

INSTITUT SUPERIEUR TECHNIQUE ADVENTISTE DE GOMA



ARRETE MINISTERIEL N°C54/MINESU/CAB.MN/SMM/KGN/JMB/2019DU 14/2/2019

E-mail: uago2015@gmail.com

Site Web: uagom.com

BP : 109 GOMA

DOMAINE DE GESTION INFORMATIQUE

ETUDE ET MISE EN PLACE D'UNE SOLUTION VOIP SECURISEE CAS DE L'UAGO

Par : BARAKA NDAYAMBAJE Bienfait

Mémoire présenté et défendu en vue de l'obtention
du diplôme de licence en informatique.

Directeur : CT BYAMUNGU SHINDANO

SEPTEMBRE 2023



DECLARATION DE L'ETUDIANT

Nous soussignons **BARAKA NDAYAMBAJE Bienfait**, déclare solennellement et en toute honnêteté que, ce mémoire de licence que nous présentons et défendu publiquement ce jour est issu de nos propres efforts en collaboration avec de célèbres personnalités tant morale, physique, que scientifique de haute portée. Ce travail n'a donc jamais fait l'objet d'aucune autre présentation ni défense sous forme dans laquelle nous le présentons aujourd'hui.

Fait à GOMA le 22/09/2023

BARAKA NDAYAMBAJE Bienfait



DECLARATION DU DIRECTEUR

*Je soussigné, CT **BYAMUNGU SHINDANO** certifié d'avoir dirigé le travail de l'étudiant **BARAKA NDAYAMBAJE Bienfait** intitulé : **Etude et mise en place d'une solution VOIP sécurisée : cas de l'UAGO.***

Fait à Goma le 22/09/2023

CT BYAMUNGU SHINDANO



EPIGRAPHE

« Informatique : Algorithmes, bases de données, réseaux ».

Gilles Dowek

IN MEMORIUM

« Nous garderons en mémoire les moments partagés avec UKIZE NKABURA, une personne aimante et généreuse qui a laissé une empreinte indélébile dans nos vies. ».



DEDICACE

*À nos chers parents **NDAYAMBAJE** et **MUKABERA** pour leur soutien inconditionnel et leur amour constant.*

BARAKA NDAYAMBAJE Bienfait

REMERCIEMENTS

De Prime à bord, à exprimer ma profonde gratitude envers Dieu. Pour Sa présence et Son soutien constants tout au long de mon parcours académique.

*Nos sincères remerciements s'adressent aux autorités administratives de **l'UAGO/ISTAGO**, A nos autorités pour la formation de qualité.*

*Nous remercions le **CT SHINDANO BYAMUNGU** qui, en dépit de ses multiples occupations, a bien voulu assurer la direction de ce travail ; ses remarques et ses sages conseils nous ont été d'un grand secours. A travers lui, nous reconnaissons l'effort combien louable de tout le corps académique et scientifique de **l'UAGO/ISTAGO** qui a accepté d'assurer notre formation.*

*Nos reconnaissances s'adressent également à la famille **Daniel UKIZE** pour son soutien et ses conseils plein de sagesse. Malgré les difficultés et les peines rencontrées.*

Je tiens à adresser des remerciements spéciaux à mes frères et sœurs, qui ont joué un rôle essentiel dans mon parcours académique et personnel.

En fin à tous ceux qui, de près ou de loin ont témoigné leur soutien, mais dont les noms ne sont pas repris sur cette page, trouvent ici l'expression de notre profonde gratitude.

SIGLES ET ABBREVIATIONS

Φ *IDS : Intrusion Détection System ;*

Φ *IP = internet Protocol ;*

Φ *IPS : Intrusion Prévention System ;*

Φ *ISTAGO : Institut Supérieur Universitaire Adventiste de Goma*

Φ *Sip : Session Initiation Protocol ;*

Φ *UAGO : Université Adventiste de Goma*

Φ *VoIP = Voicer overy internet ;*

Φ *VoIP : Voice over Internet Protocol ;*

LISTES DE TABLEAUX

Tableau 1 Identification de tache	28
Tableau 2 Estimation du cout du projet.....	29
Tableau 3 Estimation du cout matériels	29

LISTES DES FIGURES

Figure 1 ELABORATION DU GRAPHET PERT	29
Figure 2 Date au plus tôt et date au plus tard	30
Figure 3 Calculs de marge.....	31
Figure 4 DETERMINATION DU CHEMIN CRITIQUE	33
Figure 5 CALENDRIER DU PROJET	33
Figure 6 CALENDRIER DU PROJET	Erreur ! Signet non défini.
Figure 7 ARCHITECTURE	9
Figure 8 SIP SERVER	11
Figure 9 UN PROXY SIP	11
Figure 10 FORMAT DU PAQUET SRTP.....	14
Figure 11 Architecture du réseau VoIP déployé	37



RESUMÉ

Ce mémoire traite la mise en place d'une solution de voix sur IP dans une Infrastructure de trois couches via la solution VoIP open source « Asterisk » au sein de l'entreprise « UAGO ». Nous parlerons en premier lieu les notions de base essentielles pour la compréhension du déroulement de cette technologie ainsi que sa sécurisation.

Nous mettrons ensuite notre solution dans un environnement de test avec le serveur Asterisk, deux clients LINPHONE. Nous avons installé par la suite des logiciels d'attaque : pour l'écoute du trafic via la voix IP et réaliser une série d'attaque visant les vulnérabilités d'une communication via la voix sur IP, suite à ses attaques, Nous venons de proposer les mesures de sécurité à implémenter dans l'infrastructure existante.

ABSTRACT

This thesis deals with the implementation of a voice over IP solution in a Three-layer infrastructure via the open source VoIP solution “Asterisk” within the company “UAGO”. We will first talk about the basic concepts essential for understanding how this technology works as well as its security.

We will then put our solution in a test environment with the Asterisk server, two LINPHONE clients. We subsequently installed attack software: for listening to traffic via voice over IP and carrying out a series of attacks targeting the vulnerabilities of communication via voice over IP, following these attacks, we have just propose security measures to be implemented in the existing infrastructure.

CHAP.I INTRODUCTION

I.1. CONTEXTE DE L'ÉTUDE

Dans l'environnement informatique, la VoIP a été l'une des révolutions majeures de ces dernières années, permettant de faire transiter via des réseaux routés IP, la voix est ainsi pour permettre la communication entre personnes via un média universel, Internet. L'enjeu principal également de la VoIP, quand elle est intégrée dans une entreprise, est la rentabilité. Les entreprises peuvent ainsi économiser un budget très important grâce à ce support. Il ne faut pas néanmoins perdre de vue la fiabilité et la scalabilité que doivent offrir ces infrastructures pour éviter les régressions par rapport aux réseaux analogiques traditionnels. Cette étude aborde la VoIP d'un point de vue général avant d'entamer la configuration basique et avancée de linphone. Il est établi dans celui-ci des Scénarios simples et complets ainsi que l'implémentation de la sécurité dans une telle infrastructure.

La voix sur IP (VoIP) constitue un tournant dans le monde de la communication. En effet, la convergence du « triple Play » (voix, données et vidéo) fait partie des enjeux principaux des acteurs de la télécommunication aujourd'hui. Plus récemment l'Internet s'est étendu partiellement dans l'Intranet de chaque organisation, voyant le trafic total basé sur un transport réseau de paquets IP surpasse le trafic traditionnel du réseau voix (réseau à commutation de circuits). Il devenait clair que dans le sillage de cette avancée technologique, les opérateurs, entreprises ou organisations et fournisseurs devraient bénéficier de l'avantage du transport unique IP, introduire de nouveaux services voix et vidéos. Ainsi, l'une des solutions qui marquent le « boom » de la voix sur IP au sein des entreprises est la solution PABX IP (PrivateAutomaticBrancheXchange IP) qui est l'équivalent des PBX traditionnels pour un réseau IP.

Ce vaste marché, longtemps dominé par des solutions propriétaires proposées par des entreprises renommées (Cisco, 3Com, EADS, etc.) voit aujourd'hui, avec la maturité des technologies « Open Source », l'émergence de la la technologie IP (Internet Protocol) est un protocole de communication qui permet de transférer des données numériques à travers des réseaux informatiques. Il s'agit d'un protocole de couche réseau qui permet de transmettre des paquets de données entre différents appareils connectés à un réseau IP.

Dans le contexte de l'étude sur la solution VoIP sécurisée, l'IP est utilisée pour transporter les informations audio et vidéo des appels téléphoniques sur le réseau informatique. La VoIP utilise l'IP pour convertir les signaux analogiques en données numériques et les transmettre sur le réseau, ce qui permet de réduire les coûts de communication et d'offrir des

fonctionnalités avancées telles que la vidéoconférence et la messagerie vocale. Le contexte de l'étude porte sur la sécurité de la solution VoIP utilisant l'IP, en particulier sur les risques de sécurité associés à la VoIP et les solutions pour les atténuer. Les sujets de recherche incluent l'analyse des risques de sécurité, l'évaluation des solutions de sécurité existantes, et la proposition d'améliorations pour la sécurité de la solution VoIP.

La VoIP est une technologie qui permet de faire des appels téléphoniques et de la communication en temps réel en utilisant Internet comme support de transport, plutôt que les réseaux traditionnels de téléphonie. Cependant, comme les appels VoIP sont transmis sur Internet, ils peuvent être vulnérables aux attaques de sécurité telles que l'interception, la falsification ou le vol de données. Le contexte de l'étude consiste donc à explorer les risques de sécurité associés à la VoIP, à analyser les solutions de sécurité existantes et à proposer des améliorations pour une solution VoIP sécurisée.

I.2. PROBLÉMATIQUE

Pour garantir la sécurité des communications VoIP sur Internet, il est important de prendre en compte les risques de sécurité associés à cette technologie. Les risques de sécurité les plus courants pour la VoIP comprennent :

1. L'interception des appels : les attaquants peuvent intercepter les appels VoIP pour écouter les conversations ou voler des informations sensibles telles que les mots de passe.
2. La falsification de l'identité : les attaquants peuvent falsifier l'identité de l'appelant pour tromper la personne qui reçoit l'appel.
3. Les attaques par déni de service (DoS) : les attaquants peuvent envoyer un grand nombre de requêtes de connexion pour surcharger le système et empêcher les utilisateurs légitimes d'utiliser le service.

Pour garantir la sécurité des communications VoIP, il est donc important de mettre en place des mesures de sécurité appropriées. Pour y arriver nous nous sommes posé les questions suivantes :

- ❖ **Quelle étude devons-nous proposer au sein de l'UAGO enfin d'éviter les erreurs constatées dans la gestion des communications VoIP ?**
- ❖ **Quelle solution palliative pouvons-nous proposer dans les attaques par déni de service au sein de l'UAGO ?**

Pour améliorer la sécurité de la solution VoIP, il est recommandé de mettre en place une combinaison de ces solutions de sécurité. Il est également important de mettre à jour régulièrement les logiciels et les systèmes pour s'assurer qu'ils sont protégés contre les dernières menaces de sécurité.

I.3. OBJECTIF DU TRAVAIL

I.3.1. OBJECTIF GENERAL

L'objectif général de cette étude vise à proposer des améliorations et des recommandations pour une solution de VoIP sécurisée qui garantit la sécurité des communications sur Internet tout en prenant en compte les risques de sécurité associés. En résumé, l'objectif de cette recherche est de trouver une solution pratique et efficace pour garantir la sécurité des communications VoIP sur Internet.

I.3.2. OBJECTIFS SPÉCIFIQUES

Nous avons les objectifs suivants :

1. Identifier les risques de sécurité associés à la VoIP et de comprendre comment ces risques peuvent affecter les communications VoIP sur Internet.
2. Proposer des améliorations et des recommandations pour une solution de VoIP sécurisée qui garantit la sécurité des communications sur Internet tout en prenant en compte les risques de sécurité associés.

I.4. MÉTHODES ET TECHNIQUES

La méthode est un ensemble des opérations intellectuelles permettant par lesquelles une discipline cherche à atteindre les vérités qu'elle poursuit, les démontre et le vérifie. (Bayle).

A, La méthode est un ensemble des opérations intellectuelles permettant par lesquelles une discipline cherche à atteindre les vérités qu'elle poursuit, les démontre et le vérifie. (Bayle)

Mme COHENDET² définit la méthode comme un instrument devant permettre à l'esprit de s'épanouir ; l'expression de s'éclaircir. L'utilisation d'une bonne méthode a pour objectif de mettre en valeur la qualité de la réflexion.³

Aussi comme le dit GRAWITZ, la méthode est l'ensemble des opérations intellectuelles par lesquelles une discipline cherche à atteindre les vérités qu'elle poursuit, les démontrés et les vérifiés.⁴

Pour mener à bien notre étude, nous avons choisi d'utiliser la méthode :

PERT qui nous a aidés à analyser les stratégies utilisées par le réseau de l'institut supérieur Technique adventiste de Goma.

I.5. CHOIX ET INTERET DU SUJET

Le choix de ce sujet est très pertinent et intéressant étant donné que la VoIP est devenue une technologie de communication très populaire et largement utilisée dans le monde des affaires et dans les foyers. Cependant, la sécurité de la VoIP est une question importante qui doit être prise en compte car elle est vulnérable aux attaques de sécurité telles que l'interception, la falsification et le vol de données. Par conséquent, l'étude de la sécurité de la VoIP est cruciale pour garantir la confidentialité, l'intégrité et la disponibilité des communications VoIP sur Internet.

Enfin, ce sujet est également pertinent en raison de la popularité croissante du travail à distance et de la communication à distance, en particulier en réponse aux préoccupations de l'entreprise. Les entreprises et les individus utilisent de plus en plus la VoIP pour les appels professionnels et personnels, ce qui augmente l'importance de la sécurité de la VoIP pour protéger les informations confidentielles et les données personnelles.

I.6. DELIMITATION DU TRAVAIL

Pour réaliser un travail d'une manière efficace on doit se limiter dans le temps et dans l'espace ainsi dans le temps notre travail va se réaliser dans l'année académique 2022-2023, Dans l'espace vu que la matière de réseau informatique est plus complexe nous avons pensé mettre en place une solution VOIP sécurisée. Spécifiquement à l'Université Adventiste de Goma, Se trouvant dans la Commune de Karisimbi.

I.7. SUBDIVISION DU TRAVAIL

Vu la grandeur du sujet que nous avons abordé notre travail sera subdivisé en quatre chapitres.

- Ø Chapitre 1 : Introduction ;**
- Ø Chapitre 2 : Revue de la littérature ;**
- Ø Chapitre 3 : Planning provisionnel du projet ;**
- Ø Chapitre 4 : Présentation des résultats ;**

CHAP II. REVUE DE LA LITTERATURE

II.1 INTRODUCTION

Dans ce chapitre nous allons présenter les différents travaux qui nous ont inspiré pour pouvoir choisir ce sujet en suite nous allons parler de quelques concepts en rapport avec le sujet enfin la présentation du milieu d'étude.

II.2 REVUE DE LA LITTERATURE EMPIRIQUE

En toute recherche scientifique même dite originale, une personne ne part pas zéro au de rien ; il y a toujours un point de départ que constituent les connaissances. Ainsi au cours de notre recherche nous avons constaté que plusieurs études ont été menées pour évaluer l'efficacité des solutions de sécurité pour la VoIP.

- 1) une étude menée par **Zhu et al. (2016)** a évalué l'efficacité de diverses solutions de sécurité de la VoIP en termes de protection contre les attaques par déni de service (Dos). Les résultats ont montré que les solutions de détection et de prévention des intrusions ont été les plus efficaces pour protéger les systèmes VoIP contre les attaques Dos. (al, 2016).
- 2) Une autre étude menée **par Bera et al. (2018)** a évalué l'efficacité des protocoles de cryptage pour protéger les flux de voix contre l'écoute clandestine. Les résultats ont montré que les protocoles de cryptage, tels que SRTP (Secure Real-time Transport Protocol) et ZRTP (Zimmermann Real-time Transport Protocol), étaient efficaces pour protéger les flux de voix contre l'écoute clandestine. (Bera, 2018).
- 3) Une troisième étude menée par **Al-Fayoumi et al. (2020)** a évalué les pratiques de sécurité pour la VoIP dans les entreprises. Les résultats ont montré que la plupart des entreprises utilisaient des solutions de sécurité pour protéger leurs systèmes VoIP, mais que certaines pratiques de sécurité, telles que la configuration des équipements et la gestion des identités et des accès, n'étaient pas suffisamment mises en place. (Fayoumi, 2020)
- 4) Enfin, une autre étude menée par **Khan et al. (2019)** a évalué l'impact de la sensibilisation des utilisateurs sur la sécurité de la VoIP. Les résultats ont montré que la sensibilisation des utilisateurs à la sécurité de la VoIP était un facteur important pour réduire les risques liés aux attaques de phishing et d'ingénierie sociale. (al K. e., 2019).

Notre travail est différent des chercheurs précédemment cités avec l'appréhension des solutions de sécurité pour la VoIP qui sont efficaces pour protéger les flux de voix et les systèmes contre les menaces, mais que leur efficacité dépend de la mise en place correcte des pratiques de sécurité et de la sensibilisation des utilisateurs.

II.3. REVUE DE LA LITTÉRATURE THEORIQUES (Johson, 2019)

Voici quelques définitions de concepts clés associés à la VoIP sécurisée :

- Φ **VoIP : La VoIP** (Voice over Internet Protocol) est une technologie qui permet de faire transiter des flux de voix sur un réseau IP, comme Internet, plutôt que sur un réseau téléphonique traditionnel.
- Φ **Cryptage** : Le cryptage est le processus de conversion des données en un code secret afin de protéger leur confidentialité. Dans le cas de la VoIP, le cryptage est utilisé pour protéger les flux de voix contre l'interception et l'écoute clandestine.
- Φ **Authentification** : L'authentification est le processus de vérification de l'identité d'un utilisateur ou d'un périphérique. Dans le cas de la VoIP, l'authentification est utilisée pour s'assurer que les appels proviennent de sources autorisées et empêcher les attaquants de se faire passer pour des utilisateurs autorisés.
- Φ **Détection et prévention des intrusions** : La détection et la prévention des intrusions sont des mécanismes de sécurité qui permettent de détecter les tentatives d'intrusion et de les bloquer avant qu'elles ne causent des dommages. Dans le cas de la VoIP, les solutions de détection et de prévention des intrusions sont utilisées pour protéger les systèmes VoIP contre les attaques.
- Φ **Pare-feu** : Un pare-feu est un dispositif de sécurité qui permet de filtrer le trafic réseau entrant et sortant pour protéger les systèmes contre les attaques. Dans le cas de la VoIP, les pare-feu sont utilisés pour détecter et bloquer les tentatives d'intrusion.
- Φ **IDS (Intrusion Détection System)** : Un IDS est un système de détection des intrusions qui permet de détecter les tentatives d'intrusion en surveillant le trafic réseau. Dans le cas de la VoIP, les IDS sont utilisés pour détecter les tentatives d'intrusion sur les systèmes VoIP.
- Φ **IPS (Intrusion Prévention System)** : Un IPS est un système de prévention des intrusions qui permet de bloquer les tentatives d'intrusion en temps réel. Dans le cas de la VoIP, les IPS sont utilisés pour bloquer les tentatives d'intrusion sur les systèmes VoIP avant qu'elles ne causent des dommages.
- Φ **Gestion des identités et des accès** : La gestion des identités et des accès est le processus de gestion des identités et des droits d'accès des utilisateurs aux ressources informatiques. Dans le cas de la VoIP, la gestion des identités et des accès est utilisée pour s'assurer que seules les personnes autorisées ont accès aux systèmes VoIP.

II.4 Revue de la littérature conceptuelle

II.4.1. La voip

La VoIP, ou Voice over Internet Protocol, est une méthode qui permet de transmettre des appels vocaux en utilisant Internet plutôt que les lignes téléphoniques traditionnelles. Cela signifie que vous pouvez passer des appels téléphoniques en utilisant votre connexion Internet existante, ce qui peut être très pratique et économique.

II.4.2 Fonctionnement et Rôles

II.4.2.1. Fonctionnement

La VoIP offre de nombreux avantages par rapport aux systèmes téléphoniques traditionnels. Elle est généralement moins chère, car elle utilise le réseau Internet existant plutôt que des lignes téléphoniques dédiées. De plus, la VoIP permet une plus grande flexibilité, car vous pouvez passer des appels depuis n'importe quel appareil connecté à Internet, que ce soit un ordinateur, un téléphone portable ou une tablette.

En outre, la VoIP offre également des fonctionnalités avancées telles que la messagerie vocale, la gestion des appels, la conférence téléphonique et la vidéoconférence. Cela en fait un outil précieux pour les entreprises qui ont besoin de communiquer efficacement avec leurs employés ou leurs clients.

II.4.2.2. Rôle

La voip peut assurer plusieurs rôles :

- **Transmetteur de voix** : La VoIP est principalement utilisée pour transmettre des voix sur des réseaux IP tels qu'Internet. Son rôle principal est de convertir les signaux vocaux en données numériques, de les compresser et de les transmettre via des protocoles IP. Cela permet aux utilisateurs de passer des appels vocaux en utilisant des appareils connectés à Internet.
- **Remplacement des lignes téléphoniques traditionnelles** : La VoIP remplace progressivement les lignes téléphoniques traditionnelles. Elle offre une alternative plus rentable et flexible en utilisant le réseau IP existant. Les appels peuvent être acheminés via Internet plutôt que par des lignes téléphoniques dédiées, ce qui permet de réduire les coûts de communication.
- **Intégration des services de communication** : La VoIP permet d'intégrer différents services de communication, tels que la messagerie vocale, la vidéoconférence, la messagerie instantanée et la présence. Elle offre une plateforme unifiée pour la communication, ce qui facilite la collaboration et la productivité au sein des entreprises.

- **Fournisseur de services VoIP** : Les fournisseurs de services VoIP jouent un rôle clé dans la mise en œuvre de la VoIP. Ils proposent des services de téléphonie basés sur la VoIP aux utilisateurs finaux. Ils gèrent l'infrastructure, les serveurs et les logiciels nécessaires pour acheminer les appels et fournir des fonctionnalités supplémentaires, telles que la gestion des appels, les options de routage, etc.
- **Administrateur système VoIP** : Les administrateurs système VoIP sont responsables de la configuration, de la gestion et de la surveillance des systèmes VoIP. Ils veillent à ce que les équipements, les serveurs et les logiciels de VoIP fonctionnent correctement. Ils gèrent également les problèmes de qualité de service, la sécurité et les mises à jour du système.
- **Utilisateur final** : Les utilisateurs finaux sont les personnes qui utilisent la VoIP pour passer des appels vocaux. Cela peut inclure des particuliers, des entreprises, des centres d'appels, etc. Les utilisateurs finaux utilisent des appareils compatibles VoIP, tels que des téléphones IP, des applications de linphone sur ordinateur ou des applications mobiles, pour passer et recevoir des appels.

II.4.2.3. Sortes de voip

Il existe plusieurs types de voip, chacun ayant de fonctionnalités et des avantages différents.

Voici quelques-uns des types de Voip les plus courants :

1. **VoIP basée sur le protocole SIP** : SIP (Session Initiation Protocol) est un protocole de signalisation largement utilisé dans la VoIP. La VoIP basée sur SIP permet d'établir, de modifier et de terminer des sessions de communication en temps réel, comme les appels vocaux, la vidéoconférence et la messagerie instantanée. Elle est très répandue et compatible avec de nombreux appareils et logiciels.
2. **VoIP basée sur le protocole H.323** : H.323 est un autre protocole de signalisation utilisé dans la VoIP. Bien qu'il soit moins courant que SIP, il est utilisé dans certains systèmes de téléphonie IP et de vidéoconférence. Il permet la communication entre différents appareils et réseaux, mais il peut nécessiter une configuration plus complexe.
3. **VoIP propriétaire** : Certains fabricants d'équipements de téléphonie IP proposent leurs propres solutions VoIP propriétaires. Ces systèmes sont souvent intégrés à des équipements spécifiques du fabricant et sont conçus pour fonctionner uniquement avec leurs produits. Ils offrent généralement des fonctionnalités avancées et une intégration étroite, mais peuvent être moins flexibles en termes d'interopérabilité avec d'autres systèmes.

4. **VoIP via applications mobiles** : De nombreuses applications mobiles populaires, telles que WhatsApp, Skype, Viber et FaceTime, utilisent la VoIP pour permettre les appels vocaux et vidéo via Internet. Ces applications utilisent généralement des protocoles propriétaires et nécessitent une connexion Internet pour fonctionner. Elles sont largement utilisées pour les appels internationaux et les communications entre utilisateurs de différentes plateformes.
5. **VoIP d'entreprise** : La VoIP d'entreprise est spécifiquement conçue pour répondre aux besoins des organisations. Elle offre des fonctionnalités avancées telles que la gestion centralisée des appels, la messagerie vocale, la conférence téléphonique, la file d'attente d'appels, l'intégration avec les systèmes CRM, etc. Les systèmes de VoIP d'entreprise peuvent être basés sur SIP ou utiliser des solutions propriétaires.

II.4.3. ARCHITECTURE

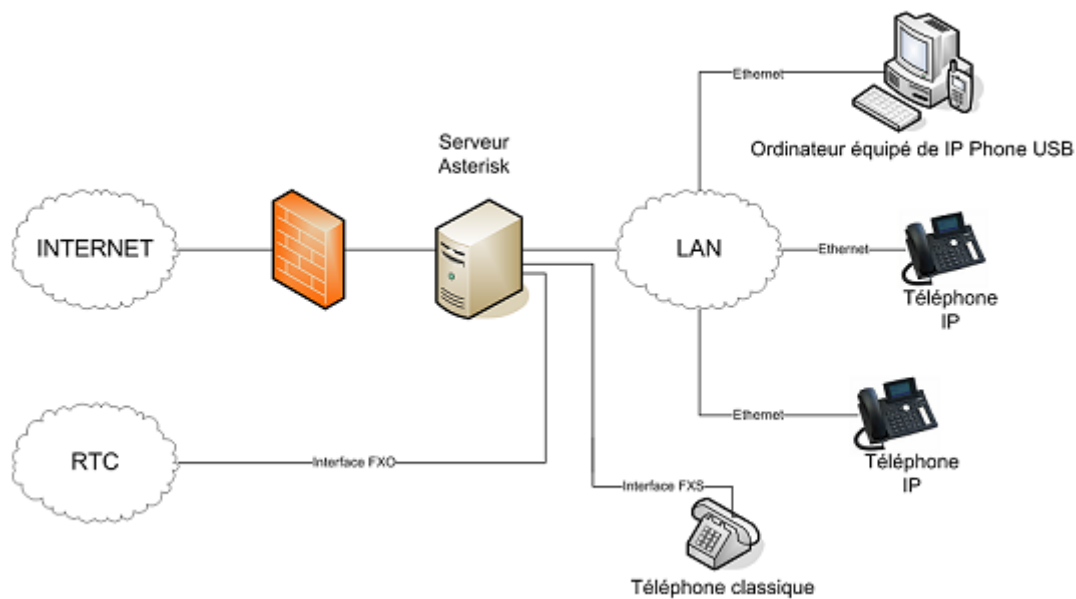


Figure 1 ARCHITECTURE

II.4.4. PROTOCOLE SIP

II.4.4.1 DESCRIPTION GENERALE DU PROTOCOLE SIP

Le Session Initiation Protocol (SIP) est un protocole de signalisation largement utilisé dans les communications en temps réel, notamment pour établir, modifier et terminer des sessions multimédias telles que les appels vocaux et vidéo sur les réseaux IP. Il est utilisé pour initier et contrôler les sessions de communication entre les participants. Voici quelques points clés à retenir sur le protocole SIP :

1. **Objectif principal** : Le principal objectif du protocole SIP est de faciliter l'établissement, la modification et la fin des sessions multimédias entre les utilisateurs. Cela inclut l'initiation des appels, le transfert d'appels, la mise en attente, la gestion de la présence, la messagerie instantanée, les conférences, etc.
 2. **Fonctionnement basé sur les requêtes et réponses** : SIP suit un modèle de communication basé sur les requêtes et réponses, similaire au protocole HTTP. Les agents SIP échangent des messages de requête et de réponse pour communiquer entre eux et établir les sessions souhaitées.
 3. **Éléments de base du protocole** : Les éléments fondamentaux du protocole SIP comprennent les utilisateurs (appelés User Agents), les serveurs SIP, les proxies SIP et les Redirect Servers. Les User Agents sont les terminaux utilisés par les utilisateurs pour initier les sessions, tandis que les serveurs SIP facilitent l'acheminement et le traitement des requêtes SIP.
 4. **Adresse SIP** : Chaque utilisateur SIP est identifié par une adresse SIP unique, similaire à une adresse e-mail. L'adresse SIP est au format "utilisateur domaine", où le domaine peut être une adresse IP ou un nom de domaine.
 5. **Méthodes SIP** : SIP utilise différentes méthodes pour les requêtes, telles qu'INVITE (pour initier une session), REGISTER (pour enregistrer une adresse SIP auprès d'un serveur), BYE (pour terminer une session), OPTIONS (pour obtenir les capacités d'un utilisateur), etc.
 6. **Réponse SIP** : Les réponses SIP sont utilisées pour indiquer le résultat d'une requête SIP. Les réponses sont identifiées par un code de statut à trois chiffres, indiquant le résultat de la requête (par exemple, 200 OK pour une requête réussie).
 7. **Extension et compatibilité** : SIP est un protocole extensible qui permet l'ajout de nouvelles fonctionnalités et de nouvelles méthodes en utilisant des extensions. Il est également compatible avec d'autres protocoles de communication et peut être utilisé conjointement avec d'autres protocoles, tels que le protocole RTP (Real-time Transport Protocol) pour le transport des flux multimédias.
 8. **Sécurité** : Pour assurer la sécurité des communications SIP, des protocoles complémentaires tels que le Transport Layer Security (TLS) et le Secure Real-time Transport Protocol (SRTP) peuvent être utilisés pour le chiffrement des communications et la protection contre les attaques.
- SIP est un protocole ouvert et largement utilisé dans les systèmes de téléphonie IP et les solutions de communication en temps réel. Il fournit une base solide pour l'interopérabilité

entre les différents équipements et services de communication IP, permettant ainsi des sessions multimédias flexibles et évolutives sur les réseaux IP.

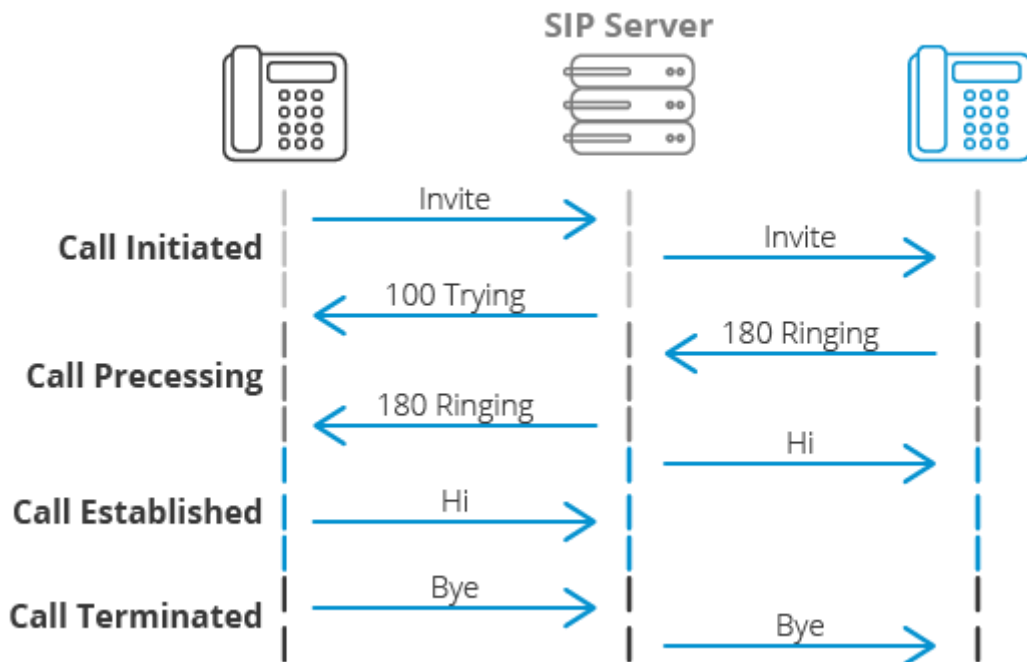


Figure 2 SIP SERVER

II.4.4.2. UN PROXY SIP

Un Proxy SIP sert d'être l'intermédiaire entre deux User Agents qui ne connaissent pas leurs emplacements respectifs (adresse IP). En effet, l'association URI-Adresse IP a été stockée préalablement dans une base de données par un Registrar. Le Proxy peut donc interroger cette base de données pour diriger les messages vers le destinataire. La figure 5 montre les étapes de l'interrogation du proxy la base de données.

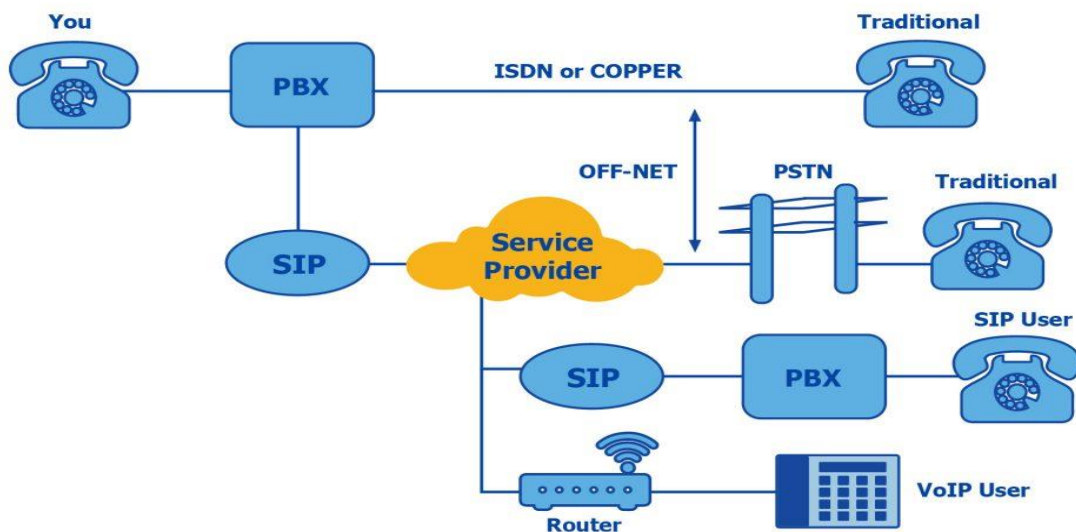


Figure 3 UN PROXY SIP

II.4.4.3. LE PROTOCOLE RTCP

Le protocole RTCP est fondé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP. Le protocole RTP utilise le protocole RTCP, Real-time Transport Control Protocol, qui transporte les informations supplémentaires suivantes pour la gestion de la session. Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS.

Ces rapports comprennent le nombre de paquets perdus, le paramètre indiquant la variance d'une distribution (plus communément appelé la gigue : c'est à dire les paquets qui arrivent régulièrement ou irrégulièrement) et le délai aller-retour. Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS. Parmi les principales fonctions qu'offre le protocole RTCP sont les suivants :

- **Une synchronisation supplémentaire entre les médias** : Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérées et suivre des chemins différents.
- **L'identification des participants à une session** : en effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique. Le contrôle de la session : en effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement.

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. On peut détailler les paquets de supervision en 5 types:

- **SR (Sender Report)** : Ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé de paquets perdus, variation de délai (gigue), etc.). Ces rapports sont issus d'émetteurs actifs d'une session.

- **RR (Receiver Report)** : Ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.
- **SDES (Source Description)** : Carte de visite de la source (nom, e-mail, localisation).
- **BYE** : Message de fin de participation à une session.
- **APP** : Fonctions spécifiques à une application.

II.4.4.4. ATTAQUES CONTRE LA VOIP ET BONNES PRATIQUES DE SÉCURISATION

Voici une liste d'attaques courantes contre la VoIP et des bonnes pratiques de sécurisation spécifiques à prendre en compte lors de l'étude et de la mise en place d'une solution VoIP :

Attaques contre la VoIP :

1. **Attaques par déni de service (DoS)** : ici nous allons mettre en place des mécanismes de détection et de prévention des attaques DoS pour limiter l'impact des tentatives de saturation du réseau ou des serveurs VoIP.
2. **Attaques par détournement de session (Call Hijacking)** : Nous allons pouvoir ajouter des protocoles de chiffrement tels que TLS et SRTP pour sécuriser les communications et empêcher l'interception ou la modification des sessions VoIP.
3. **Attaques par usurpation d'identité (Identity Spoofing)** : Implémentez des mécanismes d'authentification forte, tels que l'utilisation de certificats numériques ou d'authentification à deux facteurs, pour empêcher les attaquants de se faire passer pour des utilisateurs légitimes.
4. **Attaques d'enregistrement frauduleux (Registration Hijacking)** : Renforcez la sécurité du processus d'enregistrement en utilisant des mécanismes de validation supplémentaires, tels que des codes de vérification ou des vérifications d'adresse IP, pour éviter les enregistrements frauduleux.
5. **Attaques par injection de média (Media Injection)** : Mettez en place des contrôles de sécurité pour valider et filtrer les médias entrants, en utilisant des pare-feu ou des dispositifs de filtrage pour prévenir l'injection de médias non autorisés.

Bonnes pratiques de sécurisation de la VoIP :

1. **Segmentation du réseau** : Séparez les réseaux VoIP du réseau principal en utilisant des VLAN (Virtual Local Area Networks) ou d'autres mécanismes de segmentation pour limiter l'impact des attaques potentielles.
2. **Pare-feu** : Utilisez des pare-feu pour contrôler le trafic entrant et sortant des systèmes VoIP. Configurez-les de manière appropriée pour autoriser uniquement les connexions nécessaires et bloquer les connexions non autorisées.

3. **Chiffrement des communications** : Utilisez des protocoles de chiffrement tels que TLS (Transport Layer Security) et SRTP (Secure Real-time Transport Protocol) pour protéger les communications VoIP contre l'interception et la manipulation.

4. **Authentification et contrôle d'accès** : Mettez en place des mécanismes d'authentification forte pour l'accès aux systèmes VoIP, tels que des mots de passe forts, des certificats numériques et des mécanismes d'authentification à deux facteurs. Limitez également les privilèges d'accès aux utilisateurs autorisés uniquement.

5. **Mises à jour régulières** : Assurez-vous de maintenir à jour les équipements et les logiciels VoIP en installant les dernières mises à jour et correctifs de sécurité pour prévenir les vulnérabilités connues.

6. **Surveillance et détection des anomalies** : Mettez en place des systèmes de surveillance pour détecter les activités suspectes, les comportements anormaux et les tentatives d'intrusion. Utilisez des outils de détection d'intrusion pour alerter en cas de violation de sécurité.

7. **Sensibilisation à la sécurité** : Formez les utilisateurs sur les bonnes pratiques de sécurité, telles que la protection des mots de passe, la vigilance vis-à-vis des e-mails et des liens suspects, et la détection des signes d'attaques potentielles.

Ces bonnes pratiques de sécurité peuvent servir de base pour étudier et mettre en place une solution VoIP sécurisée. Il est également recommandé de consulter des experts en sécurité et des fournisseurs de solutions VoIP pour obtenir des conseils spécifiques à votre environnement et vos besoins.

II.4.4.5. FORMAT DU PAQUET SRTP

Un paquet SRTP est généré par transformation d'un paquet RTP grâce à des mécanismes de sécurité. Donc le protocole SRTP effectue une certaine mise en forme des paquets RTP avant qu'ils ne soient sur le réseau. La figure suivante présente le format d'un paquet SRT

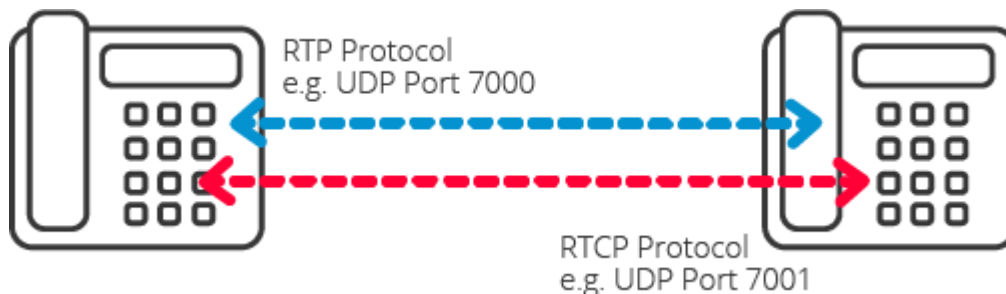


Figure 4 FORMAT DU PAQUET SRTP

II.4.4.6. Sécurisation de l'application

Plusieurs méthodes peuvent être appliquées pour sécuriser l'application, ces méthodes varient selon le type d'application (serveur ou client). Pour sécuriser le serveur il faut :

- L'utilisation d'une version stable, Il est bien connu que toute application non stable contient sûrement des erreurs et des vulnérabilités. Pour minimiser les risques, il est impératif d'utiliser une version stable.
- Tester les mises à jour des logiciels softwares dans un laboratoire de test. Il est très important de tester toute mise à jour de l'application dans un laboratoire de test avant de les appliquer sur le système en production
- Ne pas tester les correctifs sur le serveur lui-même :
- Ne pas utiliser la configuration par défaut qui sert juste à établir des appels.
- Elle ne contient aucune protection contre les attaques.
- Ne pas installer une application client dans le serveur.

II.4.4.7. Sécurisation du système d'exploitation

Il est très important de sécuriser le système sur lequel est implémenté le serveur de VoIP. En effet, si le système est compromis, l'attaque peut se propager sur l'application serveur. Celle-ci risque d'affecter les fichiers de configuration contenant des informations sur les clients Enregistrés. Il y a plusieurs mesures de sécurités à prendre pour protéger le système d'exploitation :

- Utiliser un système d'exploitation stable. Les nouvelles versions toujours contiennent des bugs et des failles qui doivent être corrigées et maîtrisées avant.
- Mettre à jour le système d'exploitation en installant les correctifs de sécurité

Recommandé pour la sécurité.

- Ne pas mettre des mots de passe simples et robustes. Ils sont fondamentaux contre les intrusions. Et ils ne doivent pas être des dates de naissances, des noms, ou des numéros de téléphones.
- Un mot de passe doit être assez long et formé d'une combinaison de lettre, de chiffres et ponctuations.
- Ne pas exécuter le serveur VoIP avec un utilisateur privilégié. Si un utilisateur malveillant arrive à accéder au système via une exploitation de vulnérabilité sur le serveur VoIP, il héritera tous les privilèges de cet utilisateur.

II.4.4.7. Asterisk in CHROOT :

Il empêche le serveur VoIP d'avoir une visibilité complète de l'arborescence du disque, en l'exécutant dans un environnement sécurisé qui l'empêche d'interagir librement avec le système.

- Sauvegarde des fichiers log à distance : les fichiers log sont très importants, il est conseillé de les enregistrer sur un serveur distant.
- Installer seulement les composants nécessaires : pour limiter les menaces sur le système d'exploitation. Il vaut mieux installer sur la machine le système d'exploitation et le serveur.
- Supprimer tous programmes, logiciels ou des choses qui n'ont pas d'importance et qui peuvent être une cible d'attaque pour accéder au système.
- Renforcer la sécurité du système d'exploitation en installant des patches qui permettent de renforcer la sécurité générale du noyau.

On peut aussi utiliser les pare feu ou/et les ACL pour limiter l'accès à des personnes bien déterminé et fermer les ports inutiles et ne laisser que les ports utilisés (5060, 5061, 4569,...). Le pare feu (firewall) est un software ou hardware qui a pour fonction de sécuriser un réseau ou un ordinateur contre les intrusions venant d'autres machines. Le pare feu utilise le système de filtrage de paquet après analyse de l'entête des paquets IP qui s'échange entre les machines. Le firewall peut être implémenté avec un ACL qui est une liste d'Access Control Entry (ACE) ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe. On aura besoin d'ACL pour donner des droits à des personnes bien déterminés selon leurs besoins et leurs autorités.

Pour un serveur VoIP, il est important d'implémenter les ACL pour sécuriser le serveur en limitant l'accès à des personnes indésirables. Par exemple, seuls les agents enregistrés peuvent envoyer des requêtes au serveur. Il existe trois catégories d'ACL : La liste de contrôle d'accès peut être installée en réseau sur les pare feu ou les routeurs, mais aussi ils existent dans les systèmes d'exploitation.

II.4.4.8 WIRESHARK

Wireshark est un logiciel open-source de capture et d'analyse de paquets réseau. Il est largement utilisé par les professionnels de la sécurité informatique, les administrateurs réseau et les développeurs pour examiner le trafic réseau en détail.

Wireshark permet de capturer et d'analyser le trafic réseau en temps réel ou à partir de fichiers de capture préalablement enregistrés. Il prend en charge une large gamme de protocoles réseau tels que TCP, UDP, IP, HTTP, DNS, FTP, et bien d'autres. En utilisant Wireshark, vous pouvez visualiser les paquets de données qui circulent sur votre réseau, analyser les échanges entre les différentes machines, et observer les informations telles que les adresses source et destination, les en-têtes de protocole, les données transmises, etc. Lors de l'analyse du trafic réseau avec Wireshark pour détecter une attaque DDoS, voici quelques signes caractéristiques que vous pouvez rechercher :

1. **Augmentation anormale du trafic** : Les attaques DDoS cherchent à submerger les ressources du réseau cible en générant un trafic excessif. Recherchez des pics de trafic significatifs ou une augmentation soudaine et importante du nombre de paquets capturés.
 2. **Protocoles inhabituels** : Les attaques DDoS peuvent utiliser différents protocoles pour saturer les ressources réseau. Recherchez des protocoles inhabituels ou des combinaisons inattendues de protocoles dans le trafic capturé.
 3. **Adresses IP sources multiples** : Les attaques DDoS impliquent souvent l'utilisation d'un grand nombre de machines infectées (bonnets) pour générer du trafic. Recherchez des adresses IP sources multiples dans les paquets capturés.
 4. **Paquets UDP ou ICMP volumineux** : Les attaques DDoS peuvent utiliser des paquets UDP (User Datagram Protocol) ou ICMP (Internet Control Message Protocol) volumineux pour saturer la bande passante du réseau cible. Recherchez des paquets UDP ou ICMP de grande taille dans le trafic capturé.
 5. **Paquets avec des motifs répétitifs** : Certaines attaques DDoS utilisent des motifs répétitifs dans les paquets pour consommer les ressources du réseau cible. Recherchez des schémas de paquets identiques ou similaires qui se répètent fréquemment.
 6. **Paquets avec des flags TCP inhabituels** : Les attaques DDoS peuvent impliquer des manipulations des en-têtes TCP pour épuiser les ressources du réseau. Recherchez des paquets TCP avec des combinaisons inhabituelles de flags, tels que SYN flood, ACK flood, etc.
 7. **Sources de trafic suspectes** : Identifiez les adresses IP sources suspectes ou non autorisées qui génèrent un trafic élevé. Recherchez des adresses IP connues pour être associées à des activités malveillantes ou des botnets.
- Analyse des patterns** : En analysant les patterns et les comportements du trafic, vous pouvez identifier des schémas anormaux ou répétitifs qui indiquent une attaque DDoS. Par

exemple, l'apparition soudaine d'un grand nombre de requêtes identiques provenant de différentes adresses IP.

II.5. PRESENTATION DU MILIEU D'ETUDE

II.5.1. Situation géographique

L'UAGO est implantée en République Démocratique du Congo dans la province du Nord-Kivu, ville de Goma, commune de KARISIMBI, dans l'avenue SALAMABILA, à côté de l'école secondaire Adventiste MARANATHA.

Elle est limitée :

- **Au nord** : par l'école primaire adventiste UZIMA ;
- **Au sud** : par la grande route de Goma vers SAKE ;
- **A l'Est** : par la route vers MAJENGO ;
- **A l'Ouest** : par l'institut MARANATHA ;

II.5.2. Historique de l'institution

L'Université Adventiste de Goma(UAGO) a vu le jour le 15 octobre 2000. En effet, c'est sous l'initiative des laïcs Adventistes de l'Association du Kivu centrale(AKC) qui ont ressenti un besoin d'organiser une institution d'enseignement universitaire. A cette époque, l'effectif des membres de l'Église Adventiste dans l'AKC s'élevait plus de 50.000 et avec un grand nombre d'école primaire et secondaire tous les finalistes de ces écoles ainsi que le personnel avaient besoin d'une formation universitaire.

Immédiatement, les activités académiques et les travaux de construction ont démarré sous la direction du premier Recteur en la personne de Mr. **NIYONSENGA MBIZI Eliel**. Deux facultés furent organisées : psychologie et science de l'éducation ; science économique et de Gestion. **L'UAGO** entretient des bonnes relations avec le ministre de l'enseignement supérieure et universitaire de la République Démocratique du Congo (**RDC**). Elle a été autorisée à fonctionner par l'arrêté départemental **N°JURS/CABCD/023/99 du 18 octobre 1999**. Le cycle de licence en science de L'éducation et en Sciences Economiques fut confirmé par l'arrête départemental **N°DEN/CABC/2002** et dont le début fut fixe au 1er décembre 2003. **L'arrêté ministériel n°1196/MINESU/CAB/SSM/2006 du 02/06/2006** portant agreement provisoire d'un établissement privé d'enseignement supérieur et universitaire dénommée « **UNIVERSITE ADVENTISTE DE GOMA** » fut octroyé. **Le décret présidentiel n° 06/0106 du 12 juin 2006 de l'UAGO** une personnalité juridique et les diplômes délivrés son homologue par le gouverneur congolais En 2004, la conférence générale de l'Église Adventiste a envoyé une mission d'inspection et l'UAGO est hissée au

niveau de « pré-candidat » L'UAGO connaît une progression remarquable depuis qu'elle a ouvert ses portes : elle a démarré avec deux facultés et un effectif de cinquante étudiants, aujourd'hui organise huit facultés avec cinq cents vingt-neuf étudiants. Dès son début jusqu'à présent, l'UAGO a déjà délivré 903 diplômes de gradué et 704 diplômes de licencié et compte 529 étudiants pour l'année académique 2018-2019. Ce bref parcours de l'UAGO augure un avenir plein d'espoir et avec l'appui du très haut, nous attendons la voir hisser à un niveau des institutions d'éducation supérieure selon les critères de l'Église Adventiste.

II.5.3. Mission

Pouvoir une éducation holistique qui rend les étudiants capables d'acquérir une connaissance pertinente et de capacité pratique fondées sur la vision biblique du monde envie de répondre aux besoins locaux.

II.5.4. Vision

- Promouvoir la science qui harmonise avec la foi et résultant le progrès qui honore Dieu et de focalisé sur le bien – être de l'humanité.

II.5.5. Valeur

- Non-violence
- Intégrité
- Créativité
- Travail en équipe

II.5.6. Objectifs

L'université Adventiste de Goma est une institution d'enseignement supérieur et universitaire privée, dirigée par l'église Adventiste du septième jour. Etant qu'une université Adventiste, ses objectifs sont les suivants :

- Participer au développement du pays à travers l'éducation dans certain domaine notamment : Gestion, agronomie, lettre, sante publique, science de l'éducation ;
- Initier ou appuyer la recherche-développement.
- Rayonnement de transformer l'environnement et produire de diplômés adapte l'avenir, capable de transformer la société et de construire la société de demain telle que le peuple le souhaite. (Annuaire UAGO, 2017).

II.5.7. Organisation et fonctionnement

II.5.7.1. Organisation

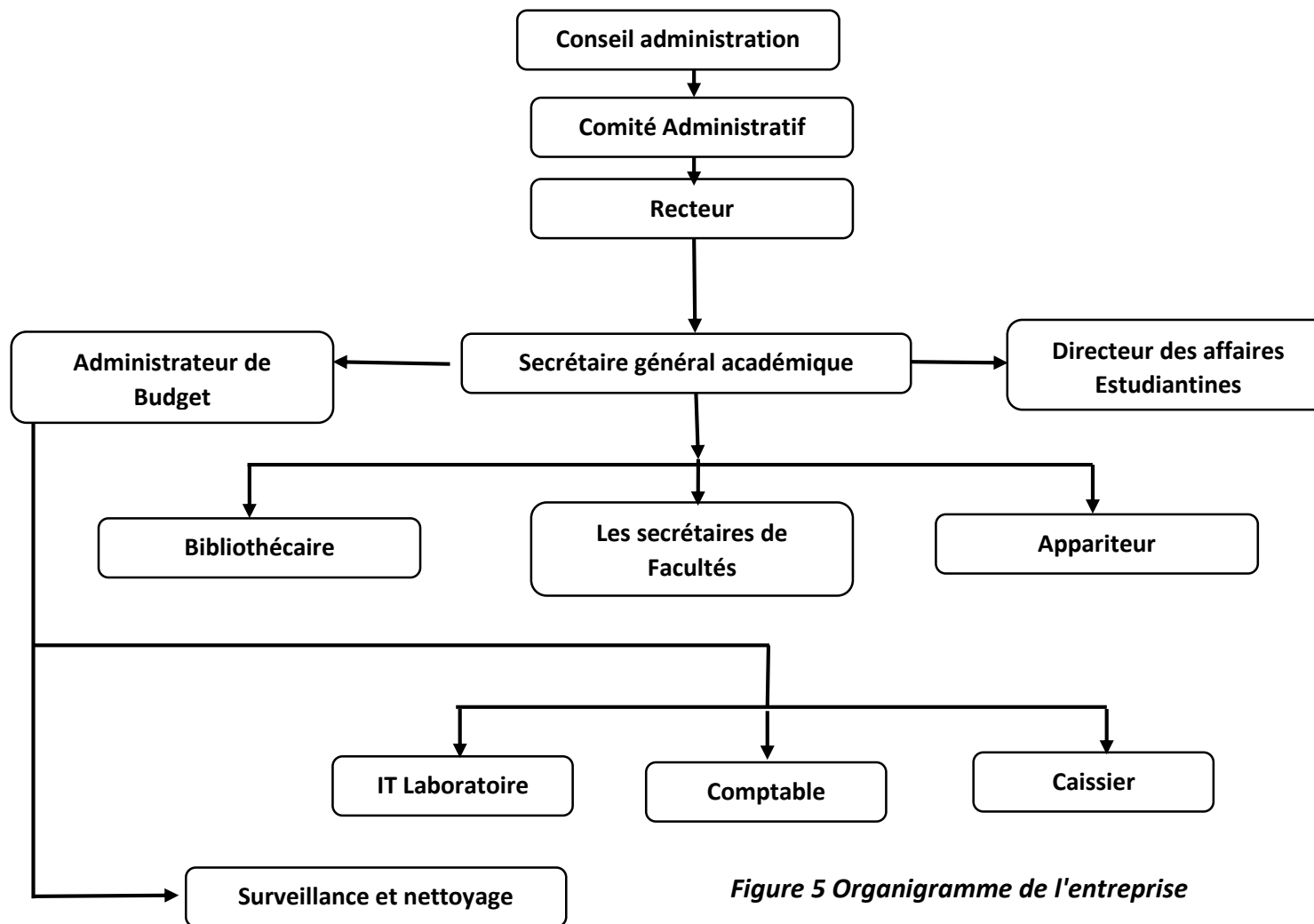


Figure 5 Organigramme de l'entreprise

II.5.7.2. Fonctionnement

1. Conseil d'administration

Le conseil d'administration est le principal comité universitaire responsable de l'ensemble des activités quotidiennes de l'université. Il s'agit à titre de responsable du traitement de toutes les questions relevant de la responsabilité du conseil universitaire. Il sert de manière législative, en tant que pouvoir déléguer, dans toutes les autres questions.

2. Comité Administratif

Ce comité prend ses décisions et recommandations d'une manière collégiale ;

Il est solidairement responsable devant le comité exécutif,

Il est chargé de,

- ✓ Assurer la gestion courante de l'U.A. GO & I.S.T.A. GO ;
- ✓ Recommander au comité exécutif les prévisions budgétaires préparées par le service de finance ;
- ✓ Préparer l'agenda du comité exécutif ;

Le comité Administratif a pour membre :

- Le recteur en même temps directeur général qui est le président du comité.
- Le secrétaire général administratif : secrétaire du comité
- Le secrétaire général académique : Membre
- Le secrétaire Général des affaires estudiantines : Membre

Le mandat pour les administrateurs de l'université est de 5 ans. Ce mandat est renouvelable une seule fois et l'intérim ne peut excéder une année.

3. Recteur

Le recteur doit être détenteur d'un doctorat à thèse avec moins le grade de professeur associé et a la charge de diriger l'ensemble de l'UAGO & ISTAGO d'en promouvoir par les moyens appropriés, l'unité, la collaboration et progrès. Outre ses qualifications spirituelles et membre de l'église adventiste du septième jour, parmi ces attributions nous avons :

- Diriger, promouvoir et coordonner toutes les activités de la communauté universitaire de l'UAGO et l'ISTAGO ;
- Représenter l'UAGO et l'ISTAGO auprès de tiers
- Présider les réunions du comité exécutif et administratif et veiller à l'application des décisions prises ;
- Etc....

4. Secrétaire Général Académique

Le Secrétaire Général Académique doit être détenteur d'un doctorant à thèse, et il est assiste le chef d'Etablissement dans ses fonctions. Le secrétaire général académique est membre du comité de gestion. Il supervise et coordonne les activités des services relevant de son ressort. Il fait rapport des activités de ses services au chef d'Etablissement dans les conditions prévues par le règlement organique.

A ce titre, parmi ces attributions il y'a :

- La gestion du personnel académique et scientifique qui s'occupe des dossiers de cette catégorie du personnel, leur carrière, leur promotion, leur appréciations, avancement de cours, etc. ;
- Suivre, au jour le jour, les activités de tout le secteur académique de l'établissement, en particulier les plans annuels des cours offerts par les facultés et les calendriers des cours avec l'aide des doyens des facultés.
- Présider les comités académiques ;
- Rédiger chaque semestre un rapport détaillé sur la vie académique de l'établissement ;
- Aider le corps enseignant à améliorer la qualité des enseignements et encourager la recherche ;
- Etc...

5. Secrétaire Général Administratif et Administrateur de Budget

Il est chargé de l'administration et de finances de l'UAGO et l'ISTAGO, il est directement responsable devant le recteur et le chef d'établissement. Il a la charge générale de l'administration financière de l'établissement, des biens physiques et des unités des productions.

Ses fonctions et responsabilités sont les suivantes :

- Il coordonne et supervise la gestion financière quotidienne de l'établissement dans le strict respect du règlement financier et des dispositions réglementaires en vigueur ;
- Rédige et commente, sous le couvert du comité de gestion, le rapport annuel de gestion financière.
- Supervise la comptabilité de l'établissement et suit les mouvements des comptes bancaires ;
- Préparer le budget annuel et veille au respect des règles budgétaires et à sa réparation dans les différents services de l'établissement ;
- Etc...

5. Directeur des Affaires Estudiantines

Le directeur des affaires estudiantines doit être au moins un détenteur d'une License (Maitrise). Il a comme attributions :

- Superviser les œuvres estudiantines ainsi que les espaces environnants ;
- Présider le comité mensuel des œuvres (gestion des homes, dortoirs et toutes autres infrastructures servant au logement des étudiants) ;
- Promouvoir la discipline et tenir le comité de discipline ;
- Etc...

6. Bibliothèque

La bibliothèque est un service base universitaire pour le personnel, les étudiants et les utilisateurs externes. Dans le but d'empêcher que la bibliothèque ne soit entraînée par des événements ou des enthousiasmes individuels, le bibliothécaire a l'obligation d'instituer des systèmes qui améliorent le fonctionnement de la bibliothèque et préservent le matériel d'information afin qu'il n'en soit pas perdu. Cela garantit que les informations sont identifiées, saisies, organisées et utilisées sous la forme de connaissances afin qu'aucune ne soit gaspillée et rendent les connaissances disponibles de sorte qu'aucune ne doive être privée dans les fonctions opérationnelles quotidiennes de la bibliothèque.

7. Apparitorat Central

L'appariteur est la porte d'entrée des étudiants pour entrer et sortir de l'université. En tant que département, ses principales fonctions sont : les admissions, la génération et la tenue des dossiers des étudiants, l'inscription et la remise des diplômes, la délivrance de certificats et de relevés de notes, la lettre de bourse et la délivrance de cartes d'étudiant aux étudiants.

8. Services de sécurité

Le département de de sécurité de l'UAGO et l'ISTAGO est chargé de la sécurité et de la protection des vies et biens de l'université et de la communauté universitaire, Nous prévenons les infractions de manière proactive et faisons tout ce qui est nécessaire pour réagir rapidement à une telle menace une fois remarquée.

9. Le Service de nettoyage

Ce service a été créé pour surveiller la propreté, fournir un environnement sur et sécurisé pour les étudiants, les employés et les visiteurs également pour prévenir la perte ou l'endommagement du bâtiment de l'université.

II.5.8. DIAGNOSTIC DE L'EXISTANT

La critique de l'existant, appelée aussi bilan de l'existant, va nous aider à l'évaluation du système existant par rapport à l'analyse faite à l'Université Adventiste de Goma sous étude tout en établissant un diagnostic. Ce diagnostic est établi dans le but de rechercher des solutions futures à des problèmes posés.

Le but de la critique de l'existant est d'établir un diagnostic précis sur les procédures utilisées, relever l'utilisation VOIP, les qualités et les défauts du système existant. Par ailleurs, deux aspects sont toujours dégagés lors de cette critique dont l'un est positif et l'autre négatif.

Ces deux aspects méritent d'être soulevés étant donné que le besoin de la perfection sera toujours souhaité par les utilisateurs en vue de bon fonctionnement.

II.5.8.1. Aspects positifs

Amélioration de la sécurité des communications : La mise en place d'une solution VoIP sécurisée permet de renforcer la confidentialité des appels et de protéger les données vocales sensibles contre les interceptions ou les écoutes indésirables.

Réduction des risques de fraudes téléphoniques : Les solutions VoIP sécurisées intègrent généralement des mécanismes d'authentification des utilisateurs, ce qui réduit les risques de fraudes téléphoniques et les appels non autorisés.

II.5.8.2. Point forts

Pour ce qui concerne le cote fort du réseau existant de l'UAGO en ce qui concerne l'administration du réseau nous trouvons que le réseau est bien administré, les clients reçoivent les adresse IP à partir du serveur DHCP ainsi donc tous les services dans le même réseau locale

II.5.8.3. Point faibles

Pour le réseau existant à l'UAGO nous avons constaté que le point faible réside au niveau de communication pour la réduction du cout pour passe l'appel facilement.

II.5.8.4. Proposition des solutions

Dans ce travail nous avons vu mieux de mettre en place une solution voip sécurisée distribue pour l'architecture client-serveur pouvant à partager les données sans tenir compte du système d'exploitation ainsi que l'accès aux données par le certificat wireshark.

CHAP III : PLANNING PREVISIONNEL DU PROJET

Dans ce chapitre nous allons parler en grande partie sur plan de notre travail ainsi que l'estimation du cout du projet informatique.

III.1. DEFINITIONS DE CONCEPTS

III.1.1 Projet

Un projet est un effort temporaire entrepris dans le but de créer un produit, un service ou un résultat unique. Il implique généralement des activités spécifiques et coordonnées, menées par une équipe ou une organisation, pour atteindre des objectifs clairement définis dans des délais et avec des ressources prédéterminées.

Voici quelques caractéristiques clés d'un projet :

Un début et une fin : Un projet a un début précis et une date de clôture prévue. Il est limité dans le temps, contrairement aux opérations continues qui ont une nature répétitive.

Le projet : ensemble d'activité regroupant les trois caractéristiques suivantes :

Il est entrepris pour satisfaire un besoin spécifique, sa durée et les moyens accordés sont limites et enfin il aboutit à un résultat unique censé satisfaire le besoin. (Y, p. 2019)

Nous avons trois organisations qui ont défini le mot projet de la manière suivante :

Selon la norme ISO 10006(version 2003) : un projet est un processus unique qui consiste en un ensemble d'activités coordonnées et maîtrisées, comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifique, incluant des contraintes de délais , de couts et de ressources . (Y, 2019)

Selon le PEMBOK : un projet est considéré comme une entreprise temporaire décidée pour obtenir un produit ou un service unique. (Y, 2019)

Selon L'AFITEP définit un projet comme : ensemble d'actions a réaliser pour satisfaire un objectif définit, dans le cadre d'une mission précise, et pour la réalisation lesquelles on a identifié non seulement un début ; mais aussi une fin((Y, 2019))

III.3 REALISATION DU PROJET

La réalisation d'un projet nécessite souvent une succession des taches auxquelles s'attachent certaines contraintes notamment :

- **Le temps :** délai à respecter pour l'exécution
- **L'antériorité :** certaines taches doivent être exécutent avant d'autres
- **La Simultanéité :** certaines taches doivent être réalisées en même temps

- **La production** : temps d'occupation du matériel par les hommes qui l'utilisent (Emmanuel, 2022)

III.4 DETERMINATION DES OBJECTIFS

La conduite de projet est représentée comme une pyramide dont le sommet le système pilotage du projet au travers des trois types de gestion à mettre en œuvre : gestion du temps, gestions des ressources et gestion de la production. Pour atteindre les objectifs, il faut détermine toutes les taches et la phase constituant ce projet soient exécutées dans le temps et avec les moyens nécessaires. La connaissance des différentes tâches à accomplir ne suffit pas pour réaliser un projet. Il faut encore une parfaite connaissance de l'articulation permettant de le réaliser dans les conditions du cout et de délais impose. Cependant son déroulement, vérifie constamment si le plan établi est respecté.

III.5 METHODE D'ORDONNANCEMENT

Il existe 3 méthodes d'ordonnement utilisées :

- **La méthode en barre au Diagramme de GANT**
- **La méthode potentielle Métra(MPM) et**
- **La méthode program evaluation and research task (PERT)**

Dans notre travail nous allons nous focalise au diagramme PERT parce qu'elle nous permet de d'écrire l'enchainement des taches en tenant compte des contraintes d'ordonnement qui le lient. Cette méthode introduit la notion des taches fictives de durée égale à 0 au début et la fin. La tache fictive de début reliant toutes les taches sans prédécesseurs a la tache fictive de fin reliée sans successeur.

III.6. DETERMINATION DE TACHES

La première phase pour établir un réseau PERT consiste à déterminer les taches. Elle consiste à identifier et listes les taches nécessaires à la construction effective du projet. Chaque tâche est associée à une durée estime en unité de temps.

Code	Tache	Tache antérieur	Durée à jour
A	Conceptualisation projet	Aucune	3
B	Recherche de la documentation, lecture des ouvrages et recueil de données	A	3

C	Collecte des données et formalisation du projet (cadre du projet)	B	4
D	Analyse de l'existant	C	3
E	Spécification des besoins	D	3
F	Modélisation du nouveau système et installation asterisk sous Ubuntu	E	3
G	Configuration et déploiement du nouveau système de vidéos conférence	F	4
H	Test du nouveau système	G	3
I	Formation utilisateur	H	1
	TOTAL		27jrs

Tableau n°1 identification de tâche

L'objectif de l'étude et de la mise en place d'une solution VoIP est de créer et de déployer une infrastructure et une architecture de communication qui permettent des appels vocaux et vidéo sécurisés via Internet. Le but est de garantir la qualité, la fiabilité et la sécurité des communications VoIP, tout en répondant aux besoins spécifiques de l'organisation ou des utilisateurs concernés. La mise en œuvre de tout projet exige qu'on évalue les besoins en termes de coût.

Tableau 1 Identification de tache

Code tache	Description de tache	Tache précédent	Nombre jour	Nbre personnes	Cout unitaire en \$	Cout total en \$
A	Conceptualisation du projet	-	3	1	20	60
B	Recherche de la documentation lecture des ouvrages et recueil de données.	A	3	2	20	120
C	Collecte des données et formalisation du projet(cadrage du projet	A	4	1	20	80
D	Analyse de l'existant	C	3	1	20	80
E	Spécification de besoins	D	3	2	20	60
F	Modélisation du nouveau système et installation du serveur téléphonique Asterisk	D,E	3	1	30	60
G	Test du nouveau système d'appel audio et vidéo conférence	F	4	1	20	140
H	Déploiement et test de la solution	G	3	2	20	140
I	Formation utilisateur	H	1	3	20	140
TOTAL			24			670\$
Imprévue	10%					70
Cout total générale du projet						740\$

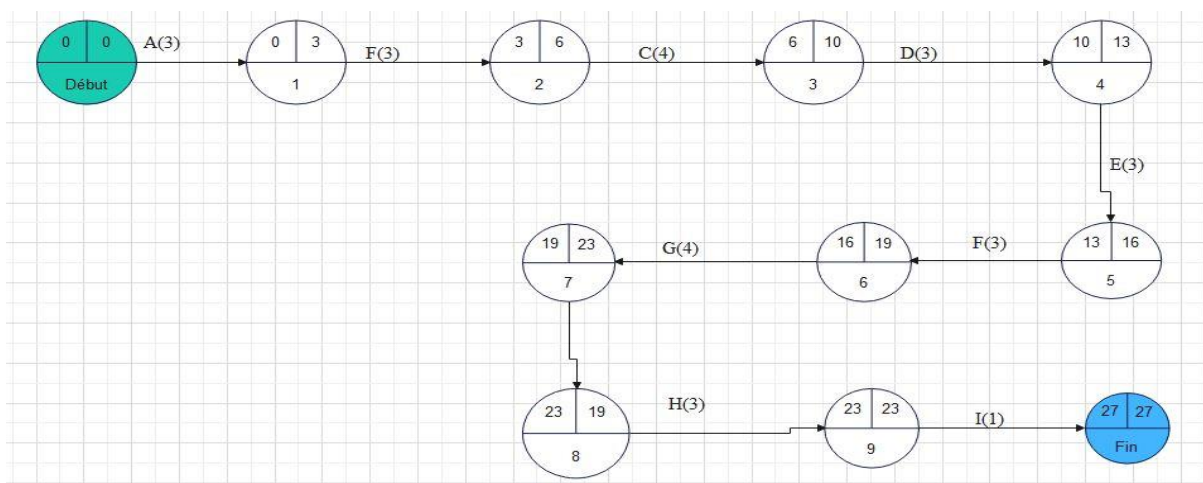
Tableau 2 Estimation du cout du projet

MATERIEL	CARACTERISTIQUE	NOMBRE	PU	PT
Ordinateur	Elite book 2570p,500GO, Ram :4GO, processor : 2.50GHz 2.50 GHz	5	300\$	1500\$
Internet	Connexion global broadcast	12 mois	400\$	4800\$
Serveur	Asterisk	1	4000\$	4000\$
Câble	UTP	1 carton	100\$	100\$
Connecteur	RJ45	1 carton	5\$	164\$
Switch	2960	1	750\$	750\$
Modem	AIRBOX4G+ orange	1	200\$	200\$
Total				11514\$

Tableau 3 Estimation du cout matériels

Numéro	Désignation	Montant
1	Main d'œuvre	46056\$
2	Cout des matériels	11514\$
Cout total générale du projet		57570\$

III.7. ELABORATION DU GRAPHET PERT

**Figure 6 : ELABORATION DU GRAPHET PERT**

III.8) DETERMINATION DE LA DATE AU PLUS TOT, DATE AU PLUS TARD, MARGE LIBRE ET MARGE TOTAL

III.8.1. Date au plus tôt

Les dates au plus tôt (D+ tôt) sont synonymes de début des dates plus tôt « les calculs des dates commencent tout d'abord par les dates au plus tôt. Pour une étape donnée, cette information détermine à quelle date minimum depuis le début du projet sera atteinte, au plus tôt, l'étape considérée. Pour ce faire, on se base sur l'estimation de la durée de taches.

On part de l'étape du début, pour laquelle la date au plus tôt est initialisée a 0, et on parcourt le réseau en suivant l'agencement des taches détermine auparavant. Pour calculer les dates d'une tache, on procède de la manière suivante : ce que nous devons savoir est qu'il y a un seul chemin possible pour atteindre l'étape ; la date au plus tôt vaut la date au plus tôt antérieure a quelle on ajoute la durée de la tache liant les étapes :

Pour plusieurs taches il y a plusieurs chemins possibles pour atteindre l'étape. On applique le procédé décrit ci-dessus (pour une seule tache) pour chacune de taches antérieures ; la date au plus tôt vaut le maximum parmi ces résultats :

III.8.2 Date au plus tard

Les dates au plus tard signifie la date début au plus tard et la date fine au plus tard « pour une étape donnée, cette information détermine à quelle date maximum, depuis le début du projet doit être atteinte, au plus tard, l'étape considérée, afin que le délai de l'ensemble du projet ne soit pas modifié. Pour ce faire, on se base sur l'estimation de la durée des taches. On part de l'étape de fin, pour laquelle la date au plus tard est initialisée à la même valeur que la date au plus tôt déterminée précédemment, et on parcourt le réseau en suivant l'agencement inverse des taches ».

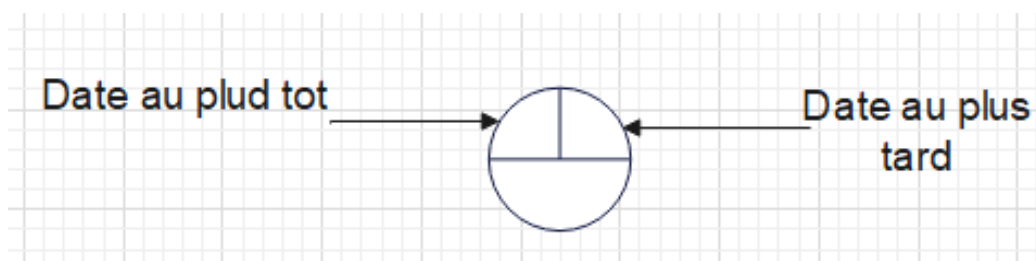


Figure 7 Date au plus tôt et date au plus tard

III.8.3. Calculs de marge

On appelle « marge » d'une tâche le retard qu'il est possible de tolérer dans la réalisation de celle-ci, sans que la durée optimale prévue du projet global en soit affectée. Il s'agit donc de la possibilité qu'a une tâche d'être retardée sans pour autant impacter sur le chronogramme du projet. Deux sortes de marges sont à distinguer.

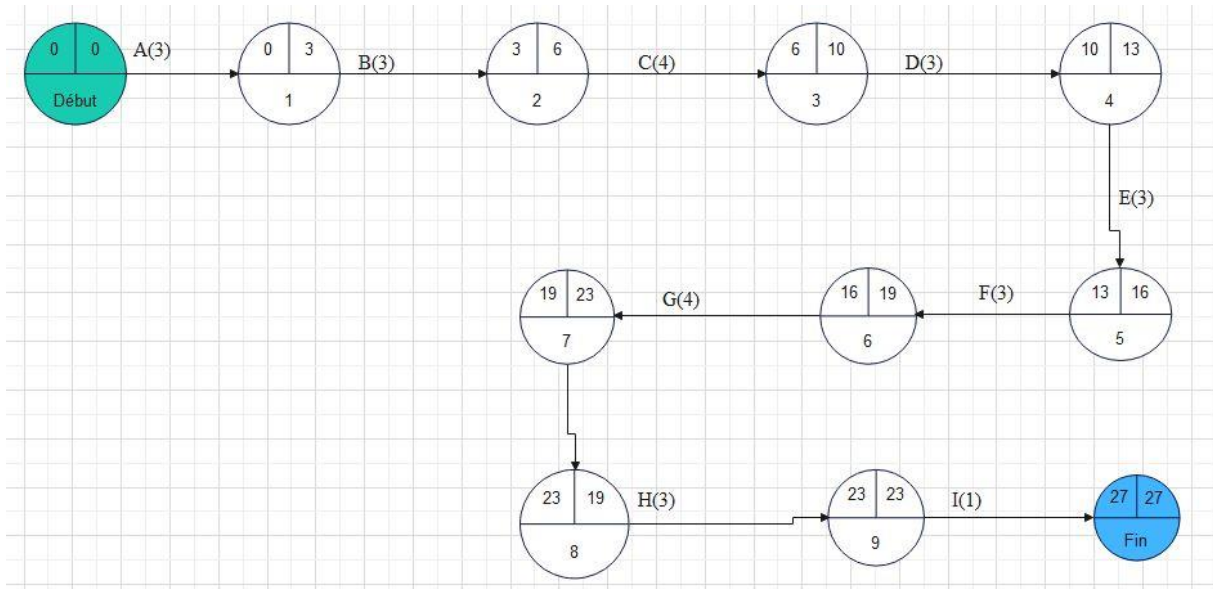


Figure 8 Calculs de marge

III.8.4. La marge libre(ML)

La marge libre d'une tâche indique le retard que l'on peut admettre dans la réalisation de cette tâche sans modifier les dates au plus tôt des tâches suivantes et sans allonger la durée optimale du projet. Cette image se calcule par la formule

$$ML = \text{la date au plus tôt de la tâche suivante} - \text{la durée} - \text{la date au plus tôt de la tâche précédente}$$

$$ML(A) = 3 - 1 - 3 = 0$$

$$ML(B) = 6 - 3 - 3 = 0$$

$$ML(C) = 10 - 6 - 4 = 0$$

$$ML(D) = 13 - 10 - 3 = 0$$

$$ML(E) = 23 - 16 - 3 = 4$$

$$ML(F) = 19 - 16 - 3 = 0$$

$$ML(G) = 16 - 19 - 4 = -3$$

$$ML(H) = 19 - 3 - 16 = 0$$

$$ML(I) = 23 - 4 - 19 = 0$$

$$ML(J) = 27 - 5 - 22 = 0$$

$$ML(J) = 27 - 0 - 27 = 0$$

III.8.5. La marge totale

La marge totale d'une tâche indique le retard maximal que l'on peut admettre dans la réalisation de cette tâche sans allonger la durée optimale du projet. Ainsi, pour notre projet, Bref : la marge totale est égale à la date au plus tard moins la date au plus tôt. Les marges totales de différentes tâches se présentent comme suit :

$$MT(A) = 3 - 3 = 0$$

$$MT(B) = 6 - 6 = 0$$

$$MT(C) = 10 - 10 = 0$$

$$MT(D) = 13 - 13 = 0$$

$$MT(E) = 23 - 23 = 0$$

$$MT(F) = 19 - 19 = 0$$

$$MT(G) = 16 - 16 = 0$$

$$MT(I) = 19 - 19 = 0$$

$$MT(H) = 23 - 23 = 0$$

$$MT(I) = 27 - 27 = 0$$

III.8.6. DETERMINATION DU CHEMIN CRITIQUE

On appelle chemin critique du réseau PERT, la succession de tâches pour lesquelles aucun retard n'est possible sans remettre en cause la durée optimale du projet. Il s'agit donc d'un chemin qui reprend les tâches pour lesquelles la date au plus tôt est égale à la date plus tard.

C'est le chemin le plus long du projet. Ainsi, le chemin critique est trouvé en calculant la marge libre et la marge totale de chaque tâche. De ce fait, le chemin critique est le chemin du graphe passant par les tâches dont les marges libres et les marges totales sont nulles. Dans le cadre de ce travail, les tâches du chemin critique sont : A, B, C, D, E, F, G, H, I, et J tel qu'illustre sur la figure ci-dessous :

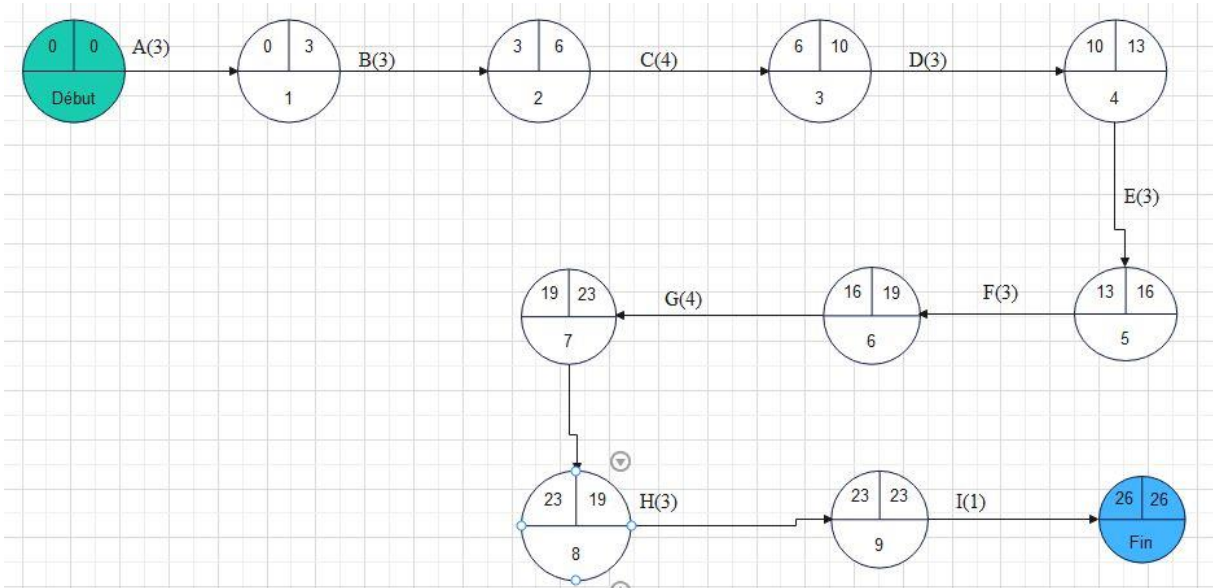


Figure 9 DETERMINATION DU CHEMIN CRITIQUE

III.5 CALENDRIER DU PROJET ET DIAGRAMME DE GANTT

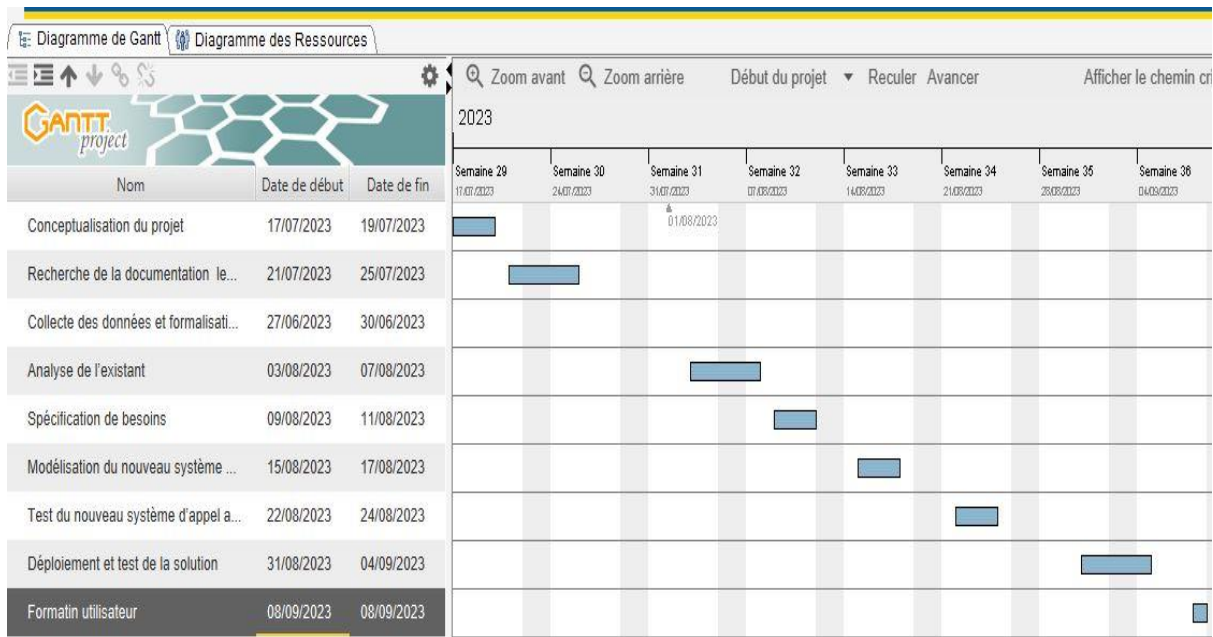


Figure 10

Figure 11 CALENDRIER DU PROJET

CHAP.IV PRESENTATION DES RESULTATS

IV.1 ENVIRONNEMENT MATÉRIELS ET LOGICIEL

Dans cette section, il sera question de présenter les environnements matériel et logiciel pour l'étude et la mise en place d'une solution VoIP sécurisée :

IV.1.1. Environnement matériel :

1. Serveur ou ordinateur de traitement :

- Un serveur ou un ordinateur suffisamment puissant pour exécuter le logiciel PBX (Private Branch Exchange) VoIP, tel que Asterisk.
- Une quantité adéquate de mémoire RAM et d'espace de stockage pour prendre en charge les opérations du système.

2. Téléphones IP :

- Des téléphones IP compatibles avec la solution VoIP choisie.
- Assurez-vous que les téléphones IP prennent en charge les protocoles de sécurité, tels que le Transport Layer Security (TLS) pour le chiffrement des communications.

3. Passerelles VoIP :

- Les passerelles VoIP permettent de connecter le réseau VoIP à des lignes téléphoniques traditionnelles (PSTN).
- Choisissez des passerelles VoIP qui prennent en charge des protocoles de sécurité tels que le Secure Real-time Transport Protocol (SRTP) pour le chiffrement des appels.

4. Équipement réseau :

- Des commutateurs Ethernet pour connecter les téléphones IP, les passerelles et le serveur PBX.
- Un pare-feu pour protéger le réseau VoIP contre les accès non autorisés.

IV.2. Environnement logiciel :

1. Système d'exploitation :

- Choisissez un système d'exploitation sécurisé et régulièrement mis à jour, tel que Linux (par exemple, Ubuntu Server) pour héberger le serveur PBX.

1. Logiciel PBX VoIP :

- Utilisez un logiciel PBX VoIP tel que Asterisk, qui est un logiciel open-source populaire et offre de nombreuses fonctionnalités avancées.

- Assurez-vous d'utiliser une version stable et mise à jour du logiciel pour bénéficier des dernières améliorations de sécurité.

3. Protocoles de sécurité :

- Utilisez des protocoles de sécurité tels que Transport Layer Security (TLS) pour chiffrer les communications SIP entre le serveur PBX et les téléphones IP.
- Implémentez Secure Real-time Transport Protocol (SRTP) pour chiffrer les flux audio afin d'assurer la confidentialité des appels.

4. Gestion des identités et des accès :

- Mettez en place des méthodes d'authentification forte, comme l'utilisation de mots de passe forts et de certificats numériques.
- Configurez des règles de pare-feu pour limiter l'accès au réseau VoIP aux adresses IP autorisées.

5. Mises à jour et surveillance :

- Veillez à maintenir votre environnement logiciel à jour en appliquant les correctifs de sécurité et les mises à jour recommandées.
- Mettez en place une surveillance du système pour détecter toute activité suspecte ou toute violation de sécurité potentielle

IV.3. Présentation des interfaces graphiques

- 1) **Capturez le trafic réseau** : Lancez Wireshark et commencez à capturer le trafic réseau sur l'interface réseau que vous souhaitez surveiller. Vous pouvez sélectionner l'interface appropriée dans la liste déroulante "Interface" de Wireshark. Assurez-vous de limiter la capture au trafic pertinent en utilisant des filtres tels que l'adresse IP source/destination ou le port....

The screenshot shows the Wireshark interface with a list of captured packets. The selected packet (No. 8) is a TCP RST packet from 10.0.2.15 to 10.0.2.15. The packet details pane shows the following information:

- Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface enp0s3, id 0
- Ethernet II, Src: PcsCompu_f7:d5:cd (08:00:27:f7:d5:cd), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 102.132.96.54
- Transmission Control Protocol, Src Port: 39386, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
- Transport Layer Security

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000  52 54 00 12 35 02 08 00 27 f7 d5 cd 08 00 45 00  RT..5...E
0010  00 4f 30 bc 40 00 40 06 37 24 0a 00 02 0f 66 84  -00@.@7$...f
0020  60 36 99 da 01 bb 54 16 2e 85 47 4b 02 c9 50 18  ^6...T...GK.P
0030  f5 3c d3 0a 00 00 17 03 03 00 22 14 42 22 a6 2d  <...B"
0040  3a 5e 36 6b 0f e2 5b 52 f1 df 66 02 cd 1f 08 d8  :A6k[R..f....
0050  cd ba de 26 9d 6a c5 50 24 33 aa 72 01          ...&i-P$3r
  
```

2) INSTALLATION ET CONFIGURATION D'UNE SOLUTION DE VOIP BASÉE SUR L'OUTIL ASTERISK.

Asterisk est un autocommutateur téléphonique privée (PABX) open source pour les Systèmes d'exploitation UNIX(Ubuntu), il est publié sous licence GPL. Asterisk comprend un nombre très élevé de fonctions, tel que les appels téléphoniques, la Messagerie vocale, les files d'attente, les conférences, etc. Il implémente plusieurs protocoles.

H.320, H.323, SIP et IAX.

Durant ce chapitre, on montrera les étapes d'installation et de configuration d'Asterisk sous le Système d'exploitation Linux, ainsi que l'installation et la configuration de X-Lite qui est un Téléphone VoIP soft phone, freeware.

2.1) Architecture du réseau VoIP déployé

Cette figure montre l'architecture adoptée au cours de la configuration de la solution de VoIP à base d'Asterisk.

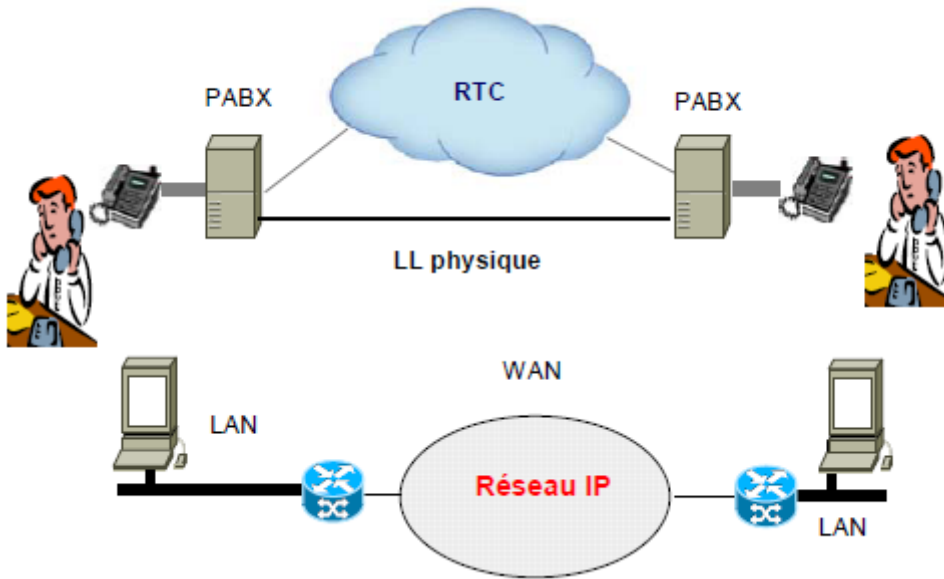


Figure 12 Architecture du réseau VoIP déployé

2.2) INSTALLATION UBUNTU LINUX


Install (as superuser)

Help and support

The Official documentation covers many of the most common areas about Ubuntu. It's available both [online](#) and via the Ubuntu Help item in the System menu.

At [Ask Ubuntu](#) you can ask questions and search an impressive collection of already answered questions. Support in your own language may be provided by your [Local Community Team](#).

For pointers to other useful resources, please visit community.ubuntu.com/help-information or ubuntu.com/support.



▸ Copying files...

Activer W

Sep 14 16:33

Installation

Qui êtes-vous ?

Votre nom : ✓

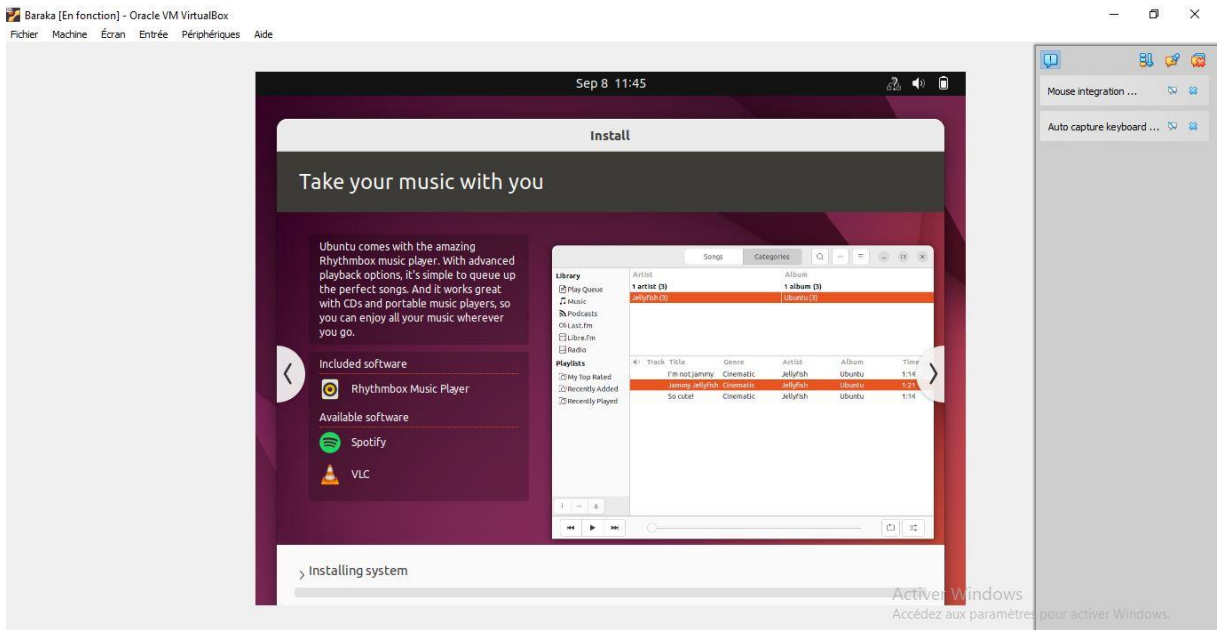
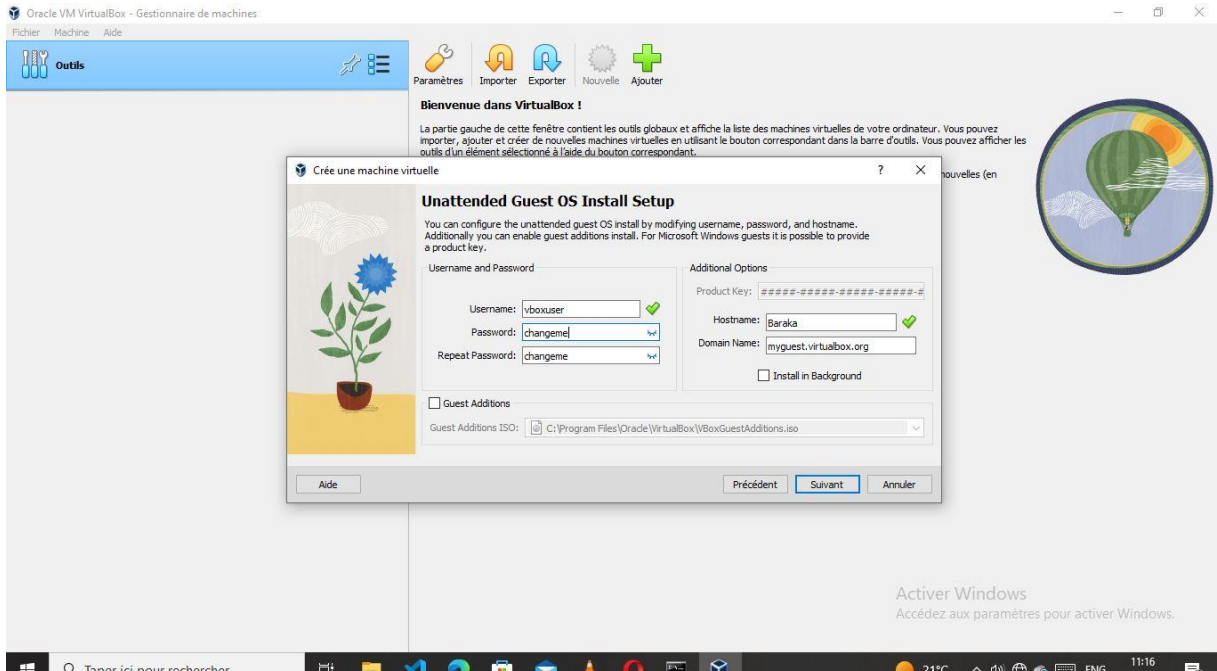
Le nom de votre ordinateur : ✓
Le nom qu'il utilise pour communiquer avec d'autres ordinateurs.

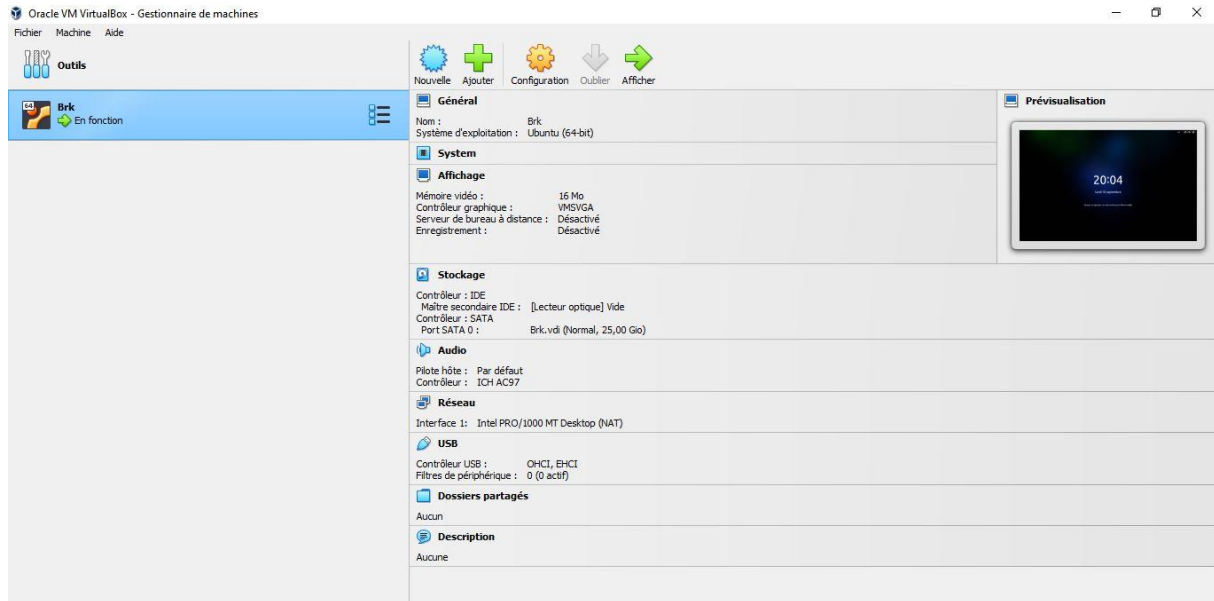
Choisir un nom d'utilisateur : ✓

Choisir un mot de passe : Mot de passe acceptable

Confirmez votre mot de passe : ✓

Ouvrir la session automatiquement
 Demander mon mot de passe pour ouvrir une session
 Utiliser Active Directory
Vous saisissez le domaine et d'autres détails à l'étape suivante.





2.3) INSTALLATION D'ASTERISK

Pour installer l'asterisk, il faut d'abord mettre à jour le système en utilisant la commande :

```
Sudo apt update
```

```
sudo apt upgrade
```

Après la mise à jour, nous allons taper: `sudo apt install asterisk`

```
baraka@baraka-VirtualBox:~$ sudo apt install asterisk
[sudo] Mot de passe de baraka :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
 libflashrom1 libftdi1-2 libllvm13
```

2.4.) INSTALLATION DE SIP

SIP (Session Initiation Protocol) est un protocole de communication utilisé dans les réseaux IP pour établir, modifier et terminer des sessions de communication, telles que des appels téléphoniques, des conférences audio/vidéo et des sessions de messagerie instantanée.

```
baraka@baraka-VirtualBox:~$ sudo apt install sip-dev
[sudo] Mot de passe de baraka :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
```


2.7) DECLARATION DES UTILISATEUR

```
[general]
;
; Full name of a user
;
fullname = New User
;
; Starting point of allocation of extensions
;
userbase = 6000
;
; Create voicemail mailbox and use use macro-stdexten
;
hasvoicemail = yes
;
; Set voicemail mailbox 6000 password to 1234
;
vmsecret = 1234
;
; Create SIP Peer
;
hassip = yes
;
```

Sudo systemctl start asterisk

Ici vous pouvez également utiliser les commandes suivantes pour arrêter, redémarrer ou vérifier l'état d'Asterisk : `sudo systemctl start asterisk`.

`sudo systemctl stop asterisk`

`sudo systemctl restart asterisk`

`sudo systemctl status asterisk`

2.8) CONFIGURATION DE LINPHONE POUR UN COMPTE SIP

Pour configurer Linphone avec Asterisk sous Ubuntu en utilisant le terminal, vous pouvez suivre les étapes suivantes :

- Assurez-vous d'avoir Asterisk installé et configuré correctement sur votre serveur Ubuntu.
- Ouvrez un terminal sur votre système Ubuntu.
- Installez Linphone en exécutant la commande suivante :

`Sudo apt install linphone`

- Une fois l'installation terminée, lancez Linphone en exécutant la commande suivante :

`Linphone`

- Linphone s'ouvrira avec l'Assistant de configuration initial. Suivez les instructions à l'écran pour configurer votre compte SIP :
- Choisissez votre langue préférée.
- Acceptez les termes de la licence.
- Dans la section "Configurer un compte", sélectionnez "Configurer un compte SIP".
- Entrez les informations requises pour configurer votre compte SIP, y compris le nom d'utilisateur, le mot de passe, le domaine ou l'adresse IP du serveur Asterisk, ainsi que d'autres paramètres pertinents.
- Validez la configuration du compte SIP.

Une fois que vous avez configuré votre compte SIP, Linphone sera prêt à se connecter à votre serveur Asterisk. Vous pouvez maintenant utiliser Linphone pour passer et recevoir des appels via votre serveur Asterisk.

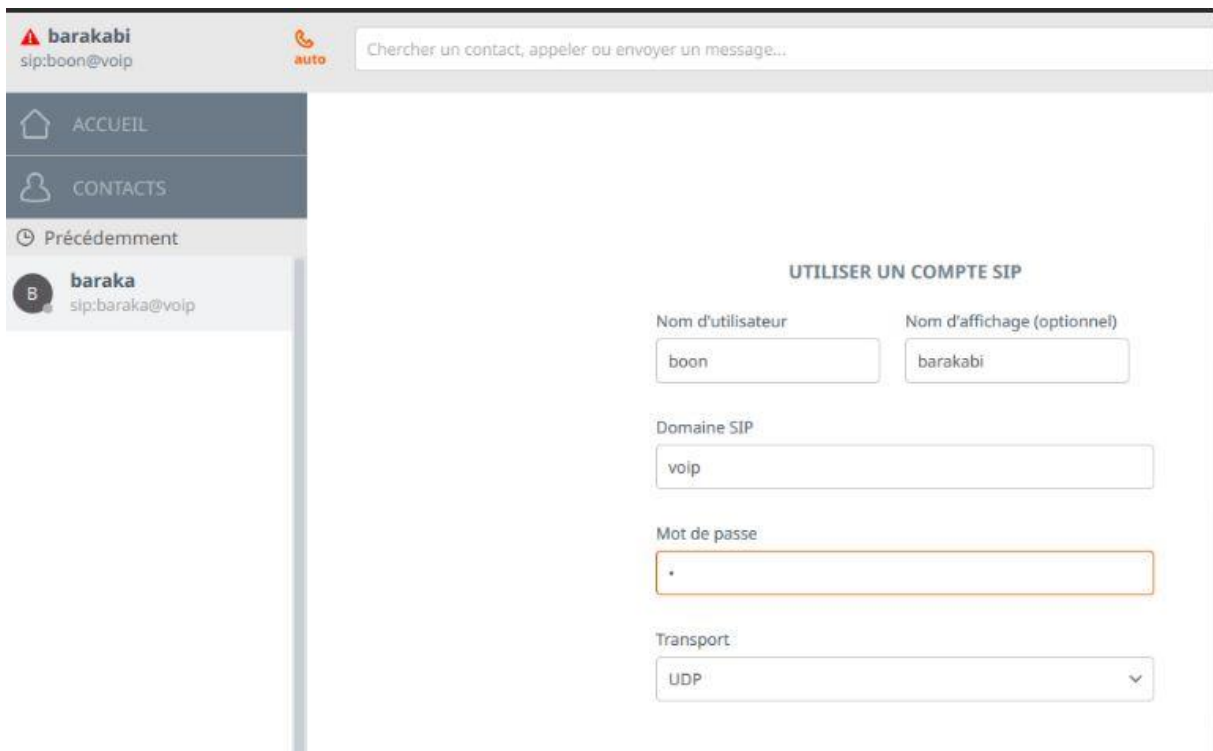
2.8.1) Démarrage de linphone

```

baraka@baraka-VirtualBox: ~
baraka@baraka-VirtualBox: ~$ linphone
Warning: Ignoring XDG_SESSION_TYPE=wayland on Gnome. Use QT_QPA_PLATFORM=wayland to run on Wayland anyway.
[07:27:03:193][0x55e1e3ef03d0][info]app/App.cpp:212: "Starting Linphone (bin: linphone)"
[07:27:03:193][0x55e1e3ef03d0][info]app/App.cpp:213: "Use locale: fr_FR"
[07:27:03:591][0x55e1e3ef03d0][info]app/AppController.cpp:90: Available fonts : ("aakar", "Abyssinica SIL", "Ani", "AnjaliOldLipi",
"Bitstream Charter", "C059 [UKWN]", "C059 [urw]", "Chandas", "Chilanka", "Courier 10 Pitch", "D050000L [urw]", "D050000L [URW ]",
"DejaVu Sans", "DejaVu Sans Mono", "DejaVu Serif", "Dhurjati", "Droid Sans Fallback", "Dyuthi", "FreeMono", "FreeSans", "FreeSerif",
"Gargi", "Garuda", "Gayathri", "Gayathri Thin", "Gidugu", "Gubbi", "Gurajada", "Jamrul", "KacstArt", "KacstBook", "KacstDecorative",
"KacstDigital", "KacstFarsi", "KacstLetter", "KacstNaskh", "KacstOffice", "KacstOne", "KacstPen", "KacstPoster", "KacstQurn", "Kacs
tScreen", "KacstTitle", "KacstTitleL", "Kalapi", "Kalinati", "Karumbi", "Keraleeyam", "Khmer OS", "Khmer OS System", "Kinnari", "Lak
kiReddy", "Laksaman", "Liberation Mono", "Liberation Sans", "Liberation Sans Narrow", "Liberation Serif", "Likhan", "LKLUG", "Lohit
Assamese", "Lohit Bengali", "Lohit Devanagari", "Lohit Gujarati", "Lohit Gurmukhi", "Lohit Kannada", "Lohit Malayalam", "Lohit Odia",
"Lohit Tamil", "Lohit Tamil Classical", "Lohit Telugu", "Lona", "Mallanna", "Mandali", "Manjari", "Manjari Thin", "Meera", "Mitra",
"Monospace", "nry_KacstQurn", "Mukti", "Nakula", "NATS", "Navilu", "Nimbus Mono PS [urw]", "Nimbus Mono PS [UKWN]", "Nimbus Roman
[urw]", "Nimbus Roman [UKWN]", "Nimbus Sans [urw]", "Nimbus Sans [URW ]", "Nimbus Sans [UKWN]", "Nimbus Sans Narrow [urw]", "Nimbus
Sans Narrow [UKWN]", "Norasi", "Noto Color Emoji", "Noto Mono", "Noto Sans", "Noto Sans CJK HK", "Noto Sans CJK JP", "Noto Sans CJK
KR", "Noto Sans CJK SC", "Noto Sans CJK TC", "Noto Sans Mono", "Noto Sans Mono CJK HK", "Noto Sans Mono CJK JP", "Noto Sans Mono CJK
KR", "Noto Sans Mono CJK SC", "Noto Sans Mono CJK TC", "Noto Sans UI", "Noto Serif CJK HK", "Noto Serif CJK JP", "Noto Serif CJK KR",
"Noto Serif CJK SC", "Noto Serif CJK TC", "NTR", "OpenSymbol", "oriUnl", "P052 [UKWN]", "P052 [urw]", "Padauk", "Padauk Book", "
padmaa", "padmaa-Bold.1.1", "Pagul", "Paddana", "Phetsarath OT", "Ponnala", "Pothana2000", "Potti Sreeramulu", "Purisa", "Rachana",
"RaghuMalayalamSans", "Ramabhadra", "Ramaraja", "Rasa", "Rasa Light", "Rasa Medium", "Rasa SemiBold", "RaviPrakash", "Rekha", "Saab",
"Sahadeva", "Samanata", "Sanyak Devanagari", "Sanyak Gujarati", "Sanyak Malayalam", "Sanyak Tamil", "Sans Serif", "Sarat", "Sawasd
ee", "Serif", "Sree Krushnadevaraya", "Standard Symbols PS [URW ]", "Standard Symbols PS [urw]", "Suranna", "Suravaram", "Suruna",
Syanala Ramana", "TenaliRanakrishna", "Tibetan Machine Uni", "Timmana", "Tlwg Mono", "Tlwg Typewriter", "Tlwg Typist", "Tlwg Typo",
"Ubuntu", "Ubuntu Condensed", "Ubuntu Light", "Ubuntu Mono", "Ubuntu Thin", "Umpush", "Uroob", "URW Bookman [urw]", "URW Bookman [UK
WN]", "URW Gothic [UKWN]", "URW Gothic [urw]", "Venana2000", "Waree", "Yrsa", "Yrsa Light", "Yrsa Medium", "Yrsa SemiBold", "Z003 [U
rw]", "Z003 [UKWN]")
[07:27:03:592][0x55e1e3ef03d0][info]:0: "Running app..."
[07:27:03:930][0x55e1e3ef03d0][info]app/App.cpp:316: "Activated selectors: ("custom", "fr_FR", "unix", "linux", "ubuntu")"
[07:27:03:975][0x55e1e3ef03d0][info]app/App.cpp:507: "Registering types..."
[07:27:04:013][0x55e1e3ef03d0][info]app/App.cpp:545: "Registering shared types..."
[07:27:04:013][0x55e1e3ef03d0][info]app/App.cpp:557: "Registering tool types..."
[07:27:04:013][0x55e1e3ef03d0][info]app/App.cpp:566: "Registering shared tool types..."
[07:27:06:483][0x55e1e3ef03d0][info]app/App.cpp:340: "Loading main view..."

```

2.8.2. Création d'un compte sip



barakabi
sip:boon@voip

Chercher un contact, appeler ou envoyer un message...

ACCUEIL

CONTACTS

Précédemment

baraka
sip:baraka@voip

UTILISER UN COMPTE SIP

Nom d'utilisateur: boon

Nom d'affichage (optionnel): barakabi

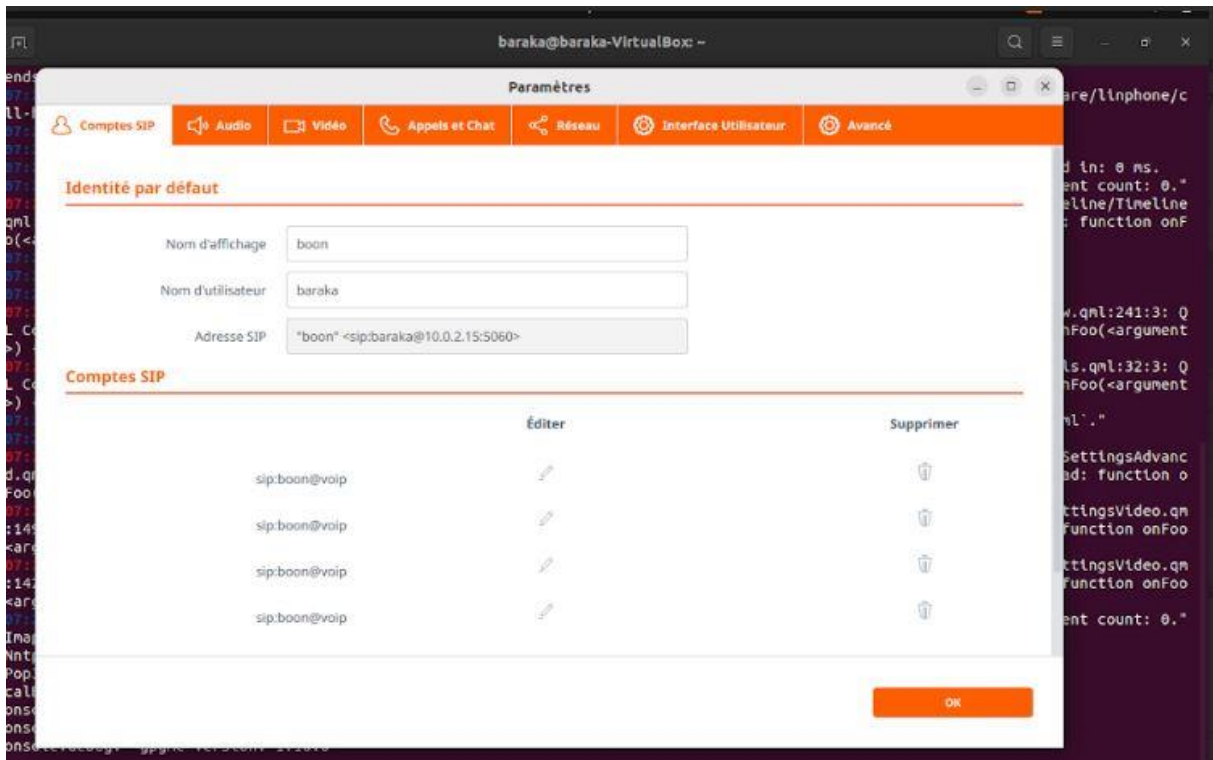
Domaine SIP: voip

Mot de passe: *

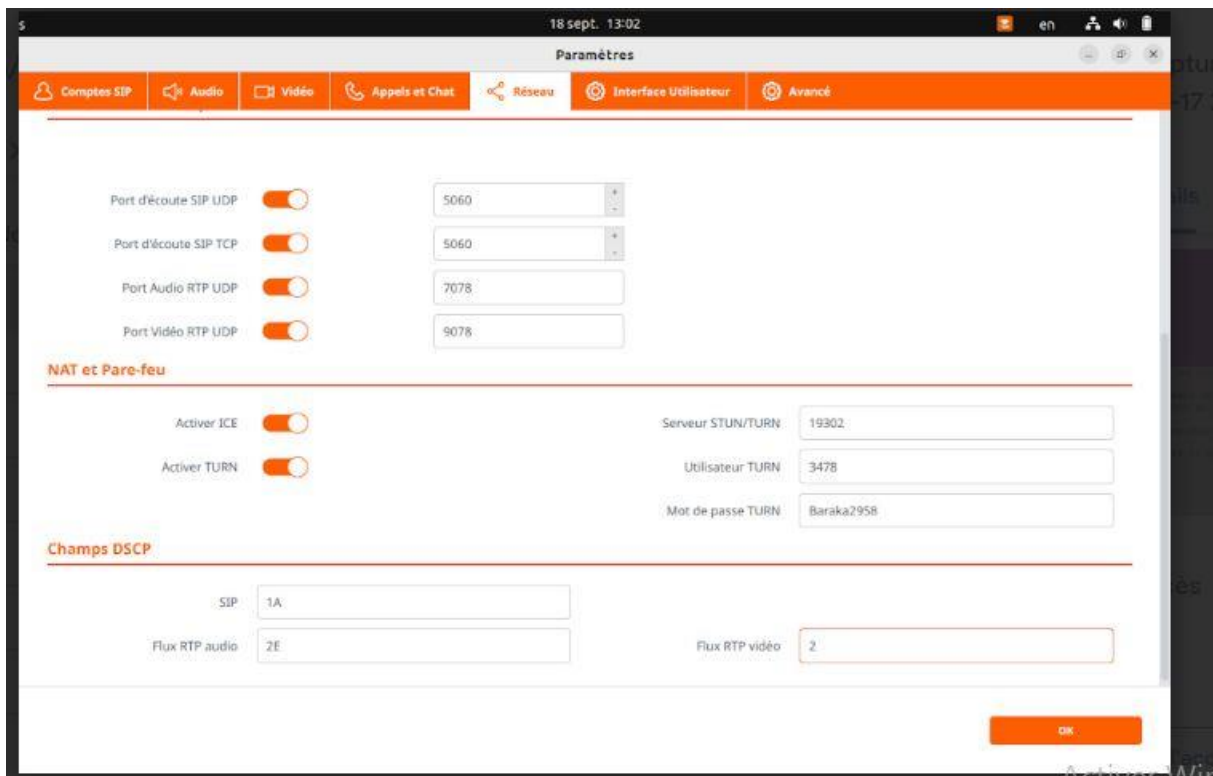
Transport: UDP

Le message qui s'affiche lors de la configuration

2.8.3. Démarrage d'appel



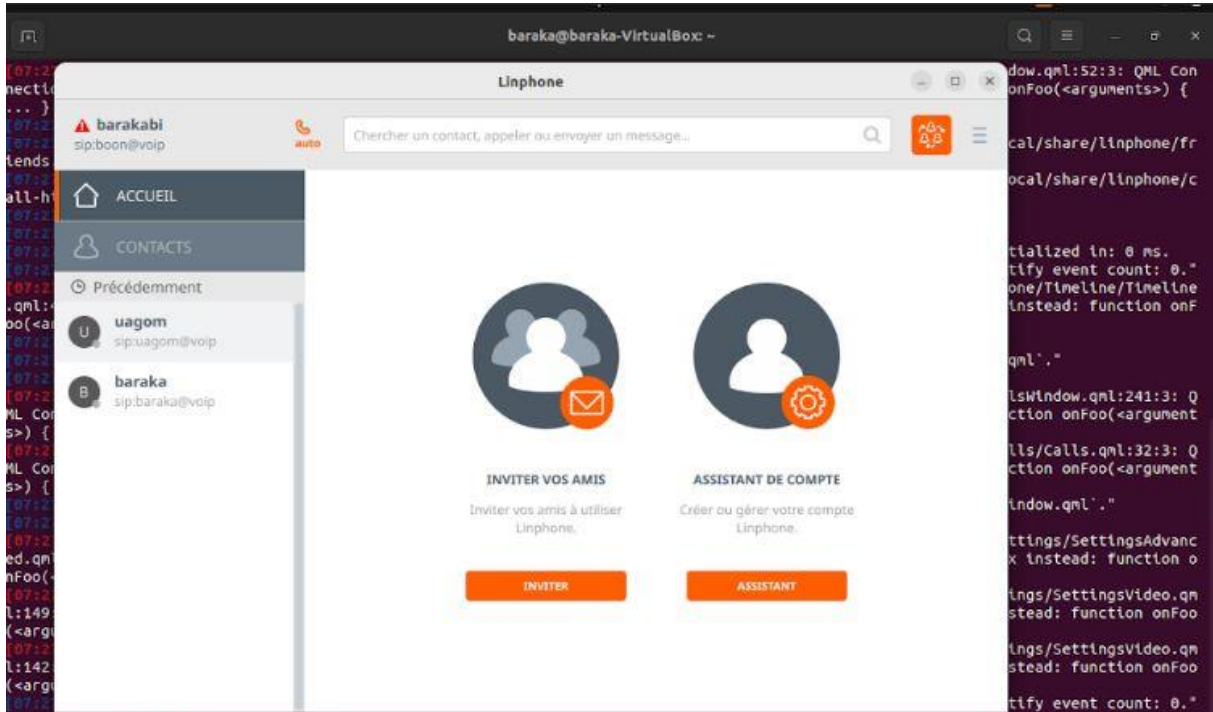
2.8.4. Le numéro qui s'affiche lors de la configuration



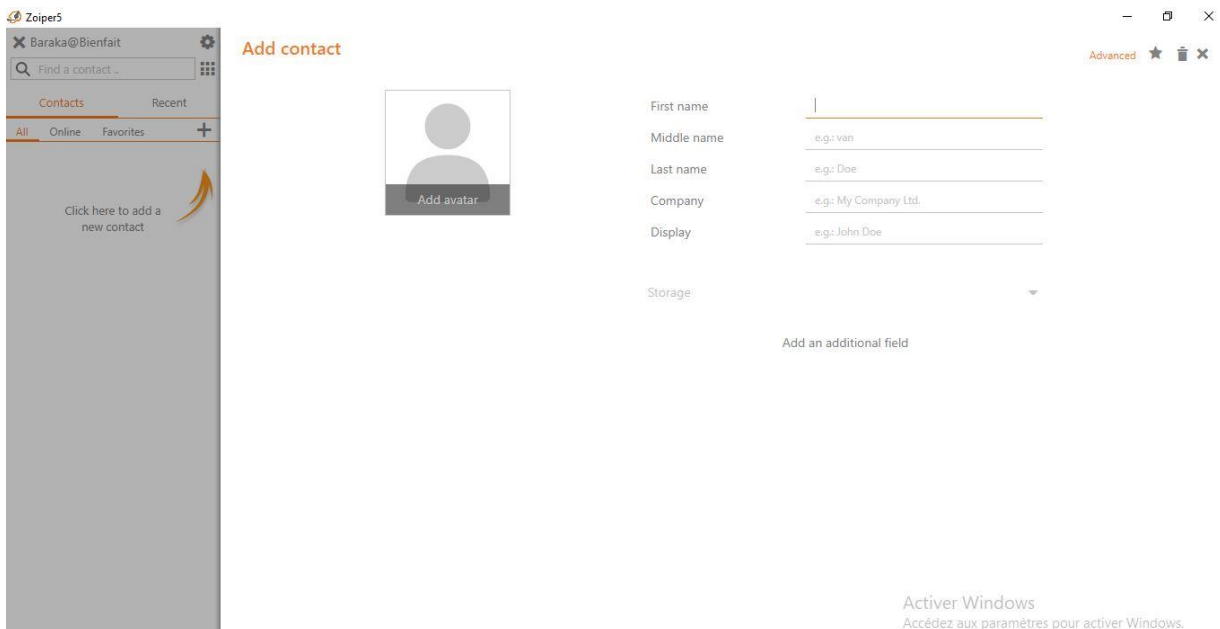
2.8.5) Cryptage de donnée l'ors de démarrage de l'appel

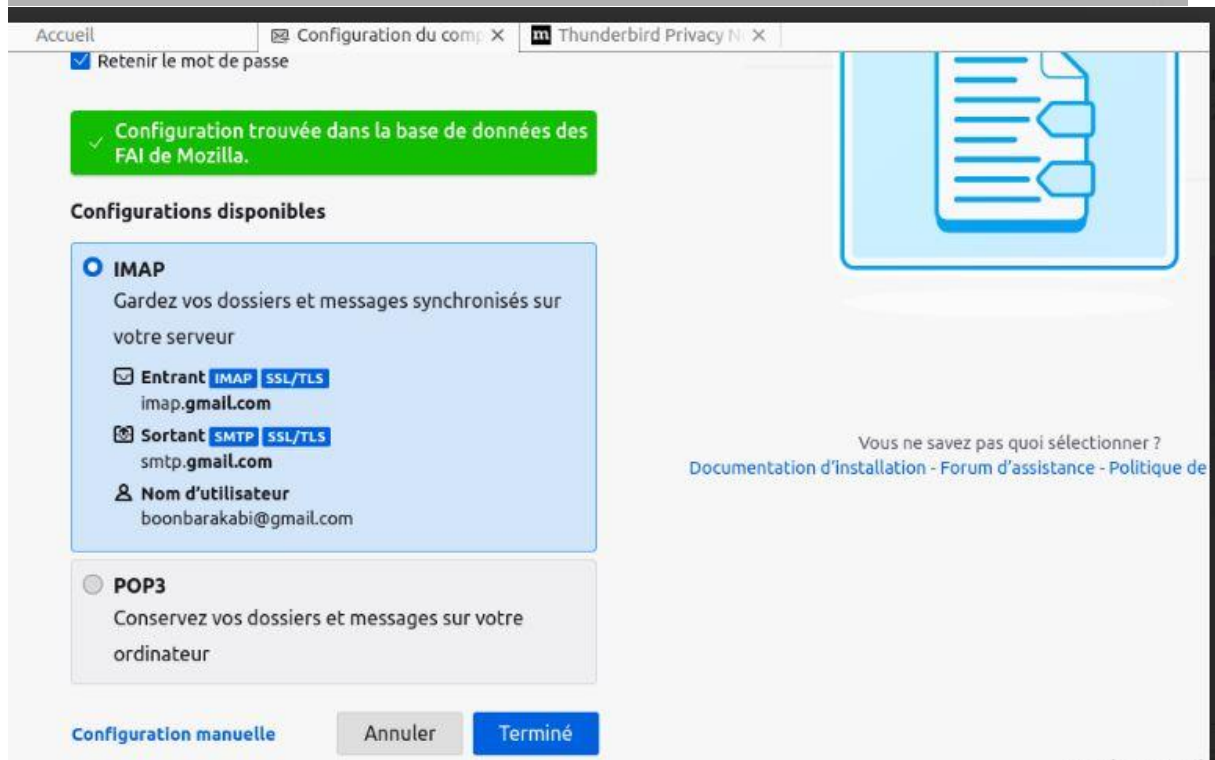
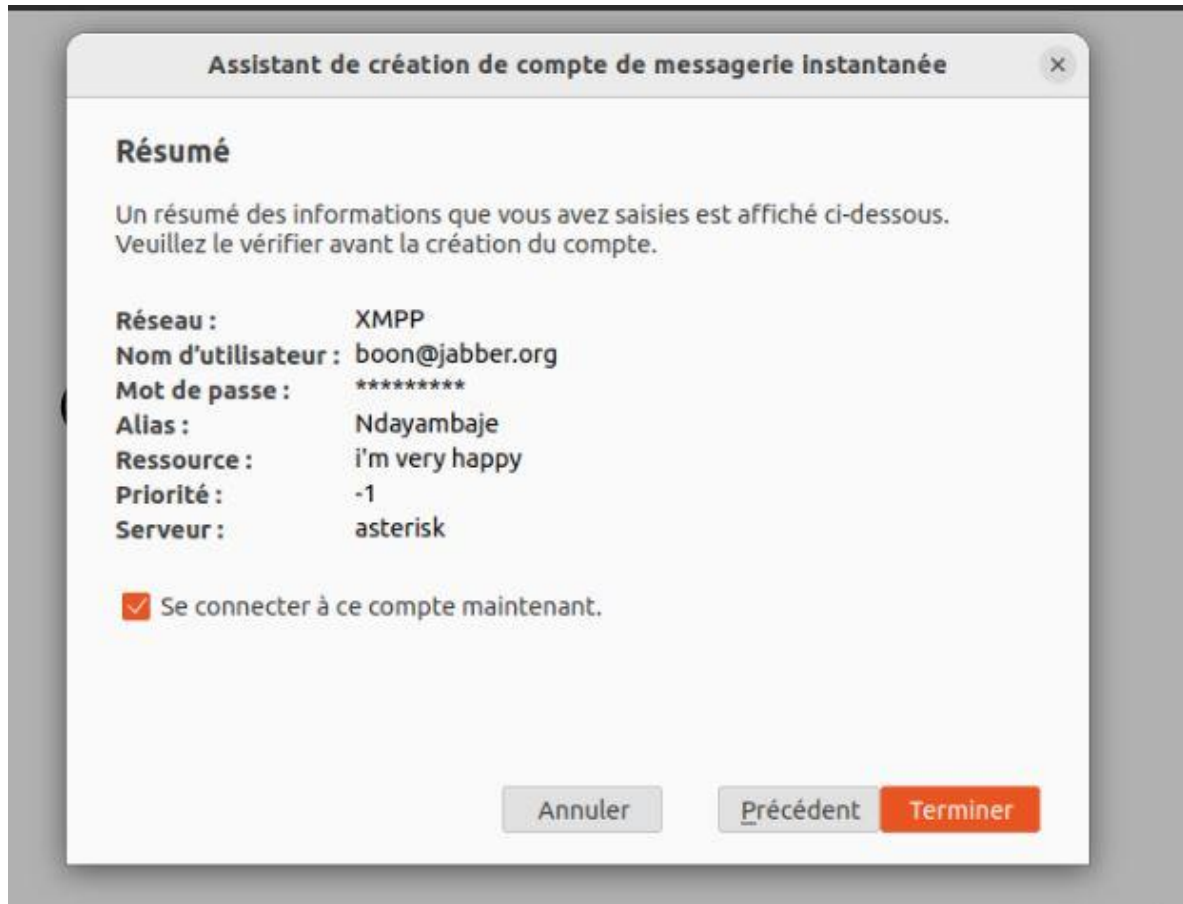
```
no "reens.mkv"
[4:889][0x55e1e3ef03d0][Info]app/App.cpp:791: "Update nat policy."
[7:828][0x55e1e3ef03d0][Info]components/core/event-count-notifier/AbstractEventCountNotifier.cpp:71: "Notify event count: 0."
```

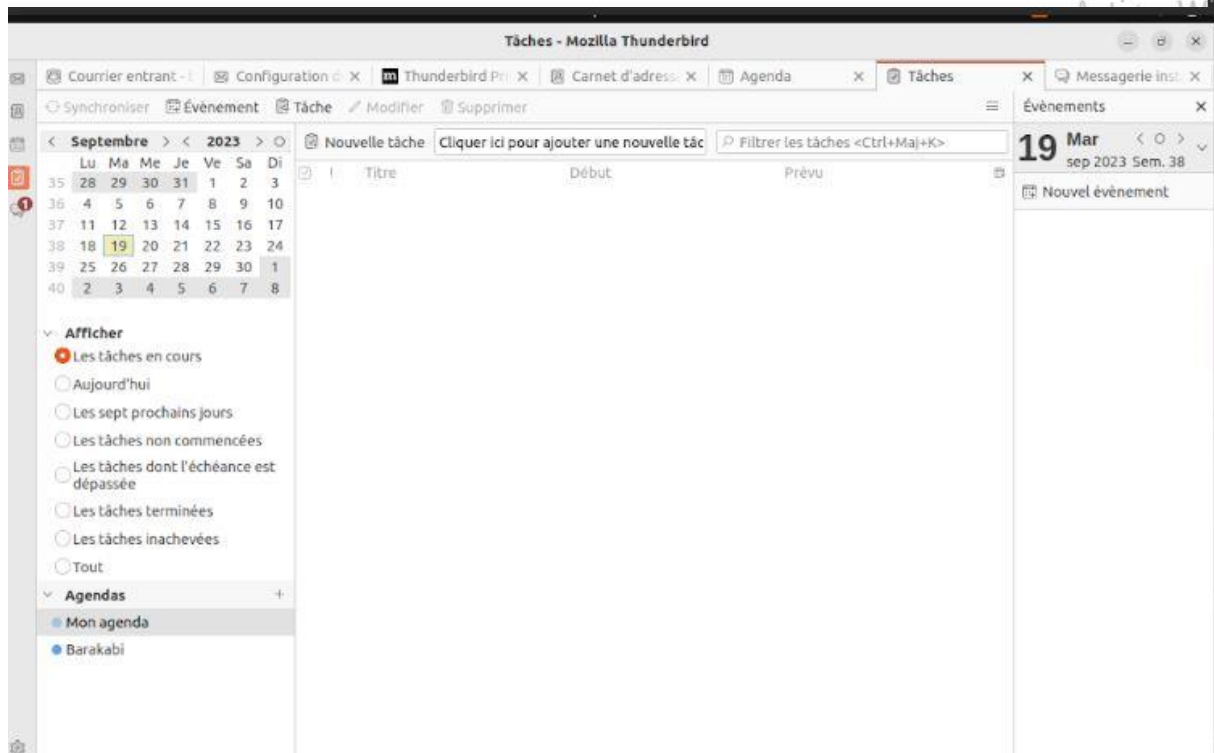
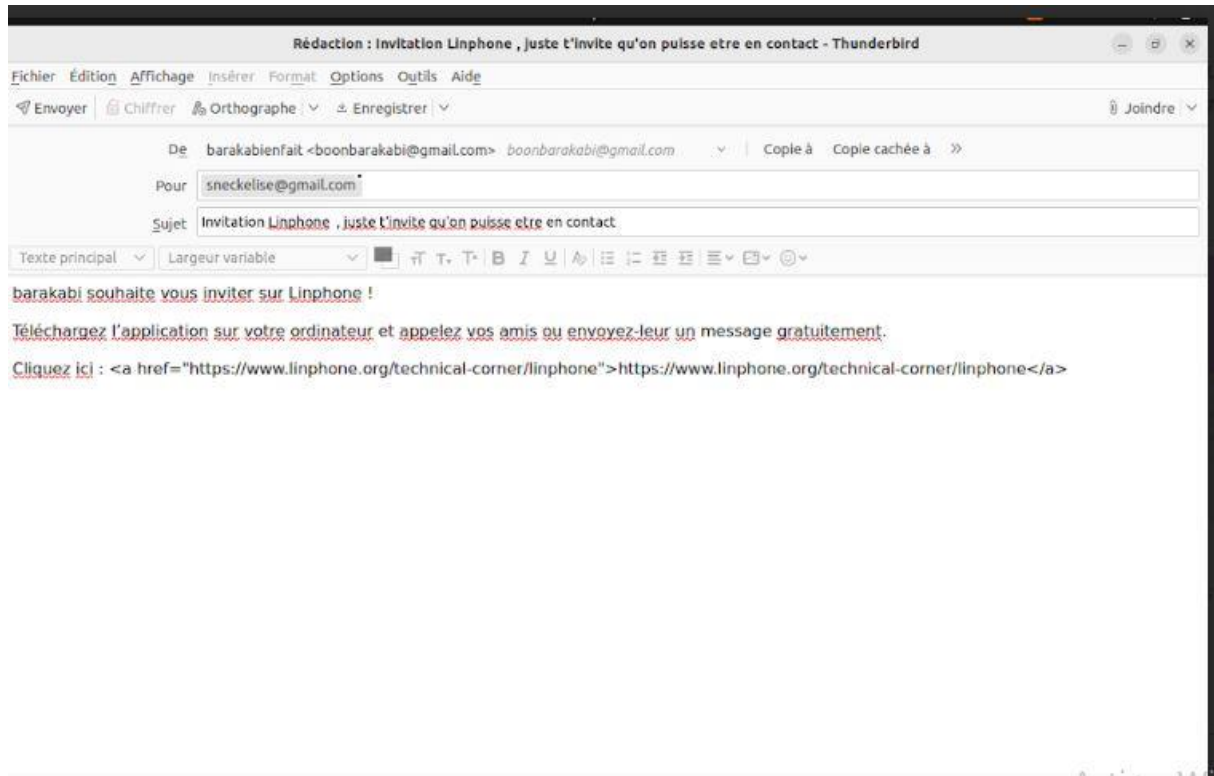
Invite un ami d'utiliser linphone et faire de vidéos conférence

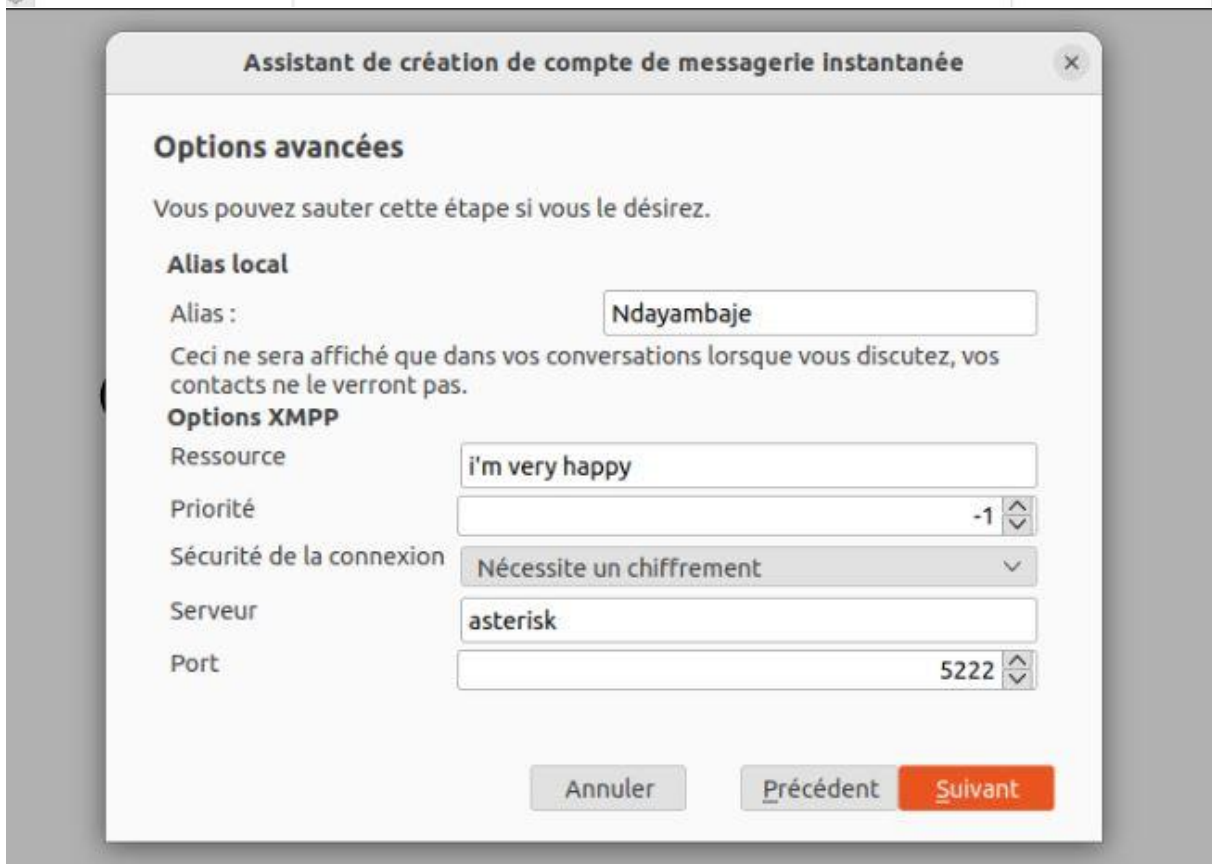
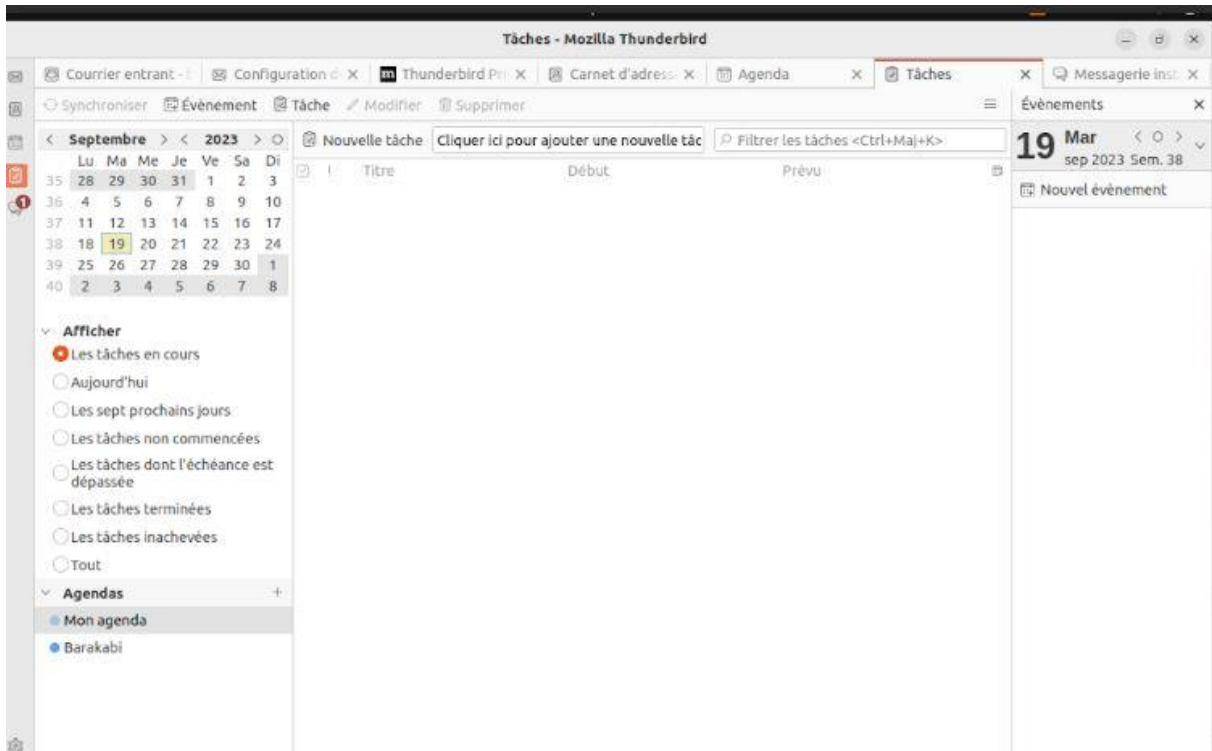


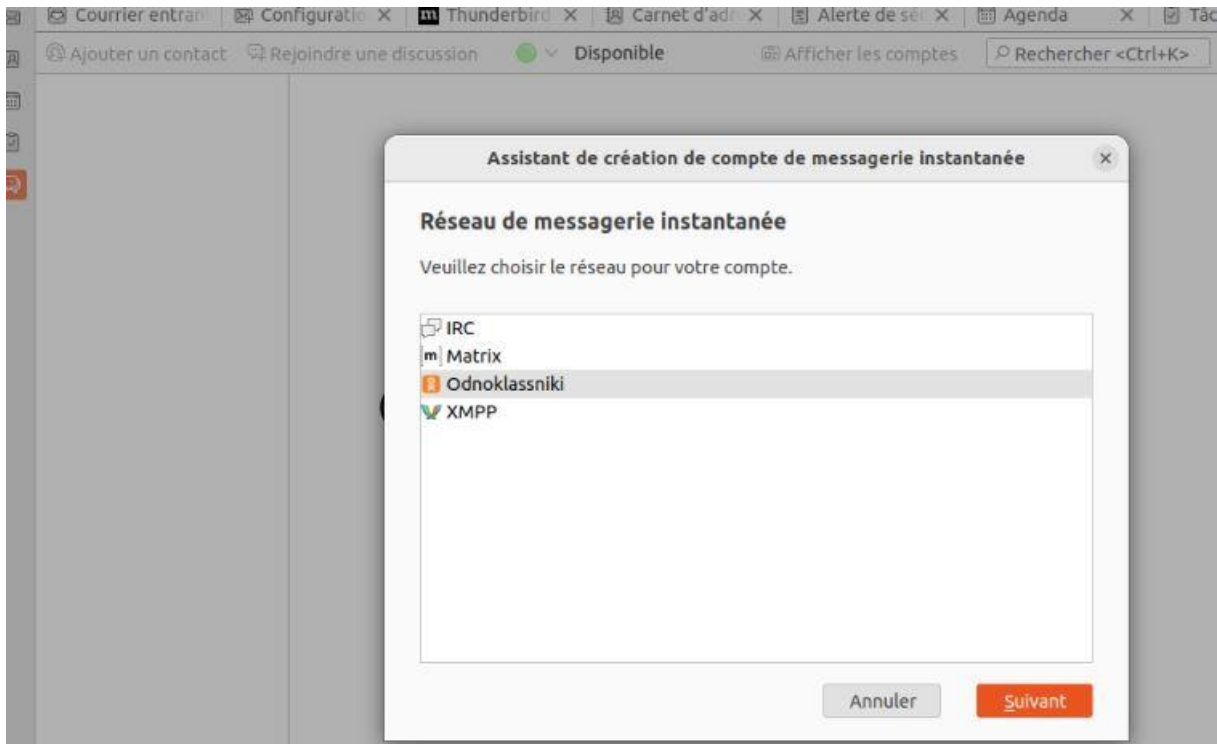
Ajouter un contact de sip











IV.4. RECOMMANDATIONS ET ANALYSES D'IMPACTS

La documentation officielle d'Asterisk : Asterisk est une plateforme VoIP open source populaire. Leur documentation officielle fournit des informations approfondies sur la mise en place de la sécurité dans un environnement VoIP. Vous pouvez consulter leur site web à l'adresse suivante : <https://www.asterisk.org/documentation/>.

RFC (Request for Comments) de l'IETF : L'IETF (Internet Engineering Task Force) publie des RFC qui définissent les normes et les bonnes pratiques pour de nombreux protocoles VoIP, tels que SIP (Session Initiation Protocol) et SRTP (Secure Real-time Transport Protocol). Vous pouvez accéder aux RFC sur le site officiel de l'IETF : <https://www.ietf.org/rfc.html>.

Livres spécialisés : Il existe plusieurs livres qui traitent de la sécurité dans les systèmes VoIP. Certains de ces livres sont largement reconnus dans le domaine et offrent une couverture approfondie des aspects de sécurité spécifiques à la VoIP. Par exemple, "VoIP Hacks" de Ted Wallingford et "Securing VoIP Networks" de Peter Thermos et Ari Takanen sont deux livres populaires dans ce domaine.

Blogs et sites web spécialisés : Il existe de nombreux blogs et sites web spécialisés dans la VoIP et la sécurité des communications. Certains d'entre eux publient régulièrement des articles et des analyses approfondies sur les dernières tendances et les meilleures pratiques en

matière de sécurité VoIP. Quelques exemples de sites web populaires comprennent VoIP-Info (<https://www.voip-info.org/>) et NoJitter (<https://www.nojitter.com/>).

Revue et publications académiques : Les revues et les publications académiques dans le domaine des communications et de la sécurité des réseaux peuvent également constituer une source fiable d'informations sur la VoIP sécurisée. Des revues telles que IEEE Communications Magazine et ACM Transactions on MultiMedia Computing, Communications, and Applications publient régulièrement des articles de recherche dans ce domaine.

ANNEXES

Sudo apt upgrade

Pour Ubuntu/Debian :

```
sudo apt-get update && sudo apt-get install -y build-essential libncurses5-dev libxml2-dev libssl-dev  
libsqlite3-dev libedit-dev uuid-dev
```

```
sudo nano /etc/asterisk/sip.conf
```

```
sudo nano /etc/asterisk/extensions.conf
```

```
[BARAKA]
```

```
type=friend
```

```
host=dynamic
```

```
secret=Baraka@2024
```

```
context=BBienfait
```

Nom du contexte

```
[BBienfait]
```

```
exten => 100,1,Dial(SIP/mon_compte,20)
```

```
exten => 100,n,Hangup()
```

pour redémarrer le service Asterisk

```
sudo systemctl restart asterisk
```


BIBLIOGRAPHIE

al, K. e. (2019). *L'impact de la sensibilisation des utilisateur sur la securité de la VOIP*.

al, Z. e. (2016). *Efficacité de prevention des intrusions*.

Bera. (2018). *Efficacité protocole de cryptage pour protéger les flux de voix contre l'ecoute clandestine*.

Fayoumi. (2020). *Pratique de securite pour la VOIP dans les entreprises*.

Johson, M. (2019). *Understanding Concepts: A Comprehensive Review*".

Jones, L. (2021). *"Conceptualizing Concepts: A Framework for Effective Planning"*.
paris,france, 5 rue Gaston Gallimard,75007: Éditions Gallimard.

<https://www.ietf.org/rfc.html>.

TABLE DE MATIERES

DECLARATION DE L'ETUDIANT	i
DECLARATION DU DIRECTEUR	ii
EPIGRAPHE	iii
DEDICACE	iv
REMERCIEMENTS.....	vi
SIGLES ET ABREVIATIONS	vii
LISTES DE TABLEAUX.....	viii
LISTES DES FIGURES	ix
RESUMÉ	x
ABSTRACT	xi
CHAP.I INTRODUCTION	1
I.1. CONTEXTE DE L'ÉTUDE	1
I.2. PROBLÉMATIQUE	2
I.3. OBJECTIF DU TRAVAIL.....	3
I.3.1. OBJECTIF GENERAL	3
I.3.2. OBJECTIFS SPÉCIFIQUES	3
I.4. MÉTHODES ET TECHNIQUES.....	3
I.5. CHOIX ET INTERET DU SUJET	4
I.6. DELIMITATION DU TRAVAIL	4
I.7. SUBDIVISION DU TRAVAIL	4
CHAP II. REVUE DE LA LITTERATURE.....	5
II.1 INTRODUCTION	5
II.2 REVUE DE LA LITTERATURE EMPIRIQUE.....	5
II.3. REVUE DE LA LITTERATURE THEORIQUES (Johson, 2019)	6
II.4 Revue de la littérature conceptuelle.....	7
II.4.1. La voip	7
II.4.2 Fonctionnement et Rôles	7
II.4.3. ARCHITECTURE.....	9
II.4.4. PROTOCOLE SIP.....	9
II.4.4.5. FORMAT DU PAQUET SRTP	14
II.5. PRESENTATION DU MILIEU D'ETUDE	18
II.5.1. Situation géographique	18

II.5.3. Mission	19
II.5.4. Vision	19
II.5.5. Valeur	19
II.5.6. Objectifs	19
II.5.7. Organisation et fonctionnement	20
II.5.8. DIAGNOSTIC DE L'EXISTANT	24
CHAP III : PLANNING PREVISIONNEL DU PROJET	25
III.1. DEFINITIONS DE CONCEPTS.....	25
III.1.1 Projet.....	25
III.3 REALISATION DU PROJET	25
III.4 DETERMINATION DES OBJECTIFS.....	26
III.5 METHODE D'ORDONNANCEMENT	26
III.6. DETERMINATION DE TACHES	26
III.7. ELABORATION DU GRAPHET PERT	29
III.8) DETERMINATION DE LA DATE AU PLUS TOT, DATE AU PLUS TARD, MARGE LIBRE ET MARGE TOTAL	30
III.8.1. Date au plus tôt.....	30
III.8.2 Date au plus tard	30
III.8.3. Calculs de marge.....	31
III.8.4. La marge libre(ML).....	31
III.8.5. La marge totale	32
III.8.6. DETERMINATION DU CHEMIN CRITIQUE	32
III.5 CALENDRIER DU PROJET ET DIAGRAMME DE GANT	33
CHAP.IV PRESENTATION DES RESULTATS.....	34
IV.1 ENVIRONNEMENT MATÉRIELS ET LOGICIEL.....	34
IV.1.1. Environnement matériel :	34
1. Serveur ou ordinateur de traitement	34
2. Téléphones IP	34
3. Passerelles VoIP	34
IV.2. Environnement logiciel :	34
IV.3. Présentation des interfaces graphiques.....	36
IV.4. RECOMMANDATIONS ET ANALYSES D'IMPACTS	49
BIBLIOGRAPHIE	53