وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة عبد الحميد ابن باديس مستغانم
Université Abdelhamid Ibn Badis de Mostaganem
كلية العلوم و التكنولوجيا
Faculté des Sciences et de la Technologie

N° d'ordre : M2…./GE/2022

MEMOIRE DE FIN D'ETUDE

DE MASTER ACADEMIQUE

Filière : Génie électrique
Spécialité : Télécommunication

Thème

Étude et simulation d'une architecture réseau basée sur le VOIP dans un environnement VPN IP SEC multi site.

***Présenté par : Melle* : Hadj Sabrina**

Soutenu le **07/ 08/** ***2022 devant le jury composé de :***

Présidente de jury : Mme MIMI Malika Professeur UMAB

Examinateur : M. OULD MAMMAR.M MCA UMAB

Rapporteur : M. RESFA Abbes MCB UMAB

Année Universitaire : 2021 / 2022

Remerciements

Avant tout, je remercie Dieu pour la volonté et la détermination, ainsi que la santé et la patience qu'il m'a données pour faire ce travail.
Je tiens à remercier mon encadreur, M. Resfa Abbes, Pour sa présence à tout moment, ainsi que sa Communication continue avec moi, sa confiance et sa patience, en plus de ses excellentes remarques et Contributions tout le temps jusqu'à la fin du ce travail.

*Nous adressons également nos vifs remerciements à **Pr Mme MIMI MALIKA**, Enseignante à l'Université de Mostaganem, d'avoir bien voulu présider le jury.*

*Nous sommes également très reconnaissants à Mr **OULD MAMMAR MADANI**, Enseignant à l'Université de Mostaganem, d'avoir accepté d'examiner ce modeste travail.*

Nos remerciements s'adressent également :

A tous nos enseignants durant toutes les étapes de notre parcours universitaire, sans exception...

Dédicaces

Avec plaisir, bon cœur et grande joie, je dédie cet Humble travail à mes chers parents, pour leur amour Inestimable pour moi, leur grande confiance, leur soutien Constant et leur grand sacrifice pour moi.

A mon encadreur directeur de mémoire Dr RESFA ABBES pour toutes ses conseils et son aide jusqu'à la dernière minute, que Dieu la garde en bonne Santé ; pour tous ses conseils, et assistance jusqu'au dernier moment, que Dieu le préserve en bonne santé.

Hadj sabrina

Résumé

Le développement de la technologie en général et de l'informatique en particulier suscité un engouement pour la modernisation du traitement des systèmes d'information.

Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux. Mais le succès de ces systèmes d'information a fait aussi apparaître un de leur écueil.

Cette étude nous a permis de mieux appréhender les problèmes liés aux réseaux locaux dont ceux relatifs au déploiement d'un réseau VPN comprenant plusieurs sites distants tout en garantissant une qualité de service.

En outre il nous a permis de nous familiariser davantage aux équipements CISCO.
Il ressort entre autres de cette présente étude qu'il y a accord entre la réflexion théorique menée et la mise en place pratique des VPN, constat qui à notre sens valide notre projet.
Depuis l'apparition de l'informatique dans les années 1950, celui-ci s'est imposé graduellement comme un instrument primordial dans le monde professionnel, devenant l'outil incontournable pour la gestion de l'information allant jusqu' à la prise de décision d'une importance capitale pour les entreprises.

Et comme tout progrès engendre de nouveaux défis, au fil du temps naquit un autre besoin qui était celui d'avoir accès à tout moment et de n'importe où aux ressources offertes par les entités informatisées (entreprise, foyer, administrations, etc..) de manière sécurisée d'où la naissance du besoin en VPN (Virtual Private Network ou Réseau Privé Virtuel.
La VoIP dans un environnement VPN IP SEC multi site est d'appliquer à la voix le même traitement que les autres types de données circulant sur Internet. Grâce au protocole IP, des paquets de données, constitués de la voix numérisée, y sont transportés. En effet, à force de transférer des fichiers d'information en temps de plus en plus réel, les utilisateurs d'Internet en vinrent à transférer de la voix, en temps suffisamment réel pour faire compétition au téléphone.

Toutes fois nous admettons que nos théories et nos réflexions bien qu'empiriques ne soient pas des vérités indubitables et définitives.

Elles sont susceptibles d'être réfutées par des modèles plus robustes ou par des observations postérieures divergentes qui seraient liées à l'évolution des technologies, elles-mêmes en constante mutation. C'est le propre de toute proposition intellectuelle de s'attendre à être un jour ou l'autre dépassée.

Mot clés : réseau informatique, Virtual, privé, sécurité, réseau VoIP.

Abstract

The development of technology in general and computing in particular has generated a craze for the modernization of the processing of information systems.

These technologies have been able to develop thanks to the ever-increasing performance of local networks. But the success of these information systems has also revealed one of their pitfalls.

This study allowed us to better understand the problems related to local networks, including those relating to the deployment of a VPN network comprising several remote sites while guaranteeing a quality of service.

In addition, it allowed us to become more familiar with CISCO equipment.
Among other things, this study shows that there is agreement between the theoretical reflection carried out and the practical implementation of VPNs, an observation which in our view validates our project.

Since the appearance of computers in the 1950s, it has gradually established itself as an essential instrument in the professional world, becoming the essential tool for information management up to decision-making. of paramount importance for businesses.

And as all progress creates new challenges, over time another need arose, which was to have access at any time and from anywhere to the resources offered by computerized entities (business, household, administrations, etc.).) securely, hence the need for a VPN (Virtual Private Network).

VoIP in a multi-site IP SEC VPN environment is to apply the same treatment to voice as other types of data circulating on the Internet. Thanks to the IP protocol, data packets, consisting of digitized voice, are transported there. Indeed, by dint of transferring information files in more and more real time, Internet users came to transfer voice, in real time enough to compete on the telephone.

However, we admit that our theories and reflections, although empirical, are not indubitable and definitive truths.

They are likely to be refuted by more robust models or by divergent subsequent observations that would be linked to the evolution of technologies, which are themselves constantly changing. It is the nature of any intellectual proposition to expect to be obsolete one day or another.

But it can just as easily be reinforced later by other approaches and put in place.

*Keys words:*network, Virtual, private, security, Voice over Internet Protocol.

ملخـــص

أدى تطور التكنولوجيا بشكل عام والحوسبة بشكل خاص إلى نشوء جنون لتحديث معالجة أنظمة المعلومات.

تمكنت هذه التقنيات من التطور بفضل الأداء المتزايد باستمرار للشبكات المحلية. لكن نجاح أنظمة المعلومات هذه كشف أيضًا عن أحد مآزقها.

سمحت لنا هذه الدراسة بفهم المشكلات المتعلقة بالشبكات المحلية بشكل أفضل ، بما في ذلك تلك المتعلقة بنشر شبكة VPN تضم العديد من المواقع البعيدة مع ضمان جودة الخدمة.

بالإضافة إلى ذلك ، فقد سمح لنا بالتعرف أكثر على معدات CISCO.

من بين أشياء أخرى ، تُظهر هذه الدراسة أن هناك اتفاقًا بين التفكير النظري المنفذ والتطبيق العملي لشبكات VPN ، وهي ملاحظة تؤكد مشروعنا في رأينا.

منذ ظهور أجهزة الكمبيوتر في الخمسينيات من القرن الماضي ، رسخت نفسها تدريجيًا كأداة أساسية في العالم المهني ، وأصبحت الأداة الأساسية لإدارة المعلومات حتى اتخاذ القرار.

وبما أن كل التقدم يخلق تحديات جديدة ، فقد نشأت مع مرور الوقت حاجة أخرى ، وهي الوصول في أي وقت ومن أي مكان إلى الموارد التي تقدمها الكيانات المحوسبة (الأعمال ، والأسرة ، والإدارات ، وما إلى ذلك) بطريقة آمنة ، ومن ثم الحاجة إلى) VPN شبكة افتراضية خاصة.

VoIP في بيئة IP SEC VPN متعددة المواقع هو تطبيق نفس المعاملة على الصوت مثل الأنواع الأخرى من البيانات المتداولة على الإنترنت. بفضل بروتوكول IP ، يتم نقل حزم البيانات ، التي تتكون من صوت رقمي ، هناك. في الواقع ، من خلال نقل ملفات المعلومات في الوقت الحقيقي بشكل متزايد ، جاء مستخدمو الإنترنت لنقل الصوت ، في الوقت الحقيقي بما يكفي للتنافس على الهاتف.

ومع ذلك ، فإننا نعترف بأن نظرياتنا وانعكاساتنا ، على الرغم من كونها تجريبية ، ليست حقائق مؤكدة وغير قابلة للشك.

من المحتمل أن يتم دحضها من خلال نماذج أكثر قوة أو من خلال الملاحظات اللاحقة المتباينة التي قد تكون مرتبطة بتطور التقنيات ، والتي هي نفسها تتغير باستمرار. من طبيعة أي اقتراح فكري أن نتوقع أن يصبح عفا عليه الزمن في يوم أو آخر.

ولكن يمكن بسهولة تعزيزها لاحقًا من خلال مناهج أخرى وتطبيقها.

Liste des abréviations et Acronymes

ACL : Access Control List
ARP: AdressResolution Protocol
BID: BridgedIdentity.
ATM: Asynchronous Transfer Mode
BNC: Bayonet Neill–ConcelmanConnector
BPDU: Bridge Protocol Data Unit
CDM: Code Division Multiple.
CISCO: Société de matériel informatique
CLI: Command Line Interface.
DHCP: Dynamics Host Configuration Protocole.
EIGRP: Extended Interior Gateway Routing Protocol.
FC:FerruleConnector
FDDI: FiberDistributed Data Interface
FO: Fibre Optique**.**
HTTP: Hypertext Transfer Protocol.
HUB: Concentrateur réseau
IP: Internet Protocole.
ISO : Organisation Internationale de normalisation.
JPEG : Joint Photographic Experts Group.
LAN: Local Area Network.
LC: Lucent Connector
LLC:contrôle de liaison logique
MAC: Media Access Control
MAN: Metropolitan Area Network.
ISL: Inter-Switch Link
OSI: Open Systems Interconnections
OSPF : Open Shortest Path First. PC : Personel Computer.
PABX: PrivateAutomaticBrancheXchange
PAN: Personal Area Network
PDU : Protocol Data Unit
PING: Packet Internet Groper**.**
RFC : Request For Comments (Ensemble de documents qui font référence auprès de la communité internet).
RIP : Routing Information Protocol.
SNAP:protocole d'accès au sous-réseau
SC: Standard Connector
ST: Straight Tip
STB: Set-top box.
STP : Spanning-Tree Protocol
TCP: Transmission Control Protocol.
TRUNK:plate-forme de transport ferroviaire destiné pour les objets lourds ou encombrants.

UDP: User Detagram Protocol.
USB: Universal Serial Bus
UTP: UnshieldedTwisted Pair
VLAN:Réseau Local Virtuel**.**
VOIP: Voice over IP.
VTP:VLAN Trunking Protocol**.**
WAN: Wide Area Network
WIFI: Wireless Fadent (ensemble des protocoles de communication sans fil).
AES = Advanced Encryption Standard
ARP = AddressResolution Protocol
DHCP = Dynamic Host Configuration
DNS = Domain Name System
DoS = Deny of Service
Flooding = inondation
HMAC= Hash-based Message Authentication Code
IAX = Inter-AsteriskeXchange
IDS: Intrusion Detection System
IETF = Internet Engineering Task Force
IP = Internet Protocol
IPSec = Internet Protocol Security
IPS: Intrusion Detection System
LAN = Local Area Network
MD5 = Message Digest 5
MITM = Man In The Middle
NAT = Network Address Translation
PABX = PrivateAutomaticBranch
PSTN = Public SwitchedTelephone
RSA = Rivest Shamir Adleman
RTCP = Real-time Transport Control Protocol
RTP = Real-Time Transport Protocol
SHA= Secure Hash Algorithm
SIP = Session Initiation Protocol
SRTP = Secure Real-time Transport Protocol
SSL = Secure Socket Layer
TCP = Transport Control Protocol
TLS = Transport Layer Security
UDP = User Datagram Protocol
VLAN = Virtual LAN
VoIP = Voice over Internet Protocol
VPN = Virtual Private Network.
MCU = Multipoint Control Unit
SMTP = Simple Mail Transfer Protocol
PBX IP = Private Branch eXchange Internet Protocol
UIT= Union Internationale des Télécommunications

Sommaire

Chapitre I : Généralités sur les réseaux informatique

Chapitre II : les réseaux privés virtuels

Chapitre III : La voix IP VoIP Administration et sécurité

IV : Résultat du Simulation et Discussion.

Liste des figures :

Liste des tableaux :

1. Introduction générale

Depuis quelques années, la technologie VoIP commence à intéresser les entreprises, surtout celles de service comme les centres d'appels. La migration des entreprises vers ce genre de technologie n'est pas pour rien. Le but est principalement est de : minimiser le coût des communications ; utiliser le même réseau pour offrir des services de données, de voix, et d'images ; et simplifier les coûts de configuration et d'assistance.
Au vu de ces chiffres qui interpellent, il est d'autant plus important de penser à la sécurité des réseaux utilisant cette technologie .Plusieurs fournisseurs offrent certaines solutions qui permettent aux entreprises de migrer vers le monde IP. Des constructeurs tels que Nortel, Siemens, et Alcatel préfèrent la solution de l'intégration progressive de la VoIP en ajoutant des cartes extensions IP.Ledéveloppementdelatechnologieengénéraletdel'informatiqueenparticulierasuscité un engouement pour la modernisation du traitement des systèmes d'information.

Cette approche facilite l'adoption du téléphone IP surtout dans les grandes sociétés possédant une plateforme classique et voulant bénéficier de la voix sur IP. Mais elle ne permet pas de bénéficier de tous les services et la bonne intégration vers le monde des données.

L'objectif de la VoIP dans un environnement VPN IP SEC multi site est d'appliquer à la voix le même traitement que les autres types de données circulant sur Internet. Grâce au protocole IP, des paquets de données, constitués de la voix numérisée, y sont transportés. En effet, à force de transférer des fichiers d'information en temps de plus en plus réel, les utilisateurs d'Internet en vinrent à transférer de la voix, en temps suffisamment réel pour faire compétition au téléphone. Les principales caractéristiques de cette technologie sont ses protocoles de signalisation et de transport, les codes qu'ils utilisent ainsi que ses équipements particuliers.

Chapitre I

Généralité sur les réseaux informatiques

1. Introduction :

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et en fin des machines terminales, telles que des stations de travail ou des serveurs. Dans l'univers des télécommunications, nous allons nous occuper d'un espace bien définis, celui des communications numérique, c'est à dire des échanges d'informations déjà numérisées, soit d'origine digitale (données informatique), soit échantillonnées et quantifiées préalablement (par exemple un fichier d'une séquence vidéo compressée avant stockage).Dans cette catégorie d'échange se situent tous les transferts de données existant sous forme binaire ou octet

(généralement exprimer en base hexadécimal).

2. Définition de réseau informatique :

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux

Distants avec usité central puis des ordinateurs entre eux. Dans un premier temps ces

Communications étaient juste destinées aux transports de données informatiques alors
Qu'aujourd'hui onze dirige plutôt vers des réseaux qui intègrent à la fois des données
Mais en plus, la parole, et la vidéo. Les Réseaux informatiques sont les résultats de

Rapprochement de deux domaines : l'informatique et la **télécommunication**. En fait

La télécommunication recouvre toutes les techniques (filaires, radio, optiques, etc.)

De transfert d'information quelle qu'en soit la nature (symboles, écrits, images fixes

Ou animées, son **réseaux**, ou autres) [1].

3. Les types de réseaux d'informatiques :

On peut distinguer différent types de réseaux selon plusieurs critères tels que (la taille de réseau, sa vitesse de transfert des données et aussi leur étendue) :

3.1-Les réseaux personnels (PAN) : PAN (Personale Area Network ou Réseau personnel) : c'est un réseau informatique centré sur l'utilisateur. Il désigne l'interconnexion de plusieurs mètres autour de celui-ci. Dans ce type des réseaux, des liaisons sans fil sont souvent utilisées.

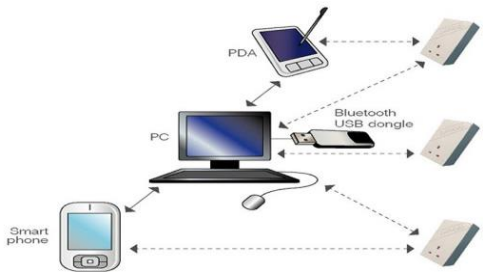


Figure **I.**01 : réseau PAN.

3.2-Les réseaux locaux (LAN) : LAN (Local Area Network ou réseau local): peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise. Les L'ans se distinguent des autres classes de réseaux par leur taille, leur technologie de transmission, leur vitesse de transmission et leur topologie. Ayant des débits de quelques Mb/s avec un support partagé.

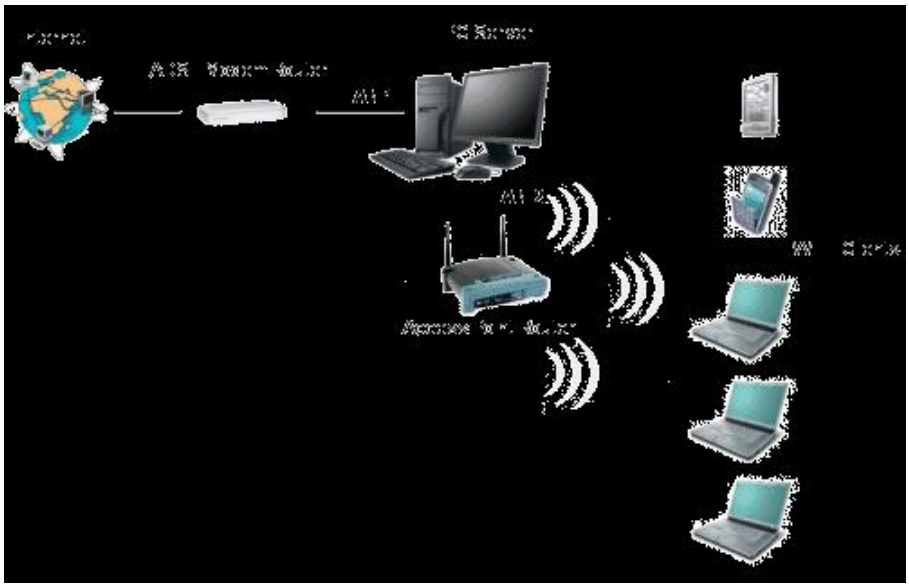


Figure **I.**02 : réseau LAN.

3.3-Les réseaux métropolitains (MAN) : d**a**mans **AN (Métropolitain Area Network ou réseau métropolitain) :** interconnecte plusieurs lieux situés une même vile, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local. Leur topologie ressemble à celle des années, mais ayant des normes différents de celles-ci. Leur débit peut être de quelques centaines de Kbits/s à quelques Mbits/s [1-2].

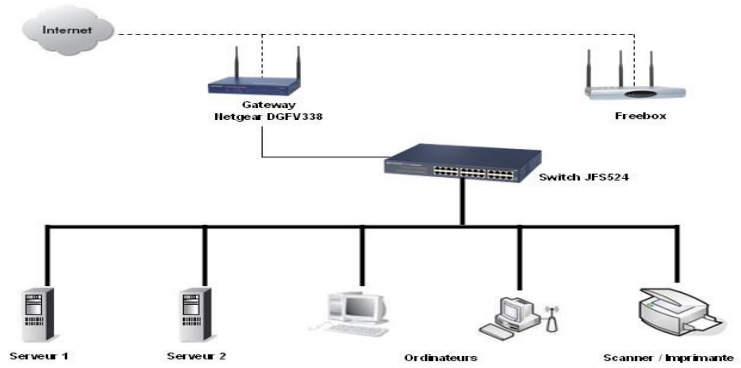


Figure **I.**03 : réseau MAN.

3.4-Les réseaux étendus (WAN) : WAN (Wilde Area Network ou réseau étendu): permet de communiquer à l'échelle d'un pays, ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications.

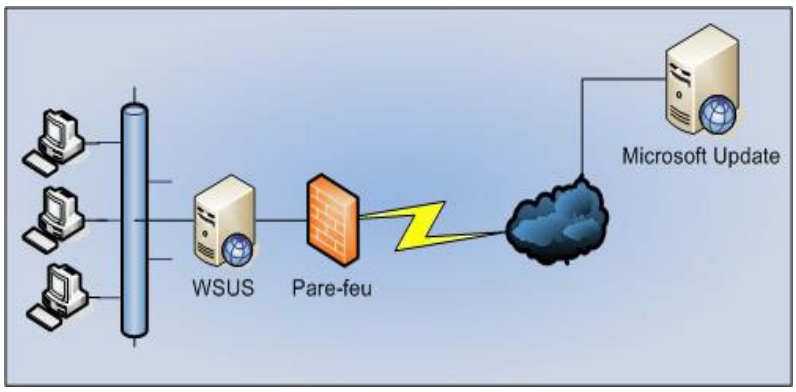


Figure **I.**04 : réseau WAN.

4. Les supports de connexion :

Il existe deux types de **supports** de communication : les câbles réseaux et les sans-fils. ... Ils parlent à la place de liaison guidée (avec fils) et non-guidée (sans fils). Dans les deux cas, le **support** de transmission va propager des ondes électromagnétiques, qui codent les informations transmises [3].

4.1-Définition des éléments du réseau informatique : Il existe essentiellement 4 éléments de mise en réseau informatique :

1. Ordinateurs :

Un ordinateur est un appareil numérique capable d'accepter des données en entrée,

Un processus de traitement des données à l'aide d'algorithmes et de structures de données prédéfinis, et d'effectuer des tâches en sortie qui comprend la transformation de données brutes en informations, puis en connaissances, et enfin un aperçu du domaine des données. La sortie prend également la forme de l'exécution de tâches physiques avec le stockage de données, la transformation de données et la récupération de données. Le réseau est également constitué d'ordinateurs à des fins d'échange de données et d'exploitation d'un modèle de programmation distribuée [3].

2. Support de transmission :

Le moyen par lequel nous envoyons nos données d'un endroit à un autre est appelé support de transmission.
Les signaux sont utilisés pour représenter les données par les ordinateurs et autres appareils de télécommunication. Les signaux (c'est-à-dire des données ou des informations) sont transmis sous forme d'énergie électromagnétique d'un appareil à un autre. Ces signaux voyagent à travers le vide, l'air ou d'autres supports de transmission pour se déplacer d'un point à un autre (de l'émetteur).

3. Protocoles :

il existe des règles et des conventions définies pour la communication entre les périphériques réseau.
Ceux-ci sont appelés protocoles. Les protocoles réseau incluent des mécanismes permettant aux appareils d'identifier et d'établir des connexions les uns avec les autres, ainsi que des règles de formatage qui spécifient comment les données sont conditionnées dans les messages envoyés et reçus.

4.2. A-Support d'interconnexion filaire : Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation comporte généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux.

4.2. A1-Câbles à paires métalliques ou torsadées : Le câble à paire torsadée est souvent utilisé pour les communications de téléphone et la plupart des réseaux Ethernet modernes. C'est une sorte de câblage dans lequel deux conducteurs d'un même circuit sont torsadés ensemble. Une paire de fils forme un circuit capable de transmettre des données. Et les paires sont torsadées ensemble pour fournir une protection contre la diaphonie, le bruit généré par les paires adjacentes.

Figure **I.**05 : câble à paire métallique ou torsadée.

4.2.A2-Câbles coaxiaux : Les câbles coaxiaux sont généralement constitués d'un conducteur central (âme), d'une enveloppe isolante (diélectrique) et d'un conducteur extérieur (tresse, ruban ou tube), le rapport des diamètres des conducteurs (central et extérieur) étant constant afin de garantir une impédance caractéristique constante tout au long du câble. Il existe dans l'industrie électronique une très grande variété de câbles coaxiaux souples ou semi-rigides et la plupart font l'objet de spécifications nationales ou internationales.

4.2. A3-La fibre optique : Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété d'être un conducteur de la lumière et sert dans la transmission de données et de lumière. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et peuvent servir de support à un réseau « large bande » par lequel transitent aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques [4].

Figure **I.***06 : La Fibre Optique.*

4.2. B- Les Connecteurs : Servent à relier entre elles toutes les parties d'un même réseau physique, généralement tous les ordinateurs sont reliés à un Hub, sauf dans le cas d'un câblage coaxial où le Hub est inutile. Lorsqu'une information arrive sur un Hub, elle est rediffusée vers toutes les destinations possibles à partir de celui-ci, c'est à dire vers toutes ses prises [3-4].

Figure **I.**07 : connecteur Hub

4.2. B1-Connecteur RJ45: Un connecteur RJ45 est une interface physique souvent utilisée pour terminer les câbles de type paire torsadée. Il est souvent utilisé avec des standards comme le TIA/EIA-568-B qui décrit le brochage de terminaison du câblage [4].

Figure **I.**08 : connecteur RJ45

4.2. B2-connecteurs optiques : Le connecteur optique ou connecteur optique permet d'aligner et de coupler les fibres optiques pour que la lumière puisse être transmise.

Le connecteur doit être soigneusement aligne à la fibre de verre afin que la lumière émise par la câble optique soit le moins possible interrompue.

4.2. B3-Connecteurs BNC :

Est un connecteur électrique utilisé en terminaison de câble coaxial, en particulier dans le domaine radio –fréquence .Simple d'utilisation et rapide à fixer, il s'agit d'un connecteur tubulaire portant, sur sa partie femelle, deux petites broches baïonnette diamétralement opposées qui s'encastrent dans des encoches situées sur le connecteur mâle. La fixation est assurée en effectuant un quart de tour à la bague qui enserre le connecteur.

Figure **I.**09 : Connecteurs BNC.

5. Définition de topologie :

Une topologie désigne la manière dont les équipements d'un réseau sont organisés. En effet, il convient de distinguer deux classes de topologies : la *topologie logique* de la *topologie physique.* Dans la topologie logique on considère le parcours de l'information entre les différents éléments de réseau. Les aspects de partage de support et les méthodes d'accès à ce dernier sont des éléments essentiels dans ce type de topologie.

5.1- Topologie en bus :

Dans ce type des réseaux les différentes stations sont reliées à travers le même câble par le biais des connecteurs spécialisés. A toutes les extrémités du câble est fixé un bouchon (un terminateur) qui empêche le signal de se réfléchir. Parce que là été câble partagé par toutes les stations, on ne trouve qu'une seule qui transmettre des données dans une instant donnée. Les réseaux en bus sont simples, peu coûteux, facile à mettre en place et à maintenir. Si une machine tombe en panne sur un réseau en bus, alors le réseau fonctionne toujours, mais si le câble est défectueux alors le réseau tout entier ne fonctionne plus. L'augmentation de nombre des stations connectées au réseau dégrade les performances de ce dernier [5].

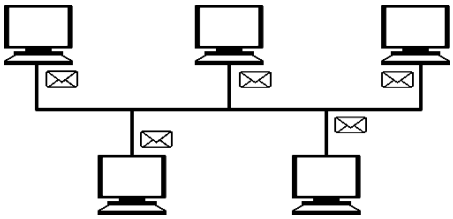


Figure **I.**10 : topologie en BUS

5.2-Topologie en étoile : dans ce type plusieurs câbles sont axés auteur d'un nœud central. Les réseaux en étoile sont simples à administrer parce que la gestion des ressources est centralisée. En plus, les réseaux en étoile fonctionnent toujours, même si une station tombe en panne ou une liaison est coupée, tant que le nœud central est fonctionnel. Si le nœud central tombe en panne, le réseau entier devient hors service. Sur le plan économique, les réseaux en étoile sont coûteux surtout pour les réseaux WAN. On distingue deux types de nœud centraux : les hubs et le Switch .Le fonctionnement de hub consiste à faire la diffusion de l'information sur tous ses ports. Par contre, le Switch assure la fonction de commutation (c'est-à-dire il envoie l'information seulement sur le port concerné).

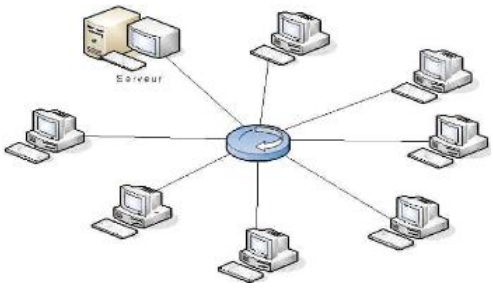


Figure **I.**11 : topologie en étoile

5.3-Topologie en anneau : Il s'agit de la topologie en bus que l'on a refermé sur elle- même. Le sens de parcours du réseau est déterminé- ce qui évite les conflits. Dans ce type, la collision est évitée par une gestion basée sur le droit d'accès au support. En général, l'anneau se trouve à l'intérieur d'un boîtier qui s'appelle un **MAU** (Multi station Access Unit). Toutes les stations sont reliées au **MAU**. Le temps d'accès est déterminé (une machine sait à quel moment elle va pouvoir envoyer des informations). Pour éviter la panne du réseau en cas de destruction de câble, une autre boucle de secours est ajoutée dans la topologie anneaux doubles.

Figure **I.**12 : topologie en anneau

5.4-Topologie en arbre : Aussi connu sous le nom de *topologie hiérarchique*, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre [5].

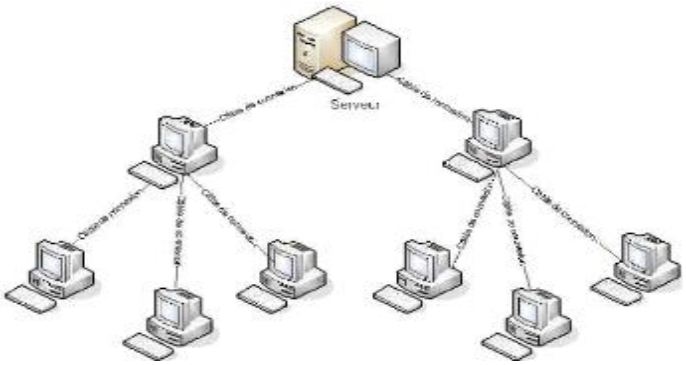


Figure **I.**13 : topologie en arbre.

5.5-Topologie en maillée : ce réseau est constitué d'un ensemble de stations reliées par des voies. Selon le nombre des relations établies on distingue des réseaux maillés complètement et des réseaux maillés irrigueraient.

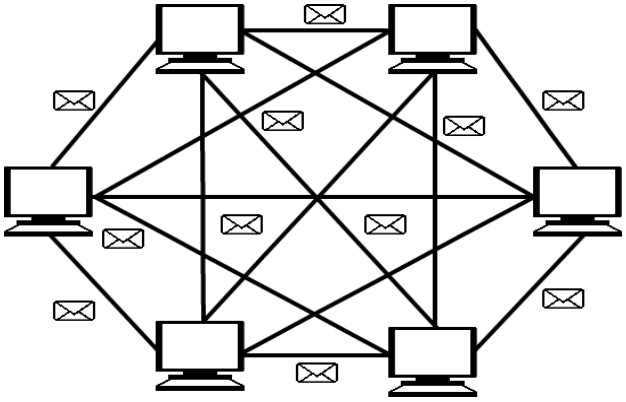


Figure **I.**14 : topologie en maillée

6. Le mode OSI :

Pour faire circuler l'information sur un réseau on peut utiliser principalement deux stratégies. L'information est envoyée de façon complète. L'information est fragmentée en petits morceaux (paquets), chaque paquet est envoyé séparément sur le réseau, les paquets sont ensuite réassemblés sur la machine destinataire. Dans la seconde stratégie on parle réseau à commutations de paquets. La première stratégie n'est pas utilisée car les risques d'erreurs et les problèmes sous-jacents sont trop complexes à résoudre. Le modèle OSI est un modèle à 7 couches qui décrit le fonctionnement d'un réseau à commutations de paquets. Chacune des couches de ce modèle représente une catégorie de problème que l'on rencontre dans un réseau.

Découper les problèmes en couche présente des couches. L'utilisation de couches permet également de changer de solution technique pour une couche sans pour autant être obligé de tout repenser. Le premier objectif de la norme OSI a été de définir un modèle de toute architecture de réseau basé sur un découpage en sept couches, chacune de ces couches d'un réseau. Les couches 1, 2, 3 sont dites basses (ou couches orientées transmission) et les couches 5, 6 et 7 sont dites hautes (couches orientées traitement).

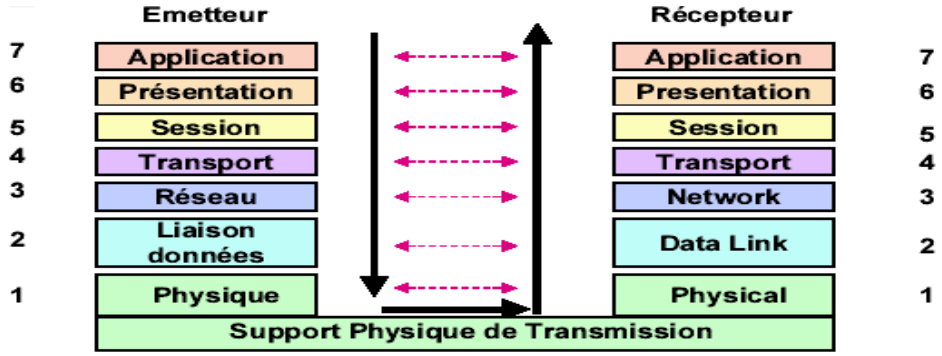


Figure **I.**15 : les couches de modèle OSI [5]

6.1. a-Couche physique :

Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédure les nécessaires à l'activation et à la désactivation des connexions physiques destinées à la Transmission de bits entres deux entités de la couche liaisons de données. Transmet les bits sur un support physique. À cet effet, elle définit les supports et les moyens d'y accéder

6.1. b-Couche liaison :

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à L'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de donnes entre les entités du réseau.
Cette couche détecte et corrige, quand cela est possible, les erreurs de la coche physique et Signale à la couche réseau les erreurs irrécupérables. Dans cette couche on cherche à savoir comment deux stations sur le même support physique (cf. Couche 1) vont être identifiées. Pour ce faire, on peut par exemple assigner à chaque station une adresse (cas des réseaux Ethernet,....).

6.1. c-Couche réseau :

Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c'est-à-dire l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

Le rôle de cette couche est de trouver un chemin pour acheminer un paquet entre 2 machines qui ne sont pas sur le même support physique

VIII- 6.1 Couche transport :

Cette douche définit un transfert de données entre les entités en les déchargeant des détails d'exécution (contrôle entre l'OSI et le support de transmission).
Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre Coût les performances requise par la couche session.
La couche transport doit normalement permettre à la machine source de communiquer directement avec la machine destinatrice. On parle de communication de bout en bout (end to end).

6.1. e-Couche session :

Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de Synchroniser les dialogues et les échanges de données.
Il s'agit de la gestion d'accès, de sécurité et d'identification des services. Cette couche a pour rôle de transmettre cette fois les informations de programmes à programmes.

6.1. f-Couche présentation :

Cette couche assure la transparence du format des données à la couche application.

A ce niveau on doit se préoccuper de la manière dont les données sont échangées entre les Applications.

6.1. g-Couche application :

Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tous les services directement utilisables par l'application (transfert e données, allocation De ressources, intégrité et cohérence des informations, synchronisation des applications).
Dans la couche 7 on trouve normalement les applications qui communiquent ensemble. (Courrier électronique, transfert de fichiers,...)

6.2-Définition de base :

Une base de données est un système de stockage ordonné d'informations, généralement géré par ordinateur et exploité à l'aide du langage de requêtes SQL

Une base de faits est la mémoire dynamique d'un système expert, généralement organisée de manière et telle qu'une base de données

Une base de connaissances est le cœur d'un système expert contenant les connaissances d'une application experte, généralement exploitées à l'aide d'un moteur d'inférence

7. Mode TCP/IP :

7.1-Introduction :

TCP/IP est actuellement le protocole de communication le plus utilisé dans les réseaux locaux. C'est aussi le protocole de transport utilisé par le réseau Internet
Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches

7.2. A-Couche réseau :

Assure la transmission d'un datagramme venant de la couche IP en l'encapsulant dans une trame physique et en transmettant cette dernière sur un Réseau physique. Des réseaux peuvent être locaux : les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard (Répéteur, routeur …etc.) Fit à réaliser physiquement la liaison L'interconnexion peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces Réseaux par une liaison téléphonique (modems, etc..).

7.2. B-Couche internet :

Encapsule les paquets reçus de la couche Transport dans des data grammes .IP Mode non connecté et non fiable.

7.2. C-Couche transport :

Chargé de fournir un moyen de communication de bout en bout Entre 2 programmes d'application. Agi en mode connecté et en mode non connecté. Elle
Divise le flux de données venant des applications en paquets, transmis avec l'adresse Destination IP au niveau IP.

7.2. D-Couche application :

Les applications interagissent avec les protocoles de la couche
Transport pour envoyer ou recevoir des données.

8. Réseaux sans fil :

8.1-Introduction :

Est un réseau informatique numérique qui connecte différents postes ou systèmes entre eux par ondes radio. Il peut être associé à un réseau de télécommunications pour réaliser des interconnexions à distance entre nœuds.

Les réseaux sans fil constituent une alternative aux réseaux câblés. Leur compatibilité avec les réseaux câblés permet également de les y ajouter comme extensions.

La norme la plus utilisée actuellement pour les réseaux sans fil est la norme IEEE 802.11, plus connue sous le nom de Wi Fi tant donné la faible puissance d'émission des solutions matérielles actuelles

Le rayonnement géographique des ondes est relativement limité é. Pour cette raison, les réseaux sans fil se sont avant tout développés comme réseaux internes, propres à un bâtiment, soit comme réseau d'entreprise, soit comme réseau domestique.

8.2-Classification des réseaux sans fil :

Plusieurs critères peuvent être utilisés pour la classification des réseaux comme : la taille, la topologie ou la technique de transmission [5-6].

8.2.1-Les réseaux WPAN :

(Personale *Area Network,* **PAN**) désigne un type de réseau informatique restreint en matière d'équipements, généralement mis en œuvre dans un espace d'une dizaine de mètres. D'autres appellations pour ce type de réseau sont : réseau domestique ou réseau individuel.

L'idée est d'envoyer des informations entre des périphériques proches. Au lieu de les envoyer via un LAN ou un WLAN nécessitant une infrastructure, une nouvelle classification, PAN est créée. PAN est généralement utilisé pour créer un réseau d'appareils personnels, comme un ordinateur portable

8.2.2-Les réseaux WLAN :

(*Local Area Network* en français ***Réseau Local*)**
Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).
La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s (pour un réseau Ethernet par exemple) et 1 G bit/s (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs

8.2.3-Les réseaux WMAN :

(Métropolitain Area Network**)** Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de Km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer Comme si ils faisaient partie d'un même réseau local. Un

MAN est formée de commutateurs ou des routeurs interconnectés par des liens hauts débits (en général en fibre optique).

8.2.4-Les réseaux WWAN :

(Wide Area Network)

Interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui Augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau.

Le plus connu des WAN est Internet [6].

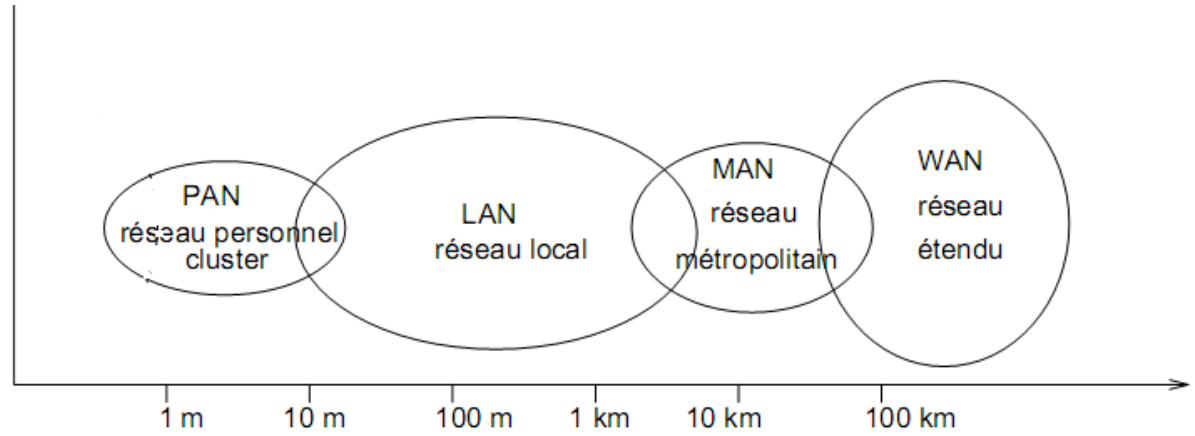


Figure **I.**16 : classification des réseaux sans fil.

9. Conclusion :

Pour satisfaire notre besoin dans un réseau il faut tout d'abord bien choisir : une topologie Adéquat, un bon système de câblage, les meilleur techniques de transmission et de Commutation et sans oublié de choisir une architecture conforme aux organismes de normalisation pour les réseaux.
D'autre part, la reconnaissance des flux aide à l'introduction de nouvelles fonctions, on remarque que les besoins sont croissants en matière de communication qui converge de plus en plus vers le multimédia (voix, son, image, vidéo) ne seront supportés par les réseaux que si ces derniers évoluent vers les hauts débits alliant performance, qualité de service, rapidité.

Chapitre II

Les réseaux privés virtuels VPN(Virtual Private Network)

1. Introduction :

En raison des terribles développements qui se produisent dans le monde de la technologie, en particulier dans les réseaux informatiques, Les techniques VPN sont utilisées depuis longtemps par les opérateurs télécoms. Depuis quelques années, des protocoles tels qu'IP Sec permettent de créer des VPN en utilisant Internet. Cette utilisation peut concerner les employés nomades d'une entreprise mais aussi les utilisateurs d'un site ayant accès aux ressources d'un autre site. Par exemple, un siège et ses filiales.

Quelques soient les choix techniques effectués, l'objectif est de fournir aux Utilisateurs des conditions d'utilisation identiques à un réseau privé (intranet), à travers le réseau public (Internet). L'utilisateur doit pouvoir effectuer les mêmes opérations que s'il était physiquement sur le réseau de l'entreprise.

2. Réseau Transpac :

2.1-Définition de Réseau Transpac : Transpac était une filiale de l'opérateur public de télécommunications France, Transpac est le Premier réseau[1] commercial de transmission de données par paquets en France. Son nom est d'ailleurs tiré des premières syllabes de « transmission par paquets ».

Elle détenait le monopole commercial pour la fourniture d'accès X.25 (protocole de communication normalisé par commutation de paquets).

TRANSPAC était destiné à écouler une forte proportion du trafic téléinformatique de l'époque avec les principales caractéristiques suivantes :

- un temps moyen de traversée du réseau de 0,2 seconde ;
- une disponibilité élevée ;
- des vitesses de raccordement s'échelonnant entre 50 bits/seconde (terminaux télex) à 64 kilobits/seconde (gros ordinateurs);
- déploiement sur l'ensemble du territoire avec une douzaine de Commutateurs, 30 points de raccordement pour 10.000 terminaux asynchrones [7].

2.2-Historique de Réseau Transpac : L'objectif de Transpac était de répondre aux besoins nouveaux qui découlaient de l'utilisation de matériels informatiques variés.

A l'origine, le réseau possédait 4 commutateurs, en 1985 il en comportait plus de 25.En 1993 le réseau compte plus 150 commutateurs. Les commutateurs de Transpac sont reliés entre eux par des liaisons spécialisées louées à France-Télécom. Le service de Transpac permet de rationaliser l'usage (par multiplexage statistique) de ces liaisons permanentes pour des usagers qui réalisent des communications de courte durée. L'une des originalités de ce réseau de commutation de paquets est d'offrir aux abonnés une tarification indépendante de la distance entre les équipements, mais uniquement fonction du temps de connexion et de la quantité de données transportées.

Transpac proposa à partir du printemps 1994 une ligne de produits de connexion à Internet essentiellement centrée autour d'X.25. Ce réseau commuté a subi la concurrence de protocoles permettant des vitesses de transferts supérieures, surtout celle d'Internet et de l'IP (Internet Protocole) moins coûteux à mettre en œuvre, échappant à la notion de monopole et donc L'activité de Transpac a alors évolué à la fin des années 1990 vers la fourniture de réseaux IP, mais également vers les offres d'hébergement et de fourniture de services. Cette filiale a fusionné avec France Télécom le 1er janvier 2006. Après le 1er juin 2006, les offres commerciales de Transpac ont été exploitées par Orange Business Services.

Orange Business Services a assuré la commercialisation et la maintenance du réseau X.25 jusqu'en juin 2012, date de fin d'exploitation technique et commerciale. Cette fermeture a entrainé l'arrêt des services Minitel qui s'appuyaient sur ce réseau Transpac a rapidement connu une forte croissance : ouvert en 1978 avec 1500 accès directs possibles, il atteint 5.300 accès effectifs en 1981, puis 10.000 en 1983, 21.500 en 1984 (une

Administrations, et 13 % dans les banques et la finance. Dans le secteur bancaire, Transpac a été utilisé entre les distributeurs automatiques des billets et leurs serveurs par des liaisons permanentes. Il a aussi été le *rése*au via lequel les lecteurs de cartes bancaires des commerçants, qui y accédaient au réseau par des communications téléphoniques locales, consultaient les serveurs des. Sollicitées. Au mondial, la société Swift, qui gérait les échanges interbancaires [7].

2.3-Architecture de Réseau Transpac : Seuls les trois premiers niveaux du modèle OSI de l'ISO sont implantés dans Transpac :
Le niveau 3 (couche réseau) offre à l'usager un service de transmission de données sur connexion, appelé X25. Les informations circulant à ce niveau s'appellent des paquets, N PDU.
Le niveau 2 (couche liaison) assure la transmission des données par blocs, L SDU sans erreurs. Les informations circulant à ce niveau s'appellent des trames, L PDU. Ce niveau gère le protocole de transmission entre les deux entités (gestion des ressources, traitement des erreurs) et s'occupe de l'enveloppe des trames pour leur délimitation dans le flot continu de données. Le protocole utilisé, appelé LAP B (Link Access Protocol version B), est un protocole de transfert de données sur connexion. Transpac utilise diverses versions de protocoles (LAP D...). Néanmoins le segment terminal d'accès usager utilise toujours le protocole LAP B.
Le niveau 1 (couche physique) permet le transport des informations élémentaires (bits) à un rythme fixe (vitesse de la liaison). Il utilise un format de trame, MA PDU, connu sous le nom de HDLC (High Lève Data Link Control). La couche physique est mise en œuvre sur les liaisons spécialisées.

2.4 -Avantages et inconvénients de réseau Transpac [8]:

2.4.1. Les Avantages :

Les avantages de réseau Transpac, on trouve :

- Couverture du territoire.
- Connexion de matériels hétérogènes.
- La sécurité et la fiabilité sont garanties par la société Transpac.
- Services complémentaires (Groupe fermé d'abonnés, Doublement de lignes) qui augmente la sécurité.

2.4.2. Les inconvénients :

Les inconvénients de réseau Transpac, on trouve :

- Adaptation aux nouvelles technologies.
- Dépenses supplémentaires.
- Configuration plus longue.

3. Définition de réseau privé virtuel :

Un **réseau privé virtuel** (*Virtual Privat Network* en anglais, abrégé en *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». La technique consiste à utiliser Internet comme support de transmission en utilisant un protocole de tunnel (en anglais *tunneling*), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de VPN pour désigner le réseau ainsi artificiellement créé. Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent accéder aux données en clair.

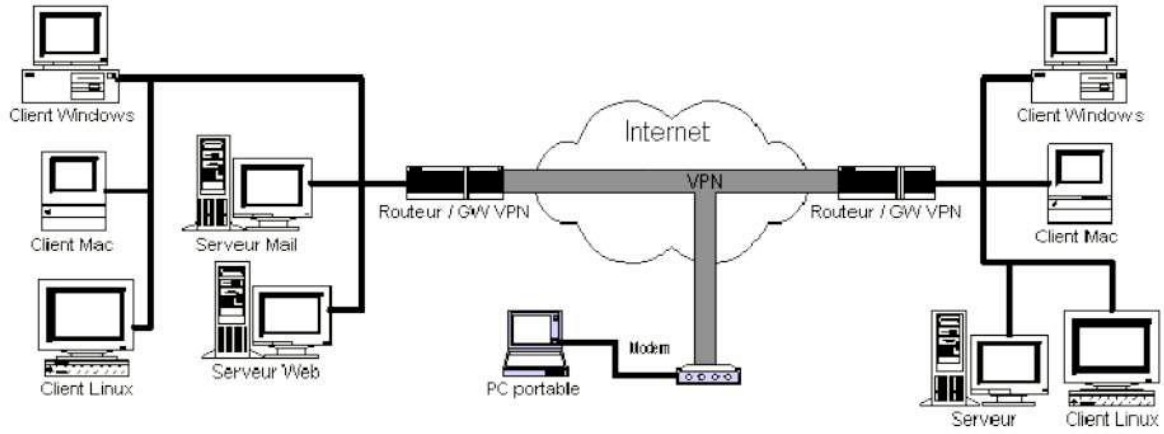


Figure II. 1: Exemple de VPN**.**

3.1 Le fonctionnement du VPN :

Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. La source
Peut ensuite éventuellement chiffrer les données (on parle alors de VPN chiffrés) et les Achemine en empruntant ce chemin virtuel.
Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le Protocole de tunneling encapsule les données en rajoutant une entête. Permettant le Routage des trames dans le tunnel. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulations.
La technique consiste à utiliser Internet comme support de transmission en utilisant un protocole de « tunnel » (en anglais *tunneling*), c'es**t**-à-dire encapsulant les données à transmettre de façon Chiffrée. On parle alors de VPN pour désigner le réseau ainsi artificiellement créé. Les données vont transiter via un serveur VPN (ou serveur d'accès distant) qui va interroger les pages demandées pour nous renvoyer le résultat crypté. Le client VPN installé sur l'ordinateur va lui décrypter ces informations. Plusieurs protocoles d'encapsulation peuvent être utilisés : L2F, PPTP, L2TP, IP Sec, SSL... Il est important de souligner que le VPN n'est pas un réseau physique en lui-même mais passe par le réseau Internet classique en Créant un **« tunnel** [4]**»** sécurisé à l'intérieur [9] .

Le VPN nécessite un serveur qui fonctionne comme une liaison entre les PC, ce serveur VPN peut être un ordinateur avec une application de serveur VPN ou un routeur, Pour démarrer une connexion, l'ordinateur avec l'application client VPN contacte le serveur VPN, le serveur VPN vérifie ensuite le nom d'utilisateur et le mot de passe et en cas de succès, le serveur VPN fournit une nouvelle adresse IP sur l'ordinateur client, puis une connexion / tunnel sera formé. Désormais, les ordinateurs clients peuvent être utilisés pour accéder à diverses ressources (ordinateurs ou LAN) qui se trouvent derrière le serveur VPN, par exemple, transférer des données, imprimer des documents, naviguer avec la passerelle fournie par le serveur VPN, faire un bureau à distance, etc.

3.2 Les principaux protocoles de VPN :

Voici une brève description des protocoles les plus communément utilisés dans le cadre de VPN qu'ils soient d'entreprise ou d'opérateur.
Un VPN sécurise la connexion Internet en se connectant à un serveur distant avant toute ouverture de site Web. La connexion à ce serveur est également cryptée, ce qui signifie qu'aucune de requêtes Web ne peut être vue par le monde extérieur. Le type et le niveau de cryptage sont déterminés par le protocole de sécurité. Selon le protocole utilisé, on se connecte au VPN via différents ports et avec différents niveaux de sécurité. Bien que le type de cryptage soit la principale différence entre les protocoles. Les principaux protocoles de tunneling VPN sont les suivants :

3.2.1. Open VPN : développée par James Yonan en 13 mai 2001, est un protocole populaire à utiliser car il est open source et gratuit. Open VPN est un protocole relativement nouveau et très configurable. La version utilisée par Express VPN supporte les ports UDP et TCP.
Il utilise la bibliothèque Open SSL, ce qui signifie qu'il a accès à tous les algorithmes de chiffrement qui s'y trouvent. Il utilise également un protocole de sécurité personnalisé basé sur SSL/TLS qui fournit un cryptage allant jusqu'à 256 bits. Mais supporté par tous les appareils [9].

3.2.2-PPTP (Point to Point Tunneling Protocol): Ce protocole fortement soutenu par Microsoft est très simple mais assez limité. Il est en fort déclin maintenant selon Jean-Paul ARCHIER l'auteur du livre « les VPN fonctionnement, mise en œuvre et maintenance des Réseaux Privé Virtuels ».

En Principe, il permet de créer des trames sous le protocole PPP et les encapsuler dans un datagramme IP.

Est un protocole de niveau 2 développe par Microsoft, 3Com, ASC end, US Robotiques et ECI Télématiques. Qui opère sur le port 1723 de TCP, est l'un des plus anciens protocoles VPN toujours en utilisation. Il est supporté sur des appareils anciens et plus rapide mais moins sécurisé. Il permettre d'acheminer des protocoles non Internet (NetBIOS, IPX, Appletalk…) sur un réseau Internet. Le meilleur cas d'utilisation pour PPTP est
L'accès externe au réseau interne d'un bâtiment d'entreprise, c'est pourquoi les VPN ont été développés en premier lieu. PPTP ne spécifie pas le cryptage. Il s'appuie plutôt sur le protocole point à point pour mettre en œuvre les fonctions de sécurité.

3.2.3-L2F (Layer 2 For wading) : Cisco a développé ce protocole autour des années 1996.L'IETF a en fait un standard en 1998 avec le RFC 2341.Son fonctionnement est assez voisin de PPTP.

3.2.4-L2TP (Layer 2 Tunneling Protocol) : Dérivé de PPTP et de L2F ce protocole est maintenant un des protocoles VPN implantés nativement sur les machines Windows, ce qui explique son succès. a été proposé pour la première fois en 1999 comme amélioration à la fois de L2F et de PPTP Sachant que L2TP ne permet pas un chiffrement ou un système d'identification robuste. Parfois bloqué par des pare-feu mais Plus sécurisé que PPTP. IL permet au trafic IP, IPX ou N

et BEUI d'être encrypté et ensuite d'être envoyé à travers n'importe quel type de média qui supporte la livraison de datagramme point à point, comme IP, X.25, Frame Relay ou ATM.

3.2.5-IP Sec : Est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il est très flexible pour une sécurité complète qui authentifie et chiffre chaque paquet individuel d'IP dans une communication donnée. Les applications d'IP sec sont multiples dans la couche Internet de la suite de protocoles Internet [10].

3.2.6-SSL : (Secure Socket Layer) est un protocole de niveau 4 utilise par une application Pour établir un canal de communication sécurise avec une autre application. Il permet de l'authentification du serveur et du client et de chiffrement des données.

3.3-Comparaisons entre les protocoles VPN :

Protocole	Avantages	Inconvénients
Open VPN	-bien sécurisé. -permet d'éviter les pare-feu. -utiliser un large choix d'algorithmes de chiffrement.	-complexe à mettre en place. - supportée par certains appareils mobiles.
PPTP	- très simple à utiliser et à mettre en place. - système rapide. - ne nécessite pas l'installation	- mal sécurisée.
L2TP/IP sec	- offre une bonne protection. - intégré dans les principaux OS.	- une propriété de Microsoft.

Tableau II.1 : avantages et inconvénients des protocoles VPN.

3.4-Motivations pour le choix d'une solution VPN :

Dans cet environnement, il est financièrement préférable de combiner un certain nombre de communications secrètes sur une plateforme de communication de grande capacité, permettant aux prix des composants d'être éteints par un grand nombre de clients, plutôt que d'utiliser une ligne dédiée. Pour chaque appel. Par conséquent, un groupe de VPN mis en œuvre sur un support physique partagé est moins cher qu'un ensemble équivalent de petits supports séparés, chacun connecté à un client réseau. La principale motivation pour choisir une solution VPN couvre les aspects économiques des communications. Les systèmes de communication d'aujourd'hui ont l'avantage d'avoir un prix Fixe et élevé avec de petits coûts variables qui changent en fonction de la capacité de transport ou de la bande passante du système.

3.5-Types de VPN :

Suivant les besoins, on référence 03 types de VPN :

3.5. A- Le VPN d'accès (poste à site) : Un utilisateur distant a simplement besoin d'un client VPN installé sur son PC pour se connecter au site de l'entreprise via sa connexion Internet. Le développement de l'ADSL favorise ce genre d'utilisation [11]..
Attention toutefois à interdire l'accès Internet depuis le poste « localement ». Pour une question de sécurité, la navigation devra se faire via le réseau de l'entreprise.
Ce point est important et rejoint la réflexion plus large de la sécurité des sites mis-en relation par un VPN. Lorsque les niveaux de sécurité sont différents, lorsque les deux sites sont reliés, le niveau de sécurité le plus bas est applicable aux deux. S'il existe une faille de sécurité sur un site (ou sur un poste nomade), celle-ci peut être exploitée.

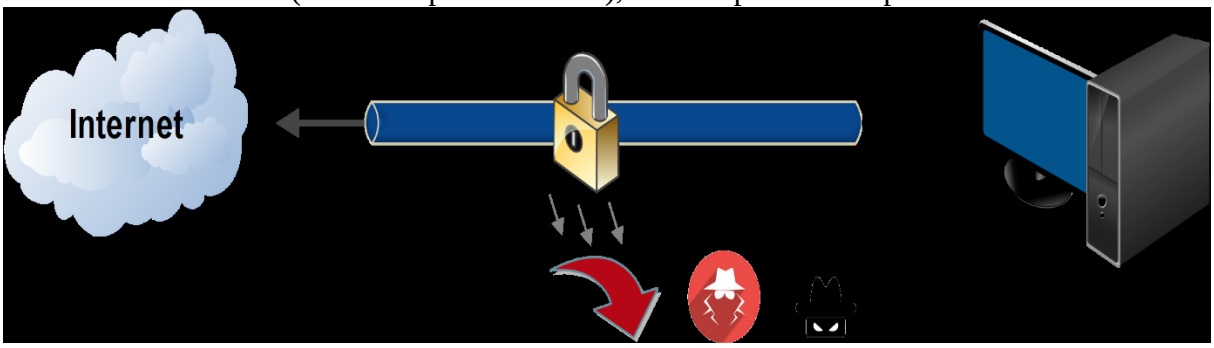


Figure **II.2**: Exemple d'un VPN poste à site

Avantages et inconvénients :

Parmi les avantages de cette solution, on trouve :

- ✓ L'accès du poste nomade (mobile) peut se faire de n'importe quel point de la planète doté d'un accès Internet.
- ✓ La transition des données entre le poste distant et le site central d'une façon sécurisée grâce à l'authentification.

Nous pouvons aussi trouver des inconvénients à cette configuration :

- ✓ Une installation logicielle est généralement nécessaire sur le poste distant.

- ✓ Le cryptage impose une charge non négligeable au poste distant, ce qui peut en dégrader les performances.
- ✓ Le cryptage n'est pas assuré au-delà du firewall du site central.

3.5. B-Site à site (LAN to LAN) : C'est un des cas les plus fréquents. Il s'agit de relier deux sites d'une même entreprise ou bien le site d'une entreprise et celui d'un fournisseur, ou d'un client. Il suffit que chaque site établisse une connexion locale sur le même réseau public, ce qui signifie des économies par rapport aux longues lignes louées privées.

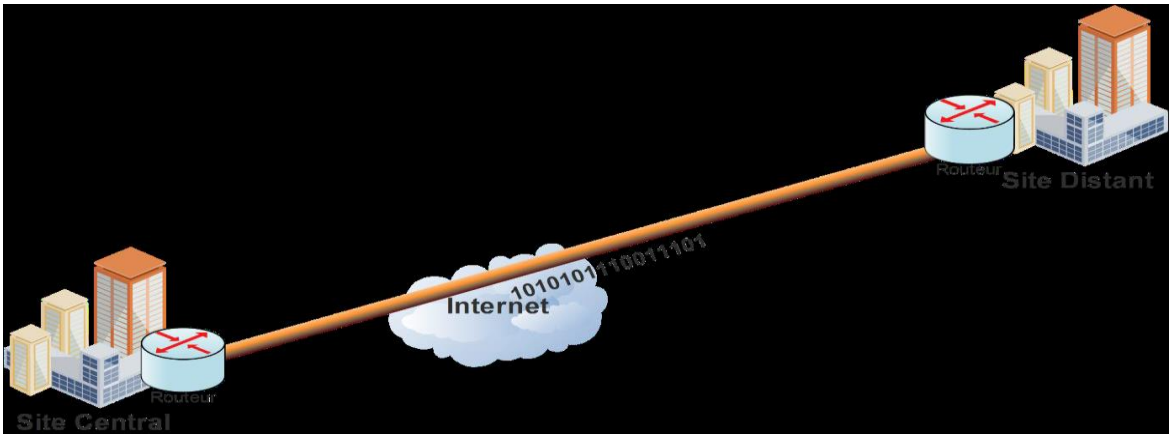


Figure **II.** 3: Exemple d'un VPN Site à site.

Généralement ce type de VPN est mis en place par l'interconnexion de deux éléments Matériels (routeurs ou pare-feu) situés à la frontière entre le réseau interne et le réseau publique de chaque site. Ce sont ces matériels qui prennent en charge le cryptage, l'authentification et le routage des paquets. Dans le cas de l'utilisation des matériels spécifiques, des processeurs spécialisés peuvent prendre en charge la partie cryptographique la plus consommatrice de ressources CPU [10-11].

Avantages et inconvénients :

Parmi les avantages procurés par cette configuration nous pouvons citer :

- ✓ Le cryptage est souvent pris en charge par des processeurs spécialisés, ce qui améliore notablement les performances.
- ✓ Une grande facilité pour le contrôle de trafic autorisé.
- ✓ Aucun impact sur les performances des poste puisque ceux-ci ne font pas de cryptage.
- ✓ La possibilité d'initier les VPN d'un côté ou de l'autre.

Mais cette solution présente aussi quelques inconvénients :

- ✓ Aucune protection de données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux firewalls.
- ✓ L'établissement des VPN nécessite que les deux extrémités soient bien identifiées soit par une adresse IP publique fixe, soit par un nom référencé dans des DNS officiels.

3.5. C-Poste à poste (Host to Host) : l'objectif est d'établir un canal sécurisé de bout en bout entre deux postes , ou plus couramment entre un poste et un serveur pour des raisons de confidentialité , On crée donc un VPN entre eux, et Toutes les données y transmises sont encryptées et compréhensibles que par les deux paires correspondantes. Le poste et le serveur peuvent être situés sur le même réseau ou sur deux réseaux différents reliés eux-mêmes par un VPN site à site.
Pour cette configuration, nous ne faisons intervenir que des composants logiciels : un logiciel client sur le poste « demandeur » et un logiciel utilisé en serveur sur le poste « destinataire ».

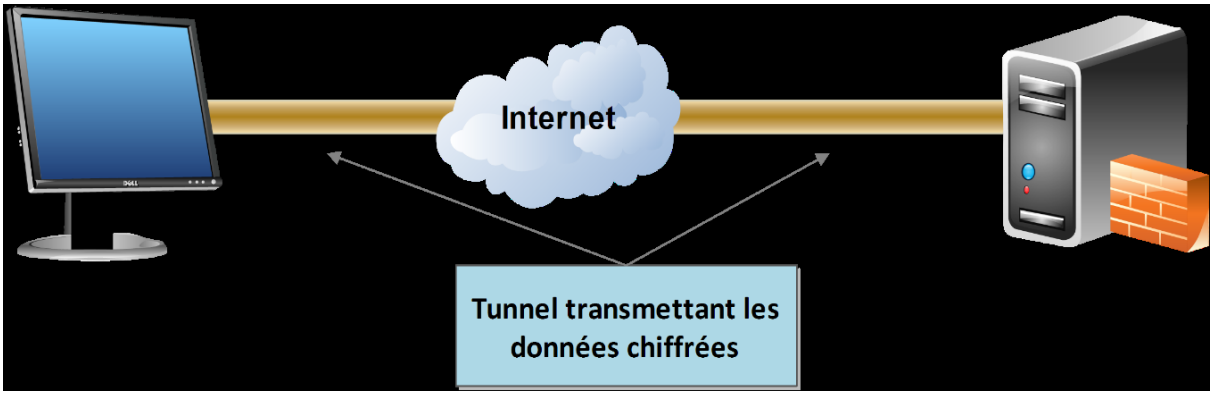


Figure **II.4** : Exemple d'un VPN poste à poste.

Avantages et inconvénients :

Le principal intérêt dans cette solution est que la conversation entre les deux postes est parfaitement protégée de bout en bout. C'est donc une très bonne option pour les communications les plus sensibles.
Par contre, elle présente de nombreux inconvénients

- ✓ le cryptage est uniquement logiciel d'où un possible impact sur les performances en cas de fort débit, notamment quand les deux extrémités sont sur le même réseau local.
- ✓ quand les postes se situent sur des locaux sépares par internet il est nécessaire que les deux extrémités puissent échanger leurs messages sur des protocoles et des ports qui doivent autorisés par les firewalls situés sur chaque site, cela nécessite également des
- ✓ translations d'adresses puisque les machines concernées sont rarement dotées d'adresses IP publiques et cela n'est pas sans poser quelques problèmes.
- ✓ Elle est inapplicable pour atteindre des matériels peu intelligents.

3.6-Les exigences de base de réseau privé virtuel [11] **:**
Pour garantir la confidentialité et l'intégrité des données lors de leur passage sur l'Internet, des mécanismes de sécurité et mesures.

Les mécanismes de sécurité les plus importants pour les réseaux privés virtuel sont les suivants **:**

- ✓ Authentification.
- ✓ mode d'encapsulation.
- ✓ chiffrement des données.
- ✓ intégrité des paquets.
- ✓ gestion des clés.
- ✓ la non-répudiation.
- ✓ support de protocole et applications.
- ✓ gestion des adresses.

3.6.1-Authentification *:* L'authentification est une procédure, par laquelle un système informatique certifie l'identité d'une personne ou d'un ordinateur. Le but de cette procédure étant autorisé la personne à accéder à certaines ressources sécurisées. Il va comparer les informations des utilisateurs autorisés stockées dans une base de données (en local ou sur un serveur d'authentification) à celles fournies. L'accès sera autorisé seulement si les informations sont identiques. C'est l'administrateur du système d'information qui octroie les droits et paramètre l'accès. L'utilisateur possédant un compte d'accès (identifiant + mot de passe) n'aura accès qu'aux ressources dont il est autorisé à voir.

3.6.2-Chiffrement des données : Le chiffrement est le processus de modification des données dans un format qui ne peut être lu que par le destinataire prévu. Pour lire le message, le destinataire doit avoir la bonne clé de déchiffrement. Le cryptage des données est utilisé pour résoudre les problèmes d'écoute. Le cryptage des données comprend principalement les données utilisateur et la valeur de la clé de décryptage et fonctionne grâce à un algorithme de cryptage comme DES, 3DES, AES, Blow Fish, RSA, IDEA, SEAL et RC4.

3.6.3-Intégrité d'un paquet : En raison de falsification possible des paquets ou d'usurpation, certaines implémentations VPN Utilisent l'authentification des paquets. SHA et MD5 sont deux des fonctions les plus courantes de hachage utilisées pour vérifier l'intégrité des paquets.

3.6.4-Gestion des clés : Pour utiliser le cryptage, la solution VPN doit fournir un certain type de mécanisme de cryptage de clé pour créer la session de tunnel. La solution doit créer des réciproques afin que la sécurité et la confidentialité puissent être maintenues.
Une clé *est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature).*
Une clé de chiffrement peut être symétrique (cryptographie symétrique) ou asymétrique (cryptographie asymétrique). Dans le premier cas, la même clé sert à chiffrer et à déchiffrer. Dans le second cas on utilise deux clés différentes, les clés publique *est utilisée au chiffrement alors que celle servant au déchiffrement est gardée secrète : la clé Secrète, ou clé privée, et ne peut pas se déduire de la clé publique.*

Une clé peut se présenter sous plusieurs formes : mots ou phrases, procédure pour préparer une machine de chiffrement (connexions, câblage, etc. Voir machine Énigme), données codées sous une forme binaire (cryptologie moderne).

La protection apportée par un algorithme de chiffrement est liée à la longueur de la clé, qui peut s'exprimer en bits. La longueur de la clé quantifie le nombre maximal d'opérations nécessaires au décryptage. C'est donc une borne supérieure sur la sécurité du système.

3.6.5-La non-répudiation : La non-répudiation est le fait de s'assurer qu'un contrat, notamment un contrat signé via internet, ne peut être remis en cause par l'une des parties. Dans l'économie globale actuelle, où les parties ne peuvent souvent pas être face à face pour signer un contrat, la non-répudiation devient extrêmement importante pour le commerce en ligne.

Dans le domaine de la sécurité des systèmes d'information, la non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées[2], et la non-répudiation de l'arrivée prouve qu'elles ont été reçues [11-12].

Généralement, il est admis par la communauté que la non-répudiation peut être atteinte seulement en utilisant la technologie du certificat électronique. En effet cette technologie permet de prouver l'identité d'une personne par la possession de sa propre clé privée. La protection de cette clé devient alors une préoccupation pour l'utilisateur. Celui-ci peut utiliser des authentificateurs tels que carte à puce ou Toren USB, etc.

3.6.6-L'autorisation : L'autorisation est le processus d'octroi ou de refus de l'accès aux ressources situées dans un réseau après que l'utilisateur ait été identifié et authentifié.

3.6.7-Gestion des adresses : est une méthodologie mise en œuvre dans les logiciels informatiques pour planifier et gérer l'attribution et l'utilisation des adresses IP et des ressources étroitement liées d'un réseau informatique. Il ne fournit généralement pas de services DNS (Domain Name System) et DHCP (Dynamics Host Configuration Protocol), mais gère les informations pour ces composants.

Des fonctionnalités supplémentaires, telles que le contrôle des réservations dans DHCP et d'autres capacités d'agrégation de données et de génération de rapports, sont également courantes. Les données suivies par un système IPAM peuvent inclure des informations telles que les adresses IP utilisées et les appareils et utilisateurs associés. La collecte centralisée de ces informations peut prendre en charge le dépannage et les enquêtes sur les abus.

Les outils IPAM sont de plus en plus importants à mesure que de nouveaux réseaux IPv6 sont déployés avec de grands pools d'adresses de nombres hexadécimaux de 128 bits et de nouvelles techniques de sous-réseau.

Un client VPN doit avoir une adresse sur l'intranet et s'assurer que les adresses utilisées dans l'intranet sont gardées confidentielles. Pour cela une solution commune consiste à utiliser un serveur DHCP externe ou un serveur AAA (authentification, autorisation et comptabilité)

Pour l'attribution d'une adresse à l'utilisateur. En outre, certaines informations pour permettre au client d'accéder aux ressources sur le réseau protégé doivent être fournies.

3.7-L'équipements d'un VPN :

Pour établir un tunnel VPN entre deux sites, il faut bien qu'il y ait un ou plusieurs équipements pour gérer cette connexion.
Le choix de l'équipement dépendra le type de tunnel VPN que nous souhaitons et le niveau de sécurité recherché.

Généralement, le pare-feu de l'entreprise est utilisé comme serveur VPN, ce qui permettra également d'ajouter une couche de filtrage. Exemple : l'utilisateur VPN n°1 peut accéder seulement au serveur A, alors que l'utilisateur VPN n°2 peut accéder aux serveurs A et B. Malgré cela, il me semble plus adapté d'utiliser le pare-feu.
Dans le cadre d'un VPN Site-to-site, le tunnel VPN sera configuré entre vos deux équipements, par exemple entre le pare-feu de chaque site. Dans le scénario VPN Client-to-site, le PC client va établir la connexion à l'aide d'un logiciel client VPN auprès du pare-feu. Comme je le disais, il existe Open VPN qui est multiplateformes mais les fabricants proposent aussi généralement leur propre logiciel (exemple : Fortin et avec son Fortin Client).

3.8-Les offres de VPN :

La technologie VPN qui a fonctions principales qu'elle offre à ses utilisateurs :

3.8.1-Confidentialité : La technologie VPN dispose d'un système fonctionnel qui chiffre toutes les données qui la traversent. Avec cette technologie de cryptage, notre confidentialité sera mieux préservée. Même s'il y a des parties qui peuvent exploiter nos données d'avant en arrière, mais pas nécessairement, elles peuvent les lire facilement car elles ont été randomisées. En mettant en œuvre ce système de cryptage, personne ne peut facilement accéder et lire le contenu de notre réseau de données.

3.8.2-Intégrité des données : désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation. L'intégrité des données comprend quatre éléments : l'intégralité, la précision, l'exactitude/authenticité et la validité.

L'intégrité est l'une des exigences de base de la sécurité informatique, de la gestion documentaire et de l'archivistique [12-13]..

Lorsque nous traversons Internet, nos données vont en fait très loin dans différents pays. Au milieu de son voyage, tout peut arriver à son contenu. Qu'il soit perdu, endommagé, voire manipulé par un farceur. Le VPN possède une technologie qui peut maintenir l'intégrité des données que nous envoyons pour arriver à destination sans défauts, perdues, endommagées ou manipulées par d'autres.

3.8.3-Authentification d'origine : La technologie VPN a la capacité d'authentifier les sources des expéditeurs de données à recevoir. Le VPN vérifiera toutes les données entrantes et récupérera des informations sur la source de données. Cette adresse de source de données sera alors approuvée si le processus d'authentification réussit. En tant que tel, VPN garantit toutes les données envoyées et reçues par vous de la bonne source. Aucune donnée n'est falsifiée ou envoyée par d'autres parties.
L'authentification des participants à la première phase peut se faire soit au moyen d'un secret partagé (PSK : « Pré-Shaked Key ») soit par utilisation d'un mécanisme de cryptographie asymétrique tel que RSA. Dans ce cas, il est possible d'utiliser une Infrastructure de Gestion de Clés (IGC ou PKI) pour certifier les clés publiques des participants et ainsi ne pas devoir pré-positionner toutes les clés publiques sur l'ensemble des hôtes [13].

3.9-Avantages et inconvénients du VPN :

3.9.1-Les avantages de VPN :

Les principaux avantages du VPN sont les suivants :

- ✓ une grande souplesse pour déplacer les tunnels, en changer les périmètres ou contrôler le trafic y circulant.
- ✓ Universalité, la possibilité d'accéder à partir de différentes technologies.
- ✓ Nous pouvons transférer des données ou une vue à distance pour contrôler les Ordinateurs à la maison / au bureau n'importe où.
- ✓ Augmentez la connectivité.
- ✓ Échange sécurisé d'informations.

3.9.2-Les inconvénients de VPN :

- ✓ L'utilisation illégale des VPN.
- ✓ Ne pas savoir si le cryptage fournit par votre VPN est fort.
- ✓ La journalisation et potentiellement la revente de vos données à des tiers.
- ✓ Une connexion internet plus lente.
- ✓ Pertes de connexion.
- ✓ Un sentiment injustifié d'impunité en ligne.

4. Conclusion :

Dans ce chapitre on a présenté les notions de base nécessaires au fonctionnement et la réalisation d'une solution VPN ainsi que le réseau TRANSPAC qui était le premier réseau commercial avec ses principes fondamentaux les différents protocoles utilisés notamment IP sec, sur qui est porté notre choix.
Le chapitre fera l'objet de la réalisation et simulation d'une connexion VPN site-à-site.

Chapitre III

La voix sur IP (VoIP)

Administration et Sécurité

1. Introduction :

La gestion des réseaux informatiques constitue un problème dont l'enjeu est de garantir au meilleur cout, non seulement la qualité du service rendu aux utilisateurs mais la réactivité dû aux changements et à l'évolution rapide du secteur informatique.

Les réseaux informatiques nécessitent un administrateur pour gérer tous les services fonctions de transmission entre les réseaux. Ils ont également besoin d'un ensemble d'outils, de techniques, de méthodes et d'appareils pour protéger les informations contre le piratage et réduire l'exposition du système aux menaces accidentelles ou intentionnelles, en particulier lorsqu'ils sont connectés à Internet.

La voix sur IP constitue actuellement l'évolution la plus importante du 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 majeure a été le passage à la transmission numérique (TDM). La transmission de la voix sur les réseaux informatiques à commutation de paquets IP constitue aujourd'hui une nouvelle évolution majeure comparable aux précédentes.

L'objectif de ce chapitre est l'étude de cette technologie et de ses différents aspects. On parlera en détail de l'architecture de la VoIP, ses éléments et son principe de fonctionnement. On détaillera aussi des protocoles VoIP de signalisation et de transport ainsi que leurs principes de fonctionnement et de leurs principaux avantages et inconvénients.

1.1. Présentation de la voix sur IP

Définition

VoIP signifie **Voice over Internet Protocol** ou Voix sur IP. Comme son nom l'indique, la VoIP permet de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur Internet. La VoIP peut utiliser du matériel d'accélération pour réaliser ce but et peut aussi être utilisée en environnement de PC.

1.2. Architecture

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

Il existe donc plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP.

Certaines placent l'intelligence dans le réseau alors que d'autres préfèrent une approche égale à égale avec l'intelligence répartie à la périphérie. Chacune ayant ses avantages et ses Inconvénients [14]..

L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/ contrôleur de commutation, appelées Gatekeeper. On retrouve les éléments communs suivants :

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

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

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

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

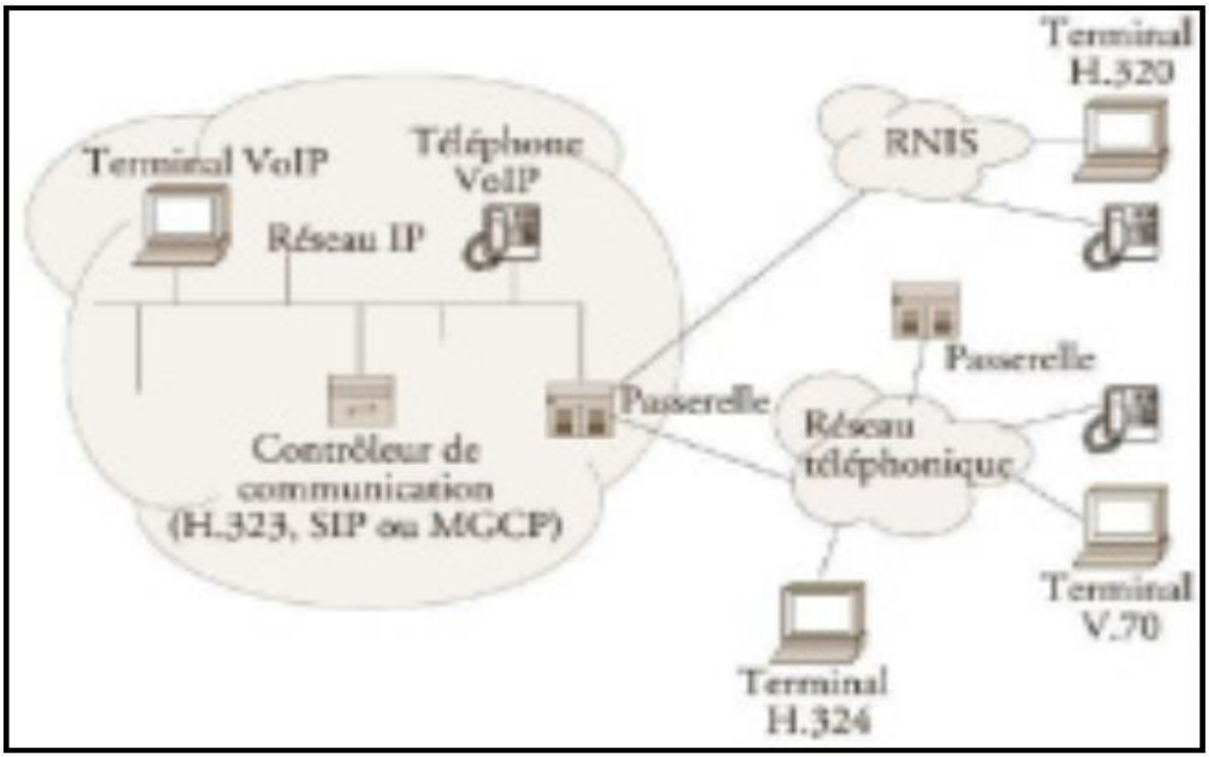


Figure III 1 : Architecture générale de la voix sur IP

1.3. Principe de fonctionnement

La VoIP fonctionne par numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Le signal numérique est plus tolérant au bruit que l'analogique.
Les réseaux TCP/IP sont des supports de circulation de paquets IP contenant un en-tête (pour contrôler la communication) et une charge utile pour transporter les données.
Il existe plusieurs protocoles qui peuvent supporter la voix sur IP tel que le H.323, SIP et MGCP.
Les deux protocoles les plus utilisées actuellement dans les solutions VoIP présentes sur le marché sont le H.323 et le SIP [14]..

2. Protocole H.323

2.1 Description générale du protocole H.323

Le standard H.323 fournit, depuis son approbation en 1996, un cadre pour les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (International Telecommunications Union) pour les réseaux qui ne garantissent pas une qualité de service (QoS), tels qu'IP IPX sur Ethernet, Fast Ethernet et Token Ring. Il est présent dans plus de 30 produits et il concerne le contrôle des appels, la gestion multimédia, la gestion de la bande passante pour les conférences point-à-point et multipoints. H.323 traite également de l'interfaçage entre le LAN et les autres réseaux.

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

2.2 Description générale du protocole SIP

Le protocole SIP (Session Initiation Protocol) est un protocole normalisé et standardisé par l'IETF (décrit par le RFC 3261 qui rend obsolète le RFC 2543, et complété par le RFC 3265) qui a été conçu pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol). SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP étant indépendant de la transmission des données, tout type de données et de protocoles peut être utilisé pour cet échange. Cependant le protocole RTP (Real-time Transport Protocol) assure le plus souvent les sessions audio et vidéo. SIP remplace progressivement H323.
SIP est le standard ouvert de VoIP, interopérable, le plus étendu et vise à devenir le standard des télécommunications multimédia (son, image, etc.). Skype par exemple, qui utilise un format propriétaire, ne permet pas l'interopérabilité avec un autre réseau de voix sur IP et ne fournit que des passerelles payantes vers la téléphonie standard. SIP n'est donc pas seulement destiné à la VoIP mais pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo [13-14].

2.3. Protocoles de transport

Nous décrivons deux autres protocoles de transport utilisés dans la voix sur IP à savoir l'RTP et le RTCP

2.3.1 Le protocole RTP

4.1.1 Description générale de RTP

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

2.3.2 Le protocole RTCP

4.2.1 Description générale de RTCP

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

- Une synchronisation supplémentaire entre les médias : Les applications multimédias sont souvent transportées par des flots distincts.
- L'identification des participants à une session : en effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Le contrôle de la session[15].

3.1 Points forts et limites de la voix sur IP

Différentes sont les raisons qui peuvent pousser les entreprises à s'orienter vers la VoIP comme solution pour la téléphonie. Les avantages les plus marqués sont :

- ***Réduction des coûts***
- ***Standards ouverts***
- ***Un réseau voix, vidéo et données (à la fois)***
- ***Un service PABX distribué ou centralisé***
- ***Fiabilité et qualité sonore***

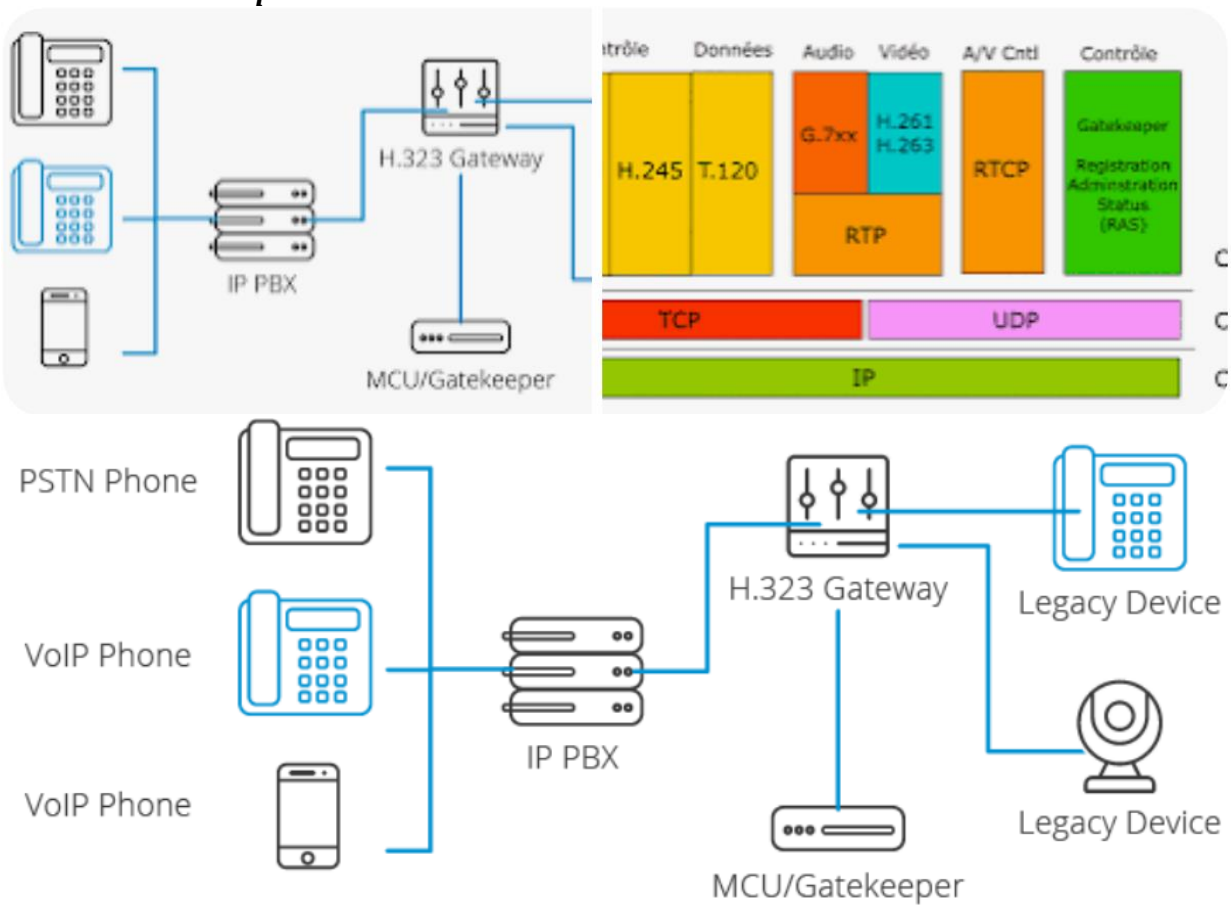


Fig III.1.2 Description générale des différents protocoles utilisées avec la voix sur IP

3.1.1 Le but de l'administration d'un réseau informatique :

3.1.2 A- La supervision :

Est une technique industrielle de suivi et de pilotage informatique de procédés de fabrication automatisés.

La supervision dans l'informatique est la surveillance du bon fonctionnement d'un système ou d'une activité.

La supervision consiste à surveiller les systèmes et à récupérer les informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes. Le plus grand souci d'un administrateur est la panne. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continu l'état afin d'éviter un arrêt prolongé de celui-ci. La supervision doit permettre d'anticiper les problèmes et de faire remonter les sur l'état des équipements et des logiciels. Une grande majorité des logiciels de supervision sont basés sur le protocole SNMP qui existe depuis de nombreuses années.

La plupart de ces outils permettent de nombreuses fonctions dont voici le principal :

- surveiller le système d'information
- Visualiser l'architecture du système
- Analyser les problèmes
- Déclencher des alertes en cas de problème

3.2. B-L'administration :

L'administration de réseau est une discipline de l'informatique qui peut éventuellement s'étendre à la téléphonie.

L'administration désigne plus spécifiquement les opérations de contrôle du réseau avec la gestion des configurations et de sécurité. De façon générale, une administration de réseaux a pour objectif d'englober un ensemble de techniques de gestion mises en œuvre pour :

- ✓ Permettre l'évolution du système en incluant de nouvelles fonctionnalités.
- ✓ Offrir aux utilisateurs une certaine qualité de service.
- ✓ Rendre opérationnel un système.

3.3. C-l 'exploitation :

En informatique, un système d'exploitation est un ensemble de programme qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs.

Les systèmes d'exploitation actuels, qui sont des systèmes *UNIX*, *MacOs* et *Windows* gèrent tous l'aspect de l'exploitation des réseaux, les procédures et les fonctions associés. Un système d'administration réseau est une collection d'outils Superviser le réseau et le contrôle qui sont intégrés dans le sens où ils sont Impliquer :

- ✓ Une interface opérateur unique avec un puissant, mais convivial ensemble de commandes pour exécuter toutes les tâches d'administration réseau ;
- ✓ Un nombre minimal d'équipements séparés qui sont le plus souvent des composants matériels et logiciels requis pour l'administration réseau, et incorporés dans les équipements utilisateurs existants.

L'administration d'un réseau suppose l'existence d'un système d'information décrivant le réseau de l'entreprise et recensant toutes les données et événements relatifs à chaque constituant du réseau administré.

3.3.1-Topologie de l'administration des réseaux informatiques :

L'administration des réseaux informatiques peut se décomposer en trois types d'administration :

- administration des utilisateurs.
- administration des ***serveurs.***
- administration ***de la machine de transport.***

3.3.2 -L'administration des utilisateurs :

L'administration des utilisateurs fournit l'ensemble des mécanismes nécessaires pour qu'une personne d'utilise le réseau, à savoir :

- ✓ Accessibilité et Connectivité aux applications. l'utilisateur doit pouvoir se connecter aux différentes applications fournit par le réseau et doit disposer d'un ensemble d'outils lui assurant une certaine transparence au niveau des méthodes d'accès et connexions aux applications ;
- ✓ L'accès aux serveurs de noms. afin de permettre la localisation des ressources et d'assurer à L'utilisateur l'existence et l'utilisation de ces ressources.
- ✓ La Confidentialité et la Sécurité. Le système doit fournir l'ensemble des mécanismes qui permettent de garantir la confidentialité des informations de l'utilisateur, de sécuriser son environnement et de prévenir toute perte ou altération des échanges effectués par l'utilisateur.
- ✓ La Qualité de service fournit à l'utilisateur. Il s'agit principalement de la disponibilité et des performances du système et sa capacité à assurer le service attendu.

3.3.3 -L'administration des serveurs :

L'administration des serveurs fournit tous les mécanismes suivant :

- ✓ La Connexion et la Distribution des applications sur tout le réseau .afin de permettre la relation entre les différents services.
- ✓ La Gestion et la Distribution des données .comme pour les utilisateurs, doivent garantir la fiabilité de transmission des informations et offrir des outils permettant le transfert de ces informations. C'est le rôle des outils de transfert de fichiers, qui permettent le partage des capacités de stockage entre plusieurs systèmes.

- ✓ La Gestion des applications. est essentiellement lié au contrôle et à la protection des accès de ces applications par la distribution de droits, et de différents protocoles de contrôle d'utilisation de ressources concernant les applications utilisées.

3.3.4 -L'administration de la machine de transport :

L'administration de la machine de transport consiste à fournir :

- ✓ *les performances fournies par le réseau*, le but est d'afficher et d'évaluer le système par un ensemble de paramètres comme le temps de réponse ou la charge du système.
- ✓ *les coûts*, afin de pouvoir les mesurer (dans un réseau, les coûts d'utilisation sont complexes à évaluer puisqu'ils concernent un ensemble de composants distribués).
- ✓ *la configuration*, le but est de déterminer la meilleure configuration du réseau afin d'améliorer les performances du système et la qualité du service.
- ✓ *les opérations de réseau* : dont le rôle est de permettre l'intervention sur le fonctionnement et la modification du réseau.
- ✓ *la liste des incidents réseaux par la mise en place de protocoles de détection et de correction* : Lorsqu'une alerte est déclenchée, des actions vont être prises pour

résoudre l'incident et de ce fait, réduire son influence et ses perturbations sur l'ensemble du réseau.

- ✓ *la configuration*, le but est de déterminer la meilleure configuration du réseau afin d'améliorer les performances du système et la qualité du service.
- ✓ *l'inventaire,* qui a pour rôle de tenir à jour en temps réel la liste des éléments logiciels et matériels qui constituent un réseau [16]..
- ✓ *l'évolution et les changements,* l'objectif est de fournir les informations permettant de déterminer les nouveaux besoins et les parties du système concernées par ces besoins de changement.

4.1-Le rôle de l'administrateur réseau :

Le rôle de l'administrateur réseau consiste à :

- ✓ Installer et maintenir les services nécessaires au fonctionnement du réseau.

- ✓ Gérer les « login » (noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières,….).
- ✓ Mettre en place et maintenir l'infrastructure du réseau.

- ✓ S'assurer que les utilisateurs « n'outrepassent » pas leur droite.
- ✓ Gérer les systèmes de fichiers partagés et les maintenir.

4.2-La sécurisation des réseaux :

Avec l'application des nouvelles technologies et la diversification des types de réseaux Comme la multiplication des mobiles connectés et de développement des solutions de Cloud comptine de sécurité réseau est devenue une tâche complexe.
Divers équipements peuvent être mis en place pour protéger les enstères et sorties réseau :

4.3-Programme antivirus :

L'antivirus sont des logiciel conçus pour identifie, neutraliser et éliminer des logiciel malveillant.

Logiciel de sécurité qui procède, automatiquement ou sur demande, à l'analyse des fichiers et de la mémoire d'un ordinateur, soit pour empêcher toute introduction parasite, soit pour détecter et éradiquer tout virus dans un système informatique.
Les logiciels antivirus remplissent trois fonctions essentielles :
La vérification permanente, visant à contrer toute tentative d'infection informatique, la détection des virus introduits dans un système et, enfin, leur élimination.
Les produits commercialisés peuvent n'offrir qu'une de ces fonctions, ou les proposer toutes. En effet, certaines solutions antivirus se composent à la fois d'un programme détecteur de virus, d'un ou de plusieurs utilitaires de destruction ainsi que d'un programme préventif agissant en amont des tentatives d'infection. Comme exemples de logiciels antivirus, on peut mentionner Norton.
Antivirus de Symantec, Inoculât IT de Computer Associates, ainsi que VirusScan, Web Sheds, Net Shed et Group Sheds de Network Associates.

4.4. -Pare-feu :

Le pare-feu est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types communication autorisés sur ce réseau informatique .il surveille et contrôle les applications et les flux de données (paquets). Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent généralement, les zones de confiance incluent internet et au moins un réseau interne.

Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

Une interface pour le réseau à protéger (réseau interne).

Une interface pour le réseau externe.

Types de pare-feu : Les différents types de pare-feu intègrent le logiciel, le matériel ou une association des deux. Tous ont des utilisations, des points forts et des faibles différents.

Figure III.2: appareil pare-feu

4.5 -Proxy :

Est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

Le proxy est un programme qui sert d'intermédiaire entre un ordinateur et un réseau, le plus souvent internet. Un serveur proxy est un outil de protection assez efficace quand on se connecte à internet, et permet de naviguer anonymement en masquant notre adresse IP.

Le serveur mandataire, complète le pare-feu, il est particulièrement utilisé dans le cadre de tracs Hyper Texte Transfer Protocol (http), et File Transfer Protocol (FTP) entre le LAN et l'Internet.

Il intercepte une demande vers l'extérieur et le fait en son propre nom, puis stocke les données renvoyées. Ensuite, il les retransmet au demandeur initial. Il a pour avantage de amoure les

adresses IP internes et d'autoriser les filtrages, mais aussi la capacité la gérer une mémoire cache.

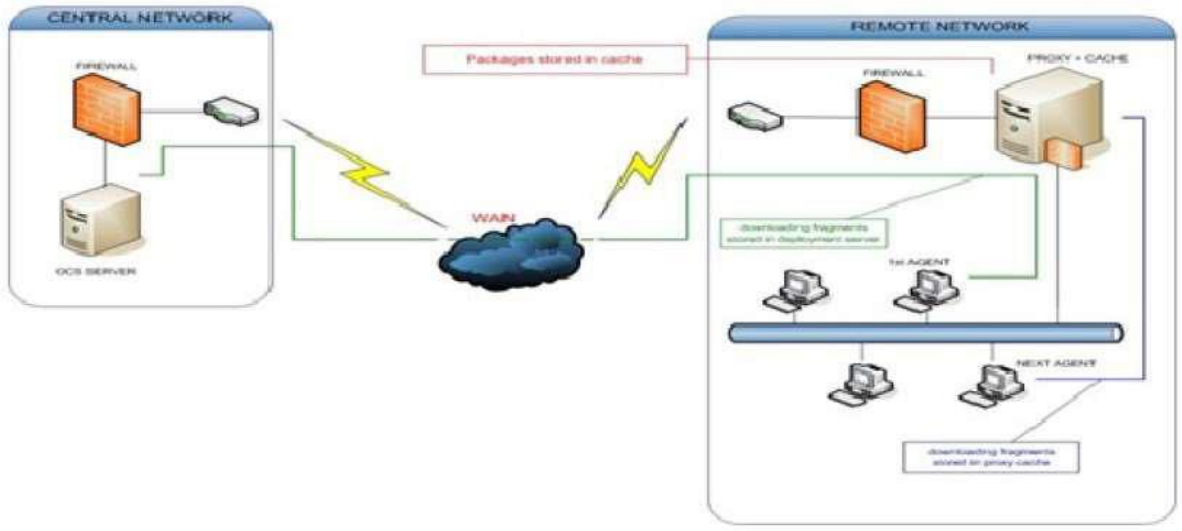


Figure III.3: Le serveur proxy.

4.6 -Routeur filtrant [16]:

Routeur filtrant est un dispositif informatique qui filtre les flux d'informations entre un réseau Interne à un organisme et un réseau externe en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur.
Les mécanismes de filtrage qui peuvent être associés à l'équipement routeur autorisent des analyses de couche 3 du modèle OSI. L'examen des paquets portera ainsi sur l'entête IP, ce qui permet le blocage des adresses IP (source et destination) ainsi que l'interdiction de transmission de protocole de couche 3 ou 4 utilisés (UDP, TCP . . .).

4.7 -Zone démilitarisée :

La Zone démilitarisée : Une DMZ (Démilitarise zone) est une zone tampon d'un réseau D'entreprise, située entre le réseau local et Internet, derrière le pare-feu. Il s'agit d'un réseau Inter média ire regroupant des serveurs publics (HTTP, DHCP, mails, DNS, etc.). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis les réseaux externes.
Le but est ainsi d'éviter toute connexion directe au réseau internet [16].

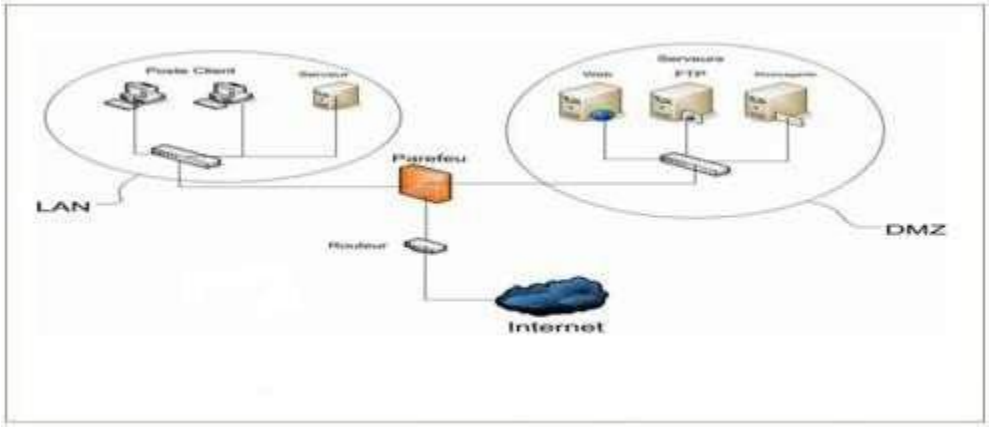


Figure III.4 : Zone Démilitarisée

5.1. Les classes d'adresses :

- **Adresse IP :**

L'adresse IP (Internet Protocol), un protocole qui permet d'identifier les machines et de router les informations sur Internet. Ces adresses sont codées sur 4 octets sont la plupart du temps écrites en numérotation décimale en séparant les octets par des points. Ça donne quelque chose comme ça : 192.168.132.24.

La plage d'adresses IP est découpé en cinq parties distinctes. Les classes A, B, C, D et E, que l'on appelle aussi adresses globales.

• *Classe A* : Premier bit de l'adresse à 0, et masque de sous-réseau en 255.0.0.0. Ce qui donne la plage d'adresse 0.0.0.0 à 126.255.255.255 soit 16 777 214 adresses par réseau de classe A

• *Classe B* : Deux premiers bits de l'adresse à 10 (1 et 0), et masque de sous-réseau en 255.255.0.0. Ce qui donne la plage d'adresse 128.0.0.0 à 191.255.255.255 soit 65 534 Adresses par réseau de classe B.

• *Classe C* : Trois premiers bits de l'adresse à 110, et masque de sous-réseau en 255.255.255.0. Ce qui donne la plage d'adresse 192.0.0.0 à 223.255.255.255 soit 255 Adresses par réseau de classe C

• *Classe D* : Quatre premiers bits de l'adresse à 1110, et masque de sous-réseau en 255.255.255.240. Ce qui donne la plage d'adresse 224.0.0.0 à 239.255.255.255 soit 255 Adresses par réseau de classe D

• *Classe E* : Quatre premiers bits de l'adresse à 1111, et masque de sous-réseau en 255.255.255.240. Ce qui donne la plage d'adresse 240.0.0.0 à 255.255.255.255
Les classes A, B et C, sont réservées pour les utilisateurs d'Internet (entreprises, administrations, fournisseurs d'accès, etc.) La classe D est réservée pour les flux multicast et la classe E n'est pas utilisée aujourd'hui.

5.2 -Notions de base sur le routage :

Lorsque le réseau interne d'une entreprise prend de l'ampleur, il peut devenir nécessaire, pour des raisons de sécurité et d'organisation, de le diviser en plusieurs petits réseaux. Pour ce faire, on crée généralement des sous-réseaux. La création de sous-réseaux implique l'existence d'un routeur qui achemine le trafic d'un sous-réseau vers un autre.
Un routeur utilise une table de routage pour déterminer le lieu d'expédition des paquets. La table de routage contient un ensemble de routes. Chaque route décrit la passerelle ou l'interface utilisée par le routeur pour atteindre un réseau donné.

5.3 - Les protocoles de TUNNELISATION :

Il s'agit d'un protocole réseau utilisé pour créer des réseaux privés virtuels (VPN), Le plus souvent entre un opérateur de collecte de trafic et le fournisseur d'accès à internet.
Un protocole de ***TUNNELISATION*** est un protocole qui encapsule dans son datagramme un autre paquet de données complet utilisant un protocole de communication différent.
Un tunnel est ainsi créé entre deux points sur un réseau pour transmettre en toute sécurité tout type de données de l'un à l'autre. En règle générale, ces types de protocoles sont utilisés pour envoyer des données de réseau privé sur un réseau public, principalement lors de la création

d'un réseau VPN, mais ils peuvent également être utilisés pour renforcer la sécurité de transmission des données chiffrées sur un réseau
Public. Il existe plusieurs protocoles de ***TUNNELISATION*** répandus, comme Secure Shell (SSH), Pinto-Point Tunneling (PPTP) et IP sec, chacun étant adapté à un objectif de ***TUNNELISATION*** spécifique.

- *Fonctionnalité :*

Dans le processus de construction du tunnel, les données seront décomposées en plus petits morceaux, qui se déplaceront le long du "tunnel" pour être transportés jusqu'à leur destination finale. Lorsque ces paquets traversent le tunnel, ils sont cryptés et encapsulés. Les données du réseau privé et le protocole d'information qui l'accompagne sont également encapsulés dans des unités de transmission du réseau public pour l'envoi. Le processus de décapsulation et de décryptage aura lieu à la réception. De plus, le tunnel est considéré comme le chemin logique ou la connexion qui encapsulera les paquets qui traversent le réseau de transit. Ce protocole de tunneling cryptera la trame d'origine afin que le contenu ne soit pas interprété en dehors de sa route. Pour que le processus fonctionne vraiment, les données seront envoyées une fois que le tunnel est déjà en place et que les clients ou le serveur utiliseront le même tunnel pour envoyer et recevoir les données sur le réseau Internet [16]..

6.1 -Les protocoles d'un routage :

Les protocoles de routages permettent l'échange des informations à l'intérieur d'un système autonome. On retient les protocoles suivants :
• Vecteur de distance, chaque routeur communique aux autres routeurs la distance qui les sépare. Ils élaborent intelligemment une cartographie de leurs voisins sur le réseau : RIP
• Hybride des deux premiers, comme EIGRP

• États de lien, ils s'appuient sur la qualité et les performances du média de communication qui les séparent. Ainsi chaque routeur est capable de dresser une carte de l'état duré se au pour utiliser la meilleure route : OSPF [16].

Les protocoles couramment utilisés sont :
•Enhanche interior Gateway Routing Protocol **(EIGRP).**
• Routing Information Protocol **(RIP).**
• Open Short est Pathé First **(OSPF).**

6.3-Les réseaux locaux virtuels (VLAN) :

Avant d'arriver à la conception technique globale de la solution retenue, nous ferons une étude brève sur les fonctionnalités des VLAN. Celle-ci nous permettra de définir à travers ces fonctionnalités, une meilleure planification du déploiement future.

6.4 -Généralités :

Par définition, un VLAN (Virtual Local Area Network) Ethernet est un réseau local virtuel (logique) utilisant la technologie Ethernet pour regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenance à un département, etc.), sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, etc.).

6.5 -Avantages offerts par les Vlan :

La technologie de VLAN comporte ainsi de nombreux avantages et permet de nombreuses applications intéressantes. Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment :

• La flexibilité de segmentation du réseau

• La simplification de la gestion

• Une meilleure utilisation des serveurs réseaux.

• Le renforcement de la sécurité du réseau

• L'augmentation considérable des performances du réseau (réduction du domaine de collision).

6.6 -Technique et méthodes d'implantation des Vlan :

Pour réaliser les VLAN, il faut tout d'abord disposer de commutateurs spéciaux de niveau 2 du modèle OSI qui supportent le VLAN.

On distingue généralement trois techniques pour construire des VLAN. Nous pouvons les associer à une couche particulière du modèle OSI :

- **VLAN par ports :** On affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN

est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.

- **VLAN MAC :** On affecte chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminé par son adresse MAC.

En fait, il s'agit à partir de l'association MAC/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

- **VLAN d'adresses réseaux :** On affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise.

7.1 -Principe du routage INTER-VLAN :

Quand un hôte d'un VLAN veut communiquer avec un hôte d'un autre VLAN, un routeur est Nécessaire ou un commutateur de couche 3.

La connectivité entre les VLAN peut être établie par le biais d'une connectivité physique ou logique. Une connectivité logique implique une connexion unique, ou agrégation, du commutateur au routeur. Cette agrégation peut accepter plusieurs VLAN. Cette topologie est appelée «router-on-a-stick» car il n'existe qu'une seule connexion physique avec le routeur. En revanche, il existe plusieurs connexions logiques entre le routeur et le commutateur.

Une connectivité physique implique une connexion physique séparée pour chaque VLAN. Cela signifie une interface physique distincte pour chaque VLAN.

Les premières configurations de VLAN reposaient sur des routeurs externes connectés à des commutateurs compatibles VLAN.

Pour permettre aux hôtes de VLAN de communiquer entre eux, il faut utiliser un routeur

Commutateur de couche 3. Le terme commutateur de couche 3 désigne un commutateur capable d'assurer une fonction de routage en plus de ses fonctions habituelles. Ainsi, au lieu d'un routeur externe, on aura un routeur interne au commutateur.

7.2 -Charte de sécurité :

La charte de sécurité définit un ensemble de règles de bonne conduite à respecter par les utilisateurs dans le but de faciliter le déploiement de la politique sécurité.
Il s'agit d'un document qui garantit à tous une libre circulation de l'information, un libre accès aux Ressources informatiques, électroniques et numériques dans le respect de la légalité.
Elle sert également à faire prendre conscience aux utilisateurs de certains risques qu'ils pourraient encourir et des conséquences de tels risques.

7.3 -Sécurité logicielle :

C'est l'ensemble des règles applicatives implémentées au niveau des nœuds pour protéger le réseau contre toutes sortes de compromissions, d'agressions venant de l'extérieur et même de l'intérieur.

7.4 -La sécurité d'un réseau :

Quel que soit le réseau local de l'entreprise, il n'est pas isolé car il doit être connecté à Internet ou à d'autres réseaux et cela le met à risque de piratage, il est notamment nécessaire de protéger les entrées et sorties sur un réseau interne. Mais même si nous adoptons les meilleures pratiques de cyber sécurité, si nous laissons nos serveurs en plein air, n'importe qui pourra les voler. Une bonne sécurité informatique commence par une bonne sécurité physique.

7.5 -Définition de la sécurité informatique :

C'est une tâche difficile, tout particulièrement dans un contexte de connectivité croissante.
Pour améliorer la sécurité, il faut mettre en place des mécanismes, d'une part pour assurer que seules les personnes autorisées peuvent consulter ou modifier des données, d'autre part pour assurer que les services peuvent être rendus correctement.
La sécurité des systèmes d'information vise à garantir :

- ✓ la confidentialité consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- ✓ l'intégrité consistant à garantir que les données sont bien celles que l'on croit être.
- ✓ la disponibilité des services : permettant de maintenir le bon fonctionnement du système d'information.
- ✓ L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

8. Conclusion :

Comme on a pu le voir tout au long de ce chapitre, la VoIP est la solution la plus rentable pour effectuer des conversations. Actuellement il est évident que la VoIP va continuer à évoluer.
La téléphonie IP est une bonne solution en matière d'intégration, fiabilité et de coût. On a vu que la voix sur IP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. Chaque standard possède ses propres caractéristiques pour garantir une bonne qualité de service. En effet, le respect des contraintes temporelles est le facteur le plus important lors de transport de la voix.

Malgré que la normalisation n'ait pas atteint la maturité suffisante pour sa généralisation au niveau des réseaux IP, il n'est pas dangereux de miser sur ces standards vu qu'ils ont été acceptés par l'ensemble de la communauté de la téléphonie.

Pour finir lors de la mise en œuvre de cette technologie, il faut poser la question suivante : le développement de cette technologie représente t'il un risque ou une opportunité pour les utilisateurs et les opérateurs téléphoniques ?

Chapitre IV
Résultat du Simulation et Discussion

1. INTRODUCTION :

Pour faciliter le travail de notre projet on va étudier et simulé nos réseaux avec le logiciel qui s'appelle Cisco Packet Tracer, ce dernier fait la conception, la configuration, la simulation et vérification du fonctionnement de chaque réseau inclue cette étude.
Nous allons voir dans ce chapitre la simulation de quatre réseaux suivants :
1. Le premier réseau (Scénario 01) Réseau VoIP, (Conception, Configuration, Simulation).
2. Le deuxième réseau (Scénario 02) Réseau VoIP entre deux sites distants, (Conception, Configuration, Simulation).
3. Le troisième réseau (Scénario 03) installation du réseau VPN entre deux sites distants, (Conception, Configuration, Simulation).
4. Le quatrième réseau (Scénario 04), l'installation du (Réseau VPN_+ Réseau VOIP _ final), (Conception, Configuration, Simulation).

2. INTERFACE DE LOGICIEL CISCO PACKET TRACER :

2.1. DEFINITION DE CISCO SYSTEMS :

Cisco Systems est une entreprise informatique américaine spécialisée beaucoup plus dans les Matériels réseaux tels que les routeurs et les commutateurs Ethernet, opérant dans le monde entier, elle a été établie en 1984 par Leonard Bosch et Sandra Lerne, et a son siège social à San Jose, en Californie.

3. LOGICIEL CISCO PACKET TRACER :

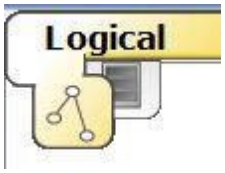
3.1. Introduction :

Cisco Packet Tracer est un simulateur de matériel réseau Cisco (*routeurs, commutateurs*). Cet outil est créé 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 Académie*). Le but de Pocket 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 du réseau. L'utilisateur peut bâtir son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ensuite ces équipements doivent être reliés via des connexions (câbles divers, fibre optique, Point d'accès) [17].

Lorsque l'ensemble des équipements soient reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP et les services disponibles, etc.…

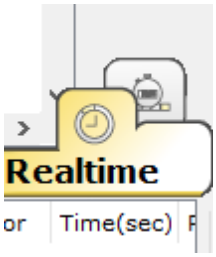
3.2. Interface et outils :

A. La zone de travail où nous définirons graphiquement notre réseau



B. Le bouton logiciel permettant de naviguer entre le réseau logique et physique.

C. Le barre de réaltine, pour alterner entre le mode temps-réel et mode simulation (-pas-a-pas).



D. Une barre d'outils à droite contient les outils nécessaires, aussi que trois boîtes à outils en bas pour le choix du type de matériel tel qu'ordinateur, Router, etc....

E. Les types de matériels utilisés :

1. Les routeurs : Ils fonctionnent au niveau réseau (couche 3 du modèle OSI), son objectif est l'interconnexion des sous-réseaux go-localisés ou distants à travers des liaisons longues distances.

2.Les concentrateurs: Un concentrateur ou (Hub, étoile, multi-répéteur) est employé dans les réseaux locaux Ethernet, il a une fonction de répéteur, mais permet de mixer différents médias (paire torsadée, AUI, Thuin Ethernet, fibre optique).

3. Les commutateurs: aussi appelé SWITCH, fonctionnent au niveau Liaison, il a la mêmes Fonction qu'un pont mais utilisent des ports dédiés et non partagés.

4.Les ordinateurs.

5. Les réseaux étendus (WAN).

6.Les bornes sans fil (wifi).

7. Les connexions ou appelé (câblage), on trouve plusieurs types tels que la fibre optique, câble coaxial, câble croisé, câble octal,

8. la sécurité.

9. Des appareils divers.

10. Les connexions multi-usagers.

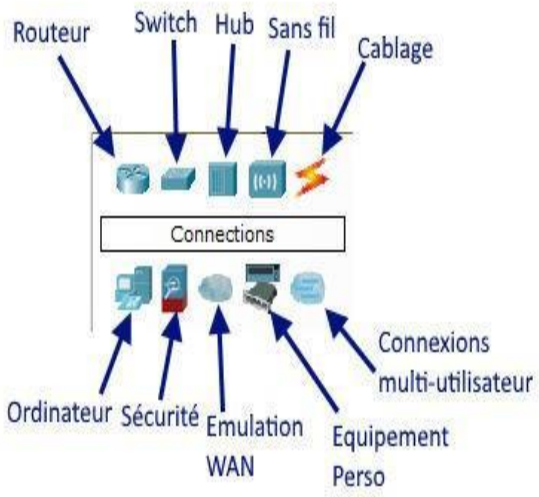


Figure IV. 1: Matériels utilisés.

Figure IV .2 : ***Exemple*** d'ordinateurs.

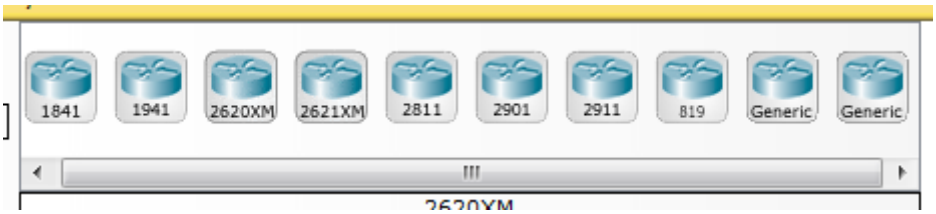


Figure IV .3 : Exemple de router.

La catégorie câblage pour connecter les appareils :

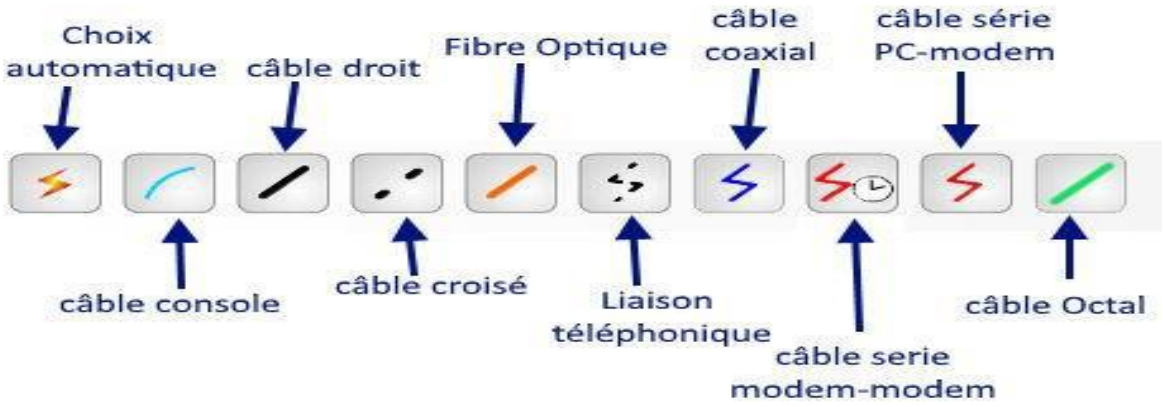


Figure IV .4: Les connecteurs des équipements.

La fenêtre "Desktop" et "IP Configuration" :

Pour configurer un PC, on doit cliquer sur le PC, puis sur l'onglet Desktop, enfin sur l'icône IP Configuration.

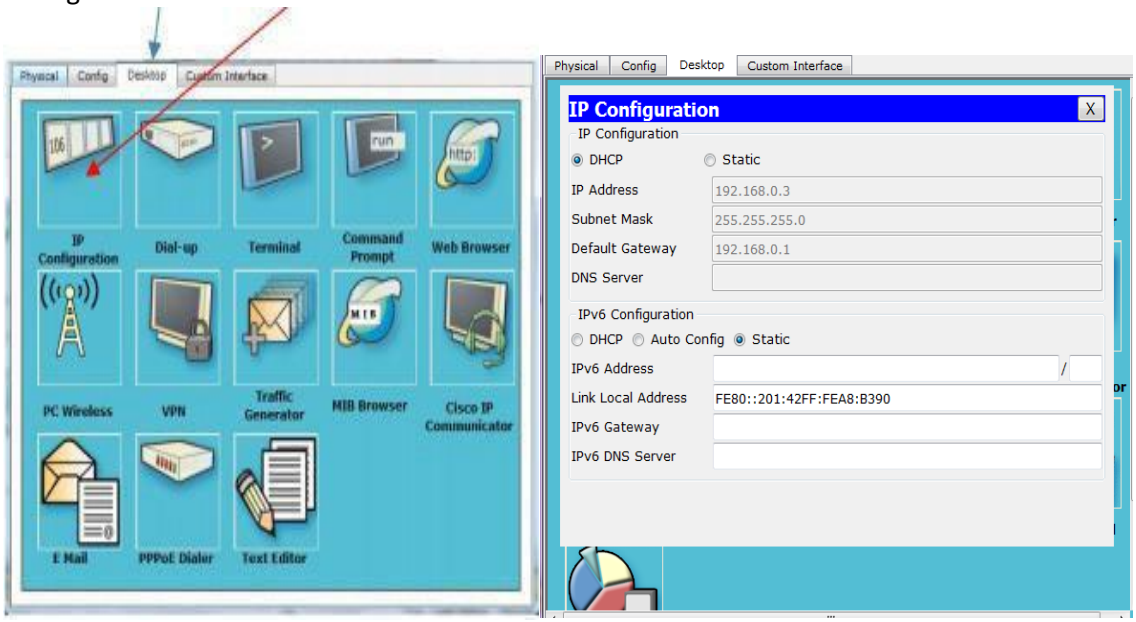


Figure IV .5 :exemple desktop ip configuration

4. LA PARTIE DE SIMULATION :

4.1. LA CREATION DU RESEAU :

Nous allons au cours de cette partie de simulation de simuler quatre réseaux afin de clarifier le but et l'objectif de cette étude, tout d'abord en commençant par la configuration d'un réseau simple embarquant le VoIP (Voice over Internet Protocol). Le réseau comportera également un serveur DHCP qui servira a distribué une IP à chaque terminal du réseau.
Nous aurons donc besoin d'une typologie simple avec le matériel suivant :

- Un routeur (2811)
- Un Switch (2960-24TT)
- Deux IP Phones (7960).
- Deux PC connectés aux IP Phones.

4.2 Simulation réseau 01 (Scénario 01) Réseau VoIP:

Dans notre cas voici la typologie utilisée :

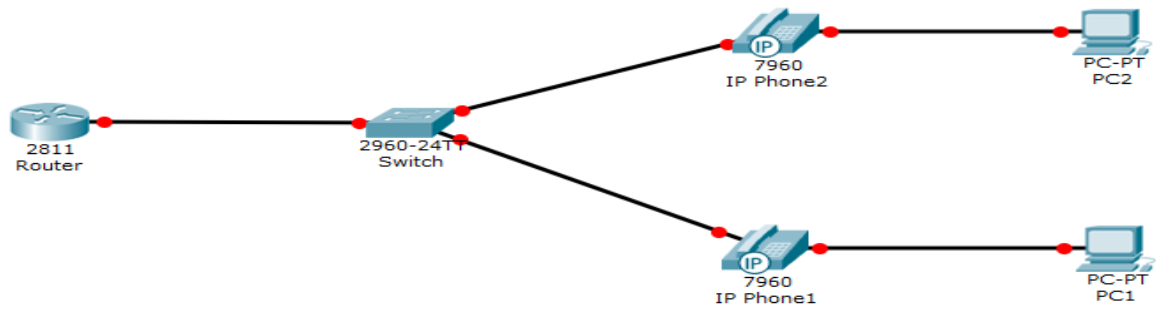


Figure IV .6 : schéma de réseau VOIP

Pour configurer le réseau VOIP, on doit utiliser les étapes de configuration suivantes [18-19] :

-Première étape : Configuration de l'interface faste Ethernet 0/0 du Router et création du serveur DHCP.

Commençons par l'interface Fa 0/0.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

Router(config-if)#exit
Router(config)#
```

Puis nous créons et nous configurons le serveur DHCP utilisé pour distribué une adresse IP à chaque terminal IP du réseau.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#option 150 ip 192.168.0.1
Router(dhcp-config)#exit
Router(config)#exit
Router#
```

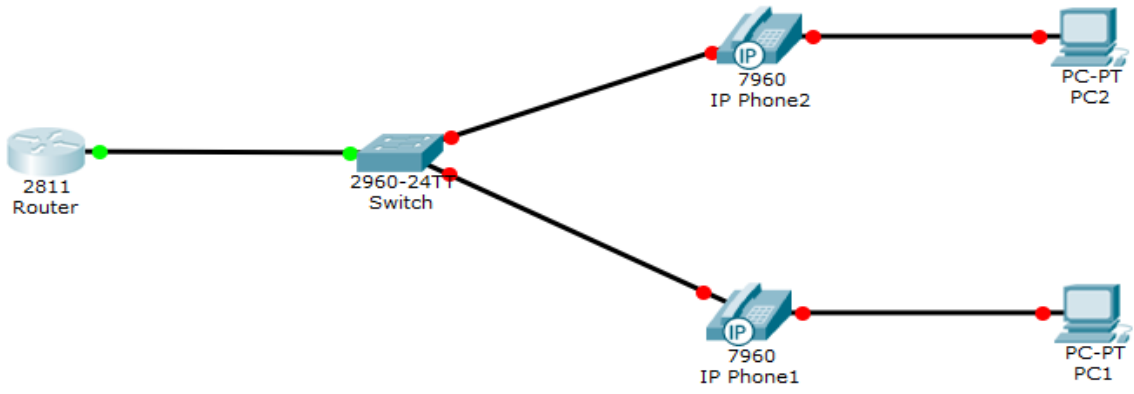


Figure IV .7: schéma de réseau VOIP

Ensuite nous allons démarrer les IP Phones, en cliquant dessus nous allons brancher l'adaptateur secteur afin de l'alimenter (vous pouvez également utiliser des Switch POE Power Over Ethernet, afin de ne pas avoir à utiliser le secteur pour alimenter vos téléphones).

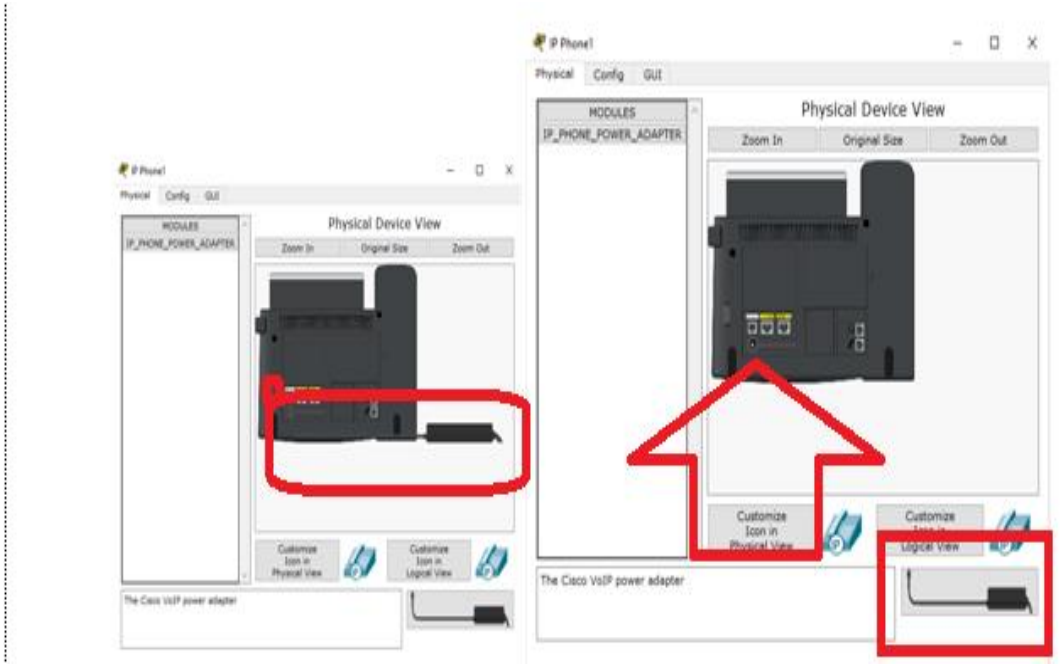


Figure IV .8 : configuration de téléphone

Normalement, toutes les connexions devraient être affichées en vertes :

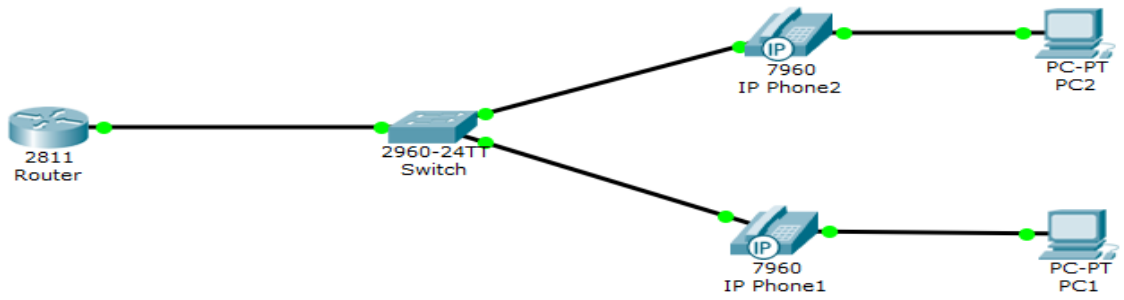


Figure IV .9 : Schéma de réseau VOIP

-Deuxième étape : Configuration du service de téléphonie « Call Manager Express »

Nous allons donc configurer Call Manager Express afin d'activer le support VoIP sur notre réseau. Sur le Router.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#telephony-service
Router(config-telephony)#max-dn 5
Router(config-telephony)#max-ephones 5
Router(config-telephony)#ip source-address 192.168.0.1 port 2000
Router(config-telephony)#auto assign 4 to 6
Router(config-telephony)#auto assign 1 to 5
Router(config-telephony)#exit
Router(config)#
```

-Troisième étape : Configuration d'un Vlan Voice sur le Switch.

Nous allons configurer les interfaces du Switch afin de séparer les données (transferts de fichiers par exemple) et les communications.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range FastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 1
Switch(config-if-range)#exit
Switch(config)#
```

-Quatrième étape : Configuration du téléphone IP 1 sur le Routeur.

Les téléphones sont connectés et le réseau configuré, seulement il faut ajouter une configuration supplémentaire afin de leur permettre de communiquer. Il faut donc leur assigner un numéro de téléphone afin de les mettre en relation.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 54001
Router(config-ephone-dn)#
```

-Cinquième étape : Configuration du téléphone IP 2 sur le Routeur.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 54002
```

-Sixième étape : Vérification de la bonne attribution des IP et des numéros de téléphones.

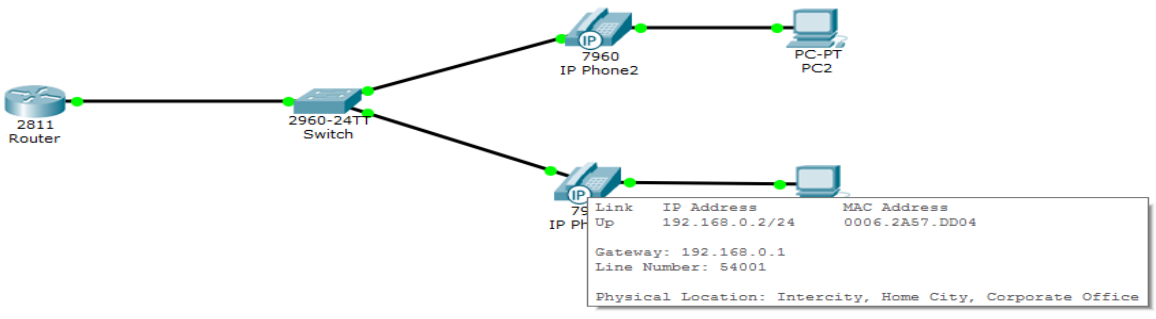


Figure IV .10 : schéma de réseau VOIP configuré

Nous voyons donc qu'une adresse IP a été distribué en dessous de « IP Address » (notez là elle nous resservira) et qu'un numéro de téléphone a été associé à côté de « Line Number » (notez là également). Si les deux IP Phones sont configurés comme prévu nous pouvons continuer.

-Septième étape : Attribution des adresses IP des PC par le serveur DHCP.

Maintenant une des dernières étapes est de prévenir nos ordinateurs qu'ils peuvent obtenir leurs adresses IP grâce au serveur DHCP. Pour cela il suffit de cliquer sur l'ordinateur en question,

Dans l'onglet « Desktop » puis « IP Configuration » vous cocher DHCP.

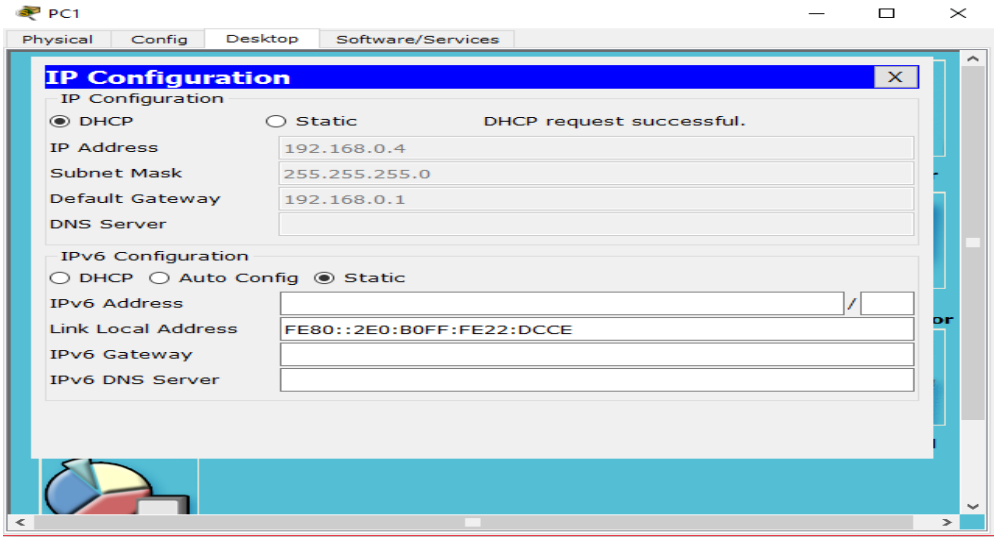


Figure IV. 11: IP configuration

Lorsque vous cochez DHCP, votre ordinateur envoie une requête au serveur afin de recevoir son adresse IP. Attendez quelques secondes puis vous devriez voir apparaitre « DHCP request successful ». Faites de même avec vos autres machines disponibles sur le réseau.

-*Huitième étape* : Expérimenter le bon fonctionnement.

Maintenant que votre réseau basique est configuré, nous allons nous assurer que le tout fonctionne correctement.

Commençons par passer un appel depuis le téléphone 1 vers le téléphone 2. Cliquons sur notre IP Phone 1, puis dans l'onglet « GUI » nous tapons le numéro du second IP Phone (pour savoir le numéro de destination, survolez le téléphone afin de voir dans la fiche de description son numéro, ici c'est 54002).

Quand vous avez tapes votre numéro il vous reste à décrocher afin de lancer l'appel.


```
Link    IP Address          MAC Address
Up      192.168.0.3/24      000B.BE78.7422

Gateway: 192.168.0.1
Line Number: 54002

Physical Location: Intercity, Home City, Corporate Office
```

Figure IV .12 : Les caractéristiques de configuration de Téléphone.

Figure IV .13 : « Ring Out » Contacte de téléphone

Il est bien indiqué « Ring Out » ce qui signifie que le second téléphone est contacté et qu'il sonne. Maintenant allons sur l'interface IP Phone 2 pour recevoir l'appel en décrochant de la même manière.

La lumière rouge du téléphone clignote et l'écran nous indique un appel provenant de 54001 (donc l'IP Phone 1). On décroche, et on voit apparaitre « Connecte » sur l'écran du téléphone. On peut ensuite raccrocher.

Le service de téléphonie est donc fonctionnel puisque les appels sont envoyés et reçus avec succès.

Il ne nous reste plus qu'à vérifier si les ordinateurs sont capables de communiquer, nous allons donc le voir avec la commande « PING ». Pour cela il faut cliquer sur l'ordinateur 1 puis dans l'onglet « Desktop » choisir « Command Prompt ». Une fois le terminal ouvert tapez simplement « ping [adresse ip de destination] ». Utilisez donc l'IP du second PC que vous avez relevé au préalable puis fait Entrée.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.5

Pinging 192.168.0.5 with 32 bytes of data:

Reply from 192.168.0.5: bytes=32 time=0ms TTL=128
Reply from 192.168.0.5: bytes=32 time=0ms TTL=128
Reply from 192.168.0.5: bytes=32 time=1ms TTL=128
Reply from 192.168.0.5: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Si le terminal vous renvoie ceci alors vos ordinateurs peuvent communiquer entre eux, nous avons donc réussi à établir un service téléphonique sur un réseau simple tout en permettant l'échange de données entre les machines du réseau [19].

4.3 Simulation réseau 02 (Scénario 02)

4.3.1 Réseau VoIP entre deux sites distants

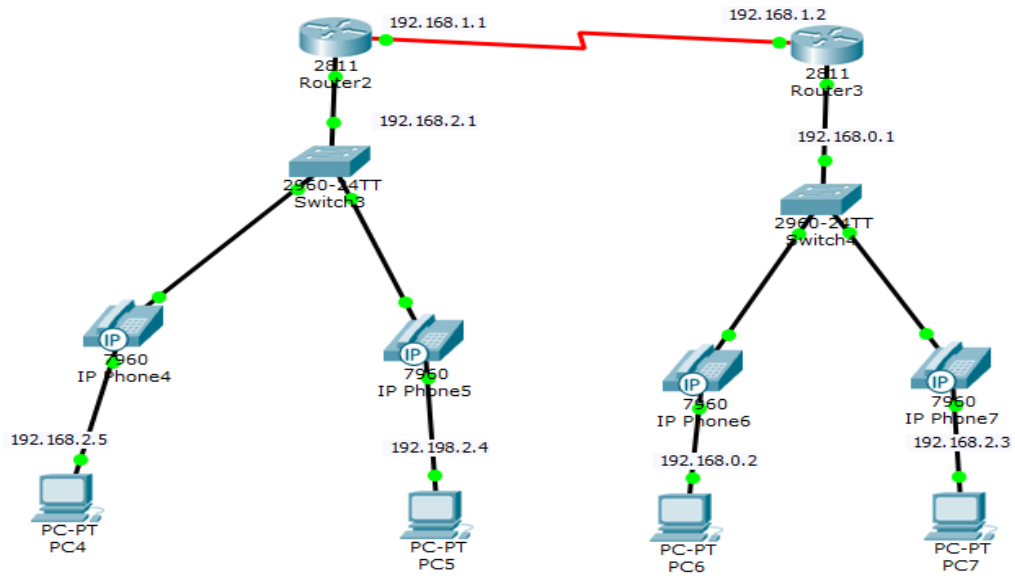


Figure IV.14 :schéma de réseau VOIP entre deux sites distants

Dans la figure ci-dessus il ya deux réseaux VOIP connecté ensemble, que nous utilisons des routeurs de type 2811 pour la simple raison que le seule type de routeur qui possède l'algorithme de cryptage avec le service de téléphonie qu'on peut les utilisés pour la configuration de réseau VoIP bien sûr en utilisant le protocole DHCP.

Nous écrivons toutes les lignes commandes pour la configuration de routeur dans la fenêtre CLI (Command Line Interface).

Pour configurer le réseau VOIP on doit utiliser la méthode DHCP. Avant la configuration, nous devons appuyer sur le pc et choisir le DHCP. (IP configuration DHCP).

Station	Adresse IP	Masque Réseau	Ports	Switch	Routeurs
PC-PT PC4	192.168.2.5	255.255.255.0	Fa0/1	2950-24	2811
PC-PT PC5	192.168.2.4	255.255.255.0	Fa0/2	2950-24	2811
PC-PT PC6	192.168.0.2	255.255.255.0	Fa0/1	2950-24	2811
PC-PT PC7	192.168.0.3	255.255.255.0	Fa0/2	2950-24	2811

Tableau**IV1 :** *Tableau Récapitulatif du réseau (Routeur / Switch / Stations)*

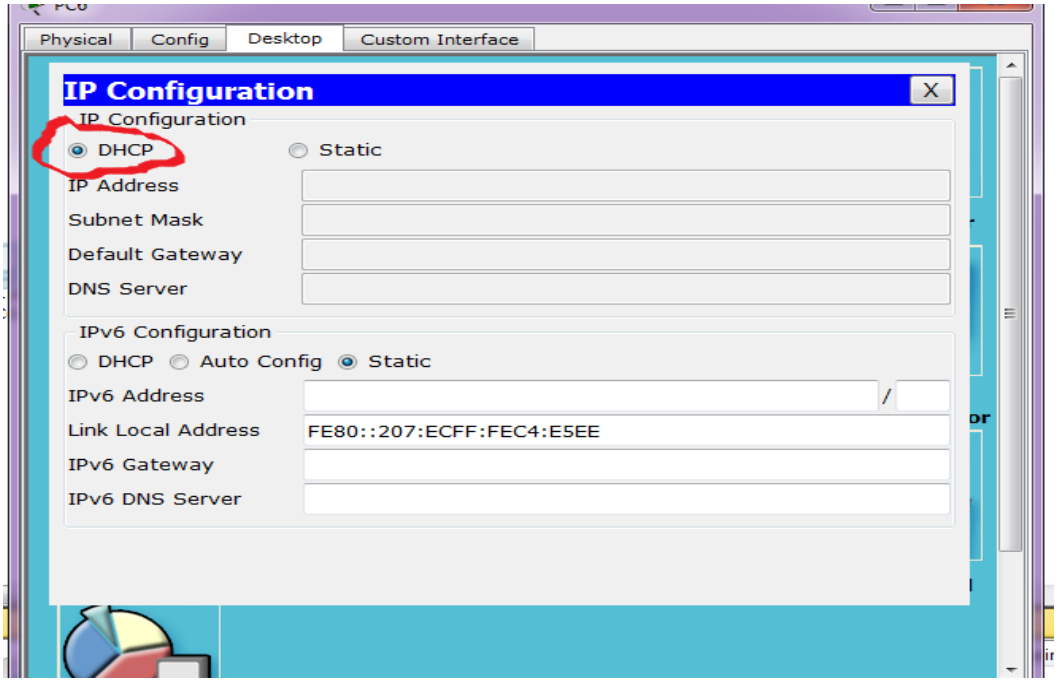


Figure IV.15 : I P configuration (DHCP)

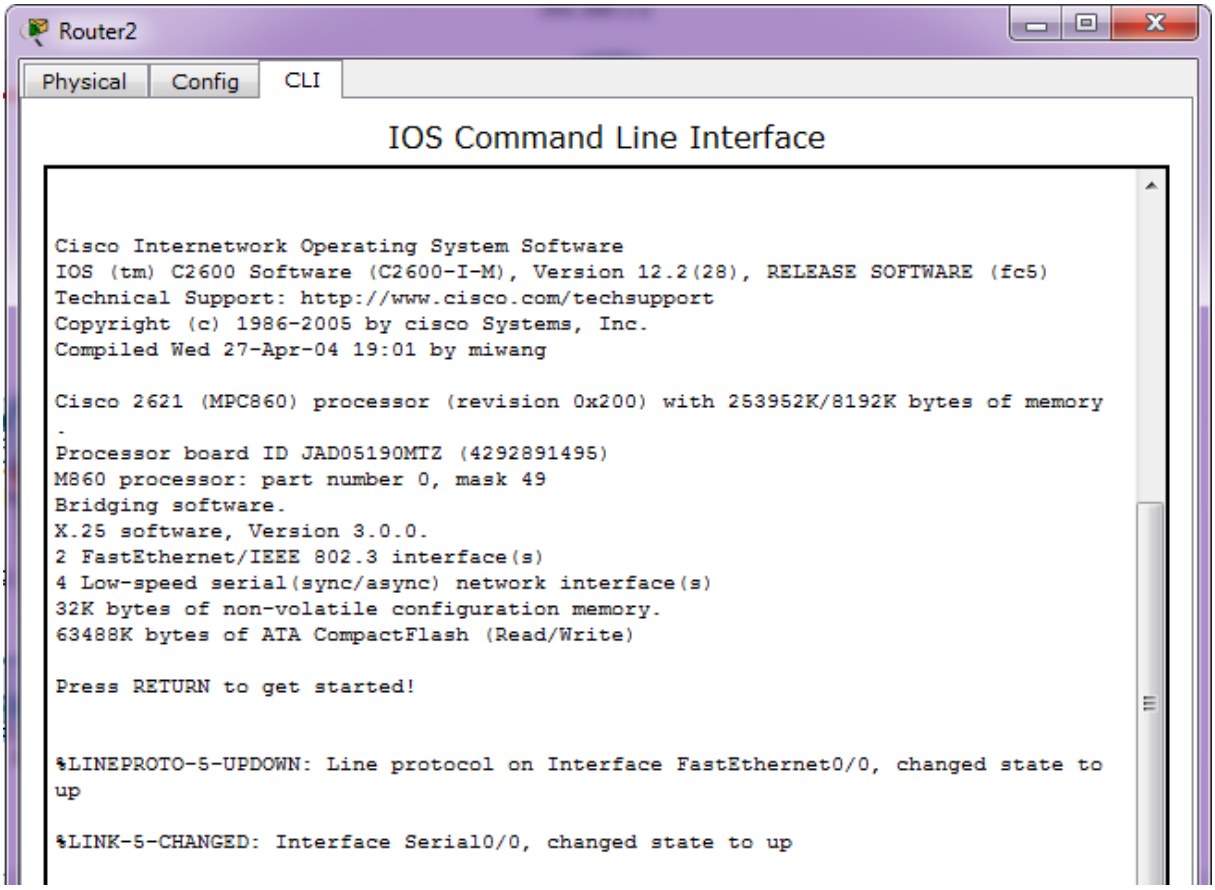


Figure IV.16 : ***exemple par*** **les commandes** ***CLI***

Apres avoir déterminé la DHCP sur tous les pc, nous allons maintenant discuter de l'application des étapes précédentes dans le premier réseau, et après avoir connecté les deux réseaux , nous verrons si le message passera d'un pc vers l'autre et d'un téléphone vers l'autre.

Commençons par serial 0/2/0

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial0/2/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Après interface f 0/0

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Puis nous créons et configurons le serveur DHCP utilisé pour distribué une adresse IP à chaque terminal IP du réseau [20].

Commençons par serial 0/2/0.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Configurer DHCP par interface fa0/0.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#option 150 ip 192.168.2.1
Router(dhcp-config)#exit
Router(config)#exit
Router#
```

Ensuite nous allons démarrer les IP Phones, en cliquant dessus nous allons brancher l'adaptateur secteur afin de l'alimenter (vous pouvez également utiliser des Switch POE Power Over Ethernet, afin de ne pas avoir à utiliser le secteur pour alimenter vos téléphones).

Apres la configuration de DHCP sur le router, Nous allons donc configurer Call Manager Express afin d'activer le support VOIP sur notre réseau.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#telephony-service
Router(config-telephony)#max-dn 5
Router(config-telephony)#max-ephones 5
Router(config-telephony)#ip source-address 192.168.0.1 port 2000
Router(config-telephony)#auto assign 4 to 6
Router(config-telephony)#auto assign 1 to 5
Router(config-telephony)#exit
Router(config)#
```

Et après, Nous allons configurer les interfaces du Switch afin de séparer les données.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range FastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 1
Switch(config-if-range)#exit
Switch(config)#
```

Les téléphones sont connectés et le réseau configuré, seulement il faut ajouter une configuration supplémentaire afin de leur permettre de communiquer.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 10000
Router(config-ephone-dn)#
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 20000
Router(config-ephone-dn)#
```

Maintenant une des dernières étapes est de prévenir nos ordinateurs qu'ils peuvent obtenir leurs adresses IP grâce au serveur DHCP.

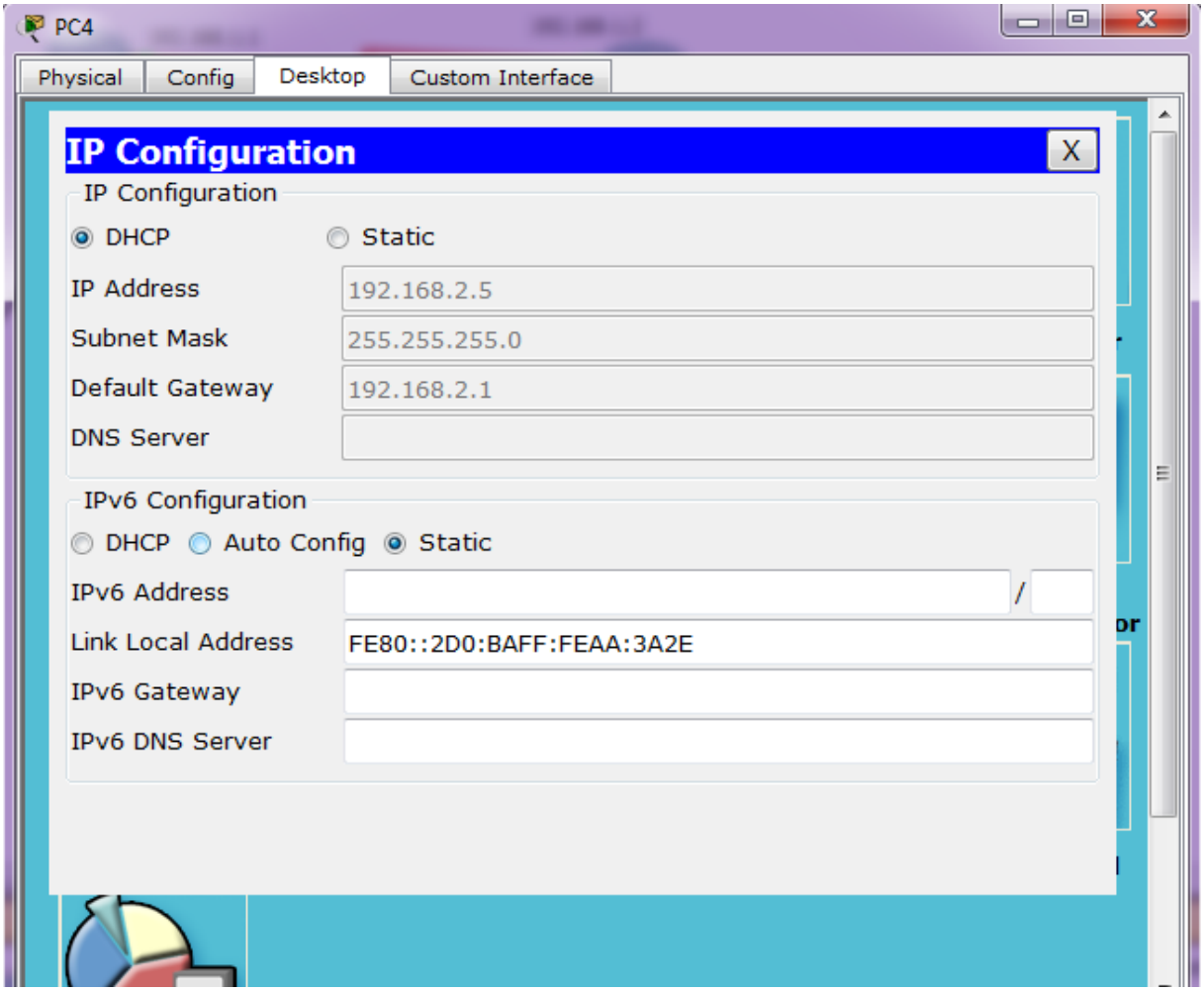


Figure IV.17 : La configuration DHCP

Lorsque vous cochez DHCP, votre ordinateur envoie une requête au serveur afin de recevoir son adresse IP.

On doit utiliser les mêmes étapes pour la configuration de deuxième réseau VOIP.

Nous concluons qu'il existe une connexion entre les deux réseaux Grace au routeur 2811, qui joue un rôle très important dans l'établissement de la liaison VOIP.

L'avantage de l'utilisation et l'application des VOIP avec le protocole -DHCP dans un réseau constitué des Routeurs et des Switches réside dans la capacité des PC connectés qui ne dépasse pas la capacité des ports constituant le switch et dans la facilité du control de ce réseau avec des adresses IP différentes et c'est robuste à contrôlés ainsi rapide.

Chaque périphérique sur un réseau informatique doit avoir sa propre adresse de protocole Internet unique, permettant aux routeurs et commutateurs réseau pour envoyer des données à l'ordinateur spécifique la demande. Un nouvel utilisateur au réseau peut entrer son adresse IP manuellement, ou le protocole de configuration d'hôte dynamique ou DHCP, un serveur peut attribuer une adresse IP à l'ordinateur automatiquement.

4.4 Simulation réseau 03 (Scénario 03)

4.4.1 Réseau VPN

4.4.2 Configuration VPN du routeur CISCO :

Nos sites ont besoin d'une connexion WAN entre leur siège et les agences du réseau, nous allons donc crée une liaison tunnel IPSEC.

IP sec est un protocole VPN qui fonctionne sur la couche 3 du modèle OSI, C'est aussi un standard de la norme IETF.

- **Rappel :**

Les VPN IPSEC permettent :

-Une vérification de l'intégrité des données de chaque paquet.
-De rendre confidentiels les données de chaque paquet IP.
-Une authentification de chaque paquet.

Le scénario ci-dessous contient trois sites distants à des adresses IP publique statique, comme indiqué dans le scénario.
R1 est configuré avec 192.168.7.1/24 et R2 avec l'adresse IP 192.168.9.1/24.
À partir de maintenant, les deux routeurs ont une configuration très basique telle que adresses IP, NAT overload, route par défaut, noms d'hôte, connexions SSH, etc.
Chaque site étant une image d'un petit réseau disposant d'un accès à internet, la configuration se fera en 02 étapes :

❖ Configuration du routage pour que les deux réseaux puissent communiquer.

❖ Configuration du VPN.

La configuration du routage pour que les deux réseaux puissent communiquer
Avant de commencer à configurer le VPN IP SEC, toujours s'assurer que les deux routeurs peuvent se joindre.

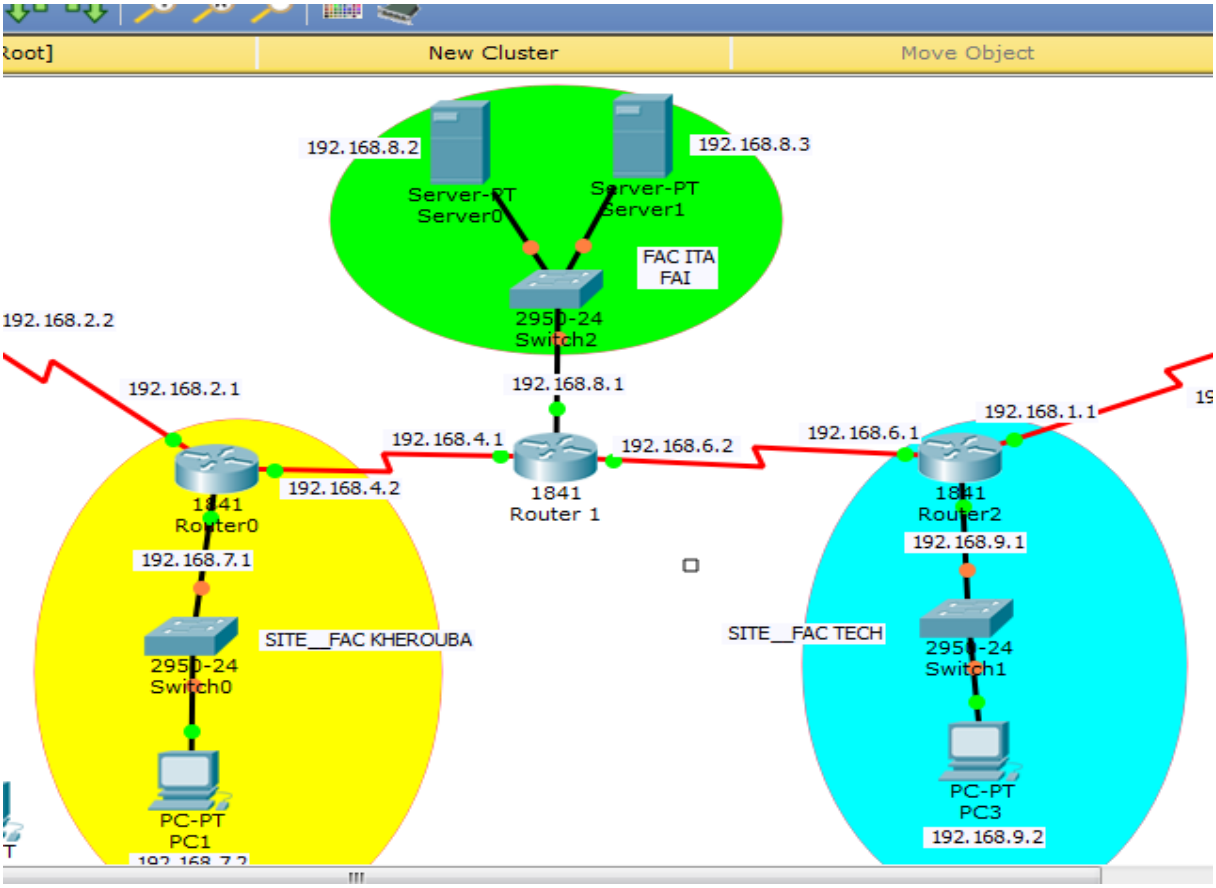


Figure IV.18 : Schéma de réseau contient 03 sites

4.4.3 LA CREATION DU RESEAU VPN :

Nos sites ayant besoin d'une connexion WAN entre son siège et ses succursales basées à l'intérieur du réseau, nous allons créer une liaison avec un tunnel IP SEC.
IP Sec est un protocole VPN qui fonctionne sur la couche 3 du modèle OSI.
C'est aussi un standard IETF, ce qui signifie que nous pouvons l'utiliser entre les équipements de différents fabricants.

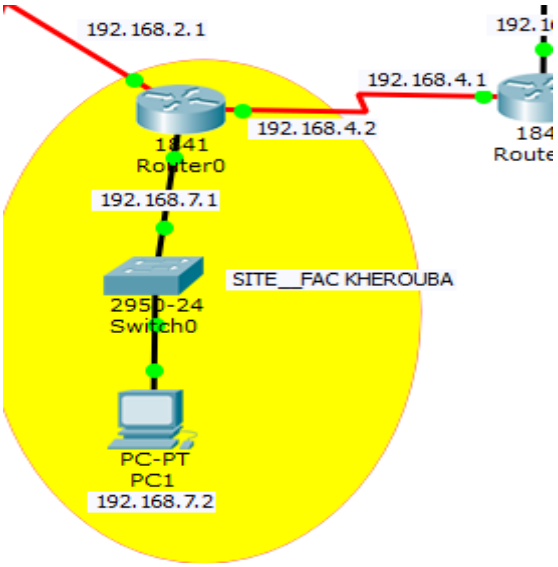
Notre thème se base sur la création du réseau VPN IP SEC, en suivant le choix des matériels et appareils pour crée ce réseau.

Notre réseau contient 03 sites (jaune, vert, bleu) sites que nous avons configurés de la manière décrite ci-dessous.

Station	Adresse IP	Masque Réseau	Ports	Switch	Routeurs
PC-PT PC1	192.168.7.2	255.255.255.0	Fa0/1	2950-24	1841
PC-PT PC3	192.168.9.2	255.255.255.0	Fa0/1	2950-24	1841
Server-PT Server 0	192.168.8.2	255.255.255.0	Fa0/1	2950-24	1841
Server-PT Server 1	192.168.8.3	255.255.255.0	Fa0/1	2950-24	1841

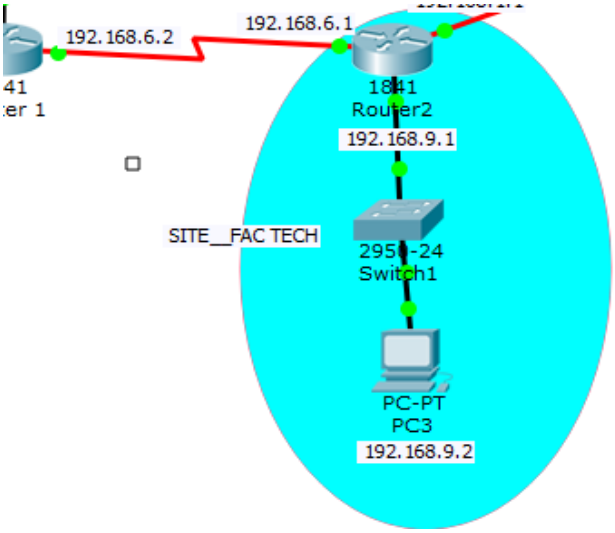
Tableau **IV2 :** *Tableau Récapitulatif du réseau (Routeur / Switch / Stations)*

❖ **Site jaune correspondant au site de la faculté KHAROUBA:**



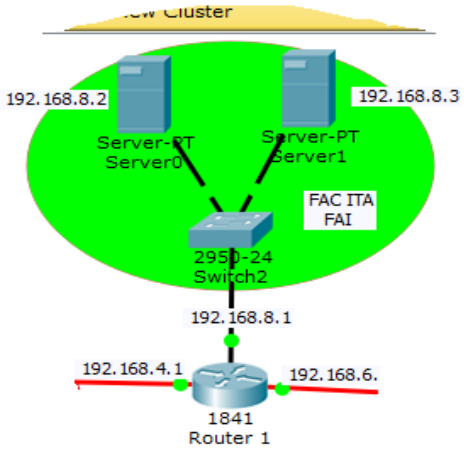
Réseau : 192.168.7.1.
PC1: 192.168.7.2.
Router : 192.168.4.2. (Serail0/0/0)
192.168.7.1. (Fast Ethernet 0/1).
Le masque de réseau: 255.255.255.0

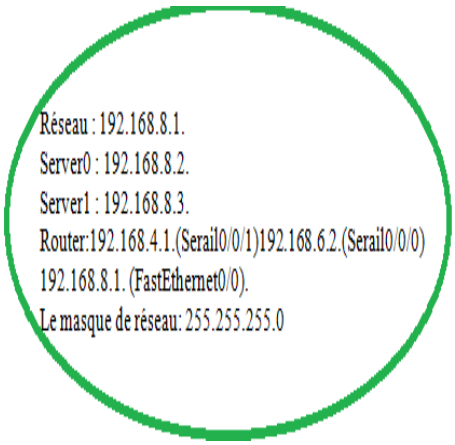
❖ **Site bleu correspondant au site de la faculté TECH :**



Réseau : 192.168.9.1.
PC : 192.168.9.2.
Router : 192.168.6.1. (Serail0/0/0)
192.168.9.1. (Fast Ethernet 0/1).
Le masque de réseau: 255.255.255.0

❖ **Le site vert correspondant à la faculté ITA :**





4.4.4 Configuration de base des routeurs (KHEROUBA-FAI-ITA-FACTECH) [20-21-22] :

* Configuration des **interfaces WAN et LAN (KHEROUBA)**

```
Router (config)#hostname KHEROUBA
KHEROUBA (config)#interface s0/0/0
KHEROUBA (config-if)# ip address 192.168.4.2 255.255.255.0
RSIEGE (config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
KHEROUBA (config-if)#exit
```

* Configuration des **interfaces WAN (FAI-ITA)**

```
FAI-ITA#configure terminal
FAI-ITA (config)#interface s0/0/1
FAI-ITA (config-if)#ip addresse 192.168.4.1   255.255.255.0
FAI (config-if)#no shut
FAI-ITA (config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
FAI-ITA (config-if)#exit
FAI-ITA (config)#interface s0/0/0
FAI-ITA (config-if)#ip addresse 192.168.6.2 255.255.255.0
```

* Configuration de **l'interface WAN et LAN (FAC TECH) [20-21-22]:**

```
FAC TECH(config)#interface s0/0/0
FAC TECH (config-if)#ip address 192.168.6.1 255.255.255.0
RTAABO(config-if)#no shutdown
FAC TECH (config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
FACTECH (config-if)#exit
FAC TECH (config)#interface g0/0
FAC TECH (config-if)#ip address 192.168.2.254 255.255.255.0
RTAABO(config-if)#no shut down
FAC TECH (config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state toup
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
FAC TECH (config-if)#exit
```

Configuration de la route par défaut, routeurs (KHEROUBA-FAI-FACTECH) [22]:

Configuration des **routes sur routeur (FAC TECH)**

```
FAC TECH (config)#IP route 0.0.0.0 0 .0.0.0 192.168.6.2
```

Configuration des **routes sur routeur (FAI)**

```
FAI (config)#IP route 0.0.0.0 0. 0.0.0 192.168.6.1

FAI (config)#IP route 0.0.0.0 0. 0.0.0 192.168.4.2
```

Configuration des **routes sur routeur (KHEROUBA)**

```
KHEROUBA (config)#IP route 0.0.0.0 0. 0.0.0 192.168.4.1
```

Maintenant que le routage s'est bien passé nous allons sécuriser le réseau.

- ✓ **Mise en place d'un VPN IPSec :**

Il faut suivre 06 pour configurer un VPN :

• Définir la politique **ISAKMP (IKE Phase1:** Méthode de chiffrement, durée de vie, méthode d'intégrité, ce qui va permettre de définir *une IKE Security Association*).
• Créer la **clé partagée**
• Créer une **transform-set (IKE Phase2:** Nous allons configurer les politiques de sécurité Ise «protocole esp, vérifier le type de liaison »afin d'avoir *un IPSec Security Association*).

• Mettre en place une **ACL (qui définira quel trafic peut/doit emprunter le VPN)**

• Créer un crypto **map**
• Appliquer le crypto map à l'**interface de sortie du routeur**

- **Configuration du routeur site 1 (Routeur KHEROUBA) [20-21-22]:**

On s'assure tout d'abord que l'IOS de notre routeur supporte le VPN à travers la commande « Sh version» en mode configuration ou faire une MAJ de l'IOS vers un /K9, ensuite nous entamons **la première partie** qui consiste à configurer la politique c'est-à-dire qu'elle encryption on utilise, qu'elle hash quel type d'authentification.

```
KHEROUBA(config)#crypto isakmp enable
KHEROUBA (config)#crypto isakmp policy 1
KHEROUBA (config-isakmp)#encryption aes
KHEROUBA (config-isakmp)#hash md5
KHEROUBA (config-isakmp)#authentication pre-share
KHEROUBA (config-isakmp)#group 2
KHEROUBA (config-isakmp)#lifetime 86400
KHEROUBA (config-isakmp)#exit
```

Étape1. Définition de la politique **ISAKMP.**

Voici les détails de chaque commande utilisée :

Crypto isakmp Policy 1-Cette commande crée la stratégie ISAKMP numéro 1. Nous pouvions créer plusieurs stratégies,

Authentication pre-Sare - La **méthode d'authentification** est la clé pré-partagée.

Encryptions 3aes - L'algorithme de cryptage 3AES **(Advanced Encryptions Standard)** Sera utilisé **pour la confidentialité**.

Hash md5 - L'algorithme de hachage md5 sera utilisé **pour l'intégrité**.
group 2 – Méthode de distribution des clés partagées DH-2. Le **groupe Déifie-Helpmann** Utilisé ici est le groupe 2 pour la **méthode d'échange des clés**.
Lifetime 86400 – Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

Toujours dans la première partie, nous créons la clé partagée.

Étape 2. Création de **la clé de partage**

```
KHEROUBA (config)#crypto isakmp key cisco@123 address 192.168.6.1
```

Crypto isakmp key cisco@123 address 192.168.6.1- On crée ainsi **la clé pré-partagée**, ici *«cisco@123»* qu'on associe avec l'adresse IP de l'homologue à l'autre bout du tunnel ici 192.168.6.1

On définit par ailleurs si on doit identifier le routeur par son adresse ou par son hostname (ici on choisit l'adresse publique fixe), l'identification par hostname peut être utile si on fonctionne avec une adresse publique dynamique, ce qui permet d'éviter trop de modifications de configuration en cas de changement d'adresse.

La deuxième partie :

Elle consiste à définir **comment les données seront cryptées**. Tout d'abord on crée la méthode de cryptage (transform-set) que l'on nomme ici vpnset.

Étape3. Création d'une **transforme-set**

```
KHEROUBA (config)#crypto ipsec transform-set vpnset esp-aes esp-md5-hmac
KHEROUBA (cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 3600
KHEROUBA (cfg-crypto-trans)#exit
```

Le détail de la commande utilisée :

• **Crypto IP sec transforme-set VPN set –** Crée un ensemble de transformation appelé VPN set
• **esp-Aes–** la méthode de cryptage AES et le protocole ESP IPSec seront utilisés.
• **esp-md5-hamac**- L'algorithme de hachage MD5 sera utilisé.
• **Crypto IP sec Security-association life time seconds-** Il s'agit de la durée de vie de la clé de cryptage.

Étape4. Configuration de la liste de **contrôle d'accès étendu pour un trafic intéressant (ACL).**

Nous créons la crypto ACL qui est une ACL qui va identifier le trafic «intéressant» c'est-à-dire le trafic qui doit passer par le tunnel VPN (ici c'est le trafic depuis le LAN KHEROUBA vers le LAN FAC TECH **[15],** ça sera l'inverse sur l'autre routeur). Le trafic permit par cette ACL sera chiffré dans le tunnel IPSEC, le reste non…On crée donc une Access-List étendue.

```
KHEROUBA (config)#ip access-list extended vpn-traffic
KHEROUBA (config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255
KHEROUBA (config-ext-nacl)#exit
```

Cette ACL définit le trafic qui doit passer par le tunnel VPN. Ici, le trafic en provenance du réseau 192.168.1.0 vers le réseau 192.168.2.0 sera acheminé via le tunnel VPN.
Cette ACL sera utilisé à l'étape 5 de Crypto Map.

Étape5. Configuration de **Crypto Map.**

Nous créons la crypto map qui définit le chemin qu'emprunte notre tunnel avec : La politique IPSec, l'adresse IP du routeur distant avec lequel on veut communiquer, la crypto ACL et le transform-set pour la politique IPSec.

```
KHEROUBA (config)#crypto map IPSEC-VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
KHEROUBA (config-crypto-map)#set peer 192.168.6.1
KHEROUBA (config-crypto-map)#match address vpn-traffic
KHEROUBA (config-crypto-map)#set transform-set vpnset
```

Voici les détails de chaque commande utilisée ci-dessus **[22]:**

IPsec-isakmp – Crée une nouvelle carte de chiffrement avec le numéro de séquence 10.
Set Peer 192.168. 6.1 Associe l'IP destination, ici l'adresse IP publique de FAC TECH

Match address VPN-traffic – Associe l'ACL précédemment crée et nommé **VPN-traffic**.

Settransform-set VPNset – Ceci relie le transforme-set à la configuration de la crypto map.

Étape 6. Application de la Crypto map à l'interface sortante de KHEROUBA

La configuration de KHEROUBA est presque terminée nous devons appliquer la crypto map sur L'interface de sortie de ce routeur, dans notre cas s0/0/0.

```
KHEROUBA (config)#int s0/0/0

KHEROUBA (config-if)#crypto map IPSEC-VPN

*Mar119:16:14.231: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Un message vous indique que la crypto map fonctionne.

Étape7. Exclue **le trafic VPN du NAT Overload**

```
KHEROUBA (config)#ip access-list extended 101

KHEROUBA (config-ext-nacl)#deny ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255

KHEROUBA (config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255
any RSIEGE(config-ext-nacl)#exit

KHEROUBA (config)#ip nat inside source list 101 interface S0/0/0 overload
```

Au-dessus de l'ACL101, le trafic intéressant sera exclu du NAT.

La configuration est la même que pour le Routeur Siège à certaines exceptions :

- **Configuration du routeur site 2 (Routeur FAC TECH) [20-21-22]:**

Dans l'ACL «vpn-traffic» on doit inverser l'adresse IP de l'hôte source et de l'hôte de destination
• Dans la définition du transform-set on doit changer l'adresse du peer en mettant l'adresse IP de KHEROUBA.
• Dans l'ACL CRYPTO ACL on doit inverser le réseau source et le réseau de destination
• Dans la crypto map on doit mettre comme adresse du peer l'adresse IP de KHEROUBA.
La configuration est la même que pour le Routeur Siège à certaines exceptions :
Nous allons répéter les étapes de KHEROUBA à l'identique sur le routeur FAC TECH à l'exception de l'Access-List qui doit être inversé au vu de la source et de la destination.

Étape1. Définition de la politique **ISAKMP.**

```
FAC TECH(config)#crypto isakmp enable
FAC TECH (config)#crypto isakmp policy 1
FAC TECH (config-isakmp)#encryption aes
FAC TECH (config-isakmp)#hash md5
FAC TECH (config-isakmp)#authentication pre-share
FAC TECH (config-isakmp)#group 2
FAC TECH (config-isakmp)#lifetime 86400
FAC TECH (config-isakmp)#exit
```

Étape2. Création de **la clé de partage.**

```
FAC TECH (config)#crypto isakmp key cisco@123 address 192.168.4.2
```

Étape3. Création d'une **transforme-set.**

```
FAC TECH (config)#crypto ipsec transform-set vpnset esp-aes esp-md5-hmac FAC
TECH (cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 3600
```

Étape4. Configuration de la liste de **contrôle d'accès étendu pour un trafic intéressant (ACL).**

```
FAC TECH (config)#ip access-list extended vpn-traffic

FAC TECH (config-ext-nacl)#permit ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
```

Étape5. Configuration de **Crypto Map.**

```
FAC TECH (config)#crypto map IPSEC-VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
FAC TECH (config-crypto-map)#set peer 192.168.4.2
FAC TECH (config-crypto-map)#match address vpn-traffic
FAC TECH (config-crypto-map)#set transform-set vpnset
```

Étape6. Application de la Crypto Map à l'interface sortante de FAC TECH.

```
FAC TECH (config)#int s0/0/0

FAC TECH (config-if)#crypto map IPSEC-VPN

*Mar 1 19:46:10.123: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Étape7. Exclue **le trafic VPN du NATO overload.**

```
FAC TECH (config)#ip access-list extended 101
FAC TECH (config-ext-nacl)#deny ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
FAC TECH (config-ext-nacl)#permit ip 192.168.9.0 0.0.0.255 any
FAC TECH (config-ext-nacl)#exit
FAC TECH (config)#ip nat inside source list 101 interface S0/0/0 overload
```

VERIFICATION ET TEST :
Pour tester la connexion VPN, nous envoyons tout d'abord une **requête ping de PC KHEROUBA à PC FAC TECH.**

```
PC>ping 192.168.9.2

Pinging 192.168.9.2 with 32 bytes of data :

Reply from 192.168.9.2: bytes=32  time=2ms  TTL=126
Reply from 192.168.9.2: bytes=32  time=7ms  TTL=126
Reply from 192.168.9.2: bytes=32  time=2ms  TTL=126
Reply from 192.168.9.2: bytes=32  time=2ms  TTL=126

Ping statistics for 192.168.9.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms,  Maximum = 7ms, Average= 3ms
```

Pour vérifier la connexion IP Sec Phase 1, on tape **«show crypto isakmp sa»** comme indiqué.
Vous aurez ce qui y est dessous :

```
KHEROUBA#show crypto
isakmp sa IPv4 Crypto ISAKMP
SA                                  state       conn-id  slot    status
192.168.4.2         192.168.6.1     QM_IDLE      1026      0     active
------------------------------------------------------------------------------------------
FAC TECH#show crypto isakmp
sa IPv4 Crypto ISAKMP SA
Dst                 src             state       conn-id  slot    status
192.168.6.1         192.168.4.2     QM_IDLE      1026      0     active
```

QM_IDLE : Signifie que le Tunnel est bien monté.
Pour vérifier la connexion IP Sec Phase 2, On tape **«show crypto IP sec sa»** comme indiqué :

```
KHEROUBA#show crypto ipsec sa

interface: Serial0/0/0
Crypto map tag: IPSEC-VPN, local addr 192.168.4.2
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.7.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.9.0/255.255.255.0/0/0)
current_peer 192.168.6.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
.....

local crypto endpt.: 192.168.4.2, remote crypto endpt.:160.120.6.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x133B6163(322658659)

inbound esp sas:
spi: 0x49363F4A(1228291914)
transform: esp-aes esp-md5-hmac ,
in use settings ={Tunnel, }
.....
Status: ACTIVE
-----------------------------------------------------------------------------------------------------------
```

```
-----------------------------------------------------------------------------------------------------------

FAC TECH#show crypto ipsec
sa interface: Serial0/0/0
Crypto map tag: IPSEC-VPN, local addr 160.120.6.1
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.9.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.7.0/255.255.255.0/0/0)
current_peer 192.168.4.2 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
.....
local crypto endpt.: 192.168.6.1, remote crypto endpt.:192.168.4.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x49363F4A(1228291914)

inbound esp sas:
spi: 0x133B6163(322658659)
transform: esp-aes esp-md5-hmac ,
in use settings ={Tunnel, }
.....
Status: ACTIVE
```

Puis vous tapez :

Sh crypto ipsec sa

```
R #sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: IPSEC-VPN, local addr 192.168.6.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.9.0/255.255.255.0/0
  remote  ident (addr/mask/prot/port): (192.168.7.0/255.255.255.0/
  current_peer 192.168.4.2 port 500
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
  #pkts decaps: 2, #pkts decrypt: 2, #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 0

    local crypto endpt.: 192.168.6.1, remote crypto endpt.:192.168
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
    current outbound spi: 0x23DF55E9(601839081)

    inbound esp sas:
     spi: 0x287F37AA(679425962)
       transform: esp-aes esp-md5-hmac
       in use settings ={Tunnel, }
       conn id: 2002, flow_id: FPGA:1, crypto map: IPSEC-VPN
       sa timing: remaining key lifetime (k/sec): (4525504/3526)
       IV size: 16 bytes
       replay detection support: N
       Status: ACTIVE
```

Pour vérifier la crypto map, on tape «show crypto map» sur chacun des routeurs comme indiqué.

```
KHEROUBA#show crypto map
Crypto Map IPSEC-VPN 10 ipsec-isakmp
Peer = 160.120.145.178
Extended IP access list vpn-traffic
access-list vpn-traffic permit ip 192.168.7.0 0.0.0.255 192.168.9.0 0.0.0.255
Current peer: 192.168.6.1
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
vpnset,
}
Interfaces using crypto map IPSEC-VPN:
Serial0/0/0

---
FAC TECH#show crypto map
Crypto Map IPSEC-VPN 10 ipsec-isakmp
Peer = 192.168.6.1
Extended IP access list vpn-traffic
access-list vpn-traffic permit ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
Current peer: 105.235.19.10
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
vpnset,
}
Interfaces using crypto map IPSEC-VPN:
Serial0/0/0
```

Sur l'ordinateur PC-KHEROUBA nous faisons un «traceroute» vers PC-FAC TECH.

```
PC>tracert 192.168.9.1
Type escape sequence to abort.
Tracing the route to 192.168.7.1

Tracing route to 192.168.2.10 over a maximum of 30 hops:

1 0 ms 0 ms 0 ms 192.168.4.1  <= On voit ici l'IP de FAC TECH
2 2 ms * 1 ms 192.168.6.1

Trace complete.
```

Sur l'ordinateur PC-FAC TECH nous faisons un «traceroute» vers PC-KHEROUBA.

```
PC>tracert 192.168.7.1
Type escape sequence to abort.
Tracing the route to 192.168.7.1
Tracing route to 192.168.2.10 over a maximum of 30 hops:
1 192.168.6.2 1 msec 0 msec 1 msec
 2 192.168.4.2 1 msec 2 msec 2 msec <= On voit ici l'IP de FAC TECH


Trace complete.
```

4.5 Simulation réseau 04 (Scénario 04)

4.5.1 (Réseau VPN_+ Réseau VOIP _ final) :

Le réseau que nous allons étudier maintenant est une combinaison de deux réseaux étudiés précédemment, le réseau VPN et le réseau VoIP.

Autrement dit, au départ nous avons simulé le réseau VOIP, que nous vous l'avons expliqué son fonctionnement avec la numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Le signal numérique est plus tolérant au bruit que l'analogique.

Aussi en ce qui concerne le réseau VPN toute seul et expliqué toutes les étapes de configuration en implémentant les algorithmes de cryptage qui s'y appliquent, ainsi que le fonctionnement du ce réseau.

Maintenant on va raccorder les deux réseaux précédents, qui sont bien entendu le réseau VPN et le réseau VOIP, dans le même réseau globale pour arriver finalement à simuler le comportement des deux réseaux qui constituent notre étude qui y est basée sur la conception et la simulation d'une architecture réseau basée sur le VOIP dans un environnement VPN IP SEC multi site.

.

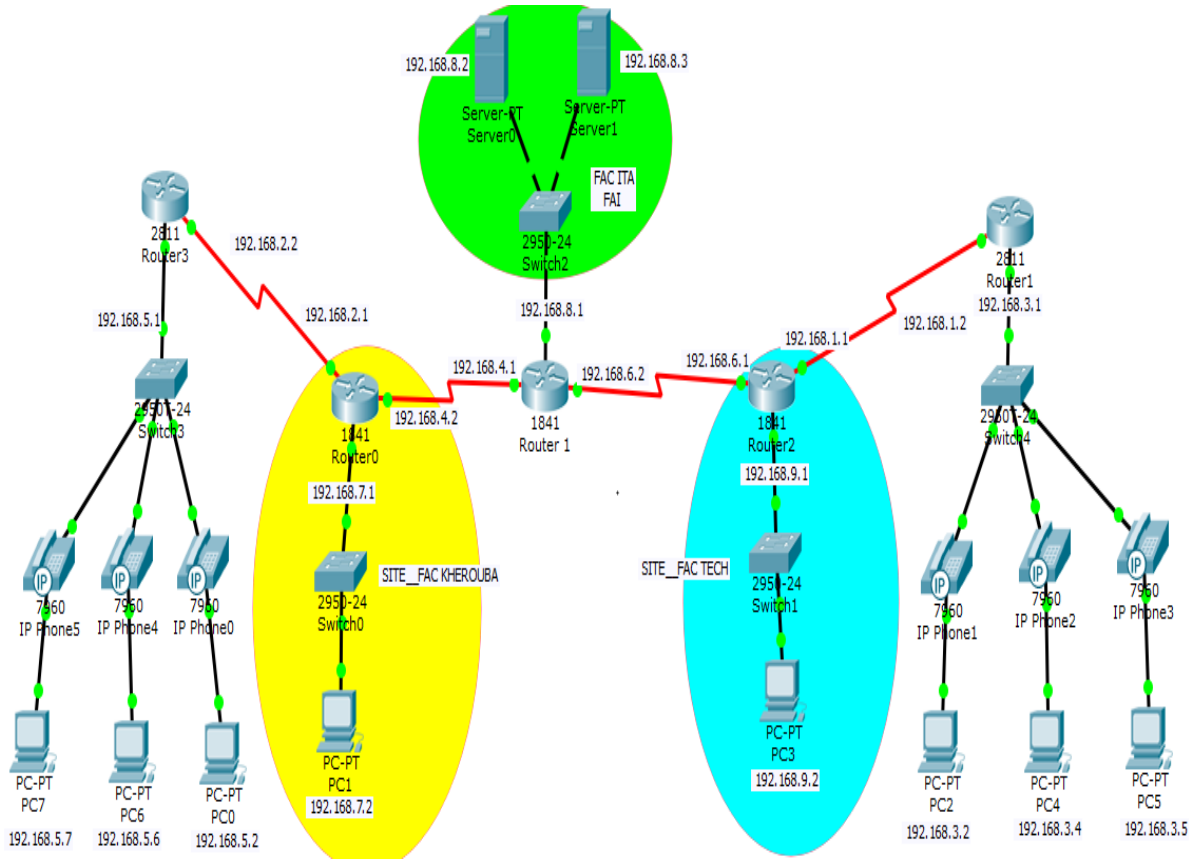


Figure IV.19: Schéma de réseau VPN+VOIP.

Station	Adresse IP	Masque Réseau	Ports	Switch	Routeurs
PC-PT PC0	192.168.5.2	255.255.255.0	Fa0/3	2950-24	2811
PC-PT PC 1	192.168.7.2	255.255.255.0	Fa0/1	2950-24	1841
PC-PT PC 2	192.168.3.2	255.255.255.0	Fa0/1	2950-24	2811
PC-PT PC 3	192.168.9.2	255.255.255.0	Fa0/1	2950-24	1841
PC-PT PC 4	192.168.3.4	255.255.255.0	Fa0/2	2950-24	2811
PC-PT PC 5	192.168.3.5	255.255.255.0	Fa0/3	2950-24	2811
PC-PT PC 6	192.168.5.6	255.255.255.0	Fa0/2	2950-24	2811
PC-PT PC 7	192.168.5.7	255.255.255.0	Fa0/1	2950-24	2811
Server-PT Server 0	192.168.8.2	255.255.255.0	Fa0/1	2950-24	1841
Server-PT Server 1	192.168.8.3	255.255.255.0	Fa0/1	2950-24	1841

Tableau **IV3 :** *Tableau Récapitulatif du réseau (Routeur / Switch / Stations)*

❖***Configuration de site 1:***

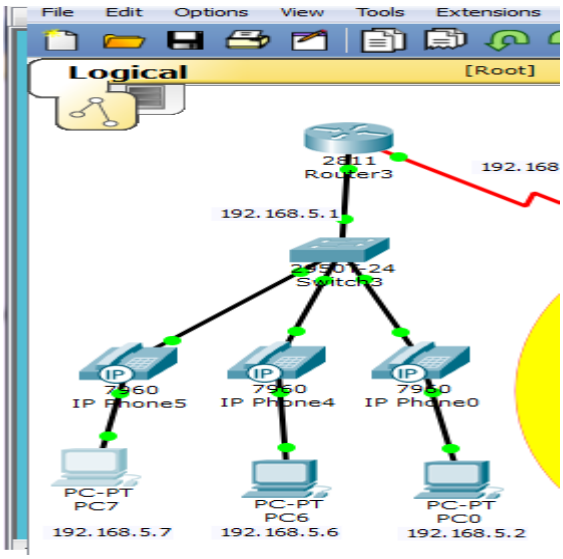


Figure IV.20 *: site 1*

- On commence par les adresses IP de chaque ordinateur : La configuration des ordinateurs ce fait *Par Desktop*, Dans ce cas en utilise la méthode DHCP, parce que le VOIP il fonctionne par la méthode de protocole DHCP.

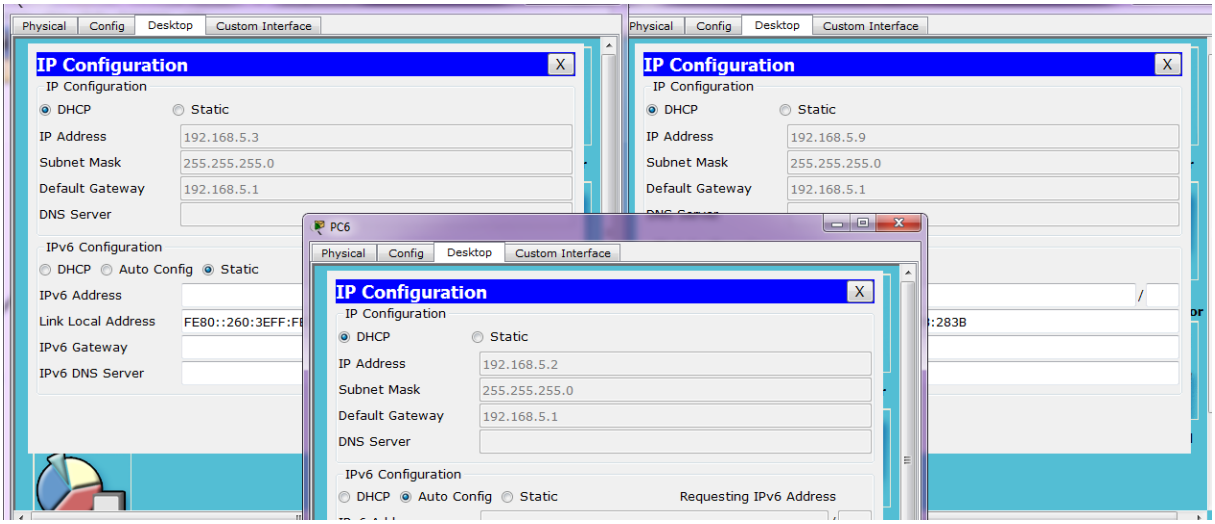


Figure IV.21 : exemple de DHCP

- ***Configuration de site 1:***

Pour configurer les Switch, on introduit les commandes suivantes sur la fenêtre de commande CLI (Command Line Interface).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range FastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 1
Switch(config-if-range)#exit
Switch(config)#
```

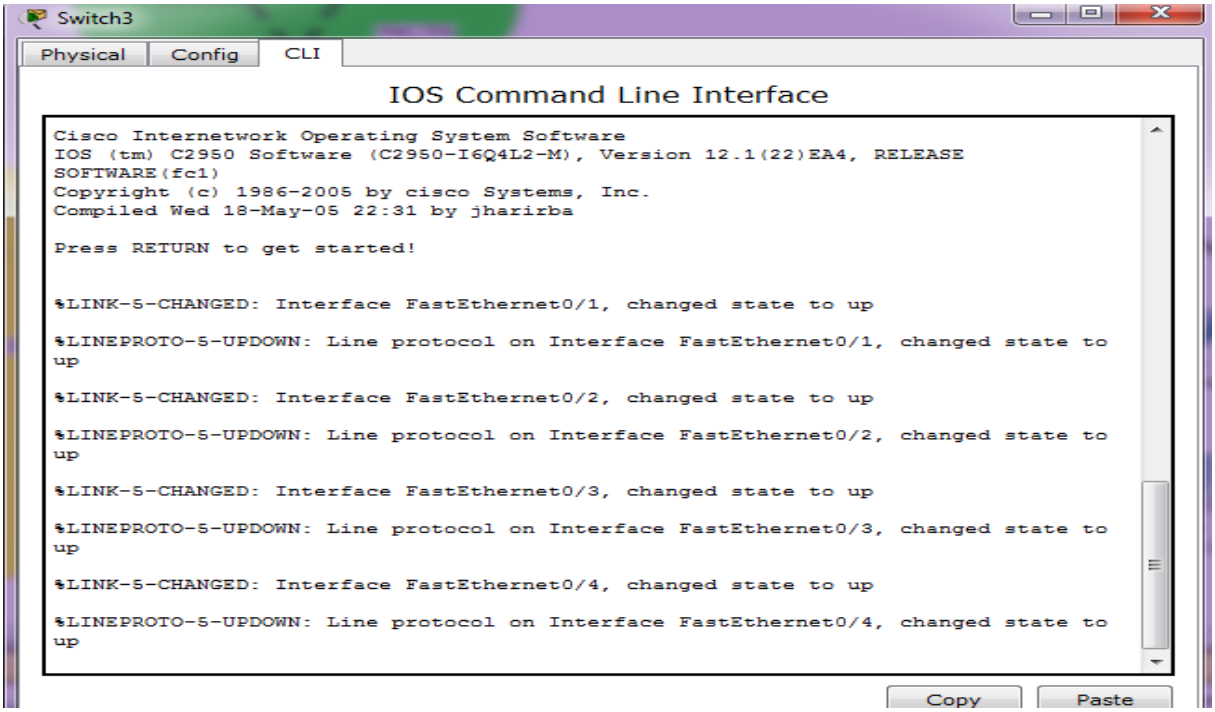
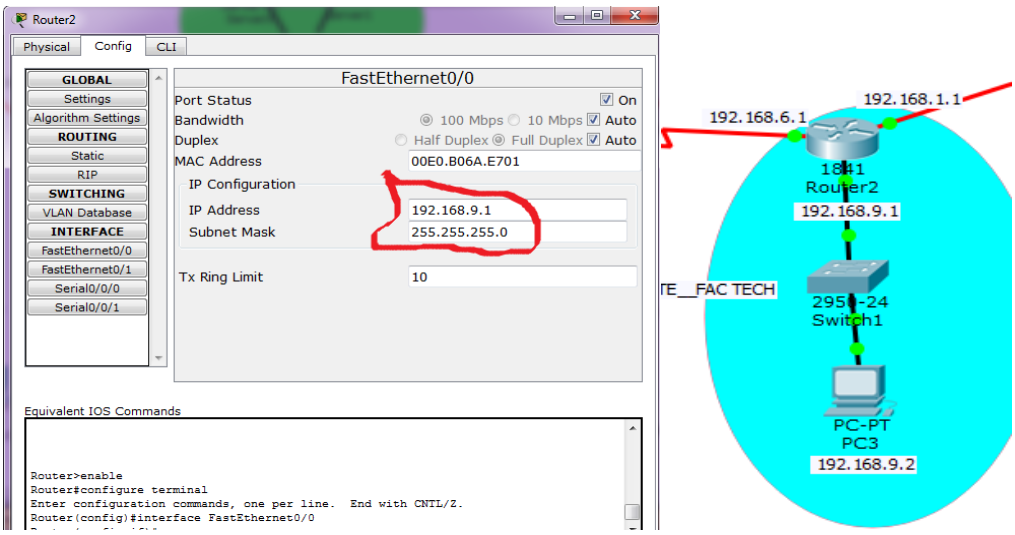


Figure IV.22 : Configure de Switch

- **Configuration des router :**

Il existe deux méthodes déférentes de configuration :

- **Configuration statique**
- **Configuration par commande CLI (Command Ligne Interface)**



Configuration des routeurs par la méthode statique.

.

- **Configuration par commande :**

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

Router(config-if)#exit
Router(config)#
```

➢ **Configuration des serveurs :**

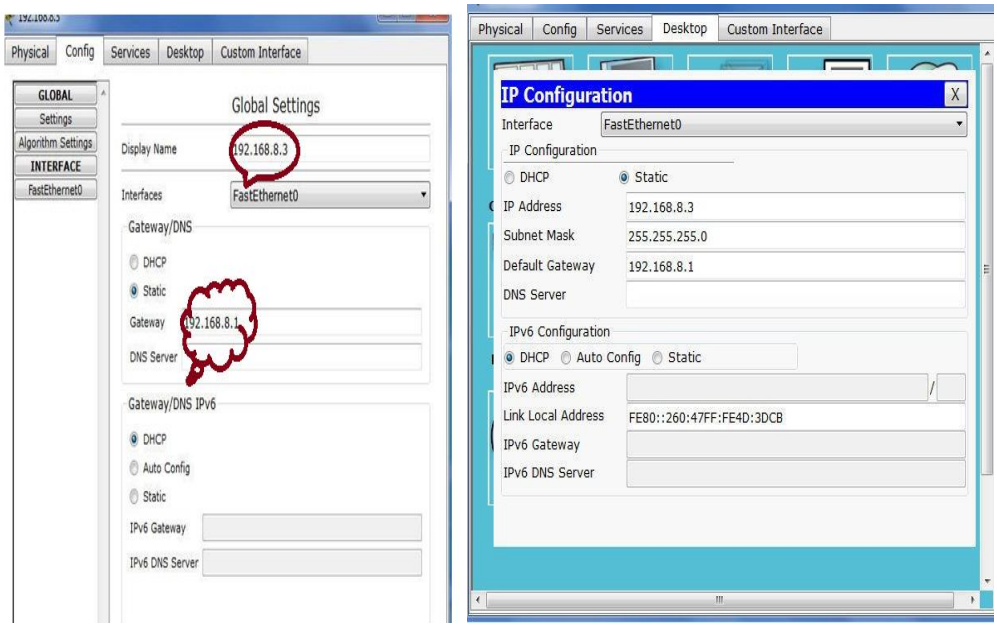


Figure IV.23: Configuration de server.

Comme vous remarquez que notre réseau est constitué de deux réseaux qui sont les suivants :

-1- Le premier réseau commence de Routeur 0 - Routeur 1 et le Routeur 2 (Ces 03 Routeurs sont de type 1841) et le carneau Tunnel (Liaison VPN) est placé entre le Routeur 0 et le Routeur 2.

-2- Le deuxième réseau VOIP est connecté entre les deux extrémités de réseau globale à droite comme à gauche, en utilisant des Routeurs de type **2811**

Remarque importante :

- **Les Routeurs de type 1841 sont destinés pour créer la liaison VPN entre deux points ou bien entre deux sites distants car ces routeurs disposent de certains algorithmes de cryptage avancés dans leurs boite noir.**
- **Les Routeurs de type 2811 sont destinés pour créer la liaison VOIP entre plusieurs points de même Nœud. Car ces routeurs disposent de service de téléphonie.**
- **On ne peut pas et jamais créer Un réseau VPN_VOIP avec le même type de Routeur, chaque Routeur a son rôle et son objectif principal.**

4.6.1 Résultats obtenus avec la technologie VoIP et VPN IP SEC:

Les résultats obtenus avec la technologie VoIP possède des avantages et des inconvénients. Parmi les avantages, nous citons :

- ***Gestion de la bande passante*** : Permet une bonne gestion de la bande passante en posant des limites au flux audio/vidéo afin d'assurer le bon fonctionnement des applications critiques sur le LAN. Chaque terminal peut procéder à l'ajustement de la bande passante et la modification du débit en fonction du comportement du réseau en temps réel.
- ***Support Multipoint*** : Permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.
- ***Support Multicast*** : Permet également de faire des transmissions en multicast.
- ***Interopérabilité :*** 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 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones…) qui peuvent partager selon le cas, de la voix de la vidéo et même des données.

4.6.2 Inconvénients de la technologie VoIP

- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la Convergence des services de téléphonie et d'Internet, ainsi qu'un manque de modularité et de souplesse comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes 'interopérabilité.

4.6.3 Résultats obtenus avec la technologie VPN :

Les résultats obtenus avec la technologie VPN possède des avantages et des inconvénients. Parmi les avantages, nous citons :

- ✓ L'accès du poste nomade (mobile) peut se faire de n'importe quel point de la planète doté d'un accès Internet.
- ✓ La transition des données entre le poste distant et le site central d'une façon sécurisée grâce à l'authentification.
- ✓ La transmission sécurisée des données, de voix et de vidéo entre deux ou plusieurs sites. À l'aide d'un certain nombre d'algorithmes de cryptage avancés pour assurer la confidentialité des données transmises.

4.6.4 Inconvénients de de la technologie VPN :

- ✓ Une installation logicielle est généralement nécessaire sur le poste distant.
- ✓ Le cryptage impose une charge non négligeable au poste distant, ce qui peut en dégrader les performances.
- ✓ Le cryptage n'est pas assuré au-delà du firewall du site central.

5. Conclusion :

Ce projet nous a permis de mieux appréhender les problèmes liés aux réseaux locaux dont ceux relatifs au déploiement d'un réseau VPN comprenant plusieurs sites distants tout en garantissant une qualité de service.

Notre étude est basée sur la création, la configuration et la simulation d'une architecture réseau basée sur le VOIP dans un environnement VPN IP SEC multi site.
Ce réseau est basé sur le transfert des données de la voix sur IP (VoIP) qui permet de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur Internet.

Le transfert des données de la voix sur IP (VoIP) est utilisée dans un environnement VPN IP sec de site à site sont utilisés pour permettre la transmission sécurisée des données, de voix et de vidéo entre deux ou plusieurs sites. À l'aide d'un certain nombre d'algorithmes de cryptage avancés pour assurer la confidentialité des données transmises entre les deux sites distants. 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». La technique consiste à utiliser Internet comme support de transmission en utilisant un protocole de tunnel, c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de VPN pour désigner le réseau ainsi artificiellement créé. Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent accéder aux données en clair.

Dans notre étude nous nous sommes appuyées sur la simulation et la discussion pour comprendre comment crées et configurer un tunnel VPN IP SEC avec un ensemble de commandes et mieux les mettre en œuvre, et la création de la liaison VOIP entre plusieurs points de même nœud. Le résultat de simulation que nous avons obtenu confirme la validité de l'étude, car le tunnel fonctionne bien en utilisant des routeurs de type 1841, et est également bien protégé, et la liaison VOIP fonctionnera bien avec des routeurs de type 2811.

Conclusion générale

Les vulnérabilités de la VoIP sont importantes et souvent intrinsèquement liées au réseau IP. L'audit a permis de déterminer ses vulnérabilités, les menaces adhérentes et les risques encourus. Parmi les solutions envisageables, l'implémentation d'une liaison VPN sécurisé permet de garantir l'authentification entre client et serveur, l'intégrité et la sécurité lors des communications. Au vu de ce travail, les vulnérabilités de la VoIP ne sont plus du domaine du vague mais plutôt un réel problème à considérer sérieusement. L'important désormais est de penser à l'intégration de la sécurité pendant le déploiement du réseau lui-même.
Les tunnels VPN IP sec de site à site sont utilisés pour permettre la transmission sécurisée de données, de voix et de vidéo entre deux ou plusieurs sites. Le tunnel VPN est créé sur le réseau public Internet et crypté à l'aide d'un certain nombre d'algorithmes de cryptage avancés pour assurer la confidentialité des données transmises entre les deux sites distants.

Ce travail nous a permis de nous familiariser avec le réseau VoIP ainsi que le réseau VPN, qui est tout aussi intéressant qu'important réseau basée sur le VoIP en particulier, n'est pas seulement un ensemble de tests de pénétration, mais toute une démarche méthodique et rationnelle, dont la finalité peut apporter énormément à l'entreprise.

Ce projet nous a permis de mieux appréhender les problèmes liés aux réseaux locaux dont ceux relatifs au déploiement d'un réseau VPN et un réseau VoIP comprenant plusieurs sites distants tout en garantissant une qualité de service.

Le développement du client VPN nous a permis de connaitre un nouveau langage réseau via le simulateur (CISCO) et de nous familiariser avec cet outil.

Evidemment, toute entreprise humaine n'est pas parfaite, et cette application attend encore beaucoup d'améliorations.
En ce qui concerne les perspectives, on peut penser à :

- Mettre en place les autres solutions de sécurité recommandées

- Améliorer l'application par l'ajout de la vidéo, boite vocale, SMS, nécessitent une amélioration de la sécurité sur les réseaux public Internet et crypté à l'aide d'un certain nombre d'algorithmes de cryptage avancés pour assurer la confidentialité des données transmises entre les sites distants qui présente une condition primordial pour l'échange et le transfert des données sur d'autres plateformes.

Référence - BIBLIOGRAPHIE

Chapitre 1 :

[1] : https: www.techno-science.net

[2] https:www.electro-cable.fr

[3] https://www.inc.com/encyclopedia/wide-area-networks-wans.html

[4] https://techterms.com/definition/modem

[5] https:www.clicours.com

[6] https://www.pcmag.com/encyclopedia/term/sc-connector

Chapitre2 :

[7] http :www.futura-sciences.com

[8] http : www.cisco.com

[9] http : www.techno-science.net

[10] http : www.docs.oracl.com

[11] http :www.tisparkle.com

[12] http://espace.etsmtl.ca/1303/1/BENZID_Djedjiga.pdf

[13] https.ww.insim-cne.com

Chapitre 3 :

[14] http://esctgabon.com

[15] **http://www.clicour.com**

[16] http://apcpedagogie.com

Chapitre4 :

[17] https://forums.commentcamarch.net

[18] http://cisco.goffinet

[19] https://labo-tech.fr/base-de-connaissance/comment-utiliser-linterface-de-cisco-packettracer/?fbclid=IwAR3MsgSyrB4jleAssQWPN7GM_HXBcR4ljB_oMaRZsS43xC9FpPLI6gErPu.

[20] : Open Vpn :https://fr.vpnmentor.com

[21] : VPN site to site Ipsec :http://idum.fr/spip.php?article214

[22] : Configure Site to Site IPSec VPN Tunnel in Cisco IOS Router : http://www.mustbegeek.com/configure-site-to-site-ipsec-vpn-tunnel-in-cisco-ios-router/