJSIP.

Figure III.39 : Vérification la disponibilité pour les deux comptes.

Figure III.40 : capture wireshark montrant des paquets RTP chiffrés(SRTP) Rendant le contenu audio illisible.

Figure III.41 : Appel sécurisé et écoute parasitée.

Figure III.42 : Architecture d'interconnexion entre le réseau RTC et le réseau VoIP basée sur un serveur Asterisk (SIP).

Figure III.43 : Définition de l'endpoint SIP du routeur Cisco dans pjsip.conf.

Figure III.44 : Enregistrement de l'extension SIP 3000 sur le serveur Asterisk.

Figure III.45 : Réception d'un appel RTC sur l'extension SIP 3000

Figure III.46 : Test de communication entre le réseau RTC et le réseau VoIP.

Figure III.47 : Capture Wireshark montrant l'établissement d'une communication entre le RTC et le réseau VoIP.

Liste des tableaux

Tableau I.1 : les codecs audios.

Tableau II.1 : Requêtes SIP.

Tableau II.2 : En-tête de requêtes.

Tableau II.3 : structure des en-têtes des messages SIP.

Tableau II.4 : En-tête de réponses.

Tableau II.5 : exemple des requêtes et réponses SIP.

Tableau II.6 : comparaison entre le protocole H.323 et SIP.

Tableau III.1 : Paquetages nécessaires pour l'installation et la compilation d'Asterisk.

Liste des acronymes

AE	Agent Émetteur
CLI	Command Line Interface
CME	Cisco Call Manager Express
CPU	Central Processing Unit
CRLF	Carriage Return Line Feed
DSP	Digital Signal Processor
FXO	Foreign Exchange Office
H.225	Protocole de signalisation H.225
H.245	Protocole de contrôle H.245
H.320	Standard de communication multimédia sur RNIS
H.323	Standard de communication multimédia sur réseaux IP
H.450	Protocole de services complémentaires H.323
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
LAN	Local Area Network
MacOS	Macintosh Operating System
MCU	Multipoint Control Unit
OS	Operating System
PABX	Private Automatic Branch Exchange
PCM	Pulse Code Modulation
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
Q.931	Protocole de signalisation RNIS
QoS	Quality of Service
RAM	Random Access Memory
RAS	Registration, Admission and Status
RNIS	Réseau Numérique à Intégration de Services
RTC	Réseau Téléphonique Commuté

RTCP	Real-time Transport Control Protocol
RTD	Round Trip Delay
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol
SS7	Signaling System No. 7
STN	Switching Telephone Network
TCP	Transmission Control Protocol
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VM	Virtual Machine
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
ZAA	Zone à Autonomie d'Acheminement
ZTP	Zone de Transit Principal
ZTS	Zone de Transit Secondaire

Introduction Générale

Avec le développement rapide des technologies de l'information et de la communication, les réseaux informatiques occupent aujourd'hui une place très importante dans notre vie quotidienne. Cette évolution a permis l'apparition de nouvelles méthodes de communication plus performantes et plus économiques que les systèmes traditionnels. Parmi ces technologies, la VoIP (Voice over Internet Protocol) représente l'une des solutions les plus utilisées pour la transmission de la voix et de la vidéo à travers les réseaux IP.

La VoIP a profondément transformé le domaine des télécommunications en permettant le transport des communications vocales sur les réseaux informatiques. Grâce à cette technologie, il est possible de réaliser des appels téléphoniques, des visioconférences et d'autres services multimédias tout en réduisant les coûts de communication. Son utilisation est devenue très répandue aussi bien dans les entreprises que chez les particuliers en raison de sa flexibilité, de sa simplicité de déploiement et de sa compatibilité avec les infrastructures réseau existantes.

Cependant, le fonctionnement d'un système VoIP repose sur plusieurs protocoles et mécanismes qui assurent l'établissement des communications, le transport des données ainsi que la qualité et la sécurité des échanges. La compréhension de ces différents éléments est indispensable pour concevoir et déployer une solution de téléphonie IP fiable et performante.

Dans le cadre de ce mémoire, nous sommes intéressés à l'étude des technologies de la voix et de la vidéo sur IP ainsi qu'à leur mise en œuvre à travers une solution pratique basée sur Asterisk. Ce travail nous a permis de découvrir les principes fondamentaux de la VoIP, d'étudier les principaux protocoles utilisés dans ce domaine et de mettre en pratique les connaissances acquises à travers la configuration d'une plateforme de téléphonie IP.

Pour atteindre cet objectif, nous avons commencé par présenter les notions générales relatives à la voix et à la vidéo sur IP. Ensuite, nous avons étudié les protocoles les plus utilisés dans les systèmes VoIP ainsi que leurs rôles dans le fonctionnement des communications. Enfin, nous avons réalisé l'installation et la configuration d'une solution de téléphonie IP basée sur Asterisk, tout en abordant la sécurisation des appels et l'interconnexion avec le réseau téléphonique commuté (RTC).

Ce mémoire est organisé en trois chapitres. Le premier chapitre présente les généralités et les concepts fondamentaux de la voix et de la vidéo sur IP. Le deuxième chapitre est consacré à l'étude des principaux protocoles de la VoIP. Le troisième chapitre présente la mise en œuvre pratique de la solution proposée, les différentes configurations réalisées ainsi que les tests effectués pour vérifier son bon fonctionnement.

À travers ce travail, nous cherchons à mieux comprendre les systèmes de téléphonie IP et à mettre en évidence l'importance des solutions open source dans le développement des réseaux de communication modernes.

Chapitre I

**Généralités et fondements de
base de la voix sur IP.**

1. Introduction

La téléphonie sur IP (VoIP) est une technologie de communication qui permet d'exploiter un réseau de données, tel qu'Internet ou un réseau local (LAN), pour établir des appels et échanger d'autres types d'informations (voix, messages, images ou vidéos). Contrairement à la téléphonie classique reposant sur le Réseau Téléphonique Commuté (RTC), la VoIP convertit la voix en paquets de données qui transitent à travers le réseau, offrant ainsi une solution plus souple et intégrée aux services multimédias.

2. Définition

La Voix sur IP (VoIP) (Voice over Internet Protocol), désigne l'ensemble des protocoles, logiciels et équipements qui rendent possible la transmission de médias en temps réel sous forme de paquet, la VoIP offre une large gamme de fonctionnalités : envoi et réception de messages vocaux, intégration de courriers électroniques, transmission de fax, mise en place de répondeurs automatiques, ainsi que participation à des conférences audio et vidéo, la VoIP exploite les réseaux informatiques pour acheminer le flux vocal. Aujourd'hui, cette technologie est accessible sur la plupart des smartphones, ordinateurs et tablettes. La VoIP représente ainsi une solution flexible et économique, permettant d'accomplir des tâches et de fournir des services difficiles ou onéreux à réaliser via le RTC traditionnel.

3. Téléphonie classique

3.1 Principe de la téléphonie analogique :

La téléphonie a été initialement prévue pour transmettre la voix humaine entre deux lieux distants l'un de l'autre. Elle utilise comme support des lignes électriques sur lesquelles transite un courant analogue aux signaux sonores. Une liaison téléphonique élémentaire est constituée par :

- ✚ Deux dispositifs émetteur-récepteur appelés postes téléphoniques,
- ✚ Une ligne bifilaire acheminant les signaux (paire torsadée),
- ✚ Une source d'énergie électrique (E). La tension continue nécessaire à l'alimentation des postes téléphoniques est fournie par une source installée au central téléphonique (batterie centrale).

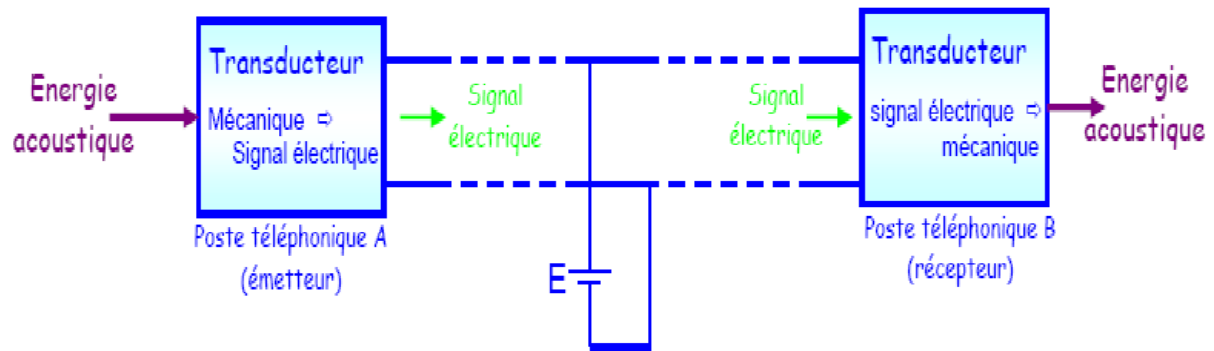


Figure I.1 : Liaison téléphonique élémentaire.

3.2 Structure générale du réseau téléphonique commuté :

Le RTC, (en anglais STN pour Switched Telephone Network) est le système de liaisons des lignes téléphoniques (fixes ou mobiles), connectaient manuellement la ligne de l'appelant à celle de l'appelé. Puis les commutateurs ont évolué, Passant de l'électrotechnique aux technologies électroniques puis, maintenant, informatique. Ils constituent les différents points ou nœuds d'un réseau téléphonique.

La commutation utilisée est la commutation de circuit, et le protocole pour établir, maintenir et rompre la relation s'appelle la signalisation.

Un réseau téléphonique est formé de trois grandes parties : La distribution, la commutation, et la transmission comme le montre la figure suivante :

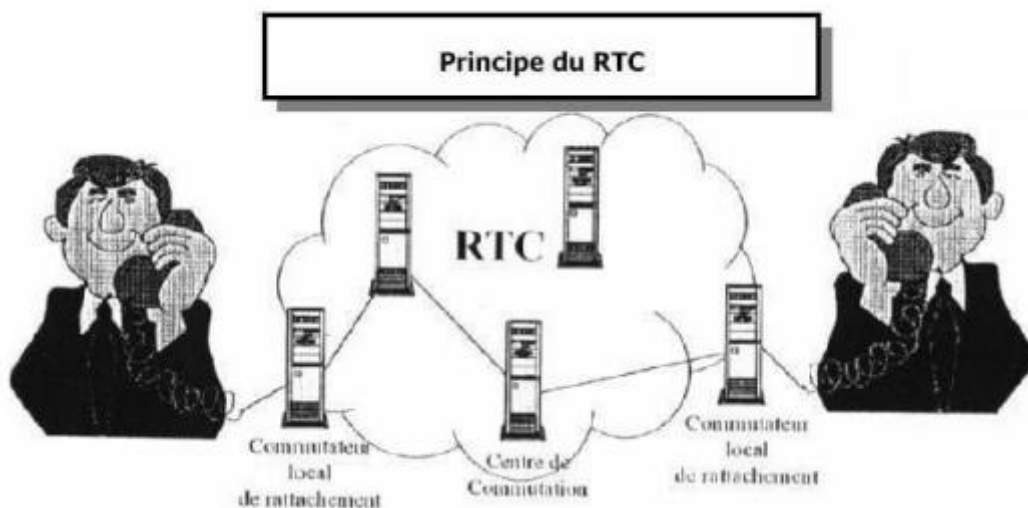


Figure I.2 : Principe du RTC [1].

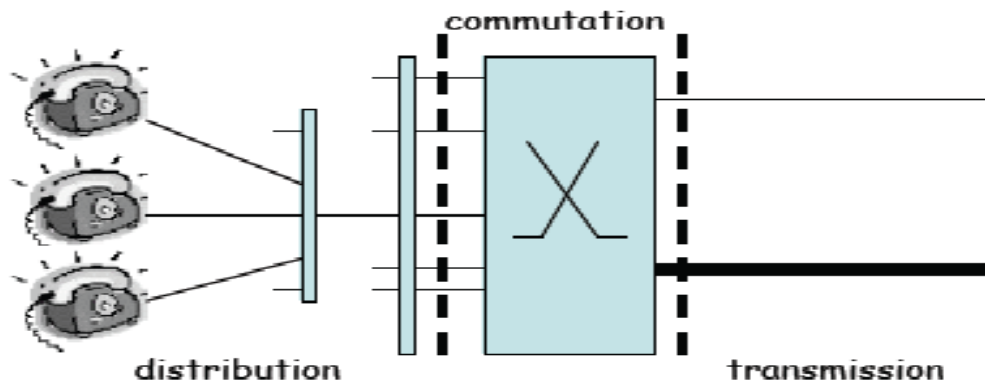


Figure I.3 : Synoptique d'un RTC.

- ✚ La distribution : C'est la partie se trouvant entre les postes d'abonnés et l'autocommutateur, elle met en relation les abonnés [1].
- ✚ La commutation : La liaison de l'ensemble des commutateurs (réseau de transmission ou réseau de transport), elle est constituée de l'étage d'abonné et l'unité de commande [1].
- ✚ La transmission : Le réseau reliant les abonnés au commutateur le plus proche (le commutateur de rattachement) [1].

3.3 La hiérarchie du RTC : Le réseau téléphonique commuté a une organisation hiérarchique à trois niveaux. Il est structuré en zones correspondant à un niveau de concentration comme suit (voir figure 4) :

- **Zone à Autonomie d'Acheminement (ZAA) :** C'est la zone la plus basse de la hiérarchie, comporte un ou plusieurs commutateurs à autonomie d'acheminement (CAA) qui eux-mêmes desservent des commutateurs locaux (CL). Les commutateurs locaux ne sont que de simples concentrateurs de lignes auxquels sont raccordés les abonnés finaux. Cette zone est un réseau étoilé, elle constitue le réseau de desserte ; [1]
- **Zone de Transit Secondaire (ZTS) :** Cette zone comporte des Commutateurs de Transit Secondaires (CTS). Il n'y a pas d'abonnés reliés à ces commutateurs. Ils assurent le brassage des circuits lorsqu'un commutateur à autonomie d'acheminement (CAA) ne peut atteindre le CAA destinataire directement (réseau imparfaitement maillé) ; [1]
- **Zone de Transit Principal (ZTP) :** Cette zone assure la commutation des liaisons longue distance. Chaque ZTP comprend un commutateur de transit principal (CTP), l'un d'eux relié au commutateur international de transit [1].

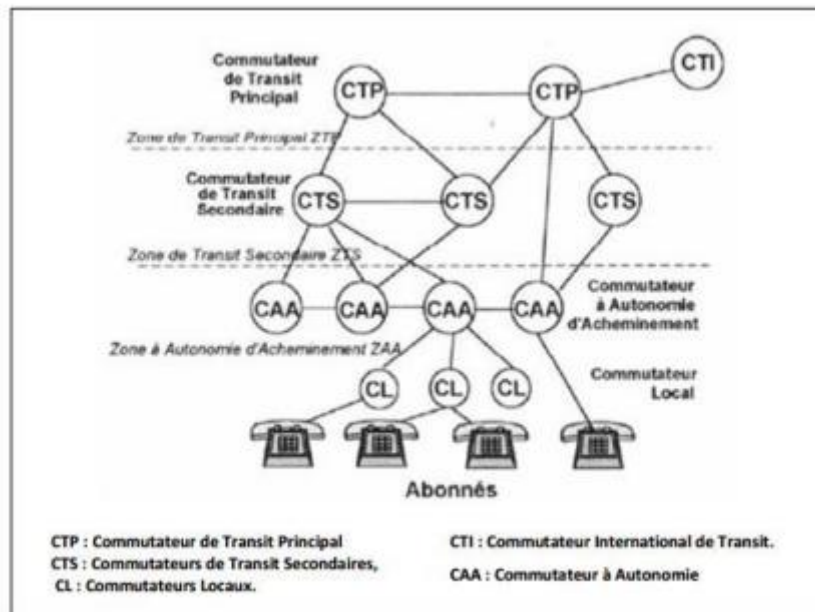


Figure I.4 : Hiérarchie du RTC [1].

3.4 Avantages : Le RTC est :

- ❖ Très pratique pour la communication vocale grâce à la transmission point à point
- ❖ Très étendu, il atteint tous les pays du globe ;
- ❖ Full duplex, deux utilisateurs peuvent émettre et recevoir en même temps, cette fonctionnalité est utilisée par les modems ;
- ❖ Peu coûteux pour les courtes distances.

3.5 Inconvénients :

- ❖ Le RTC est analogique, quelques problèmes sont rencontrés lors de la transmission des données numériques ;
- ❖ Les équipements analogiques perturbent le signal transmis, qui entraîne l'ajout du bruit sur le signal au cours de sa transmission.
- ❖ Pas de cryptage par défaut : des communications ne sont pas sécurisées, ce qui présente un risque d'écoute ou d'interception par des personnes non autorisées, la voix peut être moins claire, surtout sur les longues distances ;
- ❖ Rigidité et manque de flexibilité : il est difficile d'ajouter de nouveaux services ou fonctions.
- ❖ Coût élevé pour les longues distances.

4. La téléphonie numérique

Les trois opérations successives nécessaires à la numérisation de la parole, qu'elle soit téléphonique ou non, sont les suivantes :

- ✚ **4.1 Échantillonnage** : Consiste à prendre des points du signal analogique au fur et à mesure qu'il se déroule. Il est évident que plus la bande passante est importante, plus il faut prendre d'échantillons par seconde. C'est le théorème d'échantillonnage qui donne la solution : il faut échantillonner à une valeur égale à au moins deux fois la bande passante. Pour une bande passante de 3 100 Hz, correspondant à la bande des 300 à 3 400 Hz, il faut échantillonner au moins 6 200 fois par seconde. On comprend ainsi pourquoi la bande passante de la téléphonie est limitée.
- ✚ **4.2 Quantification** : Consiste à représenter un échantillon par une valeur numérique au moyen d'une loi de correspondance. Cette phase consiste à trouver une loi de correspondance telle que la valeur des signaux ait le plus de signification possible.
- ✚ **4.3 Codage** : Consiste à donner une valeur numérique aux échantillons. Ce sont ces valeurs qui sont transportées dans les paquets.

5. Compression numérique

En complément à la numérisation, le signal numérique est compressé pour diminuer le débit nécessaire. Les techniques de compression / décompression numérique, peu utilisées en téléphonie traditionnelle, ont largement profité de l'essor de la téléphonie mobile et de la nécessité d'économiser des ressources fréquentielles rares [2].

✚ **Principe des codecs :**

Codec est une abréviation pour Codeur/Décodeur. Un codec est basé sur un algorithme qui permet la compression des données qu'on lui donne. Il s'agit d'un procédé permettant de compresser et de décompresser un signal, de l'audio ou de la vidéo, le plus souvent en temps réel, permet une réduction de la taille du fichier original. Le codec numérise et compresse la voix de l'émetteur, ainsi les données numériques sont encapsulées dans des paquets IP et acheminées vers le destinataire. À l'arrivée au destinataire, ce dernier grâce au même codec décompresse et restitue le son. On distingue des codecs à perte et codecs sans pertes. Un codec à perte distingue les parties moins importantes des informations et les supprime pour gagner en taille [3].

Dans le monde de la VoIP, les codecs sont employés pour coder la voix pour la transmission à travers des réseaux IP. Les codecs utilisés pour l'usage de VoIP sont désignés également sous le nom de vocodeurs, pour des « encodeurs de voix ».

Les Codecs (Compresseur / Décompresseur ou Codeur / Décodeur) utilisés par les différents équipementiers sont présentés ci-dessous avec leurs principales caractéristiques :

Code	Débit (Kbit/s)	Délai de codage	Bande passante (Kbit/s)
G.711 PCM	64	0.125	87.2
G.726 ADPCM	32	0.125	55.2
G.728 LD-CELP	16	0.125	31.5
G.729aCS-ACELP	8	10	31.2
G.723.1a MP-MLQ	6.4	30	21.9
G.723.1 ACELP	5.3	30	20.8

Tableau I.1 : les codecs audios [3].

6. Décompression

Côté réception, les informations reçues sont décompressées- Il est nécessaire pour cela d'utiliser le même codec que pour la compression - puis reconverties dans le format approprié pour le destinataire (analogique, PCM 64Kbps, etc.)

7. Les différents types de communications sur IP

Trois types sont possibles pour établir une liaison téléphonique basée sur IP : La VoIP de PC à PC, la VoIP de PC à téléphone et la VoIP de téléphone à téléphone.

7.1 Communication de PC à PC :

Dans ce type, chaque ordinateur est équipé d'une carte de son, microphone et haut-parleur. Il connecte directement le réseau Internet grâce au modem ou avec une carte NIC. Les ordinateurs installent le logiciel VoIP pour faire des appels [3].

7.2 Communication PC à Téléphone :

Ce type de communication est développé que le modèle PC à PC. Il permet à l'utilisateur de passer un appel vers le réseau RTC et inversement. Dans ce modèle, le réseau IP et le réseau RTC se connectent grâce à une passerelle [3].

7.3 Communication téléphone à téléphone :

Ce type de communication utilise le réseau Internet pour faire le lien entre les réseaux PSTN. Pour passer un appel, le réseau PSTN va se connecter à la passerelle la plus proche, puis celle-ci va convertir le numéro de téléphone en adresse IP afin d'acheminer les paquets vers leur destination [3].

8. La migration vers la téléphonie sur IP

La téléphonie classique et la téléphonie IP, deux technologies offrant les mêmes services de base mais dotées de structure totalement différentes. L'une fonctionne en commutation de circuit (RTC), donc un appel équivaut à un circuit monopolisé pendant la durée de l'appel, ce qui est synonyme de perte de bande passante. La deuxième technologie fonctionne en commutation de paquet à travers un réseau IP, en devant respecter différentes règles de transport, de signalisation, ainsi que de compression de la voix, cette technologie est très bénéfique en gain de bande passante et en services (voix, données, vidéo) elle permet plusieurs connexions simultanées.

9. Les différents éléments composant un réseau

Pour mettre en œuvre des services basés sur la VoIP, il est indispensable de disposer d'une infrastructure réseau adaptée, de logiciels spécialisés ainsi que des systèmes de gestion correspondants. La figure 5 illustre de façon schématique la topologie générale d'un réseau de téléphonie IP.

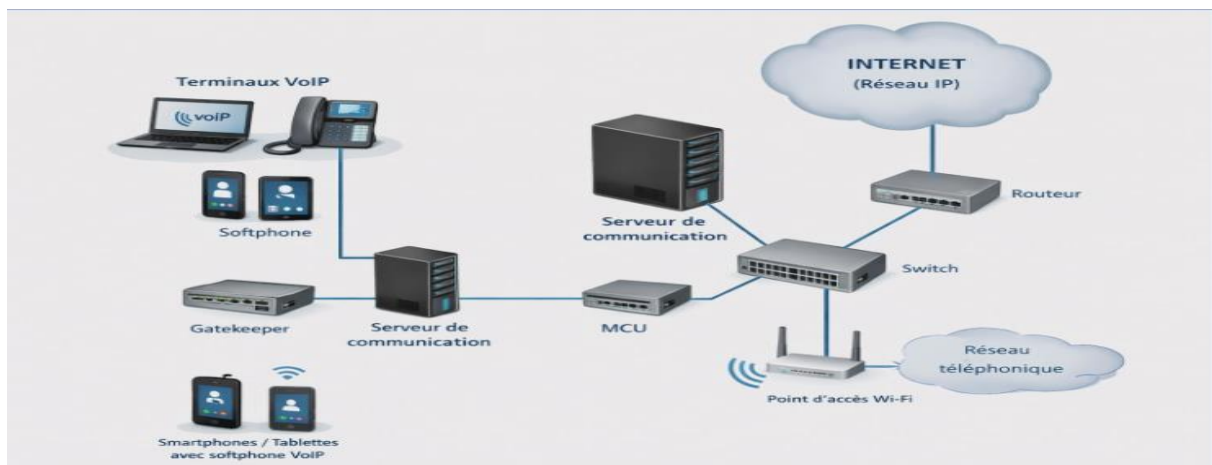


Figure I.5 : Architecture d'un réseau VOIP.

- **Terminals VoIP :** Ils sont des ordinateurs installant les logiciels qui prennent en charge les téléphones VoIP et téléphones IP. Ils établissent et terminent des appels.

- **Le serveur de communications** : Il gère les autorisations d'appels entre les terminaux IP ou des softs phones, ainsi que les différents signaux du réseau. Il peut avoir des interfaces d'opérateur de réseau (RTC ou PSTN), dans le cas contraire, les appels externes seront passés via la passerelle (Gateway).
- **La passerelle (Gateway)** : C'est un élément de routage équipé de cartes d'interfaces analogiques et/ou numériques pour s'interconnecter soit avec d'autres PABX, soit avec des opérateurs de télécommunications locaux, nationaux ou internationaux. La passerelle peut également fournir une interface pour les téléphones analogiques normaux pouvant utiliser toutes les ressources du réseau téléphonique IP (appels internes et externes, entrants et sortants).
- **Le routeur** : Il assure la commutation des paquets d'un réseau vers un autre réseau.
- **Le Switch** : Il assure la distribution et commutation sur des dizaines de ports Ethernet à 10/100 voire 1000 Mbits/s. Selon les modèles, il peut intégrer la télé alimentation des ports Ethernet à la norme 802.3af pour l'alimentation des IP-phones ou des bornes WIFI en 48V.
- **Le Gatekeeper (le garde-barrière)** il assume les fonctions de contrôle d'appels et de gestion des terminaux. Cet équipement détient l'intelligence du réseau et fournit les fonctionnalités de téléphonie aux terminaux distants. Physiquement, un garde-barrière est un serveur informatique localisé sur le même réseau que les terminaux téléphoniques IP.
- **Le MCU (Multipoint Control Unit)** : c'est un élément optionnel qui gère les conférences audio et vidéo.
- **Le Soft phone** C'est un logiciel qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. Il est géré soit par le Call Manager, soit par le PABX-IP

10. Le concept de la VoIP

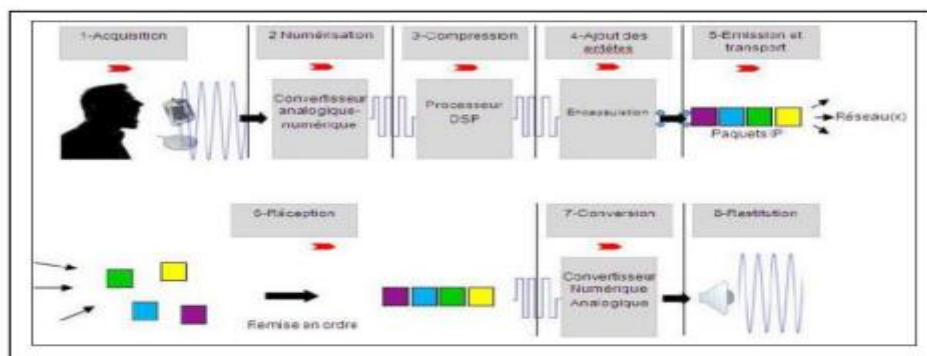


Figure I.6 : Le principe de fonctionnement de la VoIP.

- **Acquisition du signal** : La première étape consiste naturellement à capter la voix à l'aide d'un micro, que ce soit un téléphone ou un micro-casque [4].
- **Convertisseur analogique numérique** La voix passe alors dans un convertisseur analogique numérique. les opérations de numérisation de la voix et de conversion en signal analogique à l'arrivée existent déjà. Ces techniques ne constituent donc pas une nouveauté propre à la Téléphonie sur IP.
- **Compression** : Le signal une fois numérisé peut être traité par un DSP (Digital Signal Processor) qui va le compresser, c'est-à-dire réduire la quantité d'informations nécessaires pour l'exprimer. L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal [4].
- **Habillage des en-têtes** Les données doivent encore être enrichies en informations avant d'être converties en paquets de données à expédier sur le réseau [4].
- **Emission et transport** : Les paquets sont acheminés depuis le point d'émission pour atteindre le point de réception sans qu'un chemin précis soit réservé pour leur transport.
- **Réception** : Lorsque les paquets arrivent à destination, il est essentiel de les réordonner assez rapidement. Faute de quoi, une dégradation de la qualité de la voix se fera sentir [4].
- **Conversion numérique analogique** : La conversion numérique analogique est l'étape réciproque de l'étape 2 [4].
- **Restitution** : Dès lors, la voix peut être retranscrite par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur [4].

11. Qualité de service de la VoIP

La qualité de service(QoS) est un concept important à prendre en compte lors de la mise en œuvre de la VoIP. L'objectif est de s'assurer que les trames IP sont transférées à travers le réseau sans délai ni rejet des trames transportant la voix. Il y a 3 éléments clés pour distinguer la QoS [9].

✚ **Latence (Delay)** : selon la norme ITU G114, le délai d'acheminement permet :

- Entre 0 et 150 ms, une conversation normale.
- Entre 150 et 300 ms, une conversation de qualité acceptable.
- Entre 300 et 700 ms, uniquement une diffusion de voix en half duplex. [2]

✚ **Gigue (jitter)** :

La gigue est la variation statistique du délai de transmission. En d'autres termes, elle mesure la variation temporelle entre le moment où deux paquets auraient dû arriver et le

moment de leur arrivée effective. L'irrégularité de l'accès aux paquets est due à plusieurs raisons, notamment : l'encapsulation de paquets IP dans les protocoles pris en charge, la charge du réseau à un moment donné et la variation des chemins empruntés dans le réseau [2].

Perte des paquets Internet :

Ne garantit pas que tous les paquets soient déplacés vers la destination. Des paquets peuvent être perdus à cause de la congestion ou de la bande passante. Pour la VoIP, le taux de perte de paquets devrait être inférieur à 1%. En raison du délai limité, les protocoles de retransmission ne sont pas satisfaits de la solution à ce problème. Il existe certaines méthodes pour résoudre le problème de la perte de paquets. Par exemple, les paquets perdus peuvent être remplacés par des signaux calmes [2].

12. Les avantages et les inconvénients de la VoIP

12.1 Les avantages :

- La réduction des coûts : En utilisant la VoIP à la place du réseau RTC (Réseau téléphonique commuté), les entreprises peuvent réduire le coût de communications privées dans le contexte des communications internationales. Dans l'utilisation de réseaux WAN/IP intersites, les réductions de coût sont plus intéressantes surtout s'il existe de nombreux sites distants. De manière plus simple, la communication entre deux personnes utilisant la VoIP pourrait réduire leurs coûts de communication.
- Standardisation et interopérabilité entre les fournisseurs : L'architecture utilisée est unique lorsque le réseau téléphonique est intégré au réseau de données pour former un seul réseau de communication.
- Mobilité : Les utilisateurs aujourd'hui ont besoin de travailler, quel que soit le lieu où ils se trouvent, en utilisant différents terminaux (téléphone fixe, PC ou téléphone mobile) afin d'être joignables en toutes circonstances. La VoIP rend possible ce type d'usage, en facilitant les échanges d'informations par la voix, la vidéo ou par les messages textuels.

12.2 Les inconvénients :

Cette technologie a aussi des inconvénients. Son coût, son architecture, sa qualité et la fiabilité de cette technologie sont des imperfections à prendre en compte.

- Problème de sécurité : Puisque la VoIP repose sur l'utilisation du réseau IP, et vu que ce dernier est caractérisé par ses failles de sécurité, elle sera aussi mise face aux mêmes menaces de sécurité.

- Fiabilité et qualité sonore : Un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale. En effet, des désagréments tels la qualité de la reproduction de la voix du correspondant ainsi que le délai entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être extrêmement problématiques dans le milieu professionnel.

13. Conclusion

En conclusion, la voix et la vidéo sur IP représentent une technologie importante dans le domaine des télécommunications modernes. Elles permettent de transmettre la voix et la vidéo via les réseaux IP avec plus de flexibilité et un coût réduit.

Dans ce chapitre, on a présenté les notions de base, les principes de fonctionnement ainsi que les éléments essentiels d'un réseau VoIP. Ces connaissances sont nécessaires pour mieux comprendre la suite de ce travail.

Chapitre II

Les Protocoles de la voix sur IP.

1. Introduction

La voix sur IP nécessite l'utilisation de divers protocoles pour transmettre les données en temps réel et gérer la congestion du réseau.

Les protocoles VoIP sont divisés en deux parties : protocoles de signalisation, et protocoles de transport.

L'objectif de ce chapitre est de définir les différents protocoles ainsi que leur principe de fonctionnement et leurs principaux avantages et inconvénients [5].

2. Les protocoles de la VoIP

2.1. Les protocoles de signalisation :

Pour le bon déroulement d'une communication sur IP, cette dernière doit respecter un modèle de signalisation. Parmi les plus connus et les plus utilisés on cite le protocole H.323 et le protocole SIP.

2.1.1. Protocole H323 :

2.1.1.1 Description générale du protocole H323 :

H.323 est un protocole de communication englobant un ensemble de normes utilisées pour l'envoi de données audio et vidéo sur Internet. Il existe depuis 1996 et a été conçu et développé, par l'ITU (International Télécommunication Union)

Le protocole H.323 fait partie de la série H.32x qui traite de la vidéoconférence au travers différents réseaux. Il inclue H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data Network) et PSTN (Public Switched Telephone Network).

H.323 crée une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information.

2.1.1.2 Les protocoles de signalisation dans le cadre de H.323 :

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

- **RAS (Registration, Admission and Status)** : Ce protocole est utilisé pour communiquer avec un Gatekeeper. Il sert notamment aux équipements terminaux pour découvrir l'existence d'un Gatekeeper et s'enregistrer auprès de ce dernier ainsi que pour les demandes de traduction d'adresses. La signalisation RAS utilise des messages H.225.0 6 transmis sur un protocole de transport non fiable comme UDP.
- **Q.931** : H.323 utilise Q.931 (version simplifiée de signalisation RNIS) pour l'établissement et le contrôle d'appels téléphoniques sur IP.

- **H.245** : Ce protocole est utilisé pour l'échange de capacités entre deux équipements terminaux. Par exemple le type de codec à activer. Il peut également servir à mesurer le RTD (Round Trip Delay) d'une communication.

2.1.1.3 Déroulement d'une communication H.323 : Une communication H.323 se déroule en Cinq phases :

1. Le terminal demande l'autorisation au Gatekeeper (RAS).
2. L'appel est lancé avec Setup et Call Proceeding (Q.931).
3. Le téléphone sonne (Alerting) puis l'appel est accepté (Connect).
4. Les terminaux échangent leurs capacités (H.245).
5. La communication commence via RTP après ouverture des canaux.

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

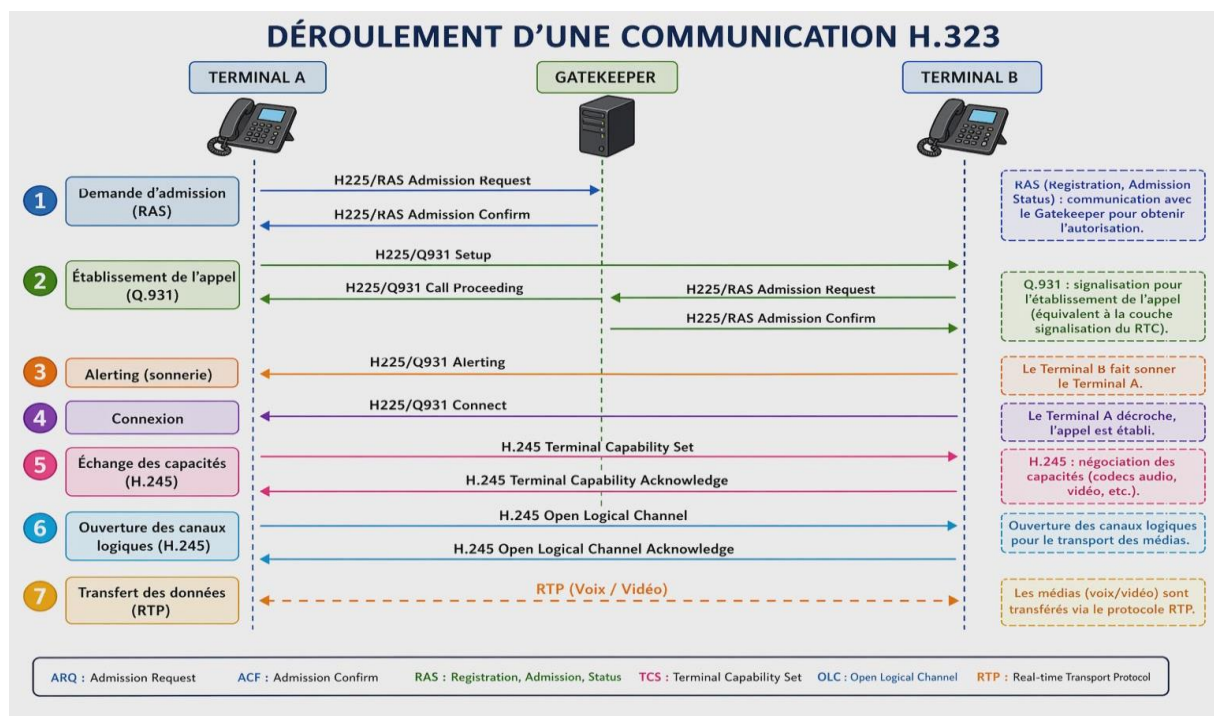


Figure II.1 : Déroulement d'une communication H.323.

2.1.1.4 Avantage et inconvénient du protocole H323 :

- **Les avantages :**

1. **Gestion de la bande passante** : Le trafic audio et vidéo est un grand consommateur de ressources réseau. Afin d'éviter que ces flux ne congestionnent le réseau, H.323 permet une gestion de la bande passante à disposition.

En particulier, le gestionnaire du réseau peut limiter le nombre simultané de connexions H.323 sur son réseau ou limiter la largeur de bande à disposition de chaque connexion.

De telles limites permettent de garantir que le trafic important ne soit pas interrompu [6].

2. **Support multipoint** : H.323 supporte des conférences entre trois terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée [6].
3. **Support multicast** : H.323 supporte le multicast dans les conférences multipoint. Multicast, c'est le fait d'envoyer un paquet vers un sous-ensemble de destinataires sans réplication, permet une utilisation optimale du réseau [6].

- **Les inconvénients :**

1. **Complexité** : Comparé à SIP, H.323 est plus difficile à configurer et à maintenir [7].
2. **Dépendance** : Requiert l'utilisation de portiers pour gérer les appels, ce qui ajoute une couche de complexité [7].
3. **Obsolescence** : Face aux technologies plus récentes comme WebRTC, H.323 commence à sembler dépassé pour certaines applications modernes [7].

2.1.2. Protocole SIP :

2.1.2.1 Définition du protocole SIP :

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

2.1.2.2 principes :

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

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

Ses caractéristiques principales qui le rendent si pratique sont :

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

– SIP est un protocole léger qui nécessite peu de ressource physique et peu de temps de développement.

2.1.2.3 Architecture du protocole SIP :

Dans SIP il y a deux types de composantes, les agents utilisateurs (UAS, UAC) et un réseau de serveurs (Registrar, Proxy).

- **U.A.S (User Agent Server) :** Une partie serveur qui est en écoute, reçoit et traite les requêtes ; c'est l'UAS qui répond à un appel [8].
- **U.A.C (User Agent Client) :** Une partie cliente chargée d'émettre les requêtes ; c'est l'UAC qui initie un appel [8].
- **Le Registrer :** c'est un serveur qui accepte les requêtes de type REGISTER. Il est typiquement couplé à un proxy ou un serveur de redirection pour permettre d'atteindre un client. Son fonctionnement est analogue à celui d'un serveur DNS dans le monde de l'internet [8].

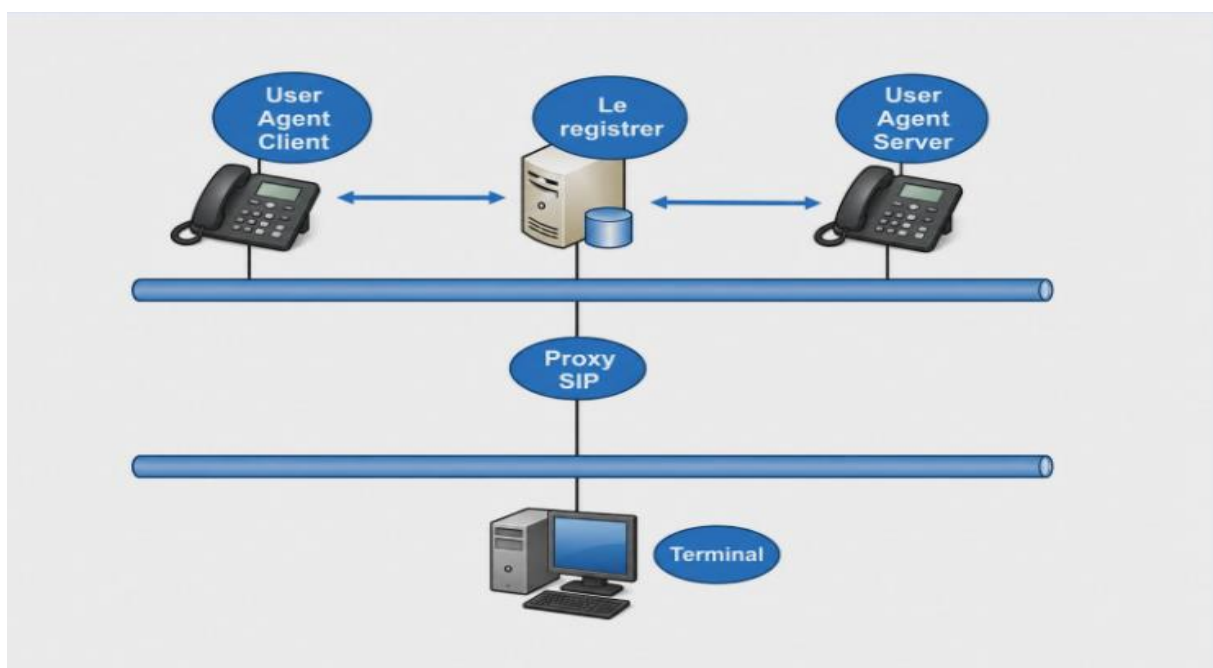


Figure II.2 : Architecture du protocole SIP [8].

- **Proxy SIP :** aussi appelé proxy ou serveur mandataire ; il permet d'initier un appel à la place de l'appelant. Il joue le rôle d'intermédiaire entre les terminaux des interlocuteurs et agit pour le compte de ces derniers

Proxy SIP remplit les différentes fonctions suivantes :

- Localiser un correspondant ;
- Réaliser éventuellement certains traitements sur les requêtes ;
- Initier, maintenir et terminer une session vers un correspondant [9].

2.1.2.4 La structure des messages SIP :

Les messages SIP se décomposent de trois parties :

- la première ligne ;
 - l'en-tête ;
 - le corps du message.
- ✓ La première ligne sert à identifier le type du message SIP ainsi que l'adresse du destinataire.
 - ✓ L'en-tête contient les informations permettant l'acheminement du message comme : la référence de l'émetteur, le destinataire, référence de la transaction et de la session, les éléments de sécurité. . Ainsi l'en-tête permet l'établissement d'une session en termes de localisation, de nommage et d'adressage, mais c'est le corps du message qui décrit le flux multimédia mis en jeu par la session.
 - ✓ Le corps du message contient généralement les éléments nécessaires à l'établissement du canal média.

```
1 INVITE sip : amine@univ-temouchent.dz SIP /2.0
2 CSeq : 1 INVITE
3 Via : SIP /2.0/ UDP 10.0.2.24:5060
4 Via : SIP /2.0/ UDP 6.7.8.9:5060
5 User - Agent : Ekiga /4.0.1
6 Call - ID : 54 d5b754 - cdbe - e611 -885 f
7 To : & lt ; sip : amine@univ-temouchent.dz & gt ;
8 Content - Length : 458
9 Content - Type : application / sdp
10 Max - Forwards : 69
11
12 v =0
13 o=- 1481542778 1 IN IP4 10.0.2.24
14 s= Ekiga /4.0.1
15 c= IN IP4 10.0.2.24
16 t =0 0
17 m= audio 54678 RTP / AVP 116 0 8 101
18 a= sendrecv
19 a= rtpmap :116 Speex /16000/1
20 a= rtpmap :8 PCMA /8000/1
21 a= rtpmap :101 telephone - event /8000
22 a= fmp :101 0 -16 ,32 ,36
```

Figure II.3 : Exemple de message SIP.

2.1.2.5 Les requêtes SIP (messages) et les réponses :

Les requêtes (messages) : il y a plusieurs types de requêtes (par ailleurs appelées « méthodes »), mais trois suffisent à établir un appel : INVITE, ACK et BYE. Deux autres requêtes, OPTIONS et REGISTER permettent de réaliser toutes les applications de téléphonie. Les autres requêtes offrent des services complémentaires. De nouvelles requêtes SIP sont régulièrement ajoutées, et permettent d'enrichir le modèle.

Les types de requêtes :

Méthode SIP	Description
REGISTER	Méthode d'enregistrement permettant à un agent (UA-User Agent) de communiquer son adresse IP et l'URL où le joindre.
INVITE	Méthode utilisée pour établir des sessions de communication entre agents.
ACK	Méthode utilisée pour confirmer la réception de la réponse finale à une requête INVITE.
CANCEL	Annulation d'une requête en cours.
BYE	Terminaison d'une session de communication entre agents.
OPTIONS	Requête permettant d'obtenir les informations relatives aux capacités d'un correspondant, sans pour autant établir d'appel.

Tableau II.1 : Requêtes SIP.

➤ Structure des en-têtes des messages « Requêtes » :

Les requêtes décrites ci-dessus, et les réponses présentées plus loin, disposent d'une pile d'en-têtes conforme aux spécifications du RFC822, valable pour http 1.1 [8].

La structure générale des en-têtes de requêtes est la suivante :

Début de ligne
En-tête de messages
CRLF : séparateur
Corps de message

Tableau II.2 : En-tête de requêtes [8].

Avec :

- Début de ligne : ligne de requête ou ligne d'état.
- En-tête : en-tête général ou en-tête de requête ou en-tête de réponse ou en-tête d'entité.
- CRLF : balise pour indiquer la fin du champ d'en-tête et début du corps du message (qui nécessite un en-tête d'entité) [8].

Exemple :

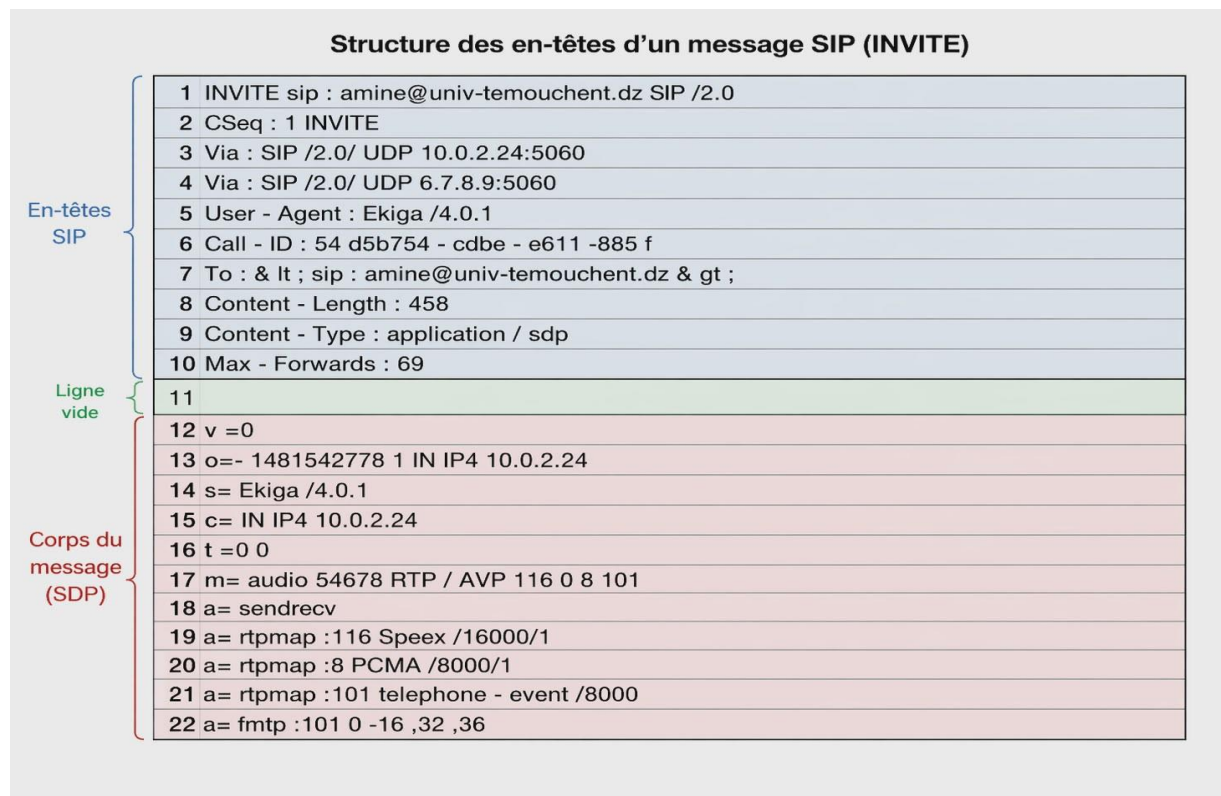


Figure II.4 : structure des en-têtes d'un message SIP.

En-tête	Description	Exemple
Request-Line	Indique le type de requête (INVITE, REGISTER...), l'URI SIP et la version du protocole	INVITE sip:amine@univ-temouchent.dz SIP/2.0
CSeq	Contient le numéro de séquence et le type de requête	CSeq: 1 INVITE
Via	Spécifie le chemin emprunté par la requête (serveurs intermédiaires)	Via : SIP/2.0/UDP 10.0.2.24 :5060
User-Agent	Indique le logiciel ou l'équipement émetteur	User-Agent : Ekiga/4.0.1
Call-ID	Identifiant unique de la session d'appel	Call-ID: 54d5b754-cdbe-e611-885f
To	Identifie le destinataire de la requête	To:<sip:amine@univ-temouchent.dz>

From	Identifie l'émetteur de la requête	From : <sip:user@domain>
Contact	Fournit l'adresse directe pour contacter l'utilisateur	Contact : <sip:user@IP>
Content-Length	Indique la taille du corps du message	Content-Length: 458
Content-Type	Spécifie le type du contenu (généralement SDP)	Content-Type : application/sdp
Max-Forwards	Limite le nombre de relais (sauts) de la requête	Max-Forwards: 69

Tableau II.3 : structure des en-têtes des messages SIP.

Les réponses de ces requêtes SIP :

- **Structure des en-têtes des messages << Réponse >> :** Les réponses ont la même structure d'en-tête que les requêtes décrites précédemment.

Ligne d'état
En-tête général ou réponse ou d'entité
CRLF
Corps de message

Tableau II.4 : En-tête de réponses.

La ligne d'état, est composée de trois parties ; c'est le caractère SP (single space) qui sert de séparateur.

- **SIP-version :** la version de SIP utilisée ;
- **Status-Code :** le code réponse est un code numérique composé de trois chiffres, qui peut être interpréter automatiquement par une machine, et qui fournit le résultat de la requête.
- **Reason-Phrase :** la raison écrite explique en quelques mots ce résultat à l'intention d'un opérateur humain [8].

Exemple :

Exemple : Entête de réponse SIP (200 OK)	
Ligne de statut	1 SIP/2.0 200 OK
	2 Via: SIP/2.0/UDP 10.0.2.24:5060;branch=z9hG4bK-1a2b3c
En-têtes SIP	3 Via: SIP/2.0/UDP 6.7.8.9:5060;branch=z9hG4bK-4d5e6f
	4 From: "Amine" <sip:amine@univ-temouchent.dz>;tag=1928301774
	5 To: <sip:amine@univ-temouchent.dz>;tag=a6c85cf
	6 Call-ID: 54d5b754-cdbe-e611-885f
	7 CSeq: 1 INVITE
Ligne vide	8 Contact: <sip:amine@10.0.2.24:5060>
	9 Content-Type: application/sdp
	10 Content-Length: 435
	11 Server: Ekiga/4.0.1
	12 Date: Tue, 28 May 2024 10:15:20 GMT
Corps du message (SDP)	13
	14 v=0
	15 o=- 1481542778 2 IN IP4 10.0.2.24
	16 s= Ekiga
	17 c= IN IP4 10.0.2.24
	18 t=0 0
	19 m= audio 49170 RTP/AVP 0 8 101
	20 a= sendrecv
	21 a= rtpmap:0 PCMU/8000
	22 a= rtpmap:8 PCMA/8000
	23 a= rtpmap:101 telephone-event/8000
	24 a= fmp:101 0-16

Figure II.5 : Entête de réponse SIP.

Il existe six classes de réponses SIP identifiées par la valeur du premier numéro du code de réponse.

- **Classe 1xx** – " Réponse temporaire " : Requête reçue et traitement de la requête.
- **Classe 2xx** – "Succès" : L'action a été reçue, comprise et acceptée avec succès.
- **Classe 3xx** – "Redirection" : Une action plus éloignée est nécessaire pour achever la requête.
- **Classe 4xx** – "Erreur de Client " : La requête contient une mauvaise syntaxe ou ne peut pas être prise en charge par le serveur.
- **Classe 5xx** – "Erreur de Server" : Le serveur n'a pas répondu correctement à la demande.
- **Classe 6xx** – " une autre erreur" : La requête ne peut être prise en charge par aucun serveur.

Exemple Requête SIP	Exemple Réponse SIP
INVITE sip:amine@univ-temouchant-univ.dz SIP/2.0 Via: SIP/2.0/UDP 10.0.2.24:5060 Via: SIP/2.0/UDP 6.7.8.9:5060 User-Agent: Ekiga/4.0.1 From: sip:client@10.0.0.24 To : sip:amine@univ-temouchant.dz Call-ID : 54d5b754-cdbe-e611-885f CSeq : 1 INVITE Max-Forwards : 69 Content-Type : application/sdp Content-Length : 458	SIP/2.0 200 OK Via : SIP/2.0/UDP 10.0.2.24:5060 Via: SIP/2.0/UDP 6.7.8.9:5060 User-Agent: Ekiga/4.0.1 From: sip:amine@univ-temouchant.dz To : sip:client@10.0.0.24 Call-ID : 54d5b754-cdbe-e611-885f CSeq : 1 INVITE Subject : apple accepté Content-Type : application/sdp Content-Length : 458

Tableau II.5 : exemple des requêtes et réponses SIP.

2.1.2.6 Le fonctionnement :

Enregistrement d'un UA (User Agent) :

Le mécanisme d'enregistrement SIP permet à un utilisateur de signaler sa présence sur le réseau en transmettant ses coordonnées au serveur Registrar. Cette opération garantit que les communications entrantes pourront être dirigées vers le terminal approprié.

Etablissement d'une connexion :

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

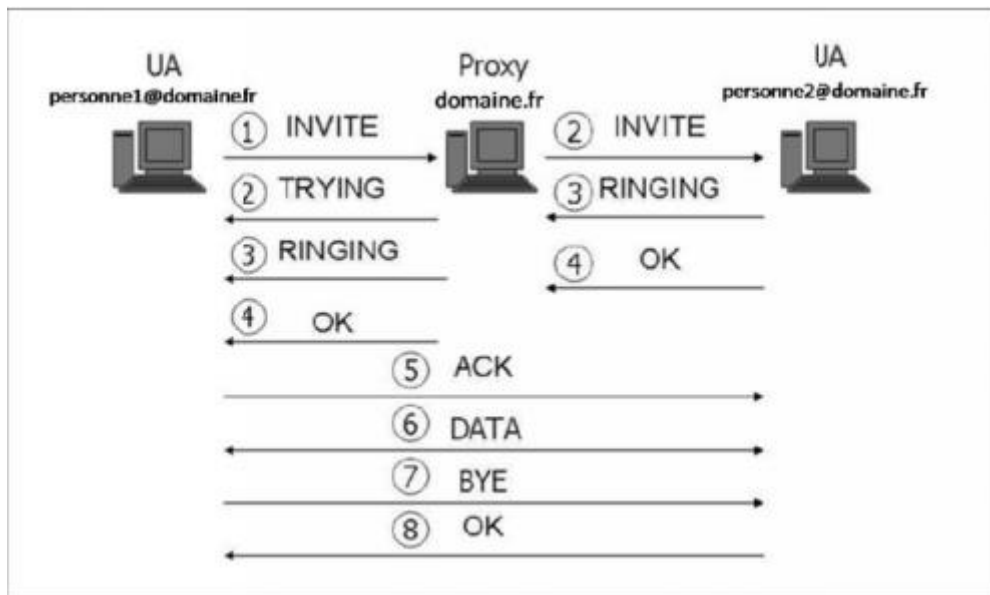


Figure II.6 : Initialisation et fermeture d'une session SIP

1. L'UA appelant envoie une requête INVITE à l'URI de l'appelé pour initier la communication.
2. Le proxy reçoit la requête et répond avec 100 TRYING pour indiquer qu'il traite la demande.
3. L'UA appelé fait sonner le téléphone et envoie 180 RINGING pour signaler que l'appel est en cours d'attente.
4. Lorsque l'appelé accepte, il envoie 200 OK, que le proxy transmet à l'appelant.
5. L'UA appelant envoie un message ACK pour confirmer, et la connexion est alors établie.
6. Les deux UA communiquent directement entre eux (sans passer par le proxy) via une connexion indépendante de la signalisation SIP.
7. Pour terminer l'appel, un UA envoie un message BYE.
8. L'autre UA répond avec 200 OK, ce qui met fin à la communication.

2.1.2.7 Mode de communication :

On distingue également deux modes précis d'ouverture de sessions avec SIP que l'on va détailler :

- Mode Point à point : communication entre deux postes ;
- Mode diffusif : Plusieurs postes membre d'un serveur.
- **Mode point à point :** Le mode point à point est donc une communication simple entre deux sans passer par une passerelle.



Figure II.7 : Mode point à point.

Pour ouvrir une session, un utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de s'accorder sur la comptabilité de leur média. L'appelant et l'appelé doivent être identifiés via son URL SIP qui est du même type qu'une URL mailto (**utilisateur@machine**). Pour le mode point à point on utilise donc l'adresse IP du poste à joindre dans le logiciel de communication : **sip:nom@adresseip**. Pour ouvrir une session, l'appelant envoie une requête contenant l'URL SIP du destinataire [10].

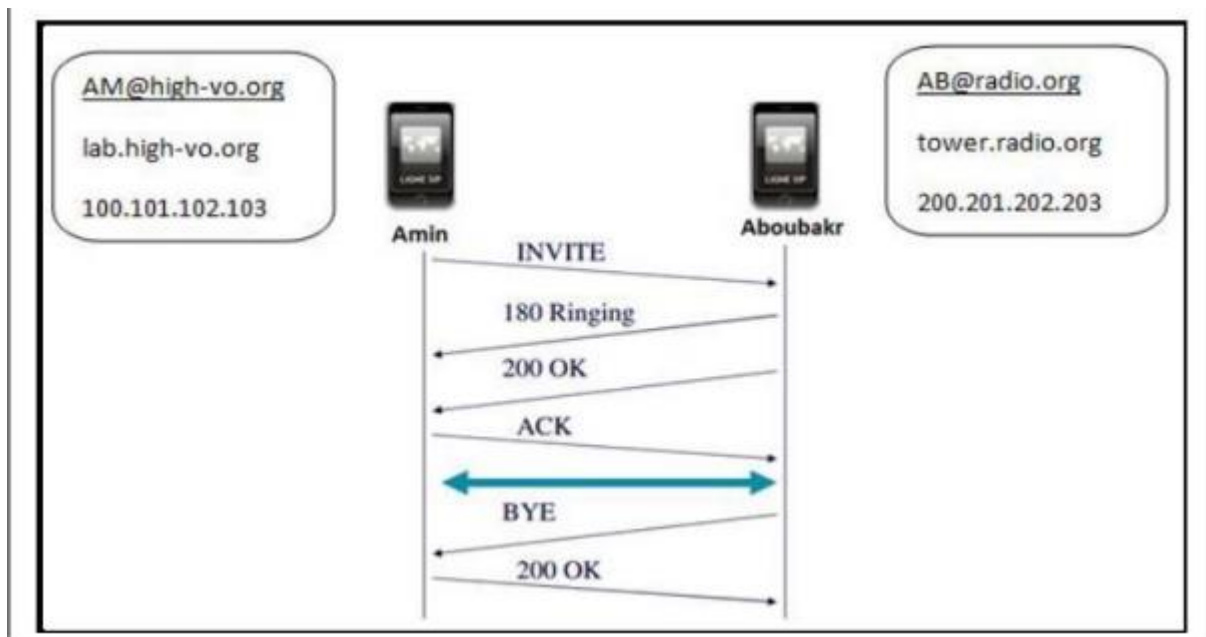


Figure II.8 : Les paquets de Mode point à point.

- **Mode diffusif** : Dans ce mode, la communication entre les utilisateurs s'effectue à travers un équipement intermédiaire chargé de transmettre les informations échangées.



Figure II.9 : mode diffusif.

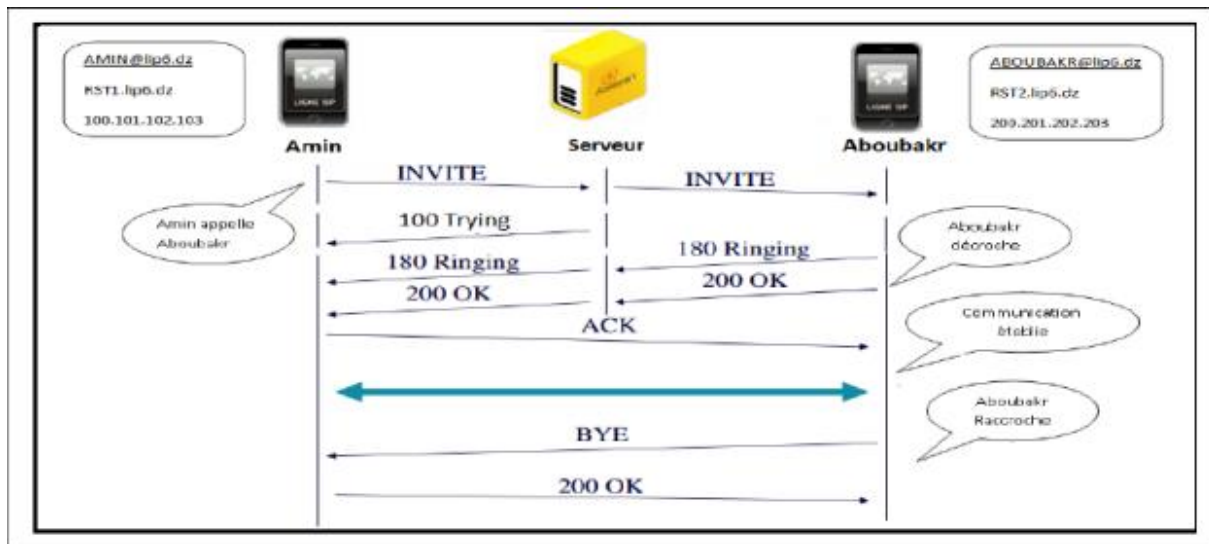


Figure II.10 : Les paquets de Mode diffusif.

2.1.2.8 Les serveurs :

Il existe trois types de serveurs :

- **Les serveurs d'enregistrement :**

Reçoivent les mises à jour concernant la localisation actuelle des utilisateurs.

- **Les serveurs proxy :**

Un serveur proxy Reçoit les requêtes des UA et les redirige vers un autre serveur proxy, un UAS ou un serveur de redirection. Il a accès aussi à une base de données ou à un service de localisation (location service) pour déterminer vers où rediriger la requête reçue.

L'interface entre le serveur proxy et la base de données/le service de localisation n'est pas définie par le protocole SIP.

Les serveurs proxy peuvent travailler en deux modes :

- **Stateless proxy :** dans ce cas le proxy est un simple élément de redirection, il ne garde pas d'information concernant la requête reçue et redirigée.

- **Stateful proxy** : contrairement à un stateless proxy, un stateful proxy mémorise toutes les informations concernant les requêtes entrantes et essaie plusieurs localisations de l'utilisateur et renvoie la meilleure réponse.
- ❖ En utilisant un serveur proxy :

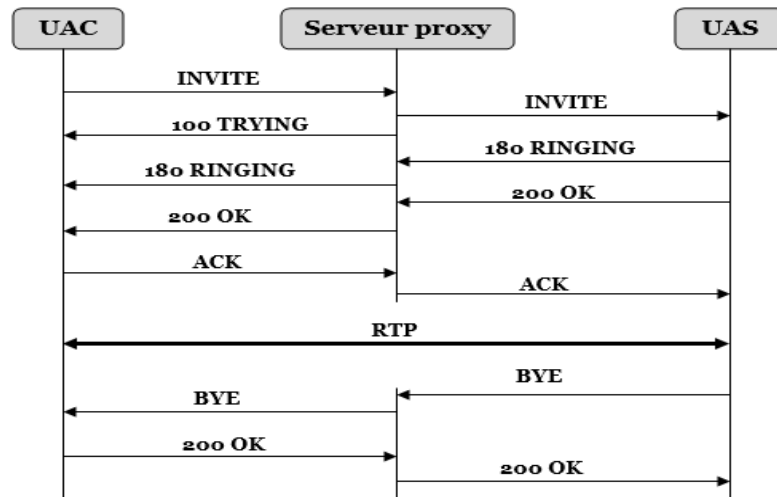


Figure II.11 : Un appel SIP en utilisant un serveur proxy.

- **Les serveurs de redirection :**

Quand un serveur de redirection reçoit une requête, au lieu de la rediriger il renvoie l'adresse du prochain serveur au client qui devra le contacter directement.

- ❖ En utilisant un serveur de redirection :

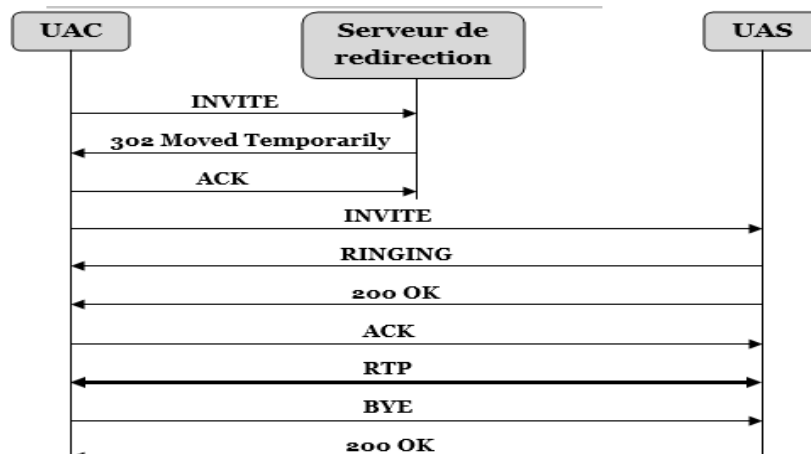


Figure II.12 : Un appel SIP en utilisant un serveur de redirection

2.1.2.9 Avantage et inconvénients du protocole SIP :

- **Les avantages :**

1. Rapide et simple d'utilisation.
2. Bonne gestion de la mobilité.
3. Le protocole SIP est également utilisé pour tout type de sessions multimédias.

- **Les inconvénients :**

1. Mauvaise implémentation.
2. Faible nombre d'utilisateurs.
3. Maturité du protocole (Version 2).

2.1.3 Comparaison entre H323 et SIP :

	SIP	H.323
Nombre d'échanges pour établir la connexion	1,5 aller-retour	6 à 7 allers - retours
Maintenance du code protocolaire	Simple	Complexe et nécessitant un compilateur
Evolution du protocole	Protocole ouvert	Ajoute d'extensions propriétaires
Fonction de conférence	Distribuée	Centralisée par l'unité MC
Fonction de télé services	Oui	H.323 v2 +H.450
Détection d'un appel en boucle	Oui	Non
Signalisation multicast	Oui	Non

Tableau II.6 : comparaison entre le protocole H.323 et SIP.

2.2 Les protocoles de transport :

2.2.1 Protocole RTP :

Le protocole RTP (Real-time Transport Protocol) est utilisé pour transporter les données multimédias, telles que la voix et la vidéo, en temps réel sur les réseaux IP. Il ajoute des informations importantes, notamment les numéros de séquence et les horodatages, afin de faciliter la réception correcte des paquets. Ces informations permettent au récepteur de détecter les pertes de paquets, de remettre les paquets dans le bon ordre si nécessaire et d'assurer une transmission fluide des flux audio et vidéo. En outre, RTP peut être utilisé avec la diffusion multicast pour envoyer un même flux à plusieurs destinataires.

2.2.2.1 Format des paquets RTP :



Format du paquet RTP

RTP est un protocole qui permet de transporter des données audio ou vidéo après leur encodage. Les données sont envoyées sous forme de paquets RTP, et chaque paquet contient :

- Un en-tête (header) pour les informations de contrôle
- Un payload qui contient les données audio ou vidéo

Ensuite, le paquet RTP passe par UDP qui ajoute son propre en-tête, puis par IP qui ajoute aussi son en-tête.

À la fin, on obtient un datagramme IP qui est envoyé sur le réseau jusqu'à la destination, où il est transmis à la bonne application pour être utilisé.

2.2.2 Le protocole RTCP :

Le protocole RTCP (Real-time Transfert Control Protocol) est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. C'est un protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service. Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus. La périodicité est calculée en fonction du nombre de participants de l'application. On peut dire que les paquets RTP ne transportent que les données des utilisateurs. Tandis que les paquets RTCP ne transportent en temps réel, que de la supervision.

2.2.3 Le protocole UDP :

Le protocole UDP (User Datagram Protocol) est un protocole de la couche transport dans le modèle TCP/IP qui fonctionne sans établir de connexion préalable. Il est très simple car il n'assure pas de mécanisme de vérification ou de correction des erreurs. Son rôle principal consiste à encapsuler les données en ajoutant des numéros de ports, qui représentent des canaux logiques permettant d'acheminer les informations vers l'application appropriée.

2.2.4 Le protocole SRTP :

SRTP est conçu pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux. Il couvre les lacunes de protocoles de sécurité existants comme IPsec (IP Security), dont le mécanisme d'échanges de clés est trop lourd. Il est aussi bâti sur le protocole temps réel RTP (Real Time Transport Protocol). Il associe aussi une demi-douzaine

de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles d'initiation de session de voix sur IP tel que SIP (Session Initiation Protocol), ainsi que le protocole de diffusion de contenu multimédia en temps réel RTSP (Real Time Streaming Protocol).

3 Conclusion

Dans ce chapitre, Nous avons analysé les protocoles de signalisation les plus répandus et établi une comparaison approfondie entre les protocoles H.323 et SIP, ainsi qu'entre les protocoles de transport RTP et RTCP. De plus, nous avons étudié les avantages et les inconvénients de chacune de ces technologies.

Chapitre III

**Mise en œuvre d'une solution
VoIP basée sur Asterisk :
configuration, sécurisation et
interconnexion RTC.**

1. Introduction

Avec le développement des réseaux informatiques, la téléphonie traditionnelle évolue vers la VoIP (Voice over IP), qui permet de transmettre la voix via les réseaux IP.

Dans ce chapitre, nous allons réaliser une solution assurant la transmission de la voix sur un réseau IP. Pour cela, nous allons utiliser la solution libre Asterisk. Nous présenterons les étapes d'installation et de configuration d'Asterisk sous le système d'exploitation linux. Le but de cette installation est de permettre le passage des appels entre différents utilisateurs d'un réseau. Dans notre cas, nous allons configurer deux utilisateurs en utilisant le système Debian 12 dans une machine virtuelle, ainsi que l'interconnexion d'une liaison RTC avec la voix IP.

2. Définitions des concepts clés

2.1.Définition d'Asterisk :

Asterisk est un logiciel open source qui transforme un ordinateur en un autocommutateur téléphonique PABX (Private Automatic Branch eXchange) qui est une entité logique, presque toujours gérée par un équipement matériel physique dont la fonction est au moins triple : router les appels au sein d'un réseau privé, interconnecter les réseaux et gérer les services de téléphonie. D'une grande puissance et souplesse, Asterisk est capable de gérer la téléphonie analogique, mais il se distingue surtout par sa prise en charge de la voix sur IP (VoIP). Il implémente plusieurs protocoles de communication, notamment H.320, H.323, SIP.

➤ Fonctions principales :

- Gestion des appels VoIP.
- Serveur SIP. (Permet d'établir et gérer les communications.)
- Messagerie vocal.
- Conférences audio.

2.2.Définition de Linux :

Linux est un système d'exploitation (OS) open source basé sur le noyau Linux. Il fonctionne sur les ordinateurs, les serveurs, les mobiles et une large gamme d'autres appareils, il est idéal pour les applications réseau comme la VoIP [11].

2.3.Définition de Debian 12 :

Debian est un système d'exploitation libre, développé et géré par le projet Debian. Il s'agit d'une distribution GNU/Linux stable et sécurisée qui intègre plusieurs dizaines de milliers d'applications prêtes à l'emploi afin de répondre à l'ensemble des besoins des utilisateurs.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

En tant que version stable et moderne du système d'exploitation, Debian 12 constitue une plateforme idéale pour installer Asterisk.

➤ **Rôle d'utilisation :**

- ✓ Utilisé comme système d'exploitation pour les serveurs grâce à sa stabilité.
- ✓ Permet la gestion et l'administration des réseaux informatiques.
- ✓ Utilisé pour l'hébergement de différentes applications et services.

➤ **Caractéristiques :**

- Gratuit et libre.
- Stable et sécurise.
- Très utilisé dans les serveurs.

2.4.Définition de la machine virtuelle :

Une machine virtuelle ou VM (*Virtual Machine*) est un environnement entièrement virtualisé qui fonctionne sur une machine physique. Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipements qu'une machine physique : CPU, mémoire RAM, disque dur et carte réseau. Plusieurs machines virtuelles avec des OS différents peuvent coexister sur le même serveur physique : Linux, MacOS, Windows..., Ces environnements sont créés et gérés à l'aide de solutions de virtualisation, telles que VMware Workstation ou Oracle VirtualBox [12].

➤ **Avantage :**

- ✓ Permet d'effectuer des tests sans modifier le système principal.
- ✓ Assure l'isolation des systèmes et des applications.
- ✓ Facilite la simulation d'un environnement réseau.
- ✓ Réduit les coûts matériels grâce à l'exécution de plusieurs systèmes sur une seule machine.
- ✓ Offre une gestion simple des sauvegardes et des restaurations.

3. Architecture de la solution VoIP

La figure illustre l'architecture réseau adoptée pour le déploiement et la configuration de la solution de VoIP à base d'Asterisk :

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

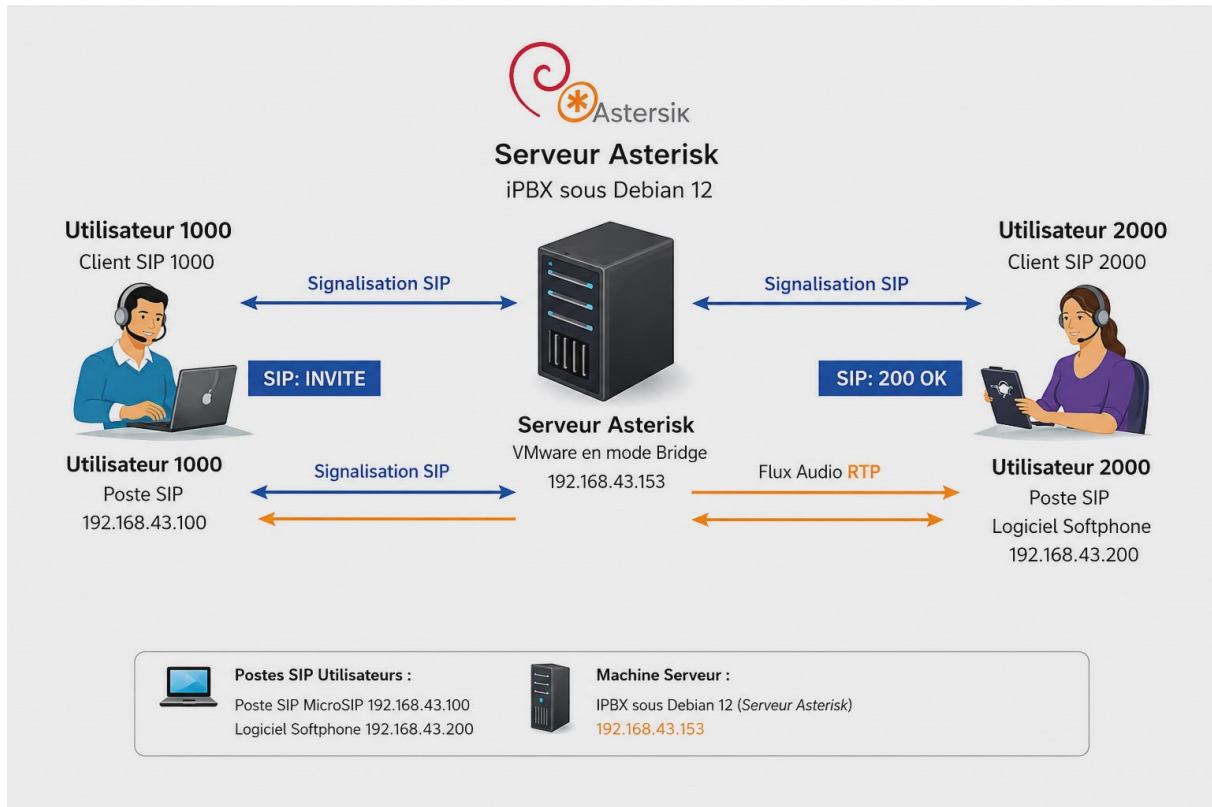


Figure III.1 : Architecture de communication SIP sous Asterisk.

4. Installation d'Asterisk sous Debian 12

Les étapes pour l'installation sont les suivantes :

4.1. Mise à jour du système : Avant d'installer Asterisk, on Commence par mettre à jour le système.

```
root@debian:~# apt-get upgrade
```

➤ Télécharger et installer toutes les mises à jour disponibles pour les programmes déjà installés.

4.2. Installation des dépendances : Il faut ensuite installer les dépendances nécessaires à Asterisk.

```
root@debian:~# apt-get install gcc make
root@debian:~# apt-get install pkg-config build-essential wget
root@debian:~# apt-get install libssl-dev libncurses5-dev
root@debian:~# apt-get install libnewt-dev libxml2-dev
root@debian:~# apt-get install linux-headers-$(uname -r) uuid-dev
root@debian:~# apt-get install libsqlite3-dev libjansson-dev
```

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

Nom du paquetage	Rôle principe	Utilisation dans Asterisk
gcc	Compilateur C	Compiler le code source d'Asterisk
make	Outil de compilation	Exécuter les scripts de build
pkg-config	Gestion des dependences	Trouver les bibliothèques installées
build-essential	Outils de development	Installer gcc, make et outils essentiels
wget	Téléchargement	Télécharger Asterisk depuis Internet
libssl-dev	Bibliothèque SSL	Sécuriser les communications (TLS)
libncurses5-dev	Interface terminal	Interface de configuration (menu config)
libnewt-dev	Interface text avancée	Menus interactifs asterisk
libxml2-dev	Traitement XML	Gestion des fichiers XML
linux-headers-\$(uname -r)	En-tête noyau	Compilation des modules
uuid-dev	Identifiants unique	Gestion des sessions
libsqlite3-dev	Base de données	Stockage des données
libjansson-dev	Bibliothèque JSON	Support API (ARI)

Tableau III.1 : Paquetages nécessaires pour l'installation et la compilation d'Asterisk

4.3.Création d'un dossier pour les sources : On crée un répertoire où on va placer les sources d'Asterisk dans **/usr/src**.

```
root@debian:~# mkdir -p /usr/src/asterisk
root@debian:~# cd /usr/src/asterisk
```

- **mkdir** : crée un dossier appelé asterisk dans **/usr/src**.
- ❖ C'est là où on va placer les sources d'Asterisk.

4.4.Télécharger et décompresser les sources d'Asterisk : On télécharge l'Asterisk, la version installée d'Asterisk était la version 18.

```
root@debian:~# cd /usr/src/asterisk/
root@debian:~# wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-18-current.tar.gz
```

- Télécharger l'archive **.tar.gz** contenant les fichiers sources d'Asterisk.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

```
root@debian:~# tar -xvzf asterisk-18-current.tar.gz
root@debian:~# rm asterisk-18-current.tar.gz
root@debian:~# cd asterisk-18.26.4/
```

- Cette commande permet d'accéder au répertoire source d'Asterisk contenant les fichiers nécessaires à la compilation et à l'installation du système.

4.5.Compilation et installation :

```
root@debian:~# sudo apt install libedit-dev -y
root@debian:~# cd /usr/src/asterisk
root@debian: /usr/src/asterisk# ls
asterisk-18.26.4  asterisk-18-current.tar.gz  index.html
root@debian: /usr/src/asterisk # cd asterisk-18.26.4
root@debian: /usr/src/asterisk/asterisk-18.26.4# ./configure
```

- Avant la configuration il manque une dépendance : **libedit-dev**



Figure III.2 : configuration d'Asterisk réussie

- C'est un peu comme une checklist des prérequis

Il faut ensuite choisir les options de compilation.

```
root@debian: /usr/src/asterisk-18.26.4# make menuselect
```

- On ajoute les sons en français dans les sections Core Sound Package, et Extras Sound Package.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

```
Add-ons (See README-addons.txt)      [ ] CORE-SOUNDS-ES-G722
Applications                          [ ] CORE-SOUNDS-ES-SLN16
Bridging Modules                      [ ] CORE-SOUNDS-ES-SIREN7
Call Detail Recording                 [ ] CORE-SOUNDS-ES-SIREN14
Channel Event Logging                 [ ] CORE-SOUNDS-FR-WAV
Channel Drivers                       [ ] CORE-SOUNDS-FR-ULAW
Codec Translators                    [*] CORE-SOUNDS-FR-ALAW
Format Interpreters                   [ ] CORE-SOUNDS-FR-GSM
Dialplan Functions                    [ ] CORE-SOUNDS-FR-G729
PBX Modules                           [ ] CORE-SOUNDS-FR-G722
Resource Modules                      [ ] CORE-SOUNDS-FR-SLN16
Test Modules                          [ ] CORE-SOUNDS-FR-SIREN7
Compiler Flags                        [ ] CORE-SOUNDS-FR-SIREN14
Voicemail Build Options               [ ] CORE-SOUNDS-IT-WAV
Utilities                             [ ] CORE-SOUNDS-IT-ULAW
AGI Samples                           [ ] CORE-SOUNDS-IT-ALAW
Core Sound Packages                   [ ] CORE-SOUNDS-IT-GSM
Music On Hold File Packages           [ ] CORE-SOUNDS-IT-G729
Extras Sound Packages                 [ ] CORE-SOUNDS-IT-G722
                                      [ ] CORE-SOUNDS-IT-SLN16
```

Figure III.3 : Ajout et configuration des packages sonores français dans le serveur Asterisk.

```
Add-ons (See README-addons.txt)      --- Core ---
Applications                          [ ] EXTRA-SOUNDS-EN-WAV
Bridging Modules                      [ ] EXTRA-SOUNDS-EN-ULAW
Call Detail Recording                 [ ] EXTRA-SOUNDS-EN-ALAW
Channel Event Logging                 [ ] EXTRA-SOUNDS-EN-GSM
Channel Drivers                       [ ] EXTRA-SOUNDS-EN-G729
Codec Translators                    [ ] EXTRA-SOUNDS-EN-G722
Format Interpreters                   [ ] EXTRA-SOUNDS-EN-SLN16
Dialplan Functions                    [ ] EXTRA-SOUNDS-EN-SIREN7
PBX Modules                           [ ] EXTRA-SOUNDS-EN-SIREN14
Resource Modules                      [ ] EXTRA-SOUNDS-EN_GB-WAV
Test Modules                          [ ] EXTRA-SOUNDS-EN_GB-ULAW
Compiler Flags                        [ ] EXTRA-SOUNDS-EN_GB-ALAW
Voicemail Build Options               [ ] EXTRA-SOUNDS-EN_GB-GSM
Utilities                             [ ] EXTRA-SOUNDS-EN_GB-G729
AGI Samples                           [ ] EXTRA-SOUNDS-EN_GB-G722
Core Sound Packages                   [ ] EXTRA-SOUNDS-EN_GB-SLN16
Music On Hold File Packages           [ ] EXTRA-SOUNDS-EN_GB-SIREN7
Extras Sound Packages                 [ ] EXTRA-SOUNDS-EN_GB-SIREN1
                                      [ ] EXTRA-SOUNDS-FR-WAV
                                      [ ] EXTRA-SOUNDS-FR-ULAW
                                      [*] EXTRA-SOUNDS-FR-ALAW
                                      [ ] EXTRA-SOUNDS-FR-GSM
                                      [ ] EXTRA-SOUNDS-FR-G729
                                      [ ] EXTRA-SOUNDS-FR-G722
                                      [ ] EXTRA-SOUNDS-FR-SLN16
                                      [ ] EXTRA-SOUNDS-FR-SIREN7
                                      [ ] EXTRA-SOUNDS-FR-SIREN14
```

Figure III.4 : Sélection des packages audio supplémentaires (Extras Sound Packages).

Vous pouvez aussi ajouter les musiques d'attente en format ALAW.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

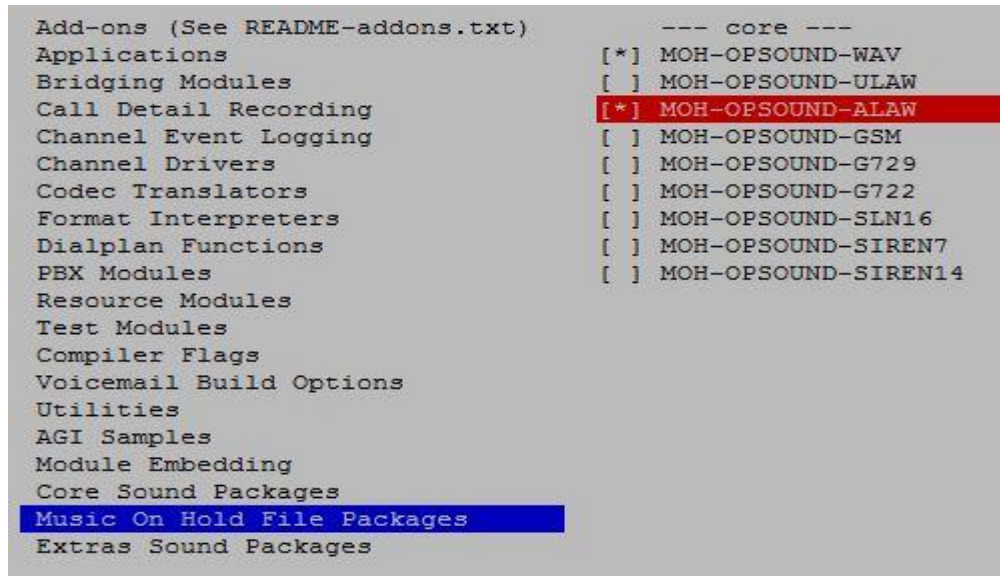


Figure III.5 : Sélection des fichiers de musique d'attente (Music On Hold).

Après on va lancer la compilation et l'installation.

```
root@debian: /usr/src/asterisk-18.26.4# make
```

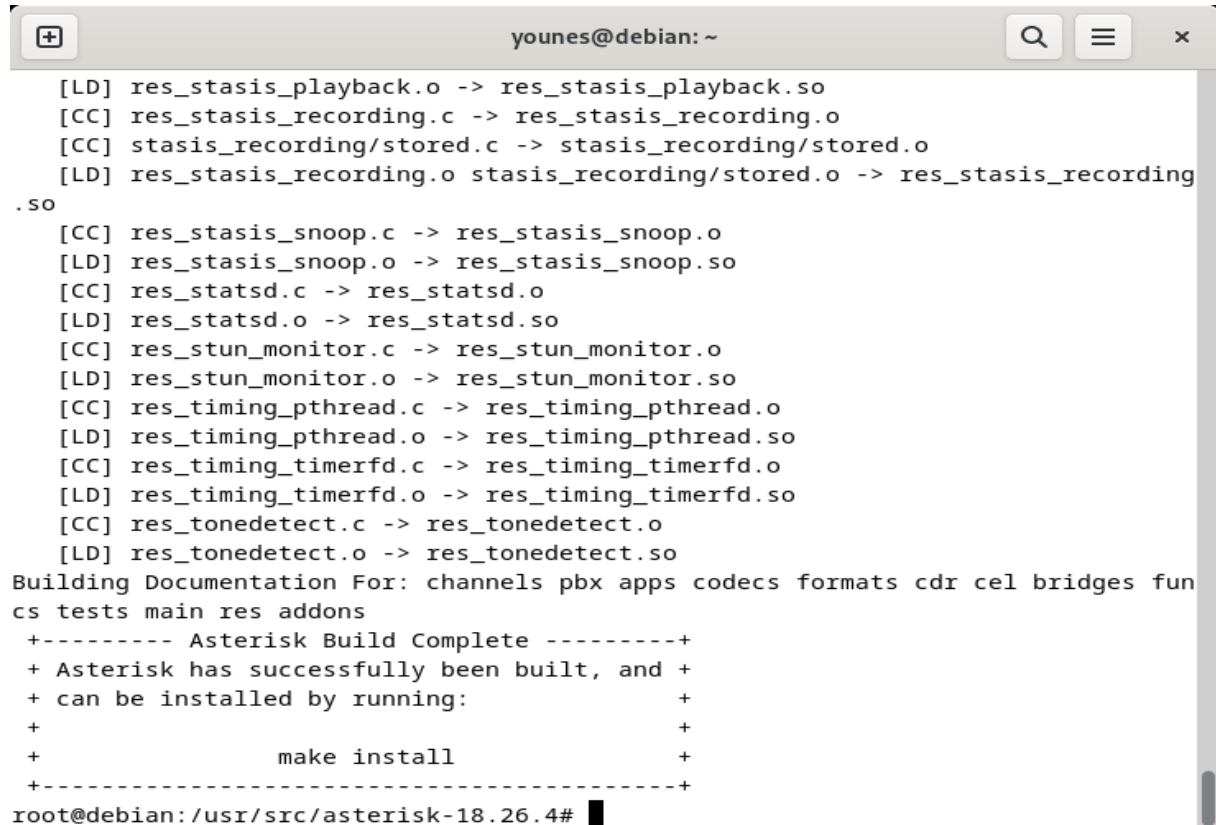
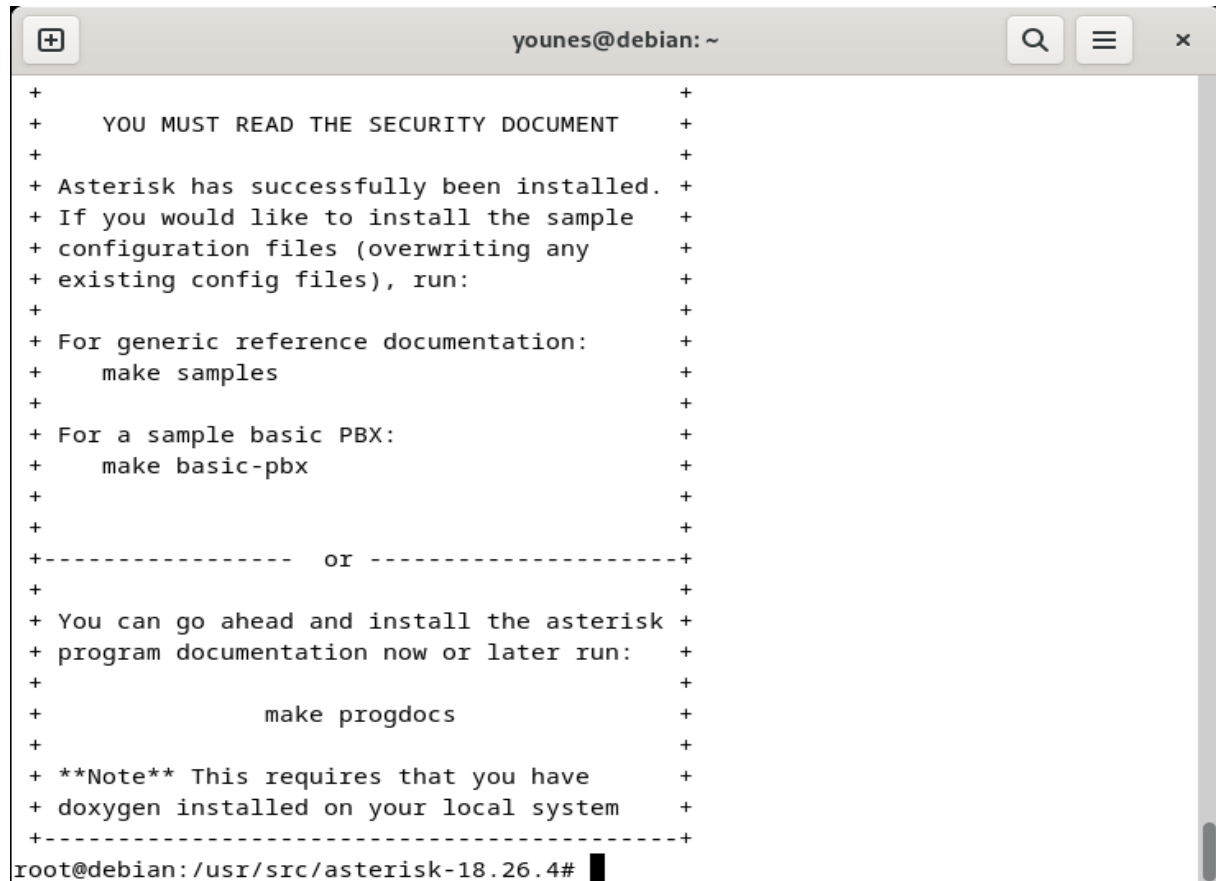


Figure III.6 : Compilation réussie d'Asterisk avant son installation.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

```
root@debian: /usr/src/asterisk-18.26.4# make install
```

- Copie les fichiers compilés dans les bons dossiers (**/etc/asterisk**).



```
younes@debian: ~  
+  
+ YOU MUST READ THE SECURITY DOCUMENT +  
+  
+ Asterisk has successfully been installed. +  
+ If you would like to install the sample +  
+ configuration files (overwriting any +  
+ existing config files), run: +  
+  
+ For generic reference documentation: +  
+ make samples +  
+  
+ For a sample basic PBX: +  
+ make basic-pbx +  
+  
+----- or -----+  
+ You can go ahead and install the asterisk +  
+ program documentation now or later run: +  
+  
+ make progdocs +  
+  
+ **Note** This requires that you have +  
+ doxygen installed on your local system +  
+-----+  
root@debian: /usr/src/asterisk-18.26.4#
```

Figure III.7 : Validation de l'installation d'Asterisk après make install.

L'étape suivante consiste à déployer les fichiers d'exemple de configuration au sein du répertoire système **etc/asterisk/**

```
root@debian: /usr/src/asterisk-18.26.4# make samples
```

- **make samples** : (optionnelle) permet de créer des fichiers de configuration de base. (Elle peut être utile par la suite pour revenir à une configuration d'origine d'asterisk).
- Enfin, on procède à la génération et à l'installation des scripts de démarrage système.

```
root@debian: /usr/src/asterisk-18.26.4# make config
```

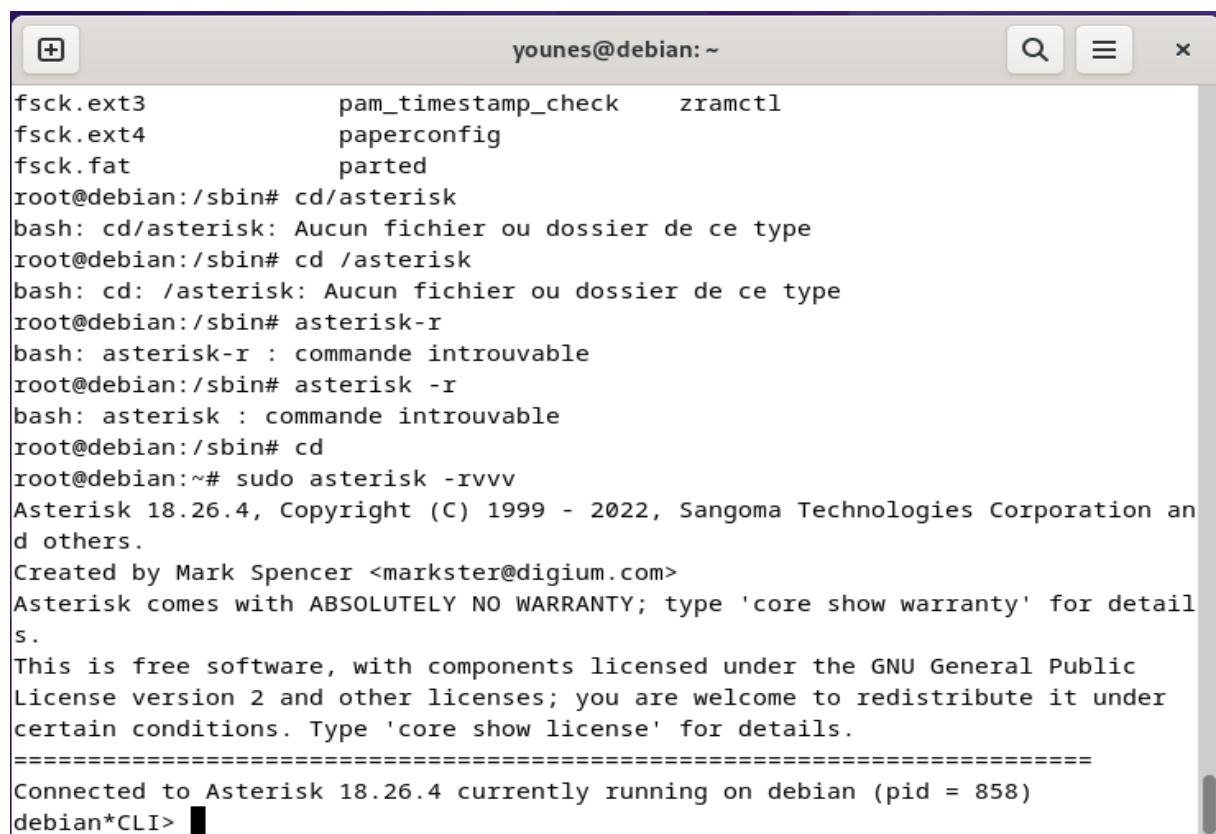
- **make config** charge le serveur Asterisk au démarrage du système.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

4.6.Démarrage du service : Lancement d'Asterisk à l'aide des commandes suivantes :

```
root@debian:~# /etc/init.d/asterisk start
root@debian:/sbin# cd
root@debian:~# sudo asterisk -rvvv
```

- Il suffit maintenant de lancer le serveur, et de se connecter à la console CLI (Command Line Interface).



```
younes@debian: ~
fsck.ext3      pam_timestamp_check  zramctl
fsck.ext4      paperconfig
fsck.fat       parted
root@debian:/sbin# cd/asterisk
bash: cd/asterisk: Aucun fichier ou dossier de ce type
root@debian:/sbin# cd /asterisk
bash: cd: /asterisk: Aucun fichier ou dossier de ce type
root@debian:/sbin# asterisk-r
bash: asterisk-r : commande introuvable
root@debian:/sbin# asterisk -r
bash: asterisk : commande introuvable
root@debian:/sbin# cd
root@debian:~# sudo asterisk -rvvv
Asterisk 18.26.4, Copyright (C) 1999 - 2022, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 18.26.4 currently running on debian (pid = 858)
debian*CLI>
```

Figure III.8 : Vérification du bon fonctionnement d'Asterisk via la commande asterisk -rvvv.

5. Configuration et création des comptes utilisateurs

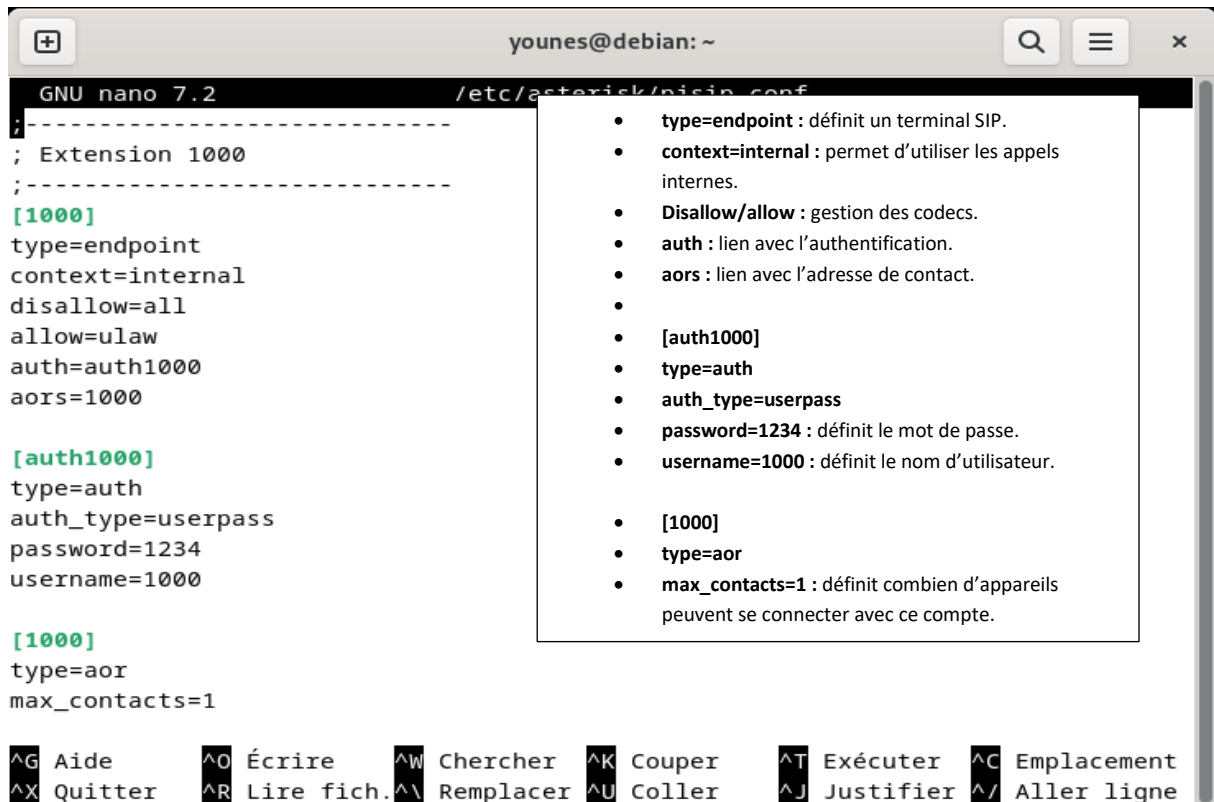
5.1.Identification des fichiers de configuration : Une fois l'installation d'Asterisk est effectuée, plusieurs fichiers sont créés :

- /usr/sbin/ : Contient le fichier binaire d'Asterisk (programme principal).
- /usr/lib/asterisk/ : Contient les fichiers binaires qu'Asterisk utilise pour fonctionner.
- /etc/asterisk/ : Contient tous les fichiers de configurations.

5.2. Configuration des comptes utilisateurs :

Dans un premier temps, les deux fichiers qui vont nous intéresser sont '**pjsip.conf**' et '**extensions.conf**', On va créer des utilisateurs utilisant le protocole SIP pour l'établissement de la connexion, on accède au fichier '**pjsip.conf**' en tapant **nano /etc/asterisk/pjsip.conf** et pour le fichier '**extensions.conf**' en tapant **nano /etc/asterisk/extensions.conf**.

✓ Voici les lignes à introduire dans le fichier **pjsip.conf** pour la création de deux clients SIP :



```
GNU nano 7.2 /etc/asterisk/pjsip.conf
;-----
; Extension 1000
;-----
[1000]
type=endpoint
context=internal
disallow=all
allow=ulaw
auth=auth1000
aors=1000

[auth1000]
type=auth
auth_type=userpass
password=1234
username=1000

[1000]
type=aor
max_contacts=1
```

- **type=endpoint** : définit un terminal SIP.
- **context=internal** : permet d'utiliser les appels internes.
- **Disallow/allow** : gestion des codecs.
- **auth** : lien avec l'authentification.
- **aors** : lien avec l'adresse de contact.
-
- **[auth1000]**
- **type=auth**
- **auth_type=userpass**
- **password=1234** : définit le mot de passe.
- **username=1000** : définit le nom d'utilisateur.
-
- **[1000]**
- **type=aor**
- **max_contacts=1** : définit combien d'appareils peuvent se connecter avec ce compte.

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne

Figure III.9 : Utilisateur 1000.

```

GNU nano 7.2 /etc/asterisk/pjsip.conf
;-----
; Extension 2000
;-----
[2000]
type=endpoint
context=internal
disallow=all
allow=ulaw
auth=auth2000
aors=2000

[auth2000]
type=auth
auth_type=userpass
password=5678
username=2000

[2000]
type=aor
max_contacts=1

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne

```

Figure III.10 : Utilisateur 2000.

5.3. Configuration du Dialplan (extensions) : La configuration des extensions s'effectue dans Le fichier extensions.conf.

```

GNU nano 7.2 /etc/asterisk/ex
; Content-Length: 14
;
; check-messages
;
;exten => 6882,1,noOp()
; same => n,Answer()
; same => n,PJSIPNotify(&Event=Custom&Co
; same => n,Wait(1)
; same => n,Hangup()
[internal]
exten => 1000,1,Dial(PJSIP/1000,20)
exten => 1000,n,Hangup()

exten => 2000,1,Dial(PJSIP/2000,20)
exten => 2000,n,Hangup()

```

- **[internal]** : même contexte que celui définit lors de la création des utilisateurs.
- **exten** : instruction pour déclarer un numéro.
- **1000,2000** : Numéro d'utilisateurs.
- **1** : la priorité de l'instruction.
- **Dial** : application pour lancer l'appel.
- **PJSIP** : protocole utilisé.
- **20** : Durée en seconde de l'application avant de passer à la priorité 2.
- **Hangup** : application pour raccrocher

```

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne

```

Figure III.11 : la rubrique extensions.

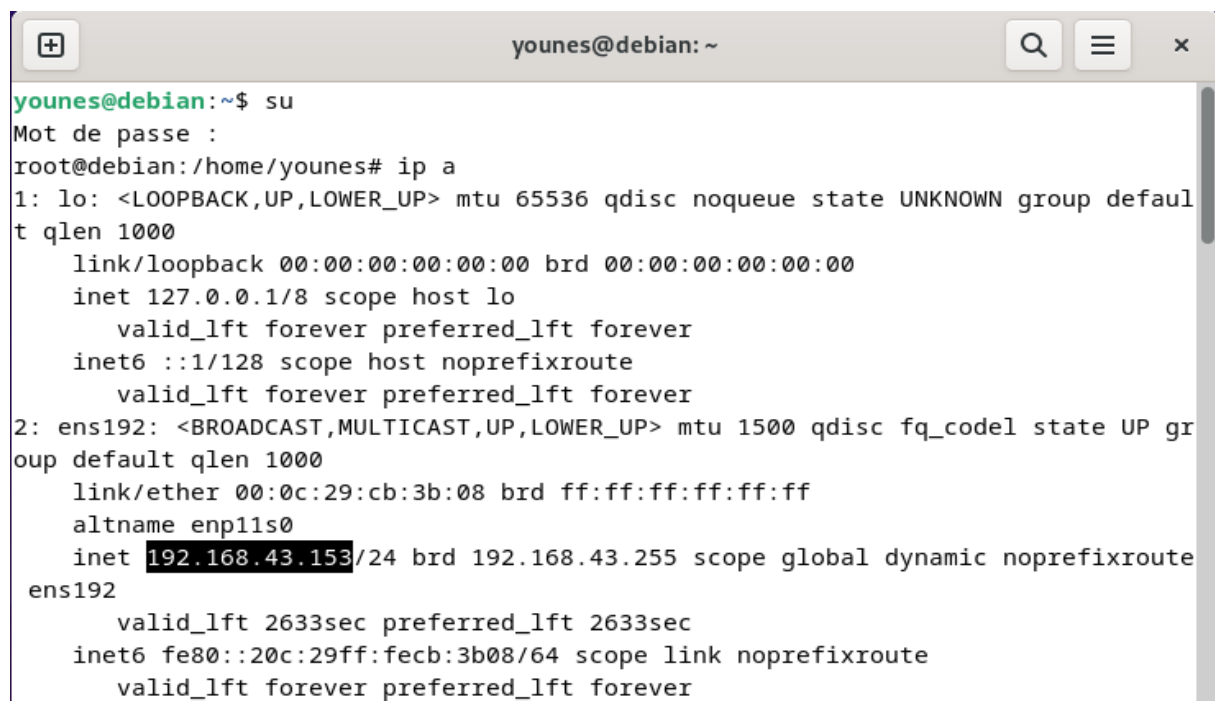
6. Configuration de MicroSIP avec Asterisk

Nous allons expliciter la démarche permettant de configurer un client SIP (MicroSIP) avec notre serveur Asterisk, afin d'établir une communication VoIP au sein du réseau interne. Cette configuration a pour objectif la création d'extensions (comptes utilisateurs) permettant de passer des appels de manière bidirectionnelle entre les différents postes.

6.1. MicroSIP : est un logiciel client SIP léger utilisé pour passer et recevoir des appels via un serveur VoIP.

6.2. Configuration de MicroSIP : Pour configurer MicroSIP, il suffit de créer un nouveau compte SIP et remplir les informations comme nom du compte et l'adresse du serveur Asterisk et le nom d'utilisateur, le mot de passe, Domain.

- ✓ Pour ajouter l'adresse du serveur Asterisk, il faut vérifier que la machine virtuelle dispose d'une configuration réseau active. L'identification de son adresse IP s'effectue dans le terminal à l'aide de la commande suivante :



```
younes@debian:~$ su
Mot de passe :
root@debian:/home/younes# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:cb:3b:08 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.43.153/24 brd 192.168.43.255 scope global dynamic noprefixroute ens192
        valid_lft 2633sec preferred_lft 2633sec
    inet6 fe80::20c:29ff:fe3b:08/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Figure III.12: l'adresse IP d'Asterisk.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

- ✓ On termine la configuration de MicroSIP en enregistrant toutes les informations qu'elle contient :

The screenshot shows the 'Compte' (Account) configuration window in MicroSIP. The fields are filled with the following values:

- Nom du compte: 1000
- Serveur SIP: 192.168.43.153
- Proxy SIP: (empty)
- Nom d'utilisateur*: 1000
- Domaine*: 192.168.43.153
- Login: (empty)
- Mot de passe: (masked with ****)
- Nom à afficher: (empty)
- N° de la boîte vocale: (empty)
- Préfixe d'appel: (empty)
- Plan de numérotation: (empty)
- ☐ Masquer l'identifiant de l'appelant
- Chiffrement: Désactivé
- Transport: UDP
- Adresse publique: Auto
- Actualiser l'enregistr...: 300
- Signalisation: 15
- ☐ Afficher ma présence
- ☐ Autoriser la réécriture de l'IP
- ☐ ICE
- ☐ Désactiver les minuteurs de session

Buttons at the bottom: Supprimer le compte, Sauvegarder, Annuler.

Figure III.13 : configuration de l'utilisateur 1000.

- ✓ Après, on prend un autre PC pour y configurer le deuxième compte (extension 2000) et entrer ses informations :

The screenshot shows the 'Compte' (Account) configuration window in MicroSIP for user 2000. The fields are filled with the following values:

- Nom du compte: 2000
- Serveur SIP: 192.168.43.153
- Proxy SIP: (empty)
- Nom d'utilisateur*: 2000
- Domaine*: 192.168.43.153
- Login: 2000
- Mot de passe: (masked with ****)
- Nom à afficher: (empty)
- N° de la boîte vocale: (empty)
- Préfixe d'appel: (empty)
- Plan de numérotation: (empty)
- ☐ Masquer l'identifiant de l'appelant
- Chiffrement: Désactivé
- Transport: UDP
- Adresse publique: Auto
- Actualiser l'enregistr...: 300
- Signalisation: 15
- ☐ Afficher ma présence
- ☐ Autoriser la réécriture de l'IP
- ☐ ICE
- ☐ Désactiver les minuteurs de session

Buttons at the bottom: Supprimer le compte, Sauvegarder, Annuler.

Figure III.14 : configuration de l'utilisateur 2000.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

- ✓ Après validation, le statut doit devenir Disponible.

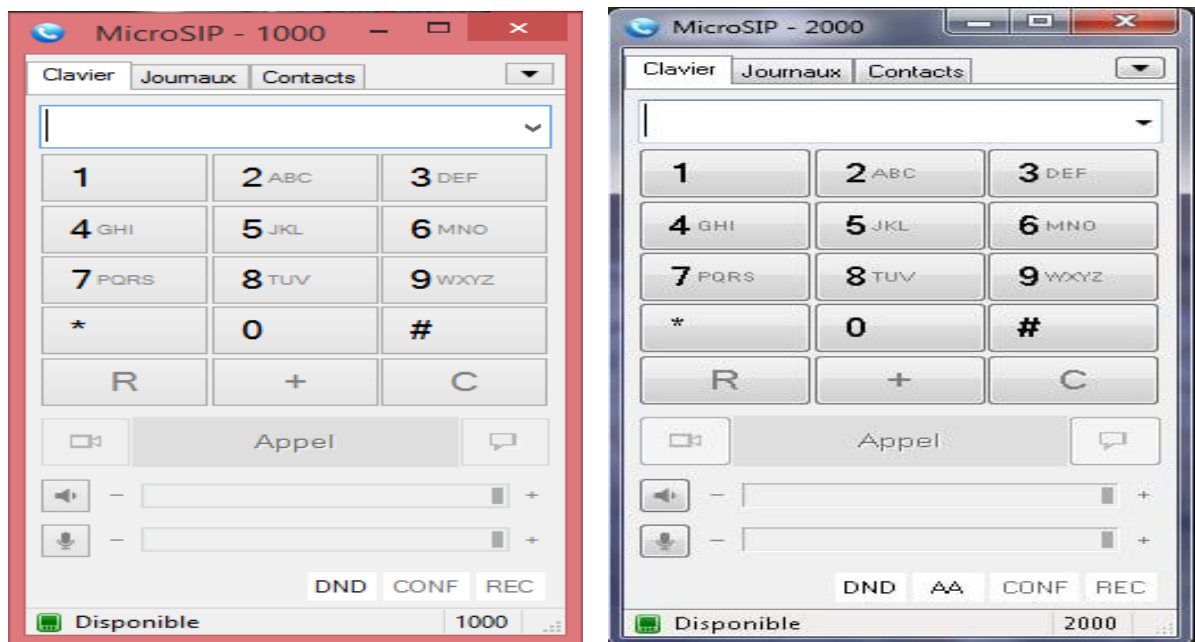


Figure III.15 : État « Disponible » des postes SIP après l'enregistrement.

- ✓ Après cette étape on va démarrer le service Asterisk on utilise :

```
younes@debian: ~  
root@debian:/home/younes# /usr/sbin/asterisk -cvvv  
Asterisk already running on /var/run/asterisk/asterisk.ctl. Use 'asterisk -r' to connect.
```

Figure III.16 : Démarrage du service Asterisk utilisant la commande `/usr/sbin/asterisk -cvvv`

- ✓ Ensuite, pour accéder à l'interface CLI d'Asterisk :

```
root@debian:/home/younes# /usr/sbin/asterisk -rvvv  
Asterisk 18.26.4, Copyright (C) 1999 - 2022, Sangoma Technologies Corporation and others.  
Created by Mark Spencer <markster@digium.com>  
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.  
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.  
=====
```

```
Connected to Asterisk 18.26.4 currently running on debian (pid = 1000)  
debian*CLI>
```

Figure III.17 : Connexion à l'interface de commande d'Asterisk avec `asterisk -rvvv`

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

- Cette commande permet de superviser le fonctionnement du serveur en temps réel.
- ✓ La vérification des extensions SIP dans l'interface CLI d'Asterisk se fait en tapant la commande suivante :

```
=====
Connected to Asterisk 18.26.4 currently running on debian (pid = 1000)
debian*CLI> pjsip show endpoints

Endpoint: <Endpoint/CID.....> <State.....> <Channels.>
I/OAuth: <AuthId/UserName.....>
Aor: <Aor.....> <MaxContact>
Contact: <Aor/ContactUri.....> <Hash.....> <Status> <RTT(ms)..>
Transport: <TransportId.....> <Type> <cos> <tos> <BindAddress.....>
Identify: <Identify/Endpoint.....>
Match: <criteria.....>
Channel: <ChannelId.....> <State.....> <Time.....>
Exten: <DialedExten.....> CLCID: <ConnectedLineCID.....>
=====

Endpoint: 1000                                Not in use      0 of inf
InAuth: auth1000/1000
Aor: 1000                                     1
Contact: 1000/sip:1000@192.168.43.148:60355;ob f00884cb67 NonQual nan

Endpoint: 2000                                Not in use      0 of inf
InAuth: auth2000/2000
Aor: 2000                                     1
Contact: 2000/sip:2000@192.168.43.10:52417;ob 1ee3e0df67 NonQual nan

Objects found: 2
debian*CLI> █
```

Figure III.18 : Résultat de la vérification de l'enregistrement des extensions SIP dans Asterisk.

- ✓ Donc, les deux extensions sont disponibles (« Not in use » signifie que l'extension est disponible et libre pour recevoir un appel).

6.3.Test de communication : pour tester le système il faut effectuer un appel de 1000 vers 2000.

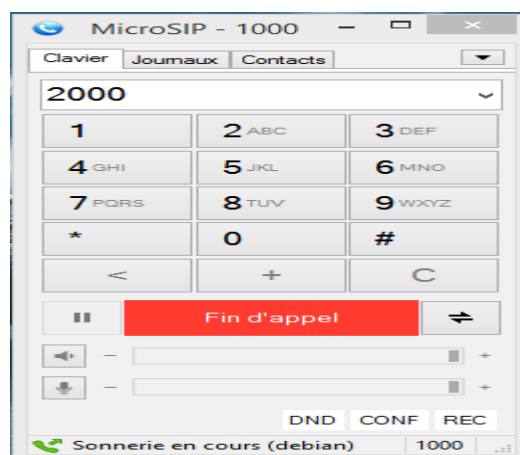


Figure III.19 : Test d'un appel de 1000 vers 2000.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

```
=====
Endpoint: 1000                                Not in use 0
of inf
  InAuth: auth1000/1000
  Aor: 1000
  Contact: 1000/sip:1000@192.168.43.148:60355;ob 1 f00884cb67 NonQual
          nan

Endpoint: 2000                                Not in use 0
of inf
  InAuth: auth2000/2000
  Aor: 2000
  Contact: 2000/sip:2000@192.168.43.10:52417;ob 1 1ee3e0df67 NonQual
          nan

Objects found: 2

-- Executing [2000@internal:1] Dial("PJSIP/1000-0000000c", "PJSIP/2000,20")
in new stack
-- Called PJSIP/2000
-- PJSIP/2000-0000000d is ringing
debian*CLI>
```

Figure III.20 : lancement de l'appel 1.

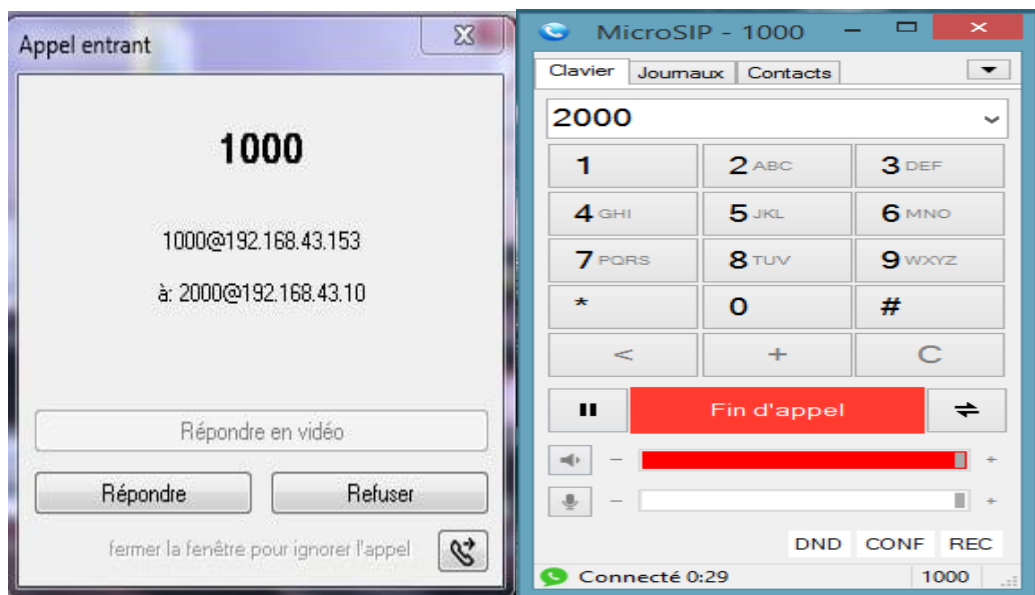


Figure III.21 : Utilisateur 2000 accepter l'appel de l'utilisateur 1000.

✓ On peut aussi tester l'appel de 2000 vers 1000.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.



Figure III.22 : Test d'un appel de 2000 vers 1000.

```
=====
Endpoint: 1000                                     Not in use  0
of inf
  InAuth: auth1000/1000
  Aor: 1000                                         1
  Contact: 1000/sip:1000@192.168.43.148:60355;ob   f00884cb67 NonQual
  nan
Endpoint: 2000                                     Not in use  0
of inf
  InAuth: auth2000/2000
  Aor: 2000                                         1
  Contact: 2000/sip:2000@192.168.43.10:55910;ob   591083edc5 NonQual
  nan
Objects found: 2
-- Executing [1000@internal:1] Dial("PJSIP/2000-00000019", "PJSIP/1000,20")
in new stack
-- Called PJSIP/1000
-- PJSIP/1000-0000001a is ringing
debian*CLI>
```

Figure III.23 : lancement de l'appel 2.

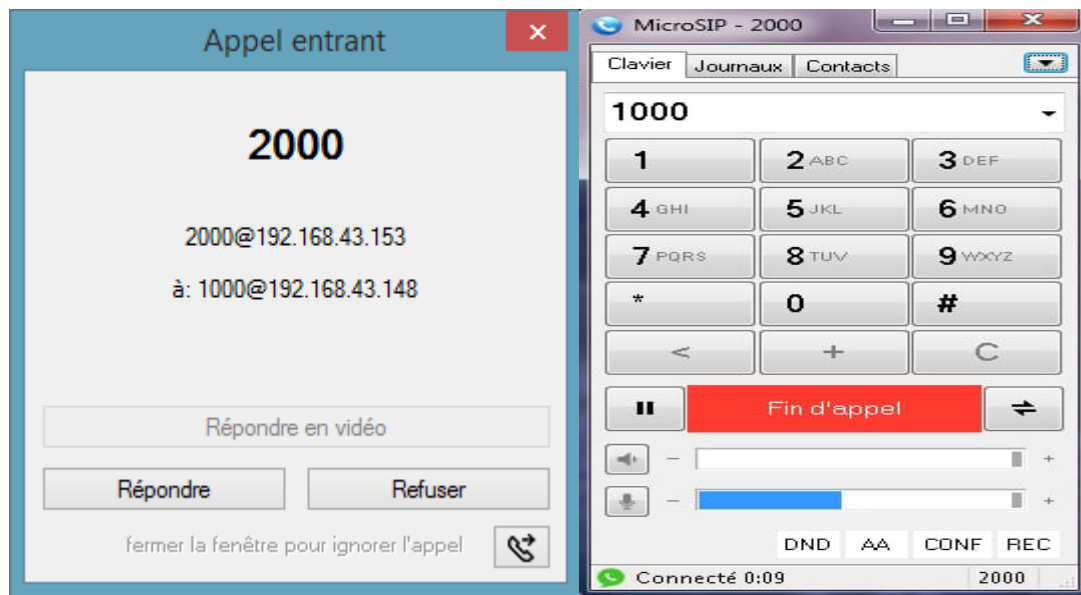


Figure III.24 : Utilisateur 1000 accepter l'appel de l'utilisateur 2000.

7. Capture du trafic en utilisant Wireshark

Wireshark est un logiciel libre d'analyse de protocoles, utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro - ingénierie, mais aussi le piratage. C'est l'analyseur réseau le plus populaire du monde. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau.

Nous essayerons de capturer les paquets qui circulent dans notre réseau et spécialement les paquets SIP et RTP qui sont utilisés dans la communication VoIP pour déterminer quelques informations telles que les adresses IP, les numéros de ports, et d'autres informations qui servent au piratage. Ainsi nous pouvons écouter une communication entre deux clients en décodant les paquets RTP.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

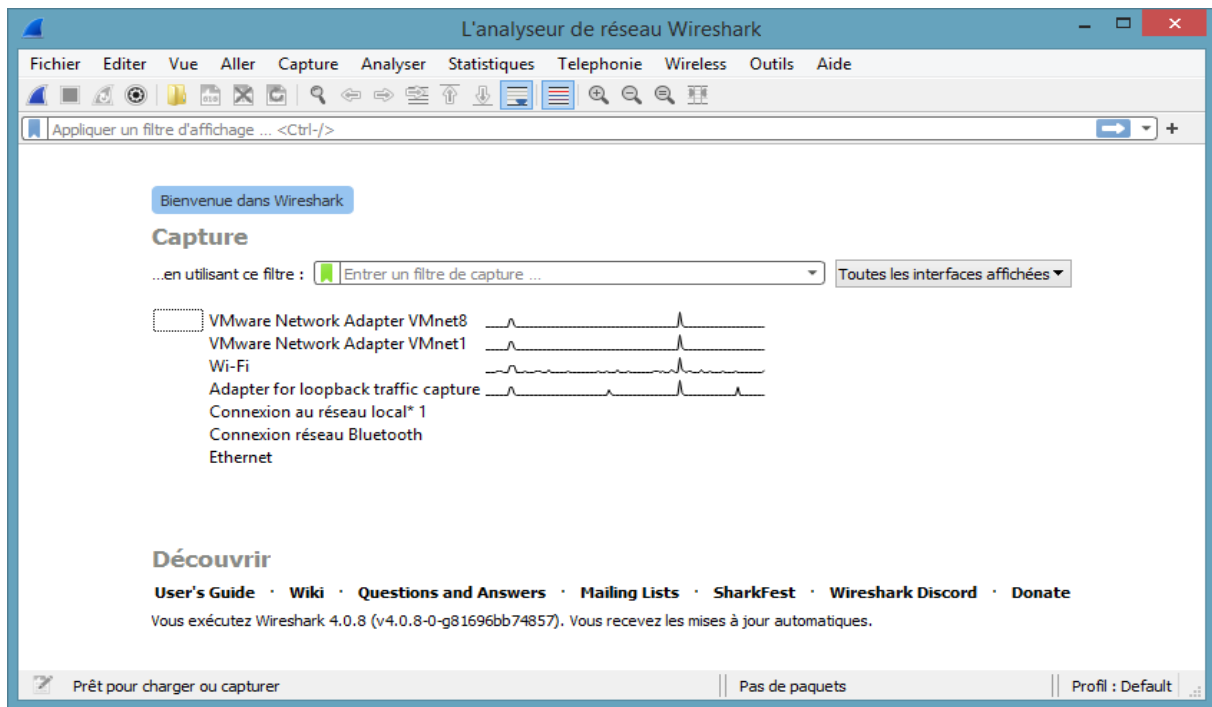


Figure III.25 : ouverture de Wireshark.

7.1.Capture de trafic : une capture réseau a été réalisée sur l'interface active (Wi-Fi).

Un appel a été lancé entre un client sur PC (MicroSIP) (1000) et un client sur téléphone (MizuDroid) (2000).

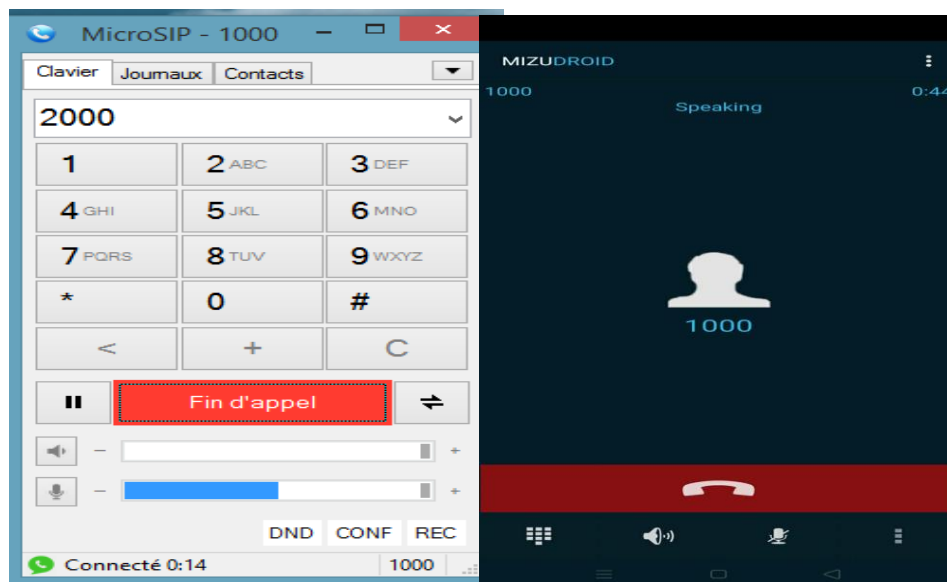


Figure III.26 : Test d'appel VoIP entre un client sur PC (MicroSIP) (1000) et un client sur téléphone (MizuDroid) (2000).

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

En appliquant le filtre suivant : **sip**

On obtient ce résultat :

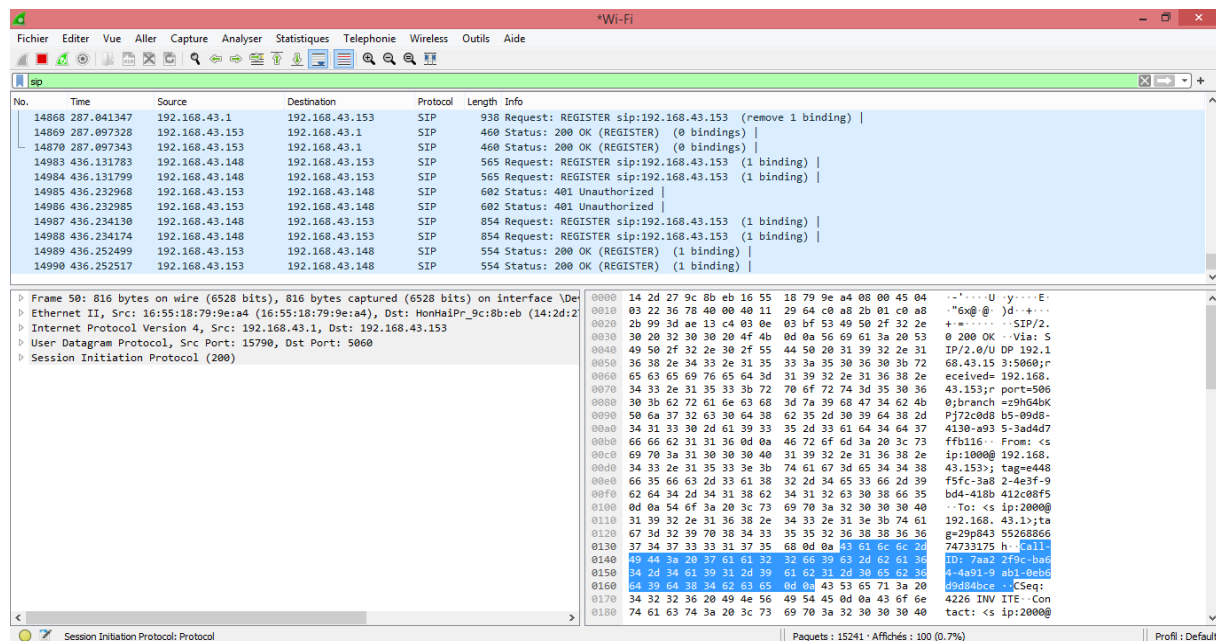


Figure III.27 : écran de Wireshark (sip).

➤ Nous avons observé la séquence complète d'établissement d'appel :

1. INVITE
2. 100 Trying
3. 180 Ringing
4. 200 OK
5. ACK
6. BYE

✓ cette séquence confirme le bon fonctionnement du protocole SIP.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

```

Frame 50: 816 bytes on wire (6528 bits), 816 bytes captured (6528 bits) on interface \Device\NPF_{002F373E-9A3A-489B-B4E4-D6B2AB9C9869}, id 0
Ethernet II, Src: 16:55:18:79:9e:a4 (16:55:18:79:9e:a4), Dst: HonHaiPr_9c:8b:eb (14:2d:27:9c:8b:eb)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.153
User Datagram Protocol, Src Port: 15790, Dst Port: 5060
Session Initiation Protocol (200)
  Status-Line: SIP/2.0 200 OK
  Message Header
    Via: SIP/2.0/UDP 192.168.43.153;received=192.168.43.153;rport=5060;branch=z9hG4bKpJ72c0d8b5-09d8-4130-a935-3ad4d7ffb116
    From: <sip:1000@192.168.43.153>;tag=e448f5fc-3a82-4e3f-9bd4-418b412c08f5
    To: <sip:2000@192.168.43.1>;tag=29p8435526886674733175h
      SIP to address: sip:2000@192.168.43.1
        SIP to address User Part: 2000
        SIP to address Host Part: 192.168.43.1
      SIP to tag: 29p8435526886674733175h
    Call-ID: 7aa22f9c-ba64-4a91-9ab1-0eb6d9d84bce
    [Generated Call-ID: 7aa22f9c-ba64-4a91-9ab1-0eb6d9d84bce]
  CSeq: 4226 INVITE
    Sequence Number: 4226
    Method: INVITE
  Contact: <sip:2000@192.168.43.1:15790>
    Contact URI: sip:2000@192.168.43.1:15790
      Contact URI User Part: 2000
      Contact URI Host Part: 192.168.43.1
      Contact URI Host Port: 15790
    User-Agent: MizuDroid/4.4.25060
    Supported: replaces
    Allow: ACK,PRACK,BYE,CANCEL,INVITE,UPDATE,MESSAGE,INFO,OPTIONS,SUBSCRIBE,NOTIFY,REFER
    Content-Type: application/sdp
    Content-Length: 200
  Message Body
    Session Description Protocol

```

Figure III.28 : Exemple de paquet contenant une réponse SIP 200 OK.

Ensuite, nous avons analysé du flux RTP en utilisant le filtre suivant : **rtp**.

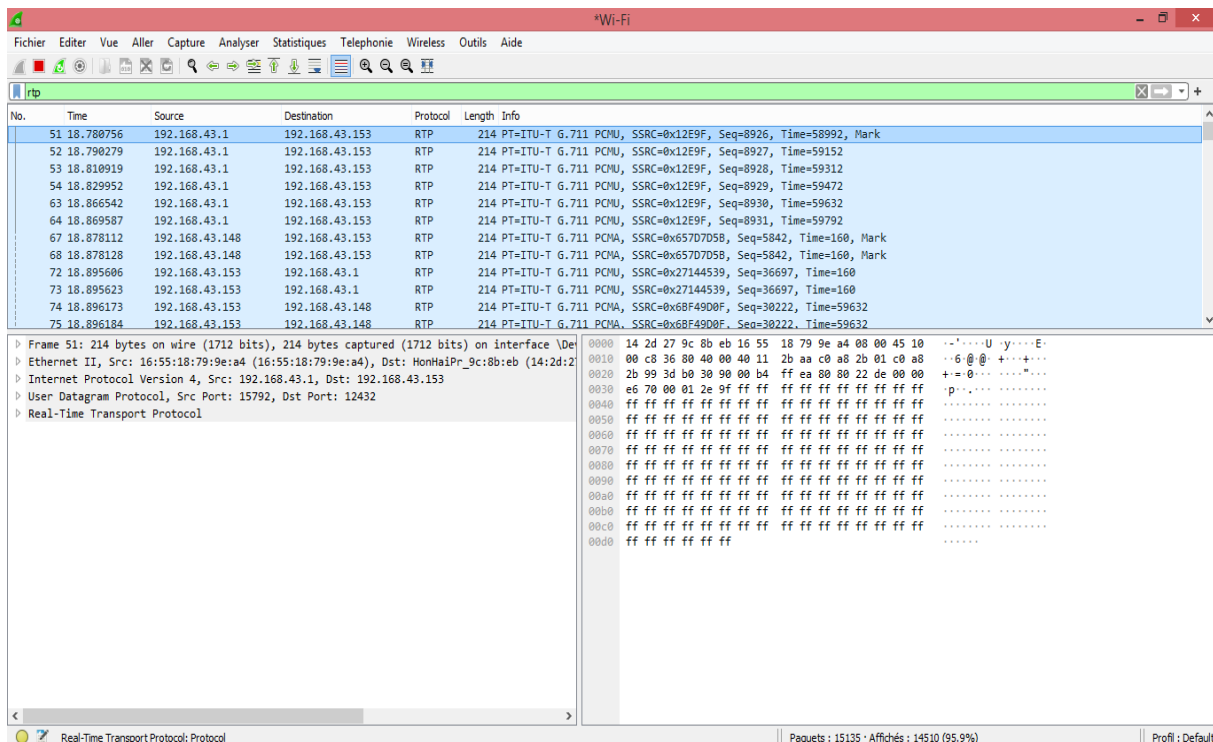


Figure III.29 : écran de Wireshark (rtp).

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

- Comme nous pouvons le voir dans les figures, la conversation entre ces deux hôtes a été capturée. La fenêtre principale de Wireshark comprend deux grandes parties. Dans la première partie, nous voyons les différentes étapes de connexion entre les deux clients. Dans la deuxième partie, celle la plus intéressante, nous pouvons lire le contenu des paquets et donc collecter des informations très indispensables pour effectuer une bonne attaque.
- ✓ Nous allons maintenant procéder au décodage de l'appel. Dans le menu de Wireshark, nous cliquons sur le bouton «Téléphonie», puis ensuite le bouton «Appels VoIP»

Téléphonie



Appels VoIP

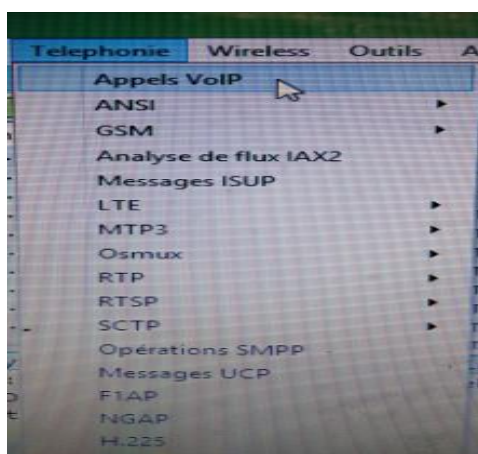


Figure III.30 : accéder au décodage d'appel

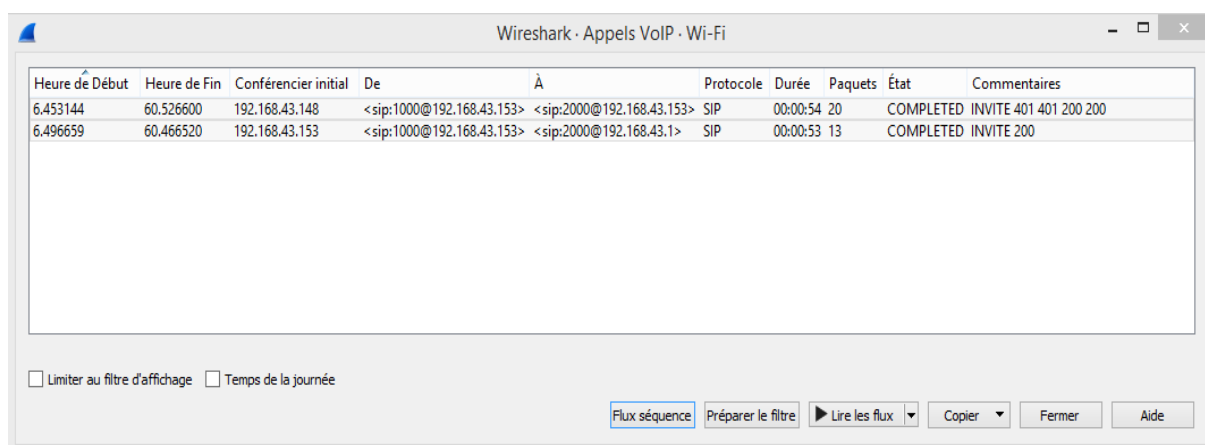


Figure III.31 : Communication téléphonique détectée.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

Après on va sélectionner les deux adresses SIP et cliquer sur le bouton «Lire les flux », une fenêtre « RTP Player » s’ouvre alors pour le décodage :

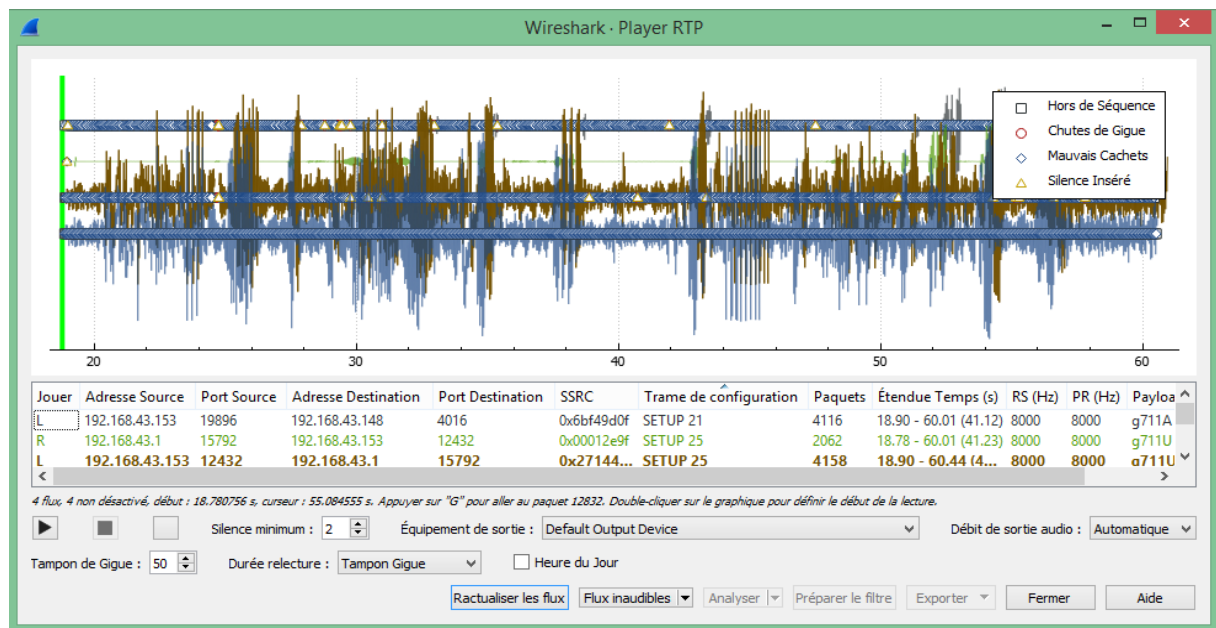


Figure III.32 : Communication décodée (RTP Player).

Maintenant que le décodage a abouti nous pouvons aussi voir sur la figure que le son est décodé et qu'il est prêt à être écouté en appuyant sur le bouton « Démarrer la lecture».

7.2.Visualisation et analyse du processus d'établissement d'un appel SIP :

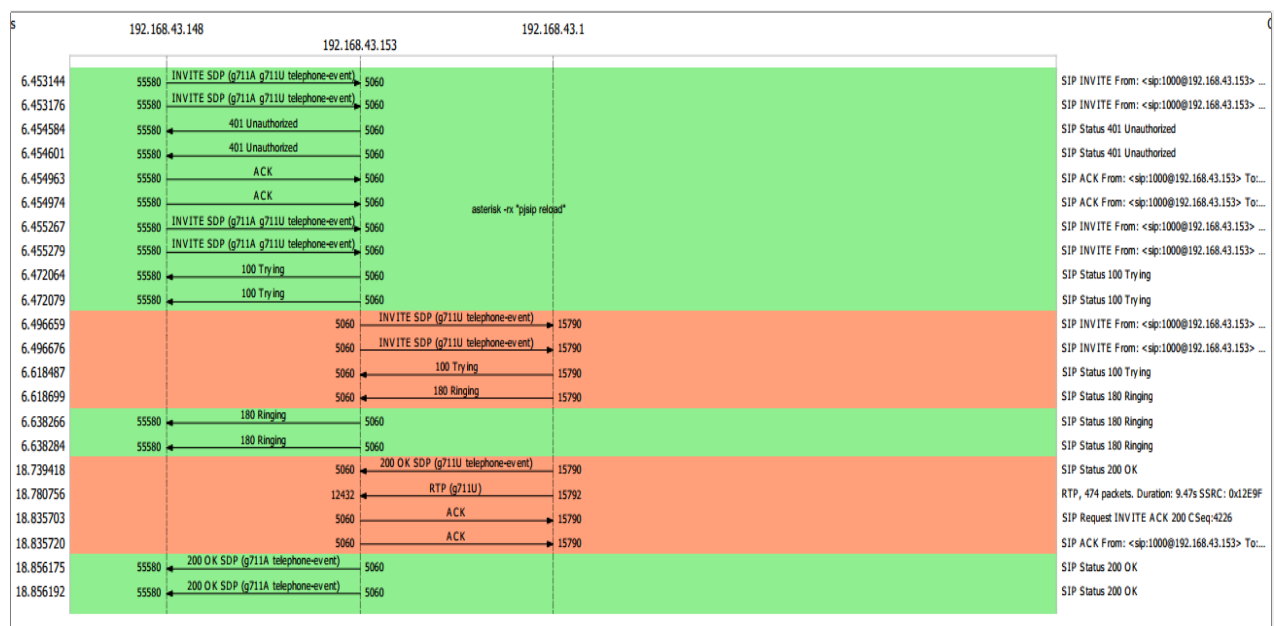


Figure III.33 : Capture du flux SIP entre les extensions 1000 et 2000.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

- Dans cette figure nous allons représenter une capture du trafic sip réalisée avec wireshark, illustrant le déroulement complet d'un appel entre deux terminaux (extensions 1000et 2000) via le serveur Asterisk.

7.2.1 Analyse du scénario : on observe les étapes suivantes :

1. INVITE : le client envoie une requête SIP INVITE pour initier l'appel.
 2. 401 Unauthorized : le serveur demande une authentification.
 3. ACK : le client accuse réception.
 4. INVITE (avec authentification) : nouvelle tentative avec identifiants.
 5. 100 Trying : le serveur traite la requête.
 6. 180 Ringing : le téléphone 2000 commence à sonner.
 7. 200 OK : acceptation de l'appel
 8. ACK : confirmation finale.
 9. RTP : début de transmission audio.
- ✓ Ces échanges confirment que la signalisation SIP fonctionne correctement et que la communication audio est établie avec succès.

8. Sécurisation des appels VoIP entre clients via SRTP

Dans cette partie, nous avons mis en place un mécanisme de sécurisation des communications VoIP en utilisant le protocole SRTP (Secure Real-Time Transport Protocol).

Cette méthode permet de chiffrer le flux RTP transportant la voix, empêchant ainsi toute interception ou écoute via des outils d'analyse réseau tels que Wireshark.

La configuration a été réalisée au niveau du serveur Asterisk ainsi que du client MicroSIP.

8.1.Etapes de sécurisation du trafic RTP par SRTP :

- ##### 8.1.1. Activation de la sécurité SRTP :
- dans le fichier **nano /etc/asterisk/pjsip.conf** on va ajouter deux choses :



```
GNU nano 7.2 /etc/asterisk/pjsip.conf
[transport-udp]
type=transport
protocol=udp
bind=0.0.0.0

;-----
; Extension 1000
;-----
[1000]
type=endpoint
context=internal
disallow=all
allow=ulaw
auth=auth1000
aors=1000
media_encryption=sdes
media_encryption_optimistic=no

[auth1000]
type=auth

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

Figure III.34 : Configuration du chiffrement des médias (SRTP) dans le fichier pjsip.conf du serveur Asterisk.

media_encryption=sdes : permet d'activer le chiffrement du flux RTP utilisant SRTP.

media_encryption_optimistic=no : impose l'utilisation obligatoire du chiffrement, garantissant ainsi que toutes les communications soient sécurisées.

8.1.2. Configuration du client MicroSIP et l'application MizuDroid : Pour configurer le client MicroSIP et l'application MizuDroid, il faut accéder aux paramètres du compte MicroSIP et ouvrir la fenêtre dédiée au chiffrement :

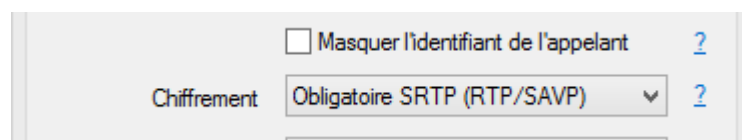


Figure III.35 : Activation du protocole SRTP dans les paramètres de MicroSIP.

➤ Cela garantit que la communication est chiffrée côté client.

De même, dans les paramètres de MizuDroid, il faut se rendre dans les paramètres (Settings), utiliser la barre de recherche pour trouver la fenêtre Media Encryption, pour sélectionner le protocole SRTP :

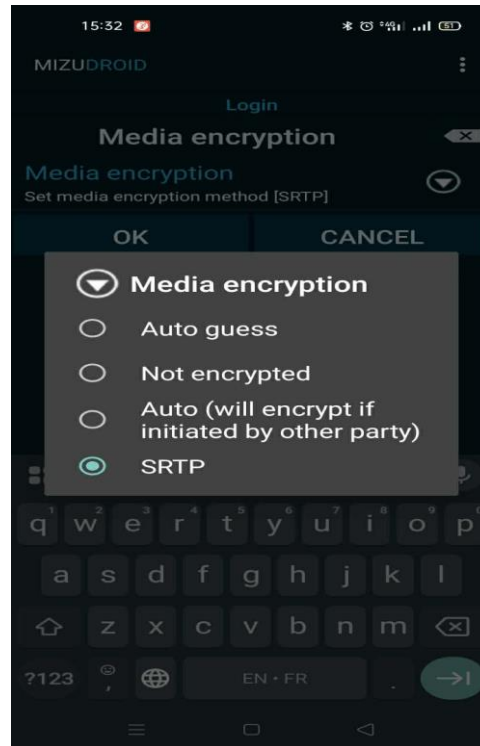


Figure III.36 : Activation du protocole SRTP dans les paramètres de MizuDroid.

8.1.3. Rechargement de la configuration : pour accéder à la console d'Asterisk, nous utilisons la commande suivante :

```
root@debian:/home/younes# sudo asterisk -cvvv
```

Figure III.37 : Ouverture de la console Asterisk.

Ensuite, pour recharger la configuration sans redémarrer le service, on exécute :

```
Asterisk Ready.  
*CLI> pjsip reload
```

Figure III.38 : Rechargement de la configuration PJSIP.

➤ Cette étape permet de prendre en compte les nouvelles modifications, notamment l'activation du chiffrement SRTP.

Après nous devons vérifier si les deux comptes sont disponibles en tapant sur ***CLI> pjsip show endpoints** :

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

```
=====
Endpoint: 1000                                     Not in use      0 of inf
  InAuth: auth1000/1000
    Aor: 1000                                         1
  Contact: 1000/sip:1000@192.168.43.148:50536;ob     0a8b3f7d22 NonQual      nan

Endpoint: 2000                                     Not in use      0 of inf
  InAuth: auth2000/2000
    Aor: 2000                                         1
  Contact: 2000/sip:2000@192.168.43.1:10210         641ea65366 NonQual      nan

Objects found: 2

*CLI> █
```

Figure III.39 : Vérification la disponibilité pour les deux comptes.

➤ Donc les deux utilisateurs sont disponibles.

8.1.4. Test après sécurisation : Après l'activation du mécanisme de sécurité SRTP sur le serveur Asterisk ainsi que les clients SIP, un test de communication a été réalisé entre les extensions 1000 et 2000.

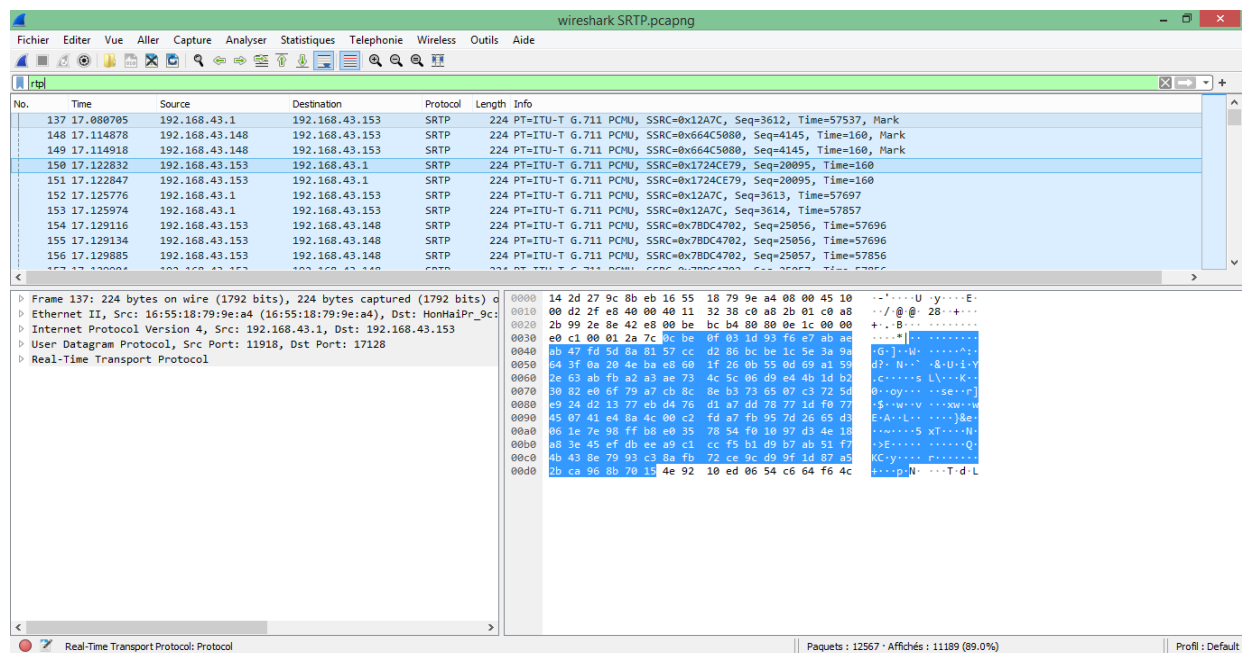


Figure III.40 : capture wireshark montrant des paquets RTP chiffrés(SRTP) Rendant le contenu audio illisible.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

Analyse de la figure : à partir de la figure nous observons que :

- Les données binaires apparaissent sous forme de valeurs hexadécimales, ce qui confirme que les données sont protégées et non interprétables.
- Le contenu des paquets est illisible et incompréhensible.

Refaire l'écoute et l'analyse des flux RTP afin d'observer le comportement du trafic audio.

Nous remarquons que la forme d'audio est déformée, en plus lorsque nous cliquons sur le bouton Démarrer nous écoutons juste de bruit.

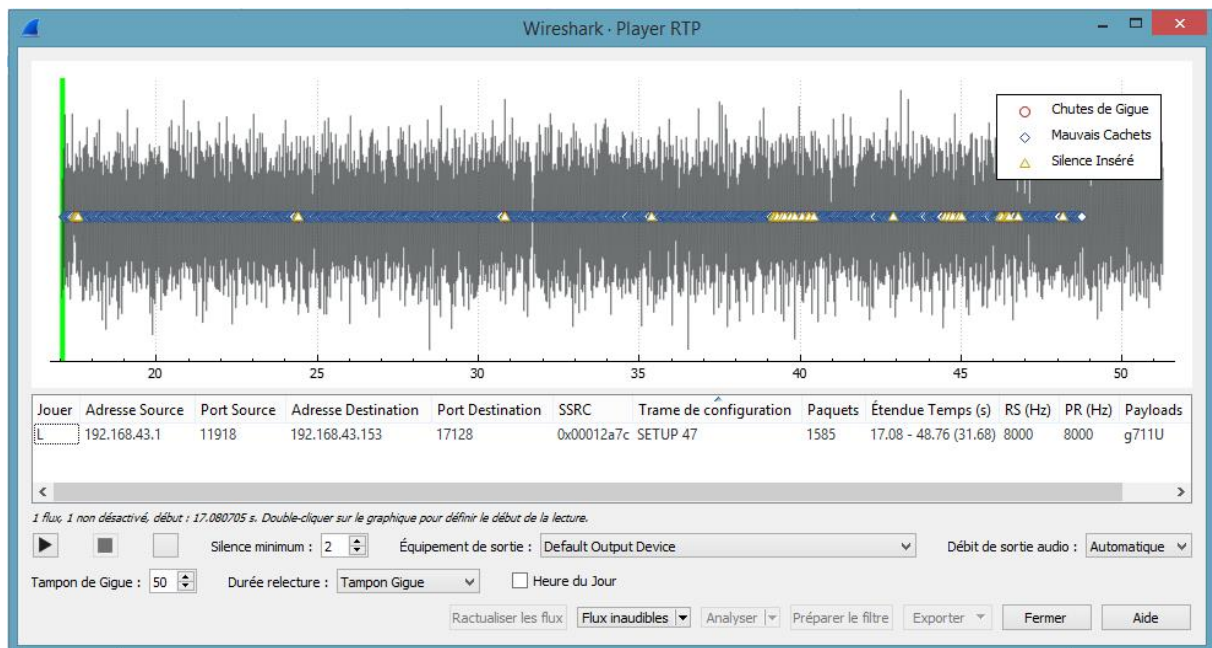


Figure III.41 : Appel sécurisé et écoute parasitée.

9. Architecture de liaison entre RTC et voix IP

L'interconnexion entre le Réseau Téléphonique Commuté (RTC) et la Voix sur IP (VoIP) permet aux utilisateurs des deux réseaux de communiquer entre eux malgré des technologies différentes (analogique vers numérique/IP).



Figure III.42 : Architecture d'interconnexion entre le réseau RTC et le réseau VoIP basée sur un serveur Asterisk (SIP).

9.1.Éléments de l'architecture :

L'architecture étudiée repose sur l'intégration d'un routeur Cisco CME et d'un serveur Asterisk, permettant la convergence entre la téléphonie RTC et la téléphonie IP.

Le schéma de fonctionnement est le suivant :

- ✚ RTC (ligne téléphonique)
- ✚ Interface FXO / PRI
- ✚ Routeur Cisco CME
- ✚ Serveur Asterisk
- ✚ Téléphones IP / Extensions SIP

9.1.1. Réseau RTC

Le réseau RTC représente l'infrastructure téléphonique traditionnelle basée sur des commutateurs et des lignes physiques.

Il utilise des protocoles de signalisation tels que SS7 pour établir et gérer les communications.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

Malgré l'évolution vers la VoIP, le RTC reste utilisé dans plusieurs environnements et nécessite une interconnexion via des passerelles VoIP.

9.1.2. Passerelle VoIP (Gateway) -Interface FXO

La passerelle VoIP constitue un élément essentiel dans une architecture de communication hybride. Elle assure l'interconnexion entre le réseau téléphonique traditionnel (RTC) et le réseau IP.

Elle permet principalement:

- La conversion du signal analogique ou numérique provenant du RTC en paquets IP.
- La conversion inverse des paquets IP en signal téléphonique.
- La gestion des codecs audio tels que G.711 et G.729, permettant l'adaptation de la qualité et de la bande passante.

Ainsi, la passerelle joue un rôle d'interface entre les infrastructures classiques et les systèmes de téléphonie

9.1.3. Routeur Cisco CME

Le routeur Cisco CME est configuré afin d'assurer l'interconnexion avec le serveur Asterisk via un trunk SIP.

Configuration d'un dial-peer VoIP

Un dial-peer est défini pour diriger les appels vers le serveur Asterisk :

- Le protocole SIP est utilisé pour la signalisation.
- Le codec G.711 est configuré pour assurer une qualité audio optimale.
- L'adresse IP du serveur Asterisk est spécifiée comme destination.

➤ Créer un dial-peer SIP vers Asterisk

```
dial-peer voice 100 voip
```

```
destination-pattern .
```

```
session protocol sipv2
```

```
session target ipv4:10.200.0.67
```

```
codec g711ulaw
```

```
no vad
```

10.200.0.67 = IP du serveur Asterisk.

Configuration de la ligne RTC (FXO)

La configuration de l'interface FXO permet de rediriger automatiquement les appels entrants vers une extension interne définie.

Cette redirection peut être réalisée soit via la commande PLAR, soit via un dial-peer de type POTS

➤ Configurer la ligne RTC (FXO)

voice-port 0/0/2

connection plar opx 3000

Cela envoie automatiquement l'appel vers l'extension 3000(nous avons créé une extension 3000 même que 1000 et 2000).

✚ Configuration du serveur Asterisk

Le serveur Asterisk est configuré pour recevoir et gérer les appels provenant du routeur Cisco CME.

➤ Fichier pjsip.conf

Un endpoint est défini pour le routeur Cisco, incluant :

- L'adresse IP du routeur
- Le contexte de traitement des appels
- Les paramètres d'authentification et de communication SIP

➤ Fichier extensions.conf

Le dialplan permet de définir le traitement des appels entrants.

Lorsqu'un appel est reçu sur une extension donnée (exemple 3000), Asterisk :

- Répond à l'appel
- Le redirige vers l'extension SIP correspondante
- Termine la communication une fois l'appel fini

Configuration sur Asterisk

✚ Dans pjsip.conf :

```
[cisco]
type=endpoint
context=from-cisco
disallow=all
allow=ulaw
transport=transport-udp
aors=cisco
[cisco]
type=aor
contact=sip:10.200.0.100
[cisco-identify]
type=identify
endpoint=cisco
match=10.200.0.100
```

Figure III.43 : Définition de l'endpoint SIP du routeur Cisco dans pjsip.conf.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

✚ Dans `extensions.conf` :

Cela envoie l'appel vers l'extension 3000.

```
[from-cisco]
exten => 3000,1,Answer()
same => n,Dial(PJSIP/3000)
same => n,Hangup()
```

Figure III.44 : Enregistrement de l'extension SIP 3000 sur le serveur Asterisk.

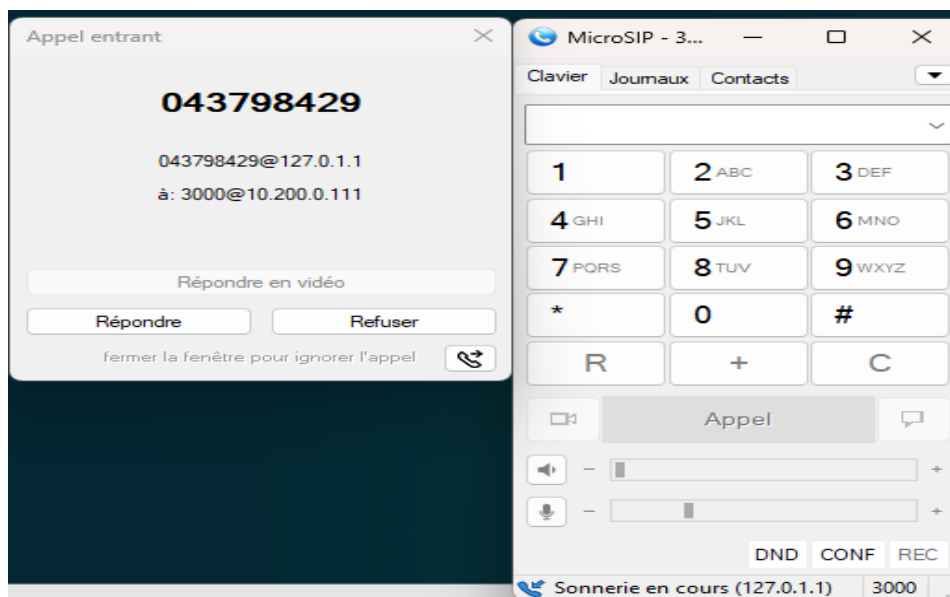


Figure III.45 : Réception d'un appel RTC sur l'extension SIP 3000.

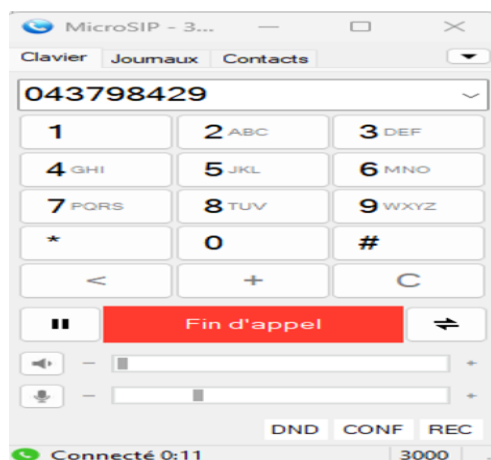


Figure III.46 : Test de communication entre le réseau RTC et le réseau VoIP.

CHAPITRE III : Mise en œuvre d'une solution VoIP basée sur Asterisk : configuration, sécurisation et interconnexion RTC.

152.830197	152.843478	10.200.0.100	<sip:043798429@10.200.0.100>	<sip:3000@10.200.0.67>	SIP	00:00:00	6	IN CALL	INVITE 200 200
152.868662	152.872905	10.200.0.67	<sip:043798429@127.0.1.1>	<sip:3000@10.200.0.111;ob>	SIP	00:00:00	6	CALL SETUP	INVITE
182.127647	182.130429	10.200.0.111	<sip:3000@10.200.0.67>	<sip:3000@10.200.0.67>	SIP	00:00:00	8	REJECTED	REGISTER 401 401

Figure III.47 : Capture Wireshark montrant l'établissement d'une communication entre le RTC et le réseau VoIP.

10. Conclusion

Dans ce chapitre, nous avons présenté une solution pour sécuriser notre serveur SIP pour la VoIP. Nous avons mis en évidence l'importance de la sécurité dans les architectures de téléphonie IP, ainsi que le rôle essentiel des mécanismes de chiffrement dans la protection des données vocales. Par ailleurs, nous avons exposé une architecture permet d'intégrer efficacement la téléphonie traditionnelle RTC avec une infrastructure VoIP basée sur Asterisk. L'utilisation d'un routeur Cisco CME comme passerelle SIP facilite l'interconnexion entre les deux environnements, assurant ainsi une communication fluide, flexible et évolutive.

Conclusion Générale

À la fin de ce travail, nous avons pu découvrir et approfondir nos connaissances dans le domaine de la voix et de la vidéo sur IP ainsi que dans les différentes technologies utilisées dans les systèmes de téléphonie IP. Cette étude nous a permis de mieux comprendre le fonctionnement de la VoIP, ses avantages et son importance croissante dans les réseaux de communication modernes.

Dans le premier chapitre, nous avons présenté les généralités et les concepts fondamentaux de la voix et de la vidéo sur IP. Nous avons étudié leur principe de fonctionnement, les différentes étapes du transport de la voix sur les réseaux IP ainsi que les avantages qu'elles offrent par rapport aux systèmes de téléphonie traditionnels.

Dans le deuxième chapitre, nous nous sommes intéressés aux principaux protocoles utilisés dans les systèmes VoIP. Nous avons analysé leur rôle dans l'établissement, la gestion et la terminaison des communications, ce qui nous a permis de mieux comprendre l'architecture et le fonctionnement global des réseaux de téléphonie sur IP.

Dans le troisième chapitre, nous avons réalisé la mise en œuvre pratique d'une solution VoIP basée sur Asterisk. Cette partie nous a permis d'installer et de configurer l'environnement de travail, de créer et gérer les différents comptes utilisateurs, d'assurer la communication entre les clients et de mettre en place les mécanismes nécessaires à la sécurisation des appels. Nous avons également étudié l'interconnexion entre le réseau téléphonique commuté (RTC) et le réseau VoIP afin de garantir une communication efficace entre les deux environnements.

Les différents tests effectués nous ont permis de vérifier le bon fonctionnement de la solution mise en place et de confirmer la fiabilité des configurations réalisées. Les résultats obtenus ont montré que la plateforme Asterisk constitue une solution performante, flexible et économique pour le déploiement de services de téléphonie IP.

La réalisation de ce mémoire nous a également permis de mettre en pratique les connaissances théoriques acquises durant notre formation de Master. Nous avons développé des compétences dans les domaines de l'administration des réseaux, de la configuration des systèmes VoIP, de la sécurité des communications et de la résolution des problèmes techniques rencontrés lors de la mise en œuvre.

Par ailleurs, ce travail nous a permis de découvrir l'importance des solutions open source dans le domaine des télécommunications, notamment grâce à leur flexibilité, leur faible coût et leur capacité à répondre aux besoins des entreprises et des organisations modernes.

Conclusion Générale

Enfin, ce projet représente une expérience très enrichissante sur les plans académique et professionnel. Il nous a permis d'acquérir une vision plus approfondie des technologies de communication IP et constitue une base solide pour de futurs travaux de recherche ou projets professionnels dans le domaine des réseaux et des télécommunications. Comme perspective, il serait intéressant d'enrichir cette plateforme par l'intégration de services avancés tels que la visioconférence, la messagerie unifiée, les mécanismes avancés de qualité de service (QoS) ou encore des solutions de haute disponibilité afin d'améliorer davantage les performances et la continuité des services.

RÉFÉRENCES BIBLIOGRAPHIQUES

- [1] ALDEVAR. *Tout sur la VoIP*. Disponible sur : http://aldevar.free.fr/data/14-Telephonie/Tout_sur_la_voip.pdf (Consulté le 12/02/2026)
- [2] International Telecommunication Union (ITU). *IP Telephony*. Geneva : ITU, 2004. Disponible sur : https://www.itu.int/dms_pub/itu-d/opb/hdb/D-HDB-IPT-2004-R1-PDF-F.pdf (Consulté le 13/02/2026)
- [3] MEBARKI, Nour El Houda. Étude et simulation d'une transmission de la voix sur IP (VoIP). Mémoire de Master, Université Badji Mokhtar – Annaba, Faculté des Sciences de l'Ingénierat, Département d'Électronique, 2019. Disponible sur : <https://biblio.univ-annaba.dz/wp-content/uploads/2020/02/These-Mebarki-Nour-El-Houda.pdf> (Consulté le 02/03/2026)
- [4] HAMADOUCHE, Mohammed Walid. *Développement d'une application Android VoIP client*. Mémoire de Master en Télécommunications, Spécialité Réseaux et Télécommunications, Faculté de Technologie, Université Abou Bekr Belkaïd – Tlemcen, 2021. Disponible sur : <https://dspace.univ-tlemcen.dz/server/api/core/bitstreams/af584385-1251-4caa-9df2-953e4987b6f9/content> (Consulté le 12/04/2026)
- [5] CHERCHARI, Chaïma. Électronique et Télécommunications – Réseaux et Télécommunications. Université 8 Mai 1945 de Guelma. Disponible sur : https://dspace.univ-guelma.dz/jspui/bitstream/123456789/11531/1/CHERCHARI_CHAÏMA_F1_Electronique%20et%20T%C3%A9l%C3%A9communications_R%C3%A9seaux%20et%20T%C3%A9l%C3%A9communications.pdf (Consulté le 02/05/2026).
- [6] WikiMemoires. H.323: protocole, gateway ET gatekeeper. Disponible sur : <https://wikimemoires.com/2011/03/h323-protocole-protocole-gateway-gatekeeper-h-323/> (Consulté le 13/02/2026).
- [7] AMI Gestion. Le protocole H.323. Disponible sur : <https://ami-gestion.fr/h-323/> (Consulté le 13/05/2026).
- [8] HAMADOUCHE, Mohammed Walid. *Développement d'une application Android VoIP client*. Mémoire de Master en Télécommunications, Spécialité Réseaux et Télécommunications, Faculté de Technologie, Université Abou Bekr Belkaïd – Tlemcen, 2021. Disponible sur : <https://dspace.univ-tlemcen.dz/server/api/core/bitstreams/7155f084-da55-45b1-abb7-66e76abcf542/content> (Consulté le 11/06/2026)
- [9] Université Mouloud Mammeri de Tizi Ouzou. Mémoire de fin d'études. Disponible sur : <https://dspace.ummto.dz/server/api/core/bitstreams/98eb7f45-4a44-4549-9327-8faa3da538f2/content> (Consulté le 20/06/2026).

Références Bibliographiques

[10] MCours. Cours sur la VoIP. Disponible sur :

<https://www.mcourses.net/cours/pdf/hasclie1/hasclie218.pdf> (Consulté le 21/06/2026).

[11] IBM. Qu'est-ce que Linux ? Disponible sur : <https://www.ibm.com/fr-fr/think/topics/linux>

(Consulté le 22/06/2026).

[12] Oracle. Qu'est-ce qu'une machine virtuelle (VM) ? Disponible sur :

<https://www.oracle.com/fr/cloud/definition-machine-virtuelle-vm/> (Consulté le 22/06/2026).