REPUBLIQUE ALGERIENNE
DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT
SUPERIEUR ET DE LA
RECHERCHE SCIENTIFIQUE

UNIVERSITE LARBI TEBESSI - TEBESSA
FACULTE DES SCIENCES ET TECHNOLOGIES
DEPARTEMENT DE GENIE ELECTRIQUE

MEMOIRE
DE FIN D'ETUDES POUR L'OBTENTION DU DIPLOME DE MASTER EN TELECOMMUNICATIONS

THEME

La sécurité de la VoIP sur un support FH

Présenté par:

- Mr Hamiche Lahcene

Devant le jury :

- Dr Houam Lotfi	**Président**
- Dr Bentahar Tarek	**Encadreur**
- Dr Saidi Riad	**Examinateur**

Année Universitaire 2019 / 2020


بسم الله الرحمن الرحيم

Remerciements

*En tout premier lieu je remercie **Allah** de m'avoir aidé à défier tous les obstacles, afin de compléter ce modeste travail.*

Je tiens à remercier très sincèrement mon encadreur « Dr BENTAHAR Tarek » qui a accepté de m'encadrer, et pour le temps qu'il m'a consacré et ses précieux conseils.

Mes remerciements s'adressent également aux Président et membres de jury pour l'intérêt qu'ils ont porté à mon travail, et pour l'honneur qu'ils me font de bien vouloir le juger.

J'ai pu aller au bout de ma recherche grâce au soutien de ma famille respective.

Je ne peux conclure sans avoir remercié tous ceux qui ont aidé de près ou de loin au succès de ma formation.

Dédicace

♥ *À mes chers parents, qui m'entouraient par leurs supplications, et je serais éternellement reconnaissant.*

♥ *À ma chère épouse et copine de ma vie qui m'a soutenu avec dévouement.*

♥ *À mes enfants: Akram, Sadjed, Dhaker.*

♥ *À mes frères, mes sœurs, et tous mes proches.*

♥ *À mon cher ami et collègue de la vie professionnelle: Fayssal.*

♥ *À tous les enseignants et les étudiants de deuxième année Master RT.*

♥ *A toutes mes connaissances.*

♥ *À tous ces gens-là, Je dédie cet humble travail.*

Lahcene

Sommaire

Liste des figures

Liste des tableaux

Liste des acronymes

AES	:	Advanced Encryption Standard	PABX	:	Private Automatic Branch eXchange
AP	:	Access Points	PAL	:	Phase Alternating Line
APK	:	Amplitude Phase Keying	PC	:	Personnal Computer
ARP	:	Address Resolution Protocol	PFS	:	Perfect Forwarding Secrecy
ASK	:	Amplitude Shift keying	PMP	:	Point-to-Multipoint
BTS	:	Base Transceiver Station	PoE	:	Power over Ethernet
CDP	:	Cisco discovery protocol	POTS	:	Plain Old Telephone Servie
CIPC	:	Cisco IP Communicator	PSK	:	Phase Shift Keying
CME	:	Call Manager Express	PSK	:	Pre-Shared Key
CPU	:	Central Processing Unit	PSTN	:	Public Switched Telephone Network
CSCF	:	Call Session Control Function	QAM	:	Quadrature Amplitude Modulation
DECT	:	Digital Enhanced Cordless Telecommunications	RAM	:	Random Access Memory
DHCP	:	Dynamic Host Configuration Protocol	RF	:	Radio Fréquence
DN	:	Directory Number	RFC	:	Request for Comments
DNS	:	Domain Name System	RI	:	Réseau Indépendant
DoS	:	Denis of Service	RNIS	:	Réseau Numérique à Intégration de Services
ESP	:	Encapsulating Security Protocol	ROP	:	Réseaux Ouverts au Public
ESP	:	Encapsulating Security Protocol	RSVP	:	Ressource ReSerVation Protocol
FEC	:	Forward Error Correction	RTC	:	Réseau Téléphonique Commuté
FFTP	:	Foiled Foiled Twisted Pair	RTCP	:	Real-time Transport Control Protocol
FH	:	Faisceau Hertzien	RTP	:	Real-time Transport Protocol
FHA	:	Faisceau Hertzien Analogique	RTSP	:	Real Time Streaming Protocol
FHN	:	Faisceau Hertzien Numérique	SA	:	Security Association
FSK	:	Frequency Shift Keying	SAP	:	Session Annonce Protocol
FTP	:	Foiled Twisted Pair	SDP	:	Session Description Protocol
FXO	:	Foreign exchange Office	SFTP	:	Shielded Foiled Pwisted Pair
FXS	:	Foreign exchange station	SIP	:	Session Initiation Protocol
HTTP	:	HyperText Transfer Protocol	SMF	:	Single Mode Fiber
ICMP	:	Internet Control Message Protocol	SNMP	:	Simple Network Management Protocol
ID	:	Identification	SRTP	:	Secure Real-time Transport Protocol
IEEE	:	Institute of Electrical and Electronics Engineers	SSI	:	Sécurité des Systèmes d'Information
IETF	:	Internet Engineering Task Force	SSL	:	Secure Sockets Layer
IKE	:	Internet Key Exchange	SSTP	:	Super Shielded Twisted Pair
IOS	:	Internetwork Operating System	STP	:	Shielded Twisted Pair
IPBX	:	Internet Protocol Private automatic Branch eXchnage	SU	:	Subscriber Units
IPSEC	:	Internet Protocol Security	SUDB	:	Subscriber Units Database
ISAKMP	:	Internet Security Association and Key Management Protocol	TCP/IP	:	Transmission Control Protocol/Internet Protocol
ISL	:	Inter Switch Link	TDM	:	Time Division Multiplexing
ISM	:	Industrial, Scientific and Medical	TLS	:	Transport Layer Security
ITS	:	IOS Telephony Service	ToIP	:	Telephony over Internet Protocol
ITU	:	International Telecommunication Union	TPH	:	Téléphone, Téléphonique
LAN	:	Local Area Network	UDP	:	User Datagram Protocol
MAC	:	Media Access Control	UHF	:	Ultra High Frequency
MIKEY	:	Multimedia Internet KEYing	U-NII	:	Unlicensed National Information Infrastructure
MMF	:	Multi Mode Fiber	UTP	:	Unshielded Twisted Pair
MSK	:	Minimum Shift Keying	VHF	:	Very High Frequency
NTSC	:	National Television System Committee	VLAN	:	Virtual Local Area Network
OOK	:	On Off Keying	VoIP	:	Voice over Internet Protocol
OSI	:	Open Systems Interconnection	VPN	:	Virtual Private Network
OSPF	:	Open Shortest Path First	WAN	:	Wide Area Network

Introduction générale

Le développement d'Internet a modifié profondément la façon d'utiliser notre téléphone. En effet, la technologie de la téléphonie classique est aujourd'hui en passe d'être supplantée par la téléphonie sur IP (Internet Protocol). La migration des entreprises vers ce genre de technologie à pour but principal de : minimiser le coût des communications, utiliser le même réseau pour offrir des services de données, de voix, et d'images, et réduire les coûts de configuration et d'assistance.

Similaire au téléphone, la voix sur IP (VoIP : Voice over Internet Protocol) permet de transmettre la voix en se référant au protocole IP et cela permet d'effectuer des appels téléphoniques via Internet. En plus, l'intégration progressive de la VoIP, en ajoutant des cartes extensions IP, facilite l'adoption du téléphone IP dans les grandes sociétés possédant une plateforme classique et voulant bénéficier de la voix sur IP.

Les principales firmes produisant ce type d'équipements présentes aujourd'hui sur le marché, comme (Cisco, Clarent, Avaya, Alcatel, Nortel Network, Siemens, Ténovis, 3COM,..) ont eu tendance à combiner les fonctionnalités (routage/passerelle, serveur VoIP, Gatekeeper) en un seul équipement. D'ailleurs, la VoIP est un marché chevauchant deux secteurs (la téléphonie et l'informatique) qui se rapprochent et étaient complètement différent auparavant, nous assistons ici à une concurrence ayant des origines différentes. En effet, nous retrouvons le géant de l'équipement réseaux Cisco en concurrence avec des entreprises de téléphonies tel que Alcatel ou Siemens. Cette approche permet de bénéficier d'une grande flexibilité, d'une très bonne intégration au monde des données et de voix, et surtout d'un prix beaucoup plus intéressant.

D'un autre côté, un réseau (VoIP ou Données) suppose plusieurs équipements informatiques et télécommunications (Serveur VoIP, Ordinateurs, Routeurs, Switchs, téléphones, divers équipements électroniques,…) situés à distance les uns des autres. La première chose à mettre en œuvre pour constituer ce réseau est la transmission des informations d'un équipement à l'autre. À partir de ce point, on utilise des supports de transmission selon le type des équipements choisi et d'infrastructures existantes et d'endroit entouré.

Le développement d'Internet s'est également accompagnée d'une évolution des modes et moyens de transmission des informations, pour répondre à la très forte croissance des données et de la connectivité de l'utilisateur moderne d'aujourd'hui, en trouvant des alternatives aux supports précédemment utilisés, et en les remplaçant par des supports à haut débit et d'une bande plus large (comme les fibres optiques). Le développement de ces supports se sont fortement orientées vers les supports sans fil tels que la technologie cellulaire, les faisceaux hertziens (FH), Wifi, Wi-Max,..etc, en raison de leur: flexibilité, mobilité, facilité d'installation à faible coût.

Comme la solution VoIP est basée sur la technologie IP, elle est toutefois affectée par les vulnérabilités qui menacent la sécurité de 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. Certaines attaques sur les réseaux VoIP, comme les attaques de déni de service, et les vols d'identité, peuvent causer des pertes catastrophiques et énormes pour les entreprises.

Pour cela, la sécurité de la VoIP, n'est pas seulement une nécessité mais plutôt une obligation, avec laquelle nous pouvons réduire, au maximum, le risque d'attaques sur la VoIP. De ce fait, une solution VoIP doit couvrir toute l'infrastructure du réseau déployé, tel que les outils et les équipements de gestion des communications et des utilisateurs, et les protocoles de signalisation et de transport de données.

Dès le titre du mémoire, on se retrouve devant trois volets: la VoIP, les faisceaux hertziens, et la sécurité de l'information. A première vue elles paraissent différentes, mais en réalité elles sont très imbriquées. C'est-a-dire les informations à transmettre (son, image, données) ont besoin d'un support pour que les parviennent au destinataire. Ce support comme l'information a besoin de protection contre tous les risques associés.

L'objectif de ce travail est:

- L'intégration du support FH dans l'architecture de notre topologie afin de simplifier la mise en place d'un réseau (données, VoIP,..) sécurisé à faible cout.
- Création d'un centre d'appel téléphonique à base d'un routeur.
- Exploitation des ordinateurs impliqués au service pour faire des communications, en utilisant l'application ***Cisco IP Communicator***.

Ce mémoire est structuré en **trois chapitres**, dans **le premier chapitre**, nous avons discuté sur les types des supports de transmission utilisés dans le transfert d'informations, en mettant en évidence les caractéristiques techniques de chaque type et ses domaines d'utilisation. Nous avons également fourni une explication détaillée sur les caractéristiques de l'une des antennes faisceaux hertziens sélectionnées à titre d'exemple pour l'utiliser comme un support de transmission dans le but d'interconnecter les réseaux LAN distincts d'une entreprise, en créant un liens haut débit entre les blocs (immeubles) éloignés de cette entreprise. Il s'agit d'une solution idéale afin de réduire et minimiser le coût et le temps d'installation. Ceci par rapport aux travaux durs et coûteux de tirage des câbles de fibres optiques ce qui augmente aussi la durée d'achèvement.

Le deuxième chapitre et décomposé en **deux parties: la première** défini la voix sur IP et ses éléments, décrit et explique son architecture et ses protocoles, et énumère les majeurs points forts de cette technologie ainsi que ses faiblesses. **La deuxième partie** s'intéresse aux vulnérabilités des systèmes sur un environnement VoIP et les techniques de sécurité.

Le troisième chapitre est dédié à l'application dans laquelle nous montrons la conception de notre topologie, avec une description sur le plan de numérotation dédié aux IP-Phones, et le plan d'adressage alloué aux différents équipements de réseau. Ainsi la configuration des équipements et des machines (Routeurs, Switchs, IP-Phones, PCs,..) connectées dans cette topologie à l'aide du simulateur *Cisco Packet Tracer*.

Chapitre 1:

Le faisceau hertzien (FH) comme un support de transmission

Chapitre I: Le faisceau hertzien (FH) comme un support de transmission

Introduction

La mise en place d'un réseau VoIP ou données au niveau d'une entreprise, nécessite la présence des supports de transmission, tant que les équipements situés à distance les uns des autres, on trouve par exemple**: les paires torsadées** pour relier les équipements à courte distance (moins de 100 m) et dans un endroit bien couvert (réseau LAN). **Les fibres optiques** pour l'accès externe et pour intégrer des autres sites éloignés (annexes) rattachés à cette entreprise sur dizaines de km (réseau WAN). **Les antennes faisceaux hertziennes** pour créer des liens entre les blocs sans avoir d'installer des supports physiques entre chaque nœud et terminaux du réseau. Et d'autres supports lesquels nous parlerons dans ce chapitre.

Dans la **première partie** de ce chapitre nous présentons les différents supports utilisés dans la transmission des informations et leurs caractéristiques, et on détaille dans la **deuxième partie** les caractéristiques techniques de l'antenne FH type Access5830, laquelle on va proposée pour réaliser notre topologie.

Partie I: Généralités sur les supports de transmission

Les supports de transmission sont nombreux. Parmi ceux-ci, on distingue : les supports métalliques, non métalliques et immatériels. Les supports métalliques, comme les paires torsadées et les câbles coaxiaux, sont les plus anciens et les plus largement utilisés ; ils transportent des courants électriques. Les supports de verre ou de plastique, comme les fibres optiques, transmettent la lumière, tandis que les supports immatériels des communications sans fil propagent des ondes électromagnétiques et sont en plein essor. Les supports de transmission sont de nature très différente les uns aux autres. Ils sont caractérisés par leur bande passante qui limite le débit maximal auquel on peut transmettre et le taux d'erreur qu'ils introduisent sur les signaux transportés. Les techniques de transmission (en bande de base ou par transposition de fréquence) ont pour objet d'adapter au mieux les signaux aux caractéristiques de ces supports. Elles sont normalisées au niveau international et mises en œuvre dans des modems et des interfaces.

1. Caractéristiques des supports de transmission

1.1. Bande passante

Ils ont une bande passante limitée c'est-à-dire que certains signaux se propagent correctement dans le support (ils sont affaiblis mais encore reconnaissables à l'autre extrémité), mais d'autres ne le traversent pas du tout (ils sont tellement affaiblis ou déformés qu'on ne les retrouve plus du tout à la sortie). La bande passante d'un support est la bande de fréquences des signaux dont la puissance à la sortie, après la traversée du support, est supérieure à un seuil donné. En général, on caractérise un support par sa bande passante, c'est-à-dire par la plage de fréquence à l'intérieur de laquelle la puissance de sortie d'un signal sinusoïdal est au pire divisée par deux. Intuitivement, plus un support a une bande passante large et plus il pourra transporter d'informations par unité de temps.

1.2. Bruits et distorsions

Les supports de transmission déforment les signaux qu'ils transportent même lorsque ceux-ci ont des fréquences adaptées. En effet, plusieurs sources de bruit perturbent les signaux et des distorsions (d'amplitude ou de phase) peuvent s'avérer gênantes pour la reconnaissance des signaux en sortie. Par ailleurs, la distance est un facteur d'affaiblissement, particulièrement important pour les liaisons par satellite. Enfin, certaines perturbations de l'environnement peuvent également introduire des bruits (foudre, orages pour le milieu aérien, champs électromagnétiques dans des ateliers pour les supports métalliques…). Même lorsque les signaux sont adaptés aux supports de transmission, on ne pourra pas garantir à 100% leur exactitude à la réception.

1.3. Capacité limitée

L'ensemble des caractéristiques que nous venons de voir fait que la capacité d'un support de transmission est limitée. Par capacité, nous entendons la quantité d'information transportée par unité de temps. Un théorème dû à Shannon (Claude Shannon, mathématicien américain du 20ème siècle qui a développé la théorie de l'information) donne une borne maximale de cette capacité, notée $\boldsymbol{Cap_{Max}}$ et exprimée en bits par seconde:

$$\boldsymbol{Cap_{Max} = W log_2(1 + S/B)}$$

W: la largeur de la bande passante (*Hz*).

S/B: Rapport (puissance du signal à puissance du bruit), la base deux du logarithme servant pour exprimer l'information en bits.

2. Modes d'exploitation de la liaison

Le transfert d'information entre deux systèmes A et B peut s'effectuer en fonction des besoins et des caractéristiques des éléments, suivants 3 modes d'exploitation de la liaison.

2.1. Liaison simplex

Le système A est un système émetteur, le système B est un système récepteur, les données sont transmises dans un seul sens. L'exploitation en mode unidirectionnel est justifié pour les systèmes dont le récepteurs n'a jamais besoin d'émettre (liaison radio ou télévision).

2.2. Liaison semi duplex (*Half duplex*)

La transmission est possible dans les deux sens mais non simultanément, l'exploitation est en mode bidirectionnel à l'alternat. Ce type de liaison est utilisée lorsque le support physique est commun aux deux sens de transmission (cas des lignes téléphoniques) ne possédant pas une largeur de bande suffisante pour permettre des liaisons bidirectionnelles simultanées par modulation de deux fréquences porteuses différentes, des procédures particulières permettant alors d'inverser le sens de transmission.

2.3. Liaison duplex intégral (*full duplex*)

Les données peuvent être émises ou reçues simultanément dans les deux sens. L'exploitation est en mode bidirectionnel simultané. A chaque sens de transmission correspond un canal de communication propre, lorsque le support physique est commun aux deux sens de transmission. Chaque canal est défini dans une bande de fréquence spécifique.

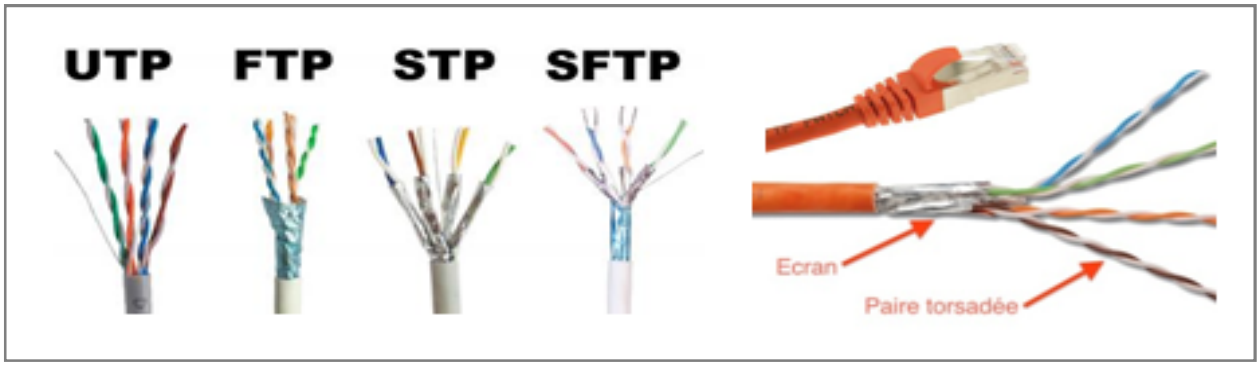
3. Les différents supports de transmission

3.1. Les paires torsadées

Une paire torsadée se compose de deux conducteurs en cuivre, isolés l'un de l'autre et enroulés de façon hélicoïdale autour de l'axe de symétrie longitudinal. L'enroulement réduit les conséquences des inductions électromagnétiques parasites dues à l'environnement. L'utilisation courante de la paire torsadée est le raccordement des usagers au central téléphonique (la boucle locale) ou la desserte des usagers de réseaux privés. Son principal inconvénient est l'affaiblissement des courants, d'autant plus important que le diamètre des conducteurs est faible. Les paires torsadées contiennent, à intervalles réguliers, des répéteurs qui régénèrent les signaux. Quand plusieurs paires sont rassemblées dans un même câble, les courants transportés interfèrent les uns avec les autres. Ce phénomène est appelé diaphonie. La paire torsadée suffit pour les réseaux locaux d'entreprise où les distances se limitent à quelques kilomètres. Ses avantages sont nombreux : technique maîtrisée, facilité de connexion et d'ajout de nouveaux équipements, faible coût.

Les constructeurs proposent plusieurs types de paires torsadées blindées, elles sont mieux protégées des rayonnements électromagnétiques parasites. Une meilleure protection prévoit un blindage par paire. [1]

- **UTP** (*Unshielded twisted pair*) Paire torsadée non blindée. La paire torsadée non blindée n'est entourée d'aucun blindage protecteur.
- **FTP** (*Foiled Twisted Pair*) Paire torsadée écrantée. L'ensemble des paires torsadées a un blindage global assuré par une feuille d'aluminium. L'écran est disposé entre la gaine extérieure et les 4 paires torsadées.
- **STP** (*Shielded Twisted Pair*) Paire torsadée blindée. Chaque paire torsadée blindée est entourée d'un feuillard en aluminium.
- **FFTP** (*Foiled Foiled Twisted Pair*) Paire torsadée doublement. Chaque paire torsadée est entourée d'une feuille de blindage en aluminium. L'ensemble des paires torsadées a une feuille de blindage collectif en aluminium.
- **SFTP** (*Shielded Foiled Twisted Pair*) Paire torsadée écrantée et blindée. Câble doté d'un double écran (feuille métallisée et tresse) commun à l'ensemble des paires.
- **SSTP** (*Super Shielded Twisted Pair*) Paire torsadée super blindée. Chacune des paires est blindée par un écran en aluminium, et en plus la gaine extérieure est blindée par une tresse en cuivre étamé.



Figure(1): Les paires torsadées (UTP, FTP, STP, SFTP)

3.2. Les câbles coaxiaux

Le câble coaxial est une ligne de transmission des signaux numériques ou analogiques à basses ou hautes fréquences. Ce câble présente de meilleures performances que la paire torsadée: affaiblissement moindre, transmission de signaux de fréquences plus élevées, pas de perturbations dues aux bruits externes, etc.

Le câble composé de deux conducteurs métalliques cylindriques (central et extérieur) de même axe séparés par un isolant. L'âme centrale, qui peut être en cuivre est entourée d'un matériau diélectrique (isolant). Le diélectrique est entouré d'une tresse conductrice ou d'un tube en cuivre, et puis d'une gaine extérieure isolante et protectrice.

La capacité de transmission d'un câble coaxial dépend de sa longueur et des caractéristiques physiques des conducteurs et de l'isolant. Sur 1 km, un débit de plusieurs centaines de Mbit/s peut être atteint. Sur des distances supérieures à 10 km, l'atténuation des signaux réduit considérablement les débits possibles. C'est la raison pour laquelle on utilise désormais les fibres optiques sur les liaisons grandes distances.

Il est possible de trouver un câble coaxial :

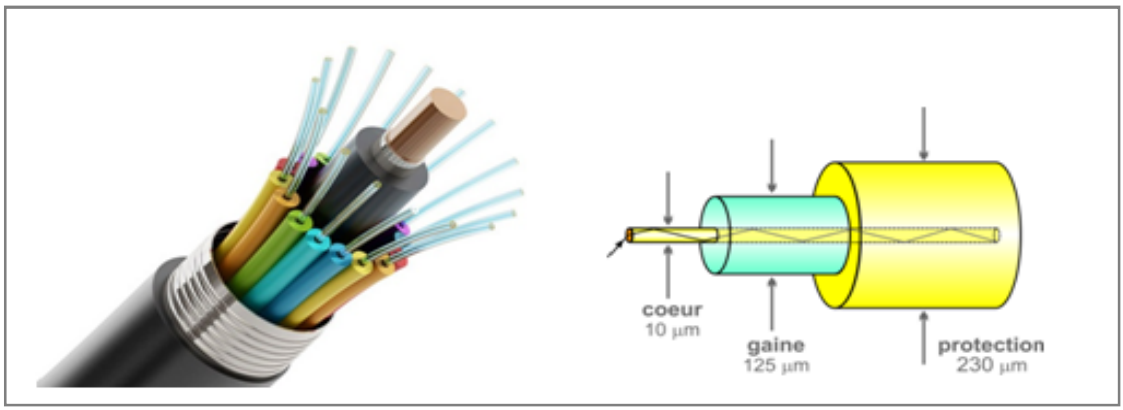
- Entre une antenne TV (râteau ou parabole satellite) et un récepteur de télévision.
- Entre un émetteur et l'antenne d'émission (les antennes des BTS, la carte Wi-Fi, antenne de radio FM..).
- Entre des équipements de traitement du son (microphone, amplificateur,..).
- Pour le transport d'un signal vidéo (caméra de surveillance).
- Dans les anciens réseaux de transmissions de données.

Figure(2): Les Câbles coaxiaux

3.3. Les fibres optiques

Une fibre optique est constituée d'un fil de verre très fin. Elle comprend un cœur, dans lequel se propage la lumière émise par une diode électroluminescente ou une source laser et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre.

Les avantages de la fibre optique sont nombreux: diamètre extérieur de l'ordre de 0,1 mm, poids de quelques grammes au kilomètre. Cette réduction de taille et de poids la rend facile à utiliser. En outre, sa très grande capacité permet la transmission simultanée de nombreux informations. Les points de régénération des signaux sont plus éloignés (jusqu'à 200 km), du fait de l'atténuation moindre de la lumière. Enfin, l'insensibilité des fibres aux parasites électromagnétiques est un avantage très apprécié. Par ailleurs, elle résiste bien aux écarts de température. La fibre optique constitue la plupart des artères des réseaux de télécommunications et des réseaux locaux à très haut débit.



Figure(3): Les fibres optiques

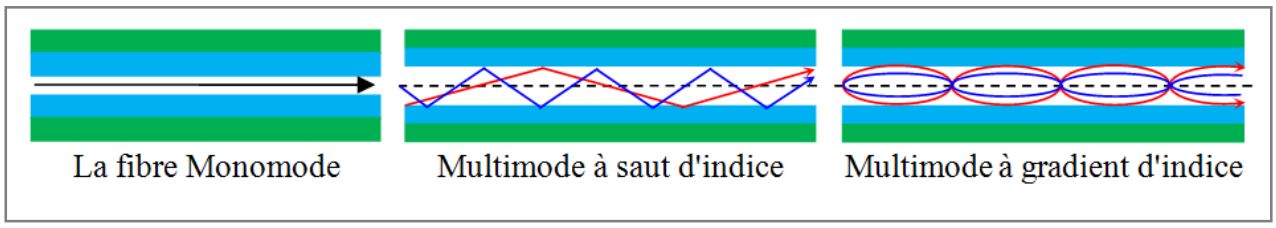
On distingue deux sortes des fibres optiques :

3.3.1. Les fibres multimodes

Les fibres multimodes Ou MMF (*Multi Mode Fiber*) ont été les premières fibres optiques sur le marché à partir des années 1970. Plusieurs longueurs d'onde bien choisies peut se propagent simultanément en de multiples trajets dans le cœur de la fibre, sur des distances de l'ordre du Km. Ces fibres étaient réservées aux débits inférieurs au Gbit/s, et sont souvent utilisées en réseaux locaux. Il existe deux sortes de fibre multimode selon l'indice de réfraction de la lumière entre le cœur et la gaine de la fibre: La fibre multimode à saut d'indice et la fibre multimode à gradient d'indice.

3.3.2. La fibre monomode

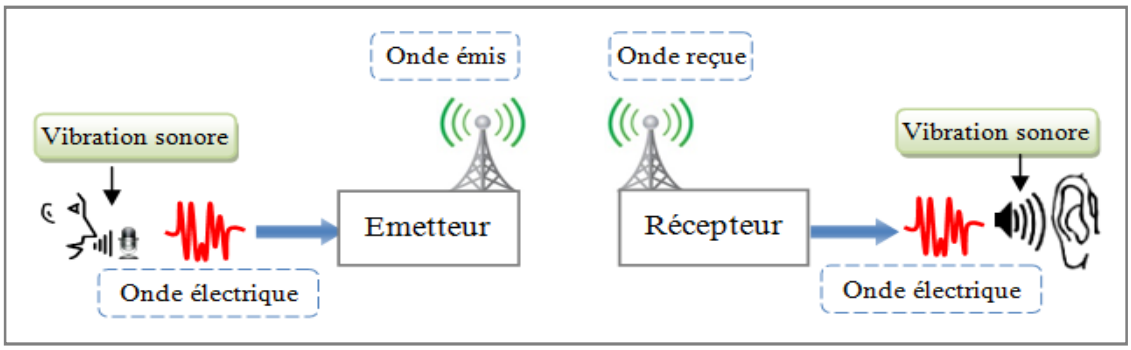
La fibre monomode Ou SMF (*Single Mode Fiber*) de fabrication plus récente, plus fine, assure la propagation d'une seule longueur d'onde dans son cœur. Elle ne peut pas transporter le signal qu'en un seul trajet sur des distances 50 fois plus que celle de la fibre multimode. Elle utilisé dans des réseaux à long distance pour des débits plus élevés.



Figure(4): Propagation des signaux dans le cœur des fibres optiques (différents modes)

3.4. Les ondes radioélectriques (radiocommunication)

Ondes radioélectriques ou ondes hertziennes: ondes électromagnétiques dont la fréquence est par convention comprises entre 9 kHz et 300 GHz, qui correspond à des longueurs d'onde de 33 km à 1mm [2], se propageant dans l'espace sans guide artificiel. Ces ondes sont diffusées d'un émetteur, on peut les capter avec des récepteurs dispersés géographiquement.



Figure(5): Exemples d'une transmission par les ondes radioélectriques

3.4.1. Propagation des ondes radioélectriques

Les ondes radioélectriques se propagent dans l'espace vide à la vitesse de la lumière et avec une atténuation de la puissance transportée par unité de surface proportionnelle au carré de la distance parcourue selon l'équation: $v = \lambda . f = \lambda / T$, Avec:

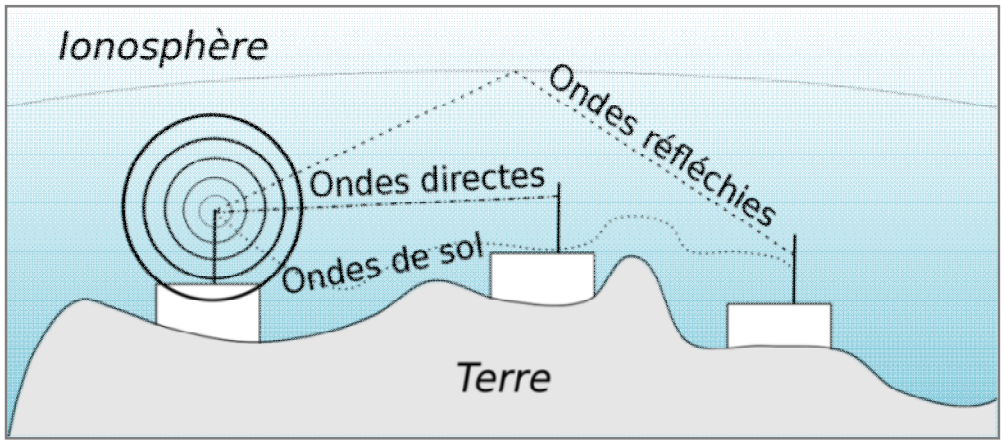
v: Vitesse de propagation d'onde (m/s),

λ: Langueur d'onde (m),

f : Fréquence (Hz),

T: Période (s).

Contrairement aux faisceaux hertziens, il n'est pas nécessaire d'avoir une visibilité directe entre l'émetteur et le récepteur car le récepteur utilise l'ensemble des ondes réfléchies et diffractées. Dans l'atmosphère, elles subissent des atténuations liées aux précipitations, et peuvent être réfléchies ou guidées par ionosphère. Elles sont atténuées ou déviées par les obstacles, selon leur longueur d'onde, la nature du matériau, sa forme et sa dimension. Pour simplifier, un matériau conducteur aura un effet de réflexion, alors qu'un matériau diélectrique produira une déviation, et l'effet est lié au rapport entre la dimension de l'objet et la longueur d'onde.



Figure(6): Propagation des ondes radioélectriques

3.4.2. Bandes de fréquences allouées

L'utilisation des ondes radioélectriques comme un support de transmission pour relier des équipements géographiquement dispersés est soumis à la sélection des fréquences, l'ensemble de ces fréquences constitue le spectre radiofréquence. Le spectre est divisé conventionnellement en bandes d'une décade [2], dont les appellations internationales sont normalisées. La table suivante illustre ces classements:

Désignation internationale	Fréquence	Longueur d'onde	Autres appellations	Exemples d'utilisation
ELF (*extremely low frequency*)	3 Hz à 30 Hz	100 000 km à 10 000 km		Détection de phénomènes naturels
SLF (*super low frequency*)	30 Hz à 300 Hz	10 000 km à 1 000 km		Communication avec les sous-marins
ULF (*ultra low frequency*)	300 Hz à 3 000 Hz	1 000 km à 100 km		Détection de phénomènes naturels
VLF (*very low frequency*)	3kHz à 30 kHz	100 km à10 km	Ondes myriamétriques	Communication avec les sous-marins, Implants médicaux, Recherches scientifiques…
LF (*low frequency*)	30 kHz à 300 kHz	10 km à 1 km	grandes ondes ou ondes longues ou kilométriques	Radioamateur, Radionavigation, Radiodiffusion GO, Radio-identification
MF (*medium frequency*)	300 kHz à 3 MHz	1 km à 100 m	petites ondes ou ondes moyennes ou hectométriques	Radioamateur, Radiodiffusion PO, Service maritime, Appareil de recherche de victimes d'avalanche
HF (*high frequency*)	3 MHz à 30 MHz	100 m à 10 m	Ondes courtes ou décamétrique	Organisations diverses, Militaire, Radiodiffusion OC, Maritime, Aéronautique, Radioamateur, Météo, Radio de catastrophe, etc.
VHF (*very high frequency*)	30 MHz à 300 MHz	10 m à 1 m	ondes ultra-courtes ou métriques	Radiodiffusion FM, Radiodiffusion RNT, Aéronautique, Maritime, Radioamateur, Gendarmerie nationale française, Pompiers, Réseaux privés, taxis, militaire, Météo, etc.
UHF (*ultra high frequency*)	300 MHz à 3 GHz	1 m à 10 cm	Ondes décimétriques	Réseaux privés, militaire, GSM, GPS, téléphones sans fil (DECT), Wi-Fi, Télévision, Radioamateur,..
SHF (*super high frequency*)	3 GHz à 30 GHz	10 cm à 1 cm	Ondes centimétriques	Réseaux privés, Wi-Fi, Micro-onde, Radiodiffusion par satellite (TV), **Faisceau hertzien**, Radar météorologique, Radioamateur, etc.
EHF (*extremely high frequency*)	30 GHz à 300 GHz	1 cm à 1 mm	Ondes millimétriques	Réseaux privés, Radars anticollision pour automobiles, Liaisons vidéo transportables, **Faisceau hertzien**, Radioamateur, etc.
Terahertz	300 GHz à 3 000 GHz	1 mm à 100 µm	Ondes submillimétriques	scanner corporel

Table (1): Occupation du spectre radiofréquence. [2]

3.4.3. Avantages des ondes radioélectriques

- le faible coût d'installation d'un réseau à grande échelle, puisqu'il ne nécessite pas d'installer des supports physiques entre chaque nœud et terminaux du réseau, il suffit d'installer une antenne.

3.4.4. Inconvénients des ondes radioélectriques

- Un mode de transmission le plus soumis aux perturbations extérieures et aux effets néfastes du support de transmission.

- Les transmissions des données à travers le canal radioélectrique ne peuvent pas être sécurisées et n'importe quelle antenne adaptée à la fréquence de transmission est susceptible de capter le signal.

- Le canal radioélectrique subit de très fortes atténuations avec l'éloignement. En espace libre (sans obstacles), le modèle de propagation d'une onde ne dépend que de la distance séparant les 2 antennes et de la fréquence.

3.5. Les faisceaux hertziens (FH)

Un faisceau hertzien est un système de transmission de signaux (aujourd'hui principalement numérique), monodirectionnel ou bidirectionnel, permanente entre deux points fixes. Il utilise la liaison point à point en hyperfréquence pour la transmission des données. Les faisceaux hertziens utilisent comme le support les ondes radioélectriques ou les fréquences de porteuses allant entre 1GHz et 86 GHz (gamme des micro-ondes), la bande de fréquences utilisée dépend du débit et de la distance entre les deux points.

Les faisceaux hertziens permettent de minimiser la perte de puissance et la concentrer dans un sens bien précis à l'aide des antennes très directives.

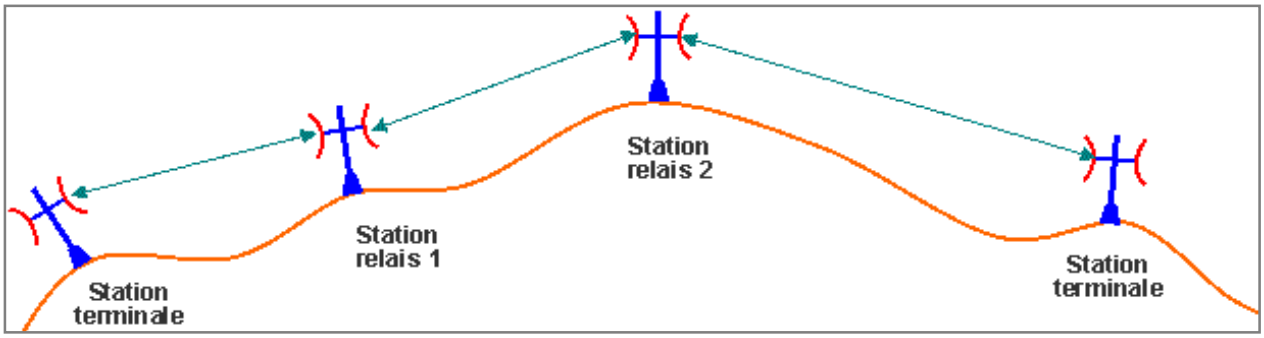
3.5.1. Domaine d'utilisation de FH

L'intérêt principal des liaisons hertziennes et qu'elles ne nécessitent pas de support physique entre l'émetteur et le récepteur de l'information, alors:

- C'est le moyen de communication idéal pour les liaisons avec les objets mobiles: piétons, automobiles, bateaux, trains, avions, satellites,..etc.

- Les liaisons hertziennes sont intéressantes dans le cas de la diffusion (radio diffusion et télédiffusion), où l'on a un émetteur et plusieurs récepteurs. En effet, pour couvrir une ville, il est plus simple et moins cher d'installer un émetteur et une antenne chez chaque particulier, plutôt que de relier par câble chaque particulier.

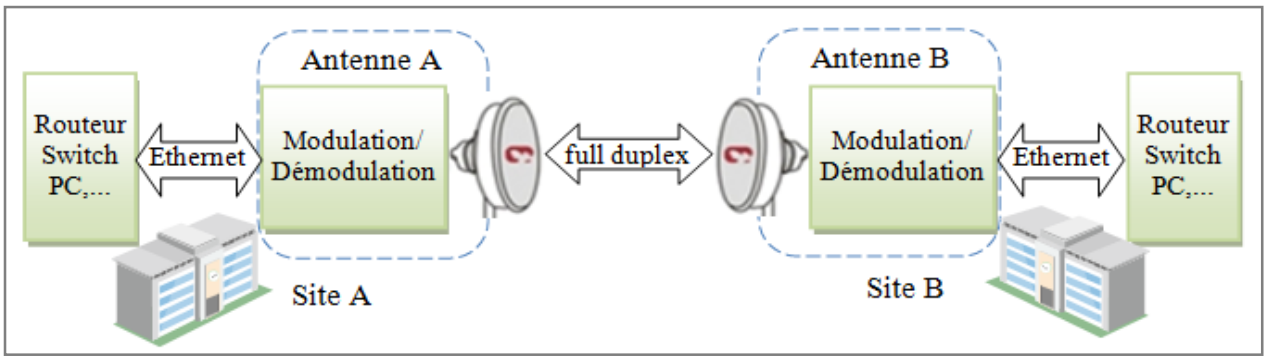
- Une liaison hertzienne permet de relier deux sites distants et difficiles d'accès (régions montagneuses), avec un débit élevé et très sécurisé, ainsi un coût d'installation et de déploiement faible.



Figure(7): Raccordement des sites éloignés par des liaisons FH

- **Les faisceaux hertziens analogiques (FHA)**: utilisés principalement pour la transmission des multiplex analogiques dont la capacité va de quelque voie téléphonique à 2700 voies téléphoniques. La transmission des images TV, et des voies de sons qui leur associées et aussi d'autres signaux tels que les données.

- **Les faisceaux hertziens numériques (FHN):** qui acheminent principalement des multiplex numériques pour les données à grande vitesse: Le visiophone, la télévision codée, comme un liens haut débit d'un réseau LAN,..etc.



Figure(8): Exemple d'utilisation d'une liaison FH

3.5.2. Les modulations utilisées en FH

Les équipements radio analogiques et numériques sont différent fondamentalement par le type de modulation qu'ils utilisent. Pendant que les FHA utilisent la modulation de fréquence, les FHN utilisent les modulations par sauts de phase ou multi états (multi niveaux) ou modulation sur fréquence porteuse.

Modulations analogiques

- **Modulation d'amplitude**: La modulation analogique, est appliquée à la porteuse ou sous-porteuse proportionnellement au signal à transmettre, en **modifiant l'amplitude** ou l'argument de l'onde sinusoïdale.

- **Modulation angulaires** (ou d'argument): Les modulations de fréquence (FM) et de phase (PM) **modifient l'argument** (ou **angle**) de l'onde sinusoïdale. L'onde résultante garde une amplitude constante, permettant d'utiliser des amplificateurs non linéaires et diminuant l'influence des perturbations additives (bruit impulsions et interférences).

- Modulation multiple: La modulation analogique de deux porteuses en quadrature est utilisée pour la transmission des composantes de couleur sur la sous- porteuse du dispositif PAL, ou la modulation simultanée en phase et amplitude dans le dispositif NTSC.

Modulation numérique

- **Modulation élémentaires**

- La modulation en tout-ou-rien (OOK: *On Off Keying*) elle est utilisée en télégraphie, et elle est particulièrement adaptée à la reconnaissance auditive par un opérateur.

- En modulation d'amplitude (ASK), l'amplitude est commutée entre plusieurs valeurs discrètes.

- En FSK ou PSK ce sont respectivement la fréquence et la phase qui sont commutées.

- En APK (ou QAM) la phase et l'amplitude prennent différentes valeurs discrètes.

- **Modulations complexes**

Des combinaisons plus complexes sont utilisées pour optimiser le débit vis à vis de la bande passante. Ainsi, la combinaison de deux modulations d'amplitude et de phase simultanées sur une même porteuse sert à doubler le débit binaire. Des cas spécifiques sont souvent utilisés pour certains avantages précis: ainsi le MSK (*Minimum Shift Keying*) est une modulation numérique de fréquence d'indice de modulation précis et de largeur spectrale minimale.

3.6. Autres supports

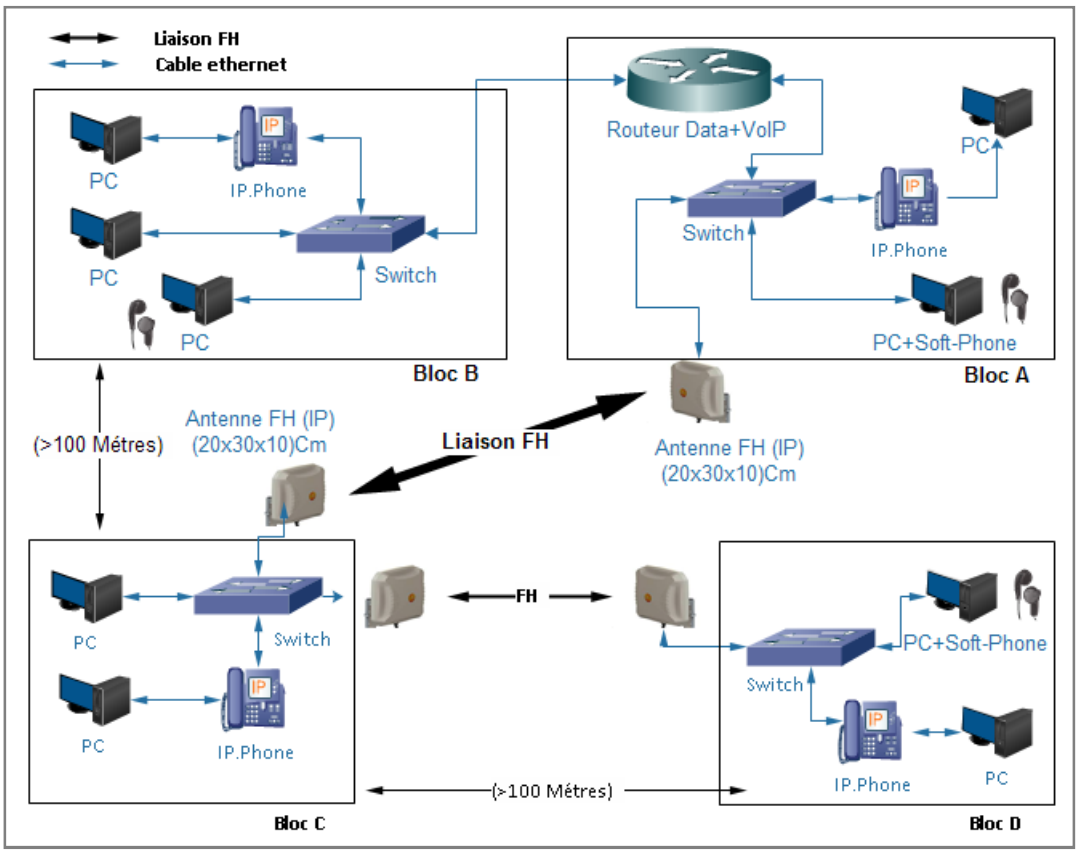
D'autres supports de transmission existent comme les supports de stockage que sont les CD, les DVD ou les disques durs. Ils représentent aussi des moyens de transfert d'information et sont aussi soumis à des contraintes spécifiques en termes de taux d'erreur. Il est important de connaître les caractéristiques d'un support de transmission ainsi que leurs limitations pour le dimensionnement d'un canal de transmission (capacité max d'information transmise, bande passante), techniques à adopter pour assurer la qualité de service. Enfin, il faut s'assurer des réglementations associées à l'utilisation d'un support.

Partie II: Les antennes FH type Access5830

Introduction

Une bonne connaissance des communications sans fil permet aux opérateurs de bien gérer les ressources, de faciliter l'évolution de leur réseau en intégrant des techniques plus performantes.

Dans cette partie, nous couvrirons la configuration d'une antenne radio FH à large bande appelée **Access5830**, et on montre les concepts opérationnels et fonctionnels de divers composants de ce système, afin de l'utiliser dans la réalisation de la topologie ci-dessous:



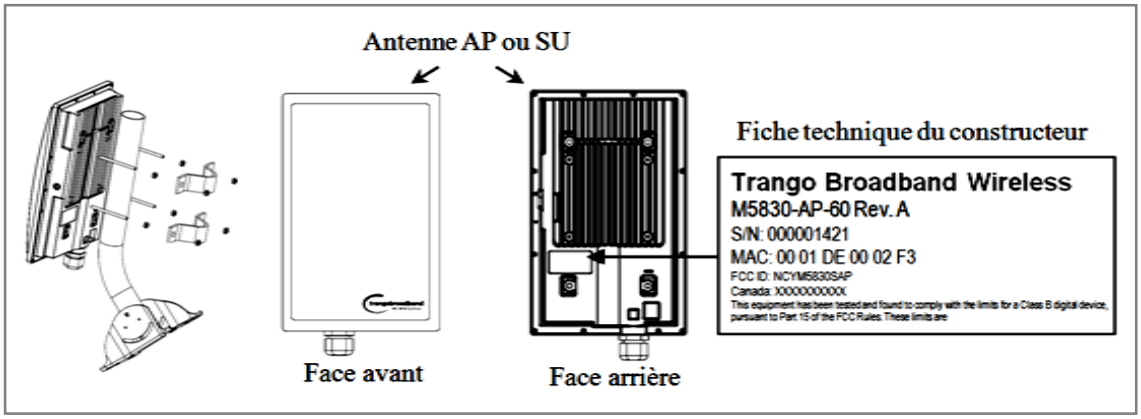
Figure(9): Intégration des antennes FH pour interconnecter les réseaux LAN

1. Aperçu

Le système Access5830 du fabricant ***Trango Broadband Wireless*** est un moyen de transmission sans fil bidirectionnel en utilisant les ondes radioélectriques en visibilité direct. Ce système se compose de deux types d'antennes radios:

- Unité ***Master*** type **Access5830-AP**: sont des points d'accès (AP: *Access Points*) bi-bande avec antenne sectorielle interne.

- Unité ***Slave*** type **Access5830-SU**: sont des unités d'abonné (SU: *Subscriber Units*) bi-bande avec antenne interne.



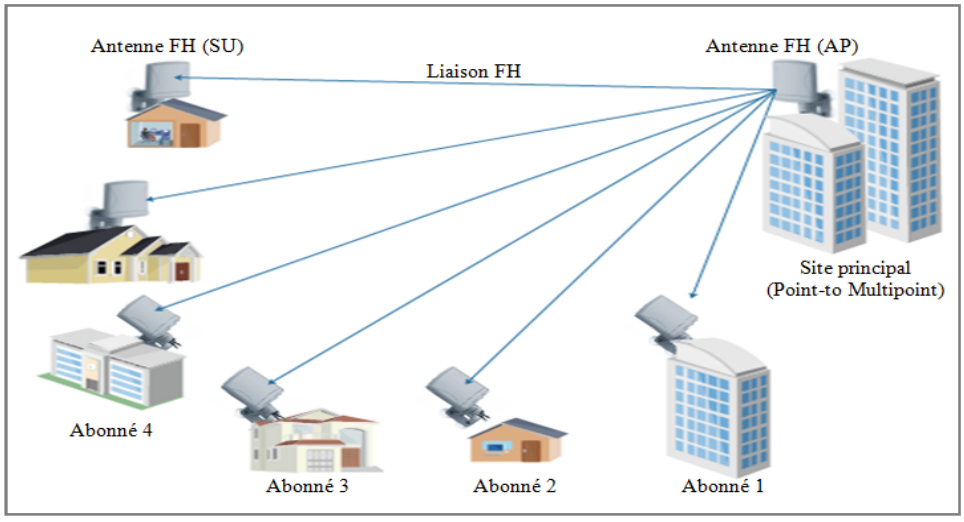
Figure(10): Forme d'antenne Access5830 (AP ou SU)

2. Principe de fonctionnement

L'unité AP agit comme un concentrateur dans un réseau sans fil multipoint de configuration en étoile prenant en charge jusqu'à 512 unités d'abonnés. Le système Access5830 est classé comme un pont multipoint de couche 2. L'authentification des SU est effectuée à l'aide d'une méthode sécurisée et propriétaire au niveau MAC (*Media Access Control*), et donc toutes les formes de trafic Ethernet et d'adresses IP illimitées passeront de manière transparente sur le système.

Les AP et les SU peuvent être facilement configurés et gérés (localement ou à distance) via des interfaces série et Ethernet intégrées, ainsi qu'un outil d'approvisionnement de navigateur Web pour une configuration et un déploiement rapides. Les antennes Access5830 sont alimentées en utilisant "Power over Ethernet" pour une installation facile et à faible coût. Les AP et les SU disposent d'un outil "d'enquête de site" pratique pour vérifier les interférences. L'AP offre un service de connexion large bande à un ou plusieurs SU selon un algorithme de sondage dynamique adaptatif propriétaire appelé *SMARTPolling*. Les opérateurs de réseau peuvent co-localiser plusieurs (jusqu'à 22) points d'accès sur un site, augmentant ainsi le débit global disponible à chaque point. [3]

Le point d'accès Access5830-AP fournit une multitude d'outils et de fonctions complets. Ce point d'accès réside généralement au centre du réseau point à multipoint (PMP) et exécute toutes les fonctions de gestion, y compris l'allocation de bande passante pour tous les SU associés.



Figure(11): Déploiement typique des antennes FH (*Point-to-Multipoint*)

Le système radio *Trango Broadband Access5830* offert un moyen fiable et robuste pour fournir un accès haut débit et une connectivité Ethernet sans fil à une vaste zone géographique.

L'Access5830 bi-bande est une solution point à multipoint très polyvalente et économique pour les applications de connectivité d'entreprise et des fournisseurs de services sans fil à large bande. L'Access5830 offre jusqu'à 100 Mbps en direct et fonctionne dans la bande ISM 5,8 GHz (*Industrial, Scientific and Medical*) ou la bande U-NII 5,3 GHz (*Unlicensed National Information Infrastructure*). Les antennes à double polarisation (sans chevauchement) commutables par un logiciel, couplées à deux bandes de fonctionnement en fréquence (total de 22 canaux). [3]

3. Etablissement de la connexion entre l'unité AP et SU

L'un des principaux avantages du système Access5830 est la capacité de l'AP à gérer plusieurs connexions SU et à partager le débit de données de 100 Mbps de manière très efficace. L'allocation de bande passante est gérée par l'algorithme *SmartPolling* du point d'accès conformément aux règles d'approvisionnement définies par l'administrateur du système. L'AP interroge chaque SU dans un format à tour de rôle pour déterminer si le SU a des données à transférer. Le SU ne transmet les données à l'AP que lorsque l'AP donne l'autorisation. Le SU analyse chaque paquet de données arrivent de l'AP et identifie les paquets qui lui sont destinés. Pour qu'un SU communique avec un AP, l'administrateur système doit d'abord ajouter l'adresse MAC et le numéro d'identification du SU à la base de données utilisateur dans l'AP.

L'algorithme *SmartPolling* interrogera les SU actifs plus souvent, pour réserver le meilleur parti de la bande passante, et négocier le débit, la taille maximal de l'information et le réglage de priorité. Chacun des paramètres ci-dessus est défini dans l'AP par l'administrateur système et ne peut pas être contrôlé au niveau du SU.

Lorsque l'alimentation est appliquée pour la première fois à un SU correctement installé, il balaye tous les canaux de sa table de balayage, recherchant un AP qui envoie des autorisations de transmission avec le même ID de base que celui défini dans ce SU particulier. Le SU s'arrêtera alors sur ce canal et répondra à l'AP en utilisant la puissance RF (Radio Fréquence) maximale. Avant que l'AP puisse ajouter le SU à la liste d'interrogation, il doit authentifier le SU en vérifiant l'adresse MAC et en effectuant une opération de localisation sur le SU. Après avoir localisé avec succès le SU, l'AP ajoutera ensuite le SU à la liste d'interrogation, et il ajustera la puissance de transmission RF dans le SU en fonction du paramètre Target RSSI dans l'AP. [3]

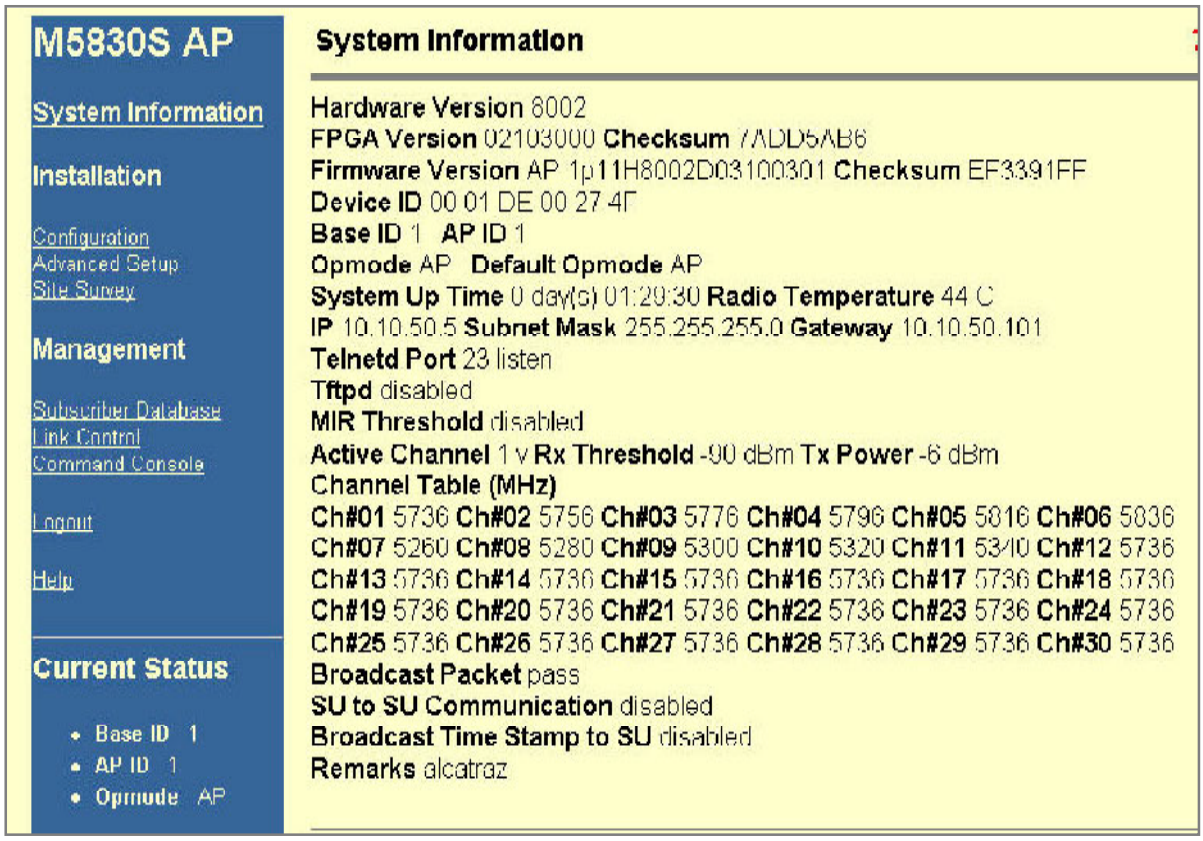
4. Configuration des antennes Access5830

Des connexions appropriées aux radios et une planification de routage IP soigneuses permettront à l'administrateur du réseau d'accéder et de gérer les radios à distance sur le réseau. La gestion de la radio sur TCP / IP peut être effectuée à partir de PC connectés au côté Ethernet de chaque radio. De plus, les PC connectés à l'AP peuvent gérer le SU via leur connexion sans fil. Cependant, un PC connecté à un SU ne peut pas accéder à l'AP via la connexion sans fil.

Après avoir allumé les antennes AP et SU, on peut accéder à la configuration de AP à travers son port Ethernet (TCP/IP), en utilisant un câble Ethernet croisé et un ordinateur (PC) a un navigateur Web (HTTP) installé. Il faut Configurer la connexion Ethernet du PC au sous-réseau qui est routable vers la radio (adresse IP par défaut = 192.168.100.100), et après, cette fenêtre apparaîtra:

Figure(12): Page de connexion au système Access5830-AP en utilisant le navigateur Web

- Tapez le mot de passe (**trango** par défaut) et continuez. Cela fera apparaître la page d'informations sur le système de la radio:



Figure(13): Page d'informations système

Ce qui suit décrit les principales fonctionnalités montré dans la figure 13:

- **Colonne de navigation**: il s'agit de cette colonne rectangulaire bleue à gauche, qui apparaît sur toutes les pages. Le haut est le numéro de modèle de la radio à laquelle vous êtes connecté. Au bas de cette colonne se trouve l'état actuel de la radio, y compris son ID de base, son ID-AP et son mode de fonctionnement actuel.

- ***System Information*** (Page d'informations système): cette page affiche la plupart des paramètres de configuration de base de la radio. Il s'agit de la première page affichée après la connexion.

- ***Configuration*** (Page de configuration): les paramètres essentiels, tels que l'ID de base, le canal et la polarisation sont définis ici.

- ***Advanced Setup*** (Configuration avancée): les paramètres RF avancés, tels que la puissance de transmission, sont définis ici.

- ***Site Survey*** (Sondage de site): À partir d'ici, en mode *Opm Off*, l'utilisateur peut effectuer une analyse du spectre.

- ***Subscriber Database*** (La base de données des abonnés): il s'agit de la page permettant de définir les SU pouvant être associés à l'AP.

- ***Link Control*** (Contrôle des liens): déterminez quels SU sont connectés et comment ils fonctionnent.

- ***Command Console*** (Console de commandes): exécute toute commande de console qui n'est pas interactive (par exemple *Ipconfig*). Les résultats sont rapportés via l'écran HTTP. Pour une liste complète des commandes de la console, tapez "help" dans le champ de saisie.

- ***Logout Link*** (Déconnexion): pour fermer la session HTTP en cours avec la radio.

- ***Help*** (Aide): l'interface du navigateur comporte des pages d'aide utiles qui expliquent tous les paramètres répertoriés.

5. Configuration de base via l'interface du navigateur

Cette section décrit quelques concepts de base supplémentaires et comment établir une liaison sans fil entre AP et SU, à l'aide de l'interface du navigateur (HTTP).

Essentiels, pour établir une liaison sans fil il faut:

- L'ID de base dans AP et SU doit correspondre.

- L'ID SU et l'adresse MAC dans SU doivent correspondre à une entrée dans la base de données de l'unité d'abonné (SUDB)

- Le canal RF et la polarisation du point d'accès AP doivent exister dans la table de balayage des canaux du SU.

- AP doit être en mode opérationnel «AP»

- SU doit être en mode opérationnel «SU»

- • La puissance du signal doit être reçue à chaque radio.

Si tous ces paramètres sont remplis et si les AP et SU sont à portée et correctement alignés, la liaison sans fil s'établira automatiquement et le trafic d'échange commencera à passer entre les radios.

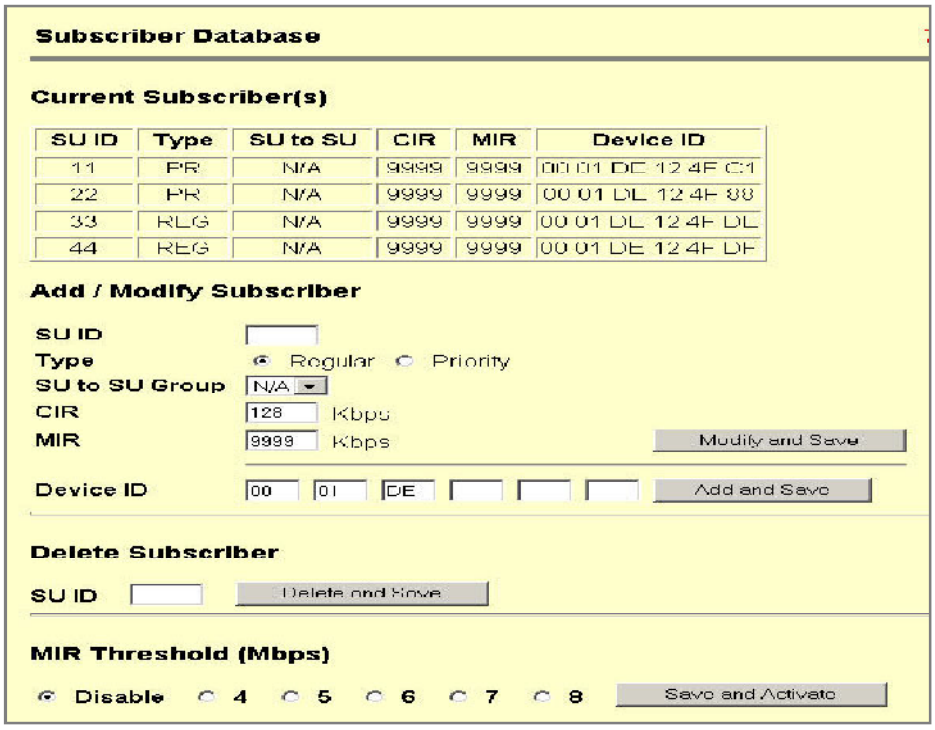
5.1. Configuration de la base de données d'AP

Avant d'établir une liaison sans fil, l'utilisateur doit configurer la base de données des unités d'abonné (SUDB) dans l'AP avec l'adresse MAC de chaque SU et les paramètres associés. La base de données des SU comprend des informations détaillées sur chaque SU. L'utilisateur utilise la page ***(Subscriber Database)*** qui se trouve dans **la Colonne de navigation** de l'interface principale pour ajouter, modifier et supprimer des SU. Les informations clés pour chaque SU sont les suivantes:

SU ID	ID de l'unité d'abonné définissable par l'utilisateur (1… 8190)
TYPE:	*PR Priority* ou *REG Regular*. Les SU prioritaires sont privilégiées dans le processus d'interrogation dynamique et répondent donc avec moins de latence que les SU ordinaires.
SU to SU:	Groupe # (1..F en hex) pour les communications SU à SU. Seuls les SU ayant le même numéro de groupe SU au SU peuvent communiquer entre eux. Les SU utilisant la communication SU à SU doivent être sur le même sous-réseau**.**
CIR	*Committed Information Rate*: Taux d'information engagé. Débit minimum (Kbps) auquel AP tentera de livrer.
MIR	*Maximum Information Rate:* bande passante à ce SU. Le maximum est 9999
Device ID	Adresse MAC du SU. L'adresse *SUID* et MAC du SU couplée à *BASE ID*, sont la base de l'authentification avec l'AP.

Table (2): Les rubriques de la page *Subscriber Database* dans l'AP

- Connectez-vous à l'AP et ouvrez la page ***Subscriber Database***, pour modifier les champs illustre dans la table précédente:



Figure(14): La page *Subscriber Database* dans l'AP

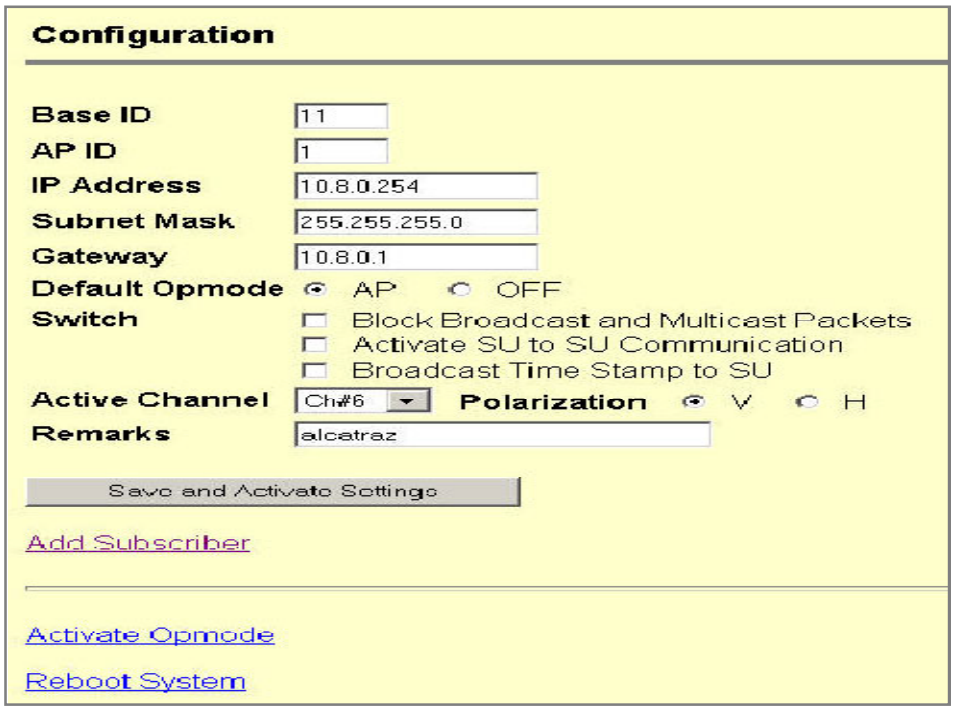
5.2. Configuration d'autres paramètres de l'AP

Les paramètres suivants de la page ***Configuration*** du AP doivent être définis (ou laissés par défaut):

Base ID	ID de station de base définissable par l'utilisateur (1-127); généralement affecté à un groupe de AP sur un site cellulaire particulier. L'ID de base dans AP doit correspondre à l'ID de base dans SU pour que le lien soit établi. Ce paramètre ne peut être modifié que lorsque le *Opmode* est "*OFF*".
AP ID:	ID AP définissable par l'utilisateur (1-255). Ce paramètre est à titre informatif uniquement et ne joue aucun rôle dans l'établissement de la liaison.
IP Address, Subnet Mask, Gateway:	La configuration IP de cette radio pour la gestion et l'accès à distance, ces paramètres ne jouent aucun rôle dans l'établissement de la liaison sans fil.
Default Opmode:	Mode de fonctionnement de la radio. Lorsque la radio entre en mode "AP", elle transmet, s'est en mode "OFF", la radio n'émet pas,
Active Channel/Polarization:	Le canal actuel et la polarisation d'antenne de cet appareil.

Table (3): Les rubriques de la page *Configuration* dans l'AP

- Connectez-vous à l'AP et ouvrez la page de ***Configuration***:



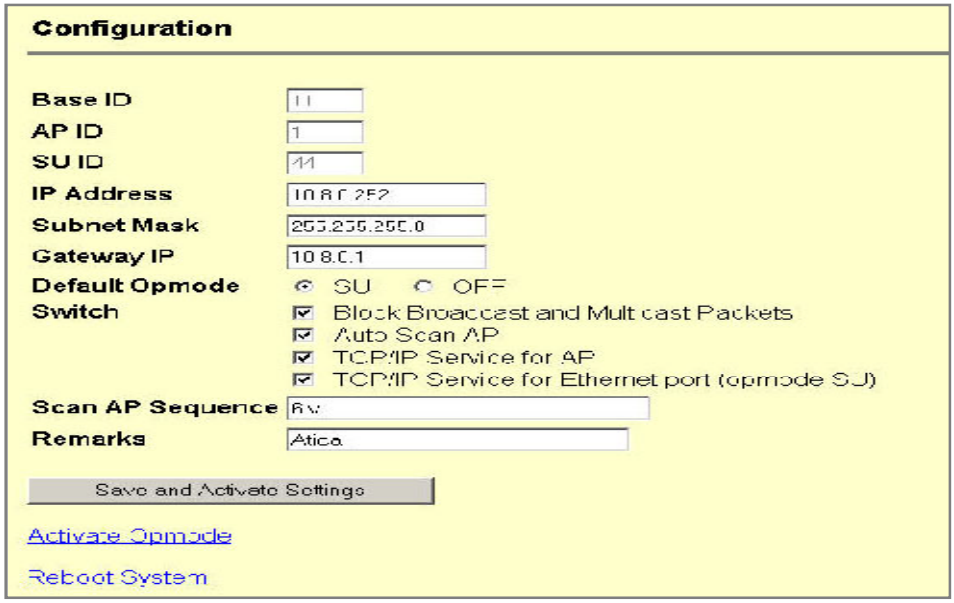
Figure(15): La page *Configuration* dans l'AP

5.3. Configuration des paramètres de base de SU

Chaque SU doit être configuré avec des informations de base pour communiquer avec l'AP. Au minimum, l'ID de base doit correspondre à l'ID de base de l'AP, l'ID SU doit correspondre à l'ID SU dans la SUDB de l'AP, et le canal actif de l'AP doit exister dans la séquence de balayage AP de la SU.

Pour configurer le SU, procédez comme suit:

1. Connectez-vous au SU et ouvrez la page: ***Configuration***.



Figure(16): La page *Configuration* dans l'SU

2. Définir l'ID de base (doit correspondre à l'AP)

3. Définir l'ID SU (doit correspondre à l'entrée dans le SUDB sur l'AP)

4. Définissez l'IP, le sous-réseau et la passerelle (pour la management)

5. Définissez ***Default Opmode*** sur "SU"

6. Entrez une série de canaux et de polarisations dans ***Scan AP Sequence*** (y compris ceux sur AP)

7. Enregistrer et activer les paramètres

8. Redémarrez le système (cela mettra fin à votre session HTTP)

À ce point, si tous les paramètres ont été correctement définis et si les radios sont à portée, une association entre AP et SU se produira.

Conclusion

Dans ce chapitre, nous avons donné une description générale des supports de transmission, le domaine de leurs utilisations, ainsi que leurs avantages et inconvénients, ensuite nous avons présenté les caractéristiques techniques de système Access5830, en précisant son architecture d'une façon détaillée et enfin nous avons clôturé par les étapes pratiques de la configuration de ce système.

Chapitre 2:

La sécurité de la VoIP

Chapitre II: La Sécurité de la VoIP

Introduction

Nous avons devisé ce chapitre sur deux parties, l'objectif de la **première partie** est l'étude de la technologie VoIP et ses différents aspects. Nous parlerons sur l'architecture de la VoIP et ses éléments, les services fournis par cette technologie. Nous détaillerons aussi ces protocoles de signalisation et de transport ainsi que leurs principes de fonctionnement et leurs principaux avantages et inconvénients.

Nous avons dédié la **deuxième partie** de ce chapitre pour présenter les vulnérabilités de réseau VoIP, et différentes attaques les plus fameux qui menacent la sécurité de ce réseau, nous parlerons aussi sur les différentes techniques de sécurité qui apportent les solutions lesquelles on peut implémenter pour minimiser les risques associes au réseau VoIP.

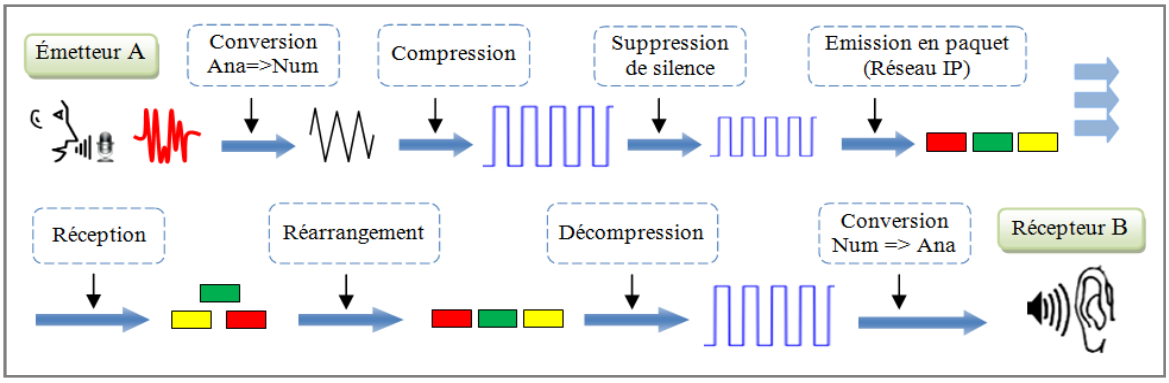
Partie I: Présentation de la VoIP

Introduction

La voix sur protocole d'internet (VoIP) constitue actuellement une évolution très importante dans le domaine des Télécommunications. Avant 1970, la transmission de la voix s'effectuait de façon analogique sur des réseaux dédiés à la téléphonie, la technologie utilisée était la technologie électromécanique (*Crossbar*). Dans les années 80, une première évolution a été le passage à la transmission numérique TDM (*Time Division Multiplexing*). La transmission de la voix sur les réseaux informatiques à commutation de paquets IP constitue aujourd'hui une évolution majeure comparable aux précédentes. [4]

1. Définition

La voix sur IP (VoIP: *Voice Over Internet Protocol*), est le fait de transmettre de la voix sur un réseau IP. La voix est digitalisée, compressée puis envoyée au récepteur par paquets de données, ces paquets doivent être acheminés dans le bon ordre et dans un délai raisonnable pour que soit correctement reproduite. Les données reçues par le destinataire sont décompressées et converties en voix audible. [5]



Figure(17): Principe de numérisation de VoIP

2. Les services fournis par la VoIP

La VoIP offre de nouvelles possibilités aux utilisateurs qui bénéficient d'un réseau IP, c'est pour cette raison là que les entreprises s'orientes vers la VoIP comme solution pour la téléphonie. Les services fournis les plus marqués sont les suivants:

- **Réduction des couts :** le trafic véhiculé à travers le réseau RTC (Réseau Téléphonique Commuté) 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). [6]

- La VoIP fournir des nouveaux services tel que: la messagerie vocale, le transfert, la mise en attente et l'identification des appels, la conférence a trois ou plus, la recomposition du numéro, la composition abrégée, l'indicateur de réception de message vocal.

- **La mobilité infinie:** Les utilisateurs de la VoIP n'ont plus besoin de rester scotché à un téléphone filaire pour recevoir ou passer des appels depuis son numéro. Désormais, depuis n'importe quel dispositif connecté à internet et situé au n'importe quel endroit dans le monde, l'utilisateur peut communiquer par son numéro. [6]

- **Un réseau voix, vidéo et données (*triple play*):** En positionnant la voix comme une application supplémentaire du réseau IP, l'entreprise ne va pas uniquement substituer un transport opérateur RTC à un transport IP, mais simplifier la gestion des trois réseaux (voix, données et vidéo) par ce seul transport. Une simplification de gestion, mais également une mutualisation des efforts financiers vers un seul outil. [6]

- Accès à votre système téléphonique à partir de votre ordinateur de bureau.

- La VoIP, en tant que signal numérisé, permet l'intégration des différents mécanismes de chiffrements afin de sécuriser les communications.

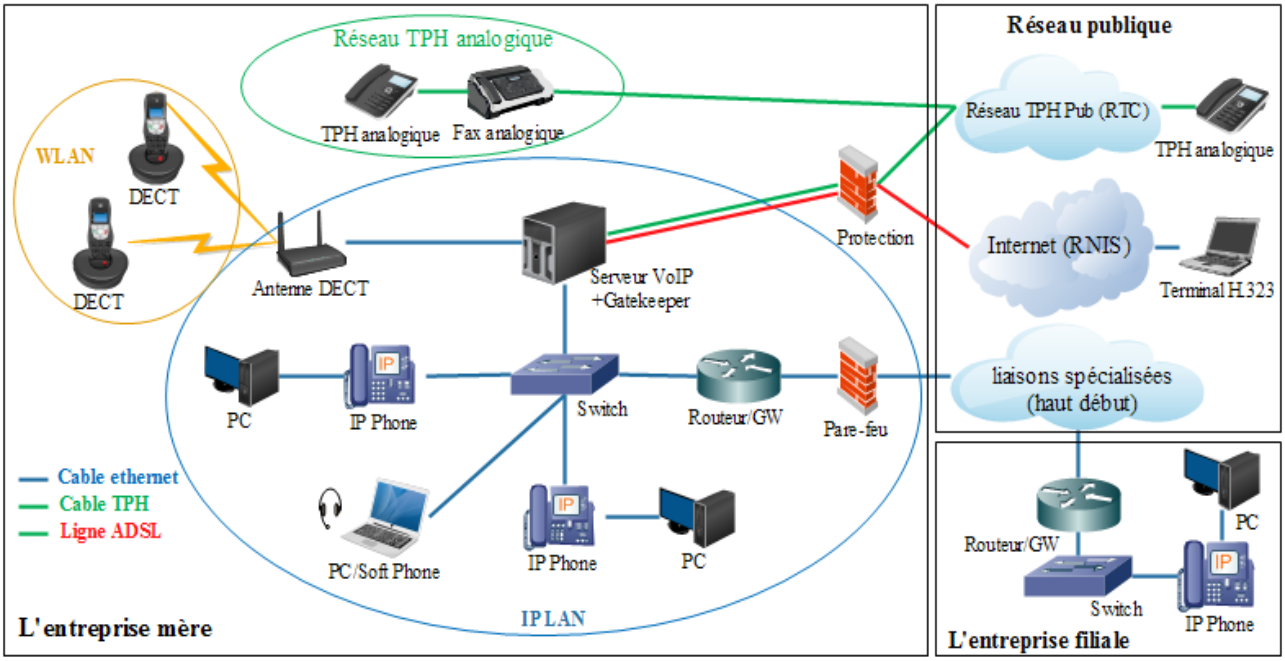
3. La différence entre VoIP et ToIP

Quand on parle de communication via internet, deux acronymes reviennent régulièrement: ToIP et VoIP. Qu'est-ce qu'ils veulent dire?

- **La VoIP** regroupe toutes les techniques permettant ce transit. Cela peut être une communication d'un téléphone IP à un PC, ou encore d'un ordinateur à un autre. Les communications voix sont transmises, par le réseau internet, de l'entreprise au standard (chez l'opérateur), puis à destination des interlocuteurs.

- **La Téléphonie sur IP** (ToIP) constitue une autre catégorie de communications, Elle va regrouper tous les échanges de téléphone à téléphone. La ToIP elle va permettre de relier chaque poste avec l'autocommutateur, via le réseau de l'entreprise.

4. Architecture de VoIP



Figure(18): Schéma générale d'un réseau VoIP dans une entreprise

La figure précédente décrit, d'une façon générale, la topologie d'un réseau VoIP. Elle comprend toujours d'un serveur VoIP, des terminaux et des passerelles vers les autres réseaux. Le réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/contrôleur de commutation, appelées Gatekeeper. **Nous retrouvons les éléments communs suivants**:

- **Serveur VoIP:** est un système de communication téléphonique complet qui fournit des appels téléphoniques à travers les réseaux de données IP. Toutes les conversations sont envoyées en tant que paquets de données sur le réseau. Un serveur VoIP peut être un PABX-IP (IPBX), soit un routeur doté d'option VoIP.

- **Le routeur (Passerelle):** Permet d'aiguiller les données et de router les paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles. Dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 du modèle OSI.

- **Gatekeeper**: (gardien de la porte) concentre aujourd'hui l'intelligence du réseau, a d'abord été introduit pour s'acquitter des tâches spécifiques. Le Gatekeeper devait assurer, dans le cas des communications RTC/IP, la traduction des adresses, le contrôle d'accès au réseau et la gestion de la bande passante. [7]

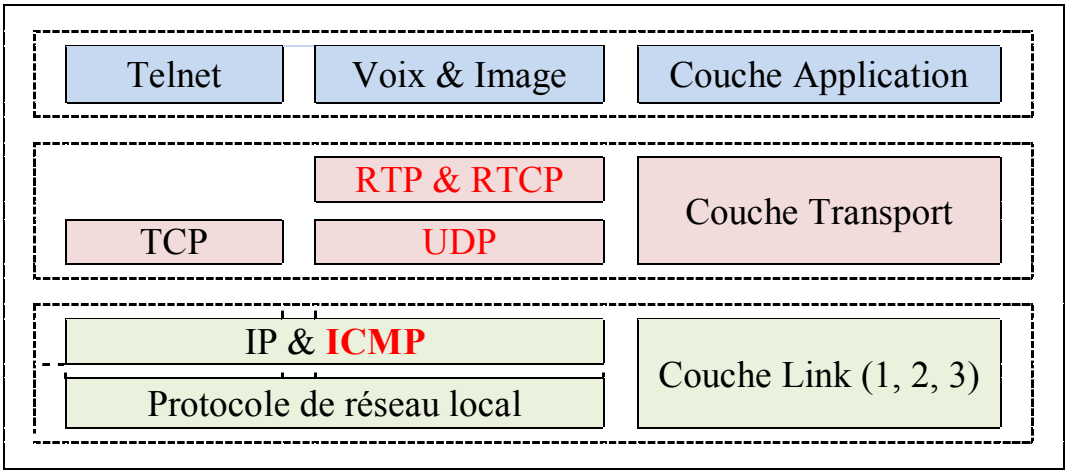
✓ *NB*: Il est nécessaire de savoir que les principales firmes produisant ce type d'équipements présentes aujourd'hui sur le marché, comme (Cisco, Clarent, Avaya, Alcatel, Nortel Network, Siemens, Ténovis, 3COM,..) ont eu tendance à combiner les fonctionnalités (routage/passerelle, serveur VoIP, Gatekeeper) en un seul équipement. D'ailleurs, la VoIP est un marché chevauchant deux secteurs (la téléphonie et l'informatique) qui se rapprochent et étaient complètement différent auparavant, nous assistons ici à une concurrence ayant des origines différentes. En effet, nous retrouvons le géant de l'équipement réseaux Cisco en concurrence avec des entreprises de téléphonies tel que: Alcatel ou Siemens.

- **Le Switch(Commutateur)**: Un Switch désigne un commutateur réseau, équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique. Dans les réseaux Ethernet la majorité des Switchs opèrent au niveau de la couche 2 du modèle OSI.

- **Les terminaux**: La voix sur IP propose trois types de terminaux différents : Les hardphones qui sont des téléphones physiques IP, les softphones qui sont des logiciels permettant de téléphoner sur IP au travers d'un PC, et les téléphones IP Wifi qui sont des téléphones sans-fil IP.

5. Les protocoles associés à la VoIP

Un protocole est un langage commun utilisé par l'ensemble des acteurs de la communication pour échanger des données. Dans cette partie on va parler des protocoles de transport de la voix et des protocoles de la signalisation.



Figure(19): Les protocoles RTP, RTCP, UDP, ICMP dans le modèle OSI

5.1. Le protocole RTP (Real-time Transport Protocol)

5.1.1. Définition:

RTP est un protocole de transport standardisé en 1996, développé par l'IETF, spécifiquement conçu pour faciliter le transport des paquets en temps réel de bout en bout, des flots multimédia (audio ou vidéo) sur les réseaux IP. RTP est si bien adapte a des applications a diffusion individuelle (*unicast*) qu'il est devenu une des pièces essentielles de la VoIP. Il se situe au niveau de la couche d'application et utilise les protocoles se sous-jacents de transport TCP ou UDP (*User Datagram Protocol*), mais l'utilisation de RTP se fait généralement au-dessus d'UDP, ce qui permet d'atteindre plus facilement le temps réel.

Le protocole RTP fournit un moyen uniforme de transmettre des données soumises à des contraintes en temps réel, tout en organisant les paquets à l'entrée du réseau et de les contrôler à la sortie. Il fournit ainsi:

- L'identification de la source et du type de charge utile, dans les applications en multicast, l'identité de la source doit être déterminée.

- La numérotation séquentielle des paquets et des marques de référence temporelles (*timestamping*): permet de détecter les paquets perdus. En revanche, il est impératif de repérer qu'un paquet a été perdu pour le remplacer éventuellement par une synthèse déterminée en fonction des paquets précédant et suivant.

5.1.2. Avantages du protocole RTP

Le protocole RTP permet de reconstituer les messages multimédia (audio, vidéo, etc.), de détecter les paquets perdus, et d'identifier le contenu des paquets pour leurs transmission sécurisée.

5.1.3. Inconvénients du protocole RTP

Les applications en temps réel, comme la parole numérique ou la visioconférence, exigent une certaine qualité de service (QoS) que RTP ne garantit pas du fait qu'il fonctionne au niveau applicatif.

5.2. Le protocole RTCP (Real-time Transport Control Protocol)

5.2.1. Définition

Le protocole RTCP est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. C'est un protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service, Le protocole RTP est utilisé au-dessus du protocole UDP en utilisant un port **pair** pour le protocole RTP et **impair** pour le protocole RTCP. [8]

Il existe cinq **types** différents de **paquets RTCP** pour chaque type d'information :

- **SR:** (*Sender Report*) contient des statistiques de transmission et de réception pour les participants qui sont des émetteurs actifs.
- **RR:** (*Receiver Report*) contient des statistiques de réception pour les participants qui ne sont pas des émetteurs actifs mais récepteurs d'une session.
- **SDES:** (*Source Description*) décrit la source : nom, email, tél, etc.
- **BYE:** permet à une station d'indiquer la fin de sa participation à une session.
- **APP:** est un paquet de signalisation spécifique à une application.

Le protocole RTCP remplit trois fonctions :

- **L'information sur la qualité de service**: RTCP fournit, en rétroaction des informations sur la qualité de réception des données transmises dans les paquets RTP.
- **L'identification permanente**: RTCP transporte une identification de la source RTP c'est-à-dire la provenance du flux, appelée CNAME (*Canonical name*). Cet identificateur permet une identification permanente de chacun des flux multimédia entrants.
- La connaissance à tout moment du nombre de participants présents dans la session.

5.2.2. Avantage du protocole RTCP

Le protocole de RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanant sur une session et ces participants.

5.2.3. Inconvénient du protocole RTCP

Par contre il fonctionne en stratégie bout à bout, Et il ne peut pas contrôler l'élément principal de la communication (le réseau).

5.3. Le protocole UDP (User Datagram Protocol)

5.3.1. Définition

L'UDP est un protocole sans connexion de la suite des protocoles Internet qui travaille au niveau de la couche transport, a été défini en 1980 dans la RFC (*Request for Comments)* 768. En tant qu'alternative au TCP fonctionnant de façon plus simple et quasiment sans retard, l'UDP est utilisé pour la transmission rapide de paquets de données dans des réseaux IP. Les domaines d'application typiques de l'UDP sont donc la diffusion audio et vidéo, les requêtes DNS, et les connexions VPN. [9]

5.3.2. Avantage du protocole UDP

Il a une vitesse de transfert relativement plus rapide grâce à des paquets légers avec un minimum d'en-têtes. Puisqu'il n'exige pas de réponse, il convient aux vidéoconférences, aux diffusions et aux jeux.

5.3.3. Inconvénient du protocole UDP

Comme il n'y a pas de séquencèrent et d'accusé de réception pendant le transfert, l'UDP est jugé peu fiable et peu sûr. Les paquets corrompus sont rejetés et ne sont pas redemandés pour être retransmis une fois qu'ils sont perdus.

5.4. Le protocole ICMP (Internet Control Message Protocol)

Le protocole ICMP permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des Datagrammes en erreurs. Chaque pile IP, que ce soit des routeurs ou des stations de travail, gèrent l'entête ICMP par défaut. [10]

Ce protocole est considéré comme faisant partie de l'ensemble des protocoles TCP/IP. Cependant, contrairement à TCP et UDP, il se situe en couche 3 et donc, il est encapsulé dans IP.

5.5. Le protocole H.323

5.5.1. Définition

Le standard H.323, a été développé par l'ITU en 1996, propose des bases pour le transport de la voix, la vidéo, et des données sur des réseaux IP, et répond aux problèmes liés à IP (pas de garantie de délais). H.323 fonctionne en mode non connecté et sans garantie de QoS selon une stratégie bout à bout. Il s'appuie sur des protocoles de communication (RTP, RTCP, …), mais également sur des codecs (G.7xx) et (H.26x). Et en plus il définit certains mécanismes de sécurité (authentification et chiffrement). H.323 offert:

- Le contrôle de la procédure d'appel.
- La gestion des flux multimédias.
- La gestion de la bande passante pour les conférences point-à-point et multipoints.
- Interconnexion à d'autres réseaux : RTC, RNIS.
- Les interactions avec les autres protocoles: H.323 crée une association de plusieurs protocoles différents qui peuvent être regroupés en trois catégories: la signalisation, la négociation de codec, et le transport de l'information.

5.5.2. Avantages du protocole H.323

- **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.

- **Flexibilité** Une conférence H.323 peut inclure des terminaux hétérogènes (PC, téléphone…) qui peuvent partager selon le cas(voix, vidéo, données).

5.5.3. Inconvénient du protocole H.323

- La complexité de mise en œuvre: le protocole H.323 incorpore des mécanismes superflus dans un contexte purement téléphonique. Ceci a notamment des incidences au niveau des terminaux H.323 (téléphones IP, par exemple) qui nécessitent de ce fait une capacité mémoire et de traitement sans incidence au niveau de leur coût.

- Elle comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité ou de plus petit dénominateur commun.

- Le protocole H.323 est une des normes envisageables pour la voix sur IP à cause de son développement inspiré de la téléphonie. Cependant, elle est pour l'instant employée par des programmes propriétaires (Microsoft, etc). La documentation est difficile car l'ITU (Union International Télécommunication) fait payer les droits d'accès aux derniers développements de cette technologie. Ainsi son adaptation au réseau IP est assez lourde. C'est pourquoi au fil des recherches est né le SIP.

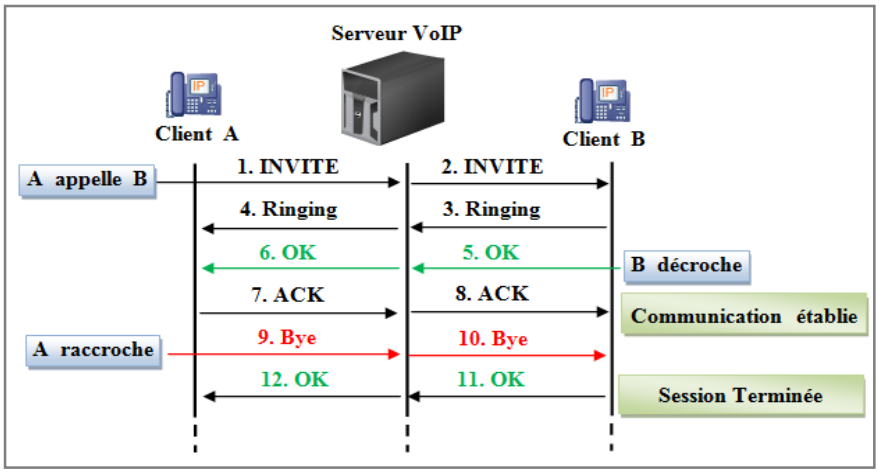
5.6. Le protocole SIP (Session Initiation Protocol)

5.6.1. Définition

SIP est un protocole de signalisation multimédia, développé par l'IETF, permet d'établir l'appel, communiquer et négocier les paramètres de session VoIP. SIP est un protocole général et non limité à la transmission de la voix, Il est également utilisé dans d'autres services (appels vidéo, les jeux collectifs en ligne, la messagerie instantanée). Il est conçu afin d'être indépendant du protocole de transport, il est considéré comme une application de gestion de sessions VoIP. SIP prend en charge la correspondance des noms et offre un service de redirection, ce qui permet la mobilité des utilisateurs. Ainsi, les utilisateurs SIP peuvent conserver un identifiant unique visible de l'extérieur quel que soit leur emplacement sur le réseau. [11]

Le rôle principal de l'utilisation du protocole SIP est d'établir une session entre les usagers. Cela nécessite la détermination de l'emplacement des terminaux, la négociation de paramètres médias, la disponibilité de terminaux engagés en cours de communication, et enfin la gestion de communication. La procédure d'établissement de session SIP se fait selon les requêtes suivantes:

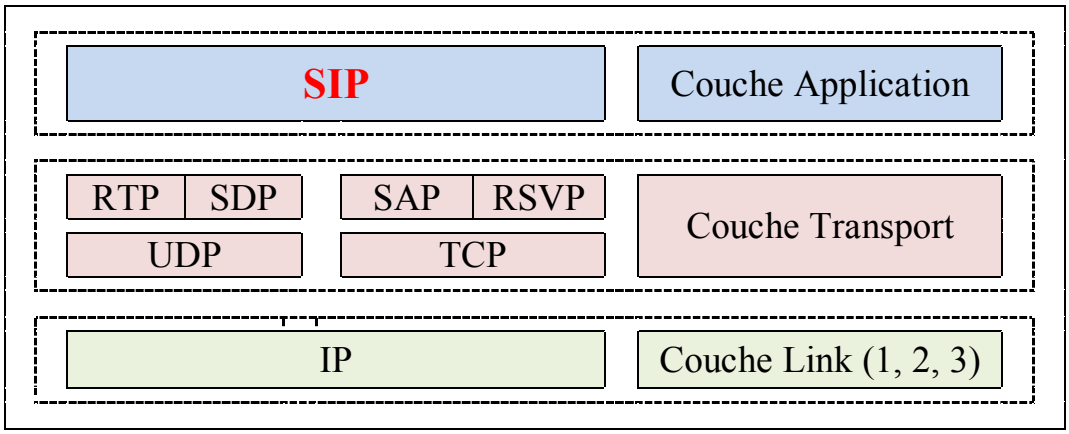
- **INVITE:** Ce message permet à un client de demander l'établissement d'une session.
- **ACK** (*acknowledgement*): confirme l'établissement d'une session **SIP**.
- **CANCEL:** Ce message annule une demande de session précédemment effectuée avec un INVITE.
- **BYE:** termine une session en cours. Contrairement au **CANCEL**, la session **SIP** doit être active pour pouvoir envoyer un message **BYE**.



Figure(20): Procédure d'établissement de session SIP [12]

L'architecture du protocole SIP dispose de toutes les composantes pour rendre la session efficace. Et utilise les protocoles: IP, UDP, TCP pour permettre une communication audio ou vidéo. D'autres protocoles peuvent collaborer tels:

- RTP permet la transmission de données en temps réel pendant une session média.
- SDP (*Session Description Protocol*) décrit les paramètres d'une session média.
- SAP *(Session Annonce Protocol)* annonce les sessions média en mode multicast.
- RSVP *(Ressource Reservation Protocol)* réserve les ressources nécessaires.



Figure(21): L'architecture du protocole SIP [13]

5.6.2. Avantages du protocole SIP

- SIP est un protocole rapide et léger. La séparation entre ses champs d'en-tête et son corps du message facilite le traitement des messages et diminue leur temps de transition dans le réseau. [8]

- **Flexible** : SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, réalité virtuelle, etc.).

5.6.3. Inconvénient du protocole SIP

- SIP est très vulnérable face à des attaques de types DoS, détournement d'appel, trafic de taxation, etc. En d'autres termes, SIP ne prend pas encore en compte de nombreux services actuellement utilisés dans les réseaux téléphoniques. [8]

6. Les codecs

6.1. Définition

Tous les types de flux média, sous forme de données, peuvent transiter par le biais du réseau IP, mais il faut auparavant convertir ces données analogiques sous forme de données digitales. C'est là le rôle des codecs. Le codec est une abréviation pour Codeur/Décodeur. Un codec est basé sur un algorithme qui permet la compression des données qu'on lui donne. Il s'agit d'un procédé permettant de compresser et de décompresser un signal, de la vidéo ou de l'audio, souvent en temps réel. Le codec permet une réduction de la taille du fichier original. Le codec compresse et numérise la voix de l'émetteur, ainsi les données numériques sont encapsulées dans des paquets IP et acheminées vers le destinataire. A la destination grâce au même codec décompresse et restitue le son. [14]

6.2. Objectifs des codecs

Quelques paramètres importants des codecs sont présentés ci-dessous :

6.2.1. Compression de silence

Pendant une conversation, nous ne parlons en général que 35 % du temps, et par conséquent il est très utile de pouvoir supprimer ces périodes de silence. Dans les conversations de point à point, cela permet d'économiser jusqu'à 50 % de la bande passante, et beaucoup plus pour des conversations multipoint. La compression de silence comprend trois composants principaux:

- La détection d'activité vocale VAD (*Voice Activity Detection*,), responsable de la discrimination des périodes d'activité vocale et de silence. Elle doit avoir un temps de réponse court (sinon le premier mot d'une période d'activité vocale risque de se perdre, et des périodes de silence inutile risquent de rester attacher à la fin des périodes actives), sans toutefois risquer d'être activée aléatoirement par du bruit de fond.

- La transmission discontinue DTX (*Discontinuous Transmission*) est la capacité d'un codec à stopper la transmission d'information quand le module VAD a détecté une période de silence.

- La génération de bruit de confort CNG (*Comfort Noise Generation*) qui vise, lorsque l'un des participants ne s'exprime pas et que la transmission est donc stoppée, à recréer une ambiance sonore au niveau de l'autre participant. [6]

6.2.2. Robustesse en présence de pertes des paquets

La perte de paquets est inévitable, à des degrés divers, sur les réseaux IP, et les délais de latence courts imposés par la voix et la vidéo interactive ne permettent pas de demander des réémissions. Puisque les paquets contiennent des trames de codecs, cela cause des pertes de trames vu du codec. Cela dit les pertes de paquets et les pertes de trames ne sont pas directement corrélées, de nombreuses techniques de redondance permettant de diminuer les pertes de trame pour une perte de paquets donnée. Ces techniques comme le FEC (*Forward Error Correction*), répliquent l'information utile sur plusieurs paquets afin que la perte d'un seul paquet ne provoque pas de perte d'information.

6.3. Codeurs audio utilisés en VoIP

6.3.1. Le codeur G.711

Approuvé en 1965, le G.711 est le grand-père des codeurs audio. Il est utilisé par le réseau d'accès RNIS et dans tous les cœurs de réseaux téléphoniques modernes. Un flux audio codé en G.711 produit un flux de données de 64 Kbps, où chaque échantillon est codé sur un octet indépendant, en conséquence la taille de trame est de seulement 125 µs. Bien sûr, toutes les applications VoIP mettent plus d'un échantillon par paquet, en général l'équivalent de 10 ms de parole (soit 80 échantillons). Le score MOS habituellement attribué à G.711 est de 4,2.

6.3.2. Le codeur G.722

G.711 restitue une bonne qualité de parole, mais la partie du spectre au-delà de 4 kHz reste coupée. G.722 fournit un codage large bande de meilleure qualité incluant le spectre jusqu'à 7 kHz. Les débits disponibles sont de 48, 56 ou 64 Kbps. Ce codeur permet de commuter à tout instant entre ces débits. G.722 est un codeur tout à fait adapté pour les applications de conférence professionnelles.

6.3.3. Le codeur G.722.1

Ce codeur plus récent, également large bande, fonctionne à 24 Kbps ou 32 Kbps. Il en existe également une version à 16 Kbps qui est supportée par Windows Messenger. Le G.722.1 génère des trames de 20 ms.

6.3.4. Le codeur G.723.1

Au début de la voix sur internet, ce codeur a été choisi par le Forum VoIP comme le codeur par défaut en communication faible débit sous H.323. G.723.1 utilise une taille de trame de 30 ms. Il fonctionne sur deux modes, l'un à 6,4 Kbps sur 24 octets, et l'autre à 5,3 Kbps sur 20 octets. G.723.1 obtient un score MOS de 3,7 en mode 5,3 Kbps, et 3,9 en mode 6,4 Kbps. Ce codeur possède une détection d'activité vocale (VAD), un mode de transmission discontinue (DTX) et une génération de bruit de confort (CNG). Le silence est codé dans des trames de seulement 4 octets, pour un débit de 1,1 Kbps. Au cas où l'information de silence n'a pas besoin d'être mise à jour, la transmission s'arrête complètement.

6.3.5. Le codeur G.729

Il est devenu, avec G.723, l'un des codeurs les plus utilisés en voix sur IP. G.729 n'est pas conçu pour la musique, et ne transmet pas les tonalités DTMF de manière fiable. G.729 code des trames de 10 ms de parole. Chaque trame compte 80 bits, le débit d'information produit est donc de 8 Kbps. G.729 obtient un score MOS de 4,0.

7. Les contraintes de la VoIP

Les réseaux IP basés principalement sur la transmission en temps réel, se démarquent progressivement des réseaux du meilleur effort en convergeant vers les réseaux avec qualité de service (QoS). Le seul souci est d'acheminer les paquets de données d'un point à un autre au travers du réseau, sans erreur et sans rien perdre. Les paquets d'une même transaction peuvent emprunter des chemins différents, ce qui peut se traduire par un déséquencement des paquets, les plus anciens arrivants après les plus récents dans les cas extrêmes [1] .Les principaux paramètres qui caractérisent la qualité de service d'un réseau de transport de données en mode paquet sont:

7.1. La gigue:

Les réseaux utilisant la commutation temporelle introduisent un délai constant dans la conversation. La situation est totalement différente dans les réseaux utilisant le multiplexage statistique: si la ligne de transmission est vide lorsque vous devez émettre les données, vous pouvez les transmettre immédiatement, par contre si elle est déjà occupée, vous devrez attendre que de la capacité soit de nouveau disponible. Ce délai variable est appelé la gigue, et doit bien sûr être compensé au niveau de récepteur. Si, au contraire, on relie les signaux de parole dès qu'on les reçoit, le flux de parole original peut devenir intelligible. Le contrôle de la gigue est important principalement pour les applications temps réel qui nécessitent l'utilisation de mémoires tampons (buffer de gigue) afin de restituer de manière régulière une information qui arrive de manière irrégulière. Plus il y a de gigue, plus ces mémoires tampons doivent être importantes, et par conséquent plus elles introduisent des délais supplémentaires dans le flux d'information de bout en bout.

7.2. Perte de paquets

Pour réaliser une transmission de la voix sur IP, le signal vocal doit être compressé à l'aide d'algorithmes spéciaux beaucoup plus élaborés qu'en téléphonie classique. Ensuite, l'information à transmettre est découpée en paquets, à raison de 20 à 30 ms de parole par paquet, avant l'envoi sur le réseau IP.

Les pertes de paquet IP se traduisent par des ruptures au niveau de la conversation avec des dégradations du signal de la parole. La perte d'un paquet se produit en effet généralement lorsqu'il y a une congestion sur un lien de transmission, qui provoque un débordement des mémoires tampons d'un routeur.

7.3. Le délai de transit

- Le délai de transit est un des paramètres critiques influençant fortement la QoS d'un service de voix sur IP. C'est le temps que va mettre en moyenne un paquet IP contenant un échantillon de voix pour traverser l'infrastructure entre deux interlocuteurs. Ce temps de transit comporte quatre composantes :

- Le délai d'échantillonnage Est la durée de numérisation de la voix à l'émission puis de conversion en signal voix à la réception. Ce temps dépend du type de codec choisi et varie de quelques millisecondes avec le codec G.711 (échantillonnage 64 kbps) à plus de 50 ms en G.723 (échantillonnage 6,3 ou 5,3 kbps). C'est une des raisons pour laquelle le choix du codec impacte le score MOS d'appréciation de la clarté de la voix, indépendamment des autres caractéristiques de l'infrastructure.

- Le délai de propagation Est la durée de transmission en ligne des données numérisées. Cette durée est normalement très faible par rapport aux autres composantes du délai de transit, de l'ordre de quelques millisecondes.

- Le délai de transport Est la durée passée à traverser les routeurs, les commutateurs et les autres composants du réseau et de l'infrastructure de téléphonie IP. L'ordre de grandeur est de plusieurs dizaines de millisecondes, voir centaines de millisecondes.

- Le délai des buffers de gigue Est le retard introduit à la réception en vue de lisser la variation de temps de transit, et donc de réduire la gigue de phase. L'ordre de grandeur est de 50 ms. Les éléments d'infrastructure, notamment les routeurs, peuvent également mettre en œuvre des buffers de gigue.

7.4. Latence

La latence est le temps écoulé entre l'envoi d'un paquet et sa réception par le destinataire. Plus la latence est importante, plus le transfert est long et sera donc décalé.

Pour garantir une communication optimale, la maîtrise du délai de transmission est un point important afin de réduire l'effet d'écho ou la sensation de voix métallique. Le temps de transmission de paquets dans un réseau de type IP dépend de nombreux éléments tels que :

- Le nombre d'équipements actifs traversés dans le réseau
- Le débit de transit disponible
- Le délai de propagation de l'information

8. Les points faibles de la VoIP

- **Fiabilité**: La VoIP dépend en grande partie de la connexion internet, ainsi la qualité de service de cette dernière sera affectée par la qualité et la fiabilité de votre service internet. Si le trafic sur le réseau est élevé, la qualité de la voix diminue. Cela se voit généralement dans les appels longue distance ou internationaux où la voix semble déformée, ce qui pose problème, principalement pour les appels professionnels pour lesquels la communication doit être rapide et des mesures doivent être prises en fonctions de la réponse.

- **Qualité de voix de VoIP**: La VoIP a un peu amélioré la qualité de la voix, mais pas dans tous les cas. La qualité de service de la VoIP dépend de plusieurs facteurs : le raccordement à bande large, le matériel utilisé, le service fourni par le fournisseur, la destination de votre appel etc. Beaucoup de gens apprécient la qualité des appels téléphoniques utilisant la VoIP, mais d'autres d'utilisateurs se plaignent toujours d'attendre beaucoup avant d'entendre une réponse.

- **Sécurité**: Les services Internet ont toujours été confrontés au problème de la sécurité. Même est le cas avec la VoIP aussi. Le piratage téléphonique a été une préoccupation majeure à cet égard. En raison du peu de temps accordé pour l'analyse des paquets de données, les performances des pare-feu peuvent être moins que satisfaisantes. La VOIP est également affectée par les vers et les virus. Tous ces éléments constituent une menace pour la sécurité. [8]

Conclusion

L'entreprise a toutes les chances de se retrouver avec un réseau de VoIP qui fonctionne correctement, mais est ouvert à tous et à tout les risques, cette solution, qui est totalement basée sur la technologie 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. Certaines attaques sur les réseaux VoIP, comme les attaques de déni de service, et les vols d'identité, peuvent causer des pertes catastrophiques et énormes pour les entreprises. Pour cela la sécurité du réseau VoIP est une obligation, avec laquelle on peut minimiser le risque d'attaques sur les réseaux VoIP. **Et ça sera notre sujet dans la partie suivante.**

Partie II: La sécurité de la VoIP

Introduction

L'opportunité de migrer de la téléphonie classique vers la téléphonie IP, a offert plusieurs avantages pour les entreprises, et les a permirent de bénéficier de nouveaux services tel que la vidéoconférence et la transmission des données. L'intégration de ces services dans une seule plateforme nécessite plus de sécurité. Dans cette partie, nous dériverons des attaques qui menacent la VoIP, et nous détaillerons quelques uns. Nous finirons par une description des bonnes pratiques pour sécuriser les communications de type voix sur IP.

Le système VoIP utilise l'Internet, et particulièrement le protocole IP. De ce fait les vulnérabilités de celui-ci. Les attaques sur les réseaux VoIP peuvent être classées en deux types : les attaques internes et les attaques externes. Les attaques externes sont lancées par des personnes autres que celle qui participe à l'appel, et ils se produisent généralement quand les paquets VoIP traversent un réseau peu fiable et/ou l'appel passe par un réseau tiers durant le transfert des paquets. Les attaques internes s'effectuent directement du réseau local dans lequel se trouve l'attaquant. Il existe deux principales classes de vulnérabilités sur un environnement VoIP. La première dépend des protocoles utilisés (SIP, H.323…) et la deuxième est reliée aux systèmes sur lesquels les éléments VoIP sont implémentés. Chaque protocole ou service a ses propres vulnérabilités.

1. Propriétés de sécurité

Avant de présenter les Principaux risques de sécurité associer à la VoIP, il convient de rappeler les définitions des propriétés de sécurité :

- **L'authentification:** garantir l'identité de l'usager qui envoie le message, dans le cadre de la VoIP, cette propriété permet par exemple à un serveur de vérifier qu'il fournit le service à l'usager légitime**.**
- **La confidentialité:** rendre la conversation compréhensible aux personnes concernées uniquement, cette propriété nécessite de chiffrer le flux audio.
- **L'intégrité:** s'assurer que les données n'ont pas été modifiées entre l'envoi d'un message et sa réception, et de s'assurer que les paramètres d'un appel n'ont pas été modifiés par une tierce partie.
- **La non répudiation de l'appel:** la non répudiation des données nécessite l'archivage des données échangées, et permet d'associer une communication à une personne de manière certaine.
- **Le non rejeu:** permet de ne pas pouvoir rejouer des échanges protocolaires par une personne tierce souhaitant accéder au service.
- **L'anonymat:** capacité du système à masquer l'identité de l'usager, cette propriété peut se traduire par le masquage de l'identité de l'appelant. [15]

2. Politique de sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système, en mettant en place des mécanismes d'authentification et de contrôle, permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés. Et pour définir une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
- Élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés.
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

3. Principaux risques

L'arrivée de la VoIP constitue de nouvelles opportunités d'attaques dans le monde des systèmes d'informations. La signalisation et la voix partageant le même réseau ou au moins les mêmes technologies que les réseaux de données IP, la VoIP partage les mêmes vulnérabilités que les réseaux de données. A cela il faut rajouter les risques propres à la signalisation et au transport de la VoIP. [15]

3.1. Attaques sur les protocoles

Un appel téléphonique VoIP est constitué de deux parties : la signalisation qui instaure l'appel, et les flux de media qui transporte la voix. Les types d'attaques les plus fréquentes contre un système VoIP sont:

3.1.1. Sniffing

Un reniflage (*Sniffing*) peut résulter un vol d'identité et la récupération des informations confidentielles, aussi bien des informations sur les systèmes VoIP. Ces informations peuvent être employées pour mettre en place une attaque contre d'autres systèmes ou données. L'IP *sniffing* est une attaque passive, il est décrit comme le suivant:

- L'intrus est placé sur un réseau.
- L'intrus met sa station en mode écoute.
- La station récupère l'ensemble du trafic échangé sur le réseau.
- L'intrus utilise un analyseur de protocoles réseau à l'insu des administrateurs du réseau. [14]

3.1.2. L'attaque par suivie des appels (*Call tracking*)

Cette attaque 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. [14]

3.1.3. Injection de paquet RTP

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

3.1.4. Le déni de service (DoS : *Denial of service*)

C'est, d'une manière générale, l'attaque qui vise à rendre une application informatique ou un équipement informatique incapable de répondre aux requêtes de ses utilisateurs et donc hors d'usage. Une machine serveur offrant des services à ses clients (par exemple : un serveur web) doit traiter des requêtes provenant de plusieurs clients. Lorsque ces derniers ne peuvent en bénéficier, pour des raisons délibérément provoquées par un tiers, il y a déni de service.

Nous allons montrer un exemple de l'attaque déni de service où l'attaquant utilise la requête CANCEL .C'est un type de déni de service lancé contre l'utilisateur. L'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique. Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant envoie immédiatement une requête CANCEL. Cette requête produit une erreur sur le dispositif de l'appelé et termine l'appel. Ce type d'attaque est employé pour interrompre la communication. [14]

3.1.5. Détournement d'appel (*Call Hijacking*)

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

Exemple: quand un agent **SIP** envoie un message **INVITE** pour initier un appel, l'attaquant envoie un message de redirection indiquant que l'appelé s'est déplacé et par la même occasion donne sa propre adresse comme adresse de renvoi. A partir de ce moment, tous les appels destinés à l'utilisateur sont transférés et c'est l'attaquant qui les reçoit. Un appel détourné en lui-même est un problème, mais c'est encore plus grave quand il est porteur d'informations sensibles et confidentielles.

3.1.6. L'écoute clandestine (*Eavesdropping*)

C'est l'écoute clandestine d'une conversation téléphonique. Un attaquant avec un accès au réseau VoIP peut sniffer le trafic et décoder la conversation vocale. Le principe de l'écoute clandestine est montré comme suit :

- Déterminer les adresses MAC des victimes (client-serveur) par l'attaquant.
- Envoi d'une requête ARP (*Address Resolution Protocol*) non sollicités au client, pour l'informer du changement de l'adresse MAC du serveur VoIP.
- Envoi d'une requête ARP non sollicités au serveur, pour l'informer du changement de l'adresse MAC du client.
- Désactiver la vérification des adresses MAC sur la machine d'attaque afin que le trafic puisse circuler entre les 2 victimes.

3.2. Les vulnérabilités de l'infrastructure

Une infrastructure VoIP est composée de téléphones IP, Gateway, serveurs. Ces derniers tournant sur un système d'exploitation, est accessible via le réseau comme n'importe quel ordinateur et comportent un processeur qui exécute des logiciels qui peuvent être attaqués ou employés en tant que points de lancement d'une attaque plus profonde. [16]

3.2.1. Faiblesses de configuration des dispositifs VoIP

Plusieurs dispositifs de la VoIP, dans leur configuration par défaut, peuvent avoir une variété de ports TCP et UDP ouverts. Les services fonctionnant sur ces ports peuvent être vulnérables aux attaques DoS ou buffer *overflow*. Plusieurs dispositifs de la VoIP exécutent également un serveur WEB pour la gestion à distance qui peut être vulnérable aux attaques buffer *overflow* et à la divulgation d'informations. Si les services accessibles ne sont pas configurés avec un mot de passe, un attaquant peut acquérir un accès non autorisé à ce dispositif. Les services SNMP (*Simple Network Management Protocol*) offerts par ces dispositifs peuvent être vulnérables aux attaques de reconnaissance ou attaques d'*overflow*. Plusieurs dispositifs de la VoIP sont configurés pour télécharger périodiquement un fichier de configuration depuis un serveur par TFTP ou d'autres mécanismes. Un attaquant peut potentiellement détourner ou mystifier cette connexion et tromper le dispositif qui va télécharger un fichier de configuration malveillant à la place du véritable fichier.

3.2.2. Les téléphones IP

Généralement un attaquant obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif, soit un téléphone IP, un Soft-phone, ou d'autres programmes ou matériels client. Le pirate pourrait modifier les aspects opérationnels d'un tel dispositif: il peut changer la pile du système d'exploitation pour masquer la présence de l'attaquant. Il peut modifier et configurer d'une manière malveillante des logiciels de téléphonie IP qui peuvent permettre :

- Aux appels entrants d'être réorientés vers un autre point final sans que l'utilisateur soit au courant ou aux appels d'être surveillés.
- A l'information de la signalisation et/ou les paquets contenant de la voix d'être routés vers un autre dispositif et également d'être enregistrés et/ou modifiés.
- Les soft-phones sont plus susceptibles aux attaques, ils sont plus susceptibles à la vulnérabilité: du system d'exploitation, de l'application, des services, des virus.etc

3.2.3. Les serveurs 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.

3.2.4. Vulnérabilités du système d'exploitation

La plupart de ces vulnérabilités sont relatives au manque de sécurité lors de la phase initiale de développement du système d'exploitation et ne sont découvertes qu'après le lancement du produit. Une des principales vulnérabilités des systèmes d'exploitation est le buffer *overflow*. Il permet à un attaquant de prendre le contrôle partiel ou complet de la machine.

Les dispositifs de la VoIP tels que les téléphones IP, Call Managers, Gateway et les serveurs proxy, héritent les mêmes vulnérabilités du système d'exploitation ou du *firmware* sur lequel ils tournent. Il existe une centaine de vulnérabilités exploitables à distance sur Windows et même sur Linux. Un grand nombre de ces exploits sont disponibles librement et prêts à être téléchargés sur l'Internet. Peu importe comment, une application de la VoIP s'avère être sûre, celle-ci devient menacé si le système d'exploitation sur lequel elle tourne est compromis.

4. Les mesures de sécurités

On a déjà vu que les vulnérabilités existent au niveau protocolaire et infrastructure. Pour cela, on a découpé la sécurisation aussi en deux niveaux: Sécurisation protocolaire, sécurisation de l'infrastructure.

4.1. Sécurisation protocolaire

La prévalence et la facilité de sniffer des paquets et d'autres techniques pour la capture des paquets IP sur un réseau pour la voix sur IP fait que le cryptage soit une nécessité. La sécurisation de la VoIP est à la protection des personnes qui sont interconnecté. Compte tenu du périmètre de l'analyse, plusieurs mécanismes peuvent être envisagés, que ce soit au niveau réseau ou au niveau applicatif et donc dans les protocoles de VoIP. Nous citerons quelques uns ci-dessous:

4.1.1. IPsec (IP Security)

IPSec est un ensemble de protocoles conçu par l'IETF afin de sécuriser le trafic IP. Initialement conçu dans la philosophie d'IPv6, IPSec est un système d'encapsulation offrant les services de sécurité requis au niveau IP. Néanmoins, étant donné que les besoins en matière de sécurité sur Internet et sur les Intranets ne peuvent attendre que la totalité (ou d'au moins une grande majorité) du parc informatique mondial ait migré vers IPv6, il est nécessaire que IPSec soit également utilisable avec IPv4. Une manière commode de procéder, qui a l'avantage de garantir la compatibilité avec toutes les implémentations existantes du protocole IP sans avoir à les modifier, est de considérer le protocole IPSec comme un protocole indépendant, implémentable comme un module additionnel sous forme d'un logiciel ou d'un équipement électronique dédié. [17]

IPsec peut être utilisé pour réaliser deux objectifs: Garantir l'identité des deux points terminaux et protéger la voix. VOIPsec (VoIP utilisant IPsec) contribue à réduire les menaces, les sniffeurs de paquets, et de nombreux types de trafic « vocal analyze ». Combiné avec un pare-feu, IPsec fait que la VOIP soit plus sûr qu'une ligne téléphonique classique. Il est important de noter, toutefois, que certains protocoles doivent continuer à compter sur leurs propres dispositifs de sécurité. [17]

IKE (Internet Key Exchange)

L'IKE est un protocole en deux phases, utilisé pour sécuriser les informations partagées dans IPsec. Le protocole IKE a pour mission de sécuriser une connexion. Avant qu'une transmission IPsec soit réalisable, IKE se charge d'authentifier les deux parties tentant de se connecter au réseau informatique sécurisé, en échangeant des clés partagées. Cette méthode admet deux types d'identification : par Pre-Shared Key (PSK ou secret partagé) ou par la contribution de certificat. Utilisant alors la méthode du chiffrement symétrique, des clés de session sont engendrées. Ces deux protocoles d'identification se différencient pourtant. [18]

4.1.2. Mise en place d'un VPN (*Virtual Private Network*)

Un réseau privé virtuel (VPN) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de tunnel. Le VPN permet de véhiculer du trafic crypté grâce à des clés de cryptage, ce qui rend leur déchiffrage presque impossible. Le VPN permettra donc de contourner les attaques d'écoute clandestine. Il 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 semble celle la plus approprié vu qu'elle offre le cryptage des données grâces a des mécanismes de cryptages, puisqu'elle permet d'offrir l'intégrité des paquets VoIP. Alors le mode tunnel assure la confidentialité et l'intégrité des clients, Puisqu'il sécurise le paquet comme un tout. 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 routeur-au-routeur.

Parmi les outils de la mise en place d'un VPN est **VPN IPSec** site à site avec l'IOS Cisco. C'est une stratégie permettant de créer un réseau virtuel basé sur IPSec et IKE. Il peut être utilisé afin de relier deux réseaux ou plus, via un tunnel chiffré à travers Internet. [17]

4.1.3. Secure RTP ou SRTP (Security Real Time Protocol)

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 dont le mécanisme d'échanges de clés est trop lourd. Il aussi est bâti sur le protocole RTP. Il associe aussi une demi-douzaine de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles d'initiation de session de voix sur IP tel que SIP, ainsi que le protocole de diffusion de contenu multimédia en temps réel RTSP (*Real Time Streaming Protocol*). Mais, surtout, il s'adjoint les services du protocole de gestion de clé MIKEY (*Multimedia Internet KEYing*).

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 rejeu des paquets. Chaque récepteur tient à jour une liste de tous les indices des paquets reçus et bien authentifiés.

4.1.4. Protocole SSL ou TLS

C'est un protocole de sécurisation des échanges au niveau de la couche transport (**TLS: *Transport Layer Security***). TLS, c'est la version développée de **SSL** (***Secure Sockets Layer*),** est un protocole de sécurisation des échanges sur Internet. C'est un protocole modulaire dont le but est de sécuriser les échanges des données entre le client et le serveur indépendamment de tout type d'application. TLS agit comme une couche supplémentaire au-dessus de TCP. Le protocole SSL et TLS est subdivisé en quatre sous protocoles :

- **Le protocole Hanshake:** C'est un protocole qui permet au client et au serveur de s'authentifier mutuellement, de négocier les algorithmes de chiffrement, de négocier les algorithmes de MAC (Message Authentification Code) et enfin de négocier les clés symétriques qui vont servir au chiffrement.

- **Le protocole Change Cipher Spec:** Ce protocole contient un seul message: change_cipher_spec. Il est envoyé par les deux parties au protocole de négociation. Ce message transite chiffré par l'algorithme symétrique précédemment négocié.

- **Le protocole Alert:** Ce protocole spécifie les messages d'erreur que peuvent s'envoyer clients et serveurs. Les messages sont composés de deux octets. Le premier est soit warning soit fatal. Si le niveau est fatal, la connexion est abandonnée. Les autres connexions sur la même session ne sont pas coupées mais on ne peut pas en établir de nouvelles. Le deuxième octet donne le code d'erreur.

- **Le protocole Record :** Ce protocole chapeaute les autres protocoles de **SSL** et **TLS**, en fournissant une interface unifiée pour la transmission des données.

4.2. Sécurisation de l'infrastructure

Tout système informatique étant susceptible de contenir des failles. Ici, il faut avoir une politique de sécurité globale pour sécuriser l'infrastructure (hard/soft) de notre systèmes (voix et données). La mise en œuvre de cette sécurité se fait selon les mécanismes suivants :

4.2.1. La séparation des équipements données et voix

Un des principes les plus recommandés pour protéger la VoIP est de séparer les équipements du réseau Data des équipements de l'infrastructure Voix. Cette séparation peut se faire de manière physique ou de manière logique. La séparation physique se traduit par deux réseaux différents avec des Switchs distincts. A ce choix relativement coûteux, il est préféré la séparation logique qui se décline de plusieurs manières :

- **Séparation des plages d'adresses IP:** ce choix consiste à attribuer une plage d'adresses par réseau, c'est-à-dire une plage pour le réseau données et une plage pour le réseau voix. Cette option nécessite que chaque réseau possède ses serveurs DHCP ou DNS.

- **Séparation par VLAN**: cette fois, la séparation des équipements données et voix est obtenue par l'utilisation des VLAN. Il est même envisageable d'avoir des VLAN voix pour chaque catégorie d'équipements (hardphone, softphone, serveurs). Les échanges entre les VLAN doivent être strictement contrôlés. Les équipements comme les Switchs ou les firewalls doivent permettre de filtrer les flux inter-VLAN.

4.2.2. Limitation du nombre d'adresses MAC *(Media Access Control)*:

Il est possible de définir, au niveau des ports de commutateurs de desserte, le nombre d'adresses MAC autorisées à accéder au réseau. Cependant il n'est pas recommandé de définir explicitement sur chaque port de commutateur l'adresse MAC du téléphone normalement connecté à ce port, cela n'apporte pas de réelle sécurité supplémentaire et induit des coûts d'exploitation importants (maintien à jour des adresses MAC dans la configuration des commutateurs). Le renforcement du niveau de sécurité des ports de commutateurs implique la mise en œuvre des procédures suivantes:

- Désactiver les ports non-utilisés.
- Placer les ports inutilisés sur un VLAN inutilisé.
- N'autoriser que les adresses MAC connues.

L'objectif principal est bien une réduction du déni de service. D'autres dispositions sont également possibles pour renforcer la sécurité, en particulier pour limiter la possibilité de se connecter avec n'importe quelle machine sur le réseau. Les recommandations précédentes peuvent donc être complétées par la mise en place de mécanismes d'authentification.

4.2.3. L'authentification

L'authentification est la fonction de sécurité qui consiste à apporter et à contrôler la preuve de l'identité d'une entité (personne, message, logiciel,…). Généralement l'authentification est à sens unique, seul le terminal est authentifié. Ce constat est issu de modèle client/serveur dans lequel un client demande un accès à des services fournis par le serveur. Les protocoles de sécurité utilisés dans ces réseaux sont basés sur un processus type défi/réponse. Le serveur envoie un défi au client et ce dernier applique une fonction cryptographique sur le défi en utilisant un secret partagé (comme un mot de passe). Ainsi seul le client est authentifié. Cette approche ne suffit pas en VoIP. Dans la mesure où la signalisation porte des informations personnelles comme les destinataires des appels, il est plus qu'important que le client soit certain qu'il dialogue avec le serveur légitime. Cet objectif nécessite donc la mise en place d'une authentification dite «mutuelle».

L'une de méthode les plus importantes pour anticiper une attaque sur un système de téléphonie est de déterminer clairement l'identité des périphériques ou des personnes participant à la conversation. Plusieurs solutions simples sont mises en œuvre pour cela, il est recommandé d'utiliser des mots de passe complexes lors de la configuration des clients SIP.

En effet, il faut savoir que certains *hackers* développent des robots en charge de sonder les réseaux informatiques et dés que l'un d'entre eux réponds au protocole SIP, un algorithme sophistiqué est engagé et teste toutes les combinaisons possibles de mots de passe. Alors, **il faut éviter**:

- Les mots de passes trop courts pour une durée longue.
- Les suites numériques (123456) ou alphabétiques (abcd).
- Les suites logiques tels prénoms ou dates.
- Un mot de passe unique pour toutes les extensions SIP.
- Un mot de passe similaire pour toute les machines incluent dans le réseau (serveur VoIP, Serveur DATA, Routeurs, Switchs, PC,..etc).

On ne saurait trop recommander un mot de passe complètement aléatoire de 8 caractères au minimum, faisant intervenir une combinaison de caractères spéciaux, lettres majuscules, lettres minuscules, chiffres non suivis..etc. La confidentialité des mots de passes est primordiale : lors de la configuration des équipements (serveur VoIP/Data, Routeurs, Switchs, PC, hard-phones, soft-phones..) sur site, il est impératif d'être discret au moment de la saisie des mots de passe, et bien entendu de ne pas les communiquer aux utilisateurs.

4.2.4. Utilisation des pare-feux:

Un pare-feu (*Firewall*) est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de contrôle d'accès. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une machine sans autorisation d'accéder à ce réseau.

Le firewall est un système permettant de protéger un système ou un réseau d'information (voix, données) des intrusions. Il filtre les paquets de données échangés en analysant les entêtes. Les champs traités à minima sont les adresses IP de l'émetteur et du destinataire, les types de paquet transporté (UDP, TCP) et le numéro de port associé.

4.2.5. Sécurisation de l'application

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

- Il est essentiel de maintenir à jour la version des logiciels grâce à un processus de management des mises à jour. Des mesures organisationnelles doivent être mises en place pour avoir des informations sur les équipements et les logiciels. Il faut pouvoir être certain d'être averti de la parution des versions et correctifs disponibles. Les évolutions doivent être testées avant d'être déployées.

- Eliminer la configuration par défaut qui sert juste à établir des appels. Elle ne contient aucune protection contre les attaques.

- Certains paramètres doivent être appliqués de manière sélective. Ces paramètres renforcent la sécurité de l'application, on peut les activer ou les interdire sur la configuration générale de l'application, comme on peut juste utiliser les paramètres nécessaires pour des clients bien déterminé et selon le besoin bien sûr. Ces paramètres protègent généralement contre le déni de service et ces différentes variantes. Il est conseiller d'utiliser les paramètres qui utilise le hachage des mots de passe, et cela assure la confidentialité.

Conclusion

La sécurité de VoIP doit pouvoir répondre à trois grandes exigences : la disponibilité, l'intégrité et la confidentialité. D'autres propriétés comme l'authentification, le non-rejeu et la non-répudiation peuvent être également nécessaires. Chacune de ces exigences demande des mécanismes protocolaires ou des choix d'architecture bien particuliers. Les solutions de sécurité envisagées actuellement répondent à ces attentes mais ne tiennent cependant pas compte de la diversité des environnements de la VoIP. Le contexte d'emploi des mécanismes de sécurité est souvent très restreint. Mais en suivant certaines bonnes pratiques parmi les cités, on peut créer un réseau bien sécurisé.

Chapitre 3:

Simulation d'un réseau VoIP

Chapitre III: Simulation d'un Réseau VoIP

Introduction

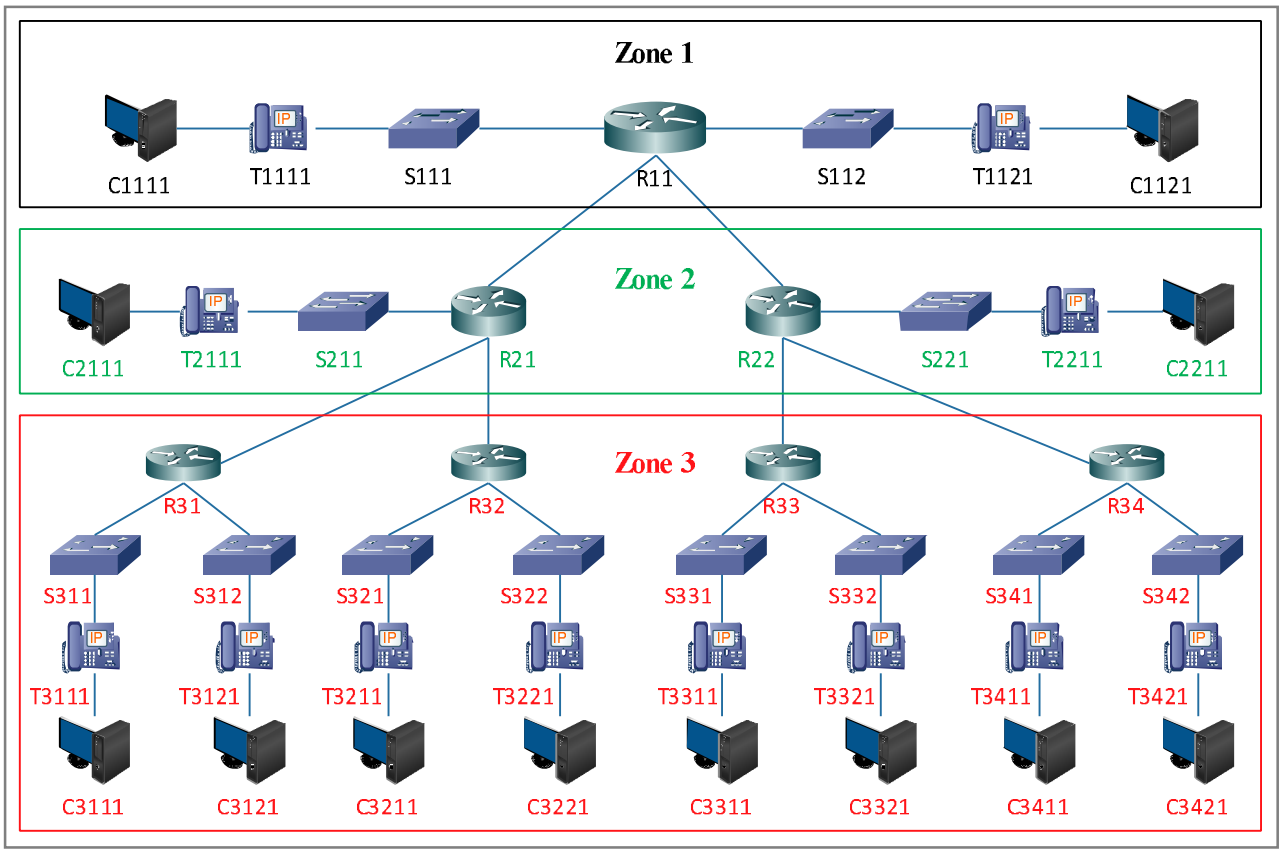
Dans ce chapitre nous présenteront la topologie de notre réseau, qui combine la technologie VoIP et données, dans une architecture hiérarchique. Nous exposeront les différentes configurations nécessaires implémentées, en se basant sur le simulateur ***Cisco Packet Tracer***. Et on appliquera certaines solutions pour sécuriser notre réseau.

1. Choix technique:

1.1. L'architecture de la topologie

Afin de maitriser la supervision de notre réseau et d'assurer un bon routage de trafic entre les différents réseaux élémentaires, nous avons implémenté une politique de planification d'une façon dont l'architecture de notre topologie est divisée en trois zones hiérarchiques:

- **La zone 1**: c'est la zone située en haut niveau hiérarchique du réseau, c'est une zone de supervision centrale avec une capacité de surveiller l'ensemble du réseau.
- **La zone 2**: située au-dessous de la zone 1, c'est une zone intermédiaire qui fait la surveillance et l'interconnexion entre les réseaux au niveau inférieur (zone 3), et permet également d'assurer la communication avec le niveau central.
- **La zone 3**: c'est une zone basale qui se trouve dans le dernier niveau hiérarchique.



Figure(22): Schéma descriptif des zones hiérarchiques dans un réseau (VoIP/données)

1.2. Plan de Dénomination, numérotation et d'adressage

La conception d'un bon réseau informatique nécessite une planification préalable sur la façon de distribution des adresses IP et dénomination des équipements connectés, afin d'éviter tout conflit au réseau dû par la duplication des noms ou des adresses IP. Et aussi un plan de numérotation téléphonique bien choisi, réservé aux abonnés selon le besoin, pour éviter tout type de saturation et de renumérotation en cas de créer une extension au ce réseau. Nous avons adopté ici la règle de l'architecture hiérarchique expliqué précédemment **pour**:

1.2.1. Dénomination des équipements

Le nom d'un équipement installé dans cette topologie, se compose de regroupement de la suite suivante:

- **Une lettre**: signifier le type d'équipement.
- **Numéro de zone**: dans laquelle cet équipement est installé.
- **Numéro séquentiel**: est incrémenté selon le nombre total des équipements de même type installés dans une zone.

Exemple: les noms des routeurs de la zone 1 seront: R11, R12, R13,...

1.2.2. Numérotation des IP-Phones

Les numéros des répertoires (DN) attribués aux IP-Phones se composent de:

- **Numéro de routeur**: est attribué selon la règle de dénomination précédente.
- **Numéro donné**: c'est un numéro contient 03 ou 04 chiffres qu'identifier l'abonné.

Alors: dans la **zone 3**, avec le **routeur N° 1**, le DN d'un IP-Phone sera: **31200**.

1.2.3. Plan d'adressage IP

Pour simplifier l'affectation des adresses IP aux différents équipements installés dans notre topologie, nous avons introduit le numéro de routeur dans la constitution des adresses IP affectés à ce réseau, dans le but de distinguer chaque réseau et ces équipements.

Exemples: L'adresse IP de l'interface du réseau interne du routeur R31 est: 192.168.31.0

- L'adresse IP de l'interface qui relie les deux routeurs R21et R31 est: 10.21.31.0

1.3. Choix de simulateur

Il existe plusieurs programmes de simulation sur Internet qui nous aident à mettre en œuvre l'application et simuler notre réseau, sans avoir besoin d'acheter tout l'équipement que nous utiliserons. Ces applications sont appelées simulateurs. Parmi eux on trouve: ***Cisco Packet Tracer***, ***GNS3, EVE-NG, CERTA, Sopireminfo, NetSim***,...Nous avons choisi le ***Cisco Packet Tracer*** pour simuler notre topologie. Le choix des équipements du réseau (routeur, switch, IP-Phone,..) est basé sur les types fourni par ce simulateur.

Cisco Packet Tracer (version 7.3.0)

Packet Tracer est un simulateur de matériel réseau Cisco. Cet outil est développé par **Cisco Systems** qui le fournit gratuitement aux centres de formation, étudiants et diplômés participant, ou ayant participé, aux programmes de formation Cisco (*Cisco Networking Academy*). Le but de Packet Tracer est d'offrir aux élèves et aux professeurs un outil permettant d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco. Il peut être utilisé pour s'entraîner, se former, préparer les examens de certification Cisco, mais également pour de la simulation réseau. [19]

1.4. Choix d'équipements

Cisco a équipé ses routeurs pour qu'il puisse transporter la voix et l'image d'un endroit à un autre. Et cela par la mise à jour de l'***IOS*** (*Internetwork Operating System*) à l'intérieur du routeur et est devenu appelé CME (*Call Manager Express*). Chaque type de routeur a sa capacité d'accueillir un certain nombre d'utilisateurs et d'abonnés (DN), selon les caractéristiques techniques de chaque type (*CPU, RAM, Flash Memory*..). En générale, ils ne supportent pas un grand nombre d'abonnés (environ de 48 IP-Phone et 192 DN virtuels dans la plateforme 72xx). Pour cette raison, Cisco a créé des **serveurs** dédies à la VoIP, il accueille environ de 5000 abonnés, et s'appelle ***CUCM*** (*Cisco Unified Communications Manager*).

Pour réaliser notre topologie nous avons choisi les équipements suivants:

- Le routeur choisi est **Cisco-2811**, c'est le seul routeur (CME) doté par l'option ***Telephony service*** (VoIP), lequel on trouve sur Cisco Packet Tracer même dans sa dernière version (7.3.0).
- Les commutateurs de type **Cisco-2960**.
- IP-Phones type **7960**.
- Les stations de travail (PC) sont dotés de plusieurs utilitaires installés comme: ***Invite de commande, hyper terminal, Cisco IP Communicator,..*** ce dernier s'utilisera pour faire des communications à partir des PCs ***(Soft-Phone)***.

2. Description des commandes de configuration Cisco

Avant de présenter les scriptes de configuration des équipements, nous expliquerons les commandes de configuration Cisco les plus importantes, que nous verrons au cours des différentes étapes de simulation du notre réseau VoIP.

2.1. Au niveau du switch

2.1.1. Gestion d'alimentation au niveau des ports du switch

Il existe trois façons d'alimenter les téléphones Cisco, en utilisant soit:

1. Un Switch PoE (*Power over Ethernet*).
2. Un panneau de brassage (*power patch panel*).
3. Le transformateur (adaptateur) fourni par le constructeur de l'IP-Phone.

Dans le cas d'un switch Cisco PoE, ce dernier détecte automatiquement quelle port est connecté à un téléphone Cisco et lequel a besoin d'alimentation, grâce au protocole CDP (*Cisco discovery protocol*).

Les commandes suivantes montrent quelques options de gestion d'alimentation:

- Afficher l'état des ports d'un switch PoE:

```
Switch# show power inline
```

- Configurer un port pour fournit l'alimentation automatiquement:

```
Switch(config)# interface fa 0/1
Switch(config-if)# power inline auto
```

- Coupez complètement l'alimentation de ce port:

```
Switch(config-if)# power inline never
```

- Dans certains cas, le redémarrage du téléphone prend un longtemps, de sorte que le switch s'assurera que ce port n'est plus utilisé. Il coupe l'alimentation sur lui. Certains pensent que le téléphone est en panne, mais il ne faut que plus de temps pour terminer la phase de téléchargement. La commande suivante empêche la coupure de l'alimentation du port pendant 20 secondes:

```
Switch(config-if)# power inline delay shutdown 20
```

2.1.2. Les VLANs

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants : Amélioration de la gestion du réseau. Optimisation de la bande passante. Séparation des flux. Réduire la taille d'un domaine de *broadcast* (Segmentation). Permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen pour communiquer entre des machines appartenant à des VLAN différents est alors de passer par un routeur.

- Pour créer un VLAN il suffirait de préciser-le par un numéro et un nom:

```
switch(config-if)# VLAN 20
switch(config-vlan)# name voice
```

→ Sur un commutateur Cisco, on trouve les ports dits (*access)* et des ports dits (*trunk*):

✓ Un port (***access)*** est utilisé pour connecter un hôte terminal (PC, IP-Phone,..) ou un serveur. Après avoir défini le mode du port, nous désignons les VLANs accessibles à partir de ce port:

```
switch(config-if)# int fa 0/10
switch(config-if)# switchport mode access
switch(config-if)# switchport access VLAN 10
switch(config-if)# switchport voice VLAN 20
```

- On peut utiliser la commande suivante pour effectuer la même configuration aux plusieurs ports, les ports de 1 à 10 seront identiques:

```
switch(config-if)# int range fa 0/1-10
switch(config-if)# switchport mode access
switch(config-if)# switchport access VLAN 10
switch(config-if)# switchport voice VLAN 20
```

✓ Un port (***trunk)*** est un port qui transportera des informations de plusieurs VLANs. On y connectera un autre commutateur ou un routeur:

```
switch(config)# int fa 0/20
switch(config-if)# switchport mode trunk
```

→ Dans sa documentation, Cisco Systems distinguent plusieurs types de VLANs:

✓ **VLAN Par défaut**: le VLAN 1 est celui qui assigné à tous les ports d'un commutateur tant qu'ils n'ont pas été configurés autrement. Le VLAN 1 ne peut jamais être supprimé, il existe d'office. Pour ces raisons, il recommandé d'éviter l'utilisation de VLAN 1dans tous les cas.

✓ **Le VLAN de gestion**: est un VLAN spécifique attribué aux commutateurs avec une adresse IP privée, pour qu'ils soient accessibles via cette adresse:

```
switch(config)# int VLAN 100
switch(config-if)# ip add 192.168.1.100 255.255.255.0
```

✓ **Native VLAN**: La notion de VLAN natif n'intervient que lorsque l'on configure un port (*Trunk*). Quand un port est configuré en tant que tel, le commutateur insère une étiquette dans l'en-tête de la trame avec le numéro de VLAN approprié (taguez-le et laissez passer):

```
switch(config)# int fa 0/10
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native VLAN 100
```

- Pour afficher les équipements Cisco connectés à ce switch, exécuter la commande:

```
switch# show cdp neighbors
```

- Pour voir l'état des ports du switch et les VLANs affecté à ces ports. Taper:

```
switch# show VLAN brief
```

2.2. Au niveau du Routeur (CME)

2.2.1. L'encapsulation dot1Q

Lorsque nous parlons du mode *Trunk* dans le switch, il est nécessaire de parler d'encapsulation au niveau du routeur, et donc on doit forcément faire appel à un protocole. Du côté de Cisco, deux protocoles existent pour l'encapsulation des données sur un *trunk*:

1. **ISL** (Inter Switch Link) qui est un protocole propriétaire Cisco qui tend à disparaître.
2. **dot1Q** (IEEE 802.1Q) le protocole standard défini par l'IEEE.

Nous nous contenterons de voir **dot1q** dans le cas présent. Toutefois il est bon de savoir que chacun a son propre fonctionnement. **ISL** pour sa part encapsule toute les trames, quelque soit le VLAN. **dot1Q**, lui ne fait qu'insérer un ***tag*** (un marqueur) dans l'entête de la trame Ethernet. L'encapsulation des trames se fait pour permettre aux trames de différents VLANs faire circuler sur la même interface, après avoir créé des sous interface a l'intérieure de l'interface physique du routeur.

- Le scripte suivant illustre comment créer dans l'interface *fast-Ethernet* 0/0 une sous-interface 0/0.50 pour le VLAN 50, avec l'affectation d'adresse IP:

```
Router(config)# int fa 0/0.50
Router(config-subif)# encapsulation dot1Q 50
Router(config-subif)# ip add 192.168.50.1 255.255.255.0
Router(config-subif)# no sh
Router(config-subif)# ex
```

2.2.2. DHCP et l'option 150

- Le protocole DHCP (*Dynamic Host Configuration Protocol*) a pour fonctionnalité de fournir aux machines qui le demandent une configuration IP complète (adresse IP, masque de sous-réseau, passerelle par défaut, serveur dns..).

- Une fois le pool DHCP configuré, le routeur va commencer à attribuer des adresses. Il est donc conseillé de configurer en premiers les adresses à exclure:

```
Router(config)# ip dhcp excluded-address 192.168.1.0
```

- **L'option 150**: cette commande dirige les IP-Phones vers l'adresse IP du serveur TFTP à partir de lequel ils pourront télécharger leur (**firmware**). Le DHCP et l'option 150 sont configurés comme suit:

```
Router(config)# ip dhcp pool voice
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# option 150 ip 192.168.1.1
```

2.2.3. Telephony service

Le service Cisco ITS (IOS *Telephony Service*), est une solution de traitement des appels de téléphonie IP intégrée au logiciel Cisco IOS, et qui s'adapte à l'architecture Cisco pour la voix, la vidéo et les données. Sans **`Telephony Service`**, le routeur ne peut pas être un CME. Pour activer ce service, taper:

```
Router(config)# telephony-service
```

- Mettre l'adresse IP source et le numéro du port de ***Telephony Service***, pour que les téléphones le reçoivent et activent ce service pour eux. C'est la même adresse de TFTP à partir duquel les téléphones obtiendront leur *firmware*, et leurs fichiers de configuration:

```
Router(config-telephony)# ip source-address 192.168.1.1 port 2000
```

- **Sachant que:**

✓ **`ephone`**: signifie le téléphone lui-même (hardware). Chaque ephone peut contenir plus d'un DN.

✓ **`ephone-dn`**: représente les propriétés affectées au téléphone (DN, nom d'utilisateur, appel en attente,..), c'est considéré comme un profil d'ephone.

- Maintenant on déclare le nombre maximum de répertoires (DN) qu'on besoin, et le nombre maximum de téléphones qui seront connectés au routeur:

```
Router(config-telephony)# max-dn 15
Router(config-telephony)# max-ephones 15
```

- Chaque CME a une capacité d'accueille limité pour les **`DN`**s et les ephones. Pour les connaitre taper:

```
Router(config-telephony)# max-dn ?
   <1-144>  Maximum directory numbers supported
Router(config-telephony)# max-ephones ?
   <1-42>   Maximum phones to support
```

- Nous allons créer l'**`ephone-dn`** et le distinguer par le numéro 5 et y ajouter le numéro d'appel 100:

```
Router(config)# ephone-dn 5
Router(config-ephone-dn)number 100
Router(config-ephone-dn)name Secrétariat RT
```

- Pour une ligne avec deuxième appel:

```
Router(config)# ephone-dn 5 dual-line
Router(config-ephone-dn)number 100
```

- Nous lierons maintenant **`ephone-dn 5`** avec **`ephone 3`** par la configuration des paramètres suivant:

✓ **`Type:`** type de l'IP-Phone (7960, 7940,..), **`CIPC`** pour les soft-phone.

✓ **`Mac-address`**: de l'équipement que nous voulons connecter (IP-Phone, soft-phone).

✓ **`Button 1:5`** signifie que le bouton **1** d'IP-Phone lié avec ephone-dn **5**.

- La configuration se fait comme suit:

```
Router(config)# ephone 3
Router(config-ephone)# type 7960
Router(config-ephone)# mac-address 1234.5672.9101
Router(config-ephone)# button 1:5
```

2.2.4. Routage

- Les routeurs implantés dans la topologie sont lies entre eux à travers l'interface ***Serial***, lors de la configuration de ces interfaces, la vitesse de transmission (échange) doit être définie sur l'un des deux routeurs, par la commande **`Clock rate`**:

```
Router(config)# int se 0/0/0
Router(config-if)# ip add 10.10.10.1 255.255.255.0
Router(config-if)# clock rate 64000
Router(config-if)# no sh
```

- Afin d'assurer le bon routage des trames (voix, data), entre les différents équipements du réseau, nous avons utilisé le protocole OSPF.

Le protocole OSPF (*Open Shortest Path First*) est le protocole de routage dynamique intérieur TCP/IP de l'IETF. OSPF collecte l'état de toutes les liaisons au niveau d'une zone (*area*) et calcule de son point de vue toutes les routes pour les destinations de la zone. Les meilleures routes sont alors intégrées dans sa table de routage. [20]

✓ **Pratiquement**, l'utilisation de ce protocole est basé sur l'ajout à la table de routage du routeur, les adresses IP avec le masque-sous réseau **inversé** et la zone (*area*), des réseaux qui sont physiquement connectés aux interfaces de ce routeur.

✓ Pour que le routage par OSPF fonctionne, vous devez commencer par **`area 0`**, après ça vous pouvez choisi n'import quel numéro pour area (area 1, 2, 10,..):

```
Router(config)# router ospf 5
Router(config-router)# network 192.168.10.0 0.0.0.255 area 0
Router(config-router)# network 192.168.20.0 0.0.0.255 area 0
Router(config-router)# network 10.10.10.0 0.0.0.255 area 1
```

2.2.5. Dial-peer

Dans la section **`dial-peer`**, on définit tous les paramètres importants pour la communication interne entre les téléphones, et la communication externe via le réseau WAN ou vers le réseau téléphonique traditionnel (RTC/PSTN). La configuration de dial-peer permet de router les appels lorsqu'ils sont transitent une passerelle vers un autre réseau en dehors de ce routeur. Afin d'atteindre ces services, Cisco a créé les modules suivants:

- **Module FXS** (*Foreign exchange station*): pour la connexion interne des téléphones analogiques simples. La création d'une ligne analogique (3301) pour ce type de téléphone se fait par l'ajout du mot **POTS** (*Plain old telephone service*) à l'instruction **`dail-peer voice`** suivi par le DN et le port auquel le téléphone est connecté:

```
Router(config)#dial-peer voice 1 pots
Router(config-dial-peer)# destination-pattern 3301
Router(config-dial-peer)#port 1/0/0
```

- **Module FXO** (*Foreign exchange Office*): pour connecter le routeur au réseau téléphonique publique (RTC). Après avoir installé une ligne téléphonique du réseau RTC dans l'un des ports de ce module, et avant de commencer la configuration de ce service, vous devez savoir que:

`Destination-pattern:` se spécifie le numéro de destination, 8: code d'accès à la ligne installée dans le port 2/0/0, les ponts (...) représentes le numéro appelé. Les points peuvent être remplacés par un `T` (`8T`):

```
Router(config)#dial-peer voice 20 pots
Router(config-dial-peer)#destination-pattern 8......... ! or 8T
Router(config-dial-peer)#port 2/0/0
```

- Envoyer les appels arrive de réseau PSTN (RTC) sur le port 2/0/0 vers le DN 100:

```
router(config)#voice-port 2/0/0
router(config-voiceport)#connection plar 100
```

- Le routage de la **VoIP** vers un réseau WAN utilise les interfaces qui exploitent le protocole TCP/IP, mêmes que les données. Dans la configuration on remplace **POTS** par **VOIP**, et on écrit les premiers numéros qui spécifient le destinataire suivi par des points (..) selon le DN, et en fin on introduit l'adresse IP du CME de destination:

```
Router(config)# dial-peer voice 2 voip
Router(config-dial-peer)# destination-pattern 2...
Router(config-dial-peer)# session target ipv4:10.10.1.2
```

- Pour afficher les **dial-peer** créés, tapez:

```
router#show dial-peer voice summary
```

- Appliquer le Codec G729A en dial-peer qu'est utilisé dans les communications externes à travers le WAN:

```
Router(config-dial-peer)#codec g729br8
```

- Afficher les appels en cours, et le Codec utilisé dans chaque appel:

```
Router#show voice call summary
```

- Afficher l'état des ports connectés aux téléphones comme (FXS), et l'activité des téléphones libres ou occupés (On-hook or Off-hook):

```
Router#show voice port summary
```

2.2.6. Quelques options supplémentaires

- **Numéro abrégé**: on peut abréger le DN 300 par le numéro 9 (sans créer le DN 9). Si on compose 9 ou 300, dans les deux cas l'appel se dirige vers le DN 300 et le téléphone sonnera. L'instruction qui rend cela possible est:

```
Router(config)#num-exp 9 300
```

✓ L'utilité de l'option précédente est minimiser les DNs longs les plus utilisés, comme le DN du standard téléphonique, DN d'urgence. Dans notre plan de numérotation, on peut utiliser cette option aux appels internes pour masquer les deux premiers numéros qui distinguent le routeur. A titre d'exemple, dans le routeur 31, pour appeler le 31100, il suffit de composer 100 (masquer 31), après l'exécution de la commande:

```
R31(config)#num-exp 100 31100
```

- Deux lignes sur un seul téléphone: le bouton 1 a eu le DN 3, le bouton 2 a eu le DN 4:

```
Router(config-ephone)# button 1:3 2:4
```

- Plusieurs lignes sur un seul bouton:

```
Router(config-ephone)# button 1o1,2,3,4
```

- Le téléphone sonne avec un seul Bip:

```
Router(config-ephone)# button 1b1
```

- Mettre le téléphone en mode silencieux:

```
Router(config-ephone)# button 1s1
```

- Le téléphone sonne avec une sonnerie différente:

```
Router(config-ephone)# button 1f1
```

- Si le DN 100 (ephone-dn 1) est **occupé**, **renvoyer** les appels l'arrive vers le DN 101:

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#call-forward busy 101
```

- Si **pas de réponse** (***noan***: *no one answer*), **renvoyer** les appels vers 101 après 20 secondes:

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#call-forward noan 101 timeout 20
```

- Mettre en attente un appelant, avec un rappel sur lui (bip) 3 fois chaque 30 secondes

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 100
Router(config-ephone-dn)#name call park
Router(config-ephone-dn)#park-slot time out 30 limit 3
```

- Vous pouvez mettre les téléphones hors-service après les heures de travail, par la définition des jours et heures du travail sur les DNs concernés:

```
Router(config)# telephony-service
Router(config-telephony)#after-hours day sun 8:00 17:00
Router(config-telephony)#after-hours day thu 8:00 17:00
```

- Pour annuler l'option précédente (after-hours) sur un téléphone:

```
Router(config)#ephone 5
Router(config-ephone)#after-hour exempt
```

3. La sécurité de la topologie

Pour protéger un réseau, la première étape est de sécuriser les points pouvant fournir une faille ou un « *way in* » à d'éventuels intrus. **Dans cette solution** nous verrons comment sécuriser les routeurs et les suitchs. Les autres équipements aient déjà été discutés dans la deuxième partie du chapitre II (Sécurisation de l'infrastructure).

3.1. Sécurisation du switch

3.1.1. Sécurisation de l'administration

Parmi les outils qui peuvent être utilisé pour restreindre l'accès à l'administration du routeur ou du switch est de protéger leurs interfaces par des mots de passe. Les commandes suivantes sont les mêmes entre le routeur et le switch de Cisco:

- Tout d'abord vérifié que le **chiffrement des mots de passes** est bien activé :

```
Router(config)# service password-encryption
```

- Fixer une longueur minimum de 10 caractères pour les mots de passe:

```
Router(config)# security passwords min-length 10
```

- Configurez le mot de passe **console** et validez le **`login`** pour le routeur: pour avoir plus de sécurité la commande **`exec-timeout`** entraine la déconnexion de la ligne au bout de 5 minutes d'inactivité:

```
Router(config)# line console 0
Router(config-line)# password [taper le mot de passe]
Router(config-line)# exec-timeout 5 0
Router(config-line)# login
```

- Configurez le mot de passe pour les lignes **vty** (***V**irtual **t**eletype*) et le port auxiliaire, de l'accès **Telnet** ***(Tel**etype **net**work)* ou **SSH** (***S**ecure **Sh**ell*) au routeur:

```
Router(config)# line vty 0 4
Router config-line)# password [taper le mot de passe]
Router(config-line)# exec-timeout 5 0
Router(config-line)# login
```

- **Sauvegarde et restauration:**

1. Sauvegardez la configuration courante dans la configuration de démarrage:

```
Router# copy running-config startup
```

2. La commande suivante vous permet de récupérer la configuration du routeur, il vous sera demandé l'IP du server TFTP ainsi que le nom sous lequel le fichier sera enregistré:

```
Router# Copy running-config
```

3. Pour copier le fichier **`flash`** de configuration, identifier son nom grâce à :

```
Router# Show flash
```

✓ Puis copié le fichier **`flash`** en TFTP, il vous sera demandé l'IP du server TFTP ainsi que le nom du fichier source et celui sous lequel le fichier sera enregistré:

```
Router# Copy flash : tftp
```

3.1.2. Sécurisation de la connexion

Après avoir vu comment sécuriser l'administration du switch, il serait intéressant de sécuriser un peu les connexions. Cela se fait par de la sécurisation des ports et la fixation d'adresse MAC dans une *whitelist*. Le **`port-security`** permet de filtrer et de restreindre le nombre d'adresse MAC autorisées à se connecter sur le port d'un switch Cisco.

- Pour activer cette fonction sur une interface:

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

- Définir le nombre maximum d'adresses MAC autorisées à se connecter sur cette interface:

```
Switch(config-if)#switchport port-security maximum 5
```

- **En cas de tentative de connexion d'un appareil non autorisé, nous avons le choix entre plusieurs types d'actions :**

1. Éteindre le port:

```
Switch(config-if)#switchport port-security violation shutdown
```

2. Couper le trafic de l'adresse MAC non autorisée et laisser passer les trames de celles autorisées :

```
Switch(config-if)#switchport port-security violation protect
```

3. Bloquer les trames avec inscription dans le sys-log et envoi SNMP:

```
Switch(config-if)#switchport port-security violation restrict
```

- **Attribution des adresses MAC :**

1. En mode Statique: la saisie des adresses MAC se fait manuellement:

```
Switch(config-if)#switchport port-security mac-address XXXX.XXXX.XXXX
```

2. En mode Sticky: le switch dans ce mode va récupérer les adresses MAC des premiers appareils connectés. Une fois le nombre maximum de MAC enregistrées, l'interface n'acceptera plus d'adresses supplémentaires. Les adresses sont alors enregistrées automatiquement et attribuées à l'interface même si les appareils ne sont plus connectés:

```
Switch(config-if)#switchport port-security mac-address sticky
```

- **Configuration de temps de validité d'une adresse MAC:**

1. Le mode **`absolute`** supprime les MAC après un temps déterminé (240 minutes):

```
Switch(config-if)#switchport port-security aging time 240
Switch(config-if)#switchport port-security aging type absolute
```

2. Le mode **`inactivity`** supprime les MAC après un temps d'inactivité déterminé.

```
Switch(config-if)#switchport port-security aging time 180
Switch(config-if)#switchport port-security aging type inactivity
```

- **Recovery**: Vous pouvez spécifier une durée pendant laquelle le port va subir les actions provoquées par une violation. Après ce délai, le port va remonter automatiquement (Après 180 mn dans l'exemple ci dessous):

```
Switch(config-if)#errdisable recovery interval 180
Switch(config-if)#errdisable recovery cause psecure-violation
```

3.2. Sécurisation du routeur

3.2.1. Sécurisation de l'administration

Pour sécuriser l'administration du routeur, appliquez les mêmes commandes que nous avons vues dans la configuration du switch.

3.2.2. Sécurisation de la connexion

Il existe plusieurs moyens pour sécuriser notre connexion au niveau de routeur, dont certains sont détaillés dans la deuxième partie du chapitre II. Parmi lesquels nous avons choisi **l'implémentation d'un VPN IPSec site à site avec l'IOS Cisco.**

Il y a deux phases principales pour l'implémentation d'un VPN IPSec:

1. La configuration des paramètres IKE *(Internet Key Exchange)*: IKE phase 1, définit la méthode d'échange de clés utilisée pour passer et valider les stratégies IKE entre les extrémités.

2. La configuration des paramètres IPSec: dans IKE phase 2, les extrémités échanges et négocient les stratégies IPSec pour l'authentification et le cryptage du trafic de données.

La réalisation de deux phases précédentes passe par les étapes suivantes:

➡ **Validation des stratégies IKE sur le routeur:**

IKE doit être validé pour que IPSec fonctionne. IKE est validé par défaut sur les images de l'IOS avec les ensembles fonctionnels de cryptographie. S'il est désactivé pour une raison quelconque, avec la commande suivante, vous pouvez le réactiver et vérifier en même temps que l'IOS du routeur supporte IKE:

```
R1(config)# crypto isakmp enable
```

Etablissement d'une stratégie ISAKMP (*Internet Security Association and Key Management Protocol*):

Pour permettre la négociation IKE Phase 1, vous devez créer une stratégie **ISAKMP** et configurer une association d'extrémité incluant la stratégie ISAKMP. Une stratégie ISAKMP définit les algorithmes d'authentification, de cryptage et de hachage utilises pour transmettre du trafic de contrôle entre les deux extrémités VPN.

- Défini la stratégie par un numéro approprié (10, 11, 12,..):

```
R1(config)# crypto isakmp policy 10
```

Votre choix d'un algorithme de cryptage détermine le degré de confidentialité du canal de contrôle entre les extrémités. L'algorithme de hachage contrôle l'intégrité des données, assurant que les données reçues d'une extrémité n'ont pas été modifiées pendant leur transit. Le type d'authentification assure que le paquet a bien été transmis et signé par cette extrémité distante. Le groupe Diffie-Hellman est utilisé pour créer une clé secrète partagée par les extrémités qui n'est pas transmise à travers le réseau.

- Configurez un type d'authentification avec clés **pré-partagées**. Utilisez **AES-256** pour le cryptage, **SHA** pour l'algorithme de hachage et Diffie-Hellman **groupe 5** pour l'échange de clés pour cette stratégie IKE, une durée de vie de 7200 secondes:

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 7200
R1(config-isakmp)#ex
```

Configuration des clés pré-partagées:

Ces clés doivent correspondre sur chaque routeur qui pointe vers l'autre extrémité du VPN pour que l'authentification soit réussie.

- Sur le routeur local on prend **cisco12345** comme une clé pré-partagée, avec l'adresse IP de l'interface distante que l'extrémité utilise pour router le trafic vers le routeur local:

```
R1(config)#crypto isakmp key cisco123 address 10.2.2.1
```

Configuration du transform set IPSec et des durées de vie:

Le **transform set IPSec** est un autre paramètre de configuration IPSec que les routeurs négocient pour former une association de sécurité.

- On va créer un **transform set** avec le tag **R100** en utilisant l'**ESP** *(Encapsulating Security Protocol)* avec cryptage **AES-256** et **md5-hmac**. Les transform set doivent être identiques sur les deux routeurs d'extrémités:

```
R1(config)#crypto ipsec transform-set R100 esp-aes 256 esp-md5-hmac
```

- Vous pouvez également changer les durées de vie des associations de sécurité IPSec qui sont par défaut 3600 secondes:

```
R1(config)#crypto ipsec security-association lifetime seconds 3600
```

Définition du trafic intéressant (`access-list`):

Pour utiliser le cryptage avec le VPN IPSec, il est nécessaire de définir une liste d'accès étendue pour indiquer au routeur quel trafic il doit crypter. Un paquet qui est permis par une liste d'accès utilisée pour définir le trafic IPSec est crypté si la session IPSec est configurée correctement. Un paquet qui est rejeté par une de ces listes d'accès n'est pas rejeté mais transmis sans être crypte. Tout comme les autres listes d'accès, il y a une instruction implicite de rejet à la fin de la liste d'accès qui dans ce cas veut dire que l'action par défaut est de ne pas crypter le trafic. S'il n'y a pas d'association IPSec correctement configurée, le trafic n'est pas crypte et il est acheminé normalement

- Le trafic que vous voulez crypter est du trafic allant du LAN Ethernet de routeur local vers le LAN Ethernet de routeur distant ou vice versa. Ces listes d'accès sont utilisées en sortie sur les interfaces des extrémités VPN et doivent être un miroir l'une de l'autre:

```
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Créer et appliquer une `crypto map`:

Une **`crypto map`** associe le trafic intéressant qui correspond à la liste d'accès avec une extrémité et différents paramètres IKE et IPSec. Apres la création de la crypto map, celle-ci peut être appliquée à une ou plusieurs interfaces. Les interfaces auxquelles elle est appliquée doit être une de celle faisant face à l'autre extrémité IPSec.

- Créez la crypto map nommée `THEME` sur R1 avec **`10`** comme numéro de séquence, en utilisant le type **`ipsec-isakmp`** qui signifie que IKE est utilisé pour établir les associations de sécurité IPSec:

```
R1(config)# crypto map THEME 10 ipsec-isakmp
```

- la commande **`match-address`** plus un numéro d'**`access-list`** pour spécifier quelle liste d'accès définit le trafic à crypter:

```
R1(config-crypto-map)# match address 111
```

- Configurer un nom de host ou une adresse IP d'extrémité est requis. On ajout l'adresse IP de l'interface de l'extrémité VPN distante du routeur R3, avec la commande suivante:

```
R1(config-crypto-map)#set peer 10.2.2.1
```

- Indiquez le **`transform set`** et le **`pfs`** (*Perfect forwarding secrecy*) à utiliser avec cette extrémité, et modifiez également la durée de vie de l'association de sécurité IPSec:

```
R1(config-crypto-map)#set transform-set R100
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#ex
```

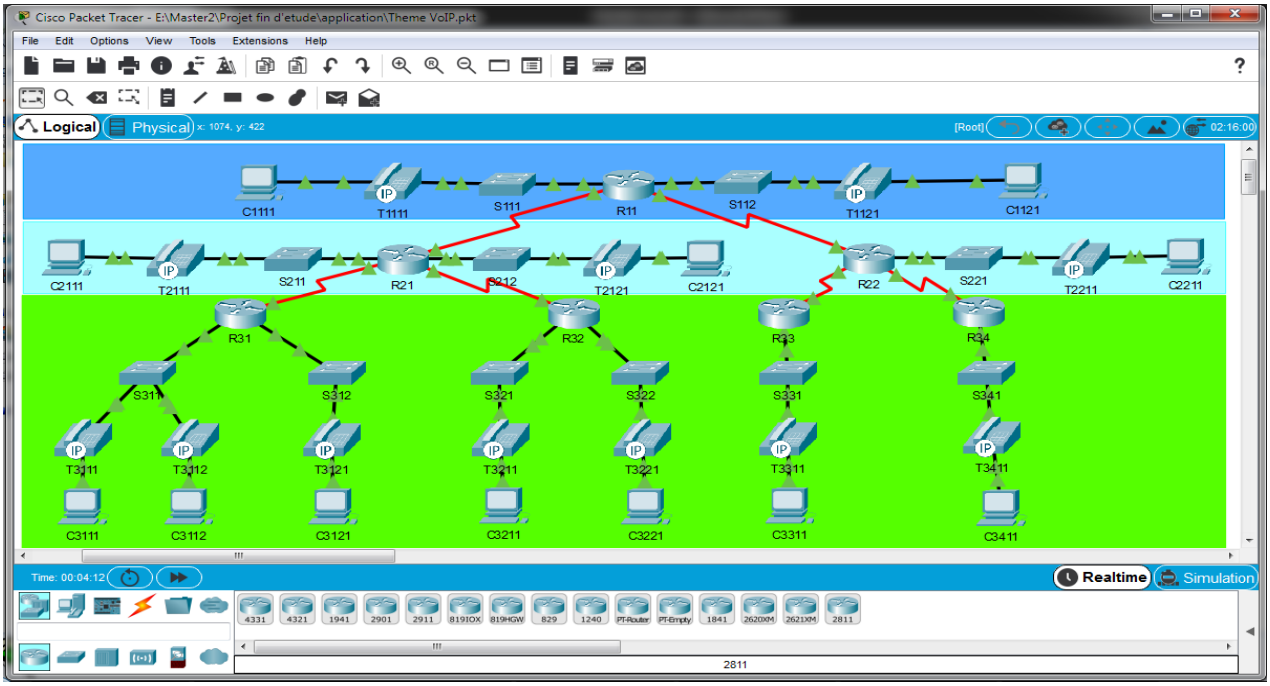
La dernière étape est l'application des crypto map aux interfaces. Notez que les associations de sécurité (SA) ne seront pas établies tant que la crypto map n'aura pas été activée par le trafic intéressant.

- Appliquez les crypto map aux interfaces appropriées sur routeur:

```
R1(config)#interface S0/0/0
R1(config-if)#crypto map THEME
R1(config-if)#ex
```

4. Configuration des équipements

Après la description des commandes intéressantes, nous verrons comment configurer les équipements de la topologie montrée dans la figure ci-dessous, en prenant un échantillon de chaque type d'équipements (un switch et un routeur). Car, les étapes et les commandes de configuration des services sont les mêmes sur tous les équipements du même type. Les indices qui se changeront dans les autres équipements sont: les noms et les adresses IP.



Figure(23): La topologie réalisée sur Cisco Packet Tracer

4.1. Configuration du switch S111

- Entrer en mode de configuration, et renommé le switch comme indiqué ci-dessous:

```
Switch>en
Switch# conf t
Switch(config)# hostname S111
```

- **Création des VLANs**: VLAN pour la voix, VLAN pour les données, et un autre pour la gestion à distance du Switch:

```
S111(config)# VLAN 10
S111(config-vlan)# name voice1
S111(config-vlan)# VLAN 20
S111(config-vlan)# name data1
S111(config-vlan)# VLAN 71
S111(config-vlan)# name remot1
S111(config-vlan)# ex
```

- Le switch Cisco-2960 se compose de 24 ports *fast-Ethernet*, nous avons réservé 23 ports pour la connexion des machines (PC, IP-Phone,..) et le 24ème port pour la communication avec le Routeur. Les ports désignés pour les machines doivent avoir la fonction d'accès: voix et données.

```
S111(config)# int range fa 0/1-23
S111(config-if-range)# switchport mode access
S111(config-if-range)# switchport voice VLAN 10
S111(config-if-range)# switchport access VLAN 20
S111(config-if-range)# no sh
S111(config-if-range)# ex
```

- Pour accéder à distance à ce switch, vous devez disposer d'une adresse privée à travers le VLAN dédie :

```
S111(config)# int VLAN 71
S111(config-if)# ip add 192.168.71.10 255.255.255.0
S111(config-if)# no sh
S111(config-if)# ex
```

- Le 24ème port du switch assure la communication avec le retour, on ajout l'option **native** au VLAN de gestion:

```
S111(config)# int fa 0/24
S111(config-if)# switchport mode trunk
S111(config-if)# switchport trunk native VLAN 71
S111(config-if)# no sh
S111(config-if)# ex
```

Sécuriser le port trunk:

```
S311(config-if)# int fa0/24
S111(config-if-range)# switchport port-security
S311(config-if)# switchport port-security mac-address sticky
S311(config-if)# switchport port-security maximum 3
S311(config-if)# switchport port-security violation shutdown
S311(config-if)# no sh
S311(config-if)# ex
```

Sécuriser les ports dédies aux utilisateurs finaux:

```
S111(config)# int range fa 0/1-23
S111(config-if-range)# switchport port-security
S111(config-if-range)# switchport port-security mac-address sticky
S111(config-if-range)# switchport port-security maximum 3
S111(config-if-range)# switchport port-security violation shutdown
S111(config-if-range)# no sh
S111(config-if-range)# ex
S111(config)# do wr
```

4.2. Configuration du routeur R11

- Entrer en mode de configuration, et renommé le routeur comme indiqué ci-dessous:

```
Router>en
Router# conf t
Router(config)# hostname R11
R11(config)#
```

- Activer l'interface physique ***fast-ethernet* 0/0** qui relie le **switch S111**:

```
R11(config)# int fa 0/0
R11(config-if)# no sh
R11(config-if)# ex
```

- Configuration des sous-interfaces de **Fa0/0:**

1. Sous-Interface pour le trafic de la voix (VLAN 10):

```
R11(config)# int fa 0/0.10
R11(config-subif)# encapsulation dot1Q 10
R11(config-subif)# ip add 192.168.11.1 255.255.255.192
R11(config-subif)# no sh
R11(config-subif)# ex
```

2. Sous-Interface pour le trafic des données (VLAN 20):

```
R11(config)# int fa 0/0.20
R11(config-subif)# encapsulation dot1Q 20
R11(config-subif)# ip add 192.168.11.65 255.255.255.192
R11(config-subif)# no sh
R11(config-subif)# ex
```

3. Sous-Interface de la gestion et du contrôle à distance (VLAN 71):

```
R11(config)# int fa 0/0.71
R11(config-subif)# encapsulation dot1Q 71
R11(config-subif)# ip add 192.168.71.1 255.255.255.0
R11(config-subif)# no sh
R11(config-subif)# ex
```

- Exclusion des adresses nécessaires (adresses des passerelles, du serveur DHCP, …):

```
R11(config)# ip dhcp excluded-address 192.168.11.0
R11(config)# ip dhcp excluded-address 192.168.11.1
R11(config)# ip dhcp excluded-address 192.168.11.63
R11(config)# ip dhcp excluded-address 192.168.11.64
R11(config)# ip dhcp excluded-address 192.168.11.65
R11(config)# ip dhcp excluded-address 192.168.11.127
R11(config)# ip dhcp excluded-address 192.168.11.128
R11(config)# ip dhcp excluded-address 192.168.11.129
R11(config)# ip dhcp excluded-address 192.168.11.191
R11(config)# ip dhcp excluded-address 192.168.11.192
R11(config)# ip dhcp excluded-address 192.168.11.193
R11(config)# ip dhcp excluded-address 192.168.11.255
```

- Configuration du serveur DHCP pour les équipements de la VoIP, avec l'option 150 de serveur TFTP:

```
R11(config)# ip dhcp pool voice1
R11(dhcp-config)# network 192.168.11.0 255.255.255.192
R11(dhcp-config)# default-router 192.168.11.1
R11(dhcp-config)# option 150 ip 192.168.11.1
R11(dhcp-config)# ex
```

- DHCP pour les données, avec l'option 150 pour les *Soft-Phone:*

```
R11(config)# ip dhcp pool data1
R11(dhcp-config)# network 192.168.11.64 255.255.255.192
R11(dhcp-config)# default-router 192.168.11.65
R11(dhcp-config)# option 150 ip 192.168.11.65
R11(dhcp-config)# ex
```

- Activer l'interface physique ***fast-ethernet* 0/1** qui relie le **switch S112**:

```
R11(config)# int fa 0/1
R11(config-if)# no sh
R11(config-if)# ex
```

- Configuration des sous-interfaces de **`Fa0/1:`**

1. Sous-Interface pour le trafic de la voix (VLAN 10):

```
R11(config)# int fa 0/1.10
R11(config-subif)# encapsulation dot1Q 10
R11(config-subif)# ip add 192.168.11.129 255.255.255.192
R11(config-subif)# no sh
R11(config-subif)# ex
```

2. Sous-Interface pour le trafic des données (VLAN 20):

```
R11(config)# int fa 0/1.20
R11(config-subif)# encapsulation dot1Q 20
```

```
R11(config-subif)# ip add 192.168.11.193 255.255.255.192
R11(config-subif)# no sh
R11(config-subif)# ex
```

3. Sous-Interface de la gestion et du contrôle à distance (VLAN 72):

```
R11(config)# int fa 0/1.72
R11(config-subif)# encapsulation dot1Q 72
R11(config-subif)# ip add 192.168.72.1 255.255.255.0
R11(config-subif)# no sh
R11(config-subif)# ex
```

- Configuration du serveur DHCP pour les équipements de la VoIP, avec l'option 150 de serveur TFTP:

```
R11(config)# ip dhcp pool voice2
R11(dhcp-config)# network 192.168.11.128 255.255.255.192
R11(dhcp-config)# default-router 192.168.11.129
R11(dhcp-config)# option 150 ip 192.168.11.129
R11(dhcp-config)# ex
```

- DHCP pour les données, avec l'option 150 pour les *Soft-Phone:*

```
R11(config)# ip dhcp pool data2
R11(dhcp-config)# network 192.168.11.192 255.255.255.192
R11(dhcp-config)# default-router 192.168.11.193
R11(dhcp-config)# option 150 ip 192.168.11.193
R11(dhcp-config)# ex
```

- Activer ***Telephony Service*** et mettre son adresse IP source et le numéro du port de:

```
R11(config)# telephony-service
R11(config-telephony)# ip source-address 192.168.11.1 port 2000
```

- Limiter les DNs et les IP-Phone par 20:

```
R11(config-telephony)# max-dn 20
R11(config-telephony)# max-ephones 20
R11(config-telephony)# ex
```

- Création des DNs:

```
R11(config)# ephone-dn 1
R11(config-ephone-dn)number 11100
R11(config-ephone-dn)ephone-dn 2
R11(config-ephone-dn)number 11101
R11(config-ephone-dn)ephone-dn 3
R11(config-ephone-dn)number 11200
R11(config-ephone-dn)ephone-dn 4
R11(config-ephone-dn)number 11201
R11(config-ephone-dn)ex
```

- Attribuer les **DN**s aux IP-Phones et soft-phones:

```
R11(config)# ephone 1
R11(config-ephone)# type 7960
R11(config-ephone)# mac-address 000a.414b.2d0a
R11(config-ephone)# button 1:1
R11(config-ephone)# ex
R11(config)# ephone 2
R11(config-ephone)# type CIPC  !pour soft-phone
R11(config-ephone)# mac-address 0001.427a.535a
R11(config-ephone)# button 1:2
R11(config-ephone)# ex
R11(config)# ephone 3
R11(config-ephone)# type 7960
R11(config-ephone)# mac-address 0030.f217.5597
```

```
R11(config-ephone)# button 1:3
R11(config-ephone)# ex
R11(config)# ephone 4
R11(config-ephone)# type CIPC
R11(config-ephone)# mac-address 0006.2a45.d6c8
R11(config-ephone)# button 1:4
R11(config-ephone)# ex
```

- Configuration des interfaces du réseau externe WAN

```
R11(config)# int se 0/0/0
R11(config-if)# ip add 10.11.21.1 255.255.255.0
R11(config-if)# clock rate 64000
R11(config-if)# no sh
R11(config-if)# ex
R11(config)# int se 0/0/1
R11(config-if)# ip add 10.11.22.1 255.255.255.0
R11(config-if)# clock rate 64000
R11(config-if)# no sh
R11(config-if)# ex
```

- Configuration de routage par le protocole OSPF:

```
R11(config)# router ospf 11
R11(config-router)# network 192.168.11.0 0.0.0.255 area 0
R11(config-router)# network 10.11.21.0 0.0.0.255 area 0
R11(config-router)# network 10.11.22.0 0.0.0.255 area 1
R11(config-router)# ex
```

- Configuration de **`dial-peer`** afin de communiquer en VoIP, avec les autres CMEs via le réseau WAN :

1. Pour communiquer en VoIP avec le routeur R21:

```
R11(config)# dial-peer voice 21 voip
R11(config-dial-peer)# destination-pattern 21...
R11(config-dial-peer)# session target ipv4:10.11.21.2
R11(config-dial-peer)# ex
```

2. Pour communiquer avec le routeur R22:

```
R11(config)# dial-peer voice 22 voip
R11(config-dial-peer)# destination-pattern 22...
R11(config-dial-peer)# session target ipv4:10.11.22.2
R11(config-dial-peer)# ex
```

3. Avec le routeur R31:

```
R11(config)# dial-peer voice 31 voip
R11(config-dial-peer)# destination-pattern 31...
R11(config-dial-peer)# session target ipv4:10.21.31.2
R11(config-dial-peer)# ex
```

4. Avec le routeur R32:

```
R11(config)# dial-peer voice 32 voip
R11(config-dial-peer)# destination-pattern 32...
R11(config-dial-peer)# session target ipv4:10.21.32.2
R11(config-dial-peer)# ex
```

5. Avec le routeur R33:

```
R11(config)# dial-peer voice 33 voip
R11(config-dial-peer)# destination-pattern 33...
R11(config-dial-peer)# session target ipv4:10.22.33.2
R11(config-dial-peer)# ex
```

6. Avec le routeur R34:

```
R11(config)# dial-peer voice 34 voip
R11(config-dial-peer)# destination-pattern 34...
R11(config-dial-peer)# session target ipv4:10.22.34.2
R11(config-dial-peer)# ex
```

Les mesures de sécurité:

- Configuration d'ISAKMP sur R11:

```
R11(config)# crypto isakmp policy 11
R11(config-isakmp)# authentication pre-share
R11(config-isakmp)# hash md5
R11(config-isakmp)# encryption aes 256
R11(config-isakmp)# group 5
R11(config-isakmp)# lifetime 86400
R11(config-isakmp)# ex
```

- Sélectionner les algorithmes de cryptage pour `IPSec transform-set` avec un nom `TSR11` (Transform-Set Routeur 11):

```
R11(config)# crypto ipsec transform-set TSR11 esp-aes 256 esp-md5-hmac
```

- Fixez la durée de vie de l'association de sécurité IPSec à 28800 secondes:

```
R11(config)# crypto ipsec security-association lifetime seconds 28800
```

1. Pour la communication cryptée avec le routeur R21:

- Définition du trafic intéressant (liste d'accès):

```
R11(config)# access-list 121 permit ip 192.168.11.0 0.0.0.255 192.168.21.0 0.0.0.255
```

- Choisi la clé de cryptage inclue dans la communication avec R21:

```
R11(config)# crypto isakmp key tebessa address 10.11.21.2
```

- Configuration de **`crypto map:`**

```
R11(config)# crypto map MAPR11 21 ipsec-isakmp
R11(config-crypto-map)# set peer 10.11.21.2
R11(config-crypto-map)# set transform-set TSR11
R11(config-crypto-map)# set pfs group5
R11(config-crypto-map)# set security-association lifetime seconds 7200
R11(config-crypto-map)# match address 121
R11(config-crypto-map)# ex
```

2. Pour la communication cryptée avec le routeur R22:

```
R11(config)# access-list 122 permit ip 192.168.11.0 0.0.0.255 192.168.22.0 0.0.0.255
R11(config)# crypto isakmp key tebessa address 10.11.22.2
R11(config)# crypto map MAPR11 22 ipsec-isakmp
R11(config-crypto-map)# set peer 10.11.22.2
R11(config-crypto-map)# set transform-set TSR11
R11(config-crypto-map)# set pfs group5
R11(config-crypto-map)# set security-association lifetime seconds 7200
R11(config-crypto-map)# match address 122
R11(config-crypto-map)# ex
```

3. Avec le routeur R31:

```
R11(config)# access-list 131 permit ip 192.168.11.0 0.0.0.255 192.168.31.0 0.0.0.255
R11(config)# crypto isakmp key tebessa address 10.21.31.2
R11(config)# crypto map MAPR11 31 ipsec-isakmp
R11(config-crypto-map)# set peer 10.21.31.2
R11(config-crypto-map)# set transform-set TSR11
```

```
R11(config-crypto-map)# set pfs group5
R11(config-crypto-map)# set security-association lifetime seconds 7200
R11(config-crypto-map)# match address 131
R11(config-crypto-map)# ex
```

4. Avec le routeur R32:

```
R11(config)# access-list 132 permit ip 192.168.11.0 0.0.0.255 192.168.32.0 0.0.0.255
R11(config)# crypto isakmp key tebessa address 10.21.32.2
R11(config)# crypto map MAPR11 32 ipsec-isakmp
R11(config-crypto-map)# set peer 10.21.32.2
R11(config-crypto-map)# set transform-set TSR11
R11(config-crypto-map)# set pfs group5
R11(config-crypto-map)# set security-association lifetime seconds 7200
R11(config-crypto-map)# match address 132
R11(config-crypto-map)# ex
```

5. Avec le routeur R33:

```
R11(config)# access-list 133 permit ip 192.168.11.0 0.0.0.255 192.168.33.0 0.0.0.255
R11(config)# crypto isakmp key tebessa address 10.22.33.2
R11(config)# crypto map MAPR11 33 ipsec-isakmp
R11(config-crypto-map)# set peer 10.22.33.2
R11(config-crypto-map)# set transform-set TSR11
R11(config-crypto-map)# set pfs group5
R11(config-crypto-map)# set security-association lifetime seconds 7200
R11(config-crypto-map)# match address 133
R11(config-crypto-map)# ex
```

6. Avec le routeur R34:

```
R11(config)# access-list 134 permit ip 192.168.11.0 0.0.0.255 192.168.34.0 0.0.0.255
R11(config)# crypto isakmp key tebessa address 10.22.34.2
R11(config)# crypto map MAPR11 34 ipsec-isakmp
R11(config-crypto-map)# set peer 10.22.34.2
R11(config-crypto-map)# set transform-set TSR11
R11(config-crypto-map)# set pfs group5
R11(config-crypto-map)# set security-association lifetime seconds 7200
R11(config-crypto-map)# match address 134
R11(config-crypto-map)# ex
```

- Appliquez la **crypto map** créé aux interfaces de sortie du routeur R31:

```
R11(config)# int se0/0/0
R11(config-if)# crypto map MAPR11
R11(config-if)# ex
R11(config)# int se0/0/1
R11(config-if)# crypto map MAPR11
R11(config-if)# ex
```

- Et en fin, n'oublier pas de sauvegarder la configuration à chaque étape:

```
R11(config)# do wr
```

4.3. Les stations de travail et les IP-Phones

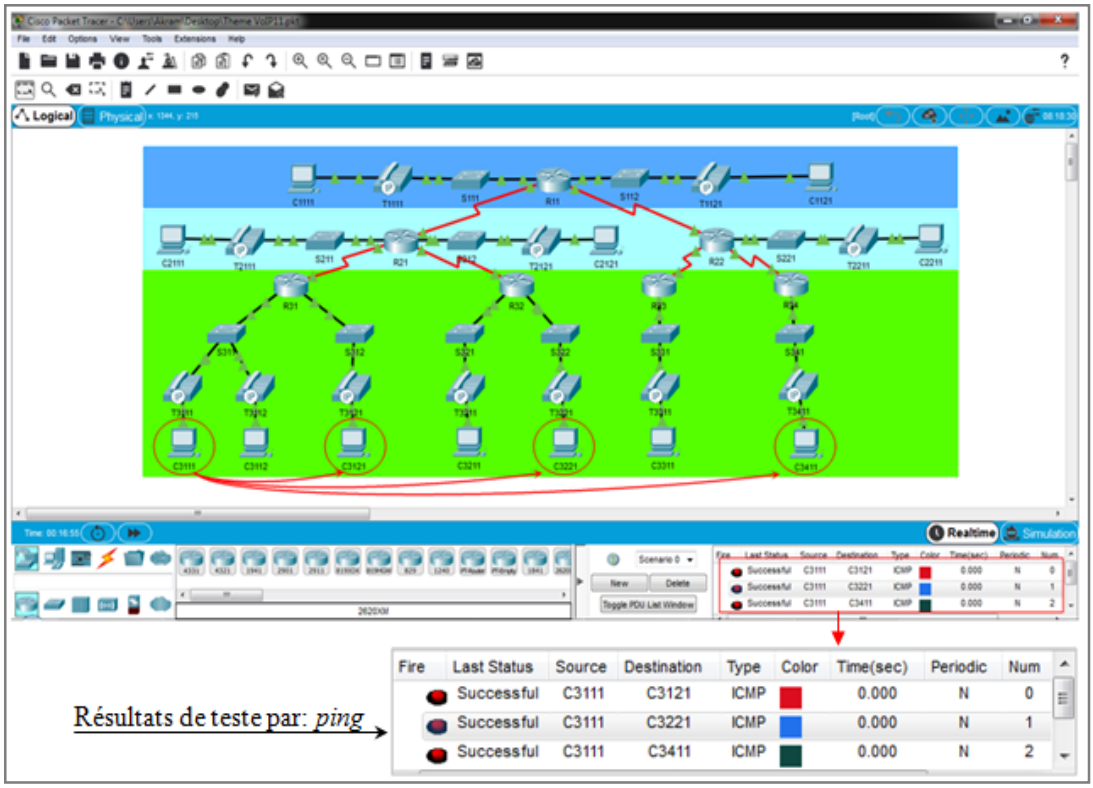
✓ Après la configuration des serveurs DHCP (voix et data) au niveau des routeurs, les paramètres IP des stations de travail (IPv4) doit être déterminés automatiquement (DHCP mode).

✓ Afin de mise en service de notre réseau téléphonique VoIP, les IP-Phones doivent être alimentés par les adaptateurs fournis avec eux, car les switchs utilisés ne sont pas des PoE.

5. Vérifications et tests

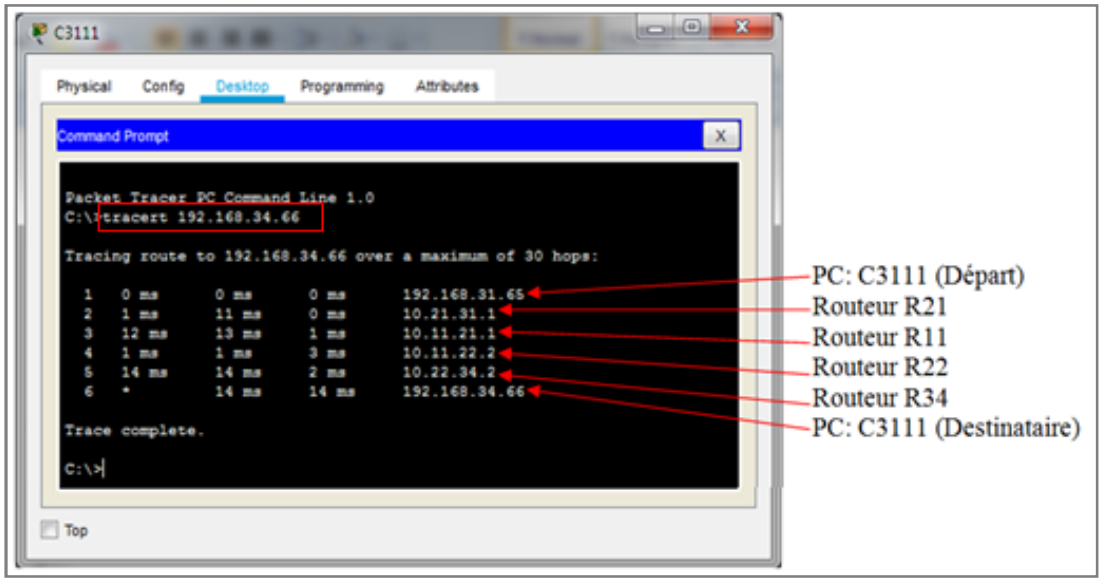
5.1. Vérification du routage des paquets

- **La requête *ping*:** Afin de vérifier la circulation des trames entre les différents routeurs de notre topologie, on utilise la requête *ping*. En envoi un paquet IP de 32 octets à partir du PC C3111 vers les PCs: C3121, C3221, C3411, la figure suivante illustre les résultats obtenus:



Figure(24): Les résultats obtenus par la requête ***ping***

- **La requête *traceroute***: est utilisé pour suivi le chemin de paquet envoyé jusqu'à l'arrive au destinataire. En utilisant l'utilitaire ***Command-Prompt*** à partir du PC C3111, en envoi un paquet IP vers le PC C3411, les résultats obtenus montrent le chemin suivi par le paquet:



Figure(25): Les résultats obtenus par la requête ***traceroute.***

5.2. Test d'appel en VoIP

Nous avons fait des tests entre tous les IP-Phones et Soft-Phones de notre topologie et les résultats étaient bons. Nous en représenterons dans la figure suivante, un cas d'un appel depuis l'IP-Phone T3111 (DN: 31100) vers le Soft-Phone C3411 (DN: 34200):

Figure(26): Simulation d'un appel VoIP entre un IP-Phone et Soft-Phone

5.3. Test de la sécurité

5.3.1. Au niveau du switch S111

- Pour voir les adresses MAC autorisées sur chacun des ports sécurisés :

```
S111#sh port-security address
Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address        Type             Ports            Remaining Age(mins)
----    -----------        ----             -----              -------------
20      0001.427A.535A     SecureSticky     FastEthernet0/1      -
20      000A.414B.2D0A     SecureSticky     FastEthernet0/1      -
71      00D0.BC11.9E01     SecureSticky     FastEthernet0/24     -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 1024
```

- Pour afficher les paramètres de sécurité des ports du switch ou de l'interface spécifiée:

```
S111#sh port-security int fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 000A.414B.2D0A:10
```

- **Security Violation Count** : Lorsque l'on débranche le PC **C1111** et que l'on branche un nouveau PC (PC0), on peut voir que la connexion est active (elle peut se désactiver), mais si on effectue un ***ping*** à partir du **PC0** vers n'importe quelle machine connectée au ce réseau, il n'y a pas de réponse. Donc, la protection s'applique bien.

5.3.2. Au niveau du routeur R11

- Vérification de la stratégie IKE :

```
R11#show crypto isakmp policy
Global IKE policy
Protection suite of priority 11
       encryption algorithm:      AES - Advanced Encryption Standard (256 bit keys).
       hash algorithm:            Message Digest 5
       authentication method:     Pre-Shared Key
       Diffie-Hellman group:      #5 (1536 bit)
       lifetime:                  86400 seconds, no volume limit
```

- **Vérification de la configuration IPSec**: la commande suivante affiche la configuration des stratégies IPSec configurées sous la forme d'un **`transform-set`**

```
R11#sh crypto ipsec transform-set
Transform set TSR11: { { esp-256-aes esp-sha-hmac } 
       will negotiate = { Tunnel, },
```

- Pour afficher les **`crypto maps`** appliquées au routeur, utilisez la commande:

```
R11#show crypto map
Crypto Map MAPR11 21 ipsec-isakmp
       Peer = 10.11.21.2
       Extended IP access list 121
           access-list 121 permit ip 192.168.11.0 0.0.0.255 192.168.21.0 0.0.0.255
       Current peer: 10.11.21.2
       Security association lifetime: 4608000 kilobytes/7200 seconds
       PFS (Y/N): Y
       Transform sets={
               TSR11,
       }
       Interfaces using crypto map MAPR11:
               Serial0/0/0
               Serial0/0/1
```

Vérification du fonctionnement du VPN IPSec

- Affichage des associations de sécurité ISAKMP:

```
R11#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state      conn-id   slot status
10.21.31.2      10.11.21.1      QM_IDLE       1047      0 ACTIVE

10.11.21.2      10.11.21.1      QM_IDLE       1046      0 ACTIVE

10.21.32.2      10.11.21.1      QM_IDLE       1060      0 ACTIVE

10.22.33.2      10.11.22.1      QM_IDLE       1037      0 ACTIVE

10.22.34.2      10.11.22.1      QM_IDLE       1081      0 ACTIVE

10.11.22.2      10.11.22.1      QM_IDLE       1082      0 ACTIVE
```

- Vérifier combien de paquets ont été cryptes entre deux routeurs:

```
R11#show crypto ipsec sa
interface: Serial0/0/0
       Crypto map tag: MAPR11, local addr 10.11.21.1
       protected vrf: (none)
       local ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.21.0/255.255.255.0/0/0)
       current_peer 10.11.21.2 port 500
       PERMIT, flags={origin_is_acl,}
       #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
       #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 0
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 0, #pkts compr. failed: 0
       #pkts not decompressed: 0, #pkts decompress failed: 0
       #send errors 0, #recv errors 4
       local crypto endpt.: 10.11.21.1, remote crypto endpt.:10.11.21.2
       path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
       current outbound spi: 0x320E2DA2(839789986)
```

Conclusion

Dans ce chapitre, nous avons vu comment préparer un plan de mise en œuvre d'un réseau WAN (voix et données), que ce soit en termes de: la structure de la topologie, le choix du matériel approprié, dénomination des équipements, numérotation des téléphones et plan d'adressage IP. Nous avons expliqué le rôle des différentes commandes utilisées pour configurer ces équipements et leurs objectifs, puis l'implémentation d'une solution pour sécuriser notre réseau. Où tout cela a été appliqué sur le simulateur *Cisco Packet Tracer*. Et nous avons conclu en menant des tests et des essais et en clarifiant les résultats obtenus.

Conclusion générale

Il n'est pas possible de transporter des informations d'un endroit à un autre, sans penser à un moyen pour y parvenir. C'est pour ça les techniciens de télécom ont réfléchi au développement et la diversification des supports de transmission qui offrent: la vitesse, la flexibilité, la bonde passantes large, et tous en faible coût. Parmi les différents supports de transmission utilisables dans les réseaux d'information, que nous avons citée dans le premier chapitre de ce mémoire, nous nous sommes concentrés sur les antennes faisceaux hertziens (FH), en mettant en évidence les caractéristiques techniques de l'une de ces antennes et ses avantages qui nous conviennent.

La VoIP est la voie de l'avenir. Elle peut considérablement réduire les coûts des appels téléphoniques par rapport au réseau téléphonique traditionnel public (RTC), en raison des avantages fournit par l'utilisation d'Internet. Ainsi, la technologie VoIP est la meilleure source de communication longue distance jusqu'à présent. Toutes les fonctionnalités et caractéristiques fournit par cette technologie sont détaillées dans la première partie du chapitre II.

Pour améliorer la sécurité des réseaux, les développeurs disposent de nombreux outils, comme les systèmes de détection d'intrusions, les pare-feux, les systèmes de cryptage. Ces outils ont connu un essor particulier au cours des dernières années, notamment en raison du nombre grandissant d'attaques. Parmi ces outils qu'on a détaillés dans la deuxième partie du chapitre II, nous avons choisi pour sécuriser notre topologie, l'implémentation d'un VPN IPSec site à site avec l'IOS Cisco. Le VPN IPSec crée un tunnel entre deux extrémités communiquées, sécurisé par l'intégration de plusieurs protocole de cryptage (IKE, ISAKMP, ESP,..), et assure le chiffrement des paquets transitent les passerelles vers le réseau WAN, en utilisant des algorithmes de chiffrement très puissants.

Parmi les buts de notre travail est de présenter une méthode systématique, sur la façon de mise en place d'un réseau WAN (VoIP et données) sécurisé et faible coût. Nous avons commencé par l'intégration des antennes FH comme un support de transmission au cœur d'un réseau LAN, en raison de ses avantages tels que: la flexibilité, la mobilité, la facilité d'installation.

En effet, l'exploitation optimale du matériel nécessite la sélection (selon le besoin) d'équipements appropriés et dotés de plusieurs fonctions, afin de minimiser les dépenses, et de réduire le nombre des équipements installés et gagner de l'espace au niveau des locaux techniques. A titre d'illustration, un routeur Cisco CME, assure le routage du trafic, et joue le rôle d'un IPBX par la fonctionnalité *telephony service*, le rôle d'une passerelle vers les autres réseaux par l'ajout des cartes d'acquisitions, et le rôle d'un dispositif de sécurité grâce aux protocoles et algorithmes de cryptage intégrés.

En dernière étape, nous avons simulé notre travail sur *Cisco Packet Tracer*, ce qui nécessite de donner la configuration nécessaire aux équipements, et on clôture par les essais et les tests de vérifications, et enfin l'évaluation des résultats obtenus.

Liste des références

Bibliographie

[3] Trango Broadband Wireless-Access5830, User Manual, Rev-D. Juin 2014.

[4] Mr\ADNANE Nasser, Mr\MERSEL Nabyl. Etude et mise en place d'une solution VoIP sécurisée, Mémoire de Master en Informatique, Université de Abderrahmane Mira-Bejaïa, 2017.

[5] Mr\LABIDI Ahmed. Etude et mise en place d'une solution voix sur IP sécurisée, mémoire de fin d'étude, Institut national des sciences appliquées et de technologie, Tunis, 2013.

[6] Mr\BOUZID Redouane, Mr\CHABANA Djahid. Etude d'un système de communication VoIP, Master en Télécommunication. Université de : Abderrahmane Mira-Bejaïa, 2019.

[8] Mlle\TACHOUGAFT Kahina, Mlle\TAGUELMIMT Loubna. Configuration et implémentation de la qualité de service de la voix sur IP (par priorisation de flux), Master en Télécommunication. Université de Abderrahmane Mira-Bejaïa, 2019.

[11] Mr\DABBEBI Oussema. Gestion des risques dans les infrastructures VoIP, thèse de Doctorat. Université de Lorraine-France, 2013.

[12] Mr\HAMID Mahamat Abdoulaye. Audit d'un réseau VoIP et implémentation d'un client SIP sécurisé. Master, TDSI, 2013.

[13] Mr\BENISSE Mohamed-Taib. Transmission media sur les réseaux IP en utilisant les protocoles SIP et IAX, Mémoire de la maitrise en génie Concentration réseaux de télécommunication. Université de Qubéc-France, 2009.

[14] Mlle\AIDA Frija. Etude et mise en place d'une solution VOIP sécurisée, Mastère professionnel en Nouvelles Technologies. Université virtuelle de Tunis, 2018.

[15] M\THOMAS Guillet. Sécurité de la téléphonie sur IP, thèse de Doctorat. université de Télécom Paris-Tech, France, 2010.

[16] Mlle\REBHA Bouzaida. Etude et mise en place d'une solution voip sécurisée, Master en nouvelles technologies des télécommunications et réseaux. Université de : UVT-Tunis, 2011.

[17] Mme\AHMIM Marwa. Etude du protocole IPSec et métriques de sécurité, thèse de Doctorat 3ème cycle. Université de Badji Mokhtar-Annaba, 2016.

Webgraphie

[1] https://fr.wikipedia.org/wiki/Paire_torsad%C3%A9e. Consulté le 26/03/2020 22:15.

[2] https://fr.wikipedia.org/wiki/Onde_radio. Consulté le 14/04/2020 19:18.

[7] http://wapiti.enic.fr/commun/ens/peda/options/ZoneH323-Gatekeeper.htm. Consulté le 03/03/2020 18:29.

[9] https://www.ionos.fr/digitalguide/serveur/udp-user-datagram-protocol. Consulté le 10/03/2020 20:15.

[10] https://www.frameip.com/entete-icmp. Consulté le 10/03/2020 23:46.

[18] https://www.journaldunet.fr/ike-protocole-informatique-detaillee. Consulté le 13/04/2020 17:28.

[19] https://fr.wikipedia.org/wiki/Packet_Tracer. Consulté le 14/05/2020 18:52.

[20] https://cisco.goffinet.org/ccna/ospf/protocole-routage-dynamique-ospf. Consulté le 27/05/2020 14:40.