INTRODUCTION GENERALE

Avant d'entrer dans le vif du sujet, il est important de reconnaître deux technologies fondamentales qui sont arrivées les premières : le téléphone et l'Internet. Le premier appel téléphonique a été passé le 10 mars 1876 par l'inventeur du gadget, Alexander Graham Bell. Avance rapide de 100 ans jusqu'en 1976, et le coût associé à un appel longue distance était encore une denrée extrêmement coûteuse. En effet, les systèmes téléphoniques traditionnels passaient par des réseaux analogiques coûteux. C'est le développement de l'internet qui a véritablement révolutionné le champ des communications. Les experts de l'époque ont prédit avec précision comment les ordinateurs et l'internet allaient, plus que tous les autres, ouvrir la voie à une capacité d'intégration mondiale et à la diffusion massive de l'information.
L'idée d'utiliser votre ordinateur pour passer des appels vocaux a vu le jour au début des années 1990, lorsque des amateurs ont commencé à bricoler pour que les utilisateurs de PC puissent éviter les appels téléphoniques longue distance coûteux. Dans les premières années de la technologie VoIP, les deux interlocuteurs devaient disposer d'un ordinateur équipé du même logiciel, d'une carte son et d'un microphone. Ces applications VoIP étaient également criblées de divers problèmes, notamment une mauvaise qualité audio et des problèmes de connectivité. Ce moment a néanmoins ouvert les portes de la promesse, les petits acteurs et les grandes marques recherchant et investissant sur les moyens d'utiliser la technologie VoIP pour améliorer les communications d'entreprise. La percée majeure dans le monde de la VoIP a commencé en 1995, lorsque les principaux fabricants de matériel informatique ont commencé à développer des fonctionnalités qui devaient auparavant être prises en charge par le processeur d'un ordinateur. L'un des principaux exemples est l'acte de « commutation », qui consiste à transformer un paquet de données vocales en quelque chose qui peut être lu par le réseau téléphonique et vice versa. Une fois que cette fonction a pu être reproduite à l'aide de dispositifs externes, le matériel de VoIP est devenu moins dépendant de l'ordinateur et plus abordable. Cela a ouvert la porte aux grandes entreprises qui ont pu mettre en œuvre la VoIP sur leurs réseaux IP internes.

L'arrivée de la VOIP a été ressenti dans le monde de la communication comme un profond changement de la même ampleur que le remplacement du télégraphe par le téléphone. La VOIP est basée sur la commutation de paquet avec l'utilisation du réseau IP. Les appels VOIP sont des appels téléphoniques qui permettent la transmission des communications vocales via des réseaux au protocole IP. Le support utilisé peut-être le réseau public internet ou un réseau privé. La téléphonie IP permet d'utiliser la puissance du protocole internet pour

accéder au réseau téléphonique ; elle permet une intégration transparente des appels vocaux, des appels vidéo, des vidéos conférences et même des sms. La téléphonie IP offre de nombreux avantage par rapport aux appels traditionnel tels que les couts réduits, une meilleure qualité audio dans des conditions optimales, une flexibilité accrue et des fonctionnalités avancées.

1. PROBLEMATIQUE

De nos jours, de nombreux services utilisent la téléphonie IP, que ce soit via des applications sur des smartphone, des logiciels, sur des ordinateurs ou sur des téléphones IP dédiés.

Dans ce contexte, la mise place d'un système de gestion des appels IP sécurisé est essentielle pour garantir la confidentialité des communications et la protection des données des utilisateurs.

Ce système peut inclure des mesures telles que le cryptage des appels, la mise en place de pare-feu, la surveillance du trafic réseau, l'authentification des utilisateurs et d'autres protocoles de sécurité pour prévenir les intrusions.

Cependant la sécurité des appels IP est un sujet crucial, car les appels peuvent être à l'interception des données sensible ou des attaques malveillante.

Après plusieurs constants faits lors de notre visite au sein de NAS différents nous avons remarqué que plusieurs besoins se font sentir en vue de facilité la meilleure communication au sein de l'entreprise.

Ainsi, au regard de tout ce que précède, dans le cadre du travail, nous tenteront de répondre aux questions suivantes :

- Comment facilité les agents de NAS d'effectuer une communication vocale entre eux vie un réseau local
- Quel mécanisme mettre en place pour y parvenir ?
- Quel logiciel choisir pour leur réseau ?

2. HYPHOTHESE

En guise de réponse à toutes ces préoccupations, nous partons des hypothèses ci-après :

- Les défis auxquels doit faire face l'entreprise sur le plan communicationnel

Facilité aux utilisateurs d'échanger les messages vocaux entre eux via le réseau Lan.

- Facilité aux agents de centraliser les communications vocales sur le réseau local.
- Eviter la mauvaise interprétation des ordres de travail.

3. CHOIX ET INTERET DU SUJET

La réalisation de ce travail sera une documentation de plus dans le domaine de réseau informatique et de télécommunication sur base de laquelle des futurs chercheurs pourraient se référer pour réaliser une œuvre scientifique.

3.1. METHODES ET TECHNIQUES

3.1.1. METHODES

La méthode est une opération intellectuelle de traitement de données relatives à une réalité objectif bien précis

A. Méthodes expérimentales

L'expérimentation est l'étude des faits dans des conditions établies par le chercheur. Elle a pour but la vérification de l'existence d'une relation entre les faits (ou les variables). Cette découverte de la relation est le fruit de l'observation.

Par cette méthode, nous avons fait une étude des conditions de fonctionnements du système par une vérification des activités existantes afin de tester notre solution.

B. Méthodes Top-Down network-design

La méthode top-down est une méthodologie qui commence au plus haut niveau d'un concept et se dirige vers le plus bas niveau. Cette méthode nous a permis de représenter l'architecture du réseau existant afin de ressortir les vrais problèmes du système. L'approche a été effectuée du général au particulier.

3.1.2. TECHNIQUES

La technique est un moyen ou un outil d'investigation scientifique que le chercheur utilise tout au long de son travail pour arriver à une interprétation facile de ses résultats.

a. Techniques documentaires

Cette technique nous a permis d'analyser et d'enregistrer les informations nécessaires à tr avers la lecture des documents qui cadrent avec l'objet d'études. Pour la réalisation de notre travail, nous avons consulté des livres, syllabus, travaux scientifiques, articles, sites internet parlant de la téléphonie IP.

b. Technique d’observation

Par cette technique, nous avons palpé la réalité du système en faisant une descente sur terrain et en y effectuant une observation systématique du déroulement de la communication sur le réseau local de l’entreprise.

4. Délimitation du sujet

Pour bien analyser, le thème de la recherche doit être délimité dans le temps et dans l'espace.

4.1. Délimitation dans le temps

Sur le plan temporel, la réalisation de ce travail est partie de l'analyse de l'ancien système de la SNEL jusque à l'implémentation de la solution, soit une période allant de Novembre 2015 au septembre 2016.

4.2. Délimitation dans l'espace

Sur le plan spatial, notre recherche s'est focalisée au réseau informatique de la Société Nationale d’Electricité en sigle SNEL, situé au numéro 119 de l'avenue Shangungu au Quartier Industrielle dans la Commune de Kampemba, Ville de Lubumbashi.

1. Subdivision du travail

Mise à part l'introduction et la conclusion générale, notre travail est subdivisé en 4 chapitres :

Le premier chapitre s'intitule « GENERALITE SUR LA TELEPHONIE IP » cette partie présentera l'introduction de la voix sur IP et ses éléments, la description et les explications de son architecture et ses protocoles, ainsi que l'énumération de ses points forts et faible de ce domaine.

Le deuxième chapitre se rapporte sur « VULNERABILITES DES RESEAUX VOIP ET MESURES DE SECURITE » Dans ce chapitre nous parlerons de la sécurité dans le système VOIP

Le troisième chapitre portera sur « CADRAGE DU PROJET ». Dans ce chapitre nous allons mettre l'accent sur l'aspect du cadrage du projet et faire une étude détaillée du projet.

Le quatrième chapitre intitulée « ETUDE DU SITE NAS » Ce chapitre nous parlerons de la présentation de l’entreprise, Mission et objectif, Emplacement

géographique, L'organigramme, fonctionnement et poste, Architecture de L'existant.

Le cinquième chapitre intitulé « DEPLOIEMENT DU SYSTEME » Dans ce chapitre, nous allons proposer le modèle de déploiement de la solution VoIP sécurise, au sein du réseau informatique de la NAS.

CHAPITRE I. GENERALITE SUR LA TELEPHONIE IP

I.0. INTRODUCTION [1]

Ces dernières années, une grande majorité des entreprises moderne l'utilise, son concept de base est l'utilisation du réseau informatique pour supporter les communications téléphoniques. La téléphonie IP est une technique qui permet de communiquer vocalement via le réseau internet. Contrairement au réseau téléphonique analogique filaires liés à un réseau téléphonique commuté (RTC) et à des centraux dédié, la téléphonie IP permet le transport de conversations téléphonique sur tout réseau, numérique ou analogique, acceptant le protocole TCP/IP (Ethernet, RNIS, PPP, etc.). La téléphonie IP ne se limite pas seulement à la création d'un réseau interne de téléphonie pour l'entreprise. Au contraire, elle offre une solution complète pour les besoins de communications des entreprises grâce à un système héberger chez un fournisseur VOIP de confiance. En effet, les entreprises ont la possibilité d'héberger leur système téléphonique chez lez operateurs spécialisé dans la téléphonie IP. La voix est ainsi transmise par le réseau internet au fournisseur qui l'achemine au destinateur

I.1. DEFINITIONS

Par définition, la téléphonie IP se base sur un principe de numérisation de la voix, via les protocoles internet.

Quelques définitions :

A. La téléphonie IP est donc un usage permettant d'échanger des informations, dont les appels vocaux, via un réseau de données, public (internet) ou privé (réseau LAN).
B. La téléphonie IP est une technologie qui permet d'acheminer, grâce au protocole IP, des paquets de données correspondant à des échantillons de voix numérisée
C. La téléphonie IP désigne la technique d'acheminement des appels téléphoniques sur un réseau de données IP
D. La téléphonie IP constitue un protocole de communication permettant d'utiliser un réseau de données, comme Internet par exemple, pour y passer des appels, mais aussi d'autre types d'échanges (texte, image, vidéo etc.).

[1] 11 DA CUNHA José, VoIP et Asterisk/Trixbox, métrise en systèmes distribués et réseaux, Université de Franche Comté, 2007-2008.

E. La téléphonie IP définit l'utilisation de liens Internet pour acheminer des appels téléphoniques d'une personne à une autre. Un appel téléphonique de type IP diffère de la téléphonie conventionnelle (RTC) dans l'encodage de la voix.
F. La téléphonie IP consiste à mettre en place des services téléphoniques sur un réseau IP en utilisant la technique de la voix sur IP

I.2. ARCHITECTURE DE LA TELEPHINIE IP

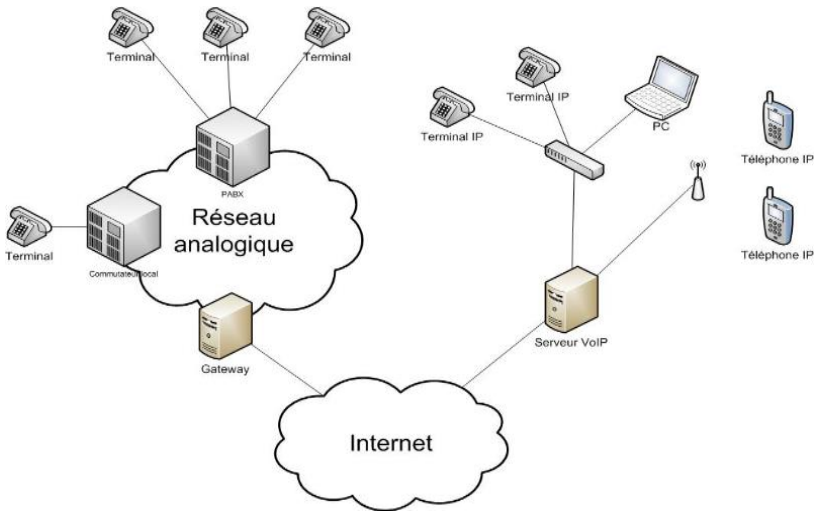


Figure 1 Architecture de la téléphonie IP

La VoIP étant est une technologie de communication, elle n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les protocoles le plus utilisés sont H.323, SIP et MGCP/MEGACO. Il existe plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP. Certains placent l'intelligence dans le réseau alors que d'autres préfèrent une approche égale à égale avec l'intelligence répartie à chaque périphérie. Chacune ayant ses avantages et ses inconvénients. Elle comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour garantir une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles contrôleur de commutation, appelées Gatekeeper. Dans une architecture VoIP, on trouve les éléments communs suivants :

Le routeur : permet d'aiguiller les données et le routage des paquets entre deux réseaux. Certains routeurs permettent de simuler un Gatekeeper grâce à l'ajout de cartes spécialisées supportant les protocoles VoIP.

La passerelle : permet d'interfacer le réseau commuté et le réseau IP.

Le PABX : est le commutateur du réseau téléphonique classique. Il permet d'établir le lien entre la passerelle ou le routeur, et le réseau téléphonique commuté (RTC). Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.

Les Terminaux : sont généralement de type logiciel (software phone) ou matériel (hardphone). Le softphone est installé dans le PC de l'utilisateur, l'interface audio peut être un microphone et des haut-parleurs branchés sur la carte son, même si un casque est recommandé. Pour une meilleure clarté, un téléphone USB ou Bluetooth peut aussi être utilisé.

Le hardphone est un téléphone IP qui utilise la technologie Voix sur IP pour permettre des appels téléphoniques sur un réseau IP, tel que l'Internet au lieu de l'ordinaire système PSTN. Les appels peuvent parcourir par le réseau internet comme par un réseau privé. Un terminal utilise des protocoles comme le SIP (Session Initiation Protocol) ou l'un des protocoles propriétaires tel que celui utilisé par Skype.

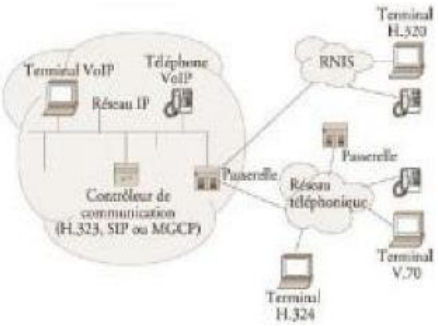


Figure 2 Architecture d'un réseau VOIP

I.3. PRINCIPE DE FONCTIONNEMENT

Le principe de la voix sur IP est basé sur la numérisation de la voix, c'est-à-dire le passage d'un signal analogique à un signal numérique. Celui-ci est compressé en fonction des codecs choisis, cette compression a comme but de réduire la quantité d'information qui est transmise sur le réseau (comme par exemple la suppression des silences). Le signal obtenu est découpé en paquets, à chaque paquet on ajoute les entêtes propres au réseau (IP, UDP, RTP.) et pour finir, il est envoyé sur le réseau.

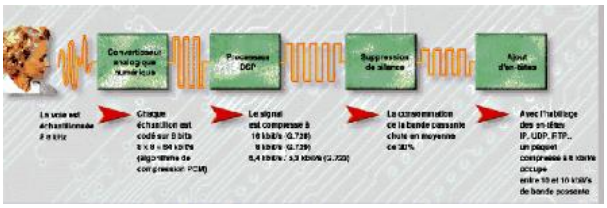


Figure 3 Passage du signal analogique au signal numérique

A l'arrivée, les paquets transmis sont réassemblés en supprimant d'abord les entêtes. Le signal de données ainsi obtenu est décompressé puis converti en signal analogique afin que l'utilisateur puisse écouter le message d'origine.

I.4. LES DIFFERENTS PROTOCOLES

Un protocole est un ensemble de spécifications décrivant les conventions et les règles à suivre dans un échange de données

I.4.1. PROTOCOLE DE SIGNALISATION

Un protocole est un ensemble de spécifications décrivant les conventions et les règles à suivre dans un échange de données. Jusqu'à présent, il existe trois standard ou protocoles qui permettent la mise en place d'un service VoIP. Le plus connu est le standard H.323, ensuite, plus ancien le MGCP (Media Gateway Control Protocol) et le plus récent SIP. Notre étude sera basée sur les protocoles les plus utilisés : H323 et SIP que nous allons développer dans cette section.

I.4.1.1. LE PROTOCOLE H.323

Le standard H.323 fournit, depuis son approbation en 1996, un cadre pour les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (International Télécommunications Union) pour les réseaux qui ne garantissent pas une qualité de service (QoS), tels qu'IPX sur Ethernet, Fast Ethernet et Token Ring. Il est présent dans plus de 30 produits et il concerne le contrôle des appels, la gestion multimédia, la gestion de la bande passante pour les conférences point-à-point et multipoints. H.323 traite également de l'interfaçage entre le LAN et les autres réseaux. Le protocole H.323 fait partie de la série H.32x qui traite de la vidéoconférence au travers différents réseaux. Il inclut H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data Network) et PSTN (Public Switcher Téléphone Network). Plus qu'un protocole, 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. Les messages de signalisation sont ceux envoyés pour demander la mise en relation de deux clients, qui indique que la ligne est occupée ou que le téléphone sonne, etc. En H.323, la signalisation s'appuie sur le protocole RAS pour l'enregistrement et l'authentification, le protocole Q.931 pour l'initialisation

et le contrôle d'appel. La négociation est utilisée pour se mettre d'accord sur la façon de coder les informations à échanger. Il est important que les téléphones (ou systèmes) utilisent un langage commun s'ils veulent se comprendre. Il s'agit du codec le moins gourmand en bande passante ou de celui qui offre la meilleure qualité. Il serait aussi préférable d'avoir plusieurs alternatives de langages. Le protocole utilisé pour la négociation de codec est le H.245. Le transport de l'information s'appuie sur le protocole RTP qui transporte la voix, la vidéo ou les données numérisées par les codecs. Les messages RTCP peuvent être utilisés pour le contrôle de la qualité, ou la renégociation des codecs si, par exemple, la bande passante diminue. Une communication H.323 se déroule en cinq phases : l'établissement d'appel, l'échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource réservation Protocol), l'établissement de la communication audio-visuelle, l'invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.) et enfin la libération de l'appel

I.4.1.1.1. LES AVANTAGES ET INCOVENIENTS DU PROTOCOLE H.323

A. AVANTAGES

Les réseaux IP sont à commutation de paquets, les flux de données transitent en commun sur une même liaison. Les débits des réseaux IP doivent donc être adaptés en fonction du trafic afin d'éviter tout risque de coupure du son (et de la vidéo). Tous les sites n'ont pas le même débit. Plus le débit sera élevé et plus le risque de coupure sera faible. Par ailleurs, tant que la qualité de service n'existera pas dans les réseaux IP, la fiabilité des visioconférences sur les lignes à faible débit sera basse.

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

- Codecs standards : H.323 établit des standards pour la compression et la décompression des flux audio et vidéo. Ceci assure que des équipements provenant de fabricants différents ont une base commune de dialogue.
- Interopérabilité : Les utilisateurs peuvent dialoguer sans avoir à se soucier de la compatibilité du terminal destinataire. En plus d'assurer que le destinataire est en mesure de décompresser l'information, H.323 établit des méthodes communes d'établissement et de contrôle d'appel.
- Indépendance vis à vis du réseau : H.323 est conçu pour fonctionner sur tout type d'architecture réseau. Comme les technologies évoluent et les techniques de gestion de la bande passante s'améliorent, les solutions basées sur H.323 seront capables de bénéficier de ces améliorations futures.
- Indépendance vis à vis des plates-formes et des applications : H.323 n'est lié à aucun équipement ou système d'exploitation.

- Support multipoint : H.323 supporte des conférences entre trois terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée.
- 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.
- 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. Indispensable pour permettre un minimum d'interopérabilité entre équipements de fournisseurs différents, ce standard présente toutefois les inconvénients suivants.

B. INCONVENIENTS

H.323 est un protocole complexe, créé initialement pour les conférences multimédia et qui incorpore des mécanismes superflus dans un contexte purement téléphonique. Ceci a notamment des incidences au niveau des terminaux H.323 (téléphones IP, par exemple) qui nécessitent de ce fait une capacité mémoire et de traitement non sans incidence au niveau de leur coût. Il comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité ou de plus petit dénominateur commun (dans le choix du codec, par exemple) ; D'autre part, comme le seul codec obligatoire est le codec G.711 (64 Kbps) et que le support des autres codecs plus efficaces est optionnel, l'interopérabilité entre produits provenant de constructeurs différents ne signifie pas qu'ils feront un usage optimal de la bande passante. En effet, dans le cas où les codecs à bas débits sont différents, le transport de la voix se fera à 64 Kbps, ce qui, en termes de bande passante, ne présente guère d'avantages par rapport à un système téléphonique classique. Le protocole H.323 est une des normes envisageables pour la voix sur IP à cause de son développement inspiré de la téléphonie. Cependant, il est pour l'instant employé par des programmes propriétaires (Microsoft, etc.). La documentation est difficile d'accès car l'ITU fait payer les droits d'accès aux derniers développements de cette technologie, en dehors des efforts faits par le projet Open H.323 pour rendre cette technologie accessible à tous. Ainsi son adaptation au réseau IP est assez lourde. C'est pourquoi au fil des recherches est né le protocole SIP.

I.4.1.2. LE PROTOCOLE SIP

SIP (Session Initiation Protocol) a été normalisé par le groupe de travail WG MMUSIC (Work Group Multi party MultiMedia Session Control) de l'IETF. La version 1 est sortie en 1997, et une seconde version majeure a été proposée en mars 1999 (RFC 2543). Cette dernière a elle-même été largement revue, complétée et corrigée en juin 2002 (RFC 3261). Des compléments au protocole ont été définis dans les RFC 3262 à 3265. SIP est au sens propre un protocole de signalisation hors bande pour l'établissement, le maintien, la modification, la gestion et la fermeture de sessions interactives entre utilisateurs pour la téléphonie et la vidéoconférence, et plus généralement pour toutes les communications multimédias. Le protocole n'assure pas le transport des données utiles, mais a pour fonction d'établir la liaison entre les interlocuteurs. Autrement dit, il ne véhicule pas la voix, ni la vidéo, mais assure simplement la signalisation. Il se situe au niveau de la couche applicative du modèle de référence OSI et fonctionne selon une architecture client-serveur, le client émettant des requêtes et le serveur exécutant en réponse les actions sollicitées par le client. SIP fournit des fonctions annexes évoluées, comme la redirection d'appel, la modification des paramètres associés à la session en cours ou l'invocation de services. En fait, SIP ne fournit pas l'implémentation des services, mais propose des primitives génériques permettant de les utiliser. De cette manière, l'implémentation des services est laissée libre, et seul le moyen d'accéder aux services est fourni.

I.4.1.2.1. ARCHITECTURE DE SIP

Contrairement à H.323, largement fondé sur une architecture physique, le protocole SIP s'appuie sur une architecture purement logicielle.

L'architecture de SIP s'articule principalement autour des cinq entités :

V' terminal utilisateur ; V' serveur d'enregistrement ; V' serveur de localisation ; V' serveur de redirection ; V' serveur proxy.

Un seul terminal étant présent sur cette figure, aucune communication n'est possible. Nous nous intéressons en fait ici aux seuls échanges entre le terminal et les services que ce dernier est susceptible d'utiliser lors de ses communications.

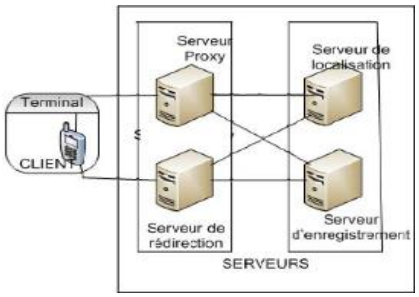


Figure 4 Architecture du protocole SIP

On peut schématiquement observer qu'il existe deux catégories de services :

L'un fourni au niveau de l'utilisateur (par le terminal), l'autre fourni au niveau des serveurs du réseau. Ces derniers sont répartis en deux classes : les serveurs de redirection et proxy, qui facilitent le routage des messages de signalisation et jouent le rôle d'intermédiaires, et les serveurs de localisation et d'enregistrement, qui ont pour fonction d'enregistrer ou de déterminer la localisation des abonnés du réseau.

- Terminal

Le terminal est l'élément dont dispose l'utilisateur pour appeler et être appelé. Il doit donc permettre de composer des numéros de téléphone. Il peut se présenter sous la forme d'un composant matériel (un téléphone) ou d'un composant logiciel (un programme lancé à partir d'un ordinateur).

Le terminal est appelé UA (User Agent), est constitué de deux sous-entités, comme illustré à la figure II.6 :

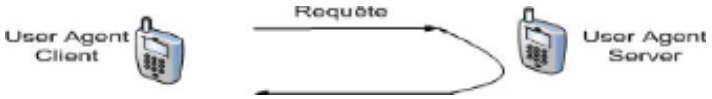


Figure 5 Communication entre UAC et UAS

- La partie cliente, appelée UAC (User Agent Client), chargée d'émettre les requêtes, initie un appel ;

- La partie serveur, appelée UAS (User Agent Server), est en écoute, reçoit et traite les requêtes, répond à un appel.

L'association des requêtes et des réponses entre deux entités de type UA constitue un dialogue.

Par analogie, on peut remarquer que la même chose se produit avec le protocole HTTP dans une application Web : un utilisateur exploite son navigateur comme

client pour envoyer des requêtes et contacter une machine serveur, laquelle répond aux requêtes du client. La différence essentielle par rapport aux applications standards utilisant HTTP est qu'en téléphonie un terminal doit être à la fois utilisé pour joindre un interlocuteur et pour appeler. Chaque terminal possède donc la double fonctionnalité de client et de serveur.

Lors de l'initialisation d'un appel, l'appelant exploite la fonctionnalité client de son terminal (UAC), tandis que celui qui reçoit la communication exploite sa fonctionnalité de serveur (UAS). La communication peut être clôturée indifféremment par l'User Agent Client ou l'User Agent Server. De nombreuses implémentations de clients SIP sont disponibles sur les plates-formes les plus courantes, Windows, Linux ou Mac. Elles sont le plus souvent gratuites, sous licence GPL.

Parmi les clients SIP es plus réputés, citons notamment les suivants :

- X-Lite Free;
- 3CX Phone Free;
- Phone Gaim;
- Wengo.

Ces clients SIP disposent de diverses fonctionnalités améliorées. En choisir un est souvent affaire de goût, selon l'ergonomie du logiciel et les caractéristiques souhaitées (support d'un codec particulier, support de la messagerie instantanée, etc.).

- Serveur d'enregistrement

Deux terminaux peuvent communiquer entre eux sans passer par un serveur d'enregistrement, à condition que l'appelant connaisse l'adresse IP de l'appelé. Cette contrainte est fastidieuse, car un utilisateur peut être mobile et donc ne pas avoir d'adresse IP fixe, par exemple s'il se déplace avec son terminal ou s'il se connecte avec la même identité à son lieu de travail et à son domicile. En outre, l'adresse IP peut être fournie de manière dynamique par un serveur DHCP. Le serveur d'enregistrement (Registre Server) offre un moyen de localiser un correspondant avec souplesse, tout en gérant la mobilité de l'utilisateur. Il peut en outre supporter l'authentification des abonnés. Dans la pratique, lors de l'activation d'un terminal dans un réseau, la première action initiée par celui-ci consiste à transmettre une requête d'enregistrement auprès du serveur d'enregistrement afin de lui indiquer sa présence et sa position de localisation courante dans le réseau. C'est la requête REGISTER, que nous détaillons plus loin, que l'utilisateur envoie à destination du serveur d'enregistrement. Celui-ci sauvegarde cette position en l'enregistrant auprès du serveur de localisation. L'enregistrement d'un utilisateur est constitué par l'association de son identifiant

et de son adresse IP. Un utilisateur peut s'enregistrer sur plusieurs serveurs d'enregistrement en même temps. Dans ce cas, il est joignable simultanément sur l'ensemble des positions qu'il a renseignées.

- Serveur de localisation

Le serveur de localisation (Location Server) joue un rôle complémentaire par rapport au serveur d'enregistrement en permettant la localisation de l'abonné. Ce serveur contient la base de données de l'ensemble des abonnés qu'il gère. Cette base est renseignée par le serveur d'enregistrement. Chaque fois qu'un utilisateur s'enregistre auprès du serveur d'enregistrement, ce dernier en informe le serveur de localisation. Presque toujours, le serveur de localisation et le serveur d'enregistrement sont implémentés au sein d'une même entité. On parle alors souvent non pas de serveur de localisation, mais de service de localisation d'un serveur d'enregistrement, tant que ces fonctionnalités sont proches et dépendantes. Les serveurs de localisation peuvent être collaboratifs. Le fonctionnement d'un serveur d'enregistrement est analogue à celui d'un serveur DNS dans le monde Internet : pour joindre un site Internet dont on ne connaît que le nom, il faut utiliser un serveur DNS, qui effectue la conversion (on parle de résolution) du nom en adresse IP. Ce serveur a connaissance d'une multitude d'adresses, qu'il peut résoudre parce qu'elles appartiennent à son domaine ou qu'il a la capacité d'apprendre dynamiquement en fonction des échanges qu'il voit passer. Dès qu'un nom lui est inconnu, il fait appel à un autre DNS, plus important ou dont le domaine est plus adéquat. De la même manière, les serveurs de localisation prennent en charge un ou plusieurs domaines et se complètent les uns les autres.

- Serveur de redirection

Le serveur de redirection (Re direct Server) agit comme un intermédiaire entre le terminal client et le serveur de localisation. Il est sollicité par le terminal client pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur. L'appelant envoie une requête de localisation d'un correspondant (il s'agit en réalité d'un message d'invitation, qui est interprété comme une requête de localisation) au serveur de redirection. Celui-ci joint le serveur de localisation afin d'effectuer la requête de localisation du correspondant à joindre. Le serveur de localisation répond au serveur de redirection, lequel informe l'appelant en lui fournissant la localisation trouvée. Ainsi, l'utilisateur n'a pas besoin de connaître l'adresse du serveur de localisation.

- Serveur proxy

Le serveur proxy (parfois appelé serveur mandataire) permet d'initier une communication à la place de l'appelant. Il joue le rôle d'intermédiaire entre les terminaux des interlocuteurs et agit pour le compte de ces derniers.

Le serveur proxy remplit les différentes fonctions suivantes :

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

Lorsqu'un utilisateur demande à un serveur proxy de localiser un correspondant, ce dernier effectue la recherche, mais au lieu de retourner le résultat au demandeur (comme le ferait un serveur de redirection), il utilise cette réponse pour effectuer lui-même l'initialisation de la communication en invitant le correspondant à ouvrir une session. Bien que fournissant le même type de service de localisation qu'un serveur de redirection, un serveur proxy va donc plus loin que la simple localisation, en initiant la mise en relation des correspondants de façon transparente pour le client. Il peut acheminer tous les messages de signalisation des terminaux, de l'initialisation de la communication à sa terminaison, en passant par sa modification. En contrepartie, le serveur proxy est une entité beaucoup plus sollicitée que le serveur de redirection, et donc plus lourde. Chaque terminal peut et devrait en principe disposer d'un tel serveur sur lequel se reposer pour interpréter, adapter et relayer les requêtes. En effet, le serveur proxy peut reformuler une requête du terminal UAC afin de la rendre compréhensible par le serveur auquel s'adresse l'UAC. Cela accroît la souplesse d'utilisation du terminal et simplifie son usage. Les serveurs proxy jouent aussi un rôle collaboratif, puisque les requêtes qu'ils véhiculent peuvent transiter d'un serveur proxy à un autre, jusqu'à atteindre le destinataire. Notons que le serveur proxy ne fait jamais transiter de données multimédias et qu'il ne traite que les messages SIP. Le proxy est une entité très souvent utilisée dans la pratique. Par analogie avec l'architecture illustrée à la figure II.7, symbolisant l'organisation des communications, on parle souvent du trapèze SIP pour désigner l'ensemble formé par ces quatre entités.

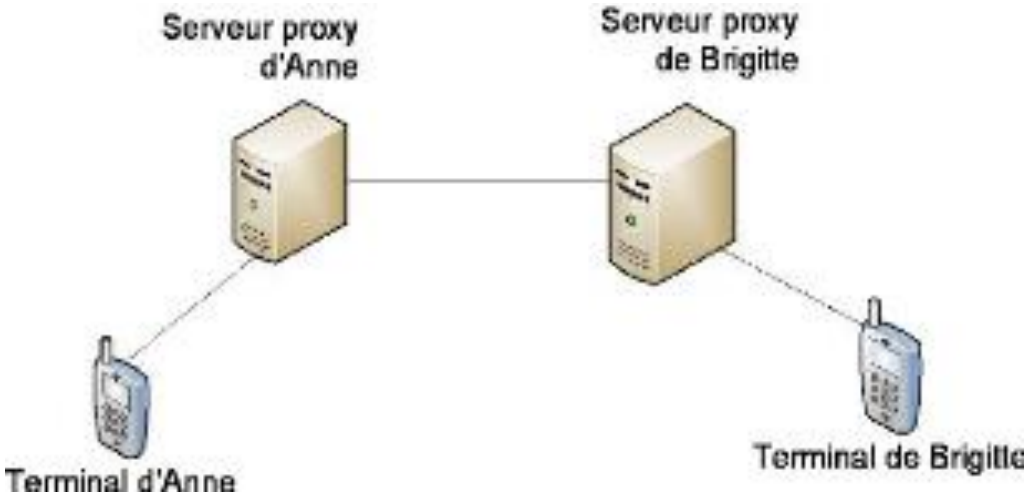


Figure 6 Trapèzes SIP

On distingue deux types de serveurs proxy, à savoir :

- ✓ Proxy state full, qui maintient pendant toute la durée des sessions l'état des connexions.
- ✓ Proxy stateless, qui achemine les messages indépendamment les uns des autres, sans sauvegarder l'état des connexions.

Les proxys stateless sont plus rapides et plus légers que les proxys statent full, mais ils ne disposent pas des mêmes capacités de traitement sur les sessions.

I.4.1.2.2. Composants d'un système SIP

Architecture standard SIP se compose des éléments suivants :

- Terminal (PDA, Phone, Messenger, . . .)

- Serveur de localisation.

- Serveur d'enregistrement.

- Serveur de redirection.

- Proxy.

- Passerelle (Gateway).

- Router

I.4.1.2.3. AVANTAGES ET INCONVENIENTS DU PROTOCOLE SIP

A. AVANTAGES

L'implémentation de la VoIP avec le protocole de signalisation SIP (Session Initiation Protocol) fournit un service efficace, rapide et simple d'utilisation. SIP est un protocole rapide et léger. La séparation entre ses champs d'en-tête et son corps du message facilite le traitement des messages et diminue leur temps de transition dans le réseau. Les utilisateurs s'adressent à ces serveurs Proxy pour s'enregistrer ou demander l'établissement de communications. Toute la puissance et la simplicité du système viennent de là. On peut s'enregistrer sur le Proxy de son choix indépendamment de sa situation géographique. L'utilisateur n'est plus "attaché" à son autocommutateur. Une entreprise avec plusieurs centaines d'implantations physique différente n'a besoin que d'un serveur Proxy quelque part sur l'Internet pour établir "son" réseau de téléphonique "gratuit" sur l'Internet un peu à la manière de l'émail. Les dizaines de milliers d'autocommutateurs peuvent être remplacés par quelques serveurs proxy. On imagine bien la

révolution. Mais comme d'habitude rien n'empêchera de remplacer un autocommutateur par un serveur Proxy réduisant ainsi l'intérêt du système. SIP est un protocole indépendant de la couche transport. Il peut aussi bien s'utiliser avec TCP que le protocole UDP.

B. INCONVENIENTS

L'une des conséquences de cette convergence est que le trafic de voix et ses systèmes associés sont devenus aussi vulnérables aux menaces de sécurité que n'importe quelle autre donnée véhiculée par le réseau. En effet, SIP est un protocole d'échange de messages basé sur HTTP. C'est pourquoi, il est très vulnérable face à des attaques de types Dos (Dénis de Service), détournement d'appel, trafic de taxation, etc. De plus, le protocole de transport audio associé RTP (Real Time Protocol) est lui aussi très peu sécurisé face à l'écoute indiscrète ou des Dos. Le SIP est une norme pour la communication multimédia, il devient de plus en plus utilisé pour la mise en place de la téléphonie sur IP, la compréhension de ce protocole aidera le professionnel à l'épreuve de la sécurité sur le réseau. Ce protocole est un concurrent direct à H.323.

I.4.2. PROTOCOLES DE TRANSPORT

Nous décrivons deux autres protocoles de transport utilisés pour la voix sur IP, à savoir : le RTP et le RTCP.

I.4.2.1. LE PROTOCOLE RTP

RTP (Real time Transport Protocol), standardisé en 1996, est un protocole qui a été développé par l'IETF afin de faciliter le transport temps réel de bout en bout des flots des données audio et vidéo sur les réseaux IP, c'est à dire sur les réseaux de paquets. RTP est un protocole qui se situe au niveau de l'application et qui utilise les protocoles sous-jacents de transport TCP ou UDP. Mais l'utilisation de RTP se fait généralement au-dessus d'UDP ce qui permet d'atteindre plus facilement le temps réel. Les applications temps réels comme la parole numérique ou la visioconférence constitue un véritable problème pour Internet. Qui dit application temps réel, dit présence d'une certaine qualité de service (QoS) que RTP ne garantit pas, du fait qu'il fonctionne au niveau Applicatif. Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi il ne garantit pas le délai de livraison. De plus RTP est un protocole qui se trouve dans un environnement multipoint, donc on peut dire qu'il possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoint.

I.4.2.1.1. LES FONCTIONS DU PROTOCOLE RTP

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie.

Ceci, de façon à reformer les flux avec ses caractéristiques de départ. C'est un protocole de bout en bout, volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application. Il laisse la responsabilité du contrôle aux équipements d'extrémité. C'est aussi un protocole adapté aux applications présentant des propriétés temps réel.

Il permet ainsi de :

- Mettre en place un séquencement des paquets par une numérotation afin de permettre ainsi la détection des paquets perdus. Ceci est un point primordial dans la reconstitution des données. Mais il faut savoir quand même que la perte d'un paquet n'est pas un gros problème si les paquets ne sont pas perdus en trop grands nombres.

Cependant il est très important de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte ;

- Identifier le contenu des données pour leurs associer un transport sécurisé et reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur) ;

- L'identification de la source, c'est à dire l'identification de l'expéditeur du paquet. Dans un multicast l'identité de la source doit être connue et déterminée ;

- Transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation). Ces trames sont incluses dans des paquets afin d'être transportées et doivent, de ce fait, être récupérées facilement au moment de la phase de segmentation des paquets afin que l'application soit décodée correctement.

I .4.2.1.2. AVANTAGES ET INCONVENIENTS DU PROTOCOLE RTP

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

I.4.2.2. 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 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 nous avons :

- La 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 gérés 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 les signaux de 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.

I.4.2.2.1. POINTS FORTS ET LIMITES DU PROTOCOLE RTCP

Le protocole RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanent sur une session et ces participants. Par contre, il fonctionne en stratégie bout en bout, et il ne peut pas contrôler l'élément principal de la communication dans le réseau.

I.5. COMPOSANTS DE LA TELEPHONIE IP

I.5.1. Les codecs

Les peuvent être des périphériques matériels ou de processus logiciels. Ils permettent de compresser, encoder et décompresser des donnes. Dans le cas de la VOIP, les codecs convertissent et compressent les signaux vocaux audio en paquets de données numérique transportable via le réseau. Ils les convertissent ensuite en signal audio à « l'autre extrémité » de l'appel.

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. A l'arrivés au destinataire, ce dernier grâce au même codec décompresse et restitue le son. Il On distingue des codecs à pertes et codecs sans pertes. Un codec à pertes distingue les parties moins importantes des informations et les supprime pour gagner en taille.

Une fois le signal numérisé et encodé, il est prêt à être transmis. Le transport des données peut se faire par l'intermédiaire de plusieurs protocoles dont notamment RTP et RTCP**,** le contrôle du flux se faisant via les autres protocoles nommés plus haut. Arrivé du côté du récepteur, le signal est décodé en utilisant le même codec et ensuite restitué.

L'objectif d'un codec est la transformation d'un signal analogique vers un signal numérique et vice-versa. Ici, le codec transforme donc le signal de la voix en données numériques facilement transportables sur un réseau. Après de transport, le même codec se charge de reconvertir le signal numérique vers un signal analogique.

Il existe une différence majeure permettant de classer les codecs existants dans deux catégories : les codecs sans pertes (lossless) et les codecs avec pertes (lossy).

Dans un codec lossless, tout le signal est transformé en binaire et le décodage restitue des données parfaitement identiques à celles données en entrée. Ce type de codecs est utilisé quand la qualité de la restitution est importante.

Dans un codec lossy, certaines parties du signal sont écartées et supprimées. Dans l'exemple de la voix, l'oreille humaine rencontre ses limites lorsqu'il s'agit d'écouter des fréquences trop basses ou trop hautes. Les codecs avec pertes (aussi appelés destructeurs) tirent parti de ce phénomène. Les sons dans les fréquences hautes ou basses sont tronqués pour diminuer la quantité d'information à transmettre. L'exploitation des particularités de l'oreille humaine s'appelle la psycho acoustique.

- Qualité de la voix :

Dans la téléphonie sur IP, les différents codecs retransmettent plus ou moins bien le signal original. Pour mesurer la qualité de la voix restituée, on parle de score MOS (Mean Opinion Score). C'est une note comprise entre 1 et 5 et attribuée par des auditeurs jugeant de la qualité de ce qu'ils entendent. Pour la VoIP, plusieurs codecs peuvent servir. Voici leurs détails :

- ✓ G.711 : Ce codec est le premier à avoir été utilisé dans la VoIP. Même s'il existe maintenant des codecs nettement plus intéressants, celui-ci continue d'être implémenté dans les équipements à des fins de compatibilité entre marques d'équipements différentes.[2]

- ✓ G.722 : A la différence du G.711, ce codec transforme le spectre jusqu'à 7kHz ce qui restitue encore mieux la voix. Les débits que ce codec fournit sont 48,56 ou 64kbit/s. Une des particularités est de pouvoir immédiatement changer de débit. Ceci est fortement appréciable lorsque la qualité du support de transmission se dégrade.

[2] Peter Thermos and Ari Takanen, Securing VoIP networks threats, vulnerabilities, and counter measures, (Addison-Wesley (c) 2007)

- ✓ G.722.1 : Dérivé du codec précédent, celui-ci propose des débits encore plus faibles (32 ou 24kbit/s). Il existe même des versions propriétaires de ce codec fournissant un débit de 16kbit/s.
- ✓ G.723.1 : C'est le codec par défaut lors des communications à faible débit. Deux modes sont disponibles. Le premier propose un débit de 6,4kbit/s et le deuxième un débit de 5,3kbit/s.

- Compression du silence :

Une des méthodes utilisées par les codecs pour réduire la quantité de données à transmettre et de détecter les silences. Dans une conversation téléphonique, chaque locuteur ne parle que 1/3 du temps en moyenne. Ce qui fait que 1/3 du temps d'une conversation est constitué de silence facilement reproductible et donc non codé par le codec. Ce mécanisme s'appelle VAD (Voice Activity Détection - DAV : Détection d'activité de la voix).

- Génération de bruits de confort :

Pendant une conversation où les silences sont effacés, l'absence de bruit chez le récepteur peut vite se révéler inconfortable. Dans cette optique, les codecs disposent d'un générateur de bruits de confort visant à simuler des bruits de fond pour améliorer le confort des utilisateurs.

- Robustesse sur la perte de paquets :

Si les conditions de circulations sur le réseau se dégradent, certains paquets contenant de l'information peuvent se perdent où arriver trop tard. Ce problème est en partie compensé par l'utilisation des buffers, mais la gigue peut être telle que le codec soit obligé de retransmettre au récepteur un paquet, alors qu'il n'est pas arrivé. Il existe plusieurs méthodes pour palier à ce problème : Il est possible par exemple de simplement répéter le contenu du dernier paquet pour combler le vide. On peut aussi répartir l'information sur plusieurs paquets de façon à introduire une redondance des données. En cas de pertes de paquets, le codec dispose ainsi d'une copie du paquet à retransmettre.

I.5.2. L'IP[3]

L ' « IP » désigne le protocole internet qui fournit un ensemble standard de règle pour la transmission et la réception de données en ligne. Ces règles standardisées

---

[3] [12]Peter Thermos and Ari Takanen, Securing VoIP networks threats, vulnerabilities, and counter measures, (Addison-Wesley (c) 2007)

permettent aux appareils fonctionnant sur différentes plateformes de communiquer entre eux. L'IP fournit également des règles de base pour la transmission de paquets de données (RTC), nécessaire à la VOIP.

I.5.3. BANDE PASSANTE

La bande passante n'est pas à proprement parler un équipement, mais elle reste indispensable au fonctionnement de la VOIP. Ce terme désigne la capacité d'un réseau à transmettre des données d'un point à un autre dans un laps de temps donné. Il est souvent mesuré en 1000 bits par seconde (Kb /s). Plus la quantité de bande passante disponible est élevé (haut début), plus un réseau peut prendre en charge les appels VOIP.

I.5.4. LE TELEPHONE IP

Le téléphone IP représente les combinés et postes matériels qui permettent de passer les appels VoIP. Il peut s'agir aussi bien d'un téléphone fixe que d'un appareil mobile. Il est aussi possible de passer des appels VoIP depuis un pc, une tablette ou un smartphone à l'aide d'un logiciel appelé « softphones ». La plupart de ces softphones ont une interface qui ressemble à un téléphone mobile lorsqu'elle apparaît sur votre écran. Ils disposent d'un clavier, d'un affichage et peuvent être utilisés via un écran tactile ou un clavier d'ordinateur. Un téléphone utilise le protocole Internet pour l'acheminement de la voix. On trouve parmi eux des terminaux fixes, mobiles ou encore des PC qui permettent de téléphoner en toute liberté.

I.6. LES DIFFERENTS TYPES DE TELEPHONE IP

La téléphonie VoIP permet de téléphoner à partir de différents terminaux. En effet, le fait que la technologie nécessite seulement un accès Internet permet d'utiliser différents terminaux pour communiquer. Que ce soit d'un téléphone classique, d'un mobile, d'une tablette ou d'un PC, les fonctionnalités évoluées de la téléphonie IP permettent d'optimiser les communications d'une entreprise. Il est ainsi possible de mettre en place un standard téléphonique virtuel, de disposer d'une qualité de son full HD lors des conversations, et de bénéficier de toutes les fonctionnalités classiques d'un standard téléphonique (transfert d'appel, conférence, appel en local, appel distant, appels simultanés, personnalisation de la messagerie, interception d'appel, numéros abrégés, etc.).

- Les téléphones matériels

Il s'agit d'un téléphone de bureau classique, comme nous en avons tous vu. Ces téléphones se branchent directement sur le réseau informatique de l'entreprise et ne nécessitent qu'un accès Ethernet.

- Les softphones

Le softphone est un logiciel installable sur PC, tablette ou smartphone. Il est de plus en plus utilisé par les professionnels, pour qui le travail à distance et en mobilité a beaucoup augmenté. Ce type de solution offre de nombreuses fonctionnalités avancées comme le partage de fichiers, la vidéo, les indicateurs de présence, le transfert d'appels, etc.

Pour les entreprises, le softphone est bien plus qu'un téléphone, tant il contribue à faciliter la communication et la collaboration entre les différentes équipes.

- Les téléphones analogiques via adaptateur ATA

Un ATA (adaptateur de terminal analogique) se présente habituellement sous la forme d'un petit boîtier qu'il est possible de raccorder à un téléphone analogique d'un côté, et au réseau Internet de l'autre.

- Les téléphones IP Bouygues Telecom Entreprises

Il existe plusieurs types de téléphones IP. Voici trois modèles qui répondent à des besoins différents et des usages variés.

- Polycom VVX 250

  Le poste classique, pour les besoins simples. Le Polycom VVX 250 est un téléphone de bureau avec trois touches programmables.

  - Ecran couleur 2.8
  - Résolution 320 x 240 pixels
  - 3 touches programmables
  - 4 touches interactives contextuelles
  - 2 ports RJ45 Giga Ethernet (10/100/1000 Mbits)
  - POE
  - USB

- Port RJ9 pour casque filaire
- Port EHS

Figure 7 Polycom vvx250

- Polycom VVX 450

Le poste multimédia Polycom VVX450 est prévu pour une utilisation optimale. Il dispose d'un grand écran couleur pour une ergonomie optimisée et convient à tous les besoins, du plus simple au plus évolué.

- Écran graphique couleur LCD rétroéclairé
- Résolution 480 x 272 pixels, 4.3 pouces
- 12 touches programmables
- 2 ports USB 2.0
- 2 ports RJ45 Giga Ethernet (10/100/1000 Mbits)
- POE
- Port RJ9 pour casque filaire
- Port EHS
- Module d'extension possible

Figure 8 Polycom VVX 450

- Polycom VVX 601

Le poste haut de gamme. Le Polycom VVX 601 est un téléphone professionnel avancé, conçu pour améliorer la collaboration et la productivité personnelle, grâce à un écran tactile et son clavier facilité.

- Écran graphique couleur tactile TFT LCD rétroéclairé
- Résolution 480 x 272 pixels, 4,3 pouces 16 :9
- 4 touches contextuelles
- 15 touches programmables
- 2 ports USB 2.0
- Bluetooth 2.1 intégré
- 2 ports RJ45 Giga Ethernet (10/100/1000 Mbits)
- POE
- Port RJ9 pour casque filaire
- Port EHS

Figure 9 Polycom VVX 601

1.7. AVANTAGES ET INCONVENNIENTS DE LA TELEPHONIE IP

a) AVANTAGES

En comparaison avec la téléphonie traditionnelle, la téléphonie IP présente plusieurs avantages. Parmi eux, la réduction considérable des coûts surtout pour les appels émis vers l'international. En effet, le réseau est basé sur la connexion internet donc les opérateurs des différents pays n'ont plus besoin de passer des accords spécifiques entre eux, raison principale des tarifs élevés pour les appels internationaux habituels. Cela offre la possibilité à l'entreprise de réaliser d'importantes économies. La voix sur IP permet également d'améliorer l'organisation de travail de l'entreprise puisque les câbles ne sont plus une contrainte. Dans le cas d'une entreprise ayant opté pour la téléphonie IP basée sur

le cloud, chaque utilisateur peut conserver son numéro sans tenir compte du lieu où il se trouve ou de l'appareil qu'il utilise. Du moment où il a accès à internet il peut passer des appels avec son numéro. Comme le marché tend de plus en plus vers cette avancée technologique, investir dans la téléphonie IP, c'est investir dans l'avenir. Comme la totalité du matériel est rassemblé sur un réseau commun, cela offre une grande souplesse et un confort au niveau de l'utilisation. Les appels sont enregistrés dans une base de données. Combinés à des logiciels CRM, ces enregistrements sont une richesse importante car ils peuvent améliorer considérablement la relation avec les clients. Il est également plus facile de contrôler les appels et les trafics.

b) INCONVENIENTS

Malgré tous les avantages présentés plus haut, il existe des risques et des inconvénients. Ces risques se situent essentiellement au niveau de la sécurité et du réseau. En effet, la téléphonie IP est exposée aux risques liés à internet comme le piratage des lignes ou le vol de données. Des personnes malveillantes peuvent également procéder à une saturation des lignes ou à leur écoute. Il est donc important de protéger sa ligne téléphonique pour éviter les pertes. Il est par exemple, envisageable de chiffrer la communication et d'utiliser un scanner de vulnérabilité VoIP. Heureusement, les fournisseurs prévoient des solutions pour éviter ces inconvénients. Le réseau téléphonique dépend également de la qualité du réseau internet et du courant. En cas de panne de ce dernier, la communication sera coupée. Il est donc primordial de s'équiper d'une bonne connexion internet et de bien choisir son opérateur.

I.8. CONCLUSIONS

La téléphonie IP est une technologie innovante qui comporte de nombreux avantages par rapport à la téléphonie traditionnelle. Son installation et son utilisation sont très simples et permettent des coûts réduits d'appels téléphoniques, de solutions de mobilité et de possibilités d'intégration avec d'autres systèmes informatiques. La téléphonie IP représente une véritable révolution dans la manière dont les entreprises gèrent leurs communications. En vous appuyant sur les étapes clés détaillées dans cet article, vous serez en mesure de mettre en place une solution de téléphonie IP adaptée à vos besoins spécifiques, tout en bénéficiant des nombreux avantages qu'elle offre.

CHAPITRE II : VULNERABILITES DES RESEAUX VOIP ET MESURES DE SECURITE

II.1. INTRODUCTION

L'opportunité de migrer de la téléphonie classique vers la téléphonie IP, a offert plusieurs avantages pour les entreprises, et les a permis de bénéficier de nouveaux services, tels que la vidéoconférence et la transmission des données. L'intégration de ces services dans une seule plateforme nécessite plus de sécurité.

Dans ce chapitre, nous allons décrire les attaques qui menacent la VoIP, et nous détaillerons quelques-unes. Nous finirons par une description des bonnes pratiques pour sécuriser les communications de type voix sur IP.

II.2. APERCUES SUR LES ATTAQUES DANS LES RESEAUX VoIP

Les attaques sur les réseaux VoIP peuvent être classées en deux types : les attaques internes et les attaques externes. Les attaques externes sont lancées par des personnes autres que celles qui participent aux appels, et ils se produisent généralement quand les paquets VoIP traversent un réseau peu fiable et/ou l'appel passe par un réseau tiers durant le transfert des paquets. Les attaques internes s'effectuent directement au réseau local dans lequel se trouve l'attaquant. Il existe deux principales classes des vulnérabilités sur un environnement VoIP. La première dépend des protocoles utilisés (SIP, H.323...) et la deuxième est liée aux systèmes sur lesquels les éléments VoIP sont implémentés. Chaque protocole ou service a ses propres attaques.

II.3. ATTAQUES SUR LES PROTOCOLES

Un appel téléphonique VoIP est constitué de deux parties : la signalisation, qui instaure l'appel, et les flux de media, qui transporte la voix.

La signalisation, en particulier SIP, transmet les entêtes et la charge utile (Payload) du paquet en texte clair, ce qui permet à un attaquant de lire et falsifier facilement les paquets. Elle est donc vulnérable aux attaques qui essaient de voler ou perturber le service téléphonique, et à l'écoute clandestine qui recherche des informations sur un compte utilisateur valide, pour passer des appels gratuits par exemple.

La signalisation utilise, en général, le port par défaut UDP/TCP 5060. Le firewall doit être capable d'inspecter les paquets de signalisation et d'ouvrir ce port afin de leurs autoriser l'accès au réseau. Un firewall qui n'est pas compatible aux protocoles de la VoIP doit être configuré manuellement pour laisser le port 5060

ouvert, créant un trou pour des attaques contre les éléments qui écoutent l'activité sur ce port.

Le protocole RTP utilisé pour le transport des flux multimédia, présente également plusieurs vulnérabilités dues à l'absence d'authentification et de chiffrement. Chaque entête d'un paquet RTP contient un numéro de séquence qui permet au destinataire de reconstituer les paquets de la voix dans l'ordre approprié. Cependant, un attaquant peut facilement injecter des paquets artificiels avec un numéro de séquence plus élevé. En conséquence, ces paquets seront diffusés à la place des vrais paquets.

Généralement, les flux multimédias contournent les serveurs proxy et circulent directement entre les points finaux. Les menaces habituelles conte le flux de la voix sont l'interruption de transport et l'écoute clandestine.

Les protocoles de la VoIP utilisent TCP et UDP comme moyen de transport et par conséquent sont aussi vulnérables à toutes les attaques contre ces protocoles, tel le détournement de session (TCP) (session Hackings) et la mystification (UDP) (Spoofing), etc.

Les types d'attaques les plus fréquentes contre un système VoIP sont :

I. SNIFFING[4]

Un renfilage (Sniffing) peut avoir comme conséquence un vol d'identité et la révélation d'informations confidentielles. Il permet également aux utilisateurs malveillants perfectionnés de rassembler des informations sur les systèmes VoIP. Ces informations peuvent par exemple être employées pour mettre en place une attaque contre d'autres systèmes ou données.

Plusieurs outils requis pour le sniffing, y compris pour le protocole H.323 et des plugins SIP, sont disponibles en open source.

II. SUIVI DES APPELS

Appelé aussi Call tracking, cette attaque se fait au niveau du réseau LAN/VPN et cible les terminaux (soft/hard phone). Elle a pour but de connaître qui est en train de communiquer et quelle est la période de la communication. L'attaquant doit

[4]Peter Thermos and Ari Takanen, Securing VoIP networks threats, vulnerabilities, and counter measures, (Addison-Wesley (c) 2007)

récupérer les messages INVITE et BYE en écoutant le réseau et peut ainsi savoir qui communique, à quelle heure, et pendant combien de temps.

Pour réaliser cette attaque, L'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE.

III. INJECTION DES PAQUETS RTP

Cette attaque se fait au niveau du réseau LAN/VPN. Elle cible le serveur register, et a pour but de perturber une communication en cours. L'attaquant devra tout d'abord écouter un flux RTP de l'appelant vers l'appelé, analyser son contenu et générer un paquet RTP contenant un en-tête similaire mais avec un plus grand numéro de séquence et timestamp, afin que ce paquet soit reproduit avant les autres paquets (s'ils sont vraiment reproduits). Ainsi, la communication sera perturbée et l'appel ne pourra pas se dérouler correctement. Pour réaliser cette attaque, l'attaquant doit être capable d'écouter le réseau afin de repérer une communication ainsi que les timestamps des paquets RTP. Il doit aussi être capable d'insérer des messages RTP qu'il a généré ayant un timestamp modifié.

IV. LES SPAMS

Trois formes principales de Spams sont jusqu'à maintenant identifiés dans SIP :

- Call Spam : Ce type de spam est défini comme une masse de tentatives d'initiation de session (des requêtes INVITE) non sollicitées. Généralement, c'est un UAC (User Agent Client) qui lance, en parallèle, un grand nombre d'appels. Si l'appel est établi, l'application génère un ACK, rejoue une annonce préenregistrée, et ensuite termine l'appel.
- IM (Instant Message) Spam : Ce type de spam est semblable à celui de l'e-mail. Il est défini comme une masse de messages instantanés non sollicitées. Les IM spams sont pour la plupart envoyés sous forme de requête SIP. Ce pourraient être des requêtes INVITE avec un entête « Subject » très grand, ou des requêtes INVITE avec un corps en format texte ou HTML.

Bien-sûr, l'IM spam est beaucoup plus intrusif que le spam e-mail, car dans les systèmes actuels, les IMs apparaissent automatiquement sous forme de pop-up à l'utilisateur.

- Présence Spam : Ce type de spam est semblable à l'IM spam. Il est défini comme une masse de requêtes de présence (des requêtes SUBSCRIBE) non sollicitées. L'attaquant fait ceci dans le but d'appartenir à la " white List " d'un utilisateur afin de lui envoyer des messages instantanés ou d'initier avec lui d'autres formes de communications. L'IM Spam est différent du

Présence Spam du fait que ce dernier ne transmet pas réellement de contenus dans les messages.

V. LE DENI DE SERVICE (DOS : Denial Of Service)

C'est d'une manière générale, l'attaque qui vise à rendre une application informatique ou un équipement informatique incapable de répondre aux requêtes de ses utilisateurs et donc le mettre hors d'usage.

Une machine serveur offrant des services à ses clients (par exemple un serveur web) doit traiter des requêtes provenant de plusieurs clients. Lorsque ces derniers ne peuvent en bénéficier, pour des raisons délibérément provoquées par un tiers, il y a déni de service. Dans une attaque de type Dos flood attack, les ressources d'un serveur ou d'un réseau sont épuisées par un flot de paquets. Un seul attaquant visant à envoyer un flot de paquets peut être identifié et isolé assez facilement. Cependant, l'approche de choix pour les attaquants a évolué vers un déni de service distribué (DDoS). Une attaque DDoS repose sur une distribution d'attaques Dos, simultanément menées par plusieurs systèmes contre un seul. Cela réduit le temps nécessaire à l'attaque et amplifie ses effets. Dans ce type d'attaque, les pirates se dissimulent parfois grâce à des machines-rebonds (ou machines zombies), utilisées à l'insu de leurs propriétaires. Un ensemble de machines-rebonds, est contrôlable par un pirate après infection de chacune d'elles par un programme de type porte dérobée (backdoor).

Une attaque de type Dos peut s'effectuer à plusieurs niveaux, soit à la couche réseau :

- A la couche transport :

  - L'UDP Flooding Attacks : Le principe de cette attaque est qu'un attaquant envoie un grand nombre de requêtes UDP vers une machine. Le trafic UDP étant prioritaire sur le trafic TCP, ce type d'attaque peut vite troubler et saturer le trafic transitant sur le réseau et donc de perturber le plus la bande passante. Presque tous les dispositifs utilisant le protocole SIP fonctionnent au-dessus du protocole UDP, ce qui en fait d'elles des cibles. De nombreux dispositifs de VoIP et de systèmes d'exploitation peuvent être paralysés grâce à des paquets UDP Flooding visant l'écoute du port SIP (5060) ou d'autres ports.

  - TCP SYN flood : est une attaque visant le protocole TCP et plus exactement la phase d'établissement de connexion. Celle-ci se fait en trois sous étapes :

1. Le client envoie un paquet SYN au serveur ;
2. Le serveur répond avec un paquet SYN-ACK ;
3. Le client envoie un paquet ACK au serveur.

L'attaque consiste en l'envoie d'un grand nombre de paquets SYN. La victime va alors répondre par un message SYN-ACK d'acquittement. Pour terminer la connexion TCP, la victime ensuite va attendre pendant une période de temps la réponse par le biais d'un paquet ACK. C'est là le cœur de l'attaque parce que les ACK final ne sont jamais envoyés, et par la suite, la mémoire système se remplit rapidement et consomme toutes les ressources disponibles à ces demandes non valides. Le résultat final est que le serveur, le téléphone, ou le routeur ne sera pas en mesure de faire la distinction entre les faux SYN et les SYN légitimes d'une réelle connexion VoIP.

- A la couche applications :

  - SIP Flooding : Dans le cas de SIP, une attaque Dos peut être directement dirigée contre les utilisateurs finaux ou les dispositifs tels que les téléphones IP, les routeurs et les proxys SIP, ou contre les serveurs concernés par le processus, en utilisant le mécanisme du protocole SIP ou d'autres techniques traditionnelles de Dos.

- Les différentes formes d'attaque Dos sont :

a) ATTAQUE PAR LA METHODE DU CANCEL

C'est un type de déni de service lancé contre l'utilisateur, l'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique. Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant envoie immédiatement une requête CANCEL. Cette requête produit une erreur sur le dispositif de l'appelé et annule l'appel. Ce type d'attaque est employé pour interrompre la communication. La figure III.1 représente une attaque Dos via une requête CANCEL.

b) ATTAQUE PAR LA METHODE DU BYE

L'attaque par la méthode du BYE est dirigée contre les usagers. L'attaquant génère un BYE et interrompt une conversation. Pour réaliser cette attaque, le pirate écoute le trafic et prend les informations nécessaires (comme par exemple le Call-Id, le From ou encore le To) pour générer un BYE frauduleux correspondant à la session qui est injecté sur le réseau. Le BYE n'étant pas authentifié, celui qui reçoit l'information l'exécute.

c) REGISTER

Le serveur d'enregistrement lui-même est une source potentielle de déni de service pour les utilisateurs. En effet, ce serveur peut accepter des enregistrements de tous les dispositifs. Un nouvel enregistrement avec une « *» dans l'entête remplacera tous les précédents enregistrements pour ce dispositif. Les attaquants, de cette façon, peuvent supprimer l'enregistrement de quelques-uns des utilisateurs, ou tous, dans un domaine, empêchant ainsi ces utilisateurs d'être invités à de nouvelles sessions.

Notez que cette fonction de suppression d'enregistrement d'un dispositif, au profit d'un autre, est un comportement voulu en SIP afin de permettre le transfert d'appel. Le dispositif de l'utilisateur doit pouvoir devenir le dispositif principal quand il vient en ligne. C'est un mécanisme très pratique pour les utilisateurs mais également pour les pirates.

VI. DETOURNEMENT D'APPEL (CALL HIJACKING)

Le Call Hijacking consiste à détourner un appel. Plusieurs fournisseurs de service VoIP utilisent le web comme interface permettant à l'utilisateur d'accéder à son système téléphonique. Un utilisateur authentifié peut changer les paramètres de ses transferts d'appel à travers cette interface web. C'est peut-être pratique, mais un utilisateur malveillant peut utiliser le même moyen pour mener une attaque.

Exemple : quand un agent SIP envoie un message INVITE pour initier un appel, l'attaquant envoie un message de redirection 3xx indiquant que l'appelé s'est déplacé et par la même occasion, il donne sa propre adresse comme adresse de renvoi. A partir de ce moment, tous les appels destinés à l'utilisateur sont transférés et c'est l'attaquant qui les reçoit.

Un appel détourné en lui-même est un problème, mais c'est encore plus grave quand il est porteur d'informations sensibles et confidentielles.

VII. LES VULNERABILITES DE L'INFRASTRUCTURE (HARD ET SOFT)

Une infrastructure VoIP est composée de téléphones IP, Gateway, serveurs (proxy, register, etc.). Chaque élément, que ce soit un système embarqué ou un serveur standard tournant sur un système d'exploitation, est accessible via le réseau comme n'importe quel ordinateur.

Chacun comporte un processeur qui exécute des logiciels qui peuvent être attaqués ou employés en tant que points de lancement d'une attaque plus profonde.

VII.1. INFRASTRUCTURE HARDWARE

1) LE TELEPHONE IP

Un pirate peut compromettre un dispositif de téléphonie sur IP, par exemple un téléphone IP, un Soft phone, ou d'autres programmes ou matériels client.

Généralement il obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif. Compromettre un point final (téléphone IP) peut être fait à distance ou par un accès physique au dispositif.

Le pirate pourrait modifier les aspects opérationnels d'un tel dispositif :

- La pile du système d'exploitation peut être changée pour masquer la présence de l'attaquant ;
- Un Firmeware modifié de manière malveillante peut avoir été téléchargé et installé. Les modifications faites à la configuration des logiciels de téléphonie IP peuvent permettre :
  - Aux appels entrants d'être réorientés vers un autre point final sans que l'utilisateur soit au courant ;
  - Aux appels d'être surveillés ;
  - A l'information de la signalisation et/ou les paquets contenant de la voix d'être routés vers un autre dispositif et également d'être enregistrés et/ou modifiés.
  - De compromettre la disponibilité du point final.

Les softphones ne réagissent pas de la même façon aux attaques comparés à leur homologues téléphone IP. Ils sont plus susceptibles aux attaques dues au nombre de vecteur inclus dans le système, à savoir les vulnérabilités du système d'exploitation, les vulnérabilités de l'application, les vulnérabilités du service, des vers, des virus, etc... En plus, le softphone demeure sur le segment de données, il est ainsi sensible aux attaques lancées contre ce segment et pas simplement contre l'hôte qui l'héberge. Les téléphones IP exécutent quant à eux leurs systèmes d'exploitation avec un nombre limité de services supportés, ils présentent donc moins de vulnérabilité.

2) LE SERVEUR VoIP

Un autre élément du réseau vulnérable est le serveur fournisseur du réseau de téléphonie sur IP, qui est peut-être la cible d'attaques pour mettre en péril tout le réseau.

Si un serveur de signalisation est compromis un attaquant peut contrôler totalement l'information de signalisation pour différents appels ce qui permettra à

un attaquant de changer n'importe quel paramètre relatif à l'appel. Pour finir, il faut préciser qu'un serveur de téléphonie IP est installé sur un système d'exploitation, il peut donc être une cible pour les virus, les vers, ou n'importe quel code malveillant.

VII.2. INFRASTRUCTURE SOFTWARE

Une des principales vulnérabilités du système d'exploitation est le buffer overflow qui permet à un attaquant de prendre le contrôle partiel ou complet de la machine.

Elle n'est pas la seule vulnérabilité et elle varie selon le fabricant et la version de l'OS. Ces attaques visant l'OS, sont pour la plupart relative au manque de sécurité de la phase initiale de développement du système d'exploitation et ne sont découvertes qu'après le lancement du produit. Les dispositifs de la VoIP tels que les téléphonies IP, Call Managers, Gateway et les serveurs proxy, héritent les mêmes vulnérabilités du système d'exploitation ou du Firmeware sur lequel ils tournent.

On déduira qu'une application de la VoIP est vulnérable dès que le système d'exploitation sur lequel elle tourne est compromis.

VIII. MESURES DE SECURISATION

On a déjà vu que les vulnérabilités existent au niveau protocolaire, application et systèmes d'exploitation. Pour cela, on a découpé la sécurisation en trois niveaux : Sécurisation protocolaire, sécurisation de l'application et sécurisation du système de l'exploitation.

VIII.1. SECURISATION AU NIVEAU DES PROTOCOLES

La prévalence et la facilité de sniffer des paquets et d'autres techniques pour la capture des paquets IP sur un réseau pour la voix sur IP fait que, le cryptage soit une nécessité pour la protection des personnes qui sont interconnectées.

IP sec peut être utilisé pour réaliser deux objectifs : Garantir l'identité des deux points terminaux et protéger la voix une fois que les paquets quittent l'Intranet de l'entreprise. VoIPsec (VoIP utilisant IP sec) contribue à réduire les menaces, les sniffeurs de paquets, et de nombreux types de trafic « vocal analyze ». Combiné avec un pare-feu, IP sec fait que la VoIP soit plus sûr qu'une ligne téléphonique classique. Il est important de noter, toutefois, qu'IP sec n'est pas toujours un bon moyen pour certaines applications, et que certains protocoles doivent continuer à compter sur leurs propres dispositifs de sécurité. Dans la section qui suit, nous allons détaillés certaines bonnes pratiques de sécurité de VoIP au niveau des protocoles.

VIII.1.1 VoIP VPN

Un VPN VoIP combine la voix sur IP et la technologie des réseaux virtuels privés pour offrir une méthode assurant la préservation de la prestation vocale. Puisque la VoIP transmet la voix numérisée en un flux de données, la solution VPN VoIP semble celle la plus approprié vu qu'elle offre le cryptage des données grâces a des mécanismes de cryptages, puisqu'elle permet d'offrir l'intégrité des paquets VoIP.

Vu que notre objectif est d'assurer la confidentialité et l'intégrité des clients, le mode choisi est donc le mode tunnel. Puisqu'il sécurise le paquet comme un tout (contrairement en mode transport qui ne sécurise que le payload IP). Le mode tunnel se base sur l'encapsulation de tout le paquet IP et ajoute un nouvel entête pour l'acheminement de ce dernier. Ce mode est généralement utilisé pour les routeur-to-routeur. En plus du mode tunnel, on choisit le protocole ESP qui lui a son tour va assurer le cryptage des données et donc la confidentialité, contrairement au protocole AH qui lui ne permet que l'authentification des paquets et non le cryptage.

Dans ce cas, la solution qu'on propose est ESP mode tunnel qui sera appliqué uniquement sur les points de terminaison à la voix IP, c'est-à-dire le routeur. Ceci nous permettra donc de minimiser le nombre de machines qui seront impliquées dans le traitement engendré par la sécurité. De plus, le nombre des clés nécessaires sera réduit.

VIII.1.2. SECURE RTP ou 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 IP sec (IP Security), dont le mécanisme d'échanges de clés est trop lourd. Il aussi est 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). Mais, surtout, il s'adjoint aux services du protocole de gestion de clé MIKEY (MultiMedia Internet KEYing).

A. Services de sécurités offertes par SRTP Les principaux services offerts par SRTP sont :

V' Rendre confidentielles les données RTP, que ce soit l'en-tête et la charge utile ou seulement la charge utile ;

V' Authentifier et vérifier l'intégrité des paquets RTP. L'émetteur calcule une empreinte du message à envoyer, puis l'envoie avec le message même ;

V' La protection contre le rejet des paquets. Chaque récepteur tient à jour la liste de tous les indices des paquets reçus et bien authentifiés.

B. Principe de fonctionnement de SRTP

Avec une gestion de clé appropriée, SRTP est sécurisé pour les applications unicast et multicast de RTP. En théorie, SRTP est une extension du protocole RTP dans lequel a été rajoutée des options de sécurité. En effet, il a pour but d'offrir plusieurs implémentations de cryptographie tout en limitant l'over Head lié à l'utilisation de chiffrement. Il propose des algorithmes qui monopoliseront au minimum les ressources et l'utilisation de la mémoire.

Surtout, il permet de rendre RTP indépendant des autres couches en ce qui concerne l'application de mécanismes de sécurité.

Pour implémenter les différents services de sécurité précités, SRTP utilise les composants principaux suivants :

- ✓ Une clé maîtresse utilisée pour générer des clés de session ; Ces dernières seront utilisées pour chiffrer ou pour authentifier les paquets ;
- ✓ Une fonction utilisée pour calculer les clés de session à partir de la clé maîtresse ;
- ✓ Des clés aléatoires utilisées pour introduire une composante aléatoire afin de contrer les éventuels rejets ou effets de mémoire.

SRTP utilise deux types de clés : clef de session et clef maîtresse. Par « clef de session » nous entendons une clef utilisée directement dans les transformations cryptographiques ; et par « clef maîtresse », nous entendons une chaîne de bits aléatoires à partir desquelles les clefs de sessions sont dérivées par une voie sécurisée avec des mécanismes cryptographiques.

C. 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 III.4 présente le format d'un paquet SRTP.

On remarque que le paquet SRTP est réalisé en rajoutant deux champs au paquet RTP :

- SRTP MKI (SRTP Master Key Identifier) : sert à réidentifier une clef maîtresse particulière dans le contexte cryptographique. Le MKI peut être utilisé par le récepteur pour retrouver la clef primaire correcte quand le besoin d'un renouvellement de clefs survient ;
- Authentification tag : est un champ inséré lorsque le message a été authentifié. Il est recommandé d'en faire usage. Il fournit l'authentification des en-têtes et données RTP, et indirectement fournit une protection contre le rejet de paquets en authentifiant le numéro de séquence

VII.1.3. LE PROTOCOLE TLS

C'est un protocole de sécurisation des échanges au niveau de la couche transport (TLS : Transport Layer Security). TLS, anciennement appelé Secure Sockets Layer (SSL), est un protocole de sécurisation des échanges sur Internet. C'est un protocole modulaire dont le but est de sécuriser les échanges Internet entre le client et le serveur indépendamment de tout type d'application. TLS agit comme une couche supplémentaire au-dessus de TCP.

Son utilisation est principalement associée à l'utilisation des certificats X.509 pour l'authentification des serveurs et le chiffrement des échanges (la signalisation).

VIII.2. SECURISATION AU NIVEAU 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 surement des erreurs et des vulnérabilités. Pour minimiser les risques, il est impératif d'utiliser une version stable ;
- Tester les mises à jour des 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 cliente dans le serveur.

Certains paramètres doivent être appliqués de manière sélective. Ces paramètres renforcent la sécurité de l'application, on peut les activer ou les interdire sur la configuration générale de l'application, comme on peut juste utiliser les paramètres nécessaires pour des clients bien déterminés et selon le besoin bien sûr. Ces paramètres protègent généralement contre le déni de service et ces

différentes variantes. Il est conseiller d'utiliser les paramètres qui utilisent le hachage des mots de passe, cela assure la confidentialité de messages.

VIII.3. SECURISATION DU SYSTEME 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 corrigés et maîtrisés 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 simple et robuste. 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 former d'une combinaison de lettre, de chiffres et ponctuations ;
- Ne pas exécuter le serveur VoIP avec un utilisateur privilège. 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 ;
- 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 une 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.

IX. CONCLUSION

Dans ce chapitre, il a été question de présenter les différentes vulnérabilités devant lesquelles le déploiement de la voix sur IP fait face, de ce fait, certaines mesures de sécurisation de l'environnement IP doivent être prises en compte afin de garantir la qualité des services.

En effet, il existe plusieurs attaques qui menacent l'utilisation de la voix sur le réseau IP, et nous avons fait allusion à quelques-unes jugées gênant et courant.

Chapitre III : CADRAGE DU PROJET

III.1. INTRODUCTION

Il est difficile de parler d'un projet avant d'avoir fait une analyse détaillée du travail à faire.

Il est cependant nécessaire d'effectuer une première estimation générale pour pouvoir délimiter ce projet

Dans ce chapitre nous allons mettre l'accent sur l'aspect du cadrage du projet et faire une étude détaillée du projet.

III.2. La définition du projet

Un projet est un processus unique, qui consiste en un ensemble d'activités coordonnées et maitrisées comportant des dates de début et de fin, l'entreprise dans le but d'attendre un objectif conforme à des exigences spécifiques telles que des contraintes des délais, de couts et de ressources.

III.3. Présentation

Le présent projet c'est la mise en place d'un réseau informatique dans une entreprise multi site qui fera à ce que ses différents sites soient relier grâce au réseau informatique que nous allons mettre en place malgré leurs distances.

III.4. Importance du projet

Ce projet a comme importance :

- Il permet de ne pas interrompre la chaîne numérique,
- D'automatiser,
- De standardiser,
- Et de centraliser certaines tâches.

III.5. Cahier de charge

Le cahier des charges est un document contractuel qui permet au maitre d'ouvrage de faire savoir au maitre d'œuvre ce qu'il attend de lui lors de la réalisation d'un projet, entrainant des pénalités en cas de non-respect. Il décrit précisément les besoins auxquels le prestataire ou le soumissionnaire doit répondre, et organise la relation entre les différents acteurs tout au long du projet.

En tant que pièce de référence du contrat, le cahier des charges protège les deux parties de toute ambiguïté : le maitre d'ouvrage est assuré que la livraison sera conforme à ses attentes, tandis que le maitre d'œuvre peut mener à bien le projet sans subir de jugements intempestifs au fur et à mesure. Toutefois, le maitre d'ouvrage a la possibilité de modifier le cahier des charges en cours de route au travers d'un avenant accepté par le maitre d'œuvre.

III.5.1. Contact

Pour la réalisation de notre projet nous avons eu à contacter les dirigeants de l'entreprise (NAS) pour leurs montrent la valeur de notre projet au sein de leur entreprise.

III.5.2. Objectif à réaliser

Notre projet repose sur trois objectifs principaux, à savoir :

- Objectifs techniques : les résultats attendus et du projet

- Objectif de délai : un chronogramme fixant la date et la fin du projet ainsi que celle des différents étapes sa mise en œuvre

- Objectifs du cout : le cout raisonnable pour réaliser ce projet.

III.5.3. Contraintes

Il y a trois contraintes qui sont liée au projet à savoir :

- Contrainte du cout (budget) : tout le monde doit être satisfait, si un geste commercial est envisagé, il ne doit surtout pas impacter le nombre de jours estimé et donc le planning. Outre le geste commercial, la simplification du cahier des charges (souvent très vaste) peut être envisagée : moins de développement, moins de test, moins de suivi donc forcément un coût moins élevé.

- Contrainte des temps (début et fin) : dans le cadre de ce projet nous nous proposons, le découpage en lots ainsi que les méthodologies agiles peuvent permettre de respecter les délais. De plus, il ne faut pas se tirer une balle dans le pied en avant-vente, les clients sont comme les enfants, ils sont impatients de voir leur nouveau joujou au plus vite, mais rien n'empêche d'entamer une discussion et de gagner quelques semaines quitte à livrer une première version simplifiée.

- Contrainte techniques (qualité du résultat) :la transparence avec NAS est de mise pour, optimiser les processus de production et mettre en place une réelle phase de

recette en prévoyant également une période de garantie et de TMA (Tierce Maintenance Applicative).

III.6. PLANIFICATION D'ORDONNANCEMENTS

III.6.1. Introduction

La construction du planning d'un projet passe par la modélisation d'un réseau de dépendance entre tâches sous forme graphique. Il s'agit d'une décomposition structurée du travail. Il faut décomposer le projet en sous-ensembles plus simples

Les méthodes d'ordonnancement des tâches permettent d'avoir une représentation graphique (immuable ou non) d'une réalisation en représentant chaque opération (ou tâche) par un arc, une liaison, ou un rectangle qui peut être proportionnel ou non à la durée. Ce graphique dans tous les cas, permet le positionnement relatif des opérations dans le temps.

III.6.2. Méthodes d'ordonnancements

La réalisation d'un projet nécessite souvent une succession de taches auxquelles s'attachent certaines contraintes : de temps, d'antériorité et de production.

Les méthodes d'ordonnancements (techniques) dans le cadre de la gestion d'un projet ont pour objectif de répondre au mieux aux besoins exprimés par un client, au meilleur cout et dans les meilleurs délais, en tenant compte des différentes contraintes. Il existe trois méthodes d'ordonnancement, à la base de toute construction d'un projet :

- Le diagramme de GANTT ;

- La méthode MPM (méthode des potentiels Métra) ;

- La méthode PERT (program Evaluation Reviewtechnic)[5(*)]

- Méthode PERT (programme évaluation review technique)

La méthode PERT est une technique américaine de modélisation de projet. Elle consiste à mettre en ordre sous forme de réseau plusieurs taches qui grâce à leurs dépendances et à leur chronologie permettent d'avoir un produit fini.

Les caractéristiques de PERT sont les suivantes :

- Les taches sont représentées par des flèches ;

- Le réseau visualise de dépendances entre tache ;

- Limite de la technique PERT : pas de représentation de notion de durée et de date

- Chaque tâche est représentée par un arc, auquel on associe un chiffre entre parenthèses ;

- Entre les arcs figurent des cercles appelés « sommets » ou « évènements » qui marquent l'aboutissement d'une ou plusieurs taches. Ces cercles sont numérotés afin de suivre l'ordre de succession des divers évènements.

- Méthode MPM

Cette méthode a été développée par une équipe de chercheur français.

Les caractéristiques du MPM sont les suivantes :

- Les tâches sont représentées par des sommets et contrainte de succession par des sommets

- Chaque tâche est renseignée par date- à laquelle elle peut commencer (date au plutôt) et celle à laquelle, elle doit se terminer (date au plus tard)

- A chaque arc est associée une valeur numérique, qui représente soit une durée d'opération (activité) soit un délai

- Méthode GANTT

Le diagramme de Gantt est la technique de représentation graphique permettant de renseigne et situer dans le temps les phases, activités, tâches et ressources du projet.

En ligne, on liste les tâches et en colonne les jours, semaine ou mois. Les tâches sont représentées par des barres dont la longueur est proportionnelle à la durée estimée.

Les tâches peuvent se succéder ou se réaliser en parallèle entièrement ou particulièrement

Ce diagramme a été conçu par un certain Henry L. GANTT (en 1917) et est encore aujourd'hui la représentation la plus utilisée.

III.6.3. Choix de la méthode

Dans le cadre de notre travail, nous choisissons la méthode PERT (Program Evaluation and ResearchTask ou Program Evaluation and Reviewtechnic). Il permet de mettre en ordre sous la forme d'un graphe, plusieurs tâches qui grâce à

leur dépendance et à leur chronologie concoure nt tous à la réalisation de notre projet.

III.6.4. Inventaire des tâches

Dans notre travail, nous avons recensé quelques tâches qui feront l'objet de notre évaluation, à savoir :

- Cadrage du projet ;

- Etude préalable ;

- Analyse détaillée ;

- Analyse technique ;

- conditionnement des locaux ;

- Acquisition des matériels ;

- Formation des utilisateurs ;

- Implémentation du nouveau système,

- Configuration des réseaux,

- Test et correction des erreurs,

- Lancement du nouveau système

III.7. Tableau d'antériorité

Le recours à la Méthode des Potentiels Métra suppose qu'aient été identifiées préalablement les différentes tâches nécessaires à la réalisation du projet, leur durée et leurs relations d'antériorité.

Ces indications sont synthétisées dans ce tableau

Taches	Activités	Durée	Antériorités
A	Cadrage du projet	10 jours	-
B	Etude préalable	15 jours	A
C	Analyse détaillée	25 jours	B
D	Analyse technique	20 jours	C
E	Conditionnement des locaux	6 jours	D
F	Acquisition des matériels	20 jours	D
G	Formation des utilisateurs	8 jours	E, F
H	Implémentation du nouveau système	6 jours	G
I	Configuration des serveurs	15 jours	G
J	Test et correction des erreurs	10 jours	H, I
K	Lancement du nouveau système	5 jours	J

Tableau 1 Table d'antériorité

III.8. Construction de graphe MPM

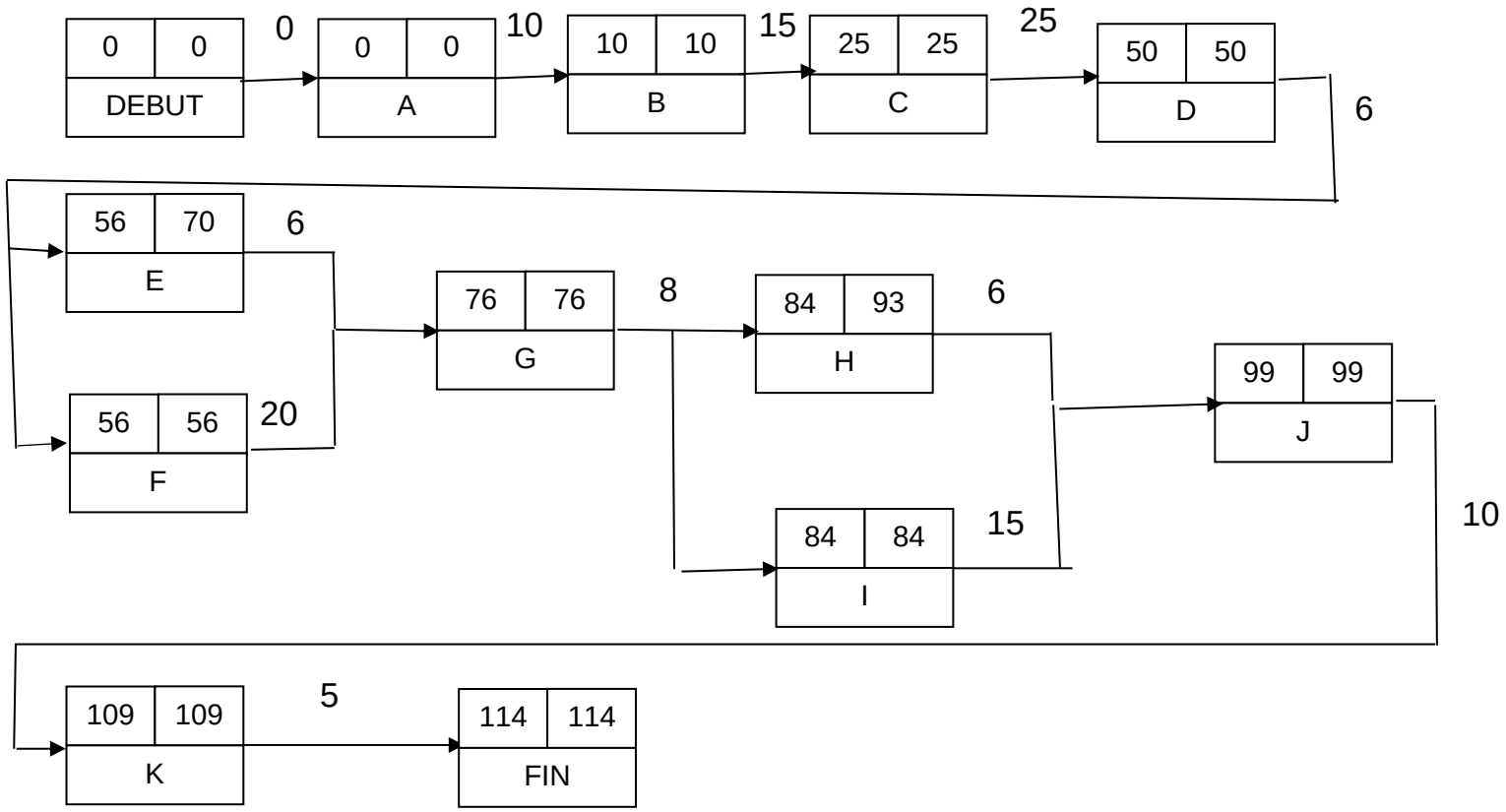


Tableau 2 Représentation du graphe MPM

III.9. Détermination du chemin critique

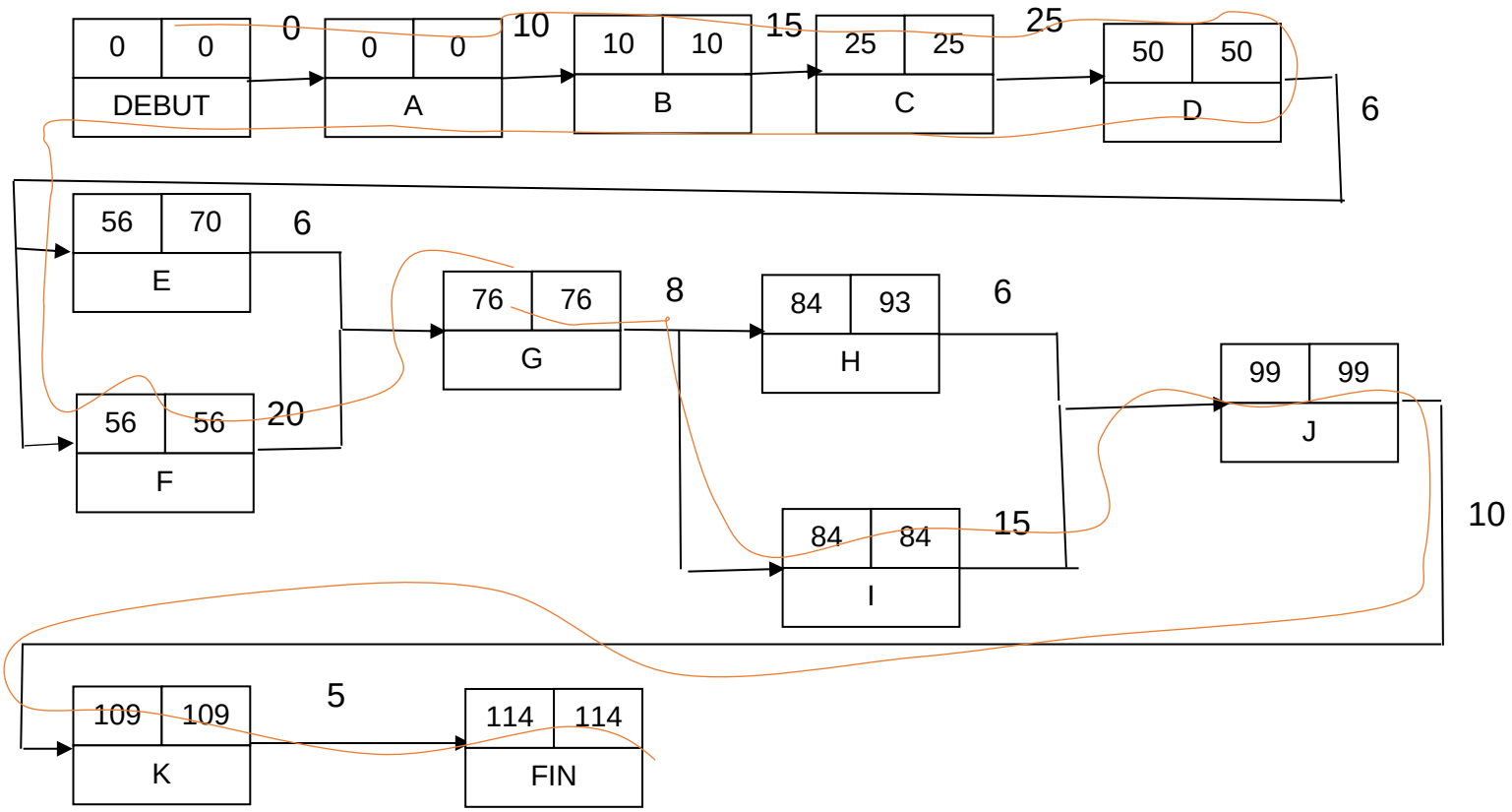


Tableau 3 Détermination du chemin critique

Donc notre chemin critique (C.C) : C.C = A, B, C, D, F, G, I, J, K

DUREE TOTAL

=d(A) + d(B) + d(C) + d(D) + d(E) + d(G) + d(H) + d(J) + d(K) + d(L)

= 10+15+25+20+6+8+6+10+5

=105

III.10. Coût

Le tableau ci-dessous nous donne le coût des activités selon leurs contraintes.

Taches	**Activités**	**Durée**	**Couts**
A	Collecte des données	10	2000$
B	Analyse du système	15	3000$
C	Conception du nouveau système	25	6000$
D	Implémentation du nouveau système	20	6000$
E	Aménagement de locaux	6	7000$
F	Acquisition des matériels et mise en place	20	36000$
G	Installation du nouveau système	8	1000$
H	Configuration des serveurs	6	1000$
I	Correction des erreurs	15	1500$
J	Formation des utilisateurs	10	800$
K	Lancement du système	5	800$

Tableau 4 cout du projet

Le Coût Total de l'évaluation du projet est la sommation des coûts des toutes s tâches ou activités critiques ou non critiques, soit :

CTE =2000+3000+6000+6000+7000+36000+1000+1000+1500+800+800

= 65100$

III.11. Conclusion

Nous voici à la fin de notre quatrième chapitre, qui nous a permis de faire une évaluation de notre projet. Et ce chapitre nous a permis de faire la présentation du projet, de montrer l'importance du projet, d'établir le cahier de charge, de montrer les objectifs à réaliser, de nous montrer encore le types de méthode d'ordonnancement ainsi que les le contraintes qui sont liée pour au projet

CHAP IV. ETUDE DU SITE NAS

IV.1. Introduction

Ce chapitre va nous parlent de la présentation de l'entreprise, Mission et objectif, Emplacement géographique, L'organigramme, fonctionnement et poste, Architecture de L'existant

IV.2. Présentation de l'entreprise

National Aviation Services (NAS) est le fournisseur de services aériens qui connaît la plus forte croissance sur les marchés émergents. Depuis le début de ses opérations au Koweït en 2003, NAS s'est rapidement transformé en leader de la prestation de services aériens grâce à sa présence au Moyen-Orient, en Afrique et en Asie du sud. Les 8 000+ employés compétents et agréables formant le cœur de son réseau mondial se sont engagés à fournir des services aériens que nous estimons être de la meilleure qualité au monde. NAS sert plus de la moitié des plus grandes compagnies aériennes mondiales. Ces transporteurs comptent sur nous pour travailler directement avec les passagers ainsi que dans les coulisses pour fournir des services qui font toute la différence. La gamme de services comprend des services d'escale et services aux passagers, la gestion du fret, des services d'ingénierie et l'entretien en ligne, des technologies aéroportuaires, l'exploitation des services aéronautiques d'un aéroport, un centre de formation aéronautique, une agence de voyages et le produit Pearl Assist qui inclut l'accès aux salons et les services d'accueil et d'assistance sur tout le réseau de l'entreprise. NAS se félicite de fournir des solutions d'aviation d'envergure mondiale.

L'entreprise est affiliée aux organismes phares de l'industrie telles que IGCH, GASA et AESA et adhèrent aux normes ISO, SGE et OHSAS. En tant que première entreprise de services d'escale du monde à obtenir la certification ISAGO, NAS a clairement confirmé son engagement à fournir des services d'aviation exceptionnels répondant aux normes les plus exigeantes du globe.

IV.3. Mission et Objectif

IV.3.1. Mission

Par son engagement pour la qualité de service et le talent de son équipe, NAS met tout en œuvre pour étendre ses activités dans les marchés émergents et ainsi devenir une entreprise de gestion aéroportuaire proposant un éventail de services

complet. Elle a comme mission d'assister toute compagnie aérienne aux activités Aéroportuaires.

IV.3.2. Objectif

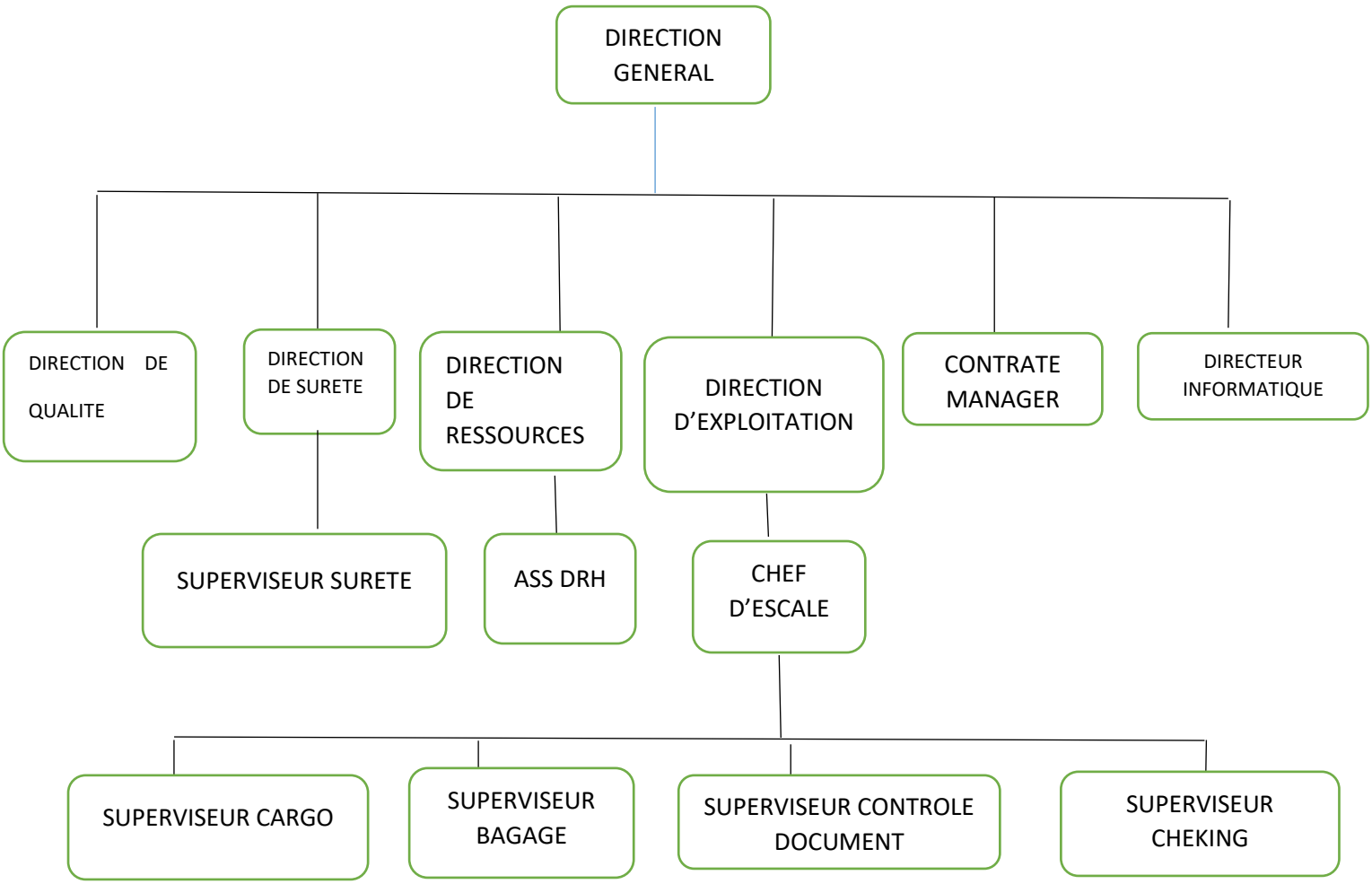
Son objectif, c'est de devenir la compagnie leader dans les marchés émergents pour les aéroports et compagnies aériennes dans ses activités. Accroitre sa présence en Afrique ou il a déjà plus de 60 % de sa croissance globale.

IV.4. Emplacement géographique

La compagnie Nationale d'Aviation Service se trouve au sein l'aéroport International de Ndjili.

L'aéroport international de Ndjili est l'aéroport principal de la ville de Kinshasa en République démocratique du Congo. Il est situé dans la commune de Nsele en bordure du Malabo, à une vingtaine de kilomètres à l'est de la ville, à laquelle il est relié par le boulevard Lumumba.

IV.5. Organigramme



IV.6. Fonctionnement et poste

- DIRECTION GENERAL

La fonction Direction et Administration générale consiste à définir les objectifs, prévoir et choisir les actions à accomplir, contrôler leur réalisation, prendre d'éventuelles mesures correctives.

Il faut pour cela avoir une vision à long terme et surtout un leadership managérial avéré.

- DIRECTION QUALITE

La fonction Direction Qualité dirige le service qualité et propose à la direction générale toute politique concernant l'ensemble des questions de qualité des services rendus. Dans ses propositions, au-delà de la valeur ajoutée technologique ou de service clients, il doit évaluer le coût induit par les développements proposés.

Le Directeur Qualité établit et met en œuvre la démarche qualité de l'entreprise en y associant des indicateurs et des processus de contrôle. Il est responsable de la conformité des produits ou services de l'entreprise aux exigences internes et externes (conformité aux normes, exigences légales, attentes des clients…). Il coordonne les activités de pilotage et de surveillance de la performance des procédures et méthodologies qualité de l'entreprise.

En plus des responsabilités techniques liées aux procédures, normes et qualifications ; le Directeur Qualité organise et maintient le système de management de la qualité et supervise sa déclinaison à tous les niveaux de l'entreprise.

- DIRECTION SURETE

La Politique de « Sûreté » s'intègre dans un socle commun et établit les principes généraux relatifs à la protection des personnes, des biens matériels et immatériels

Dont l'information, l'intégrité et l'image de l'Entreprise et de ses dirigeants contre toute menace malveillante, matérielle ou immatérielle.

- DIRECTION INFORMATIQUE

La direction informatique assure l'organisation, le suivi et la mise en œuvre de toute l'infrastructure système et informatique de l'entreprise.

- DIRECTION D'EXPLOITATION

Travaille au siège de la compagnie ou pour une société de handling. Il prépare le dossier de vol d'un avion en prenant les informations extérieures telles que la météorologie et la navigation aérienne. Avant chaque vol il effectue un briefing

avec l'équipage. Il doit être réactif en cas d'imprévu sur le vol et pouvoir proposer au commandant de bord des solutions de déroutement. Pour cela il est en constante communication avec les autorités locales, les aéroports, l'équipage de l'avion et les équipes de l'aéroport. Il doit également se tenir informé de tous les changements de données concernant les NOTAM et les espaces aériens.

- DIRECTION DES RESSOURSES HUMAINES

La fonction de directeur des ressources humaines recouvre trois missions principales. Tout d'abord, la gestion du personnel. Le DRH est chargé de définir et mettre en œuvre une politique de recrutement, de promouvoir la gestion des carrières

- CONTRAT MANAGEMENT

Les gestionnaires de contrats supervisent les projets réalisés en partenariat entre une organisation et une autre. Ils sont responsables de la coordination de tous les aspects du projet, de l'examen et de l'approbation des conditions contractuelles à la coordination des délais, en passant par l'approbation des budgets et plus encore

L'aéroport. Il doit également se tenir informé de tous les changements de données concernant les NOTAM et les espaces aériens.

IV.7 SERVICE CONCERNE

NAS possède trois modems Wi-Fi qui permettent à ses différents agents qui sont dans les diffèrent sites et locaux pour se connecter à l'internet et échanger des correspondances avec le reste du monde.

IV.7.1 Architecture existante

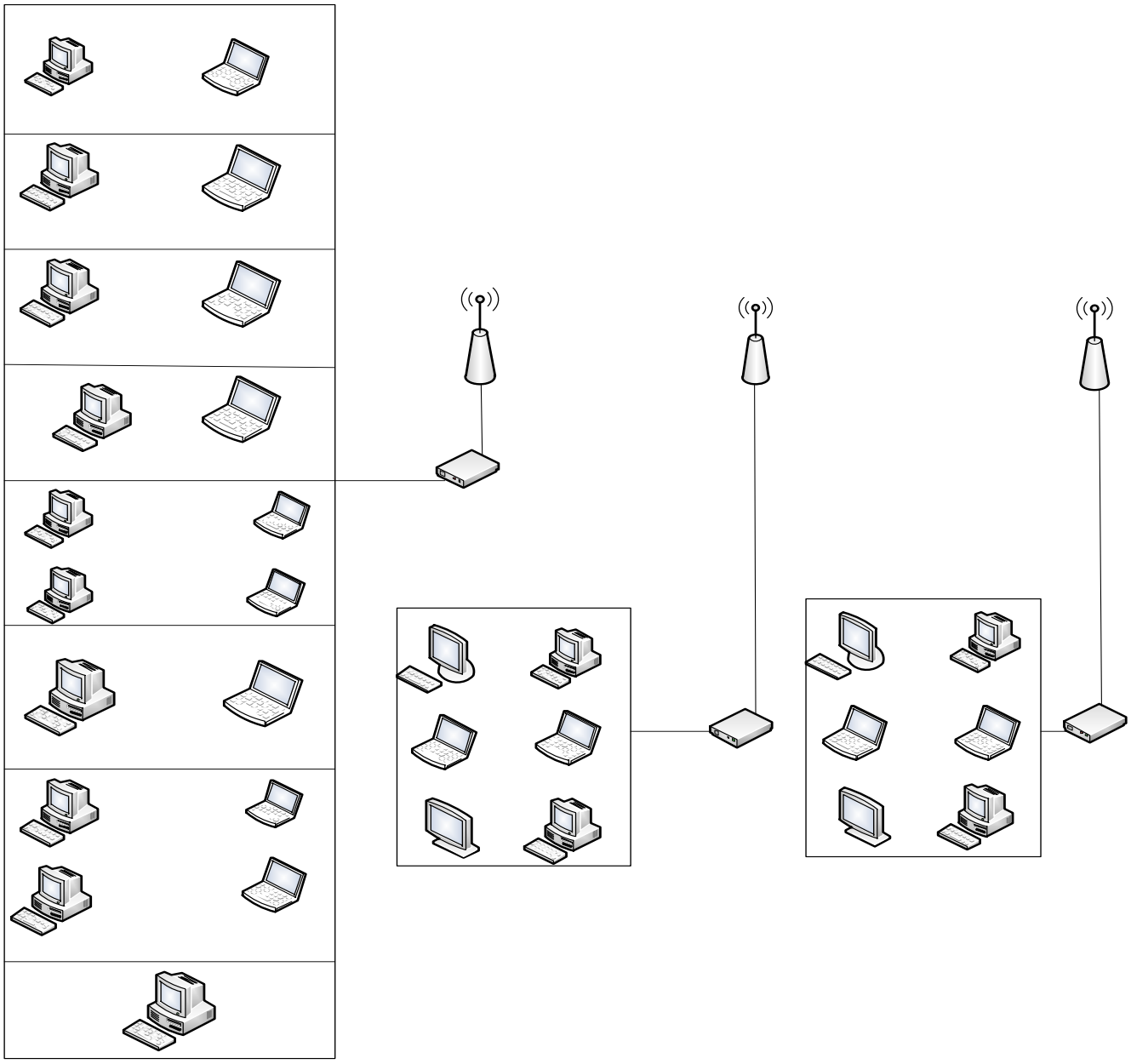


Figure 10 Architecture réseau NAS

IV.8. Critique de l’existant

IV.8.1. L’homme et organisation

Nous avons constaté que la NAS est une entreprise dotée des agents expérimenté mais sous-équipés.

Dans la situation actuelle nous avons remarqué que le réseau est déconnecté des autres sites et n’est pas sécurise.

IV.8.2 Matériels et logiciel

La compagnie Nas n’a pas suffisamment de matériel pour permettre une connexion sécurisée et pour le relie à d’autre.

Du point de vue logiciel, NAS n’a pas mis à disposition de ses techniciens (informaticien) les logiciels à approprier pour le bon déroulement des opérations (OS, Ms office, adobe, etc. …)

IV.9. Proposition de solution

Nous proposons des équipements d’interconnexion d'un réseau informatique sont les briques constitutives des réseaux informatiques physiques.

L’interconnexion des réseaux c’est la possibilité de faire dialoguer plusieurs sous réseaux initialement isolés, par l’intermédiaire de périphériques spécifiques (récepteur, Concentrateur, pont, Routeur, Modem), ils servent aussi à interconnecter les ordinateurs d’une entreprise. Il est parfois indispensable de les relier.

IV.10. Conclusion

En définitive, ce chapitre sur l'étude du site, nous a permis d'avoir une vision claire sur le fonctionnement de l'entreprise, l’Etat enfin de lieux de service informatique, les équipements informatiques qu'elle dispose, ses besoins ; pour enfin définir quel système de communication pourrions-nous mettre en place.

CHAPITRE V : DEPLOIEMENT DU SYSTEME

V.0. INTRODUCTION

Dans ce chapitre, nous allons proposer le modèle de déploiement de la solution VoIP sécurise, au sein du réseau informatique de la NAS.

Ce modèle reposera sur les principes de base se rapportant à sa mise en œuvre effective, étant donné que, dans le cadre de ce travail nous resterons essentiellement très théoriques. Toutefois, nous allons faire un petit montage expérimental avec du matériel essentiel.

V.1. Prérequis

V.2. CHOIX DU MATERIEL

Pour implémenter notre solution, tout en tenant compte des facteurs tels que : capacité de traitement des requêtes, temps de réponse aux requêtes des clients, ainsi de suite, nous avons porté notre choix sur un Serveur ProLiant DL 140 G3 du réseau existant.

Le serveur HP ProLiant DL 140 G3 est économique au format 2U, doté de capacité biprocesseur et équipé des fonctionnalités essentielles hautes performances, qui offrent aux clients une plate-forme leur permettant de concevoir une solution entièrement optimisée. Il est parfaitement adapté pour l'informatique courante et haute performance, idéal pour les petites et moyennes entreprises.

Ce serveur est doté de :

- 2 processeurs multicœurs : Intel Xeon processor X5365, 8.0 GHz, 120W ;4EDXV
- 8Go de Mémoire vive DIMM DDR2 P-5300 extensible à 32 Go ;
- Chipset Intel 5000X ;
- 2 disques durs SATA de 20 To ;
- Carte Réseau RJ-45 (Ethernet) ; 2 ports réseau 10/100/1000 intégrés prenant en charge l'équilibrage de la charge de travail et la fonction de basculement, plus 1 port dédié pour la gestion à distance HP ProLiant Lights Out 100i ;
- Une alimentation de 650 W, avec fonction de correction du facteur de puissance.

V.3. CHOIX DES LOGICIELS

Il existe plusieurs logiciels qui permettent d'implémenter une solution VoIP dans une entreprise, que ça soit dans le monde libre, par exemple Elastix, AsteriskNow, Tri Xbox, ou dans le monde des logiciels propriétaires où l'on peut citer par exemple 3CX Phone System.

Pour implémenter notre solution, le choix a été porté sur la plateforme 3CX Phone System, que ça soit pour le softphone ou pour l'IPBX.

En ce qui concerne le système d'exploitation sur lequel notre solution doit tourner, nous ne nous sommes pas trop attelés là-dessus. Parce que notre solution est compatible aux différents systèmes d'exploitation énumérés au point

Dans la section qui suit, nous allons présenter la plateforme 3CX Phone System.

V.3.1. 3CX PHONE SYSTEM

V.3.1.1. PRESENTATION DE 3CX PHONE SYSTEM

Le 3CX Phone System est un PBX-IP logiciel compatible sur la plateforme MS Windows, pouvant remplacer un PABX traditionnel, et offrir aux utilisateurs la possibilité de téléphoner, recevoir et transférer des appels. Ce PBX-IP supporte toutes les fonctionnalités d'un PBX traditionnel et il est aussi appelé Système Téléphonique VoIP, PABX-IP ou Serveur SIP. Les appels sont transmis sous forme des paquets de données sur le réseau informatique en lieu et place du réseau téléphonique traditionnel.

Les téléphones partagent le réseau avec les ordinateurs, ainsi le câblage téléphonique peut être supprimé. Avec l'utilisation d'une passerelle VoIP, il est possible de connecter les lignes téléphoniques existantes au PBX-IP et continuer d'émettre et de recevoir des appels téléphoniques via les lignes du réseau téléphonique commuté. Le PBX-IP 3CX utilise les téléphones logiciels ou matériels au standard SIP, et fournit la commutation d'appels internes, aussi bien que les appels en provenance et vers le réseau traditionnel ou via un service de voix sur IP (VoIP).

V.3.1.2. LES COMPOSANTS DE 3CX PHONE SYSTEM

Le 3CX Phone System est constitué des composants suivants :

1. Le service SIP server : ce service Windows configure les appels utilisant le protocole SIP. Il exécute les fonctions de PBX, telles que l'acheminement d'appels, le transfert d'appels etc. ;
2. Le service Media server : ce service Windows exécute le streaming de l'appel, c'est-à-dire la conversation audio ;
3. La Console de Gestion : offre une interface de configuration Web de 3CX Phone System. Le 3CX Phone System intègre un serveur Web Apache, qui est plus rapide, évolutif et sûr ;
4. Le service Data base server (Postgre SQL) : Il s'agit d'une version allégée du serveur de base de données SQL qui stocke tous les paramètres de configuration du système téléphonique ;
5. Le service Digital Receptionist : ce service peut répondre aux appels et offrir différentes options aux interlocuteurs ;
6. Le service Voice mail manager : ce service gère les boîtes de messagerie vocale ;
7. L'Assistant d'Appel 3CX : Il s'agit d'un client léger pour Windows, lequel permet aux utilisateurs de gérer leurs extensions et appels depuis leur Bureau Windows.

V.3.1.3. LES VERSIONS DE 3CX PHONE SYSTEM

Le logiciel 3CX Phone System est disponible dans 4 versions différentes, entre autres : l'Edition gratuite, PME, Pro et Entreprise.

Pour implémenter notre plateforme de test, nous avons choisi la version gratuite 3CX Phone System version 3, car elle support moins d'utilisateurs, mais pour l'entreprise qui voudra exploiter ce logiciel, elle pourra acheter la version Edition entreprise, dans la mesure où elle est adaptée pour l'environnement regroupant plusieurs utilisateurs

V.3.1.4. INSTALLATION DE 3CX PHONE SYSTEM

- PRE-REQUIS

L'installation du système 3CX version 3 pour Windows, nécessite les éléments suivants :

- Le système d'exploitation sur lequel peut tourner le serveur VoIP, exemple : Windows XP, Vista, 2000 (serveur et professionnel) ou 2003 Serveur etc……...
- Les ports compatibles, tels que : 5060 (SIP), 5481 (Apache), 5480 (Postgres), 5482 (Media server) ;
- Les téléphones au standard SIP, matériels ou logiciels ;
- Les passerelles VoIP, si on doit connecter des lignes RTC / RNIS ;
- Un compte chez un fournisseur de service VoIP, si on souhaite téléphoner via le réseau Internet.

INSTALLATION PROPREMENT DITE

Pour installer le logiciel 3CX Phone System, nous avons les étapes ci-après :

1. Téléchargez la dernière version de 3CX Phone System

2. Il vous sera demandé de relire et d'accepter le contrat de licence, ainsi que de choisir le chemin de l'installation. **Le** 3CX Phone System nécessitera approximativement 50 Mo d'espace libre sur le disque dur. Vous devrez avoir plus de place pour stocker les messages vocaux et les directives vocales.

3. Vous devez saisir le nombre de chiffres que vous voulez pour les lignes d'extensions. Un nom d'utilisateur et un mot de passe vous seront demandés, lequel vous servirez pour vous connecter à la console de gestion et gérer le système téléphonique. Enfin, il vous sera demandé le nom de votre serveur de courrier et une adresse de réponse. Ces paramètres seront utilisés pour envoyer, par courrier électronique, les notifications de messages vocaux aux utilisateurs.

4. Cliquez sur "Install" pour commencer l'installation de 3CX Phone System. **Le** Setup va copier tous les fichiers et installer les services Windows nécessaires. Cliquez sur "Finish" une fois l'installation est finie.

Après que l'installation soit terminée, vous pouvez vous connecter à la console de gestion de 3CX Phone System, en cliquant sur le raccourci "management console" dans le groupe de programme 3CX Phone System.

Figure 11 Console de gestion de 3CX Phone system

V.3.1.5. CONFIGURATION DE 3CX PHONE SYSTEM

PLAN DE NUMEROTATION

Pour assurer une bonne administration de notre solution implémentée, nous avons mis en place un plan de numérotation à 4 chiffres afin d'avoir une marge de manœuvre assez large pouvant permettre l'incrémentation de plusieurs extensions.

En se référant au découpage du réseau informatique de LA NAS, nous avons reparti les numéros des extensions.

N°	DESIGNATION	NUMERO D'EXTENSIONS
1	DG	112
2	Direction de qualité	115
3	Direction de sureté	118
4	DRH	120
5	Direction d'exploitation	123
6	Contrate manager	125
7	Direction informatique	128
8	Superviseur de sureté	130
9	Ass. DRH	135
10	Chef d'escale	140
12	Superviseur cargo	145
13	Superviseur bagage	150
14	Superviseur document	155
15	Superviseur cheking	160

Figure 12 Plan de numérotation

CREATION DES EXTENSIONS

Après avoir installé le 3CX Phone System, on procède à la création des extensions, la configuration des téléphones SIP (logiciels ou matériels) et la configuration des lignes téléphoniques.

Pour commencer, démarrez le raccourci "3CX Management console" depuis le groupe de programmes 3CX, ou pointez sur votre navigateur web se trouvant sur la console de gestion, en saisissant le nom de la machine sur laquelle est installée le 3CX Phone System, suivi de numéro du port.

L'écran de la console de gestion de 3CX Phone System sera divisé en 2 sections principales :

Gauche, le menu qui inclus les options de configuration les plus importantes, à savoir : les Extensions, Lignes, Règles d'appels, Configuration avancée et générale.

Ces différents menus sont représentés par la capture de l'écran de la figure

Figure 13 Console de gestion et configuration de 3CX Phone System

- AJOUT DES EXTENSIONS

Pour ajouter une extension, on clique sur "Add" dans l'option Extensions. Ceci affichera la page "add extension".

Ensuite, on peut remplir les informations suivantes :

1. Informations Utilisateur

✓ Numéro d'extension : spécifiez un numéro d'extension ;
✓ Prénom : saisissez le prénom de l'utilisateur ;
✓ Nom : saisissez le nom de l'utilisateur ;
✓ Adresse e-mail (Optionnel) : celle-ci sera utilisée pour la notification de messages vocaux et comme l'identifiant SIP par défaut. Vous pouvez laisser ce champ vide si vous le souhaitez.

2. Informations d'identification.

Ici on doit spécifier l'identifiant et le mot de passe.

✓ ID : le "nom d'utilisateur" SIP. Par exemple : 1102 ;

- ✓ Mot de passe : le mot de passe SIP (le mot de passe peut être caché de l'utilisateur).

3. Information concernant la messagerie vocale.

A cette étape, on doit activer certaines options qui sont prise en charge par la messagerie vocale entre autres :

- ✓ Activer la messagerie vocale : permet d'activer la messagerie vocale pour l'extension / l'utilisateur ;

- ✓ Afficher l'ID de l'appelant : le système de messagerie vocale énoncera le numéro de l'appelant qui a laissé le message ;

- ✓ Lire la date / l'heure du message : le système de messagerie vocale énoncera la date et l'heure du message ;

- ✓ Code (interrogation) : ce code est utilisé pour protéger la boîte vocale et est utilisé par l'utilisateur pour accéder à sa boîte vocale. Le code est aussi utilisé comme mot de passe pour accéder à l'Assistant d'Appel 3CX ;

- ✓ Options email : vous permet de choisir l'une de méthode pour recevoir par courrier électronique les messages vocaux suivant les options ci-après :
- ✓ Pas de notification par e-mail : le système n'enverra pas de courrier électronique ;

- ✓ Envoyer une notification e-mail seulement : cette option notifiera l'utilisateur qu'il a un nouveau message vocal. Cependant le courrier électronique ne contiendra pas le message vocal. Le message devra être écouté par téléphone depuis la messagerie vocale ;

- ✓ Envoyer v-mail en pièce jointe : cette option enverra un courrier électronique avec le message vocal en pièce jointe au format WAV. Le message restera dans la boîte vocale au cas où vous souhaiteriez l'écouter ultérieurement (en composant le 999).

- ✓ Envoyer en pièce jointe et supprimer de la boîte vocale : enverra un courrier électronique avec le message vocal en pièce jointe et supprimera le message vocal de la boîte de messagerie sur le Serveur 3CX. Ceci évite à l'utilisateur d'effacer le message vocal depuis deux emplacements différents, par exemple depuis la boîte de réception de courrier électronique et la boîte vocale sur le serveur 3CX.

4. Informations concernant la destination ou le transfert lorsque le correspondant est occupé.

Vous pouvez configurer pour chacune des extensions, ce que doit faire le système téléphonique si l'extension ne répond pas à l'appel, ou est occupée ou non enregistrée. Dans le cas de non réponse, vous devez spécifier le temps (en secondes) durant lequel vous souhaitez que le système attende. Dans le cas d'occupation, vous devez spécifier comment vous souhaitez que le téléphone ou le PBX-IP signale l'occupation.

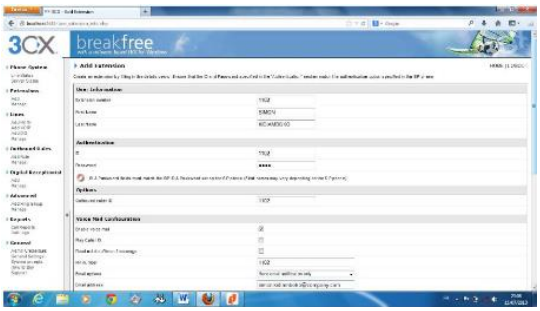


Figure 14 Illustre la Fenêtre portant les options nécessaires à la création d'une extension

Après la création des différentes extensions, on peut visualiser les identifiants et les numéros de toutes les extensions

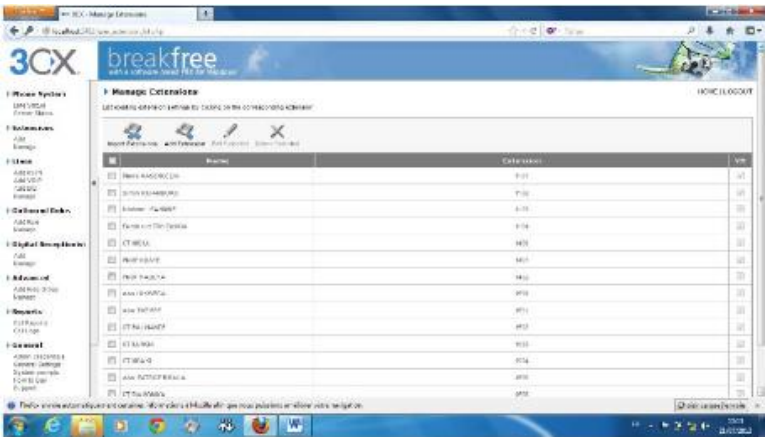


Figure 15 Listes des extensions créées

V .4. CONFIGURATION DE SOFTPHONE

Le softphone appelé aussi client SIP est un logiciel qui permet de jouer le rôle d'un téléphone IP. Pour son fonctionnement, il requiert un système de son (carte son, baffles, micro,).

Dans le cadre de notre expérimentation, nous avons utilisé le 3CX Phone, et sa configuration requiert des éléments ci-après :

- ✓ Numéro d'extension = Numéro d'appel ;
- ✓ ID d'authentification = Identifiant du compte SIP ;
- ✓ Mot de passe d'authentification = Mot de passe du compte SIP ; ?
- ✓ L'adresse IP du serveur VoIP.

Exemple de configuration d'un client ayant les paramètres suivants :

Numéro d'extension : 1102 ;

ID d'authentification : 1102 ;

Mot de passe d'authentification : 1102 ;

Coller ID : NGWEYI MASESI ;

L'adresse IP du serveur VoIP : 192.168.1.4

Figure 16 Interface de configuration de 3CXPhone

V.5. TEST DE FONCTIONNEMENT DE LA SOLUTION IMPLEMENTEE

Après avoir créé les extensions et configuré les téléphones SIP (logiciels) pour fonctionner avec ces extensions, Pour ce faire, on procède comme suit :

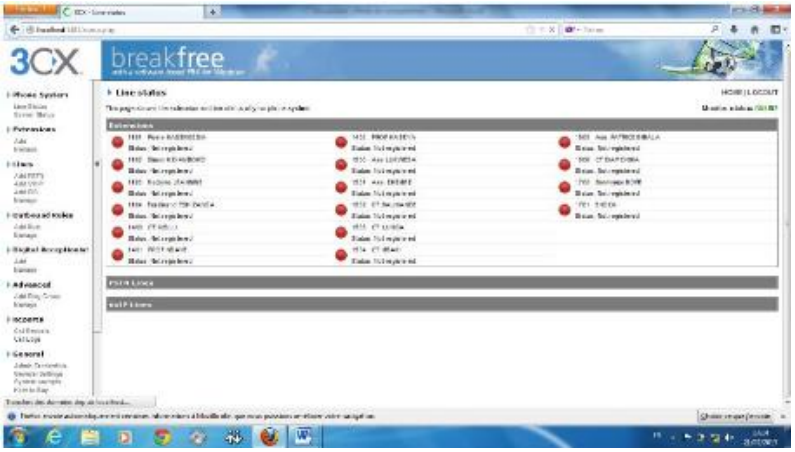


Figure 17 Illustre la façon dont on procède pour tester si l'installation fonctionne correctement

Démarrez la console de gestion de 3CX Phone System, et cliquez sur Système téléphonique > Etat des lignes (Il s'agit de la page par défaut). Vérifiez que toutes les extensions sont listées et dans l'état `Raccroché.

Le moniteur d'état affiche l'état des extensions (lignes internes) et de toutes vos lignes externes. Il s'agit de l'écran par défaut lors du démarrage de la console de gestion après que vous ayez configuré les extensions. Les états suivants sont affichés :

- Non enregistrée : l'extension a été créée, cependant le téléphone SIP n'est pas enregistré dans le serveur 3CX. Ceci peut être lié au fait que le téléphone n'est pas branché, ou que les paramètres de l'utilisateur sont erronés. Une autre cause possible peut être que le pare-feu est activé sur la machine qui exécute 3CX Phone System et qu'il bloque les communications entre le serveur et le téléphone.
- Enregistré (inactif) **:** l'extension est enregistrée et prête pour les appels téléphoniques ;
- Appel : l'extension compose un numéro ;
- Sonne : l'extension sonne ;
- Connectée : l'extension est actuellement en ligne ;
- Attente : l'extension a mis un appel en attente.

3.1.8. Architecture du nouveau réseau

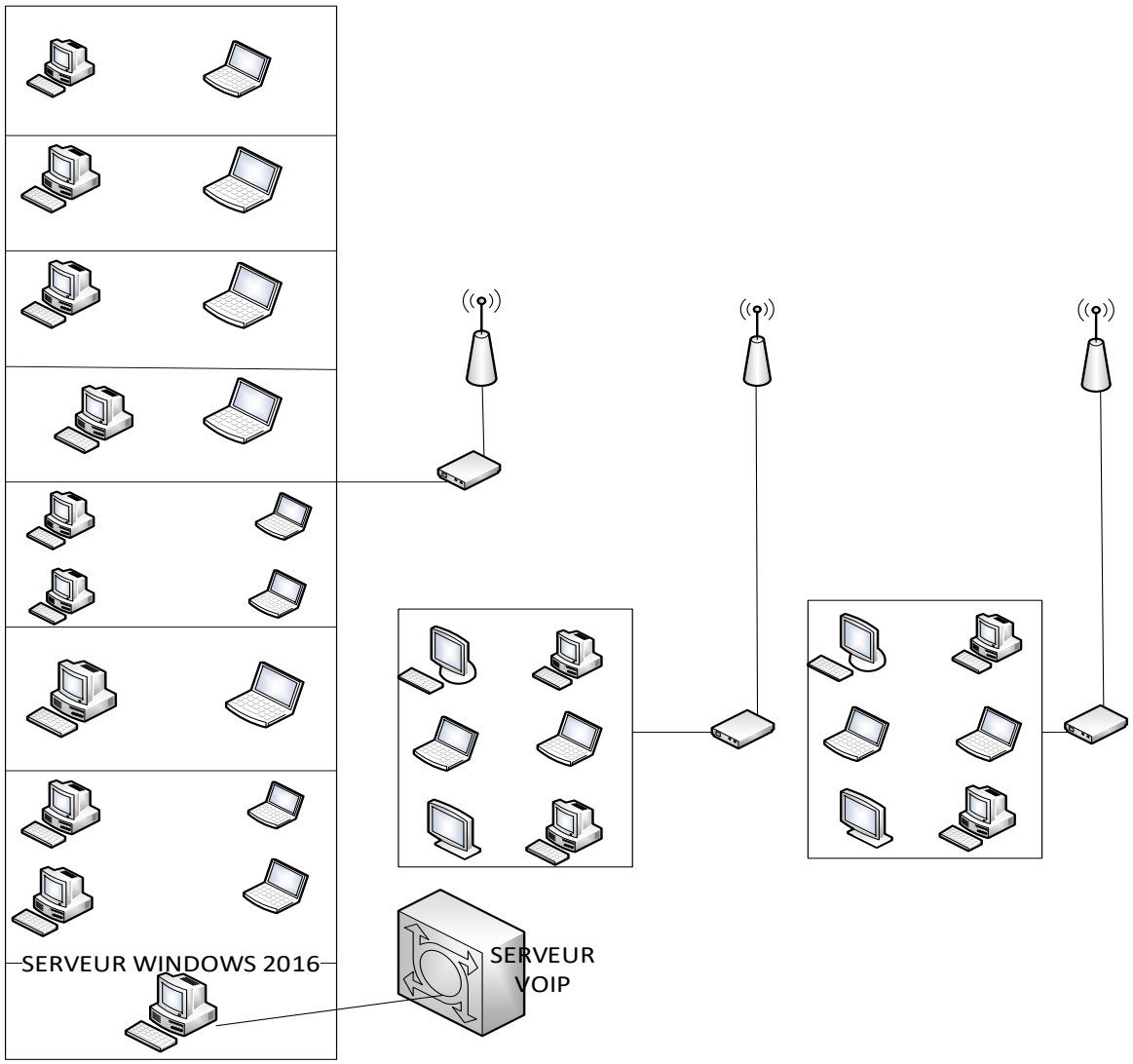


Figure 18 Architecture nouveau réseau

V.6. MESURES DE SECURISATION DE LA SOLUTION DEPLOYEE

Etant donné que la solution VoIP implémentée est une application de plus dans le réseau existant et qu'elle est exposée aux attaques diverses, il est important d'envisager des mesures de sécurisation du serveur qui hébergera cette application.

Les recommandations techniques à mettre en place sont les suivantes :

1) la protection physique du serveur

Le serveur doit être installé dans la salle informatique et bénéficier du même niveau de sécurité (alarme, anti-incendie, surveillance, etc.) que d'autres serveurs.

2) La redondance des composants critiques

Cette solution est coûteuse, mais nécessaire lorsque la criticité de l'infrastructure VoIP exige une forte disponibilité et/ou un rétablissement rapide en cas de panne. Les équipements critiques seront donc dupliqués et des mécanismes de partage de charge seront mis en place. Des tests réguliers doivent en outre être réalisés, afin de contrôler les procédures de basculement et le bon fonctionnement des appareils redondants.

3) Consolider et sécuriser le système d'exploitation du serveur

La sécurité du réseau voix implique à la fois celle des systèmes d'exploitation et des applications qui le composent. Consolider les systèmes d'exploitation est indispensable, nécessaire et obligatoire. Les ports et les services inutiles seront désactivés. Les systèmes seront mis à jour régulièrement pour corriger les vulnérabilités, et les permissions sur les registres appliquées, etc.

5) Placer les équipements derrière le pare-feu

Les firewalls seront configurés en amont des serveurs, pour éviter le déni de service, et sur les segments critiques. Ils ne contrôleront que les flux des VLANs qui sont bien restreints aux protocoles de la VoIP. Les pares-feux supporteront à la fois les protocoles SIP (Session Initiation Protocol) et les protocoles H.323.

6) Crypter les communications de bout en bout

Le cryptage concerner les flux de signalisation (chargés de mettre en relation l'appelant et l'appelé) et média (transport de l'information). Ainsi le chiffrement de la voix peut s'appuyer soit sur le protocole TLS (Transport Layer Security), DTLS (Datagramme TLS) ou SRTP (Secure RTP). Une entreprise peut également décider de recourir à IP Sec. Les communications externes peuvent aussi être acheminées via des tunnels VPN.

7) Monitoring du trafic voix

La surveillance du réseau avec des Sniffer et des IDS permettra de détecter le trafic anormal et les tentatives d'intrusion. L'analyse des logs pourra en outre révéler des attaques en brute force, des appels frauduleux (de nuit, vers des numéros surtaxés, etc.). Tandis que des pics du trafic voix traduiront des spams vocaux (Voice spam).

Toutefois, le risque zéro n'existe pas et les solutions de sécurité applicables à la VoIP peuvent s'avérer à la fois complexes et coûteuses à mettre en œuvre. L'entreprise devra donc arbitrer entre criticité, coût et niveau de risque jugé acceptable.

V.7. AVANTVAGES de 3CX

3CX est une solution de téléphonie IP basée sur le logiciel, très populaire pour les entreprises. Elle permet de gérer les communications vocales et vidéo, les conférences, la messagerie instantanée, et bien plus, tout en étant entièrement basée sur des technologies IP. 3CX peut être déployée sur des serveurs locaux ou dans le cloud, et offre une gamme de fonctionnalités avancées adaptées aux besoins des entreprises modernes. Voici les principaux avantages de 3CX :

- Réduction des coûts
- Flexibilité et mobilité
- Fonctionnalités avancées Messagerie vocale avancée
- Facilité de gestion et d'administration
- Sécurité renforcée Chiffrement des appels
- Support multisites et mise à l'échelle facile
- Intégration avec d'autres outils professionnels Intégration avec CRM et ERP
- Adaptabilité et personnalisations Personnalisation de l'interface utilisateur

V.8. CONCLUSION

Dans ce chapitre, nous avons définit l'approche d'implémentation de la solution VoIP dans le cadre d'un réseau informatique existant.

Etant donnée la vulnérabilité de cette solution, des mesures de sécurisation ont été proposées, et dans le cas d'une implémentation réelle, elles doivent être impérativement envisagées.

V.9. CONCLUSION GENERALE

Table des matières