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/2020

MEMOIRE DE FIN D'ETUDES

DE MASTER ACADEMIQUE

Filière : Télécommunications.

Spécialité : Systèmes des Télécommunications.

Thème

Etude et Simulation d'une architecture réseau mixte sécurisée d'une Carte d'itinéraire IPSEC VPN et NAT

Présenté par :

1. ZENTICI HASNIA.
2. BEDDAICH YASMINE AMINA.

Soutenu le …. / .... / 2020 devant le jury composé de :

Président :	MR Soltane Benallou	MAA	Université de Mostaganem.
Examinateur :	MR Mohamed Bentoumi	MCB	Université de Mostaganem.
Encadreur :	MR Resfa Abbes	MCB	Université de Mostaganem.

ANNEE UNIVERSITAIRE 2019/2020

Remerciements

Nous remercions, Tout d'abord, ALLAH pour la volonté, la force, la santé et la patience qu'il nous a donné afin de réaliser ce travail.

Nous tiendrons à adresser nos plus chaleureux remerciements au notre promoteur ***Mr RESFA ABBES****, pour sa présence à tout moment, sa confiance et sa patience, ainsi que pour ses remarques pertinentes et ses contributions considérables tout, au long de la réalisation de ce travail.*

Nous adressons également nos vifs remerciements à ***Mr BENALOU SOLTANE****, Enseignant à l'Université de Mostaganem, d'avoir bien voulu présider le jury.*

Nous sommes également très reconnaissants à ***Mr BENTOUMI Mohamed,*** *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…

Enfin, Nous remerciements a tous ceux qui nous ont assistés de près ou de loin dans la réalisation de ce projet de fin d'étude.

Dédicaces

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie ce modeste travail :

A ma très chère maman, pour son amour inestimable, sa confiance, son soutien, son sacrifice et toutes les valeurs qu'elle a su m'inculquer, merci maman.

A mon très cher papa qu'Allah lui fasse miséricorde qui est ma raison de mon existence et ma source de puissance, merci papa.

A mon encadreur directeur de mémoire Docteur RESFA ABBES pour toutes ses conseils et son aide jusqu'à la dernière minute, que Dieu la garde en bonne Santé ;

A mes oncles ainsi qu'à mes tantes pour leur soutien ;

A tous ma famille BEDDAICH et MEDBOUHI ainsi qu'à mes amis ;

A mon binôme et cher amie Melle Zentici Hasnia ainsi que sa famille ;

A tous ceux qui m'ont aidé dans l'élaboration de ce travail.

Beddaich Yasmine Amina

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie ce modeste travail :

A mes très chers parents pour leur amour inestimable, leur confiance, leur soutien, leurs sacrifices et toutes les valeurs qu'ils ont su m'inculquer ;

Ma mère qui a été à mes côtés et ma soutenue durant toute ma vie, et mon père qui a sacrifié toute sa vie afin de me voir devenir ce que je suis, merci mes parents.

A mon encadreur directeur de mémoire MR RESFA ABBES pour toutes ses conseils et son aide jusqu'à la dernière minute, que Dieu la garde en bonne Santé ;

A mon binôme et cher amie Melle Beddaich Yasmine ainsi que sa famille ;

A tous ceux qui m'ont aidé dans l'élaboration de ce travail.

Zentici Hasnia

Listes des abréviations et acronymes

ACL : Access Control List

ADSL: Asymmetrical bit rate Digital Subscriber Line

AES : Application Environment Service

ANSI : American National Standard Institute

ARP : Adress Resolution Protocol

ASCII: American Standard Code for Information Interchange

ATM : Asynchronous Transfer Mode

BNC : Bayonet Neill–Concelman Connector

CDMA: Code Division Multiple Access

CSMA/CD: Carrier Sense Multiple Access / Collision Detection.

DES: Data Encryption Standard

DHCP: Dynamic Host Configuration Protocol

DMZ: DeMilitarized Zone

DNS: Domain Name System/Service

DOD : Department Of Defense

EAP: Extensible Authentication Protocol

EDGE : Enhanced Data Rates for GSM Evolution

ERP : Enterprise Resource Planning

ETCD : Equipement Terminal de Circuit de Données

ETSI : European Telecommunications Standards Institute

ETTD : Equipement Terminal de Traitement de Données

FAI : Fournisseur d'Accès à Internet

FC : Ferrule Connector

FDDI : Fiber Distributed Data Interface

FTP : File Transfer Protocol

FTTH : Fiber To The Home

GAN : Global Area Network

GPRS : General Packet Radio Service

GSM : Global System for Mobile Communications

HDLC : High Level Data Link Control

HTML: Hyper Text Markup Language

HTTP: Hyper Text Transfer Protocol

HUB : Concentrateur réseau

ICMP : Internet Control Message Protocol

IEEE : Institute of Electrical and Electronics Engineers

IKE : Internet Key Exchange

IP : Internet Protocol

IPsec : Internet Protocol Security

IS : Interim Standard

ISAKMP: Internet Security Association and Key Management Protocol

ISO : International Standards Organisation.

ISP : Internet Service Provider

ITU : International Telecommunication Union

LAN : Local Area Network

LAP : Link Access Procedure

LC : Lucent Connector

L2F : Layer Tow Forwarding

L2TP : Layer Tow Tunneling Protocol

MAC : Media Access Control (chapitre 1)

MAC : Message Authentification Code (chapitre 4)

MAN : Metropolitan Area Network

MAU : Multisession Access Unit

NAS : Network Attached Storage

NAT : Network Adress Traduction

NTIC : Nouvelles Technologies de l'Information et de la Communication

NTT : Nippon Telegraph and Telephone

OSI : Open System Interconnection

OSPF : Open Shortest Path Protocol

PAN : Personal Area Network

PDU : Protocol Data Unit

PING: Packet Internet Groper.

PKI : Public Key Infrastructure

PoE : Power over Ethernet

PPP : Point to Point Protocol

PPTP : Point-to-Point Tunneling Protocol

QoS : Quality Of Service

RA : Registration Authority

RF : Radio frequency

RFC : Request For Comments

RIP : Routing Information Protocol

RJ : Registered Jack

RNIS : Réseau Numérique à Intégration de Services

SARL : Société par Actions à la Responsabilité Limité

SC : Standard Connector

SDU : Service Data Unit

SHA : Secure Hash Algorithm

SNMP: Simple Network Management Protocol

SOROUBAT : Société Route et Bâtiments

SSH : Secure Shell

SSL : Secure Socket Layer

TCP/IP: Transmission Control Protocol/Internet Protocol

TDMA: Time Division Multiple Access

TIA : Telecommunications Industry Association

TLS : Transport Layer Security

UDP : User Datagram Protocol

UMTS: Universal Mobile Telecommunications System

UTP : Unshielded Twisted Pair

VLAN : Virtual Local Area Network

VPN : Virtual Private Network

Sommaire

Chapitre II : les réseaux privés virtuels

Chapitre III : Administration et sécurité

Chapitre IV : Résultat du Simulation et Discussion.

Liste des figures

Liste des tableaux

Abstract

Since the appearance of computer science in the 1950s, it has gradually established itself as a primordial instrument in the professional world, becoming the essential tool for the management of information up to decision-making. Of importance capital for companies.

And as all progress generates 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, home, administrations, etc.) in a secure manner, hence the need for VPN (Virtual Private Network or Virtual Private Network).

The development of technology in general and computer science in particular has sparked a craze for modernizing the processing of information systems.

These technologies have been able to develop thanks to the increasingly important performances 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 associated with local networks, including those relating to the deployment of a VPN network comprising several remote sites while guaranteeing quality of service.

In addition, it allowed us to become more familiar with CISCO equipment.

It emerges, among other things, from this present study that there is agreement between the theoretical reflection carried out and the practical implementation of VPNs, a finding which in our view validates our project.

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

They are likely to be refuted by more robust models or by later diverging observations which would be linked to the evolution of technologies, themselves constantly changing. It is characteristic of any intellectual proposition to expect to be out of date one day or another.

But it can just as well be reinforced later by other approaches and implemented.

Keys words: network, Virtual, private, security.

Résumé

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).

Le développement de la technologie en général et de l'informatique en particulier a 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.

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.

Mais elle peut tout aussi bien être plus tard renforcée par d'autres approches et mises en place.

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

ملخـــص

منذ ظهور الحوسبة في الخمسينيات من القرن الماضي , رسخت نفسها تدريجيا لتصبح جزءا أساسيا في العالم المهني , حيث أصبحت أداة مهمة لترتيب و تنسيق المعلومات , التي بدورها ساهمت في تنظيم و تسيير المؤسسات و المصانع .

وبما أن كل التقدم يولد تحديات جديدة ، فقد نشأت مع مرور الوقت حاجة أخرى تتمثل في الوصول في أي وقت ومن أي مكان إلى الموارد التي تقدمها الكيانات المحوسبة (الأعمال ، والمنزل ، والإدارات ، وما إلى ذلك) بطريقة آمنة .
ومن هنا جاءت الحاجة إلى الشبكة الافتراضية الخاصة VPN .

أثار تطور التكنولوجي بشكل عام و الإعلام الآلي بشكل خاص جنونًا لتحديث معالجة أنظمة المعلومات .

تمكنت هذه التقنيات من التطور بفضل الأداء المتزايد باستمرار لشبكات المحلية الهامة .لكن نجاح أنظمة المعلومات هذه كشف أيضًا عن أحدى ثغراتها .

مكنتنا هذه الدراسة من فهم المشكلات المرتبطة 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 والبحث أكثر في معدات CISCO.

يتضح، من بين أمور أخرى، من هذه الدراسة الحالية أن هناك اتفاقًا بين التفكير النظري الذي تم تنفيذه و التنفيذ العملي لشبكات VPN ، وهي نتيجة في رأينا تؤكد صحة مشروعنا.
.ومع ذلك فإننا نعترف بأن نظرياتنا وانعكاساتنا ، على الرغم من كونها تجريبية ، ليست حقائق لا لبس فيها ونهائية .
ومن المحتمل أن يتم دحضها من خلال نماذج أكثر قوة أو من خلال ملاحظات متباينة لاحقة والتي من شأنها أن ترتبط بتطور التقنيات، والتي تتغير باستمرار. من سمات أي اقتراح فكري أن نتوقع أن يكون قديمًا في يوم أو آخر.
ولكن يمكن أيضًا تعزيزها لاحقًا من خلال مناهج أخرى وتطبيقها.

الكلمات المفتاحية : شبكة كمبيوتر ، افتراضية ، خاصة ، أمنة

Introduction générale :

Cette première partie de l'étude consiste en une réflexion purement théorique sur le sujet et expose la démarche méthodologique adoptée pour le traiter. Elle s'attache ainsi, exclusivement, à montrer l'intérêt scientifique du sujet, à poser le problème, à dégager les hypothèses de recherche, à élaborer la méthodologie sur laquelle s'appuie la recherche de notre thème, et enfin à indiquer les modes de mobilisation et de production de l'information.

La mise en place optimale d'une solution VPN, exige une connaissance suffisante en matière d'architecture informatique et de liaison d'interconnexion, tant au plan général des infrastructures réseaux qu'au niveau spécifique des télécommunications. La présente partie de l'étude s'efforce d'apporter cette indispensable connaissance.

Notre thème comporte trois chapitres :

- **Le chapitre 1** offre un aperçu général sur les différents types de réseaux et topologies informatiques, ainsi que sur les équipements d'interconnexion des réseaux qui sont des pré requis indispensables à assimiler pour notre étude technique. Il en relève par ailleurs les contraintes infrastructurelles.
- **Le chapitre 2** met en exergue la notion de VPN et fournit une évaluation des différents types de VPN afin de savoir quand implémenter chaque type.
- **Le chapitre 3** donne une indication sur l'administration et la sécurité adéquate à mettre en place afin de sécuriser le réseau. Cette réflexion constitue en quelque sorte une transition pour entamer la partie implémentation du programme de configuration des réseaux choisis pour la simulation qui instruit réellement sur la mise en œuvre de l'interconnexion et des services VPN.
- **Le chapitre 4** L'accès aux données situées sur le serveur d'un siège depuis une succursale distante de plusieurs milliers de kilomètres se fait par la solution est le VPN ou Virtual PrivateNetwork (Réseau Privé Virtuel). Avant l'arrivée des VPN, les entreprises devaient utiliser des liaisons appelées TRANSPAC, ou bien des lignes louées. Les VPN ont alors permis de démocratiser ce type de liaison. Le terme VPN sera notamment utilisé pour l'accès à des structures de type cloud computing.

L'interconnexion par le biais de la liaison spécialisée est la première alternative, toutefois son coût très élevé rend difficile son implémentation dans la plupart des entreprises.

Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d'encapsulation" (en anglais tunneling, d'où l'utilisation impropre parfois du terme "tunnelisation", c'est-à-dire encapsulant les données à transmettre de façon chiffrée.

On parle alors De réseau privé virtuel (noté RPVouVPN,acronyme de Virtual Private Network) 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 "voir" les données.

I.2 - Objectifs et Intérêt de l'étude

Toute entreprise est appelée à s'étendre selon ses activités tout en fédérant ses ressources.
Vu l'ambition des différents leaders sur l'échiquier international, et dans le but de lui permettre d'être interconnecté entre ses différents sites nationaux et même internationaux, il a été jugé bon de nous pencher sur la question de la : « Mise en place de Réseau Privé Virtuel (VPN) au sein d'une entreprise » et d'en faire une référence.

I.2.1 Objectifs principaux

Au regard des ambitions sus évoqués, notre étude devra aboutir à la mise en place d'une interconnexion entre plusieurs site distant à travers un VPN afin de faciliter les échanges distants de données au sein de notre réseau et de ce fait de mieux gérer le système d'information de chacune.

I.2.2.Objectifs spécifiques

Il est donc question ici pour nous de répondre aux attentes de notre réseau en mettant en place un réseau virtuel privé stable et opérationnel. Ceci nous amènera donc à étudier différents aspects :
- Nous évaluerons le type de VPN le mieux adapté aux besoins de notre réseau.
- Nous définirons la sécurité des données.
- Une fois le réseau installé, nous réaliserons des tests afin de vérifier son bon fonctionnement.

I.3 - Cahier de charge

Le cahier de charge qui accompagne cette étude pour sa bonne réalisation est aussi riche et prometteur que le thème. En effet les contraintes globales que nous devons respecter sont les suivantes :
- Identifier les différents services de notre réseau
- Proposer un plan d'adressage par SUBNETTING
- Configurer les routeurs VPN
- Assurer la confidentialité des connexions de nos réseaux

Chapitre I
Généralité sur les réseaux informatiques

1. INTRODUCTION :

De nos jours, nous partageons de nombreux fichiers, messages et même des applications ..... Etc.

Et ça grâce au développement de la technologie qui a créé un réseau informatique qui assure le changement des données entre l'équipement ou utilisateurs. Dans ce chapitre, nous décrirons quelques concepts de base sur les réseaux informatiques.

2. DEFINITION DE RESEAU INFORMATIQUE :

Un réseau informatique est un ensemble d'équipements qui inclure du matériels (ordinateur, imprimante, hub, modem..) interconnectés entre eux grâce à des lignes sous forme de câblage (Le support d'interconnexion filaire) ou sans fil (Wifi, Bluetooth,...).

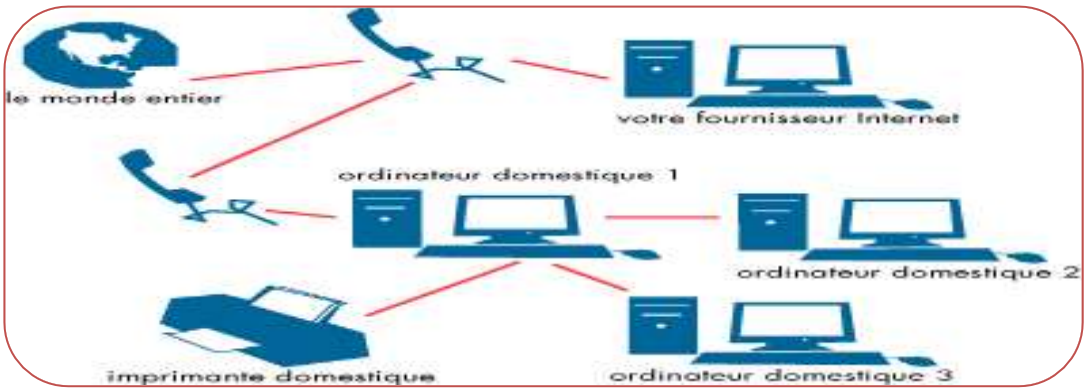


Figure 1.1 réseau informatique

- Un réseau informatique peut offrir plusieurs services différents :

- Le partage des ressources tel que les fichiers, applications ou matériels, connexion à internet, etc.
- Assurer un service de communication et d'échange d'informations de types données, voix et vidéo.
- Assurer de l'indépendance et de l'intégralité de l'accès à l'information (bases de données en réseau).
- Réduire les durées de circulation de l'information.
- Minimiser les coûts de transport des informations. [1].

Suivant l'éloignement entre ces équipements, on distingué plusieurs types de réseaux classés selon leur taille, leur vitesse et leur étendu.

Il existe généralement les catégories suivantes :

- Le PAN (Réseaux personnels).

- Le LAN (Réseaux locaux).

- Le MAN (Réseaux métropolitains).

- Le WAN (Réseaux étendus).

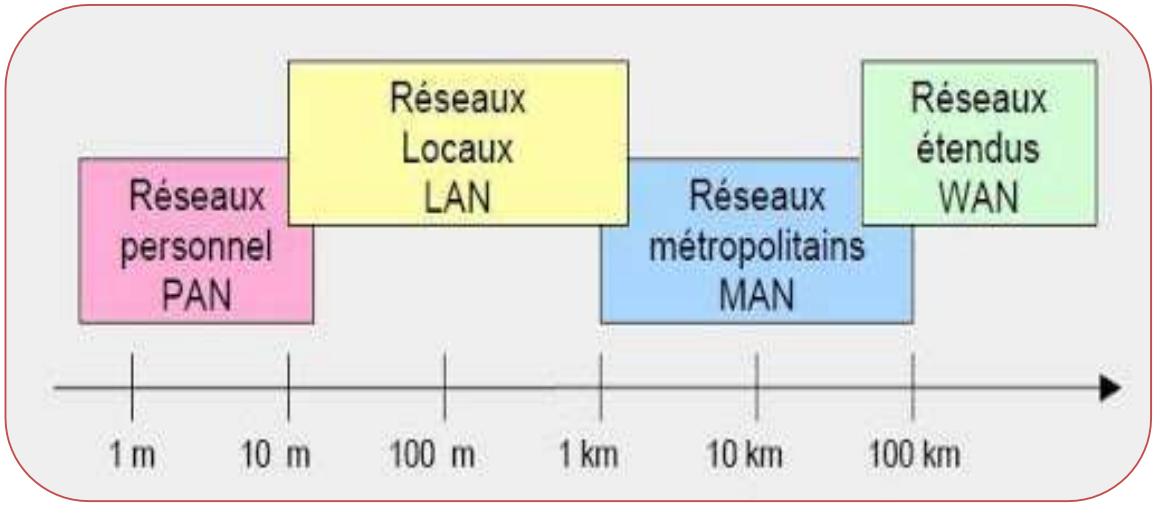


Figure 1.2 Classification des réseaux sans fil en fonction de la distance. [2]

3. LES TYPES DE RESEAU INFORMATIQUE :

3.1- Les Réseaux personnels (PAN) :

Les réseaux personnels ou également appelé Personal Area Networks, sont des réseaux à très faible portée, de l'ordre d'une dizaine de mètres. Ils sont utilisés pour relier des équipements informatiques entre eux sans liaison filaire tel que le Bluetooth, le ZigBee, les liaisons infrarouges. Chaque personne a un réseau local qui comprend son box internet et tout ce qui est connecté dessus, c'est le Personal Area Network.

3.2- Les Réseaux locaux (LAN) :

Les réseaux locaux (Local Area Networks), sont des réseaux qui ont une portée supérieure aux réseaux personnels de l'ordre de quelques centaines de mètres.

La vitesse de transfert de donnée d'un LAN peut s'échelonner entre 10 Mbps pour un réseau Ethernet et 1 Gbps en FDDI ou Gigabit Ethernet. Ce type de réseau s'étend de 1 mètre à 2 kilomètres et peut compter de 2 à 200 abonnés avec un débit de 1 à 100 Mbits/s, est généralement utilisé à l'intérieur d'une entreprise.

Il est facile à installer et à utiliser et de faible coût mais difficile à maintenir la sécurité et le nombre de station est limité. [3]

3.3- Les Réseaux métropolitains (MAN) :

Les MANs (Metropolitan Area Network) relient plusieurs LAN géographiquement proches à des débits importants. Ainsi, il permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Le réseau métropolitain se compose de commutateurs ou de routeurs interconnectés par des liens hauts débits en général la fibre optique. [1]

Ce type de réseau s'étend de 1 mètre à 100 kilomètres et peut compter de 2 à 1000 abonnés. Le débit courant est de 1 à 100 Mbits/s. [3]

3.4- Les Réseaux étendus (WAN) :

Les WANs (Wide Area Network) ou (réseau grande distance) interconnecte plusieurs LANs à travers de grande distance géographique. Ils peuvent être utilisés pour connecter des villes, des états ou même des pays. Les WAN sont souvent utilisés par des grandes sociétés ou organisations pour faciliter l'échange de données, et dans une grande variété d'industries, des sociétés disposant d'installations à plusieurs emplacements ont adopté les WANs**.** [3]

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

Ce type de réseau s'étend sur plus de 1000 kilomètres et peut compter plusieurs milliers d'abonnés. Le débit, étant donné la distance à parcourir, est plus faible, de 50 bits/s à 2 Mbits/s. [2]

Il existe aussi d'autres types de réseaux informatiques tel que :

1. *Global Area Network* (**GAN**) : Un réseau universel tel qu'Internet qui n'est cependant pas le seul réseau informatique dans ce type .Les entreprises actives à l'échelle internationale entretiennent également des réseaux isolés couvrant plusieurs WAN, connectent des ordinateurs d'entreprise dans le monde entier. Les GAN utilisent largement l'infrastructure à fibre optique pour des réseaux étendus et combinent ces derniers avec des câbles sous-marins internationaux ou des transmissions par satellite. [4]

2. *Virtual Private Network* (**VPN**) : réseau privé virtuel est un réseau de communication virtuel qui utilise l'infrastructure d'un réseau physique pour relier logiquement les systèmes informatiques. Les données sont transférées au sein d'un tunnel virtuel qui est construit entre un client VPN et un serveur VPN. IL est utilisé pour connecter les réseaux locaux sur Internet ou pour permettre l'accès à distance à un réseau ou à un seul ordinateur via la connexion publique. [4]

4. LES SUPPORTS DE CONNEXION :

La liaison d'un réseau informatique peut mettre en œuvre plusieurs types de support de transmission tels que les supports physique (câble coaxial, la fibre optique …) et des supports non physique tels que (wifi, Bluetooth,….) mais avant de spécifier les supports d'interconnexion, nous rappelons quelques définitions des éléments du réseau informatique.

4.1 Définitions des éléments du réseau informatique :

- ✓ Ordinateur : est un terminal électronique fonctionnant à l'aide d'un programme ou d'un jeu d'instructions qui lui font lire, d'exécuter des opérations, des calculs, manipuler et modifier des données numériques.

Figure 1.3

- ✓ Modem : est un dispositif qui transmet des informations entre le monde extérieur ou le réseau étendu et notre domicile. Modem est l'abréviation de "Modulator-Demodulator". Les modems sont généralement délivrés par le fournisseur d'accès à Internet (FAI). Le point d'accès Wifi principal doit être branché à un modem via un câble Ethernet. [5]

Figure 1.4

- ✓ Imprimante : un périphérique qui permet de faire une sortie imprimée des données informatiques sur papiers . Il existe de nombreuses technologies d'imprimantes telles que l'imprimante à marguerite. l'imprimante matricielle.

Figure 1.5

- ✓ Le concentrateur HUB : appareil informatique (Un concentrateur réseau) est un nœud qui diffuse des données vers les ordinateurs ou périphériques Ethernet connecté. Il est moins intelligent que le Switch.

Figure 1.6

- ✓ Le commutateur Switch : commutateur réseau est un appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique. L'information qui reçoit le Switch se dirige uniquement vers le bon destinataire contrairement au concentrateur hub qu'il envoie à tous les périphériques connectés. Donc un Switch a les mêmes fonctions qu'un hub mais le Switch est beaucoup plus performant.

Figure 1.7

- ✓ Carte réseaux : (*Network Interface Card*) est un périphérique permettant de connecter un ordinateur à un réseau auquel il est connectée. Elle sert d'interface physique entre la machine et le câble du réseau. Elle a pour fonction de préparer, d'envoyer et de contrôler le flux de données sur le réseau. Elle est constituée d'un ensemble de composants électroniques soudés entre eux sur un même circuit imprimé.

Figure 1.8 carte réseau

- ✓ Routeur : Un routeur est un périphérique intermédiaire dans un réseau informatique qui garantit que les paquets sont acheminés entre deux réseaux indépendants. Ce routage est implémenté selon l'ensemble de règles formant la table de routage, et son fonctionnement est simple. Étant connecté au boîtier via un câble Ethernet, il diffusera la connexion et la récupérera ainsi sur tous les appareils et ordinateurs connectés au réseau.

Figure 1.9

- ✓ Le répéteur : Le répéteur appelé repeater en anglais, est un équipement qui sert à régénérer le signal entre deux nœuds pour le but d'étendre la distance du réseau. Il est à noter qu'on peut utiliser un répéteur pour relier deux supports de transmission de type différents.

- ✓ Le pont : Le pont (bridge en anglais) est un équipement qui sert à relier deux réseaux utilisant le même protocole. Quand il reçoit la trame, il est capable d'identifier l'émetteur et le récepteur, il dirige la trame directement vers la machine destinataire.
- ✓ La passerelle : La passerelle est un système matériel et logiciel qui sert à relier deux réseaux utilisant deux protocoles ou architectures différents. la passerelle crée un pont entre les deux réseaux. Les informations ne sont pas directement transmises, elles sont plutôt traduites pour assurer la transmission tout en respectant les deux protocoles.

- ✓ Frame Relay (Service) : Frame Relay (ou relais de trames) est un service de télécommunication à commutation de paquets conçu pour assurer à faible coût la transmission de données pour un trafic intermittent entre réseaux locaux (LAN), et entre points de terminaison sur les réseaux étendus (WAN).

4.2. A. Support d'interconnexion filaire :

Les « supports de transport » sont tous les moyens par lesquels nous pouvons diriger un signal de son lieu de production vers sa destination avec le moins de perte, de dispersion ou de distorsion possible. Plusieurs critères jouent un rôle dans le choix d'un câble notamment:

- Le nombre d'appareils qui doivent être connectés au support.
- Utilisation de protocole de communication.
- La longueur du câble nécessaire pour connecter l'appareil.
- La vitesse de transmission que nous souhaitons atteindre.
- L'environnement où se trouvera le câble. [3]

4 .2. A1. Câbles à paires métalliques ou torsadées :

La paire torsadée : est une ligne symétrique de deux fils conducteurs enroulés en hélice ensemble. Cette configuration a pour but principal de limiter la sensibilité aux interférences dans les câbles multi-paires. Les paires torsadées se trouvent en téléphonie, et en transmission des données informatiques.

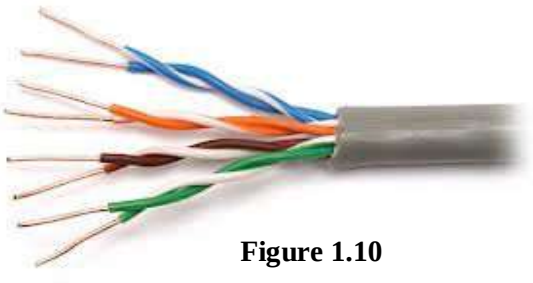


Figure 1.10

Les câbles à paires torsadées sont souvent blindés pour limiter les interférences. Le blindage peut être appliqué à l'ensemble du câble mais il peut également être appliqué individuellement à chacune des paires constituant le câble. Lorsque le blindage est appliqué à l'ensemble, on parle d'écrantage et la feuille métallique formant le blindage est appelée écran. [6]

➢ Types de blindages :

Figure 1.11

✓ **Avantage :**

* Simple à installer.

* Possibilité de travailler en Full Duplex.

* Petit diamètre (pour installation dans des conduits existants).

* Permet d'avoir un câblage dit universel: Téléphone, Fax, Info, etc. ...

✓ **Inconvénients:**

* Sensible aux interférences.

* Câblage plus cher et prend plus de place dans les gaines techniques et par conséquence Plus d'appareils actifs (Hubs, Switch).

4.2. A2. Câbles coaxiaux :

Le câble coaxial : Le câble coaxial ou ligne coaxiale est une ligne de transmission ou liaison asymétrique, utilisé en hautes fréquences, composé d'un câble à deux conducteurs. Ce type de câble est en cuivre spécialement construit avec un blindage métallique et d'autres composants conçus pour bloquer les interférences de signal. C'est une technologie utilisée à l'origine pour les antennes de télévisions. Il relie une télévision à l'antenne.

Figure 1.12

✓ **Les avantages:**

* Bande passante relativement importante (multiplexage de signaux).

* Résistance assez importante face aux perturbations électriques et électromagnétiques.

✓ **Les inconvénients :**

* Installation difficile.

* Gros diamètre (1 – 1.9 cm).

* Assez rigide difficultés de câblage et souffre aussi d'un manque d'adaptation face à de futures modifications.

* Le coût plus élevé.

4.2. A3. La fibre optique :

La fibre optique est un fil en verre ou en plastique plus fin qui transporte de grande quantité de donnée numérique très rapidement et sur longue distance. A la propriété de conduire la lumière.

Il existe deux types du fibre optique monomode et multi-mode :

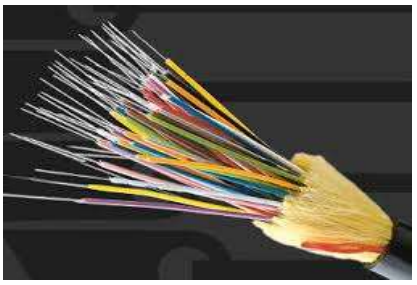


Figure 1.13 Fibre optique

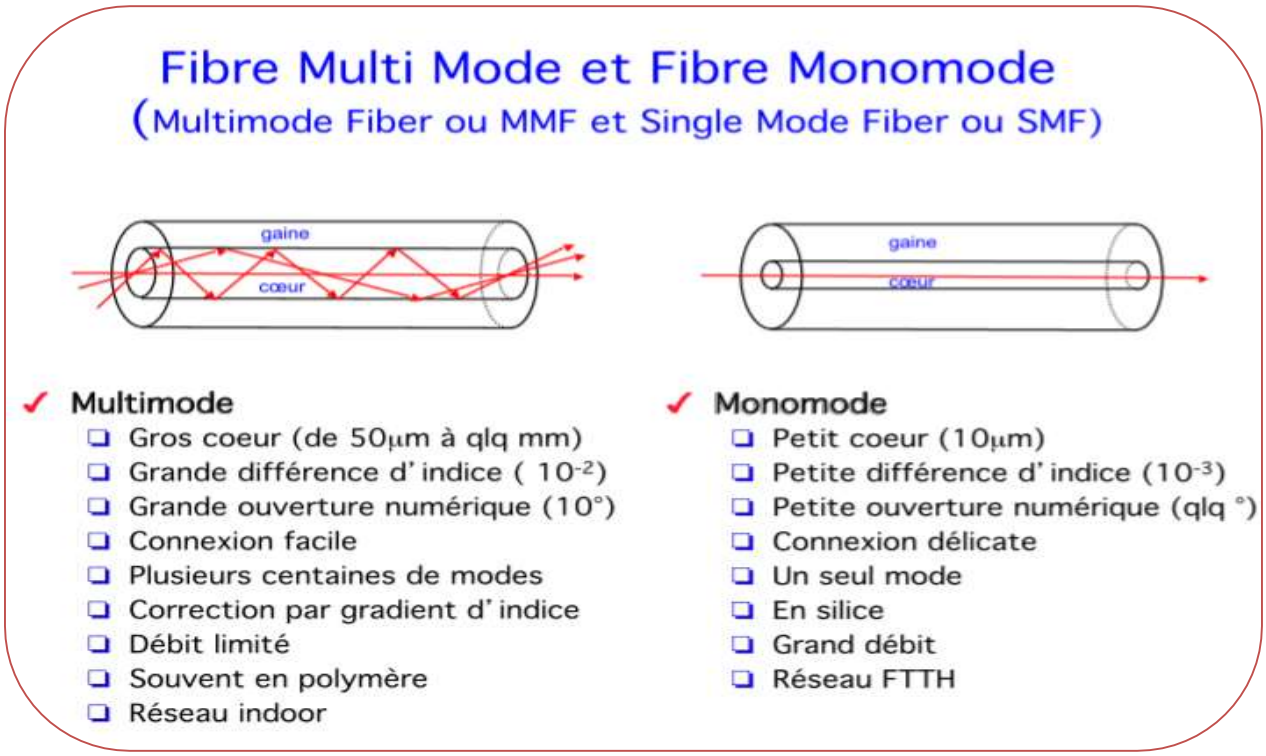


Figure 1.14 type de fibre optique

✓ **Les avantages** :

* Un débit plus rapide jusqu'à 100 Mbit/s en réception.

* Un accès ultra-rapide à Internet qui permet à l'utilisateur d'échanger et de télécharger aisément des fichiers volumineux.

* taille et poids réduits.

* Une simultanéité des usages, grâce à l'augmentation de la bande passante.

* Un faible taux d'entretien par rapport aux autres types de câblages.

* Une meilleure durée de vie généralement plus de 100 ans.

✓ **Les inconvénients :**

* Un coût élève de déploiement exige des dépenses assez importantes.

* Des composants fragiles, elle exige plus de protection autour du câble par rapport au autre câble.

4.2. B. Les connecteurs :

Les connecteurs sont deux fiches associées à un raccord, appelé couramment traversée de cloison. Il existe plusieurs type de connecteurs tels que :

4.2. B1.Connecteurs RJ45 :

RJ pour Registered Jack est un connecteur modulaire généralement utilisé dans les branchements multimédias. Il sert aux connexions Ethernet et s'utilise aussi dans la circulation de courants faibles en tant que connecteur téléphonique par exemple. Il est comme une interface physique permettant de brancher des câbles dénommés paires torsadées pourvues de quatre paires de fils de différentes couleurs (bleu, vert, orange et marron). Plusieurs autres types de connecteurs ressemblent beaucoup au RJ45 et il est très facile de les confondre. Par exemple, les connecteurs RJ11 pour les câbles téléphoniques utilisent des connecteurs à 6 positions plutôt que des connecteurs à huit positions, ils sont donc légèrement plus étroits que les connecteurs RJ45. Les connecteurs RJ45 ont une configuration 8P8C (8 positions, 8 contacts).

Figure 1.15 connecteur Rj 45**.**

4.2. B2.Les connecteurs optiques :

Les connecteurs optiques sont utilisés pour la connexion entre les périphériques réseau dans les centres de données et pour la connexion du câble à fibre optique à l'équipement dans les locaux du client (par exemple FTTH). .

- SC :

Développé par les laboratoires de Nippon Telegraph and Telephone (NTT) au milieu des années 80 « Standard Connector, Subscriber Connector » Un connecteur de câble à fibre optique qui utilise un mécanisme de verrouillage push-pull similaire à câbles audio et vidéo courants. Pour la transmission bidirectionnelle, deux câbles à fibres et deux connecteurs SC (Dual SC) sont utilisés. SC est spécifié par le TIA comme FOCIS-3. [7]

Figure 1.16.connecteur SC

- **LC :**

LUCIDE connector une version miniature de la fibre optique SC. Il ressemble un peu au SC, mais est la moitié de la taille avec une virole de 1,25 mm au lieu de 2,5 mm. [7]

Figure 1.17.connecteur LC

- **FC :**

FC (Ferrule Connector) sont devenu des connecteurs de référence pour une utilisation dans des environnements à fortes vibrations (notamment les applications industrielles et militaires).

Le FC est le plus utilisé pour les installations et raccordement des réseaux.

Figure 1.18.connecteur FC

4.2. B3. Connecteurs BNC :

Le connecteur BNC (connecteur Bayonet-Neill–Concelman) est un connecteur RF utilisé en terminaison de câble coaxial, en particulier dans le domaine radiofréquence. Le connecteur BNC est généralement utilisé dans les applications nécessitant une fréquence inférieure à 4 GHz et moins de 500 V, et correspond à l'impédance caractéristique d'un câble 50 ohms ou 75 ohms.

Figure 1.19.connecteur BNC

5. DEFINITION DE TOPOLOGIE :

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à du matériel (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique. IL existe plusieurs topologies tels que :

- La topologie en bus.
- La topologie en étoile.
- La topologie en anneau.
- La topologie arbre.
- La topologie maillée.

5.1. Topologies en bus:

Le mot "bus" indique la ligne physique qui relie les périphériques du réseau. Dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission via un câble, généralement câble coaxial.

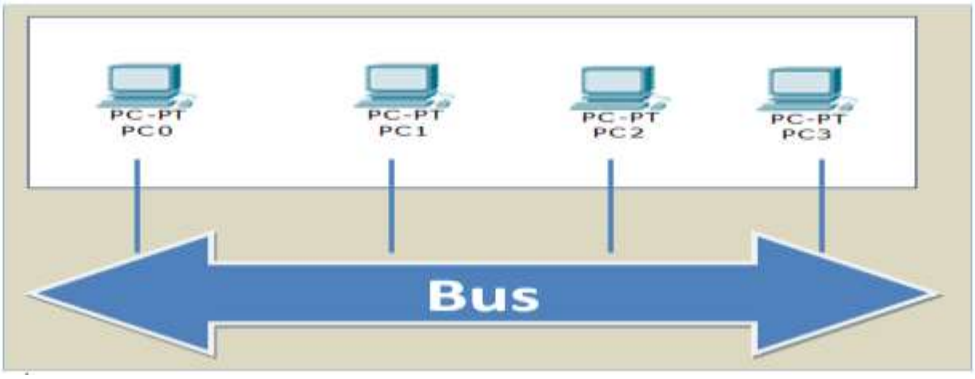


Figure 1.20 Topologie en bus.

Cette structure se caractérise par sa facilité de mise en œuvre et son fonctionnement simple et économique dans les fils et d'autre part, elle est très faible car si l'une des connexions est défectueuse, alors l'ensemble du réseau sera affecté.

5.2. Topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés avec hub ou concentrateur.

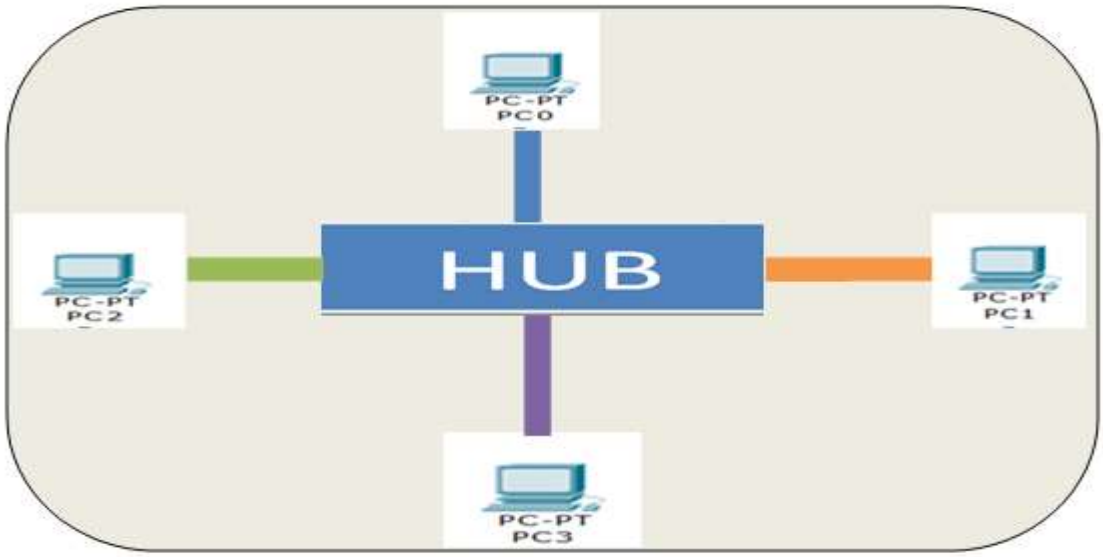


Figure I.21 Topologie en étoile

Les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car on peut facilement retirer une connexion en la débranchant du concentrateur sans paralyser le reste du réseau. De plus, les administrations de réseaux sont faciles (grâce au nœud central). En revanche un réseau à topologie en étoile est plus cher que le réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

5.3. Topologie en anneau :

Dans un réseau en topologie en anneau, les ordinateurs sont situés sur une boucle ferme et communiquent chacun à leur tour.

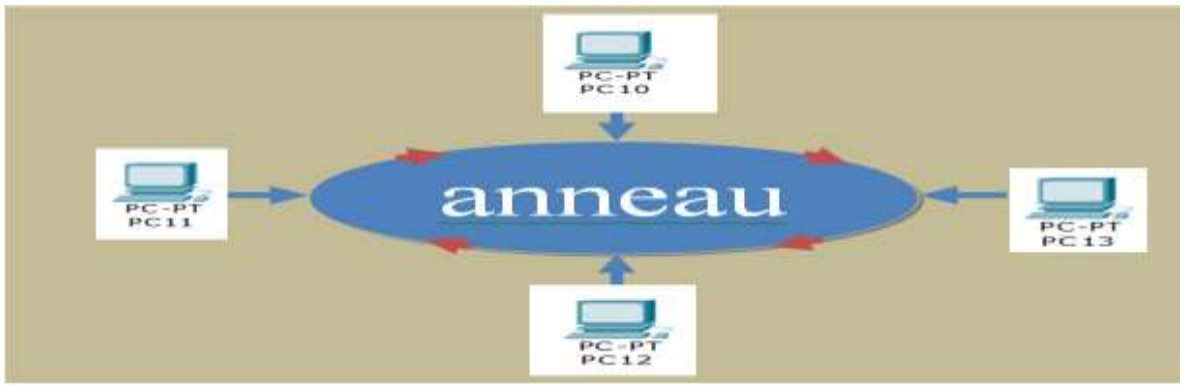


Figure 1.22 Topologie en anneau.

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multi-station Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-deux un temps de parole**.** [7]

5.4. Topologie en arbre :

Elle est également appelée topologie hiérarchique. Chaque ordinateur a relie à un autre ordinateur dans lequel chaque nœud est donnée un nouvel nœud. Le réseau est donc divisé en niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur, dans la hiérarchie.

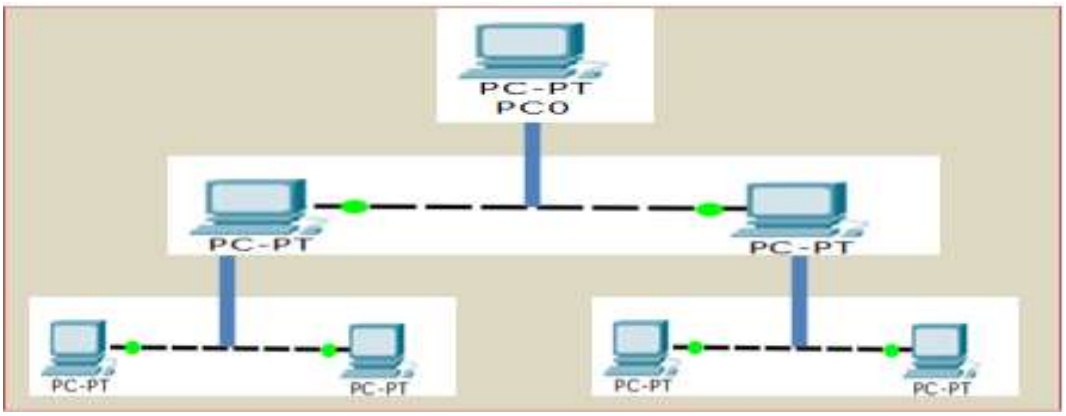


Figure 1.23 Topologie en arbre

5.5. Topologie maillée :

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à de nombreuses liaisons poindre à point. Chaque ordinateur est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé. Cette structure se retrouve dans les grands réseaux de distribution (Exemple : Internet). L'information peut être envoyée sur le réseau suivant des chemins divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.

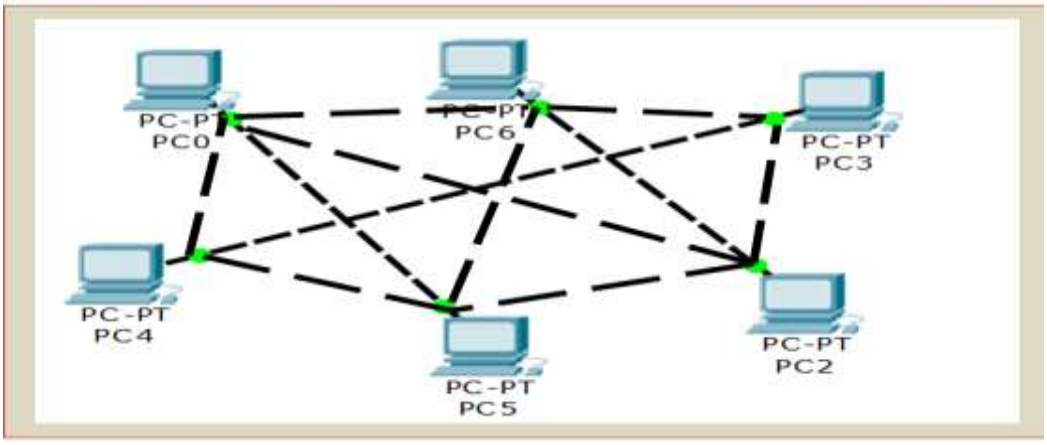


Figure 1.24 Topologie maillée

6. LE MODEL OSI :

OSI signifie (Open System Interconnections), Ce modèle a été développé par l'ISO (International Standard Organisation) afin d'établir une norme pour les communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les connexions entre les ordinateurs.

C'est un modèle conceptuel. Son objectif est d'analyser la communication en découpant les différentes étapes en 07 couches, chacune effectuant une tâche bien spécifique .Dans le modèle OSI Chaque couche:

- fourni des services à la couche supérieure.
- utilise des services de la couche inférieure.
- les données transférées par les services sont des SDU= **Service Data Unit.**
- échange de l'information suivant un protocole avec des couches distantes de même niveaux.
- les données transférées par ce protocole sont des **PDU**= Protocol Data unit.

Figure 1.25 modèle OSI

- **6.1. a. Couche physique:** il prend en charge de la connexion physique d'une machine avec le réseau.
- **6.1. b. Couche liaison:** S'occupe de l'acheminement de trames de données entre deux équipements voisins.
- **6.1. c. Couche réseau:** Définit l'unité de données de base transférée sur le réseau entre deux sites extrêmes et inclut les concepts d'adressage et de routage.
- **6.1 .d . Couche transport:** Assure un contrôle de bout en bout en permettant à un processus destinataire de communiquer directement avec le processus source.
- **6.1. e. Couche session :** Définit la manière dont les protocoles peuvent être organisés pour fournir toutes les fonctionnalités dont les programmes d'applications se servent.
- **6.1. f. Couche présentation :** Est destinée à supporter les fonctions dont beaucoup de programme ont besoin comme la compression de texte ou la conversion d'image graphique.
- **6.1. g. Couche application :** Comprend les programmes qui utilisent le réseau, la messagerie électronique ou le transfert des fichiers.

6.2. Définitions de base :

•**Message**: c'est un regroupement logique de données au niveau de la couche 7 (application).

•**Segment** : c'est un terme utilisé pour décrire une unité d'information de la couche de transport.

•**Paquet** : c'est un regroupement logique d'informations comportant un en-tête qui contient les données de contrôle et (habituellement) les données utilisateur. Le terme paquets est le plus souvent utilisé pour désigner les unités de données au niveau de la couche réseau.

•**Trame**: c'est un regroupement logique de données envoyé comme unité de couche liaison de données par un média de transmission.

•**SDU**: (Service data unit) unité de données de service. Unité d'information d'un protocole de couche supérieure qui définit une demande de service à un protocole de couche inférieure.

•**PDU**: (Protocol data unit) unité de données de protocole. Terme OSI désignant un paquet.

•**Adresse MAC** :(*Media Access Control address*) est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire et utilisé pour attribuer mondialement une adresse physique unique à une machine.

•**Adresse IP** (IP: pour Internet Protocol) est le numéro qui identifie chaque ordinateur connecté à Internet, elle est généralement notée avec quatre nombres compris entre 0 et 255, séparés par des points ; exemple : 192.168.0.50

•**Un protocole** : est un ensemble de règles qui définissent comment se produit une communication dans un réseau.

7. MODEL TCP\IP :

7.1. Introduction :

Le modèle TCP/IP est le modèle le plus utilisé actuellement que ce soit pour des réseaux locaux ou de plus grandes dimensions. Le modèle TCP/IP (Transmission Control Protocol /Internet Protocol) a été développé par le ministère de la Défense des Etats Unis (DOD) à partir du début des années 70 pour servir de base au réseau militaire ARPANET qui est devenu plus tard Internet. Ce protocole est tellement répandu qu'il en est devenu une norme de fait, aucun constructeur ne peut faire l'impasse TCP/IP. Le modèle TCP/IP, inspiré du modèle OSI, adopte l'approche standard (utilisation de modules ou couches) mais en contient uniquement quatre : [8]

Modèle TCP/IP	Modèle OSI
Couche Application	Couche Application
	Couche Présentation
	Couche Session
Couche Transport (TCP)	Couche Transport
Couche Internet (IP)	Couche Réseau
Couche Accès réseau	Couche Liaison données
	Couche Physique

Tableau I.1: Les couches des modèle TCP/IP

Les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI.

Les rôles des différentes couches sont les suivants :

7.2. A. Couche Accès réseau :

Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé

Figure I.26 La couche réseau

7.2. B. Couche Internet :

Elle est chargée de fournir le paquet de données (datagramme).

Figure I.27 La couche internet .

7.2. C .Couche Transport :

Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.

Figure I.28 La couche transport

7.2. D. Couche Application :

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

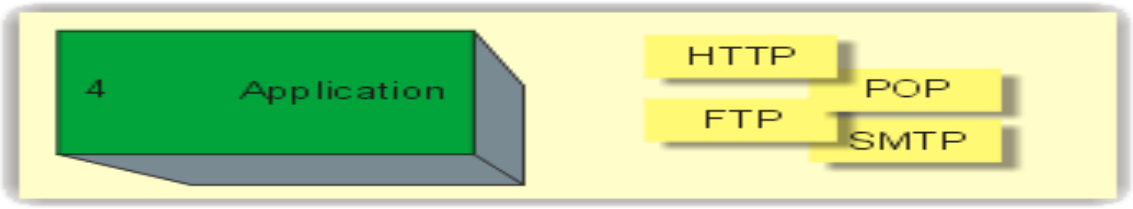


Figure I.29 La couche application.

8. RESEAUX SANS FIL :

8.1. Introduction :

Un réseau sans fil est un réseau dans lequel au moins deux stations peuvent connectées sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur peut rester connecté tout en se déplaçant dans un périmètre géographique plus ou Moins étendu.

Les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) en lieu de place des câbles .Il permet de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus l'installation de tels réseaux ne nécessite pas de lourdes installations de l'infrastructure existante comme c'est le cas dans les réseaux filaires, ce qui a conduit un développement rapide de ce type de technologies. Toutefois, les réseaux locaux sans fil ne sont pas destinés à remplacer les réseaux filaires. Ils sont plus souvent considérés comme une extension à un réseau local existant et non comme un potentiel remplaçant.

8.2. Classification des réseaux sans fil :

De manière générale, les réseaux sans fils sont classés, selon leur étendue géographique, en quatre (04) catégories.

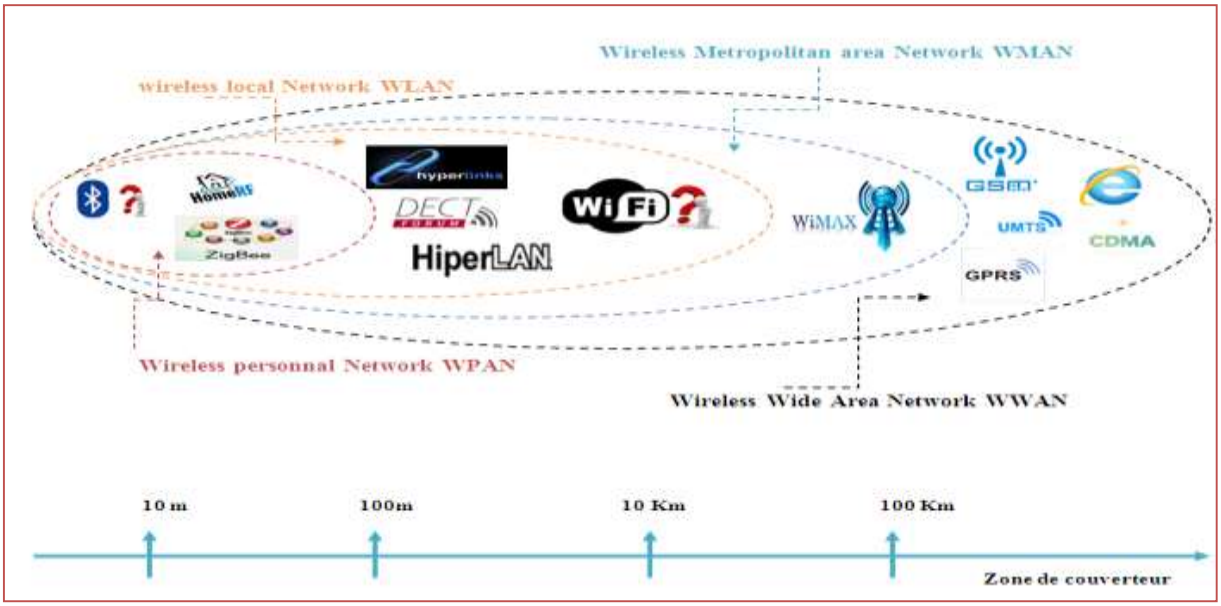


Figure I.30: Classification des réseaux sans fil.

8.2.1. Les réseaux WPAN : [9]

Ces réseaux personnels sans fils regroupent les technologies suivant :

Technologie	Norme	Débit théorique	Portée (m)	Bande de fréquence (GHz)	Observation
Bluetooth	IEEE 802.15.1	1 Mbits/s	10-30m	2,4 –2,4835	- Bas prix - L'émission de puissance dépend de la réglementation
Home RF	Consortium (Intel, HP, Siemens, Motorola et Compaq)	11 Mbits/s	50-100m	2,4 –2,4835	Permet de relier des PC portables, fixes et d'autres terminaux.
Zig Bee	IEEE 802.15.4	250 Kbits/s	100m	2,4 – 2,4835	-Très bas prix, -Très faible consommation d'énergie.

Tableau I.2 : Classification des réseaux WPAN.

8.2.2. Les réseaux WLAN: [9]

Ce sont des réseaux permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une

portée d'environ une centaine de mètres.

Technologie	Norme	Débit (Mbits/s)	Portée (mètres)	Bande de fréquence (GHz)	Observation
Wifi	IEEE 802.11	54Mbits/s	50-100m	2,4 – 2,4835 GHz (11b/11g) 5 GHz (11.a)	Elle comporte plusieurs déclinaisons IEEE 802.11 a/b/g
Hiper[1] LAN 1	ETSI[2]	23.3Mbits/s	50m	5.150- 5.300GHz	- La vitesse de déplacement de l'utilisateur ne peut excéder 10 m/s - Permet d'accéder aux réseaux ATM
HiperLAN 2		54Mbits/s	200m		
HiperLink		155Mbits/s	150 – 200m	17,2 – 17,3 GHz	Permet des liaisons fixes entre 2 points
DECT		2Mbits/s	300m	1.8-1.9 GHz	Technique d'accès TDMA

Tableau I.3 : Classification des réseaux WLAN

8.2.3. Les réseaux WMAN: [9]

Ce sont des réseaux qui couvrent partiellement ou totalement la superficie d'une ville :

Technologie	Norme	Débit (Mbits/s)	Portée (km)	Bande de fréquence (GHz)	Observation
Wi Max	IEEE 802.16	70Mbits/s	50km	2– 66GHz	-Permet le raccordement des hots spots Wifi pour l'accès à Internet -Techniques d'accès TDMA Comporte plusieurs déclinaisons
HiperAccess	ETSI	25Mbits/s	5km	5GHz	-Permet d'accéder aux réseaux ATM

Tableau I.4 : Classification des réseaux WMAN

[1] High performance
[2] Européen Télécommunications Standards Institute.

8.2.4. Les réseaux WWAN: [9]

Ils sont plus connus sous le nom de réseaux cellulaires mobiles.

Technologie	Norme	Débit	Portée (km)	Bande de fréquence	Observation
GSM	Européenne	9.6 Kbits/s	0.3 – 30	[890-915] MHz [935-960] MHz [1710-1785] MHz [1805-1880] MHz	- Utilise une commutation de circuits Système très sécurisé
GPRS	Européenne	≤ 120 Kbits/s	0.3 – 30	[890-915] MHz [935-960] MHz [1710-1785]MHz [1805 :1880]MHz	-Utilise une commutation de paquets -Prise en charge des applications de données à moyens débits - Utilise le protocole IP pour le formatage des données
UMTS[3]	Européenne (ETSI)	≤ 2 Mbits/s	0.3 – 30	2 GHz	- Offre un accès à Internet et à ses serveurs web -Supporte des applications audio et vidéo basse définition - Fonctionne en mode paquet et mode circuit
CDMA 2000	Américaine (TIA)	≤ 2 Mbits/s		2GHz	- Utilise la technique d'étalement de bande
EDGE[4]	Européenne	59.2 Kbits/s	0.3 – 30	2GHz	-Utilise la commutation de circuit
IS 95[5]	Américaine	1,2288 Mbits/s		800-900MHz 1800-1900MHz	- Utilise la technologie CDMA

Tableau I.5 : Classification des réseaux WWAN**.**

[3] L'Universal Mobile Telecommunications System
[4] Enhanced Data for GSM Evolution
[5] Interim Standard 95 : une norme définissant la communication radioélectrique entre un terminal mobile et une station de base dans un réseau de téléphonie mobile .

9. CONCLUSION :

Dans ce chapitre, nous avons défini les concepts de base des réseaux filaires informatiques, de leurs supports de transmission et les réseaux sans fil classés selon leur étendue géographique.

Nous avons étudié comment les fichiers et données circulant sur des réseaux de taille petite (ex : LAN) ou bien de taille plus grande (ex : WAN), suite a la connectique appliqué.

Le prochain chapitre sera consacré aux VPNs (Virtuel Privat Network).

Chapitre II
Les réseaux privés virtuels

1. INTRODUCTION :

En raison des terribles développements qui se produisent dans le monde de la technologie, en particulier dans les réseaux informatiques, comme nous l'avons mentionné dans le premier chapitre, les informaticiens ont crée les réseaux privés virtuels pour assurer la confidentialité pour chaque utilisateur, mais avant l'arrivée des VPN, les entreprises devaient utiliser des liaisons appelées **TRANSPAC**, ou bien des lignes louées.

Nous allons aborder dans ce deuxième chapitre, quelques notions sur les réseaux privés virtuels ainsi que les concepts sur leurs fonctionnements.

2. TRANSPAC :

2.01. DEFINITION DE TRANSPAC :

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 ».
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. [1].

2.02. HISTORIQUE DE TRANSPAC : [1]

L'objectif de Transpac était de répondre aux besoins nouveaux qui découlaient de l'utilisation de matériels informatiques variés. Avant lui, il n'existait en France que les réseaux commutés téléphoniques analogiques et le télex. Or ces réseaux ont des performances limitées et le taux d'erreur y est important (10-4). Ils ne peuvent répondre complètement aux besoins d'applications informatiques. Pour des besoins spécifiques, des lignes spécialisées (ou liaisons spécialisées) peuvent être louées à France Télécom, mais elles coûtent cher et de ce fait ne sont rentables que pour des utilisateurs importants, c'est-à-dire dont le besoin de communication permet de les utiliser de manière satisfaisante (taux d'occupation élevé). La liaison spécialisée est point à point et ne sait pas raccorder deux usagers pour un usage temporaire (comme le fait le téléphone). Cette solution

[1] **L**e Réseau TRANSPAC a été ouvert en Septembre 1978 à l'occasion du SICOB.

manque de souplesse. Ouvert en 1978, le réseau Transpac permet l'établissement de relations entre matériels hétérogènes et entre abonnés situés sur l'ensemble du territoire français.

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.

2.03. ARCHITECTURE DE 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 Level Data Link Control). La couche physique est mise en œuvre sur les liaisons spécialisées.

2.04. PRESENTATION DE X.25 :

X.25[2] est un protocole de communication normalisé par commutation de paquets en mode point à point offrant de nombreux services.

Après avoir été exploité, en France, par la société Transpac filiale de France Télécom qui en détenait le monopole, c'est sous sa nouvelle dénomination Orange Business Services que la

[2] Protocole X25 a un débit jusqu'à 256Kbits/s.

commercialisation et la maintenance en a été assurée 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 X25.

X25 est définie en 1976, la recommandation X.25 de l'ITU a pour but de décrire : « L'interface entre ETTD et ETCD pour terminaux fonctionnant en mode paquet et raccordés par circuit spécialisé à des réseaux publics de données ». Cette norme définit trois niveaux indépendants de protocole ou d'interface permettant l'interconnexion d'ETTD au travers d'un réseau à commutation de paquets. Elle ne définit en aucun cas les protocoles mis en œuvre au sein des réseaux à commutation de paquets. Les trois niveaux définis par X.25 correspondent aux trois premières couches du modèle de référence OSI (physique, liaison et réseau).

Les réseaux X 25[3] sont des réseaux de commutation de paquets avec connexion ce qui signifie qu'un circuit virtuel est établi entre deux accès avant tout échange de données. Cette philosophie, bien dans la ligne du monde des télécommunications, assure la garantie de la bonne transmission des flux de paquets. [2]

❖ Réseaux utilisant X.25 :

• Transpac (France),
• EPSS (Grande-Bretagne),
• Datapac (Canada),
• Telenet (USA),
• DZPAC : Algérie.

2.05. AVANTAGES ET INCONVENIENTS DE RESEAU TRANSPAC :

2.05.1. Avantage :

Parmi 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 de la sécurité.

[3] Un réseau X.25 est constitué d'un ensemble de commutateurs.

2.05.2. Les inconvénients :

Parmi les inconvénients de réseau Transpac, on trouve :

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

3. DEFINITION DE RESEAU PRIVE VIRTUEL :

VPN est une abréviation de Virtual Private Network, ce qui signifie créer un réseau privé virtuel sur un réseau public tel qu'Internet , donc c'est un tunnel sécurisé entre appareil et Internet. 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. Le VPN protège trafic web privé contre les interférences, l'espionnage et la censure. L'adresse IP est masquée et les données chiffrées. Même un fournisseur d'accès Internet ne peut accéder aux données de navigation. Express VPN peut aussi agir en tant que serveur proxy, ce qui permette de masquer ou modifier localisation et de naviguer sur le Web anonymement, où que vous soyez**.**

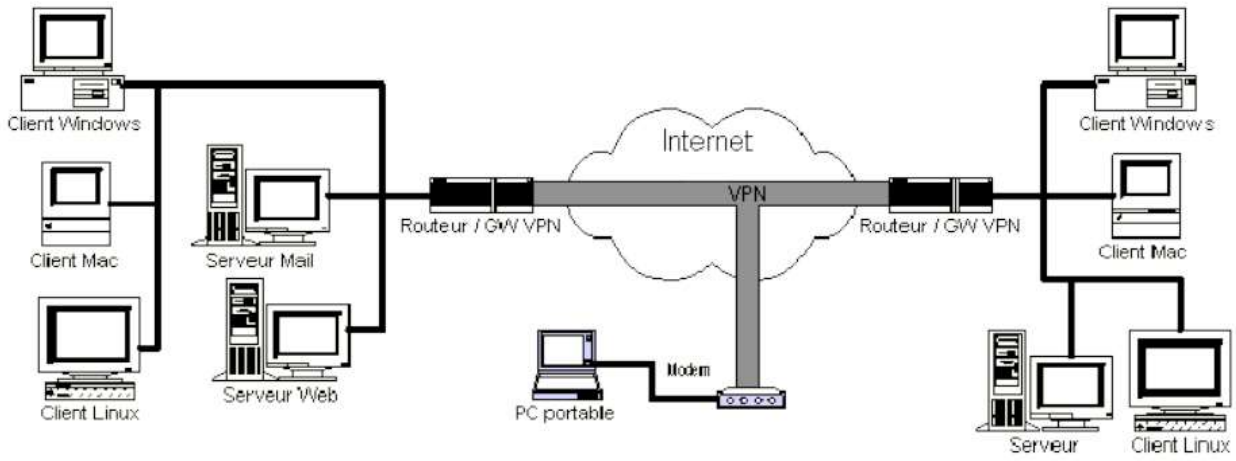


Figure 2.01 Exemple de VPN**.** [3]

3.01. LE FONCTIONNEMENT DU VPN :

La technique consiste à utiliser Internet comme support de transmission en utilisant un protocole de « tunnellisation » (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. 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, IPSec, 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. .

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. [4]

3.02. LES PRINCIPAUX PROTOCOLES DE VPN :

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 :

3.02.1. OpenVPN : développée par James Yonan en 13 mai 2001, est un protocole populaire à utiliser car il est open source et gratuit. OpenVPN est un protocole relativement nouveau et très configurable. La version utilisée par ExpressVPN supporte les ports UDP et TCP.

Il utilise la bibliothèque OpenSSL, 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.

[4] Un tunnel est une galerie souterraine livrant passage à une voie de communication (canal, route, chemin piétonnier) dans le VPN signifie une connexion chiffrée.

3.02.2. PPTP : (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développe par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics. 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 VPNs 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.

3.02.3. L2F : (Layer Two Forwarding) est un protocole de niveau 2 développe par Cisco, Northern Telecom et Shiva. IL est désormais quasi-obsolète. L2F a été spécialement conçu pour le tunnel de trafic PPP.

3.02.4. L2TP : (Layer Two Tunneling Protocol) 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 NetBEUI 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.

3.02.5. IPSec : 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'IPsec sont multiples dans la couche Internet de la suite de protocoles Internet.

3.02.6. 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 VPNS :

Protocole	Avantages	Inconvénients
OpenVPN	-totalement configurable. -bien sécurisé. -permet d'éviter les pare-feu. -utiliser un large choix d'algorithmes de chiffrement.	-nécessite l'installation d'un logiciel tiers. -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/IPsec	- offre une bonne protection. - intégré dans les principaux OS. - permet de contourner la majorité des pare-feu.	- une propriété de Microsoft.

Tableau 2.01 avantages et inconvénients des protocoles VPN**.**

3.04. MOTIVATIONS POUR LE CHOIX D'UNE SOLUTION VPN : [5]

Il y a plusieurs raisons qui induisent à utiliser le VPN, mais le point commun à chaque raison est celui de vouloir virtualiser une partie des communications d'une organisation. Autrement dit, le besoin d'avoir une partie (ou toutes) des communications, essentiellement invisible de la part d'un observateur externe, tout en préservant les avantages d'une infrastructure commune.

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.

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.

Une autre motivation est liée au secret des communications. Les caractéristiques et l'intégrité des services de télécommunications isolés diffèrent des autres environnements qui partagent un support commun. Le niveau de confidentialité dépend de la politique de l'organisation. Si le besoin de confidentialité est faible, une simple abstraction de la discrétion peut suffire. Bien que le besoin de confidentialité soit grand, il existe un fort besoin de sécuriser l'accès et l'accès aux données via des supports partagés.

3.05. TYPES DE VPN :

On peut dénombrer deux grands types de VPN, chacun d'eux caractérise une utilisation bien particulière de cette technologie.

3.05. A. Le VPN d'accès (poste à site) :

Ce type nomade, également appelé "Road Warrior" permet un utilisateur distant de son entreprise de se connecter à celle-ci pour pouvoir profiter de ses services. C'est une utilisation très fréquente des réseaux privés virtuels (VPN) pour permettre aux utilisateurs distants (travailleurs à domicile, etc.) d'accéder aux ressources de l'entreprise. Pour mettre en œuvre cette solution, les appareils (pare-feu, routeur, etc.) seront installés sur l'emplacement central, qui constitue le point de terminaison de tous ses réseaux VPN. Le logiciel qui gère le type de protocole choisi et compatible avec les appareils du site central est installé du côté des postes de travail distants. Dans certains cas, ce logiciel est déjà présent dans le système d'exploitation de ces postes de travail, et dans d'autres cas, il est nécessaire d'installer ce composant logiciel.

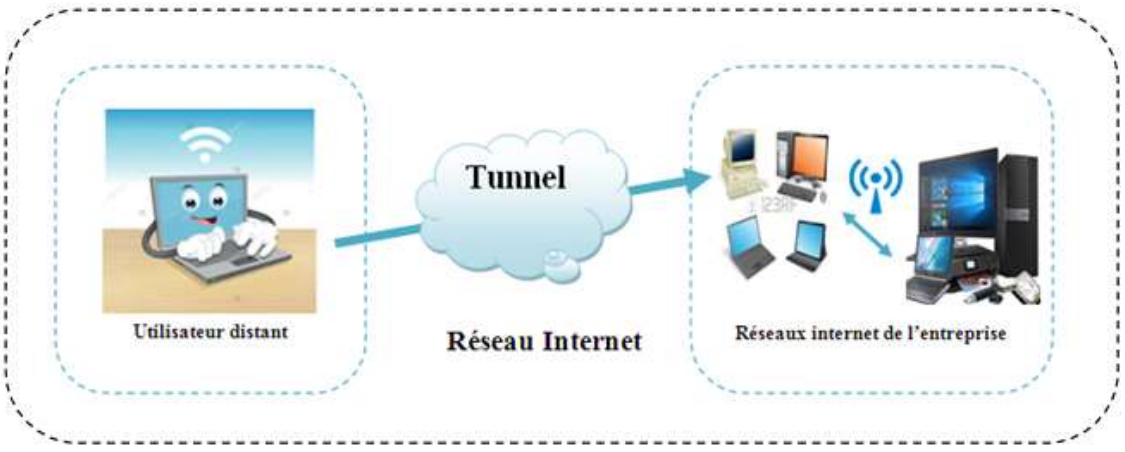


Figure 2.02 Le fonctionnement d'un VPN poste à site.

✓ **Avantages et inconvénients :**

Parmi les avantages de cette solution, on trouve :

- L'accès du poste mobile peut se faire de n'importe quel point du monde 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 :

- L'installation du logicielle est généralement nécessaire sur la station distante.

- 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.

3.05. 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.

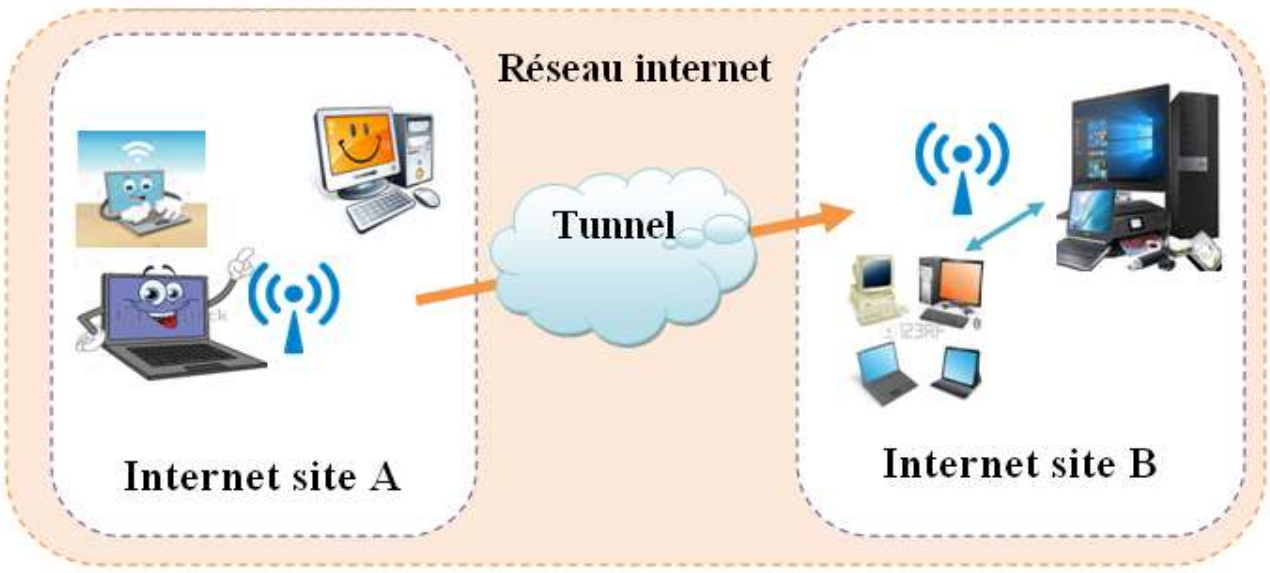


Figure 2.03. Architecture VPN LAN to LAN.

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.

Il y a deux méthodes pour connecter des réseaux locaux entre eux avec un VPN:

1. En utilisant des lignes dédiées:

Au lieu d'utiliser des lignes louées très coûteuses à longue distance entre deux LAN, on utilise une ligne dédiée locale pour se connecter à un ISP pour permettre des connexions à Internet. Le réseau privé virtuel sera donc créé à l'aide des connexions locales à l'ISP et à l'aide du réseau public Internet.

2. À l'aide d'une liaison téléphonique :

Au lieu d'utiliser des lignes dédiées pour se connecter à l'ISP, il suffit d'avoir une liaison téléphonique permettant l'appel de son propre ISP. Comme pour la solution précédente, le réseau privé virtuel sera créé à l'aide des connexions locales à l'ISP et à l'aide du réseau public Internet. [5]

Il existe deux types de VPN de site à site:

1. *Basé sur l'intranet* : Si une entreprise possède un ou plusieurs sites distants qu'elle souhaite Rejoindre dans un seul réseau privé, elle peut créer un VPN intranet pour connecter chaque LAN Séparé à un seul WAN. [5]

2. *Basé sur l'extranet* : Lorsqu'une entreprise a une relation étroite avec une autre entreprise (Comme un partenaire, un fournisseur ou un client), elle peut créer un VPN extranet qui connecte les réseaux locaux de ces entreprises. Ce VPN extranet permet aux entreprises de travailler ensemble dans un environnement réseau partagé et sécurisé tout en empêchant l'accès à leurs intranets séparés. [5]

- ✓ **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.

3.05. 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 ».

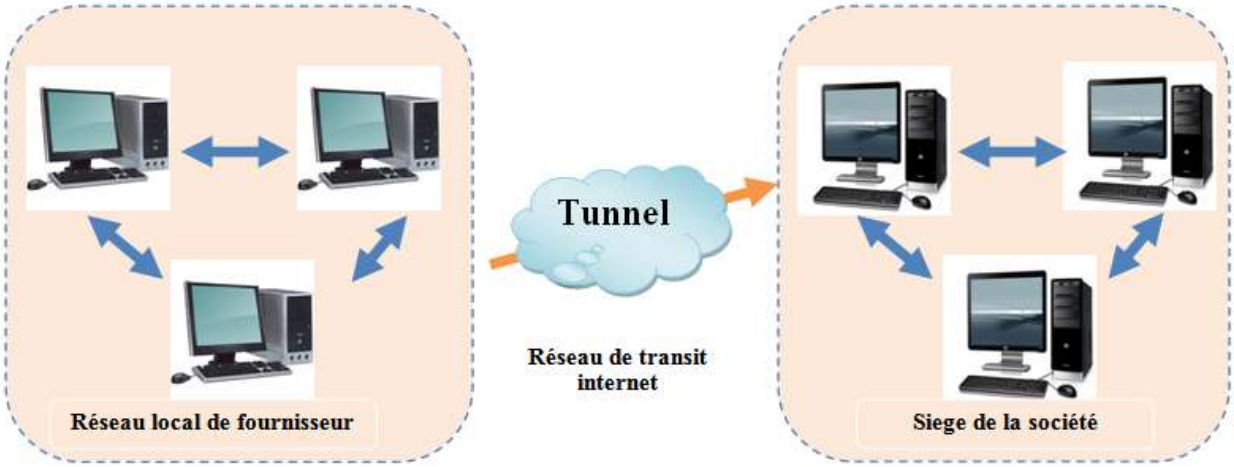


Figure 2.04 Le fonctionnement de l'extranet.

✓ **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.

3.06. LES EXIGENCES DE BASE DE RESEAU PRIVENT VIRTUEL :

Pour garantir la confidentialité[5] et l'intégrité des données lors de leur passage sur l'Internet, des mesures et des mécanismes de sécurité sont également utilisés pour assurer le transfert de ces données en toute sécurité à travers un milieu non sécurisé. [6]

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.

3.06.1 .Authentification :

L'authentification vérifie l'équipement de l'utilisateur ou l'identité de l'utilisateur lors de l'établissement d'une connexion VPN dans un réseau. Il existe deux catégories générales d'authentification :

- ➢ authentification de l'équipement : L'authentification de périphérique nous permet de restreindre l'accès VPN au réseau pour fournir des informations d'authentification à partir d'un périphérique VPN distant. Une ou plusieurs clés sont configurées et utilisées pour authentifier l'identité de l'appareil.
- ➢ authentification de l'utilisateur : De nombreuses applications VPN ajoutent une couche d'authentification supplémentaire, appelée authentification des utilisateurs, pour vérifier si une connexion VPN est autorisée Par un utilisateur qui utilise un équipement spécifique, où l'utilisateur doit fournir un nom d'utilisateur et un mot de passe. Ce mot de passe peut être un mot de passe statique ou un mot de passe immédiat.

[5] La confidentialité a été définie par (ISO) comme le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé, et est une des pierres angulaires de la sécurité de l'information. La confidentialité est l'une des raisons d'être des crypto-systèmes.

3.06.2. 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, Blowfish, RSA, IDEA, SEAL et RC4.

3.06.3. 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.

3.06.4. 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 clés de chiffrement et les renouveler périodiquement pour les données chiffrées sur un accord réciproque afin que la sécurité et la confidentialité puissent être maintenues.

3.06.5. La non-répudiation :

La non-répudiation ou la comptabilité est l'enregistrement de la session VPN. Cela pourrait inclure l'identité des deux dispositifs pour établir la connexion, la durée de la connexion qui a été utilisée, la quantité d'information qui a été transmise, le type d'informations traversé pendant la connexion, etc. Autrement dit, 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. La non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.

3.06.6. 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.

3.06.7. Gestion des adresses :

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.

Par exemple, les informations de routage, la résolution de nom de la source, et de la sécurité ainsi que des filtres de sécurité pour assurer la protection des données internes de toute utilisation non autorisée.

3.07. L'EQUIPEMENTS 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 OpenVPN qui est multi-plateformes mais les fabricants proposent aussi généralement leur propre logiciel (exemple : Fortinet avec son FortiClient).

3.08. LES SERVICES DE VPN : [3]

La technologie VPN offre trois fonctions principales à ses utilisateurs:

3.08.1. 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.

3.08.2. Intégrité des données :

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.

3.08.3. 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.

3.09. AVANTAGE ET INCONVENIENT DU VPN :

3.09.1 les avantages de VPN :

Les avantages de l'utilisation du VPN sont les suivants:

- ✓ Faible coût.
- ✓ Universalité, la possibilité d'accéder à partir de différentes technologies.
- ✓ Augmentez la connectivité.
- ✓ Échange sécurisé d'informations.
- ✓ L'évolutivité est facile à améliorer.
- ✓ La possibilité de former un réseau LAN qui n'est pas limité en place et en temps, car la connexion se fait via Internet.
- ✓ Nous pouvons imprimer de votre domicile à bureau via Internet.
- ✓ Nous pouvons transférer des données ou une vue à distance pour contrôler les ordinateurs à la maison / au bureau n'importe où.
- ✓ Surfez en toute sécurité lorsque vous êtes sur un accès Internet public / hotspots.

3.09.2 les inconvénients de VPN :

Une connexion VPN peut affecter notre utilisation d'internet de plusieurs manières. Les inconvénients les plus communs d'un VPN sont :

- ✓ Une connexion internet plus lente.
- ✓ Un blocage de l'accès par certains services (par exemple Netflix).
- ✓ 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.
- ✓ Pertes de connexion.
- ✓ Un sentiment injustifié d'impunité en ligne.

- ✓ VPN gratuits : parfois pire que rien du tout.

4. CONCLUSION :

Dans ce chapitre nous avons présenté quelques notions de base sur le réseau privé Virtuel qui fourni plusieurs service de sécurité à utilisateur, ainsi que le réseau TRANSPAC qui était le premier réseau commercial avec ses principes fondamentaux.

L'objectif du chapitre suivant sera de discuter des administrations et de la sécurité du réseau VPN.

Chapitre III

Administration et sécurité

1. INTRODUCTION :

Les réseaux informatiques nécessitent un administrateur pour gérer tous les services et 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.

L'administration est une tâche qui requiert que le réseau soit fonctionnel et que les différents services soient implémentés. Avant d'en profondeur dans le sujet il serait primordial de rappeler ce qu'il faut administrer dans le réseau : les hommes (administrateurs et utilisateurs), la configuration des équipements, le dépannage, les stations d'administration, la sécurité.

Dans ce troisième chapitre, nous aborderons quelques concepts de base sur l'administration et la sécurité des réseaux informatiques.

2. LE BUT DE L'ADMINISTRATION D'UN RESEAU INFORMATIQUE :

L'administration réseau est le processus permettant le contrôle d'un réseau de donnée pour en assurer l'efficacité et la productivité.
Le but final de l'administration réseau est d'aider à maitriser la complexité des réseaux de donnée et d'assurer que les données transitent sur le réseau avec le maximum de l'efficacité et de transparence aux utilisateurs.
L'administration des réseaux est couramment classée en trois activités :

A. La Supervision :

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 des réseaux afin d'éviter un arrêt prolongé de celui-ci. La supervision doit permettre d'anticiper les problèmes et de faire remonter les informations 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. [1]

B. l'Administration :

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 :

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

C. l'Exploitation

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.

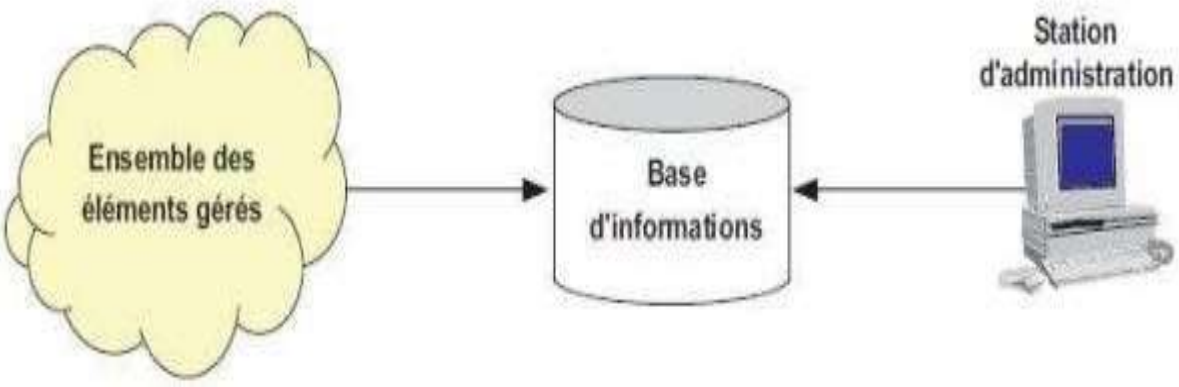


Figure 3.01. Principe générale d'un système d'administration des réseaux. [1]

2.1. TOPOLOGIE DE L'ADMINISTRATION DES RESEAUX INFORMATIQUES :

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

Figure 3.02 Topologie de l'administration de réseau .

2.2.1. L'administration des utilisateurs : [1]

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.

2.2.2. L'administration des serveurs : [1]

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 utilisés.

2.2.3. L'administration de la machine de transport : [1]

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

- *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.
- *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.
- *l'inventaire,* qui a pour rôle de tenir à jour en temps réel la liste des éléments logiciels et matériels qui constituent un réseau.
- *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.

2.3. LE ROLE DE L'ADMINISTRATEUR RESEAU :

L'administrateur réseau est responsable de ce qui peut se passer dans un réseau
Administré ; Le rôle de l'administrateur réseau consiste à :

- ✓ Mettre en place et maintenir l'infrastructure du réseau.
- ✓ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ✓ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ✓ S'assurer que les utilisateurs « n'outrepassent » pas leur droite.
- ✓ Gérer les « logins » (noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières,….).
- ✓ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui se passe à partir du réseau administré.
Le rôle de l'administrateur (root) est :

- ✓ configurer le noyau du système d'exploitation ;
- ✓ sauvegarder les données et réparer les systèmes de fichiers ;
- ✓ gérer les utilisateurs ;
- ✓ installer de nouveaux logiciels ;
- ✓ intégrer des nouveaux disques et de nouvelles partitions ;
- ✓ configurer le processus de démarrage de Linux ou autre ;
- ✓ configurer le réseau.

2.3.1. LA SECURISATION DES RESEAUX :

Divers équipements peuvent être mis en place pour protéger les entrées et sorties réseau :

2.3.2. Programme antivirus :

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, Inoculate IT de Computer Associates, ainsi que VirusScan, WebShields, NetShield et GroupShields de Network Associates. [2]

2.3.3. Pare-feu :

Un pare-feu : (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), c'est la première ligne de défense des réseaux contre les virus. C'est un système ou dispositif de protection permettant de protéger les réseaux. Il surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies. 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 3.03 appareil pare-feu

Figure 3.04 protection pare-feu

❖ Rôles d'un pare-feu :

- déterminer le type de trafic qui sera acheminé ou bloqué.
- limiter le trafic réseau et accroître les performances.
- contrôler le flux de trafic.
- fournir un niveau de sécurité d'accès réseau de base.
- autorisé un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.

2.3.4. Proxy :

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 Text Transfer Protocol (http), et File Transfer Protocol (FTP) entre le LAN et l'Internet. [3]

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

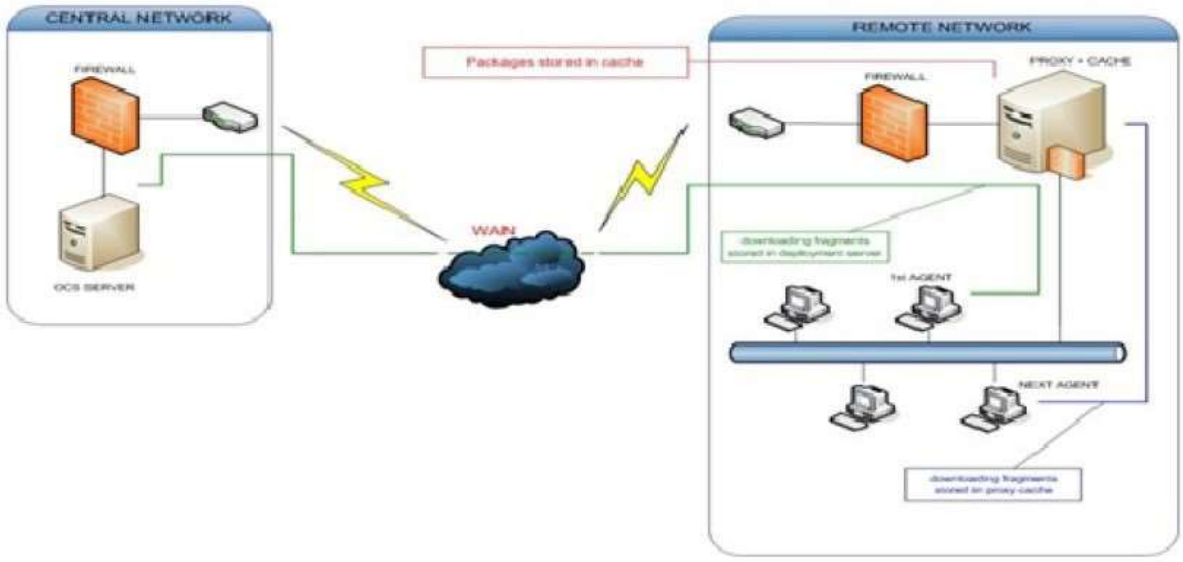


Figure 3.05 Le serveur proxy.

2.3.5. Routeur filtrant :

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 a 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 . . .).

2.3.6. Zone démilitarisée :

La Zone démilitarisée : Une DMZ (Demilitarized 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 intermédiaire 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. [4]

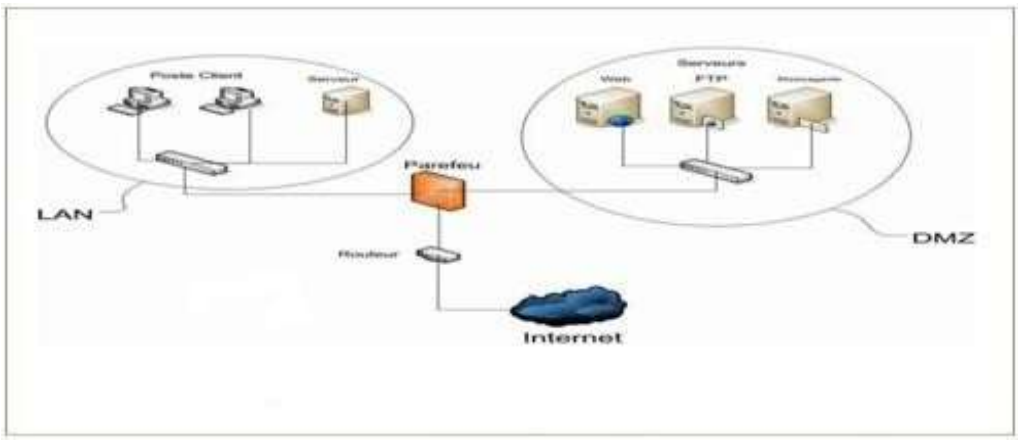


Figure 3.6. Zone Démilitarisée

3. LES CLASSES D'ADRESSES :

❖ **Adresse IP :**

D'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. Ca donne quelque chose comme ça : 192.168.132.24.

❖ **les Classes d'adresses :**

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.

Classe réseau	Début	Fin	Masque de réseau
Classe A	**0.0.0.0**	**127.255.255.255**	**255.0.0.0**
Classe B	**128.0.0.0**	**191.255.255.255**	**255.255.0.0**
Classe C	**192.0.0.0**	**223.255.255.255**	**255.255.255.0**
Classe D	**224.0.0.0**	**239.255.255.255**	**240.0.0.0**
Classe E	**240.0.0.0**	**255.255.255.255**	**Non défini**

Tableau 3.1 Les classes des réseaux.

3.1.1. NOTIONS DE BASE SUR LE ROUTAGE : [5]

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. Une route possède quatre composants principaux :

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

3.1.2. LES PROTOCOLES DE TUNNELISATION :

Un protocole de tunnellisation 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 tunnellisation répandus, comme Secure Shell (SSH), Point-to-Point Tunneling (PPTP) et IPsec, chacun étant adapté à un objectif de tunnellisation 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. [6]

3.1.3. LES PROTOCOLES DE ROUTAGE :

Les protocoles de routages permettent l'échange des informations à l'intérieur d'un système autonome. On retient les protocoles suivants :

- 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
- 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

Les protocoles couramment utilisés sont :

- Routing Information Protocol **(RIP).**

- Open Shortest Path First **(OSPF).**
- EnhancedInterior Gateway Routing Protocol **(EIGRP).** [7]

3.2. LES RESEAUX LOCAUX VIRTUELS (VLAN) : [8]

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

3.2.1. 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.).

3.2.2. Avantages offerts par les Vlan :

Ce nouveau mode de segmentation des réseaux locaux modifie radicalement la manière dont les réseaux sont conçus, administrés et maintenus. 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* : Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en considération leur localisation physique.
- *La simplification de la gestion* : L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement.
- *L'augmentation considérable des performances du réseau* (réduction du domaine de collision) : Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau.
- *Une meilleure utilisation des serveurs réseaux.*
- *Le renforcement de la sécurité du réseau* : Les frontières virtuelles créées par les VLANs ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée.

3.2.3. Technique et méthodes d'implantation des Vlan :

Pour réaliser les VLANs, 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 VLANs. Nous pouvons les associer à une couche particulière du modèle OSI:

- **VLAN de niveau 1** ou 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 de niveau 2** ou 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 de niveau 3** ou 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.

3.2.4. 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 VLANs 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 VLANs de communiquer entre eux, il faut utiliser un routeur ou 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. [8]

3.2.5. GESTION DE L'ADRESSAGE :

Plusieurs groupes d'adresses ont été définis dans le but d'optimiser l'acheminement (ou le routage) des paquets entre les différents réseaux.

Ces groupes ont été baptisés classes d'adresses IP qui correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum.

En ce qui concerne notre projet, nous utiliserons des adresses de classe C pour la configuration des différents nœuds (poste, routeur) du réseau.

En théorie, une adresse de classe C offre la possibilité d'identifier 254 machines (sans adresses broadcast et réseau) et a un masque réseau qui est 255.255.255.0.

Pour prévoir une extensibilité future du réseau, il convient d'attribuer une adresse de cette classe à chacun des sites. Les adresses étant différentes, les différents sites ne pourront pas communiquer sans l'implémentation d'un mécanisme de routage soit par un routeur ou un commutateur multicouche (commutateur faisant le routage IP). Nous opterons pour le commutateur multicouche, étant donné qu'il est plus rapide dans le traitement en interne.

Des Switch seront utilisés à plusieurs niveaux du réseau pour permettre la segmentation et réduire le domaine de collision.

Dans la même veine, pour réduire les domaines de diffusion et pour ne permettre que les communications autorisées, des VLAN et un routage Inter-VLAN sera définis. [9]

Equipments	Login par défaut
Routeur& Switch	**192.168.1.0/24**
Serveur de Domaine&Hyperviseur	**192.168.2.0/24**
Copieurs IP &Imprimantes	**192.168.3.0/24**
Laptop IP	**192.168.4.0/24**
ServeurISPFAI	**192.168.5.0/24**

Tableaux 3.02 Donnant une répartition des IP et de l'adressage

3.3. SECURITE DES LIAISONS ET DE L'ACCES AUXSERVICES :

Dès lors que le réseau privé transite par internet, le problème de la sécurité se pose :

Les informations qu'il véhicule possèdent de la valeur et ne doivent pas être accessibles à tout le monde, l'infrastructure réseau un y échappent pas aussi.

Il convient donc de mettre en place toute une politique de sécurité pour garantir un maximum de sécurité.

3.3.1. 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. Nous allons donc rédiger une stratégie de sécurité qui concernera tous les utilisateurs du réseau à déployer, en les éduquant aux bonnes conduites à tenir.

3.3.2. Sécurité logicielle : [9]

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.

❖ **Pare-feu et Antivirus:**

- Utiliser des **ACL sur le routeur en firewall** à l'entrée du réseau filtrant tout ce qui entre et tout ce qui sort du réseau (services Netbios, RPC, Telnet, NFS…).
- Mettre un pare-feu logiciel sur les serveurs de sorte à empêcher l'accès aux données confidentielles.
- Installer des programmes antivirus mis à jour régulièrement sur tous les postes.

❖ **Authentification:**

- Filtrage par adresse MAC des liens Radio avec Non-diffusion du SSID et Clé WPA2-PSK(AES).
- Authentification avec code d'accès pour les utilisateurs Wifi.
- Mise en place de mots de passe sur les nœuds les plus importants du réseau (serveur, routeur).

❖ **Autres:**

- Configurer des VLANs relatifs aux différents services à l'intérieur de chaque site dans le but de ne permettre que les communications autorisées entre ces services.
- Utiliser que des protocoles sécurisés, basés sur SSL (Secure Socket Layer) : HTTPS, SSH, IMAPS, DNSSEC, etc. [9]

3.3.3. LA SECURITE D'UN RESEAU :

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.

3.3.4. DEFINITION DE LA SECURITE INFORMATIQUE :

Le concept de sécurité informatique est un ensemble d'outils, de techniques et de méthodes utilisés pour réduire l'exposition du système aux menaces accidentelles ou intentionnelles.

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.

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.

4. CONCLUSION :

Cette partie de nos recherches, est une partie charnière qui a eu pour effet de mieux appréhender la teneur de notre projet tout en cernant mieux les contours. Il en est ressorti de son étude qu'il existe beaucoup de solutions pour mettre en place des VPN inter site et qu'une technologie, l'IPSec semble s'imposer aujourd'hui pour la construction des VPN site-to-site. Nous avons appris plusieurs points clés tel que:

- La technologie IPSec permet d'offrir des services de sécurité classiques (authentification, confidentialité, intégrité, etc.) pour chaque datagramme transitant par un réseau de transport (par exemple, Internet).
- Cette technologie peut être mise en œuvre par l'entreprise utilisatrice ou par un fournisseur de service dans le cadre d'infogérance. Deux limitations essentielles sont à retenir pour cette technologie :
  (1) elle ne permet pas de gérer la qualité de service en cœur du réseau ;
  (2) elle ne transporte que les datagrammes IP.

Chapitre IV

Résultat du Simulation et Discussion

1. INTRODUCTION :

D'après ce que on a présenté dans le chapitre précédent, la création du VPN se faîte par un logiciel qui s'appelle Cisco Packet Tracer, il va nous faciliter le travail dans notre projet de telles sortes que l'installation et la vérification du fonctionnement de VPN à travers des commandes qui s'appliquent aux niveaux des routeurs.

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 Bosack et Sandra Lerner, et a son siège social à San Jose, en Californie. [1]

Figure 4.01 Bâtiment de Cisco Systems. [1]

2.2.PACKET TRACER :

2.2.1. Introduction :

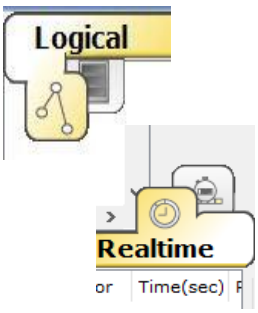
Packet Tracer est un logiciel développé par le CISCO qui permet de construire un réseau physique virtuel et de simuler le comportement des protocoles sur le réseau.

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).

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.… [2]

2.2.2. Interface et outils :



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

B. Le bouton logical permettant de naviguer entre le réseau logique et physique. [3]

C. Le barre de realtime, pour alterner entre le mode temps-réel et mode simulation (-pas-a-pas). [3]

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... [3]

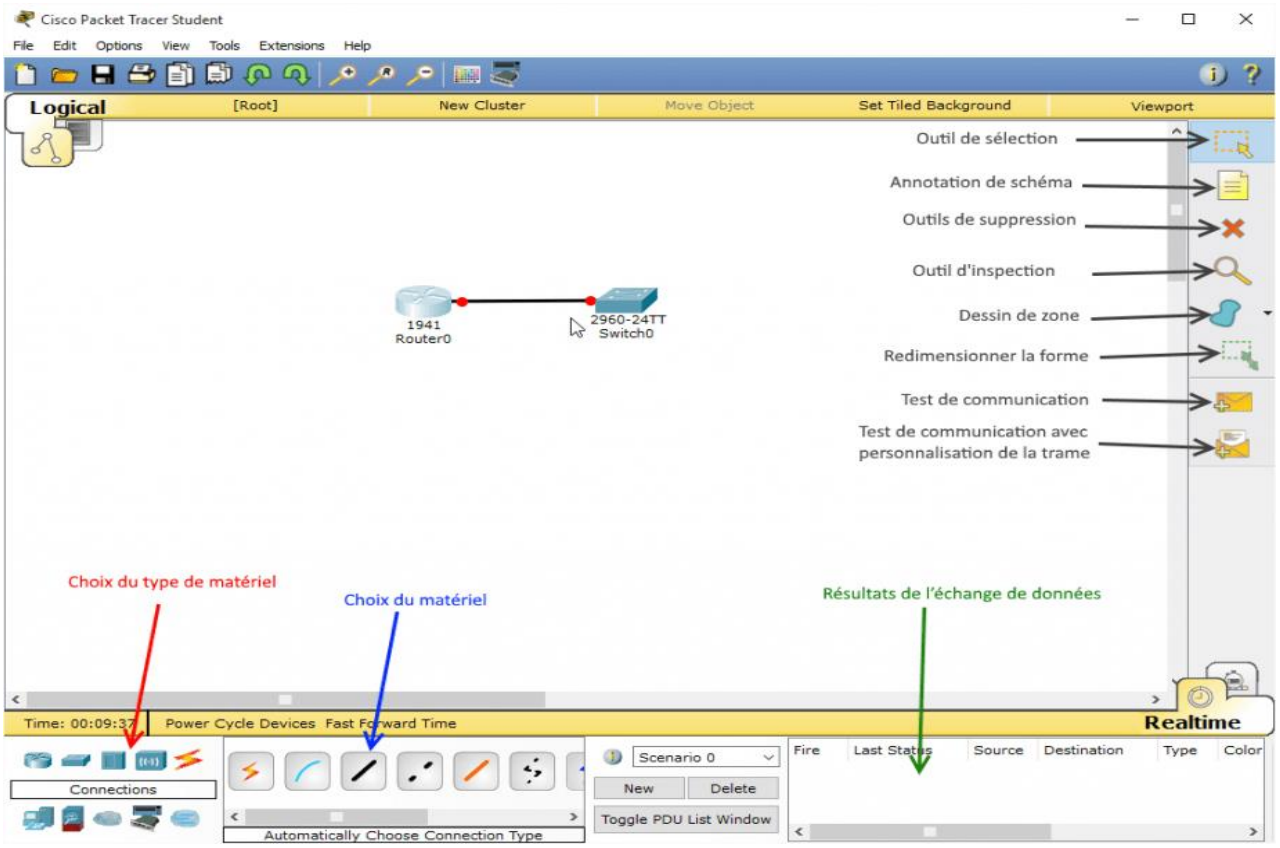


Figure 4.02 Présentation de l'interface Cisco Packet Tracer. [3]

E. Les types de matériels utilisés :

Le changement de la liste du matériel se faîte de manière dynamique selon leur type. Cette liste est conséquente et basée souvent sur des références CISCO réels. [3]

1. Les routeurs : appelé aussi Router ou Gateway (Passerelle) dans Internet, 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 commutateurs: aussi appelé SWITCH, fonctionnent au niveau Liaison, il a la mêmes Fonction qu'un pont mais utilisent des ports dédiés et non partagés.
3. 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, Thin ethernet, fibre optique).
4. Les bornes sans fil (wifi).
5. Les connexions ou appelé (câblage), on trouve plusieurs types tels que la fibre optique, câble coaxial, câble croisé, câble octal, etc. ...
6. Les ordinateurs.
7. la sécurité.
8. Les réseaux étendus (WAN).
9. Des appareils divers.
10. Les connexions multi-usagers.

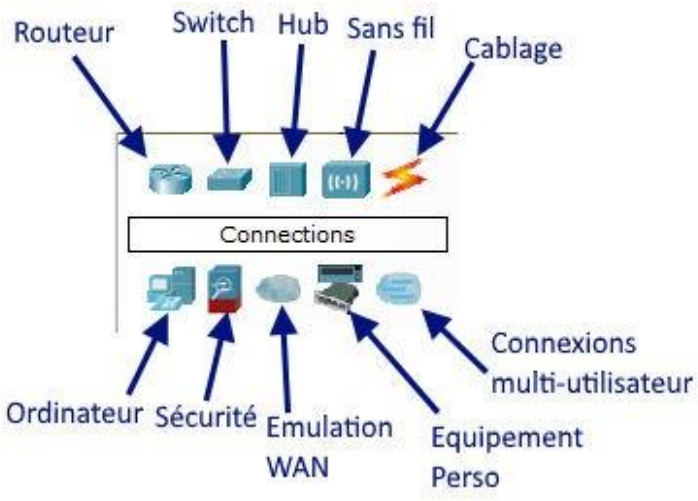


Figure 4.03 Matériels utilisés. [3]

Figure 4.04 Exemple d'ordinateurs.

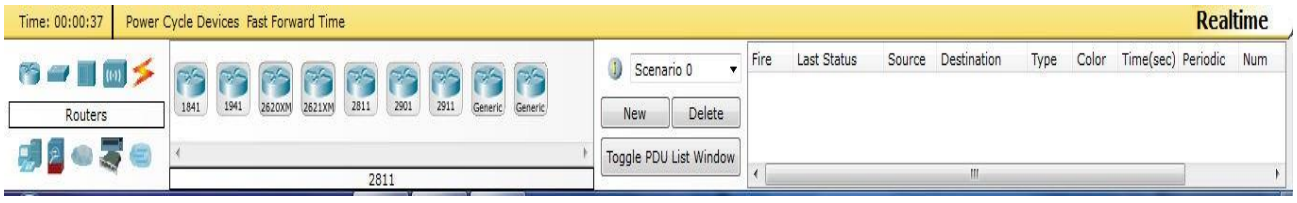


Figure 4.05 Exemple de router.

F. La catégorie câblage pour connecter les équipements :

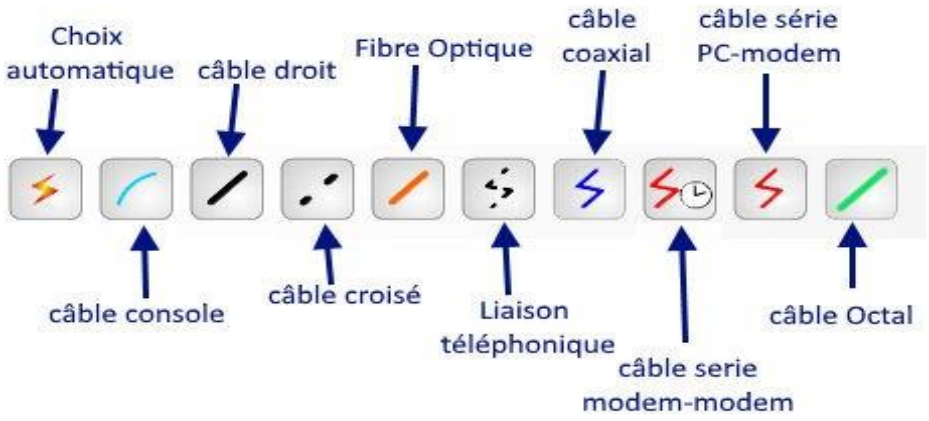
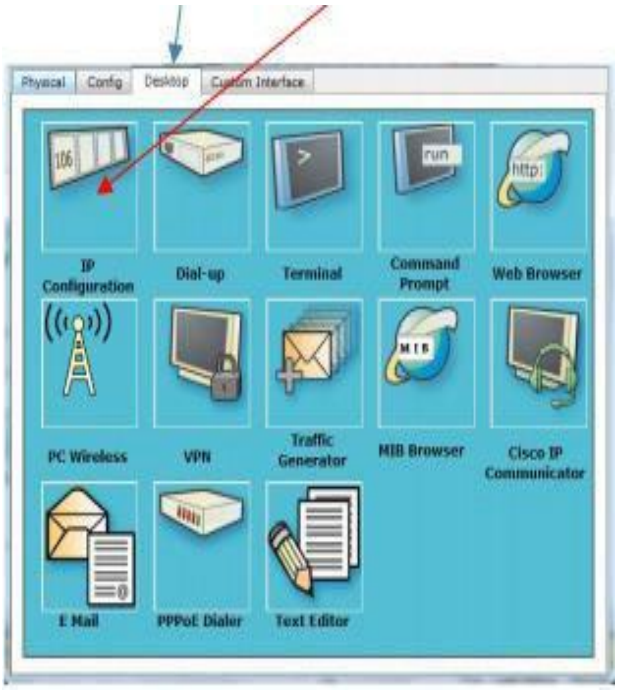


Figure 4.06 Les connecteurs des équipements.

G. 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.



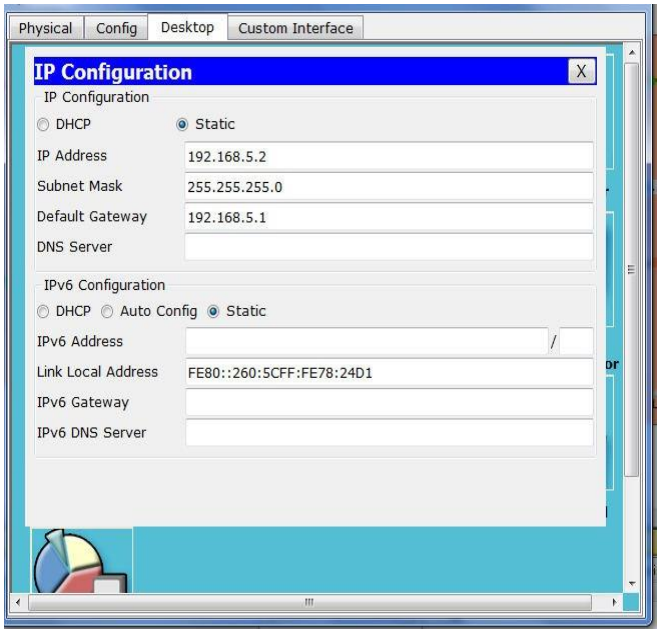


Figure 4.07 Des exemples d'ordinateur.

3. LA PARTIE DE SIMULATION :

3.1. LA CREATION DU RESEAU :

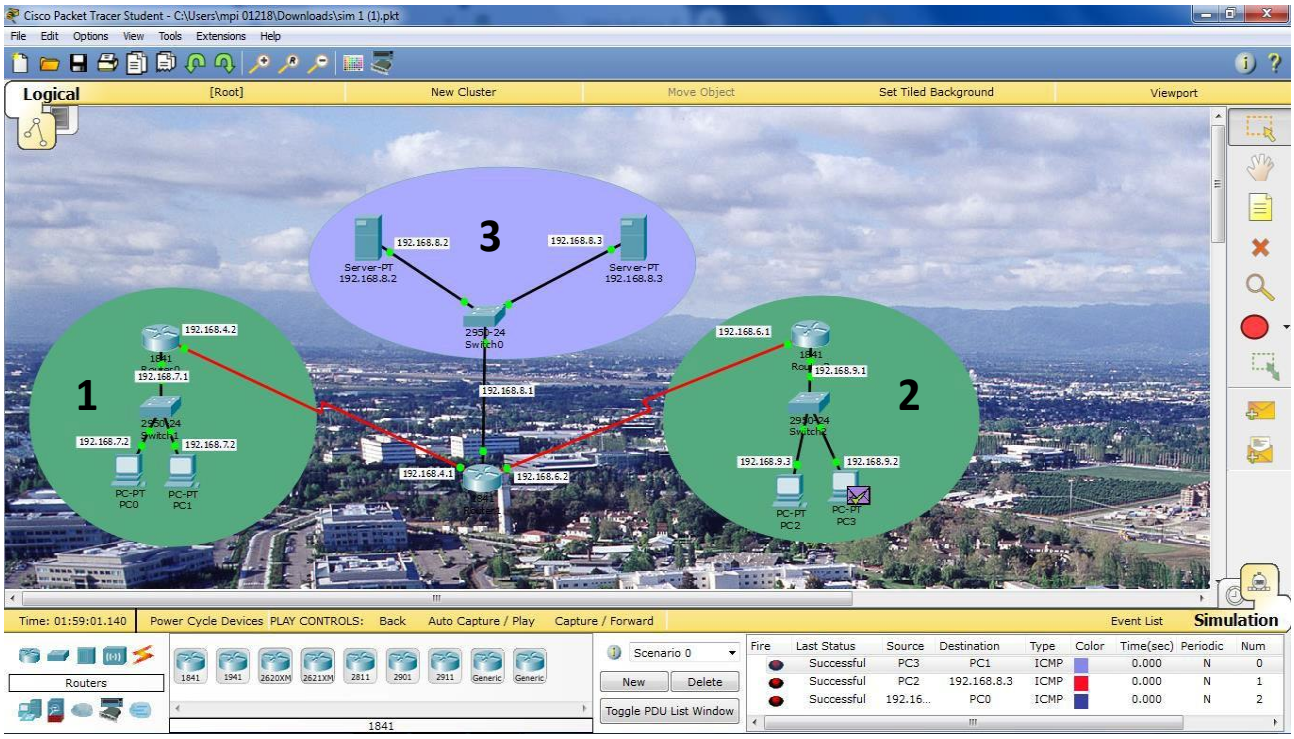


Figure 4.08 Un réseau informatique avec 3 sites.

❖ *Configuration de site 1 :*

1- On commence par les adresses IP de chaque ordinateur :

La configuration des ordinateurs ce fait par deux méthodes:

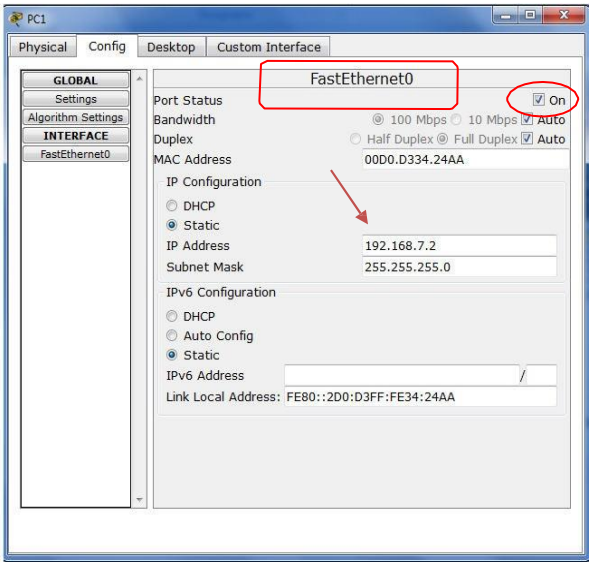


Figure 4.09 Configuration des PC.

i) Soit par la config :

On coche la case (on) pour activer l'interface, puis on tape l'adresse IP et le masque sera apparaîtra automatiquement.

Ensuite dans la case (settings) on tape le Gateway.

Display Name c'est pour nommer le PC.

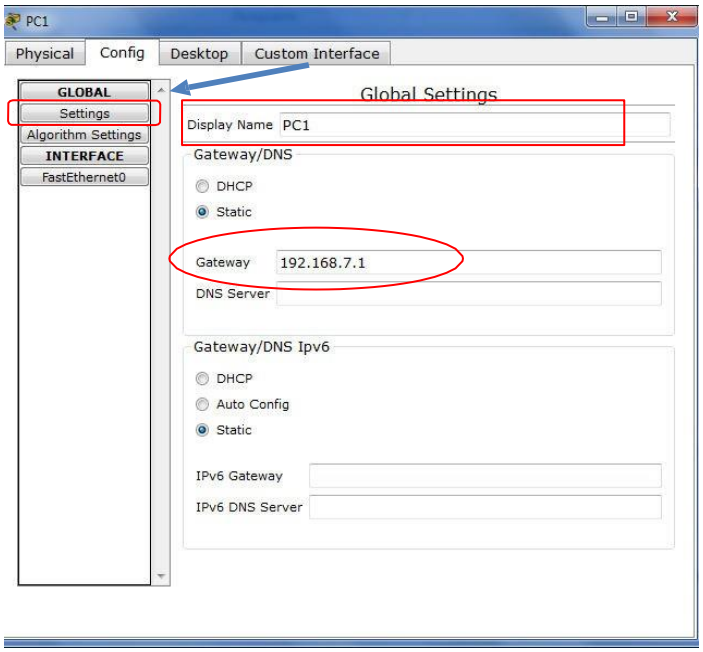


Figure 4.10 Configuration des pc.

ii) Par Desktop :

Dans ce cas on tape directement l'adresse IP, le Gateway et le masque par défaut.

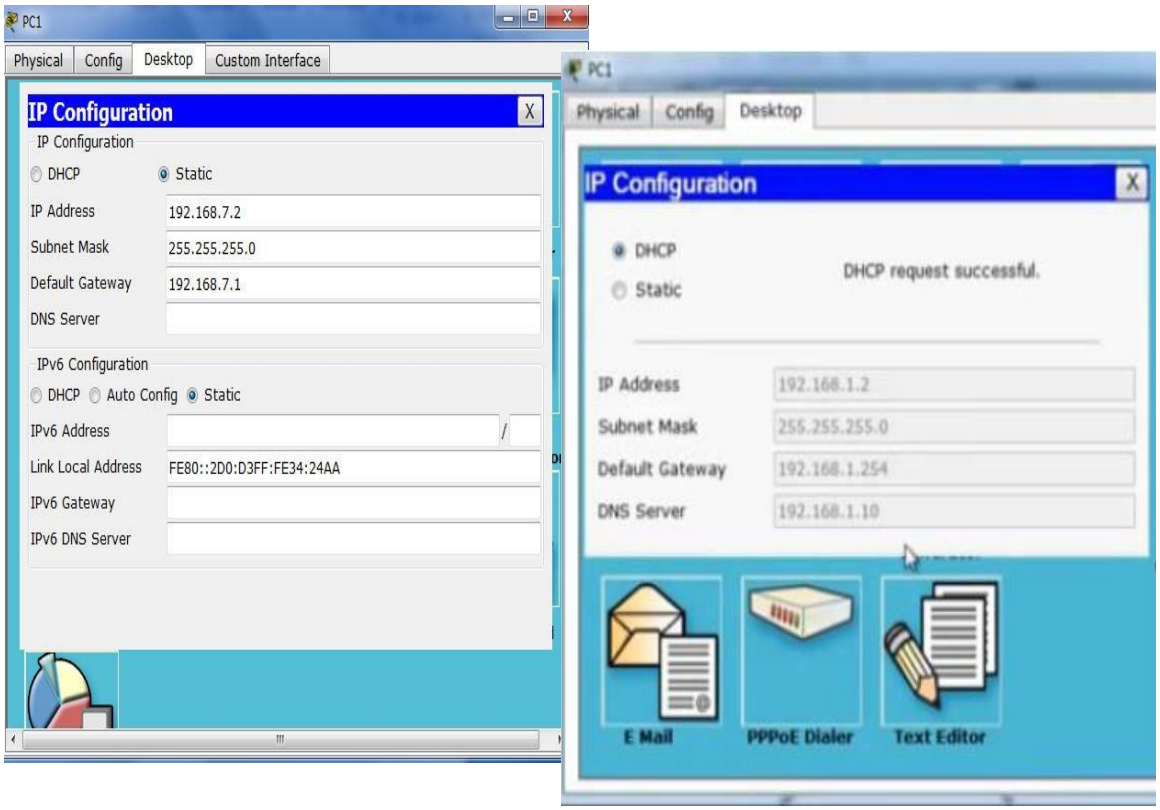


Figure 4.11 Configurations des PC par Desktop.

2- Configurations des Switch :

Pour nommer le Switch on utilise directement config ou par les commandes.

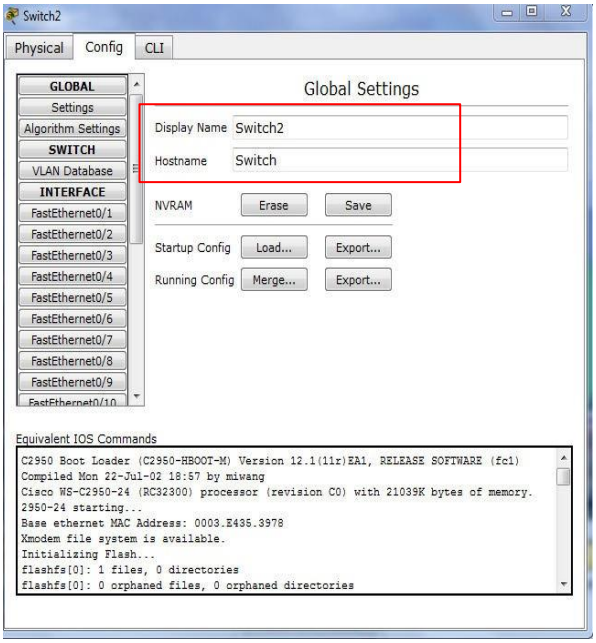


Figure 4.12 configuration des Switch.

3- Configuration des router :

Il existe deux méthodes de configuration :

- ✓ Configuration statique :

On active les interfaces puis on tape l'adresse correspondant à chaque interface.

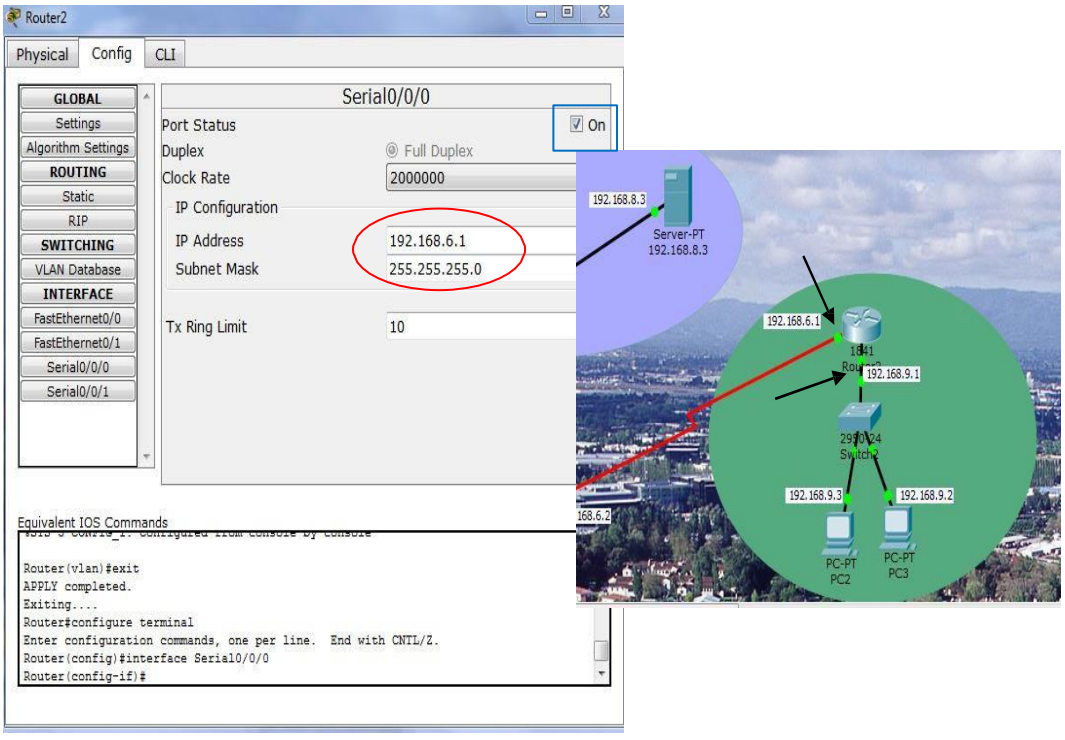


Figure 4.13 Configuration des router méthode statique.

✓ Configuration par commande :

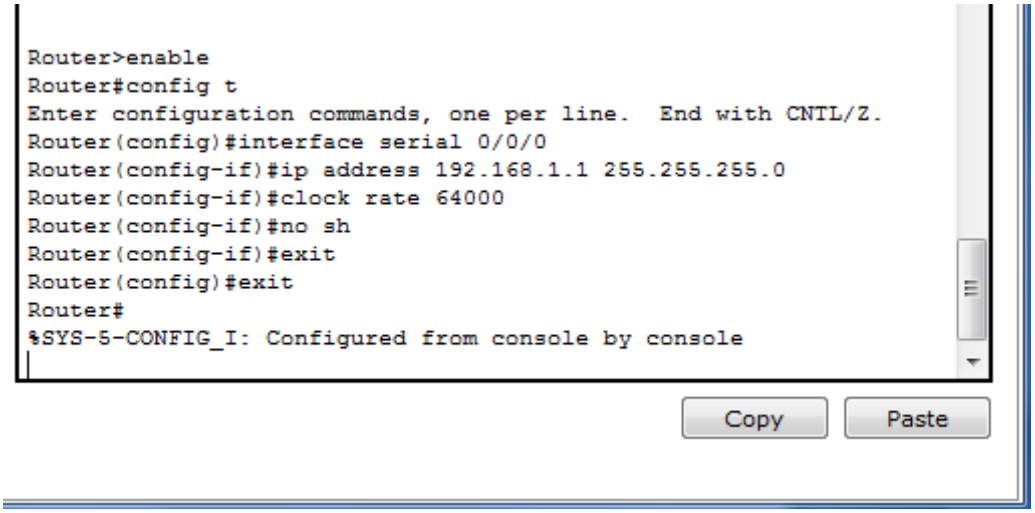


Figure 4.14 Configuration des router par des commandes.

4- Configuration des serveurs :

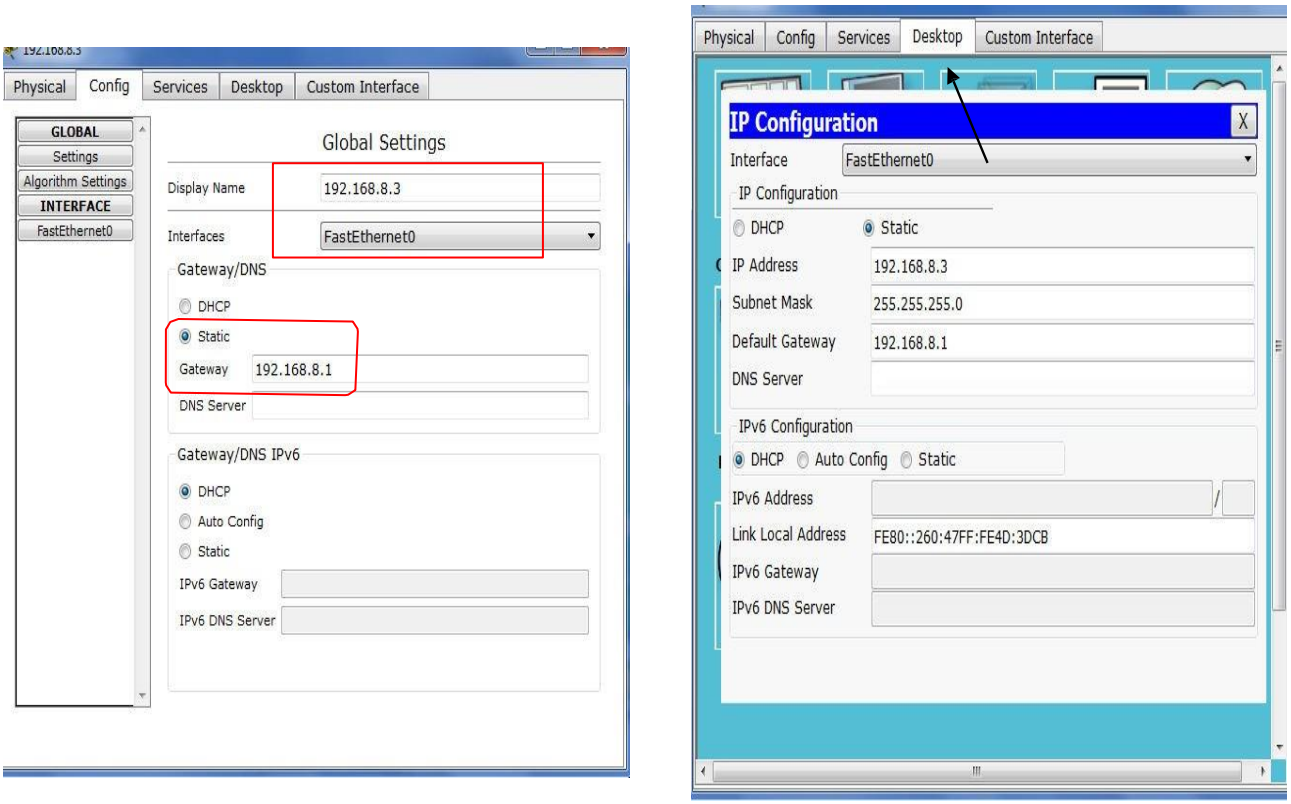


Figure 4.15 Configuration de server.

3.2. LA CREATION DU RESEAU VPN :

Notre thème se base sur la création du réseau IPsec VPN, en suivant ces étapes : [4]

A. Le choix des matériels pour définir le graphique de notre réseau.

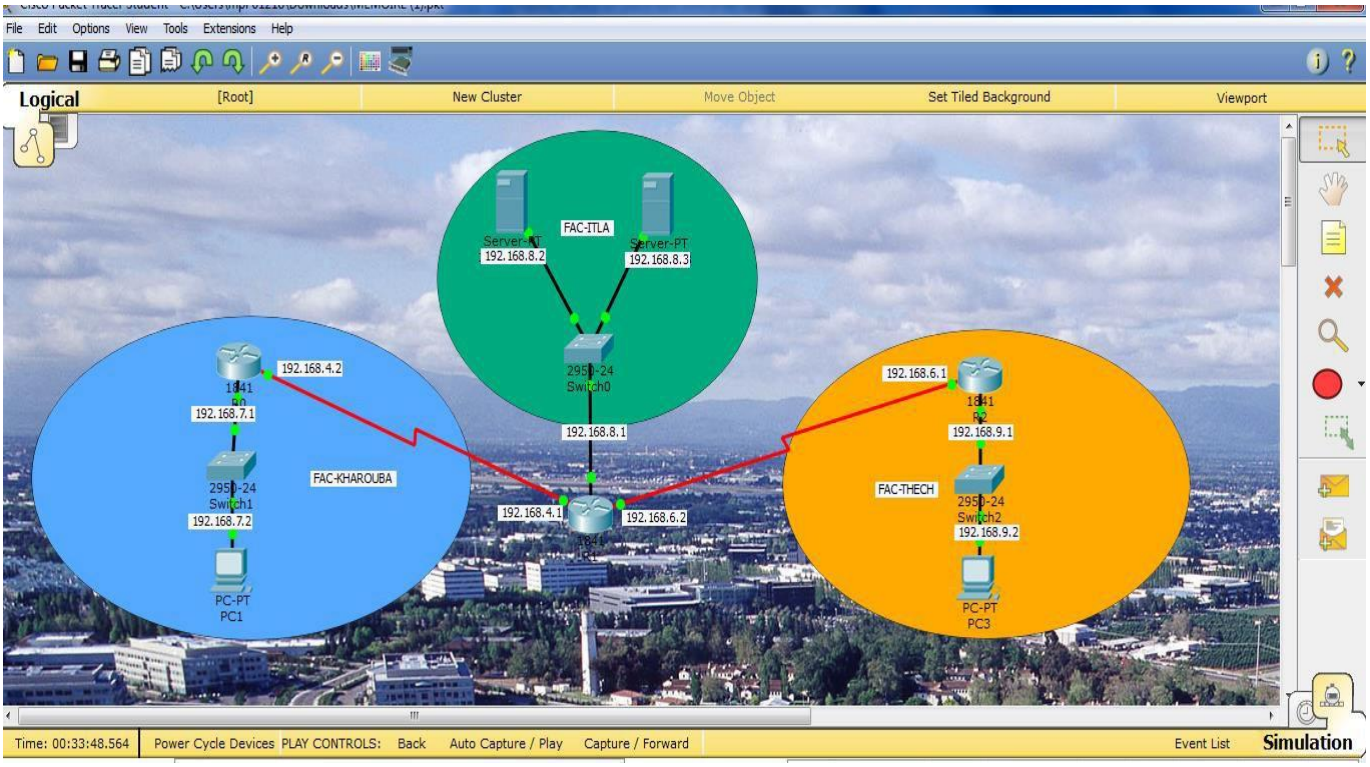
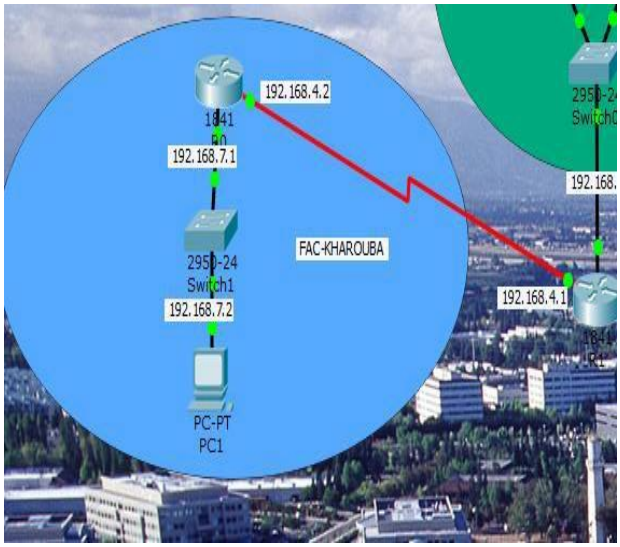


Figure 4.16 Schéma de réseau VPN.

- Notre réseau contient 3 sites (vert-bleu-orange) qui sont configuré par la méthode qui était expliqué avant.
  - ☆ Le site bleu correspondant au site de KHAROUBA:



Réseau : 192.168.7.1.

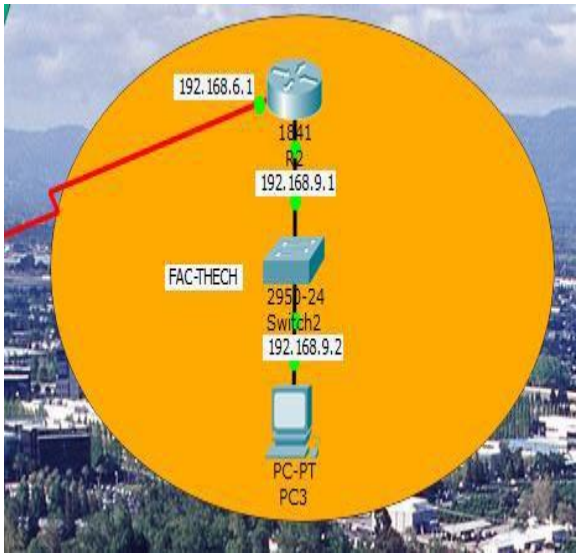
PC1: 192.168.7.2.

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 orange correspondant au site de la faculté FST :



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 :

Réseau : 192.168.8.1.

Server1 : 192.168.8.2.

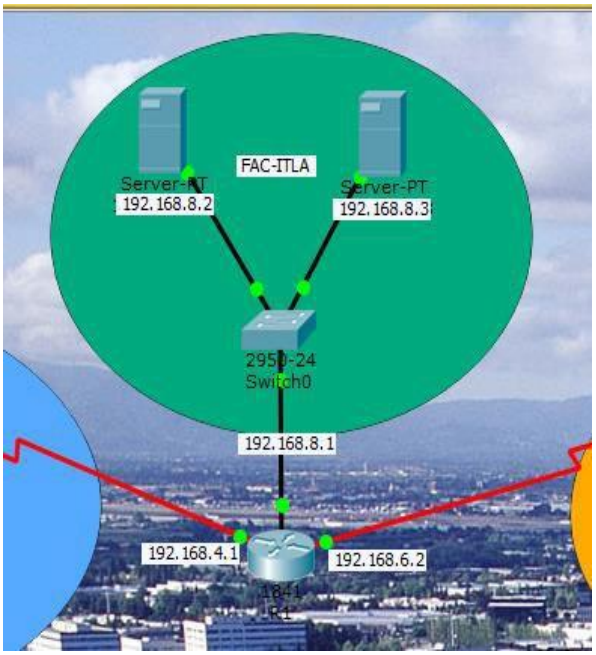
Server2 : 192.168.8.3.

Router:192.168.4.1.(Serail0/0/1)1

92.168.6.2.(Serail0/0/0)

192.168.8.1. (FastEthernet0/0).

Le masque de réseau: 255.255.255.0



4. Configuration VPN du routeur CISCO :

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 IPsec [5].

IPsec est un protocole VPN qui fonctionne sur la couche 3 du modèle OSI [6].

C'est aussi un standard IETF, ce qui signifie que nous pouvons l'utiliser entre les équipements de différents fabricants.

Les VPN IPSEC pour rappel permettent [7] *:*

-Une authentification de chaque paquet.

-Une vérification de l'intégrité des données de chaque paquet.

-De rendre confidentiels les données de chaque paquet IP.

Le diagramme ci-dessous montre notre scénario simple. Les deux sites ont une adresse IP publique statique, comme indiqué dans le diagramme.

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 [8], 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.

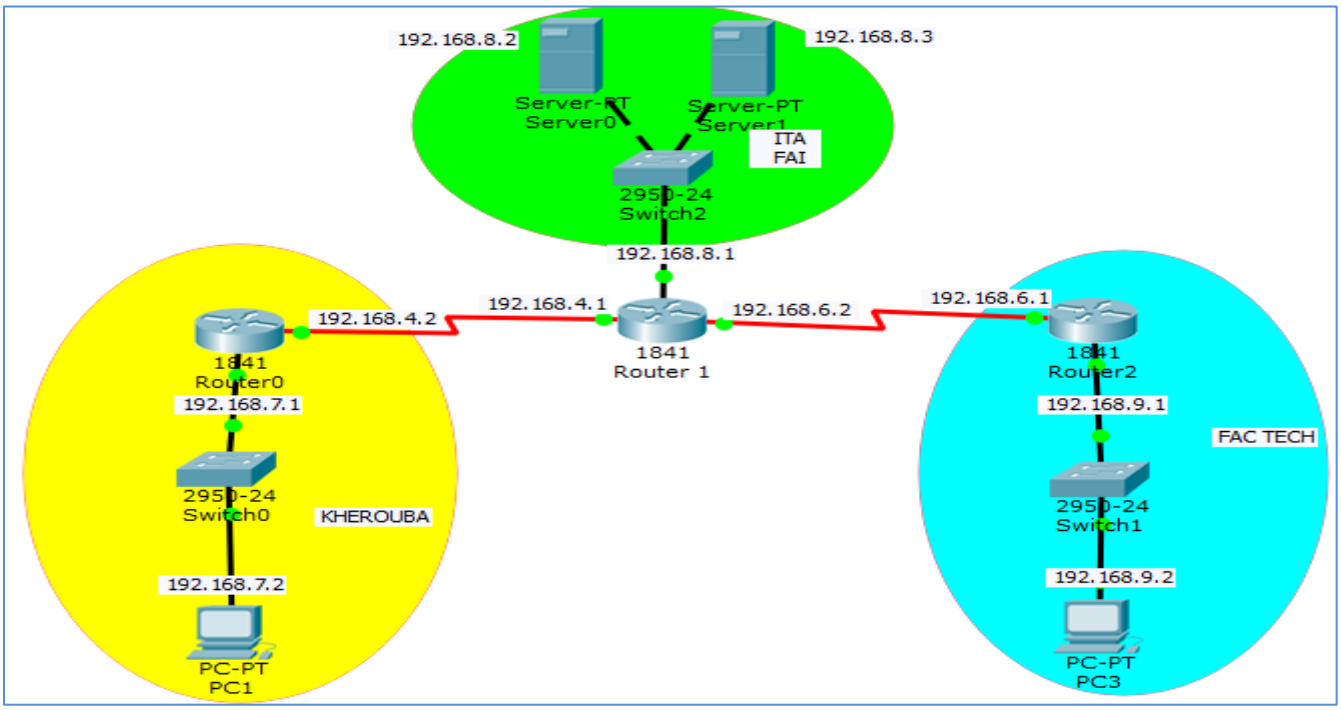


Figure 4.17 Schéma de réseau VPN.

Configuration du routage pour que les deux réseaux puissent communiquer

Prérequis

Avant de commencer à configurer le VPN IPsec, toujours s'assurer que les deux routeurs peuvent se joindre [9].

4.1. Configuration de base des routeurs (KHEROUBA-FAI-ITA-FACTECH) :

* 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)**

```
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
```

4.2. Configuration de la route par défaut, routeurs (KHEROUBA-FAI-FACTECH) :

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

```
KHEROUBA (config)#ip route 0.0.0.0 0.0.0.0 192.168.4.1
```

* 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 (FAC TECH)**

```
FAC TECH (config)#ip route 0.0.0.0 0.0.0.0 192.168.6.2
```

Après un **ping** de vérification, nous pouvons confirmer que les trois routeurs peuvent communiquer. Maintenant que le routage s'est bien passé nous allons sécuriser le réseau.

4.3. Mise en place d'un VPN IPSec :

Nous avons 6 étapes à suivre pour la mise en place du VPN : [10]

- 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 IPSec «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**

5. Configuration du routeur site 1 (Routeur KHEROUBA) :

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 [11], etc.

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

```
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
```

Voici les détails de chaque commande utilisée ci-dessus [12],

☆ **Crypto isakmp policy 1**-Cette commande crée la stratégie ISAKMP numéro 1. Nous pouvions créer plusieurs stratégies, par exemple7, 8,9 avec une configuration différente. Les routeurs participant à la négociation de la phase 1 essaient de faire correspondre une stratégie ISAKMP à la liste des stratégies une par une. Si une stratégie est mise en correspondance, la négociation IPSec passe à la phase suivante. On crée donc ici une stratégie avec un numéro de séquence 1.

Ce numéro indique la priorité de l'utilisation de la stratégie. Plus petit est ce nombre plus la priorité est grande.

- ☆ **authentication pre-share** - La **méthode d'authentification** est la clé pré-partagée.
- ☆ **encryption 3aes -** L'algorithme de cryptage 3AES **(Advanced Encryption 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 Diffie-Hellman** 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. (Valeur par défaut).

Ensuite, toujours dans la première partie, nous créons la clé partagée.

Étape 2. Création de **la clé de partage** [10] [13].

```
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 160.120.145.178.

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, quant à 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 **transform-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
```

Voici le détail de la commande utilisée ci-dessus [10] [14],

- **Crypto ipsec transform-set vpnset –** Crée un ensemble de transformation appelé vpnset
- **esp-aes** – la méthode de cryptage AES et le protocole ESP IPSec seront utilisés.
- **esp-md5-hmac** - L'algorithme de hachage MD5 sera utilisé.
- **Crypto ipsec security-association lifetime seconds-** Il s'agit de la durée de vie de la clé de cryptage.

Nous prenons soin de vérifier d'avoir utilisé les mêmes protocoles d'encryptions et de Hash utilisés Dans la première étape. Dans notre cas :***Encryption : aes, hash : md5*** [10] .

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 [10].

```
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 le détail de la commande utilisée ci-dessus,

☆ **ipsec-isakmp** – Crée une nouvelle carte de chiffrement avec le numéro de séquence

10. On peut créer plusieurs numéros de séquence avec le même nom, si on a plusieurs sites.

☆ **set peer 160.120.145.178**– 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**.

☆ **set transform-set vpnset –** Ceci relie le transform-set à la configuration de la crypto map.

Étape 6. Application de la Crypto Map à l'interface sortante de KHEROUBA [10].

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 traffic VPN du NAT Overload** [10].

```
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.

6. Configuration du routeur site 2 (Routeur FAC TECH) :

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

- 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 CRYPTOACL 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.

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 **transform-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 traffic VPN du NATO verload.**

```
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
```

7. 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 IPSec Phase 1, on tape **«show crypto isakmp sa»** comme indiqué :

```
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 IPSec Phase 2, On tape **«show crypto ipsec 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
```

Vous aurez ce qui y est dessous :

```
R2#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.4.2     192.168.6.1     QM_IDLE           1084    0 ACTIVE
```

1) Puis vous tapez :

R2# sh crypto ipsec sa

Vous aurez ce qui y est mentionné ci-dessous (en bas)

```
R2#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): (192.168.9.0/255.255.255.0/0/0)
 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: 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.:192.168.4.2
   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.
```

8. conclusion :

Dans ce chapitre, nous présentons l'interface et les performances du logiciel Cisco Packet Tracking sur lequel nous avons travaillé.

Notre étude est basée sur la simulation et la discussion de mieux appréhender la création et la configuration d'un tunnel VPN IPSec avec des commandes bien exécutées.

Les résultats de la simulation obtenus confirment la validité de l'étude car le tunnel fonctionne correctement et est bien sécurisé.

Conclusion générale

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.

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

Car 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.

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.

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.

Mais elle peut tout aussi bien être plus tard renforcée par d'autres approches et mises en place.

BIBLIOGRAPHIE, WEBOGRAPHIE et VIDEOTHEQUE

Chapitre 1 :

BIBLIOGRAPHIE :

[8] PUJOLLE.G, "les réseaux", France, Edition 2014

WEBOGRAPHIE :

[1] :file:///C:/Users/mpi%2001218/Desktop/m%C3%A9moire/uninice.pdf

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

[3] :https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/

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

[5] :https://docplayer.fr/17268016-Cours-10-les-reseaux-informatiques.html

[6] :http://eventus-networks.blogspot.com/2013/11/les-cables-et-le-cablage.html

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

[9] https://mehadjebia.wikeo.net/

http://www.sfrnet.org/sfr/societe/5-groupes-de-travail/3-Organiation-et-communication-metier/sfr-4i-dmp/sfrnet-magazine/article.phtml?id=rc%2Forg%2Fsfrnet%2Fhtm%2FArticle%2F2004%2Fmie-20040304-000000-07599

Chapitre 2 :

WEBOGRAPHIE :

[1] :https://a3c7.fr/w/index.php?title=Transpac

[2] : file:///C:/Users/mpi%2001218/Desktop/m%C3%A9moire/X25.pdf

[3] :https://www.cactusvpn.com/fr/beginners-guide-to-vpn/what-is-a-vpn-server-how-does-a-vpn-server-work/

[4] :http://renofika.blogspot.com/2015/05/makalah-virtual-private-network.html

[5]:file:///C:/Users/mpi%2001218/Downloads/Tutorial_VPN.pdf

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

Chapitre 3 :

BIBLIOGRAPHIE :

[2] Philippe Atelin and Jos_e Dordoigne." TCP/IP et les protocoles Internet". Editions ENI, 2006.

[4] DORDIOGNE.J " Reseaux informatiques "- notions fondamentales, ENI RI4RES

WEBOGRAPHIE :

[1] :
file:///C:/Users/mpi%2001218/Desktop/m%C3%A9moire/ADMINISTRATION%20DES%20RESEAUX%20INFORMATIQUES%20By%20Prof.%20YENDE%20R..pdf

[3] https://www.proxyvpn.fr/qu-est-ce-qu-un-proxy?fbclid=IwAR17t2yy-W7SFaiOc7ZCJj30kzlXZVVAjC3RqaTZTXb-KBsuHu9-m7xpwrM#:~:text=Un%20proxy%2C%20que%20l'on,r%C3%A9seau%2C%20le%20plus%20souvent%20internet

[5] file:///C:/Users/mpi%2001218/Desktop/m%C3%A9moire/www.cours-gratuit.com--m6-id039.pdf

[6] https://www.speedcheck.org/fr/wiki/tunneling/?fbclid=IwAR2eAatyj-ayP7qRghFfb1LqsWQZlK2gEPNV9O964fEPUXKQABNHvIohm_Q#:~:text=Tunnelage%20obligatoire-,Fonctionnalit%C3%A9,ils%20sont%20crypt%C3%A9s%20et%20encapsul%C3%A9s

[7] https://www.commentcamarche.net/faq/17446-qu-est-ce-qu-un-routeur?fbclid=IwAR2TPV2WiUFpXczPMcPEmuFsU8fMeNwKoD5GL6Id4iybnRCSEX1kB0V7cUE#:~:text=Les%20protocoles%20de%20routage,-Les%20protocoles%20de&text=%C3%A9tats%20de%20lien%2C%20ils%20s,utiliser%20la%20meilleur%20route%20%3A%20OSPF

[8] https://www.memoireonline.com/04/10/3431/m_Etude-et-optimisation-du-reseau-local-de-inova-si6.html?fbclid=IwAR1oZ7XmMGhAVqybLhrPU2PyBFU2fkxHoNah2SD5ZVw8wa0cAa2KFlEfJrs#:~:text=Par%20d%C3%A9finition%2C%20un%20VLAN%20(Virtual,utilisateurs%2C%20p%C3%A9riph%C3%A9riques%2C%20etc.)

[9] https://www.institut-numerique.org/chapitre-iv-administration-et-securite-reseau-51b1eda86c424

Chapitre 4 :

BIBLIOGRAPHIE :

[4] : Jean-François Challande Jean-Louis Lequeux. – Le grand livre DU DSI, Edition Eyrolles 2009;

[5] : C. Pernet. – Sécurité et espionnage informatique

[6] : Ghernaouti-HélieS., Sécurité informatique et réseaux, Edition DUNOD, Paris, 2011;

WEBOGRAPHIE :

[1] :https://www.britannica.com/topic/Cisco-Systems-Inc

[2] :http://projet.eu.org/pedago/sin/tutos/packet_tracer.pdf?fbclid=IwAR1SDLkp8gsxh75QpX2ztAQufk6KGvfKLIVk0u9DblLbwG04C59Ea0vDesA

[3] : https://labo-tech.fr/base-de-connaissance/comment-utiliser-linterface-de-cisco-packet-tracer/?fbclid=IwAR3MsgSyrB4jleAssQWPN7GM_HXBcR4ljB_oMaRZsS43xC9FpPLI6gErPuo

[7] : Réseau privé virtuel VPN :https://www.frameip.com/vpn/

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

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

[10]: 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/

[11]: VPN site to site :https://www.supinfo.com/articles/single/921--vpn-site-to-site

[12] : La mise en place d'un VPN :https://www.supinfo.com/articles/single/2384-mise-place-vpn

[13] : Configuration d'un vpn ipsec entre deux routeurs cisco :
http://www.lolokai.com/blog/2012/03/27/configuration-dun-vpn-ipsec-entre deux-routeurs-cisco/

[14] : IKE: http://pteu.fr/doku.php?id=informatique:cisco:ipsec

[15]: CONFIGURATION D'UN VLAN SUR SWITCH CISCO:

https://www.fbotutos.com/configuration-dun-vlan-sur-switch-cisco.html

VIDEOTHEQUE:

- Alphorm – Reseaux Cisco (1-2) - Maitriser la sécurité
- Faire communiquer des machines dans des vlans différents via un routeur (Prince Attobla)
https://www.youtube.com/watch?v=UXRphawCH4c