TABLES DES MATIERES

ABREVIATIONS

AAA	Authentification Autorization Accounting
AH	Authentification Header
APP	Application
ARP	Address Resolution Protocol
CDP	Cisco Discovery Protocol
CLI	Command Line Interface
DECT	Digital Enhanced Cordless Telephone
DHCP	Dynamic Host Configuration Protocol
DLCI	Data-Link Connection Identifier
DNS	Domain Name System
DoS	Deny of Service
DTP	Dynamic Trunking Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FAI	Fournisseur d'Accès Internet
HDLC	High-Level Data Link Control
HTTP	Hypertext Transfer Protocol
HTTPs	Hypertext Transport Protocol Secure
ICANN	Internet Corporation for Assigned Names Numbers
ICMP	Internet Control Message Protocol
ID	Identifiant
IETF	Internet Engireening Task Force
IEEE	Institut of Electronic and Electronics Engineers
IGMP	Internet Group Management Protocol
IHL	Internet Header Length
IOS	Internetwork Operating System
IP	Internet Protocol
IPsec	IPsecurity
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

ISO	International System Interconnexion
ITU	International Communication Union
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitan Area Network
MCU	Multipoint Control Units
MGCP	Media Gateway Control Protocol
NAT	Network Address Translator
NNI	Network to Network Interface
NTP	Network Time Protocol
OS	Operating System
OSI	Open System Interconnexion
OSPF	Open Shortest Path First
PABX	Private Automatic Branch eXchange
PBX	Private Branch eXchange
PC	Personnal Computer
PDU	Protocol Data Unit
PPP	Point to Point Protocol
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RARP	Reverse Address Resolution Protocol
RAS	Registration Admission Status
RFC	Request For Comments
RIP	Routing Information Protocole
RR	Receiver Report
RSVP	Ressource Reservation Protocol
RTC	Réseau Téléphonique Commuté
RTCP	Real Control Time Protocol
RTP	Real Time Protocol
SDES	Source DEScription

SLARP	Serial Line Address Resolution Protocol
SSH	Secure Shell
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SPAM	Spiced Ham
SR	Sender Report
SRTP	Security Real Time Protocol
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
SVC	Switched Virtual Circuit
TCP	Transport Control Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
TFT	Trivial File Transfert
TFTP	Trival File Transfert Protocol
TLS	Transport Layer Security
ToF	Type of Service
ToIP	Telephony over IP
TTL	Time To Live
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UNI	User to Network Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VD	Vector Distance
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy

INTRODUCTION GENERALE

De nouvelles techniques de communications sont apparues ces dernières années. L'une les plus en vogue actuellement, est ce que l'on appelle « Voix sur IP ». La voix sur IP (Voice over IP) est une technologie de communication vocale en pleine émergence. Elle fait partie d'un tournant dans le monde de la communication. Depuis quelques années, la technologie VoIP commence à intéresser les entreprises, surtout celles de service comme les centres d'appels. La migration des entreprises vers ce genre de technologie n'est pas pour rien. Le but est principalement de : minimiser le coût des communications ; utiliser le même réseau pour offrir des services de données, de voix, et d'images ; et simplifier les coûts de configuration et d'assistance. En effet, la convergence du triple play (voix, données et vidéo) fait partie des enjeux principaux des acteurs de la télécommunication aujourd'hui.

Cette solution est totalement basée sur le protocole IP, est donc affectée par les vulnérabilités qui menacent la sécurité de ce protocole et l'infrastructure réseau sur laquelle elle est déployée. Cette dernière est le majeur problème pour les entreprises et un grand défi pour les développeurs.

Il est donc dans l'obligation de prendre des mesures de sécurité face à ces menaces afin de réduire au maximum les risques d'attaques sur les réseaux VoIP.

Dans un premier temps, ce rapport présente les généralités sur les réseaux informatiques. Dans un second temps, il introduit la VoIP et ses éléments ainsi que son architecture et ses protocoles. Dans un troisième temps, nous allons parler des vulnérabilités et mesure de sécurité de la VoIP. Et pour finir, nous allons réaliser dans le chapitre quatre la mise en place d'un modèle VoIP sous Cisco Packet Tracer.

CHAPITRE 1
ETUDE GENERALE DES RESEAUX INFORMATIQUES

1.1 Introduction

Dans ce chapitre, nous présenterons le modèle OSI et le modèle TCP/IP. Les équipements et les protocoles réseaux sont présentés dans le reste de ce chapitre.

1.2 Définition

Le réseau informatique est un ensemble d'équipements informatiques ou systèmes digitaux interconnectés entre eux via un milieu de transmission de données en vue partage de ressources informatiques et de la communication.

1.3 Le modèle OSI

OSI signifie Open System Interconnexion, ce qui se traduit par Interconnexion de systèmes ouverts. Ce modèle a été mis en place par l'ISO afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

Le modèle de référence OSI est une représentation abstraite en couches servant de guide à la conception des protocoles réseau. Il divise le processus de réseau en sept couches logiques, chacune comportant des fonctionnalités uniques et se voyant attribuer des services et des protocoles spécifiques. La figure 1.01 représente le modèle OSI.

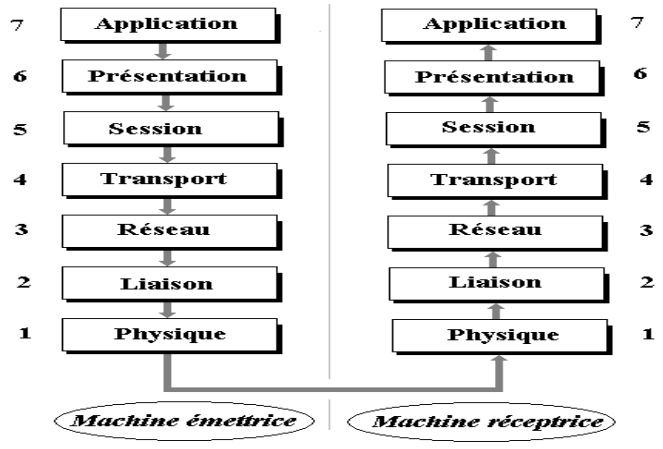


Figure 1.01 : *Le modèle OSI*

Chaque couche de niveau n communique avec la couche immédiatement supérieure n+1 (lorsqu'elle existe) et la couche immédiatement inférieure n-1 (lorsqu'elle existe).
Les couches basses (1, 2, 3) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. La couche 4 est la couche pivot entre les couches basses et les couches hautes. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques.[1][2]

1.3.2 Description des différentes couches

1.3.2.1 La couche physique

La couche physique définit la façon dont les données sont physiquement converties en signaux numériques sur le média de communication (impulsions électriques, modulation de la lumière, etc.).

Elle s'occupe de:

- La transmission de bits sur un canal de communication;
- Initialisation de la connexion et relâchement à la fin de la communication entre l'émetteur et le récepteur ;
- L'interface mécanique, électrique et fonctionnelle; Les supports physiques de transmission de données;

1.3.2.2 La couche liaison de données

La tâche principale de la couche liaison de données est de prendre un moyen de transmission brut et le transformer en une liaison.

Elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle prend les données de la couche physique et fournit ses services à la couche réseau. Les bits reçus sont groupés en unités logiques appelées trame. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale,

un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique.

1.3.2.3 La couche réseau

La couche réseau permet de gérer le sous-réseau, la façon dont les paquets sont acheminés de la source à la destination. Elle permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau.

1.3.2.4 La couche transport

La couche transport est chargée du transport des données, de leur découpage en paquets et de la gestion des éventuelles erreurs de transmission. Cela suppose un contrôle d'erreurs et de flux entre hôtes, assemblage et désassemblage de données.

1.3.2.5 La couche session

La couche session permet aux utilisateurs travaillant sur différentes machines, d'établir entre eux un type de connexions appelées « sessions ». Un utilisateur peut aussi établir une session pour se connecter à un système temps partagé ou transférer un fichier entre deux machines. Un des rôles de la couche session concerne la gestion du dialogue. Les sessions peuvent utiliser le mode unidirectionnel ou bidirectionnel du trafic. Quand on travaille en mode bidirectionnel alterné (half-duplex logique), la couche session détermine qui a le contrôle. Ce type de service est appelé gestion du jeton.

1.3.2.6 La couche présentation

La couche présentation définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.

1.3.2.7 La couche application

Cette couche comporte de nombreux protocoles utilisés tels que: terminal virtuel (ex: TELNET) ; courrier électronique; exécution de travaux à distance; consultation base de données.

Elle assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels. [1][2]

1.4 Le modèle TCP/IP

Même si le modèle de référence OSI est universellement reconnu, historiquement et techniquement, la norme ouverte d'Internet est le protocole TCP/IP (pour Transmission Control Protocol/Internet Protocol). Le modèle de référence TCP/IP et la pile de protocoles TCP/IP rendent possible l'échange de données entre deux ordinateurs, partout dans le monde, à une vitesse quasi équivalente à celle de la lumière. [4][5]
Ce modèle est divisé en 4 couches, à savoir :

- la couche accès réseau
- la couche internet
- la couche transport
- la couche application

La figure 1.02 représente le modèle TCP/IP

Figure 1.02 : *Modèle TCP/IP*

1.4.2 Couche accès réseau

La couche interface réseau du modèle TCP/IP correspond à la couche liaison de données et à la couche physique du modèle OSI. Cette couche définit les fonctions TCP/IP associées à l'étape de préparation des données avant leur transfert sur support physique, notamment l'adressage. La

couche interface réseau détermine également les types de support qui peuvent être utilisés pour la transmission des données.

1.4.3 Couche internet

La couche Internet du modèle TCP/IP définit l'adressage et la sélection du chemin. Cette fonction est identique à la couche réseau du modèle OSI. Les routeurs utilisent les protocoles de la couche Internet pour identifier le chemin que les paquets de données emprunteront lors de leur transfert d'un réseau à l'autre. Enfin, cette couche gère l'émission et la réception de messages ICMP (Internet Control Message Protocol).

1.4.4 Couche transport

Le rôle fondamental de cette couche est d'assurer la communication de bout en bout. Cette couche est globalement équivalente à la couche 4 d'OSI, notamment en ce qui concerne TCP.

La couche transport utilise le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). Ces deux protocoles gèrent les communications de nombreuses applications.

- TCP, un protocole orienté connexion qui assure le contrôle des erreurs.
- UDP, un protocole non orienté connexion dont le contrôle d'erreur est archaïque.

1.4.5 C ouche application

La couche application est la couche qui sert d'interface entre les applications que nous utilisons pour communiquer et le réseau sous-jacent via lequel nos messages sont transmis. Les protocoles de couche application sont utilisés pour échanger des données entre les programmes s'exécutant sur les hôtes source et de destination.

1.5 Le protocole IP

1.5.1 Les fonctions du protocole IP

Le protocole Internet fournit le service de transmission de paquets de base sur lequel les réseaux TCP/IP sont construits.[6]
Les fonctions du protocole IP incluent :

- La définition du datagramme
- La définition du plan d'adressage internet
- La circulation de données entre la couche accès réseau et la couche transport
- L'acheminement (routage) des datagrammes vers les ordinateurs à distance.
- La fragmentation et le réassemblage des datagrammes

1.5.2 Le format du datagramme

Le datagramme IP contient un en-tête IP suivi des données IP provenant des protocoles des couches supérieures. La figure 1.03 ci-dessous représente le format du datagramme IP

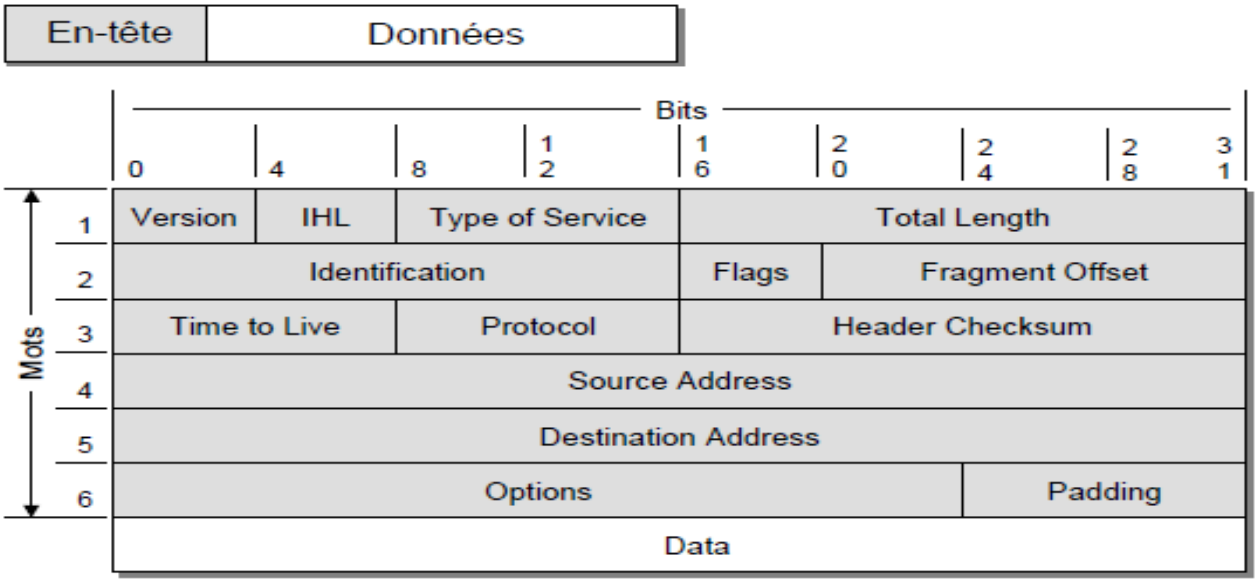


Figure 1.03 : *Le datagramme IP*

Signification des différents champs :

- Par défaut, la longueur de l'en-tête est de cinq mots de 32 bits (soit 20 octets) : le sixième mot est facultatif. Puisque la longueur de l'en-tête est variable, elle inclut un champ appelé IHL(Internet Header Lenght). L'en-tête comprend toutes les informations nécessaires à la transmission du paquet.
- Le champ Version fait quatre bits de long et indique le format de l'en-tête IP : le numéro du version actuelle est 4 (IPv4), la version suivante est la version 6 (IPv6) qui permet des adresses IP à 128 bits. Ce champ est utilisé par l'émetteur, le récepteur et tout routeur intermédiaire pour déterminer le format de l'en-tête.
- Le champ Type of Service (ToF) informe les réseaux de la qualité du service désirée.

- Le champ Total Length (longueur totale) contient la longueur de l'en-tête et des données IP en octets.
- Identification, drapeaux et déplacement de fragment sont des champs qui permettent la fragmentation des datagrammes.
- La durée de vie (Time To Live TTL) se mesure en secondes et représente la durée maximale de vie d'un datagramme sur le réseau. Cette valeur est décrémentée à chaque routeur. Lorsque le champ TTL tombe à 0, le temporisateur TTL expire et le datagramme IP est écarté par le routeur.
- Protocole (8 bits) : ce champ permet de savoir de quel protocole est issu le datagramme comme les protocoles suivants :ICMP: 1, IGMP: 2, TCP: 6, UDP: 17.
- Somme de contrôle de l'en-tête (16 bits) ou Header Checksum : ce champ permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission. La somme de contrôle est le complément à un de tous les mots de 16 bits de l'en-tête.
- Source Address (32 bits) : ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre.
- Destination Address (32 bits) : ce champ indique l'adresse IP du destinataire du message.[6]

1.6 Comparaison entre le modèle OSI et le modèle TCP/IP

Le modèle OSI divise la communication en 7 couches. Par contre, le modèle TCP/IP la divise en 4 couches dont chacune d'elles correspond à une ou plusieurs couches du modèle OSI. Cette comparaison est illustrée par la figure 1.04.

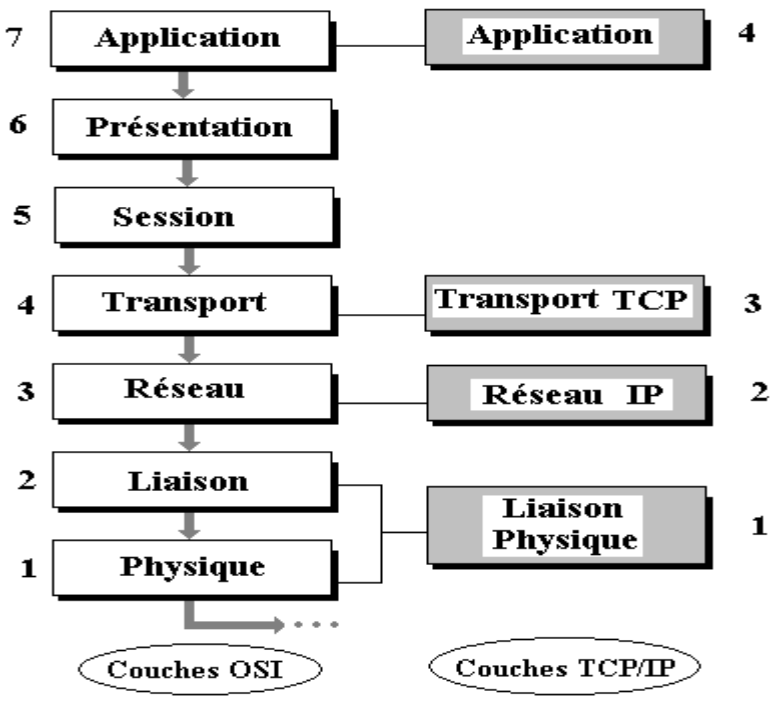


Figure 1.04 : *Comparaison entre modèle OSI et modèle TCP/IP*

1.7 Le principe de routage

1.7.1 Notions de base sur le routage

Un routeur utilise une table contenant tous les réseaux connectés localement et les interfaces qui leur sont reliées, afin que les messages parviennent à destination. Le routeur détermine la route ou le chemin à prendre en consultant les informations enregistrées dans sa table de routage. La table de routage contient également des informations sur les routes que le routeur peut emprunter pour atteindre les réseaux distants qui ne sont pas connectés localement. Les routes peuvent être attribuées au routeur de façon statique par un administrateur ou lui être indiquées de façon dynamique par un autre routeur, via un protocole de routage. [7]

Une route possède quatre composants principaux :

- le réseau de destination ;
- le masque de sous-réseau ;
- l'adresse de passerelle ou d'interface ;
- le coût de la route ou la mesure.

Lorsqu'un routeur reçoit un paquet, il examine l'adresse IP de destination pour savoir où le transférer. Le routeur recherche une valeur de destination correspondante dans la table de routage. Chaque valeur de destination d'une table de routage fait référence à une adresse réseau de destination. L'adresse IP de destination du paquet se compose, quant à elle, d'une adresse réseau et d'une adresse hôte. Pour savoir si la table contient une route vers le réseau de destination, le routeur doit déterminer s'il y a correspondance entre l'adresse IP du réseau et une des valeurs de destination de la table de routage. Le routeur doit donc identifier les bits de l'adresse IP qui représentent le réseau et ceux qui représentent l'hôte. Le routeur consulte le masque de sous-réseau attribué à chaque route potentielle dans la table. Le routeur applique chaque masque de sous-réseau à l'adresse IP de destination dans le paquet. L'adresse réseau ainsi produite est ensuite comparée à l'adresse réseau de la route dans la table. En cas de correspondance, le paquet est transféré à l'interface ou à la passerelle appropriée. Lorsqu'une adresse réseau correspond à plusieurs routes dans la table de routage, le routeur utilise la route qui présente la correspondance d'adresse réseau la plus spécifique ou la plus longue. On trouve ainsi parfois plusieurs routes vers le réseau de destination. Dans ce cas, des règles de protocole de routage déterminent la route à emprunter. Si aucune des entrées de routes ne correspond, le routeur dirige le message vers la passerelle spécifiée par la route par défaut, le cas échéant. Sinon, le paquet est abandonné.
Sur un routeur Cisco, la commande IOS « show ip route » affiche les routes contenues dans la table de routage. Plusieurs types de routes peuvent apparaître dans la table de routage. Routes connectées directement à la mise sous tension du routeur, les interfaces configurées sont activées. À mesure qu'elles deviennent opérationnelles, le routeur stocke les adresses réseau locales directement connectées en tant que routes connectées dans la table de routage. [8][9]

1.7.1.1 Routes statiques

Un administrateur réseau peut configurer manuellement une route statique vers un réseau donné. Une route statique ne change que lorsque l'administrateur la reconfigure manuellement. Ces routes sont identifiées par le préfixe **S** dans la table de routage. [3] [4]

1.7.1.2 Routes à mise à jour dynamique ou routes dynamiques

Les routes dynamiques sont créées et gérées automatiquement par les protocoles de routage. Les protocoles de routage échangent des informations de routage avec les autres routeurs du réseau. Les routes à mise à jour dynamique sont identifiées dans la table de routage à l'aide du préfixe

correspondant au type de protocole de routage utilisé pour les créer. Par exemple, R signifie RIP : Routing Information Protocol et O désigne OSPF (Open Shortest Path First). [4] [8]

1.7.1.3 Route par défaut

La route par défaut est un type de route statique qui spécifie une passerelle à utiliser lorsque la table de routage ne contient pas de chemin vers le réseau de destination. Il est courant que les routes par défaut pointent vers le routeur suivant dans le chemin vers le FAI (Fournisseur d'Accès Internet). Lorsqu'un sous-réseau ne possède qu'un seul routeur, celui-ci devient automatiquement la passerelle par défaut, car tout le trafic réseau à destination et en provenance de ce réseau local n'a pas d'autre possibilité que de transiter par ce routeur. Les tables de routage ne contiennent pas d'informations de bout en bout sur la totalité du chemin séparant le réseau source du réseau de destination. Elles ne contiennent que des informations relatives au tronçon suivant de ce chemin. Le tronçon suivant est en principe un réseau directement connecté dans la table de routage. Dans le cas d'une route statique, le tronçon suivant peut être une adresse IP, à condition qu'elle soit accessible par ce routeur. Le message est ensuite transmis à un routeur directement connecté à l'hôte de destination, puis envoyé. Les informations de routage échangées par tous les routeurs intermédiaires sur un chemin se présentent sous la forme d'adresses réseau, et non d'hôtes particuliers. C'est seulement au niveau du dernier routeur que l'adresse de destination de la table de routage pointe vers un ordinateur hôte, plutôt que vers un réseau. [10] [11]

1.7.2 Protocoles de routage

Les routes peuvent changer très rapidement. Des problèmes de câbles et de pannes matérielles peuvent rendre certaines destinations inaccessibles via l'interface désignée. Les routeurs doivent disposer d'un moyen pour mettre rapidement à jour les routes dont les changements ne dépendent pas des administrateurs. Les routeurs utilisent des protocoles de routage pour gérer dynamiquement les informations reçues depuis leurs propres interfaces et depuis d'autres routeurs. Le procédé qu'utilise un protocole de routage pour déterminer la meilleure route vers un réseau de destination s'appelle un algorithme de routage. Il existe deux classes principales d'algorithmes de routage : vecteur de distance et état de liens. Chaque type de protocole détermine différemment la route la plus appropriée vers un réseau de destination.

Dès que la topologie d'un réseau change pour cause de reconfiguration ou de panne, les tables de routage de tous les routeurs doivent illustrer la nouvelle topologie. Lorsque tous les routeurs d'un

réseau ont mis à jour leurs tables conformément à la nouvelle route, on dit que les routeurs ont convergé. L'algorithme de routage utilisé est très important pour le routage dynamique. Pour que deux routeurs échangent des routes, ils doivent utiliser le même protocole de routage et, par conséquent, le même algorithme de routage. L'algorithme de routage à vecteur de distance transmet régulièrement des copies de table de routage d'un routeur à l'autre. Ces mises à jour régulières entre les routeurs servent à communiquer les modifications topologiques. L'algorithme à vecteur de distance évalue les informations de route qu'il reçoit des autres routeurs, sur deux critères de base :[10]

- Distance : à quelle distance de ce routeur le réseau se trouve-t-il ?
- Vecteur : dans quelle direction le paquet doit-il être envoyé pour atteindre ce réseau ?

L'élément de distance d'une route est exprimé en termes de coût, ou de mesure, pouvant prendre les formes suivantes :

- Nombre de sauts ;
- Frais d'administration ;
- Bande passante ;
- Vitesse de transmission ;
- Probabilité de retard ;

1.8 Les équipements de bases des réseaux informatiques

Un réseau local est composé de nombreux types d'équipement. Ces derniers sont appelés des composants matériels du réseau local. Certains des composants matériels les plus utilisés pour les réseaux locaux sont les suivants :[2]

- Les unités hôtes
- Le commutateur
- Le routeur

1.8.1 Les unités hôtes

Les unités directement connectées à un segment de réseau sont appelées hôtes. Ces hôtes peuvent être des ordinateurs, des clients, des serveurs, des imprimantes, des scanneurs ainsi que de nombreux autres types d'équipements.

1.8.2 Commutateur

Le commutateur est donc un périphérique plus sophistiqué que le concentrateur, le commutateur conserve une table des adresses MAC des ordinateurs connectés à chacun de ses ports. Lorsqu'une trame arrive sur un port, le commutateur compare les données d'adresse de la trame à sa table d'adresses MAC. Il détermine alors quel port utilisé pour transférer la trame.

1.8.3 Routeur

Le routeur est un équipement spécialisé qui joue un rôle clé dans le fonctionnement d'un réseau de données. Les routeurs sont principalement chargés de l'interconnexion des réseaux en déterminant le meilleur chemin pour envoyer des paquets et transférer ces derniers vers leur destination.
Ils effectuent aussi le transfert de paquets en obtenant des informations sur les réseaux distants et en gérant les informations de routage. En plus de cela il est la jonction, ou intersection, qui relie plusieurs réseaux IP. [2]

1.9 Le protocole VLAN (Virtual LAN)

Un VLAN(Virtual Local Area Network) ou en français Réseau Virtuel est un réseau local regroupant un ensemble de machines de façon logique et non physique. Les unités ou les utilisateurs d'un VLAN peuvent être regroupés par fonction, service, application, etc., et ce, quel que soit le segment physique où ils se trouvent. Un VLAN crée un domaine de broadcast unique qui n'est pas limité à un segment physique et qui est traité comme un sous-réseau. La configuration d'un VLAN est effectuée, par logiciel, dans le commutateur. Les VLAN ont été uniformisés conformément à la spécification IEEE 802.1Q. Il subsiste cependant des variantes d'implémentation d'un constructeur à l'autre. [4]

1.10 Adressage IP et masque de réseau

Une adresse IP est une adresse 32 bits, généralement notée sous forme de 4 nombres entiers séparés par des points. On distingue en fait deux parties dans l'adresse IP :

- Une partie des nombres à gauche désigne le réseau est appelée ID de réseau
- Les nombres de droite désignent les ordinateurs de ce réseau est appelée ID d'hôte

Le masque est un séparateur entre la partie réseau et la partie machine d'une adresse IP, compose de quatre octet. Les adresses IP sont séparées en plusieurs classes :

- Les adresses de Classe A : 0 à 127 en décimal,

- Les adresses de Classe B : 128 à 191 en décimal,
- Les adresses de Classe C : 192 à 223 en décimal,
- Les adresses de Classe D : 224 à 239 en décimal,
- Les adresses de Classe E : 240 à 255 en décimal.

L'ICANN (Internet Corporation for Assigned Names and Numbers) a réserve une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à internet sans risquer de créer des conflits d'adresses IP sur le réseau des réseaux. Il s'agit des adresses suivantes :

- Adresses IP privées de classe A : 10.0.0.1 à 10.255.255.254, permettant la création de vastes réseaux privés comprenant des milliers d'ordinateurs,
- Adresses IP privées de classe B : 172.16.0.1 à 172.31.255.254, permettant de créer des réseaux privés de taille moyenne,
- Adresses IP privées de classe C : 192.168.0.1 à 192.168.255.254, pour la mise en place de petits réseaux privés. [1] [2]

1.11 Conclusion

Ce chapitre vient de décrire les types de réseaux, les supports de transmission ainsi que les composants matériels qui les constituent. Le chapitre suivant va aborder les considérations générales sur la VoIP.

CHAPITRE 2
GENERALITES SUR LA VOIP

2.1 Introduction

La voix sur IP constitue actuellement l'évolution la plus importante du domaine des Télécommunications. La transmission de la voix sur les réseaux informatiques à commutation de paquets IP constitue aujourd'hui une nouvelle évolution majeure comparable aux précédentes.
L'objectif de ce chapitre est l'étude de cette technologie et de ses différents aspects. On parlera en détail de l'architecture de la VoIP, ses éléments et son principe de fonctionnement. On détaillera également les protocoles utilisés par la VoIP ainsi que leurs principes de fonctionnement y compris leurs avantages et inconvénients.

2.2 Définition

VoIP signifie Voice over Internet Protocol ou Voix sur IP. Comme son nom l'indique, laVoIP permet de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur Internet. En effet, la voix sur IP est le transport de la parole sur un réseau IP de type privé (intranet/extranet).

2.3 Architecture de la VoIP

La VoIP étant une nouvelle technologie de communication n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les deux principaux protocoles utilisés sont H.323, SIP.

La topologie d'un réseau de téléphonie IP 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.

De façon générale, la topologie d'un réseau de téléphonie IP comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux.[9][10][11]

- Le routeur : il 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 : il s'agit d'une interface entre le réseau commuté et le réseau IP.
- Le PABX : c'est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur et le réseau RTC. Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.
- Les terminaux : des PCs ou des téléphones VoIP.

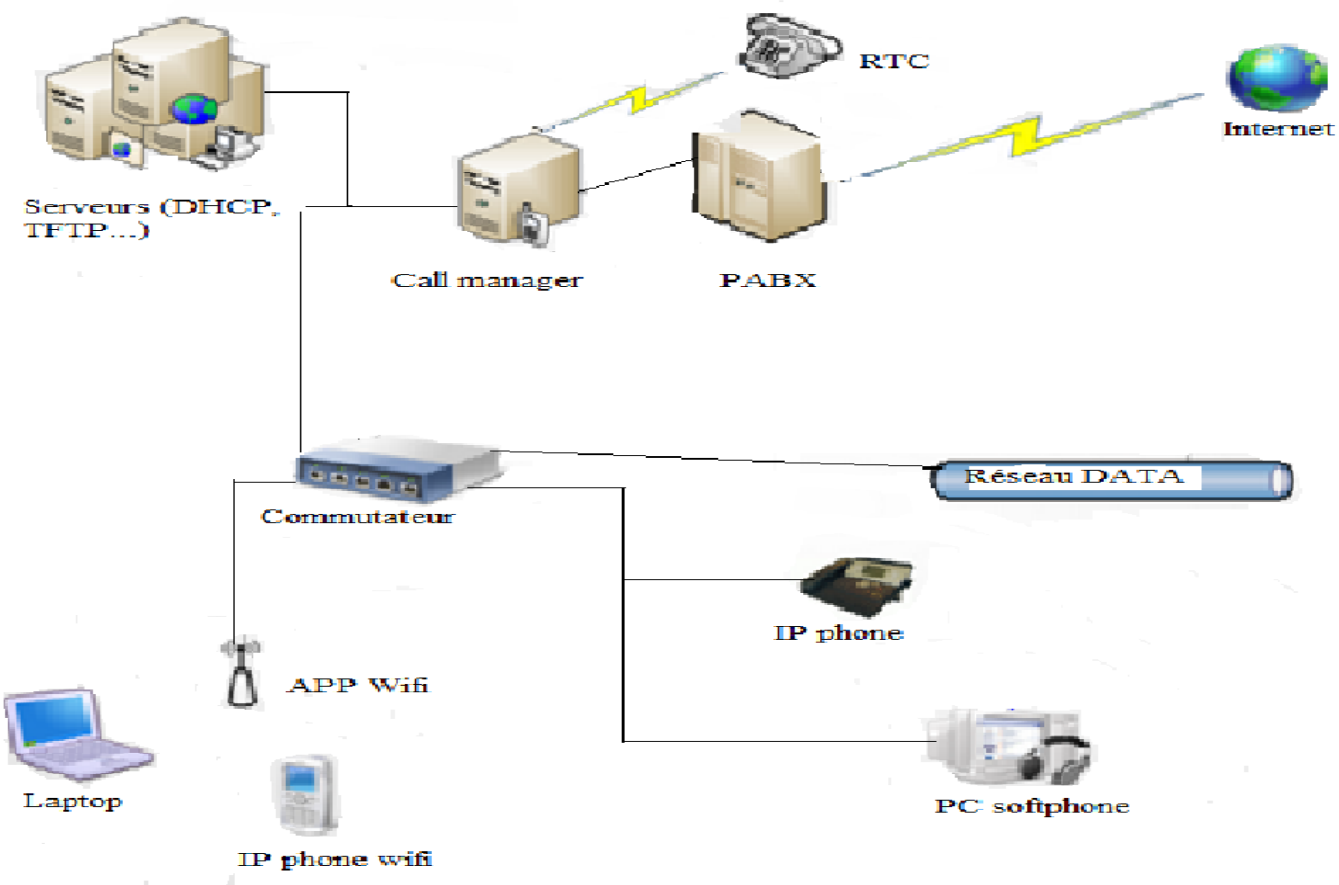


Figure 2.01 : *Architecture de la Voip*

2.4 Concept de la VoIP

Il est nécessaire que le réseau soit bien configuré du début à la fin pour supporter les applications sensibles aux métriques des réseaux de paquets, comme c'est le cas en VoIP. Le support adéquat

du trafic de la voix par paquets IP implique une série de protocoles et de fonctions bien réglées pour améliorer la qualité du service.

La topologie se présente comme suit :

Les protocoles VoIP typiquement utilisent RTP (Real Time Protocol) pour transporter le flux de la voix. RTP utilise UDP comme protocole sous-jacent de transport. Le trafic de signalisation des réseaux VoIP généralement utilise TCP comme protocole de transport. La couche IP comprend le routage et l'adressage au niveau du réseau alors que les protocoles du niveau de liaison contrôlent la transmission de l'information sur le média.

RTP et RTCP peuvent utiliser aussi bien le mode Unicast (point à point) que le mode Multicast (multipoint).

Il existe plusieurs protocoles qui peuvent supporter la voix sur IP tel que le H.323, SIP et MGCP.

Les deux protocoles les plus utilisées actuellement dans les solutions VoIP présentes sur le marché sont le H.323 et le SIP.[10]

2.5 Le protocole H323

Avec le développement du multimédia sur les réseaux, il est devenu nécessaire de créer des protocoles qui supportent ces nouvelles fonctionnalités, telles que la visioconférence : l'envoi de son et de vidéo avec un souci de données temps réel. Le protocole H.323 est l'un d'eux. H.323 est un protocole de communication englobant un ensemble de normes utilisées pour l'envoi de données audio et vidéo sur Internet. Il existe depuis 1996 et a été initié par l'ITU (International Communication Union), un groupe international de téléphonie qui développe des standards de communication. Concrètement, il est utilisé dans des équipements tels que les routeurs Cisco. H323 traite également de l'interfaçage entre le LAN et les autres réseaux.

Plus qu'un protocole, H.323 ressemble davantage à 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 que l'on envoie pour demander d'être mis en relation avec une autre personne, qui indiquent que la ligne est occupée, que le téléphone sonne… Cela comprend aussi les messages que l'on envoie pour signaler que tel téléphone est connecté au réseau et peut être joint de telle manière. En H.323, la signalisation s'appuie sur le protocole

RAS(Registration Admission Status) pour l'enregistrement et l'authentification, et 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 qu'on va s'échanger. Il est important que les téléphones (ou systèmes) parlent un langage commun s'ils veulent se comprendre. Il peut s'agir du codec le moins gourmand en bande passante ou de celui qui offre la meilleure qualité. Le protocole utilisé pour la négociation de codec est le H.245

Le transport de l'information s'appuie sur le protocole RTP (Real Time Protocol) qui transporte la voix, la vidéo ou les données numérisées par les codecs. On peut aussi utiliser les messages RTCP (Real Control Time Protocol) pour faire du contrôle de qualité, voir demander de renégocier les 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 Reservation 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.[10][11][12]

2.5.1 Les équipements du protocole

Les équipements du protocole H323 se repose sur quatre composants principaux : les terminaux, les Gateways, les Gatekeepers et les MCU (Mutlipoint Control Units) [13]

2.5.1.1 Le terminal

Le terminal peut être soit un téléphone, soit un ordinateur muni d'une carte son et d'un micro, soit d'un appareil tournant sur le modèle H.323 et exécutant des applications audio. Eventuellement le terminal peut être doté d'un système de transmission d'images et de données mais ce n'est pas obligatoire. Cet appareil joue un rôle clef dans la VoIP car, c'est à partir de lui que sont émises et reçues les conversations d'utilisateurs. Ainsi donc, le premier rôle du standard H.323 est de permettre les échanges entre les terminaux.

Le fonctionnement du terminal multimédia réside en ce qu'il peut envoyer et recevoir des messages multimédias. Il est ainsi doté d'une couche protocolaire d'application audio et vidéo.

Cette couche représente l'interface de l'application vue par l'utilisateur sur le terminal. Elle repose sur un ensemble de codecs audio et vidéo qui sont des standards de compression/décompression et d'encodage/décodage.
Le transport des informations multimédia issues du terminal est assuré par l'intermédiaire du protocole RTP et ensuite par la couche transport et l'interface réseau.

2.5.1.2 Le Gateway

Le Gateway est l'appareil qui permet d'interconnecter deux réseaux dissemblables. Il s'agit d'un nœud sur le LAN. Il traduit et transmet au réseau H.323 vers un réseau non- H.323. Cette traduction s'accomplit par les conversations de protocoles et de medias entre les deux réseaux nécessaires. Un Gateway n'est pas nécessaire s'il s'agit de connecter uniquement des terminaux H.323. La structure du Gateway se compose de deux parties. La première est attachée au réseau de paquets et la seconde au réseau public de commutation (téléphonique). Dans la partie « réseaux par paquets », on retrouve le contrôle de la signalisation H.245 et H.225 dont une partie s'occupe du « call setup & release » et l'autre de RAS vers le Gatekeeper. Les terminaux du coté « réseau par paquet » contactent le Gateway par l'intermédiaire de H.245 (control signaling) et H.225 (call signaling).

2.5.1.3 Le Gatekeeper

Le Gatekeeperest considéré comme le cerveau du réseau H.323. Il s'agit d'un point de focalisation pour tous les appels du réseau H.323. Bien qu'il ne soit pas nécessaire, le Gatekeeper est un objet commode du réseau H.323. C'est celui qui se charge d'autoriser les appels, d'authentifier les utilisateurs, d'établir une comptabilité, de contrôler la bande passante, il peut également fournir des services de routage. Un Gatekeeper administre un ensemble de réseaux de terminaux.

Le Gatekeeper doit obligatoirement s'occuper d'effectuer des conversions d'adresse: les appels originaires d'un réseau H.323 peuvent utiliser un allias pour adresser un autre terminal et de même des appels originaires d'un réseau différent du H.323 et reçus par le Gateway peuvent utiliser une adresse de type téléphone pour adresser un terminal. En plus des conversions, une caractéristique importante du Gatekeeper réside dans ce qu'il gère la fonctionnalité RAS envoyant des messages de confirmation de requête aux clients qui le contactent.

2.5.1.4 Le MCU (multipoint control unit*)*

Le MCU fournit un support pour une conférence entre trois ou plusieurs terminaux. Chacun des terminaux désirant participer à la conversation doit s'enregistrer auprès du MCU. C'est le MCU qui négocie, entre les terminaux, les codecs à utiliser durant la conférence. Il se charge également de signaler à chacun des terminaux s'il s'agit d'une audio conférence ou d'une vidéo conférence.

La figure 2.02 illustre les composants d'un protocole H323 [13]

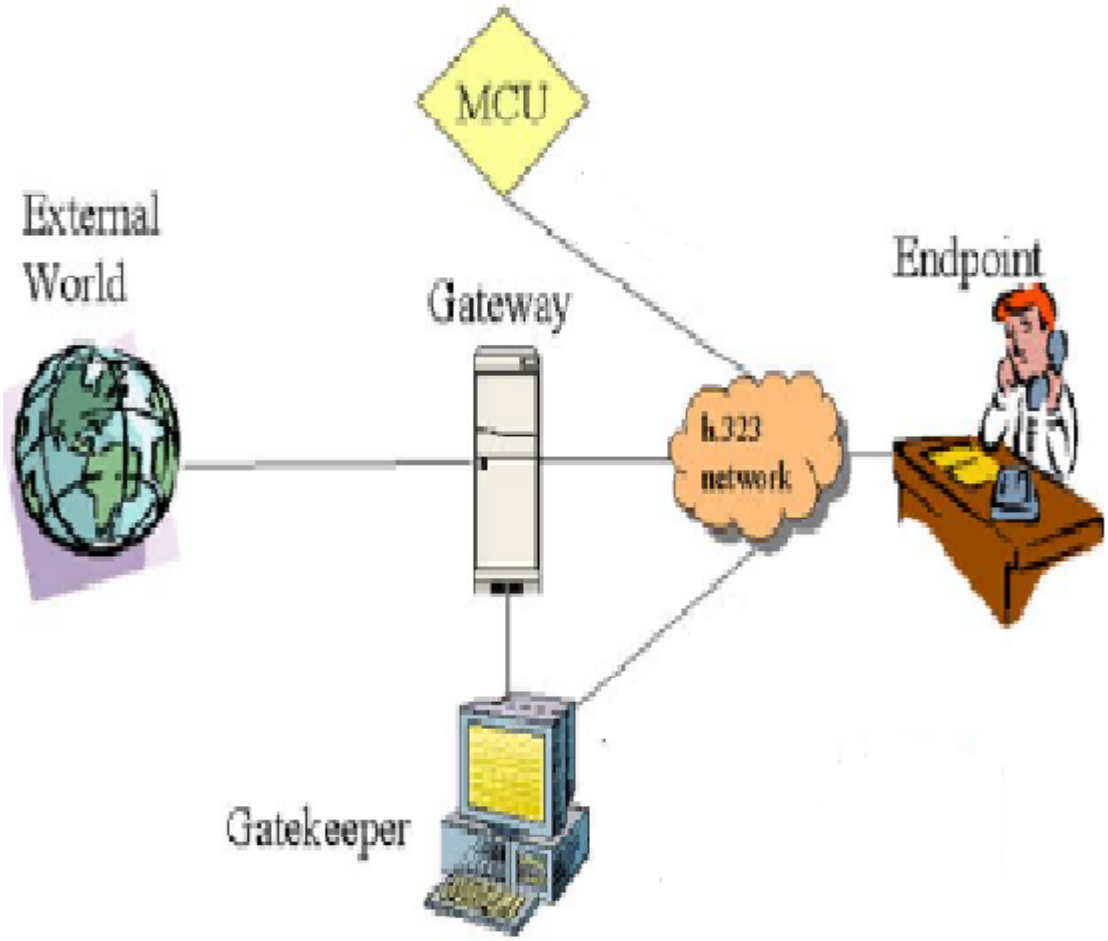


Figure 2.02 : *Les composants d'un protocole H323*

2.5.2 Les avantages du protocole H323

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: H.323 permet aux utilisateurs de ne pas se préoccuper de la manière dont se font les communications, les paramètres (les codecs, le débit…) sont négociés de manière transparente.
- Support multipoint: H.323 supporte des conférences entre trois terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée.
- 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.
- Gestion de la bande passante: Le trafic audio et vidéo est un grand consommateur de ressources 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.[12][13]

2.5.3 Les inconvénients

- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence de service de téléphonie et d'internet, ainsi qu'un manque de modularité et de souplesse
- Le protocole H323 comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité. [13]

2.6 Le protocole d'initiation des sessions SIP (Session Initiation Protocol)

Session Initiation Protocol est un protocole publié par l'I.E.T.F (Internet Engireening Task Force) sous la RFC (Request For Comments) 2543 en mars 1999. La RFC 2543 présente la source d'information la plus complète du sujet.

Selon la RFC 2543, le protocole d'initiation de session SIP est un protocole de signalisation appartenant à la couche application du modèle OSI. Son rôle est d'ouvrir, modifier et libérer les sessions ou appels ouverts entre un ou plusieurs utilisateurs. 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 fonctionne selon une architecture client-serveur, le client émettant des requêtes et le serveur exécutant en réponse les actions sollicitées par le client. Pour ouvrir une session, l'utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de s'accorder sur la compatibilité de leur média. SIP peut relier des stations mobiles en transmettant ou redirigeant les requêtes vers la position courante de la station appelée.[9]

2.6.1 Architecture de SIP

Dans un système SIP on trouve deux types de composantes, les agents utilisateurs (UAS, UAC) et un réseau de serveurs (Registrar, Proxy)

- L'UAS (User Agent Server) représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue. Et elle renvoie une réponse au nom de l'utilisateur.
- L'U.A.C (User Agent Client) représente l'agent de la partie appelante. C'est une application de type client qui initie les requêtes.
- Le Registrarest un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données (figure 4).
- Les URI SIP sont très similaires dans leur forme à des adresses email : sip:utilisateur@domaine.com. Généralement, des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI.
- Un Proxy SIP sert d'intermédiaire entre deux User Agents qui ne connaissent pas leurs emplacements respectifs (adresse IP). En effet, l'association URI-Adresse IP a été stockée préalablement dans une base de données par un Registrar. Le Proxy peut donc interroger cette base de données pour diriger les messages vers le destinataire.[14]

La figure 2.03 nous montre les entités d'un réseau SIP

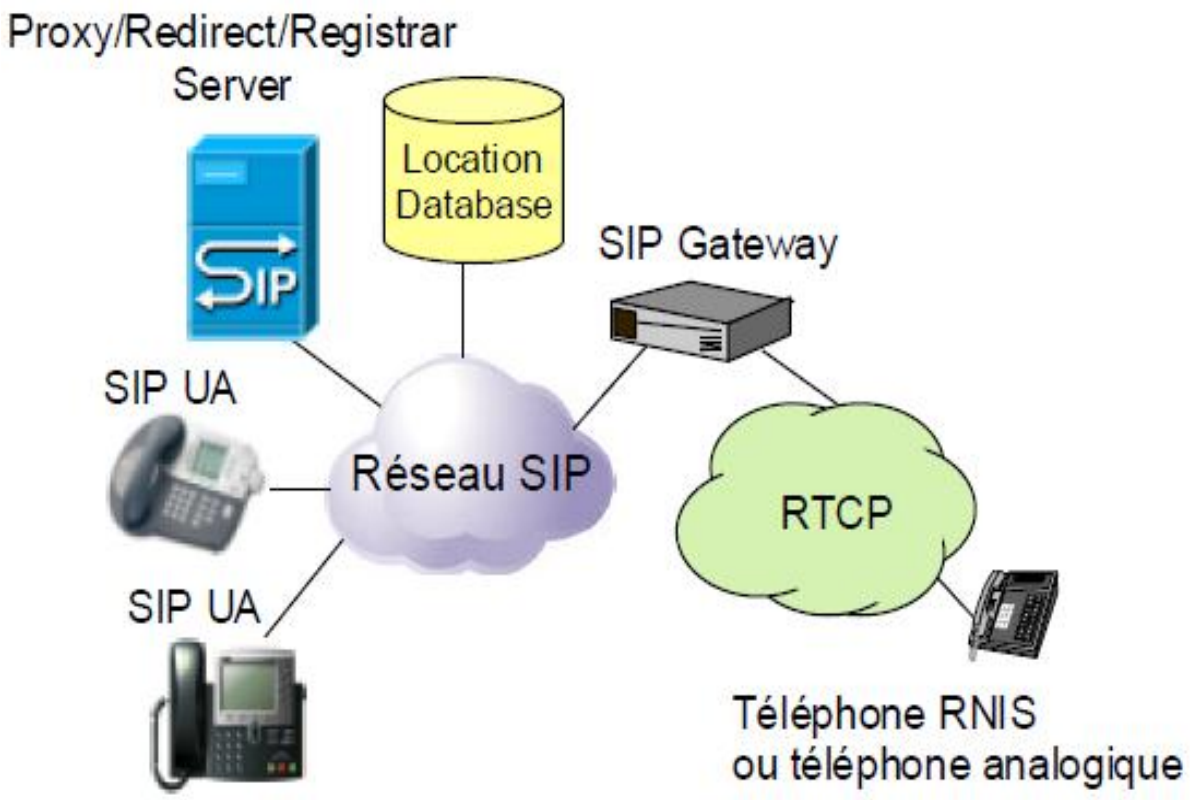


Figure 2.03 : *Les entités d'un réseau SIP*

2.6.2 Le principe de fonctionnement

2.6.2.1 Fixation d'un compte SIP

Il est important de s'assurer que la personne appelée soit toujours joignable. Pour cela, un compte SIP sera associé à un nom unique. Par exemple, si un utilisateur d'un service de voix sur IP dispose d'un compte SIP et que chaque fois qu'il redémarre son ordinateur, son adresse IP change, il doit cependant toujours être joignable. Son compte SIP doit donc être associé à un serveur SIP (proxy SIP) dont l'adresse IP est fixe. Ce serveur lui allouera un compte et il permettra d'effectuer ou de recevoir des appels quelques soit son emplacement. Ce compte sera identifiable via son nom (ou pseudo).[15] [16]

2.6.2.2 Changements des caractéristiques durant les sessions

Un utilisateur doit pouvoir modifier les caractéristiques d'un appel en cours. Par exemple, un appel initialement configuré en (voix uniquement) peut être modifié en (voix + vidéo).

2.6.2.3 Différents mode de communication

Avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci.

- Mode Point à point: on parle dans ce cas-là d'unicast qui correspond à la communication entre deux machines.
- Mode diffusif : on parle dans ce cas-là de multicast (plusieurs utilisateurs via une unité de contrôle MCU – Multipoint Control Unit).
- Combinatoire : combine les deux modes précédents. Plusieurs utilisateurs interconnectés en multicast via un réseau à maillage complet de connexion. [16]

2.6.2.4 Gestion des participants

Durant une session d'appel, de nouveaux participants peuvent joindre les participants d'une session déjà ouverte en participant directement, en étant transférés ou en étant mis en attente (cette particularité rejoint les fonctionnalités d'un PABX par exemple, où l'appelant peut être transféré vers un numéro donné ou être mis en attente).

2.6.2.5 Adressage

L'objectif de l'adressage est de localiser les utilisateurs dans un réseau. C'est une des étapes indispensables pour permettre à un utilisateur d'en joindre un autre.

Les utilisateurs disposant d'un numéro (compte) SIP disposent d'une adresse ressemblant à une adresse mail (sip:numéro@serveursip.com). Le numéro SIP est unique pour chaque utilisateur. [16]

2.6.2.6 Requête SIP

Le protocole SIP repose sur un modèle Requête/Réponse. Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. La liste des requêtes échangées est la suivante :

- Invite : cette requête indique que l'application (ou utilisateur) correspondante à l'url SIP spécifié est invité à participer à une session. Le corps du message décrit cette session (par

exemple : média supportés par l'appelant). En cas de réponse favorable, l'invité doit spécifier les médias qu'il supporte.

- Ack : cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête Invite.
- Option : un proxy server en mesure de contacter l'UAS (terminal) appelé, doit répondre à une requête Options en précisant ses capacités à contacter le même terminal.
- Bye: cette requête est utilisée par le terminal de l'appelé à fin de signaler qu'il souhaite mettre un terme à la session.
- Cancel : cette requête est envoyée par un terminal ou un proxy server à fin d'annuler une requête non validée par une réponse finale comme, par exemple, si une machine ayant été invitée à participer à une session, et ayant accepté l'invitation ne reçoit pas de requête Ack, alors elle émet une requête Cancel.
- Register : cette méthode est utilisée par le client pour enregistrer l'adresse listée dans l'URL par le serveur auquel il est relié. [15]

2.6.2.7 Les réponses SIP

Après réception et traitement d'une requête, un agent ou un serveur SIP génère un message de réponse (succès ou échec du traitement). Ces réponses sont codées par une séquence de trois chiffres, où le premier est un code de classe. Il existe 6 classes de réponses qui sont les suivantes :

- 1xx = Information - La requête a été reçue et continue à être traitée.
- 2xx = Succès - L'action a été reçue avec succès, comprise et acceptée.
- 3xx = Redirection - Une autre action doit être menée afin de valider la requête.
- 4xx = Erreur du client - La requête contient une syntaxe erronée ou ne peut pas être traitée par ce serveur.
- 5xx = Erreur du serveur - Le serveur n'a pas réussi à traiter une requête apparemment correcte.
- 6xx = Echec général - La requête ne peut être traitée par aucun serveur. [15]

2.6.3 Exemple du scénario de communication

La figure 2.04 représente une communication qui reflète la simplicité d'utilisation du protocole SIP. Quatre étapes seulement suffisent pour mettre en relation les deux utilisateurs

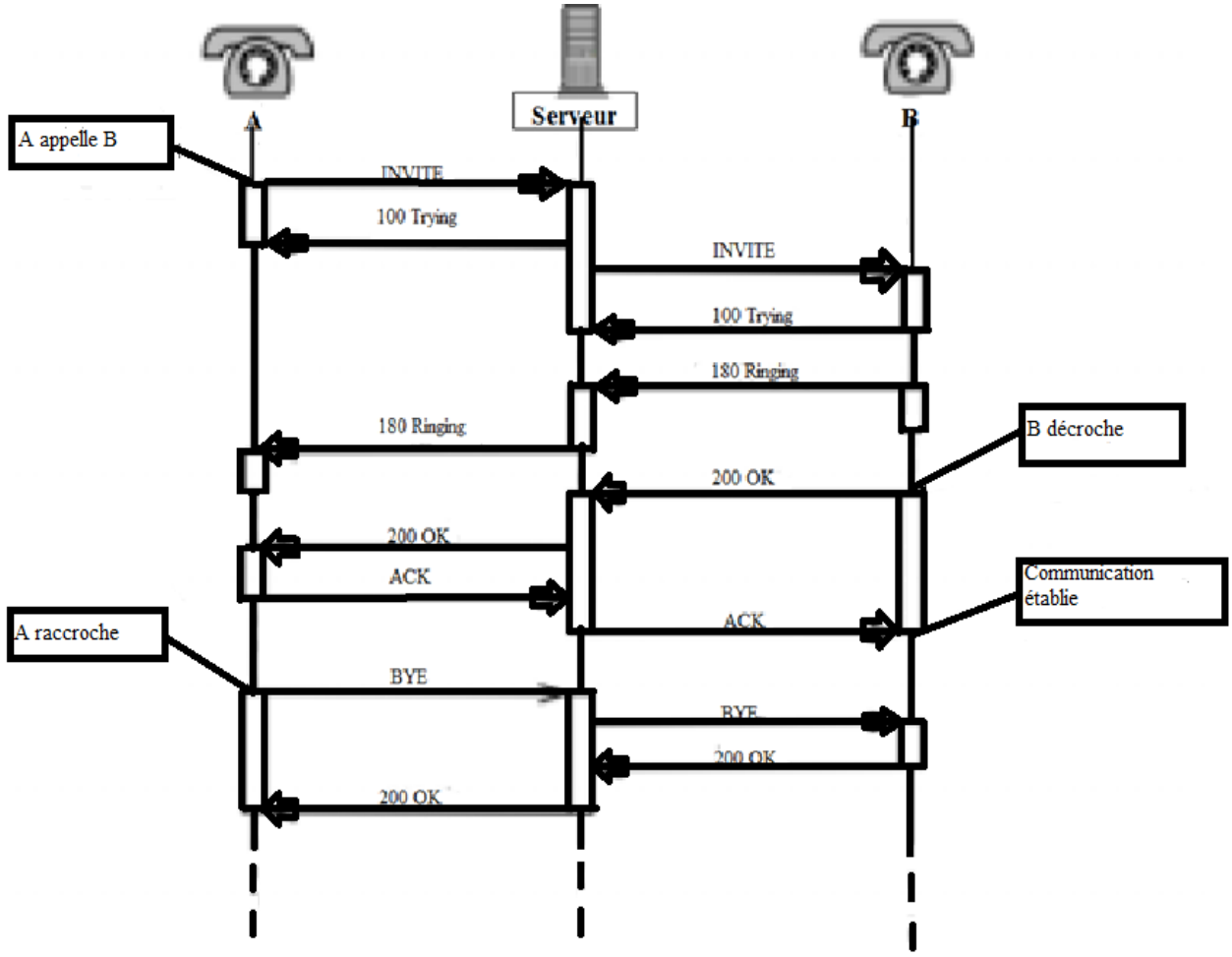


Figure 2.04 : ***Scénario de communication d'un système VoIP à partir du protocole SIP***

A compose sur son terminal l'adresse SIP de B. Cette dernière n'est pas nécessairement une adresse IP, mais peut être un identifiant qu'il faut résoudre. Un message d'invitation (requête INVITE) est envoyé de l'UAC de A vers son serveur proxy SIP. Le serveur proxy informe A qu'il prend en charge la requête et tente de la mettre en relation.

La réponse temporaire 100 TRYING indique à cette dernière que le message a été reçu et qu'il est en cours de traitement ;

Routage du message d'invitation. Le serveur proxy de A transmet l'invitation au serveur proxy de B après l'avoir localisé.

Le serveur proxy de B informe le serveur proxy de A (par un message de réponse temporaire 100 TRYING) de la réception de la requête et de la tentative d'initialisation.

Le terminal de B sonne,(éventuellement un softphone) et reçoit l'invitation et la fait connaître à l'utilisateur B, le plus souvent par une sonnerie. En parallèle, il indique à son proxy (par un message 180 RINGING) que l'appel est en train d'être notifié à B et que la communication est en attente de son acceptation.

B répond au téléphone. On suppose le cas où B a choisi de répondre à l'appel. À l'instant où elle décroche, l'UAS retourne à l'UAC un message 200 OK pour l'informer que l'appel est accepté. À ce stade, la communication n'a pas encore débuté, et aucun son n'est transmis ;

Le terminal A confirme les paramètres d'appel. En tenant compte des capacités prises en charge par les correspondants, le terminal A envoie un message d'acquittement ACK qui spécifie les paramètres définitifs à utiliser lors de cette session. Notons que le message d'acquittement peut passer directement d'un interlocuteur à l'autre, sans transiter par les serveurs proxy. À ce stade, chacun des utilisateurs a pu apprendre la localisation exacte de son interlocuteur, et il n'est donc plus nécessaire de recourir aux serveurs proxy. Toutes les transactions qui suivent sont effectuées directement, de poste utilisateur à poste utilisateur.

À la réception de ce message, la communication entre les interlocuteurs peut débuter. Tous ces échanges n'ont réclamés que quelques millisecondes, imperceptibles pour les intervenants.

Globalement, on retrouve dans cet appel, les trois phases fondamentales de l'appel direct entre les correspondants :

- Requête INVITE : invitation de l'appelant.
- Réponse 200 OK : acceptation par l'appelé [15]

2.6.4 Les avantages du protocole SIP

- SIP est un protocole plus rapide : 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.

- Le nombre d'en-têtes est limité (36 au maximum et en pratique, moins d'une dizaine d'en-têtes sans utilisées simultanément), ce qui allège l'écriture et la lecture des requêtes et réponses.
- SIP est un protocole indépendant de la couche transport : il peut aussi bien s'utiliser avec TCP que UDP[14]

2.6.5 Les inconvénients du protocole SIP

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. [14]

2.7 Comparaison entre le protocole H323 et le protocole SIP

Les deux protocoles SIP et H323 représentent les standards définis jusqu'à présent pour la signalisation à propos de la téléphonie sur Internet .Ils présentent tous les deux des approches différentes pour résoudre un même problème. H323 est basé sur une approche traditionnelle du réseau à commutation de circuits. Quant à SIP, il est plus léger car basé sur une approche similaire au protocole HTTP.

Tous les deux utilisent le protocole RTP comme protocole de transfert des données multimédia.

Au départ, H323 fut conçu pour la téléphonie sur les réseaux sans QoS (Qualité de Service), mais on l'adopta pour qu'il prenne en considération l'évolution complexe de la téléphonie sur internet.

Pour donner une idée de la complexité du protocole H323 par rapport à SIP, H323 est défini en un peu plus de 700 pages et SIP quand à lui en moins de 200 pages. La complexité de H323 provient encore du fait de la nécessité de faire appel à plusieurs protocoles simultanément pour établir un service, par contre SIP n'a pas ce problème.

SIP ne requiert pas de comptabilité descendante, c'est un protocole horizontal qui est le contraire de H323 : Les nouvelles versions de H323 doivent tenir compte des anciennes versions pour continuer à fonctionner. Ceci entraîne pour H323 de traîner un peu plus de codes pour chaque version.

H323 ne reconnaît que les Codecs standardisés pour la transmission des données multimédias proprement dit alors que SIP, au contraire, peut très bien en reconnaître d'autres. Ainsi, on peut dire que SIP est plus évolutif que H323.

En résumé, La simplicité, la rapidité et la légèreté d'utilisation, tout en étant très complet, du protocole SIP sont autant d'arguments qui pourraient lui permettre de convaincre les investisseurs. De plus, ses avancées en matière de sécurisation des messages sont un atout important par rapport à ses concurrents.[17]

2.8 Les protocoles de transports

2.8.1 Le protocole de transport temps réel RTP

2.8.1.1 Description générale du 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.[16]

2.8.1.2 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. 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 ;
- Identifier 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.

2.8.1.3 Avantages et inconvénients 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. [14]

2.8.2 Le protocole de contrôle en temps réel RTCP

2.8.2.1 Description générale du 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. [11][12]

2.8.2.2 Principales fonctions du protocole RTCP

Le protocole RTCP présente les fonctions suivantes :

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

Le protocole RTCP 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.

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. [11] [12]

2.9 Avantages de le VoIP

2.9.1 Réduction des coûts

En effet le trafic véhiculé à travers le réseau RTC est plus couteux que sur un réseau IP. Réductions importantes pour des communications internationales en utilisant la VoIP, ces réductions deviennent encore plus intéressantes dans la mutualisation voix/données du réseau IP intersites (WAN). Dans ce dernier cas, le gain est directement. [11]

2.9.2 Standards ouverts

La VoIP n'est plus uniquement H323, mais un usage multi-protocoles selon les besoins de services nécessaires. Par exemple, H323 fonctionne en mode égale à égale alors que MGCP fonctionne en mode centralisé. Ces différences de conception offrent immédiatement une différence dans l'exploitation des terminaisons considérées. [11]

2.9.3 Un réseau voix, vidéo et données (à la fois)

Grace à l'intégration de la voix comme une application supplémentaire dans un réseau IP, ce dernier va simplifier la gestion des trois applications (voix, réseau et vidéo) par un seul transport IP. Une simplification de gestion, mais également une mutualisation des efforts financiers vers un seul outil. [11] [14]

2.10 Les inconvénients de la VoIP

2.10.1 Fiabilité et qualité sonore

Un des problèmes les plus importants de la téléphonie sur IPest la qualité de la retransmission qui n'est pas encore optimale. En effet, des désagréments tels la qualité de la reproduction de la voix

du correspondant ainsi que le délai entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être extrêmement problématiques. De plus, il se peut que des morceaux de la conversation manquent (des paquets perdus pendant le transfert) sans être en mesure de savoir si des paquets ont été perdus et à quel moment. [12] [14]

2.10.2 Dépendance de l'infrastructure technologique et support administratif exigeant

Les centres de relations IP peuvent être particulièrement vulnérables en cas d'improductivité de l'infrastructure. Par exemple, si la base de données n'est pas disponible, les centres ne peuvent tout simplement pas recevoir d'appels. La convergence de la voix et des données dans un seul système signifie que la stabilité du système devient plus importante que jamais et l'organisation doit être préparée à travailler avec efficience ou à encourir les conséquences.

2.10.3 Vol

Les attaquants qui parviennent à accéder à un serveur VoIP peuvent également accéder aux messages vocaux stockés et même au service téléphonique pour écouter des conversations ou effectuer des appels gratuits aux noms d'autres comptes.

2.10.4 Attaque de virus

Si un serveur VoIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au réseau téléphonique. Le virus peut également infecter d'autres ordinateurs connectés au système. [12] [14]

2.11 Conclusion

Comme on a pu le voir tout au long de ce chapitre, Actuellement il est évident que la VoIP va continuer à évoluer. La téléphonie IP est une bonne solution en matière d'intégration, fiabilité et de coût.

Toutefois, dans le chapitre suivant, nous allons parler des vulnérabilités de la VoIP mais également de sa sécurisation.

CHAPITRE 3
SECURISATION DE LA VoIP

3.1 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.

3.2 Les menaces de la VoIP

Une menace est le résultat d'une attaque ou d'une action involontaire ou négligente qui compromet la sécurité du réseau VoIP. Des sources de menaces potentielles sont donc des personnes malintentionnées ou les utilisateurs normaux. Les sources de menaces peuvent être internes ou externes au réseau VoIP.
Que ce soit le H.323 ou le SIP, ces deux protocoles ont déjà fait l'objet de failles de sécurité. Les équipements demandent de traiter l'information en IP brute, sans l'appui du protocole TCP et donc sans utiliser la sécurisation SSL. Si les protocoles de voix sur IP peuvent être chiffrés avec IPsec, IPsec n'est pas déployé dans les réseaux d'entreprise, car il est trop complexe.
Les types de menaces les plus fréquentes sont les suivantes. [18] [19]

3.2.1 Déni de service

C'est l'une des attaques les plus répandues, le but étant de rendre le réseau téléphonique inopérant en surchargeant le PABX. L'attaque en déni de service consiste à surcharger le serveur Web de requêtes jusqu'à ce qu'il ne puisse plus suivre et s'arrête. Dès lors, il est envisageable de saturer les réseaux des sociétés équipées en voix sur IP, bloquant ainsi communications internes, externes mais aussi le système d'information. C'est une action volontaire ou involontaire entraînant l'indisponibilité d'un service. Le DoS peut provoquer les points suivants :

- Interruption de la communication en cours
- Empêchement de l'établissement de la communication
- Rendre une communication inaudible
- Epuisement des ressources
- Effacer des messages de la boîte vocale

3.2.2 L'écoute clandestine

Elle est destinée à effacer les messages enregistrés sur la boîte vocale sans l'accord de l'utilisateur légitime de cette boîte vocale.

Cette attaque consiste à écouter l'appel entre l'appelant et l'appelé, au moyen d'un empoisonnement ARP, dans le but de convaincre à la fois le serveur mandataire et les téléphones VoIP des deux utilisateurs, de communiquer avec l'attaquant et non entre eux.

Elle est divisée en quatre catégories ci-après :

- Ecoute de la conversation : interception et reconstruction, enregistrement ou extraction du contenu de conversations téléphoniques.
- Ecoute non autorisé de message de la boîte vocale : accès, reconstruction, enregistrement de message enregistré sur une boîte vocale par un utilisateur non autorisé.
- Obtention d'information sur le contenu de la communication
- Obtention d'information sur les propriétés de la communication

3.2.3 Détournement du trafic

Reroutage de la signalisation ou du contenu d'une communication vers un autre système ou une autre personne sans l'accord des utilisateurs légitimes de la communication. Le détournement est dissimulé des utilisateurs légitimes.

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.

Ce trafic est divisé en deux catégories :

- détournement de l'appel : détournement du flux média d'un appel dans le but d'intercepter, enregistrer ou extraire le contenu.
- détournement de la signalisation : détournement du trafic de signalisation dans le but d'extraire des informations sur le comportement des utilisateurs ou les caractéristiques des communications.

3.2.4 Manipulation de l'identité du contenu

Modification du contenu des messages de signalisation ou du flux média, dans le but de tromper les autres utilisateurs.

Elle se présenté en plusieurs façons :

- Usurpation de l'identité : utilisation de l'identité d'un autre utilisateur dans le but de tromper le récepteur d'un message ou appel. Les utilisateurs sont principalement identifiés par leur « Caller-ID ».
- dissimulation de l'identité : dissimulation du Caller-ID dans le but de ne pas être reconnaissable par d'autres utilisateurs. La dissimulation peut être temporaire (établissement de l'appel) ou permanente (pendant toute la durée de l'appel).
- Modification du contenu de communication

3.2.5 Vol de service

Utilisation d'un service sans avoir à rémunérer son fournisseur ou sans avoir l'autorisation. Cela peut être une :

- tromperie de la taxation ou ;
- une utilisation non autorisée de service : Utilisation d'un service par un utilisateur qui n'a pas d'autorisation pour ce service, en manipulant l'identité ou les droits de l'utilisateur.

3.2.6 Communication non désirée

Possibilité d'établir des communications que le destinataire aimerait filtrer. Bien que certains types de communications soient légaux, le destinataire doit avoir la possibilité d'empêcher des communications non désirées. Cela implique les appels SPAM qui sont un abus du service téléphonique pour l'établissement récurrent de communications non désirées.

3.2.7 Sniffing

Un reniflage (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.

3.2.8 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 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. [18] [19]

3.3 Les vulnérabilités de l'infrastructure hardware

3.3.1 Le téléphone 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
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 ;
- De compromettre la disponibilité du point final. [19]

3.3.2 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.[19]

3.4 Vulnérabilité sur les infrastructures 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 (Opening System). 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 firmware 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.[18][19]

3.5 La sécurisation

En migrant de la téléphonie analogique à une solution de ToIP, de nouvelles failles de sécurité s'ouvrent. De plus, les menaces du réseau IP s'appliquent également à l'environnement de VoIP. Les risques majeurs sont ainsi le détournement de la console d'administration de l'application de voix sur IP, le spam vocal, les attaques par DoS (déni de service) et les écoutes téléphoniques.

Comme toute application susceptible de comporter des vulnérabilités, la VoIP pose nativement des problèmes à plusieurs niveaux. Toutefois, la problématique pour les entreprises est la même que lors du déploiement d'une nouvelle application. Les démarches vont donc consister à étendre la politique de sécurité, et non faire table rase de l'existant".[19][20]

Il existe plusieurs façons de préconiser la sécurisation de la VoIP :

3.5.1 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 à 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. [20]

3.5.2 La sécurité 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 IPsec (IP Security), dont le mécanisme d'échanges de clés est trop lourd. Il est aussi bâti sur le protocole temps réel RTP (Real Time Transport Protocol). Il est donc compatible à la fois avec des protocoles d'initiation de session de voix sur IP tel que SIP (Session Initiation Protocol)

Les principaux services offerts par SRTP sont :

- Rendre confidentielles les données RTP, que ce soit l'en-tête et la charge utile ou seulement la charge utile ;
- Authentifier et vérifier l'intégrité des paquets RTP. L'émetteur calcule une empreinte du message à envoyer, puis l'envoie avec le message même ;
- La protection contre le rejet des paquets. Chaque récepteur tient à jour la liste de tous les indices des paquets reçus et bien authentifiés. [20]

3.5.3 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. Il permet de chiffrer les échanges SIP qui contiennent, par exemple, le nom d'utilisateur, le mot de passe ainsi que le numéro appelé. 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. [19]

3.5.4 Sécuriser l'application

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

- L'utilisation d'une version stable, Il est bien connu que toute application non stable contient 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. [19]

3.5.5 Eviter les fraudes

La fraude peut être limitée par la configuration correcte de la passerelle VoIP vers RTC (Réseau Téléphonique Commuté) ainsi qu'une gestion des droits/classes de service par utilisateur. Les passerelles doivent être configurées pour éviter qu'un utilisateur se connecte directement sans passer par le relais SIP. [19]

3.5.6 Durcir le système d'exploitation

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

- Utiliser un système d'exploitation stable. Les nouvelles versions toujours contiennent des bugs et des failles qui doivent être 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. [20]

3.5.7 Placer les équipements derrière le pare-feu

Les firewalls seront mis en coupure, en amont des serveurs pour éviter le déni de service, et sur les segments critiques. Ils contrôleront que les flux des VLANs sont bien restreints aux protocoles de la VoIP. Les pare-feu supporteront à la fois les protocoles SIP (Session Initiation Protocol) et H.323. [20]

3.6 Conclusion

Dans ce chapitre, il a été question de présenter les différentes vulnérabilités devant lesquelles le déploiement de la voix sur IP fait face. Il existe plusieurs autres attaques qui menacent la sécurité du VoIP, les attaques citées dans ce chapitre sont les plus fameux et courant dans les réseaux VoIP.

Mais il est possible de créer un système VoIP sécurisé en appliquant les bonnes pratiques citées.

CHAPITRE 4
REALISATION D'UN SYSTEME VoIP SOUS CISCO PACKET TRACER

4.1 Introduction

Cisco Packet Tracer est couramment utilisé pour comprendre les différents concepts de mise en réseau avec la simulation, il peut être utilisé pour concevoir un réseau par connexion de différents périphériques réseau et exécutant différents tests de dépannage pour vérifier la connectivité et de communication entre les différents réseaux devices. Ainsi Cisco Packet Tracer peut être utilisée pour comprendre les réseaux informatiques.

Durant ce chapitre, nous essayerons de configurer notre modèle type de système VoIP en utilisant le simulateur «Cisco Packet Tracer», faire aussi les configurations des différents terminaux et routeurs.

4.2 Présentation générale de Cisco Packet Tracer

Le « Cisco Packet Tracer » est un programme puissant de simulation qui permet aux étudiants d'expérimenter le comportement du réseau. En effet, Packet Tracer fournit la simulation, la visualisation, la création, l'évaluation et les capacités de collaboration et facilite l'enseignement et l'apprentissage des technologies complexes.

La figure 4.01 ci-dessous nous présente l'interface du Cisco Packet Tracer.

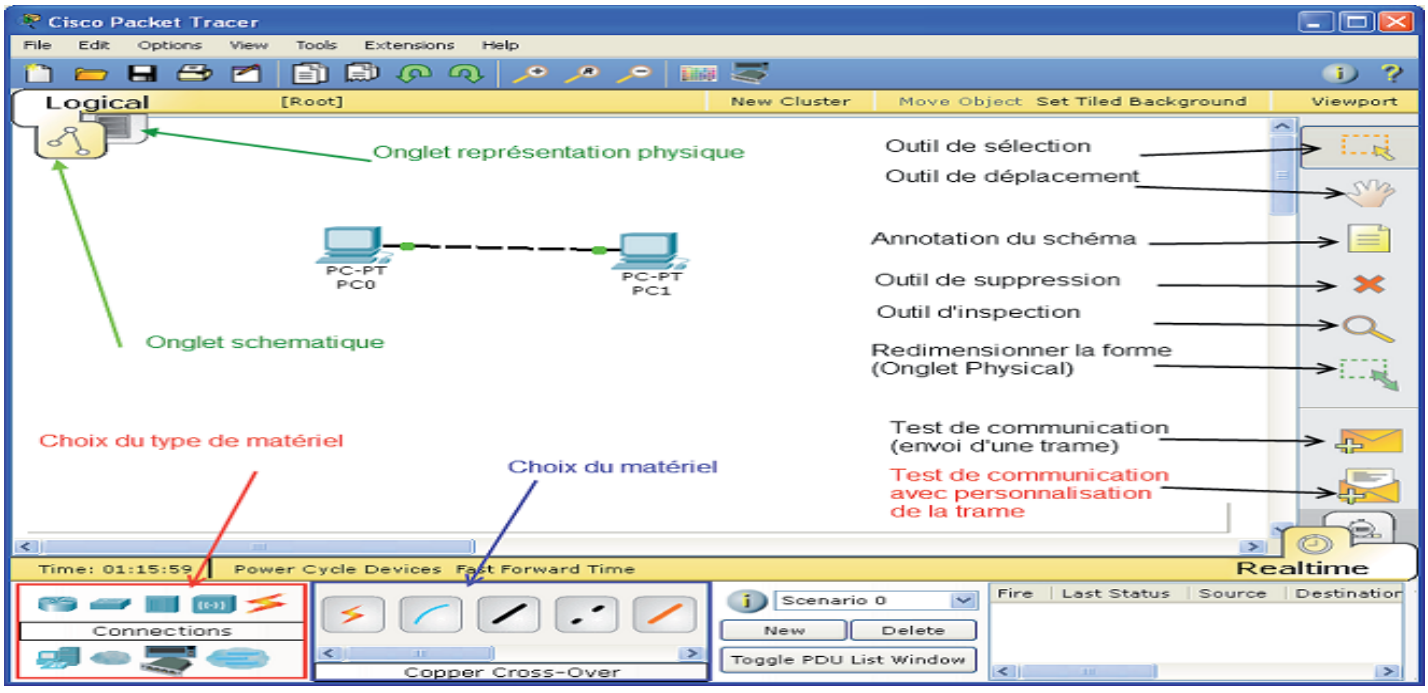


Figure 4.01 : *Ecran principal du Cisco Packet Tracer*

Pour le câblage, on doit utiliser un câble droit pour relier deux appareils différents - comme un téléphone IP et un commutateur, ou un commutateur et un routeur. On doit utiliser un câble croisé pour relier ensemble deux appareils de même type - comme deux ordinateurs ou encore deux commutateurs. [21]

4.2.2 Les principaux protocoles

Ce tableau présente les différents protocoles disponibles dans Packet Tracer selon les couches du modèle OSI.

Couches	Protocoles
Physique	Pas d'objet
Liaison	Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP STP, VTP, DTP, CDP, 802.1q, LACP , … L2 QoS, SLARP, Auto Secure Wifi: simple,WEP, WPA
Réseau	IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, Routage: RIPv1/v2/ng, Multi-Area OSPF, EIGRP, Static Routing Sécurité: Context Based Access Lists, Zone-based policy firewall et intrusion Protection System (sur certain routeur) Multilayer Switching, L3 QoS, NAT
Transport	TCP and UDP, TCP Nagle Algorithm & IP Fragmentation
Session	Pas d'objet
Présentation	Pas d'objet
Application	HTTP, HTTPS, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, Radius, Syslog, …

Tableau 4.01: *Récapitulatifs des principaux protocoles*

4.2.3 Spécification des équipements disponibles

Packet Tracer propose les principaux équipements réseaux composant nos réseaux actuels. Chaque équipement possède une vue physique comprenant des modules à ajouter, une vue configuration pour configurer les principales options via une interface graphique et une vue permettant la configuration via CLI (Command Line Interface).

- Routeur,
- Commutateur Terminaux (ordinateur, portable, serveur, imprimante et téléphone IP),
- Point d'accès Modem,
- Concentrateur.

Sachant que chaque équipement se voit attribuer un certain nombre de modules, permettant d'ajouter soit des ports supplémentaires, soit des nouveaux types de port. Les équipements propriétaires Cisco ont la possibilité de se voir attribuer les nouveaux IOS disponibles sur le site Cisco. [21] [22]

4.3 Présentation de la simulation

Pour la partie simulation, nous avons interconnecté deux sites distants bien distincts qui peuvent se communiquer dont nous allons décrire les configurations effectuées. La figure 4.02 ci-dessous nous montre l'architecture du système à étudier.

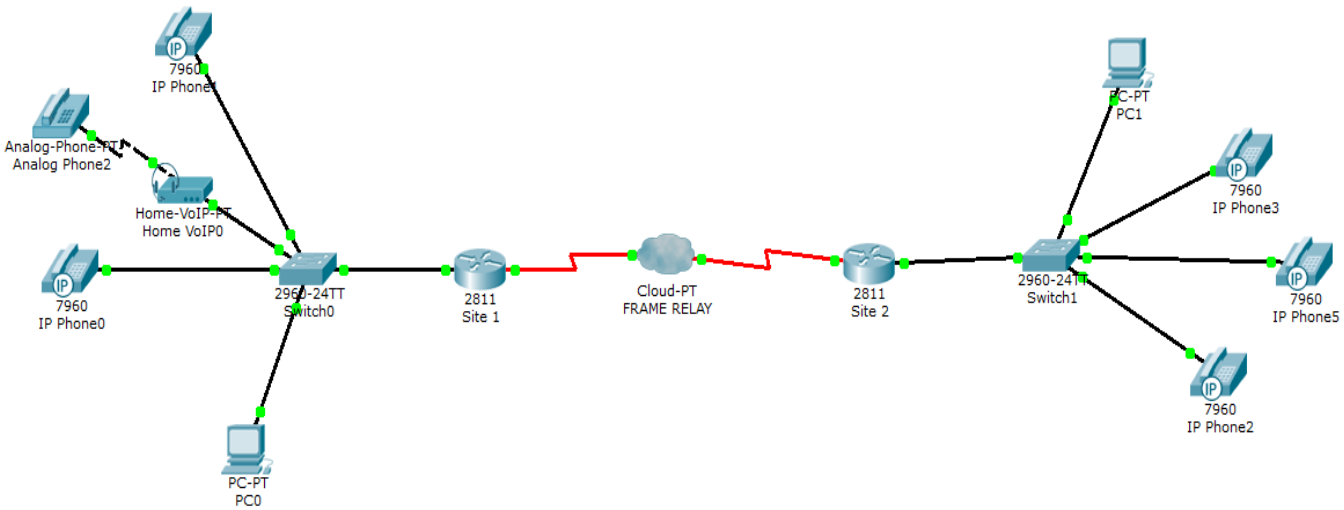


Figure 4.02 : *Architecture d'un système VoIP*

4.4 Les différentes étapes de configurations

En tout premier temps, nous allons configurer les postes, les switchs, ensuite les routeurs suivis des téléphones IP.

Pour cela, il faut tout d'abord entrer dans les interfaces de chaque matériel à configurer

4.4.1 Configuration des postes

Pour configurer un poste il faut cliquer sur le poste choisi et modifier son adresse. Il est aussi possible d'entrer l'adresse dans l'onglet desktop, ensuite choisir le menu IP configuration et enfin remplir les cases d'adressage avec son masque correspondant et l'adresse du serveur DNS s'il existe.

Pour le poste PC0, la figure 4.03 nous montre les configurations apportées à ce dernier

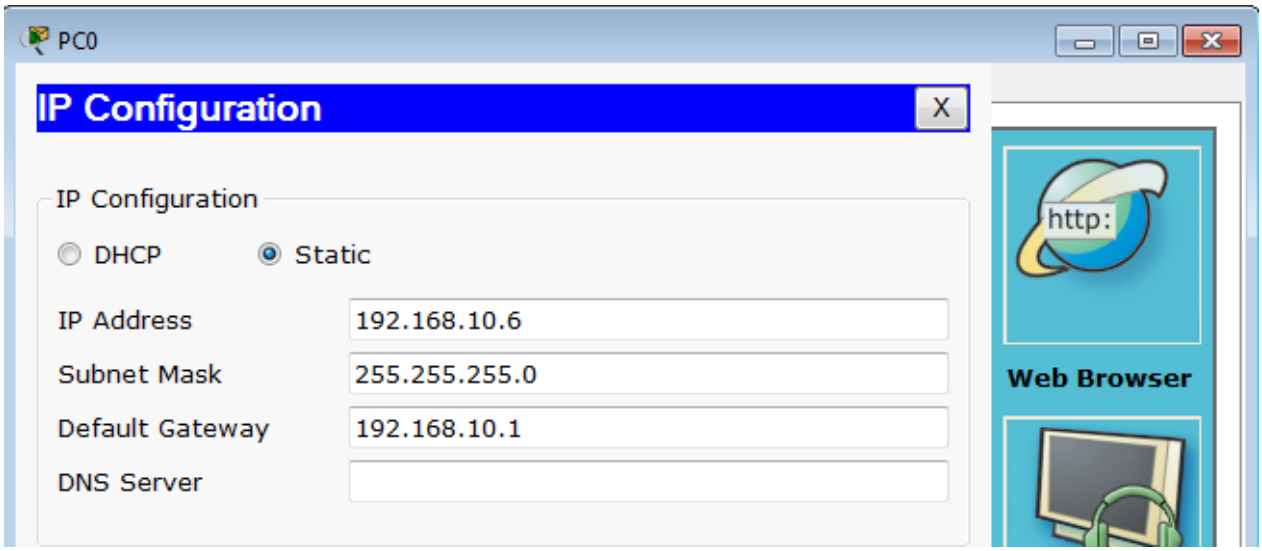


Figure 4.03 : *Configuration du poste PC0*

Comme nous l'indique la figure, nous pouvons voir que l'adresse du routeur « 192.168.10.1 » est bien la passerelle par défaut. Pour l'adresse IP de la machine, nous avons choisi d'attribuer l'adresse 192.168.10.6.

Pour le poste PC1, l'adresse machine attribuée est le 192.168.20.6

4.4.2 Configuration des switchs

Au niveau des switchs, nous allons configurer les VLAN pour séparer le trafic c'est-à-dire les flos VoIP dans les switchs. Pour se faire, nous allons entrer dans l'interface du switch en cliquant sur le switch, ensuite, nous allons le configurer dans l'option CLI de son interface. La figure 4.02 montre les différentes étapes à suivre pour la configuration.

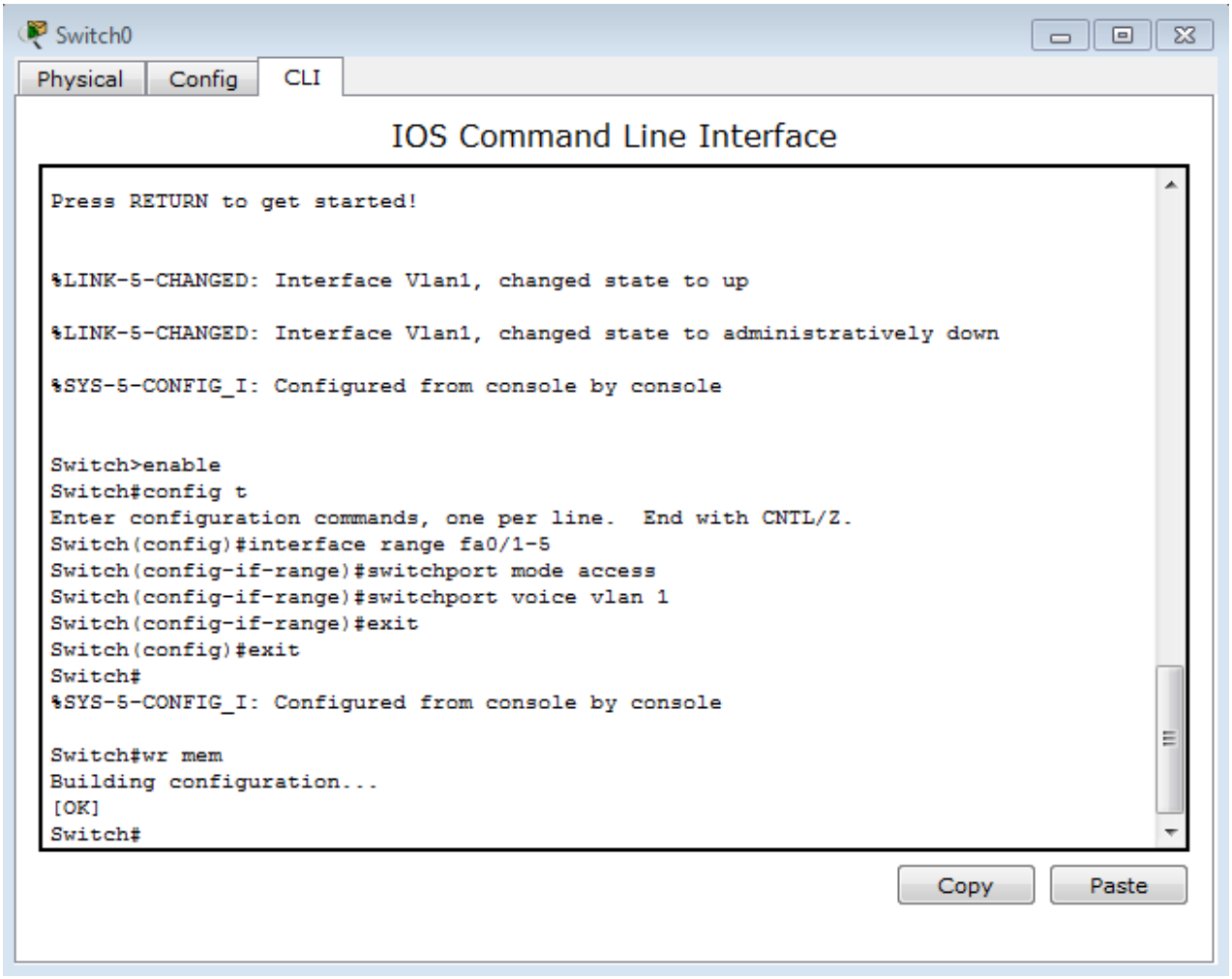


Figure 4.04 : *Configuration du switch*

Signification des commandes :

- enable : permet d'entrer en mode d'exécution privilégié
- config t : mode de configuration globale
- interface range fa0/1-5 : configure l'ensemble des interfaces de 1 à 5 du switchs
- switchport mode access : active en mode « up » les interfaces
- switchportvoice vlan 1 : définit le Vlan pour les paquets VoIP.
- exit : permet de revenir à la commande précédente
- wrmem : signifie write memory c'est-à-dire qu'elle mémorise les configurations effectuées.

4.4.3 Configuration des routeurs

La configuration des routeurs se fait en plusieurs étapes qui sont les suivants :

- configuration del'interface fastEthernet
- configuration de l'interface serial
- configuration d'un serveur DHCP
- activation du gestionnaire de communication VOIP
- activation routage RIP

4.4.3.1 Configuration de l'interface fastEthernet

Nous allons accéder dans l'interface du routeur RO ensuite configurer l'interface en question dans l'onglet CLI. La figure 4.03 décrit les différentes étapes à suivre.

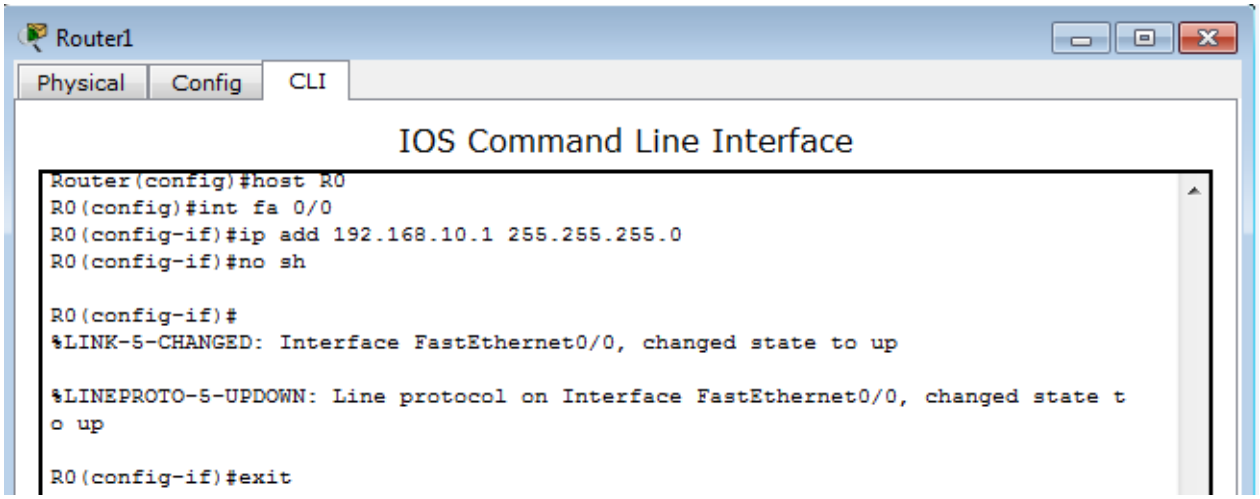


Figure 4.05 : *Configuration de l'interface fastEthernet*

Le routeur a été nommé « R0 » par la commande « host ». La commande « int fa0/0 » permet d'entrer dans l'interface fastEthernet pour la première configuration. Le routeur a été attribué une adresse IP 192.168.10.1 grâce à la commande « ipadd » et qui est évidemment une adresse de la classe C dont le masque par défaut est 255.255.255.0. L'interface est activée par la commande « no sh » qui signifie no shutdown.

Pour le routeur du site 2, l'adresse IP 192.168.20.1 lui est attribuée.

4.4.3.2 Configuration de l'interface serial

Il faut configurer l'interface série via la commande « interface Serie 0/0/0 ». Pour le routeur du site 1, une adresse IP est donnée à cette interface via la commande « ipaddress10.0.0.2 255.0.0.0 » et pour celui du site 2, l'adresse attribuée est 10.0.0.1. Il ne faut pas oublier le « clock rate » dont ici nous avons choisi 56000 pour la synchronisation de la liaison. La figure 4.04 nous montre ce mode de configuration.

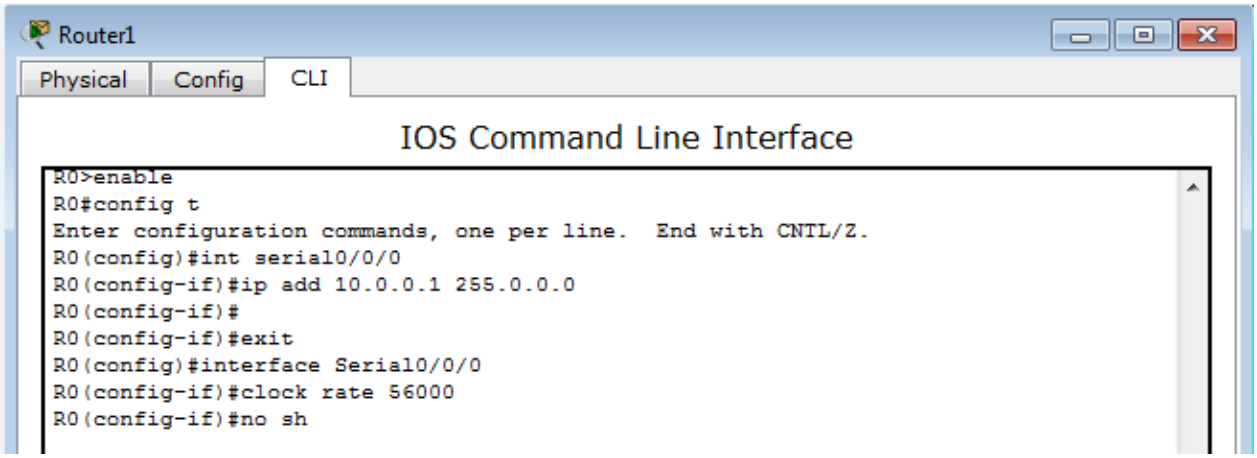


Figure 4.06 : *Configuration du serial*

Nous avons également configuré un réseau frame relay afin que les deux sites distants puissent entrer en contact. Pour cela nous avons entré les commandes suivants :

- Routeur R1 :encapsulation frame-relay
  frame-relay map ip 10.0.0.1 102 broadcast
- Routeur R0:encapsulation frame-relay
  frame-relay map ip 10.0.0.2 201 broadcast

4.4.3.3 Configuration d'un serveur DHCP

Les téléphones IP Cisco nécessitent un serveur DCHP pour l'obtention d'une adresse IP automatiquement.

Pour se faire, revenir en mode configuration global et entrer la commandes « ip DHCP pool voice1 », ensuite attribué l'adresse réseau 192.168.10.0 toujours avec le masques sous réseaux 255.255.255.0 et enfin donner une adresse par défaut du routeur qui est la même adresse saisie lors de l'activation de l'interface fastEthernet c'est-à-dire 192.168.10.1. La figure 4.04 montre ce

mode de configuration. La commande « option 150 ip » signifie que l'IP 192.168.10.1 peut fournir jusqu'à 150 adresses IP.

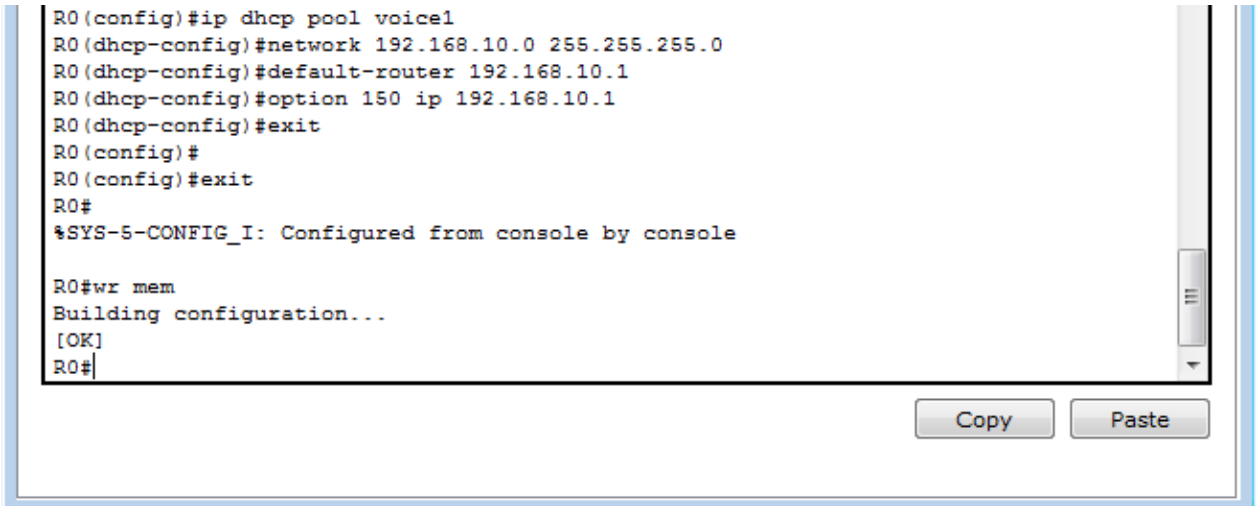


Figure 4.07 : *Configuration d'un serveur DHPC*

Ces configurations sont celles du routeur du site 1 et pour celui du site 2, la même démarche est à refaire mais comme adresse réseaux 192.168.20.0

4.4.4 Activation du gestionnaire de communication VoIP

Pour la gestion de communication téléphonique et activer une VoIP, il faut le serveur TFT ou le « Call Manager Express » . Ce serveur voit tourner le QoS du routeur.

Il faut configurer un par un les téléphones. La figure 4.05 montre ce mode de configuration pour l'activation de gestionnaire de communication.

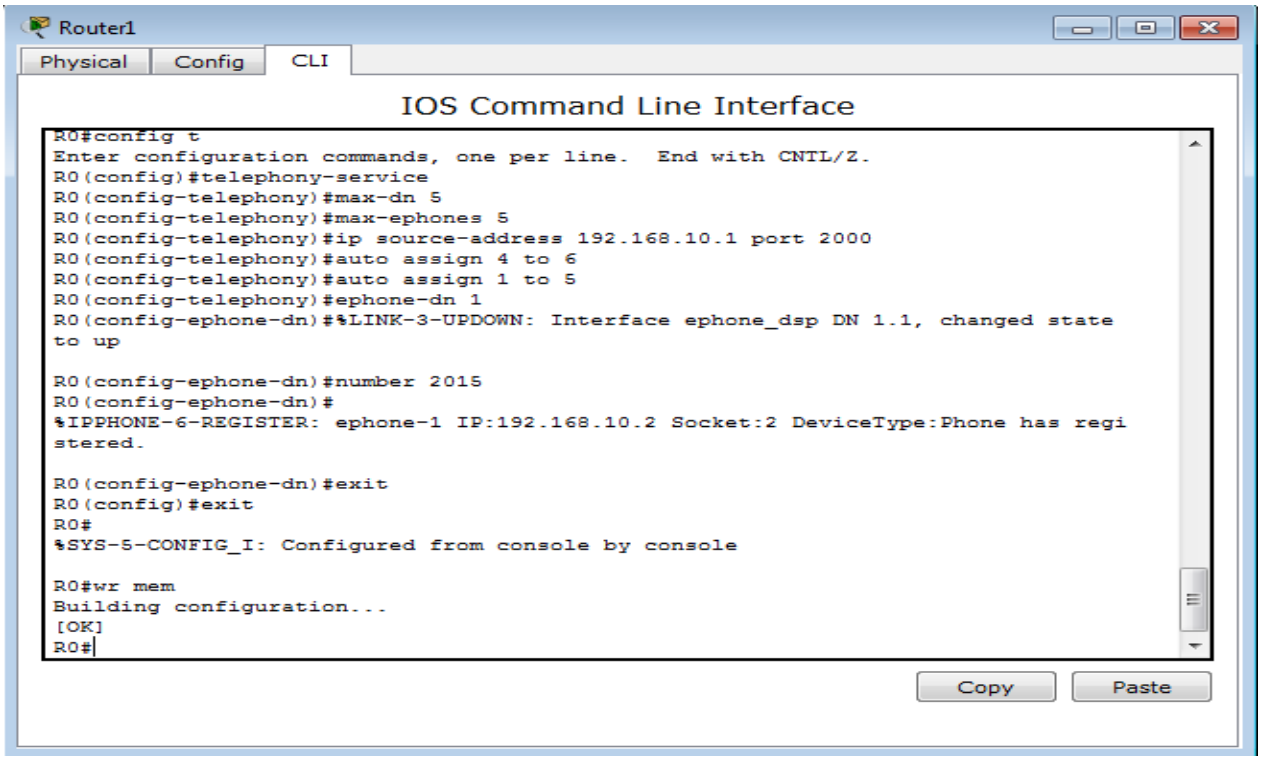


Figure 4.08 : *Activation du gestionnaire de communication VoIP*

Signification des configurations :

- telephony-service : pour la configuration des services téléphoniques du routeur.
- max-dn : définit le nombre maximum de numéros d'annuaire. Ici on a limité à 5
- max-ephones : définit le nombre maximum de téléphones. Ici on a limité aussi à 5.
- ip source-address : IP adresse source
- auto assign 4 to 6 et auto assign 1 to 5 : assigne de manière automatique l'extension des numéros au bouton.
- ephone-dn 1 : définit le premier répertoire téléphonique.
- number : attribue un numéro téléphonique à cette entrée dont ici nous avons attribué 2015.

4.4.5 Configuration du protocole RIP

RIP signifie Routing Information Protocol (protocole d'information de routage). Il s'agit d'un protocole de typeVD (Vector Distance), c'est-à-dire que chaque routeur communique aux autres routeurs la distance qui les sépare (le nombre de saut qui les sépare).

Il faut configurer les routeurs des deux sites 1 et 2 afin qu'ils puissent identifier les numéros d'appel du site distant en passant par le réseau WAN dont les configurations apportées sont :

- router rip
- version 2
- network 10.0.0.0
- network 192.168.10.0

La commande « router rip » signifie que nous allons configurer le routeur du site 1 en mode et RIP et nous avons attribué une adresse réseau 10.0.0.0/8. La commande « version 2 » permet d'entrer en contact avec les téléphones ayant les numéros commençant par « 2 » comme ce qui est bien sûr le cas pour le site 2. Il faut en faire de même avec le routeur R1 en attribuant la même adresse réseau.

Ensuite, afin que le site 1 puisse passer des appels vers le site 2, il faudra faire les configurations ci-après démontrées par la figure 4.08 pour chaque routeur des deux sites distants.

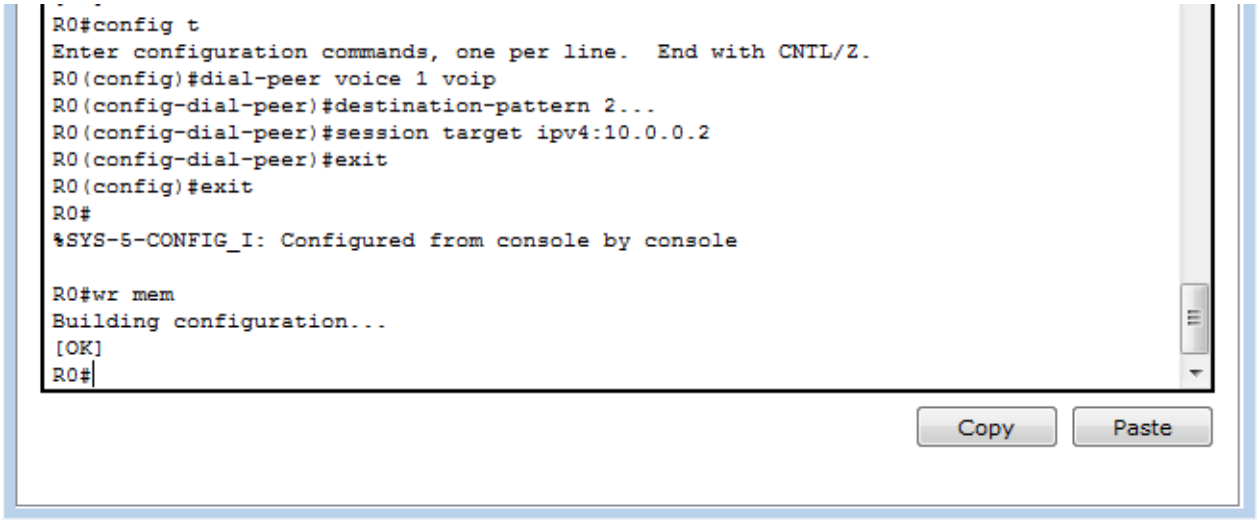


Figure 4.09 : *Interconnexion entre les deux sites distants*

- Destination-pattern 2… : signifie que la destination commence par le n°2
- Session target ipv4 :10.0.0.2 : permet l'accès au passerelle du routeur2

4.4.6 Test de la réalisation

4.4.6.1 Test de la connectivité

Dans cette simulation, nous allons montrer tout d'abord qu'il est maintenant possible de se communiquer dans un réseau à distance via le réseau de donnée.

Pour se faire, nous allons effectuer tout d'abord un trace route dans la commande prompt du PC0 venant du site 1 vers le site 2 pour montrer que le paquet sort bien de la passerelle et arrive vers une autre en passant par le réseau frame relay. La figure 4.10 nous montre les résultats du trace route effectuée.

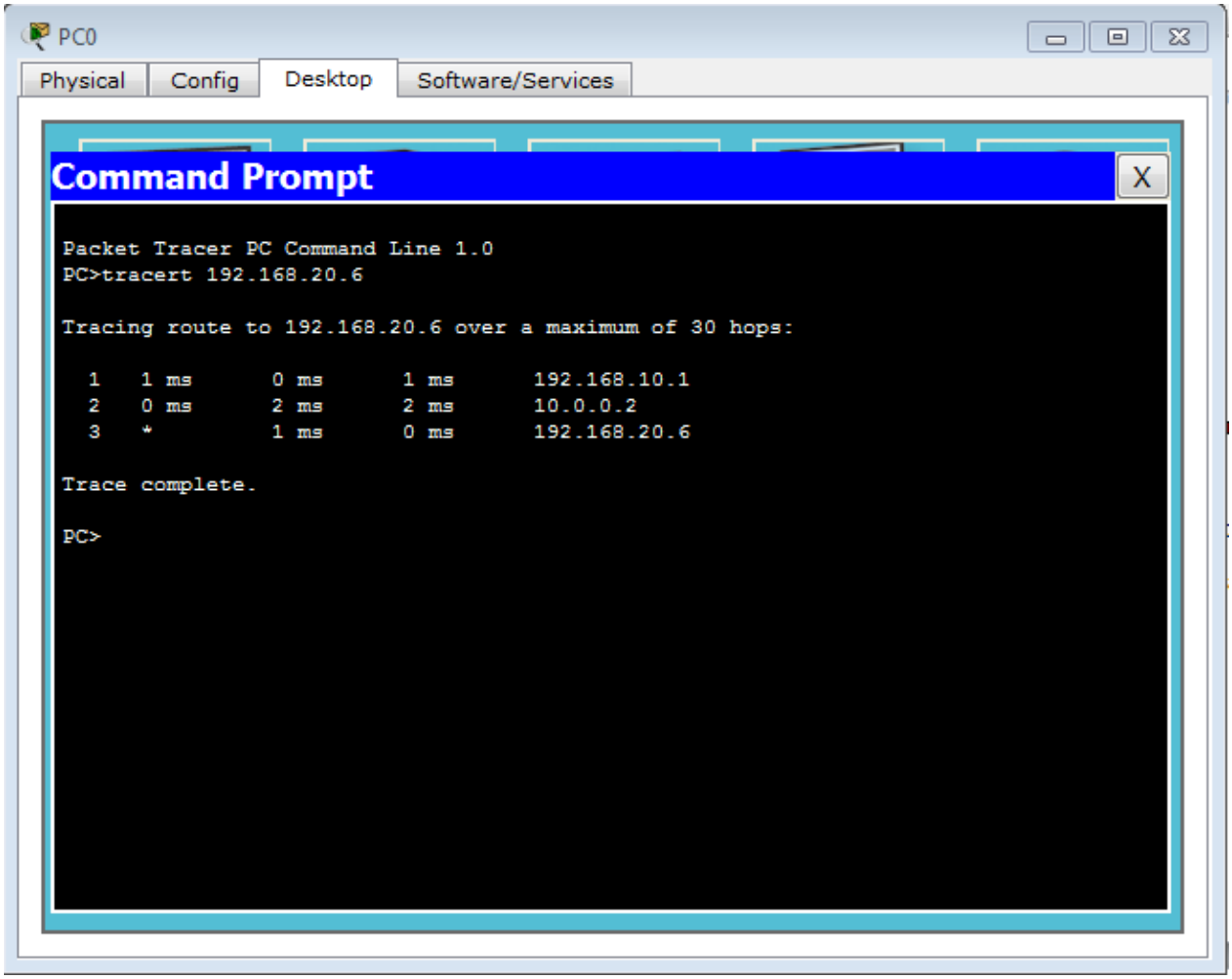


Figure 4.10 : *Trace route effectuée par le PC0 du site 1*

Comme l'indique la figure, le réseau Frame Relay joue le rôle d'un commutateur et transmet les paquets d'un réseau local vers un autre à distance en utilisant la correspondance d'adresse DLCI et adresse IP de destination et aussi en assignant un circuit virtuel permanent pour la transmission des paquets. Dans cette simulation, on a configuré la topologie du nuage frame relay en maillage globale pour assurer une parfaite connectivité. Nous voyons bien que les résultats sont tous positifs c'est-à-dire que les paquets sont envoyés et reçus avec succès.

4.4.6.2 Test de communication entre les téléphonies IP d'un réseau local

Afin de vérifier que les configurations effectuées sont bien enregistrées, il suffit juste de pointer le curseur sur un des équipements configurés comme l'indique la figure 4.09 ci-dessous

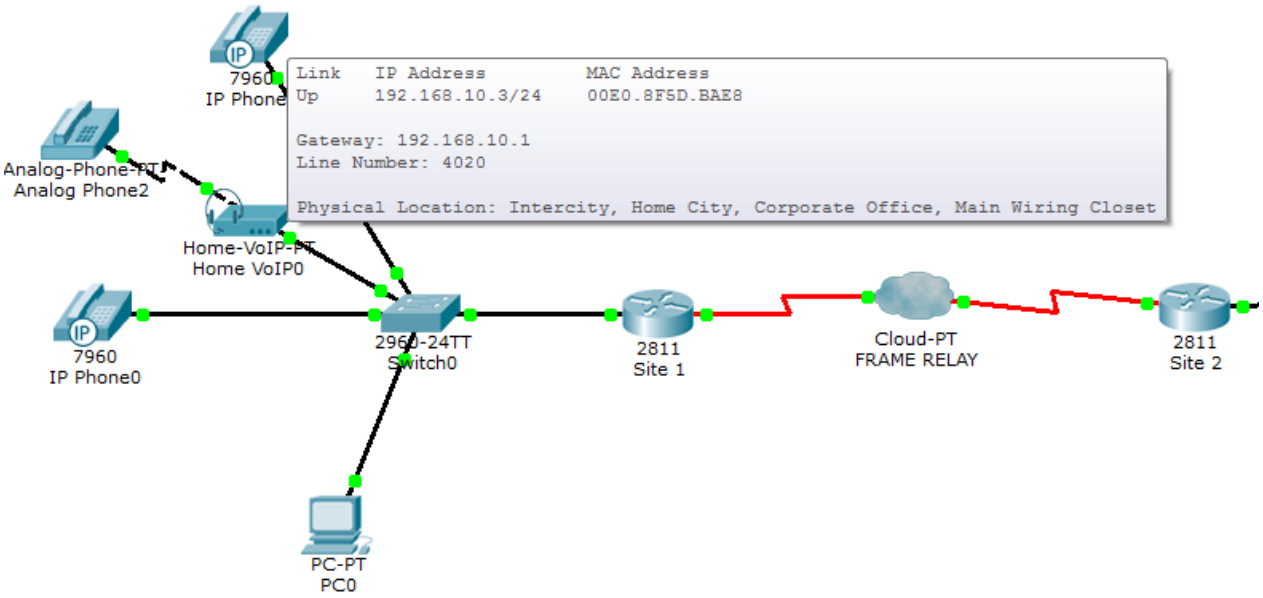


Figure 4.11 : *Visualisation de la configuration effectuée*

Nous pouvons voir sur la figure que le téléphone IP a bien enregistré le numéro qui lui était attribuée mais aussi qu'elle a enregistré l'adresse IP 192.168.10.3 attribuée par le serveur DHCP. Abordons maintenant le test de connectivité. Prenons deux téléphonies IP présentées ci-dessous par les figures 4.12 et 4.13

Figure 4.12 : *Interface de l'IP phone 0 de l'appelant*

Nous pouvons voir ici que l'analog phone 2 effectue un appel vers l'IP Phone 1 en affichant « From : 4030 » sur l'écran

Figure 4.13 : *Interface IP phone1de l'appelé*

Sur la figure nous voyons qu'ici l'analog est affiché le message « From : 4030 » sur l'écran de l'appelé

Pour savoir que ces deux derniers sont connectés, sur l'écran de l'appelé est écrit « connected ».

4.4.6.3 Test de la communication entre deux téléphonies IP à site distant.

Pour les sites distants, c'est exactement la même procédure. Lesfigures 4.14 et 4.15 nous décrivent cela en établissement la liaison entre un IP Phone du site 1 et un IP Phone du site 2.

Figure 4.14 : *IP Phone du site 1 l'appelant*

Nous pouvons interpréter le même cas pour les deux téléphonies IP des deux sites distants. Il s'affiche « To : 2097 » sur l'écran de l'appelant donc l'appelle se dirige vers l'IP phone du site 2 portant le numéro 2097.

Figure 4.15 : *IP Phone site 2 connecté à IP Phone site 1*

Les résultats nous montrent qu'il est possible de se communiquer via le réseau de données pour des sites distants.

4.5 Conclusion

Dans ce chapitre, nous avons pu prouver qu'il est possible de se communiquer via les réseaux de données. Les résultats de la simulation nous montre qu'il est extrêmement important de bien configurer étapes par étapes les différents équipements afin que la communication soit possible.

CONCLUSION GENERALE

L'objectif de ce projet, après avoir établi des études sur voix sur IP et des études de la sécurité, est de réaliser une simulation sous Cisco Packet d'un réseau VoIP afin que l'on puisse prouver qu'il est possible de téléphoner via le réseau de donnée.

Dans une première étape, nous nous sommes intéressés sur la généralité des réseaux. La connaissance préalable d'une infrastructure réseau et différents matériels utilisés dans le réseau est une étape nécessaire pour acquérir la maitrise globale d'un environnement réseau.

Dans une deuxième étape, nous avons fait l'étude de cette technologie VoIP avec ses différents protocoles et standards. La VoIP est la solution la plus rentable pour effectuer des conversations. Malgré que la normalisation n'ait pas atteint la maturité suffisante pour sa généralisation au niveau des réseaux IP, il n'est pas dangereux de miser sur ces standards vu qu'ils ont été acceptés par l'ensemble de la communauté de la téléphonie

Dans une troisième étape, nous avons étudié les problèmes de sécurité de la voix sur IP, les attaques, les vulnérabilités sur différents niveaux et les bonnes pratiques possibles pour les attaques cités.

En dernière étape, nous avons installé et configuré une solution de VoIP utilisant le simulator « Cisco Packet Tracer ».

Ce travail a été une expérience fructueuse qui nous a permis de mieux de savoir comment gérer et optimiser le temps dans le but d'en profiter au maximum.

ANNEXE 1 : CLASSIFICATION DES RESEAUX

LAN(Local Area Network) sont réseaux locaux connectent plusieurs ordinateurs situés sur une zone géographique relativement restreinte, tels qu'un domicile, un bureau, un bâtiment, un campus universitaire. Ils permettent aussi aux entreprises de partager localement des fichiers et des imprimantes de manière efficace et rendent possibles les communications internes.

MAN (Metropolitan Area Network) sont des réseaux qui interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s' ils faisaient partie d'un même réseau local. Il peut couvrir un grand campus ou une ville

WAN (Wide Area Network) : pour des raisons économiques et techniques, les réseaux locaux (LAN) ne sont pas adaptés aux communications couvrant de longues distances. C'est pour toutes ces raisons que les technologies des réseaux étendus (WAN) diffèrent de celles des réseaux locaux. Un WAN est un réseau à longue distance qui couvre une zone géographique importante (un pays, voir même un continent). [2]

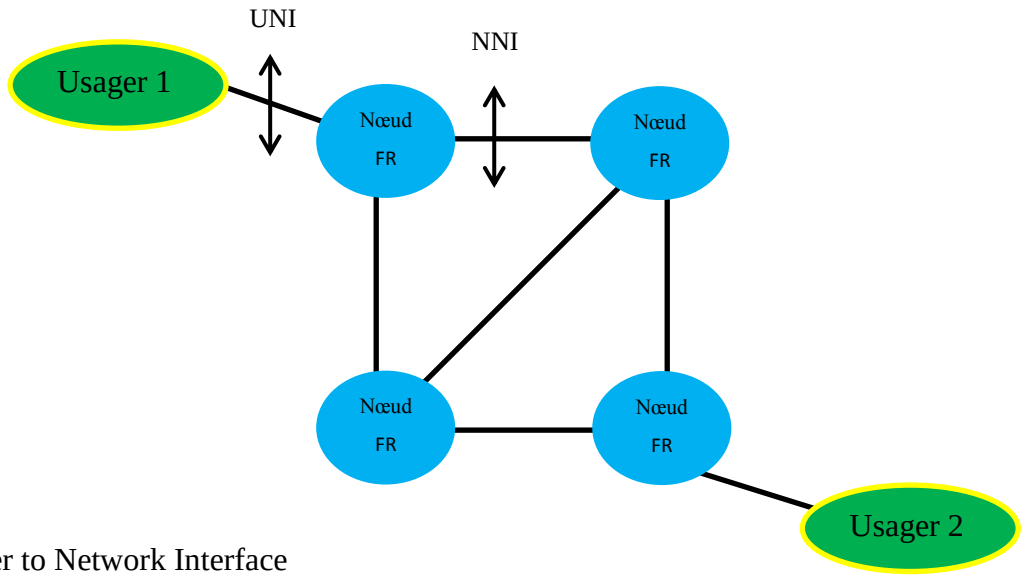
ANNEXE 2 : LE RESEAU FRAME RELAY

Le réseau Frame Relay est constitué d'un ensemble de nœuds interconnectés par un maillage quelconque, ses interconnexions sont des voies à haut débit et le réseau relais de trames travaille en mode connecté. [22]

Il existe deux types de circuits virtuels :

- Les circuits virtuels permanents (PVC) établis par l'opérateur lors de l'abonnement.
- Les circuits virtuels commutés (SVC) établis sur l'initiative de l'usager.

La figure 4.16 nous illustre une interconnexion utilisant le réseau Frame Relay



UNI: User to Network Interface
NNI: Network to Network Interface.

Figure 4.16 : *Interconnexion utilisant Frame Relay*

ANNEXE 3 : LE RESEAU TELEPHONIE COMMUTE

Le réseau téléphonique commuté (ou RTC) est le réseau des téléphones (fixes et DECT), dans lequel un poste d'abonné est relié à un central téléphonique par une paire de fils alimentée en batterie centrale (la boucle locale). Les centraux sont eux-mêmes reliés entre eux par des liens offrant un débit de 2 Mb/s.

Les bases du réseau RTCP ont été créées par Alexandre Graham Bell dans le but de faire écouter des pièces de théâtre à distance.

Au tout début, les communications étaient établies par des opérateurs et des opératrices, grâce à un système de cordons souples munis de fiches et de tableaux d'arrivée et de départ d'abonnés. Puis vinrent les systèmes de commutations automatiques, qui n'ont cessé d'être améliorés : d'abord électromécaniques, puis électroniques, ils sont désormais numériques et totalement pilotés par informatique.

De l'origine jusqu'à la fin des années 1980, il existait une continuité électrique entre les deux abonnés : un circuit électrique réel était établi entre les deux téléphones.

- Pour les liaisons entre centraux, d'encombrants câbles multipaires, puis les câbles coaxiaux numériques, sont désormais remplacés par des faisceaux de fibre optique. Cette dernière permet des débits beaucoup plus élevés, sorte d'autoroute qui profite aux technologies numériques d'information et de communication.
- Pour établir une communication point à point, l'abonné compose un numéro pour que les commutateurs des centraux relient l'appelant à l'appelé. La commutation réserve un canal de communication pour toute la durée de la communication entre les parties reliées.
- Les premiers tableaux de commutation comprenaient quelques dizaines de prises d'abonnés, les commutateurs électromécaniques ainsi que les électroniques et informatiques actuels peuvent gérer plusieurs milliers d'abonnés

Les liaisons entre terminaux mobiles et commutateurs, bien que numériques, sont quant à elles souvent moins performantes (réseaux mobiles 2G et 3G), limitées par les technologies radioélectriques utilisées pour transmettre le signal radio dans l'air.

BIBLIOGRAPHIE

[1] G. Pujolle, « *Les Réseaux* », Eyrolles, Paris, 2003.

[2] A. Ratsimbazafy, « *Réseaux Informatiques* », Cours L2-TCO, Dép. TCO-E.S.P.A., A.U. : 2010-2011.

[3] http://www.Les 7 couches du modele OSI.html

[4] L.E. Randriarijaona, « *Réseaux TCP/IP* », Cours L3-TCO, Dép. TCO-E.S.P.A., A.U. : 2011-2012.

[5] http://www.ch01s02.html

[6] C.Bulfone « *Le protocole IP* », Licence MIASS

[7] A. Vaucamps « *Cisco, Protocoles et Configuration avancée des routeurs* », Eni éditions, 2010.

[8]http://www.cisco.goffinet.org

[9] http://www.frameip.com/voip/, Voix sur IP –VoIP.

[10] D. Endler, M. Collier, « *Hacking VoiP* ».

[11] O.Hersent, D.Gurle, JP. Petit, « *L'essentiel de la VoIP* », ed. Dunod.

[12] H. Badis « Voice over Protocole », IGM, Université Paris-Est Marne-la-Vallée.

[13] http://www.effort.com, « *H323 architecture et Protocoles* ».

[14] R. Bouzaida, « *Etude et mise en place d'une VoIP sécurisée* ».

[15] S. Znaty, J.L. Dauphin, « *SIP : Session Initiation Protocol* ».

[16] F. Bidet, V. Boistuaud, M. Douis, J. Herr, F. Fraux, « *TP de Voix sur IP avec SIP et RTP* », 2007-2008.

[17] P. Papageorgiou, « *A comparison de H.323 et SIP*».

[18] J. Ehrensberger, A. Doswald, X. Hahn,S. Contreras, « *Audit de réseaux VoIP2 – Menaces* »18 octobre 2006.

[19] N. Fischbach, « *COLT Telecom/Sécurité* », 2006.

[20] P. Betouin, «*Vulnérabilité et sécurisation* », École supérieure d'informatique, d'électronique et d'automatique (ESIEA).

[21] Cisco « *Networking Academy* », Mind Wide Open

[22] E. Lalitte, F. R. Vigneau, « *Cours réseaux* », Institut privé des nouvelles technologies de l'information, 2005.