République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Réseaux et Télécommunication**

Présenté par
Lyes AOUICHE
Moussa FARSI

Thème

Etude Et Configuration De La Carte de Supervision CISCO WS-SUP720-3B

Mémoire soutenu publiquement le 29/06/ 2017 Devant le jury composé de :

M Prénom NOM
Grade, Lieu d'exercice, Président

Mr F. OUALLOUCHE
Maitre de conférence, UMMTO, Encadreur

M Prénom NOM
Grade, Lieu d'exercice, Examinateur

Promotion 2016/2017

Remerciements

On tient à remercier tout d'abord notre Promoteur, Mr F.OUALLOUCHE, pour sa patience, et surtout pour sa confiance, ses remarques et ses conseils, sa disponibilité et sa bienveillance.

Qu'il trouve ici le témoignage de notre profonde gratitude.

On voudrait également remercier les membres du jury pour avoir accepter d'évaluer ce travail et pour toutes leurs remarques et critiques.

On tient aussi à remercier le personnel du Centre des Systèmes et Réseaux d'information, de Communication, de Télé-enseignement et enseignement à Distance Ex Centre de Calcul de l'université de Mouloud Mammeri de Tizi-Ouzou qui nous a aidés dans nos recherches et leurs dispositions

Enfin, nous tenons à exprimer notre profonde gratitude à nos familles qui nous ont toujours soutenues et à tout ce qui participe de réaliser ce mémoire. Ainsi que l'ensemble des enseignants qui ont contribué à notre formation.

Dédicace

Je dédie ce modeste travail :

A la mémoire de mon défunt père,

et à tous ceux qui me sont chers et proches,

A ma chère mère pour son soutien incroyable,

A mon frère et mes sœurs qui ont été la pour moi tout le long de mon parcours,

Ainsi que tous mes amis et toute ma famille pour leurs soutiens

Et tous les étudiants de la promotion 2016/2017

Option : Réseaux et Télécommunications,

A tous ceux qui, par un mot, m'ont donné la force de continuer….

AOUICHE Lyes

Dédicace

Je dédie ce modeste travail :

A Mes très chers parents à qui je doits tout, je profite de les remercier pour leur encouragement, leur aide, le soutien qu'ils m'ont apporté et le sacrifice qu'ils ont fait pour moi, que dieu les protège et les entoure de sa bénédiction.

A la mémoire de mon grand-père **Farsi Lounes.**

A ma chère grand-mère.

A mes grands parents maternels.

A mes chères sœurs **Souad, Malha, Lamia.**

A mes cousins et cousines.

A tous mes ami(e)s qu'à tous ce qui me sont chers

Et a tous ceux qui m'ont aidé et tous ceux qui m'ont connu de près et de loin.

Moussa FARSI

Résumé

Les réseaux et les systèmes d'information sont devenus actuellement des outils indispensables au fonctionnement des entreprises, donc La pérennité de toute entreprise passe aujourd'hui par une disponibilité permanente de ces derniers.

La stabilité des réseaux est due a l'implémentation de différentes technologie que se soit matériel ou logiciel au sein de son architecture. Ce pendant, les principaux enjeux du moteur de supervision Cisco « WS-SUP720-3B » est ainsi de réussir à offrir des performances évoluées et fournir des sévices nouveaux et avancés sur les performances et la sécurité du réseau.

Durant notre travail qui s'est déroulé au sein du Centre des Systèmes et Réseaux d'information, de Communication, de Télé-enseignement et enseignement à Distance Ex Centre de Calcul de l'université de Mouloud Mammeri de Tizi-Ouzou, nous sommes basés au premier temps sur un audit sur le réseau. Ensuite, nous sommes intéressés à l'étude détails du moteur de supervision Cisco « WS-SUP720-3B », afin d'arriver à la simulation et la configuration de ce dernier sous GNS3, ou nous avons opté pour deux topologies, la première topologie est consacré pour une configuration basique du moteur de supervision ou nous sommes intéressés a la configuration des VLANs, les ACLs, et un serveur DHCP pour la distribution automatique des adresses IP dans notre réseau pour montrer son utilité au sein du réseau de l'université ou il est utilisé comme un routeur performent , et en guise de perspective nous avons opté pour la deuxième topologie pour l'implémentation d'une application de sécurité qui est le VPN reposant sur un technologie comme IPSec.

Mots clés : Cisco, Moteur de supervision, GNS3, VPN, Vlan, Carte de supervision, Routeur, Sécurité informatique, IPSec.

Chapitre I: Généralités sur les réseaux informatiques

Chapitre II: Sécurité des réseaux informatiques

Chapitre III: Etude et Présentation de supervision Ws-sup72-3B

Chapitre IV: Configuration du moteur de supervision sous GNS3

AAA	Authentication Authorization Accounting
aCEF	Cisco Express Forwarding accéléré
ACL	Access Control List
ARP	Adress Resolution Protocol
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CEF	Cisco Express Frowarding
CSMA /CD	Carrier Sense Multiple Access /Collision detection
dCEF	Cisco Express Forwarding distribué
DHCP	Dynamic Host Configuration Protocol
DNS	Domaine Name Service
FDDI	Fibre Distributed Data Interface
FTP	File Transfert Protocol
GNS3	Graphical Network Simulator
GRE	Generic Routing Encapsulation
HSRP	HostStandby Redundcy Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Détection System
IGP	Interior Gateway Protocol
IP	Internet Protocol

IPS	Intrusion Prevention System
IPSec	IP Security
IS-IS	Intermediate System to Intermediate Systems
LAN	Local Area Network
MAN	Metroplitain Area Network
MPLS	Multi Protocol Label Switching
MSFC	Multi-layer Switch Feature Card
NAT	Network address translation
NIC	Network Interface Card
OSI	Open SystèmeInterconnexion
OSPF	Open Shortest Path First
PAN	Personal Area Network
PFC	Policy Feature Card
QoS	Quality of Service
RARP	Reverse Address Resolution Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TELNET	Terminal NETwork protocol
TFTP	Trivial File transfer Protocol

UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VRRP	Virtuel Router Redundcy Protocol
VPN	Virtual Private Network
WAN	Wide Area Netwok

Chapitre I

Chapitre II

Chapitre III

Chapitre IV

Chapitre I

Chapitre III

INTRODUCTION

La pérennité de toute entreprise passe aujourd'hui par une disponibilité permanente de son système d'information. L'information nécessaire au bon fonctionnement de l'entreprise englobe aussi bien les données stratégiques que les données de tous les jours. Le système d'information représente dans ce cas un ensemble qui inclut aussi bien l'information elle-même que les systèmes nécessaires pour la mettre en œuvre[1]. Le premier souci de l'entreprise est d'avoir un fonctionnement continu du système d'information et la disponibilité de l'information nécessaire pour tous les employés de l'entreprise. Ces deux objectifs reposent sur l'utilisation d'un réseau d'entreprise sécurisé.

L'architecture physique ou logique d'un réseau dépend des équipements utilisés [2]. En effet, dans un réseau d'entreprise, plusieurs équipements sont nécessaires pour interconnectés les ordinateurs ou les segments d'un réseau [1,3]. Remplacer un équipement ou changer son emplacement dans le réseau permet de modifier l'architecture du réseau. A cet effet, il est indispensable de connaitre le fonctionnement et la configuration des différents éléments d'un réseau d'entreprise.

Dans le cadre de notre mémoire de fin d'études, nous avons effectué un stage au Centre des Systèmes et Réseaux d'information, de Communication, de Télé-enseignement et enseignement à Distance Ex Centre de Calcul de l'université de Mouloud Mammeri de Tizi-Ouzou. Ce centre a pour mission principale la gestion et la maintenance du réseau de l'université. A cet effet, des anomalies de fonctionnement du réseau ont été constatées par les ingénieurs de ce centre. Afin d'y remédier, un audit du réseau est nécessaire. Une partie de ce travail nous a été confiée. Celle-ci a pour mission l'étude et la configuration d'un équipement de supervision Cisco « WS-SUP720-3B » afin de proposer une meilleure exploitation de cet équipement. Actuellement, il est utilisé par le centre de calcul comme routeur.

Afin de montrer les étapes de configuration de la carte de supervision nous utiliserons les logiciels GNS3 et Vmware pour simuler une partie du réseau de l'université. Une autre simulation sera effectuée pour démontrer un autre fonctionnement de cette carte dans un réseau.

Ce présent mémoire est structuré en quatre chapitres

Dans le premier chapitre, nous avons procédé à une étude préliminaire sur les réseaux informatiques en générale, les différents concepts des modèles en couche le TCP/IP et l'OSI et aussi les différents protocoles susceptibles d'être utilisé dans un réseau.

Le second chapitre est consacré à la sécurité informatique. Nous évoquerons les différentes politiques de sécurité et les différentes attaques auxquelles les réseaux sont exposés. Ensuite, nous donnerons quelques mécanismes de sécurité permettant de contrer ces attaques.

Une étude détaillée du moteur de supervision Cisco « WS-SUP720-3B » fera l'objet du troisième chapitre.

Le quatrième chapitre, est consacré à la simulation de deux réseaux sous GNS3 et VmWare.

Nous terminons notre travail par une conclusion et les perspectives.

Chapitre I
Généralités sur Les Réseaux informatiques

I.1 Préambule

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à des gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types d'ordinateurs, que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (recherche, bases de données, gestion …) et des particuliers (messagerie, loisirs, services d'informations et internet…).

Dans ce chapitre, il s'agit de mettre notre travail dans son contexte général, et introduire des notions théoriques jugées nécessaire pour le déroulement de notre travail.

I.2 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements informatiques (ordinateurs et périphériques) reliés entre eux grâce à des supports matériels et logiciels. Ces derniers peuvent être matériel ou immatériel…. (Câble : réseau câble, ou onde : réseau sans fil...). Les objectifs recherchés dans le cas des réseaux informatiques sont essentiellement la communication et le partage des ressources. Permettant la communication (transfert des informations électroniques) et le **partage de ressources** (matérielles et logicielles).

I.3 Classification des réseaux informatiques

On peut classer les réseaux selon plusieurs critères :

I.3.1Classification selon la taille

On distingue généralement quatre catégories de réseaux informatiques différenciés par la distance maximale séparant les points les plus éloignés du réseau :

- **Les réseaux personnels** (PAN : Personal Area Network) :

Désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Les bus utilisés les plus courants sont l'USB, les technologies sans fil telles que Bluetooth, l'infrarouge(IR). Par exemple, une personne utilisant un téléphone portable peut très bien transférer son répertoire dans sa clé USB. Il utilisera alors BlueTooth pour passer par son ordinateur qui lui-même enverra sur la clé USB connectée par une rallonge.

➢ **Les réseaux locaux** (LAN : Local Area Network) :

Correspondent par leurs tailles aux réseaux intra-entreprises. Ils servent au transport de toutes les informations numériques de l'entreprise. En général, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à quelques centaines de mégabits par seconde.

➢ **Les réseaux métropolitain** (MAN:Metroplitain Area Network):

Permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leurs donner la possibilité de dialoguer avec l'extérieur.

➢ **Les réseaux étendus** (WAN : Wide Area Network) :

Sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voir un continent ou plusieurs continents. Le réseau est soit terrestre, en ce cas, des infrastructures sont établies au niveau du sol, essentiellement de grands réseaux de fibre optique, soit Hertzien comme les réseaux satellites.

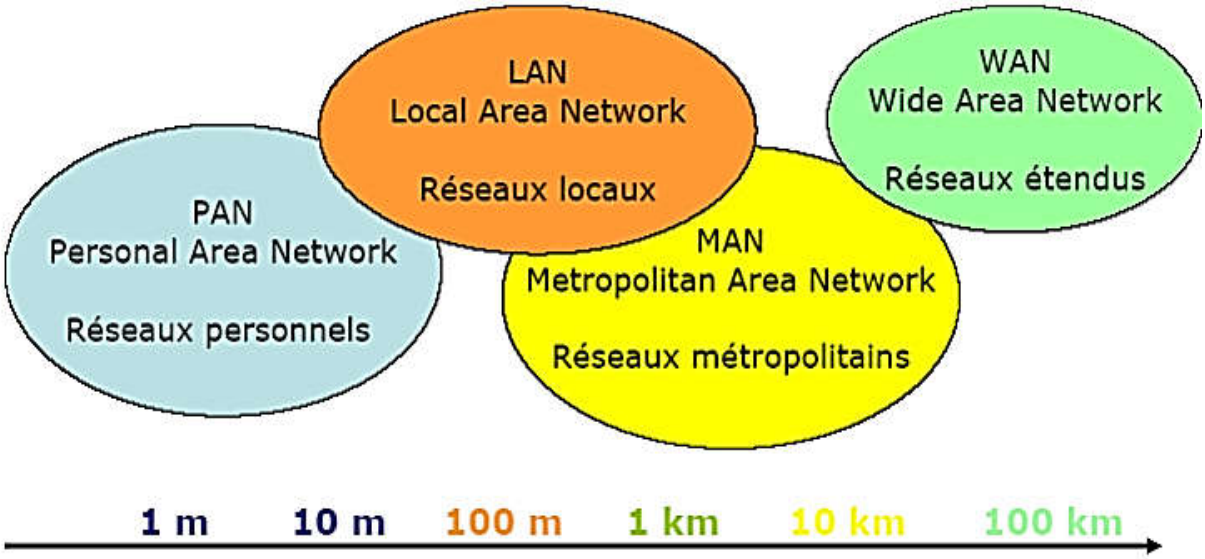

Figure I.1 : La Classification des réseaux informatiques selon leur taille

I.3.2. Classification selon la topologie

La topologie est la façon d'agencer les équipements (postes, imprimantes, serveur, etc.) interconnectés dans un réseau local.La topologie peut comporter deux aspects :

A. Topologie Physique

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique du réseau est appelé topologie physique

➢ Topologie en bus

Le bus, un segment central où circulent les informations, s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinatrice peut les récupérer. Une seule station peut émettre à la fois. En bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre.

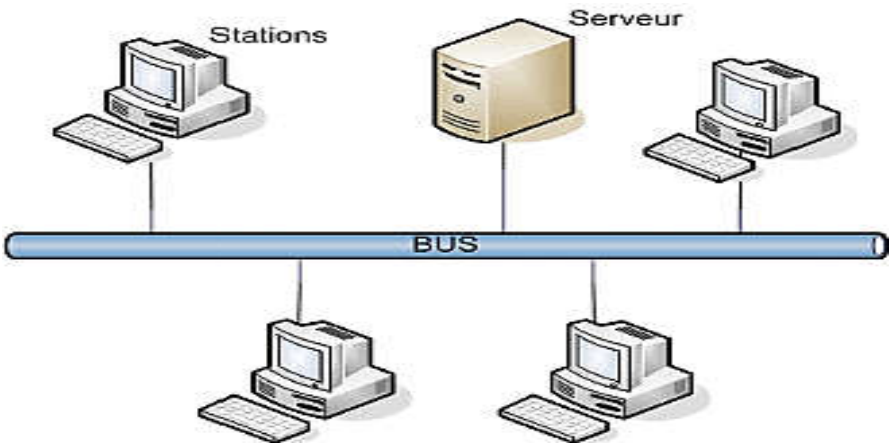

Figure I.2 : Topologie en bus.

➢ Topologie en anneau

Cette architecture est principalement utilisée par les réseaux Token Ring. Token Ring utilise la technique d'accès par « jeton ». Les informations circulent de stations en stations, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite…

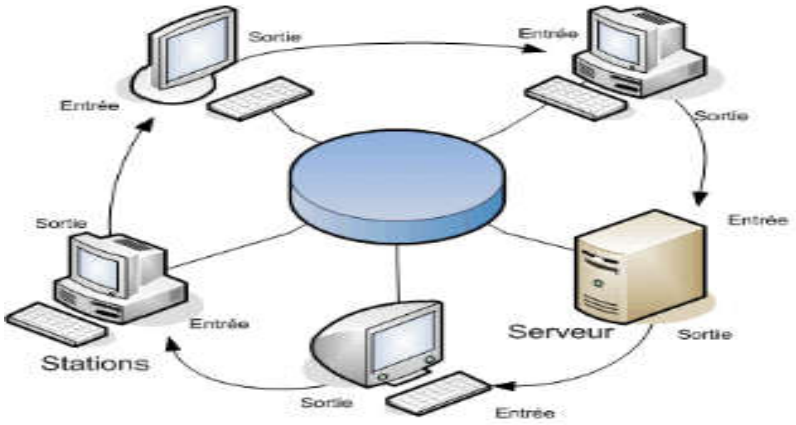

Figure I.3 Topologie en anneau.

- **Topologie en étoile**

C'est la topologie la plus courante. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet vers le concentrateur, celui-ci envoie les données à toutes les autres machines (hub) ou à celle qui en est le destinataire (Switch).

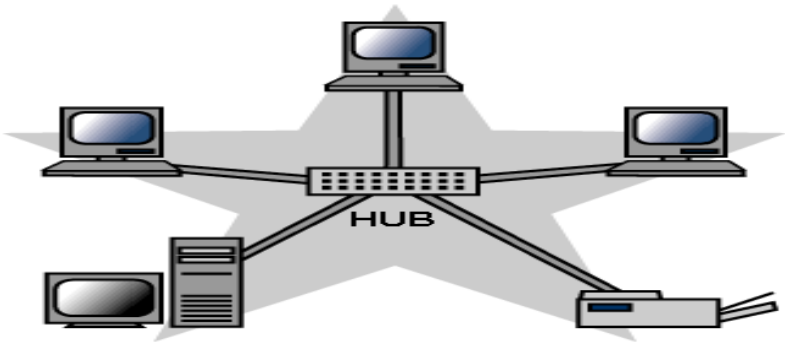

Figure I.4 : Topologie en étoile

B. Topologie logique

Correspond à la manière de faire circuler le signal parmi les composantes physiques (on parlera des méthodes d'accès au canal). Par opposition à la topologie physique, elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont :

- **Méthode d'accès CSMA/CD**

CSMA : Carrier Sense Multiple Acces

Accès Multiple avec écoute de la porteuse. Ce protocole est défini par la norme IEEE 802.3. Lorsqu'une station désire prendre un médium pour la transmission de donnes, la méthode CSMA lui impose d'écouter le support physique de liaison (câble ou fibre) pour déterminer si une autre station n'est pas déjà en train de transmettre une trame de données par détection d'une tension électrique ou présence de lumière. S'il n'y a pas d'émission en cours (donc pas de signal), elle suppose qu'elle peut émettre.

CD : Collision detection (détection de collisions)

Ce protocole est défini par la norme IEEE 802.3. Par cette méthode, une machine qui est en train d'émettre une trame, écoute en même temps le médium. Si une autre machine émet en même temps, les données émises et celles perçues ne sont plus concordantes. Il y a détection d'une collision. Dans ce cas, l'émission est stoppée immédiatement. Le système se remet en attente pendant un délai aléatoire avant de lancer une nouvelle séquence de CSMA pour tenter la réémission de la trame.

- **Token ring**

La méthode du passage du jeton est une méthode propre aux réseaux en anneau. Les collisions sont proscrites, les stations ne peuvent pas émettre simultanément. Les stations doivent attendre le jeton qui donne la permission de « parler », il y a des délais d'attente pour obtenir le jeton, mais il n'y a pas de collisions, donc pas de délais de retransmission. Le jeton est un paquet spécial qui passe de station en station, et qui autorise celle qui le détient à émettre.

- **LAN FDDI**

La technologie LAN FDDI (Fibre Distributed Data Interface) est une technologie d'accès au réseau sur des lignes de type fibre optique. Il s'agit en fait d'une paire d'anneaux (l'un est dit "primaire", l'autre, permettant de rattraper les erreurs du premier, est dit "secondaire"). Le FDDI est un anneau à jeton à détection et correction d'erreurs (c'est là que l'anneau secondaire prend son importance).

I.3.3 Classification selon le mode de connexion

a) Mode avec connexion

Il s'agit des protocoles opérant un contrôle de transmission des données pendant une communication établie entre deux machines (émettrice, réceptrice). La machine

réceptriceenvoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données qu'elle envoie.

b) Mode sans connexion

Il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyerd'avis de réception à la première.

I.4 Architecture des réseaux

Les réseaux sont structurés du point de vue fonctionnel en deux catégories :

- **Réseaux poste a poste (peer to peer)**

Dans une architecture peer to peer, contrairement à une architecture de réseau informatique de type client/serveur, il n'y a pas de serveur dédié.Ainsi chaque ordinateurdans un tel réseau est un peu serveur et un peu client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder via le réseau informatique.

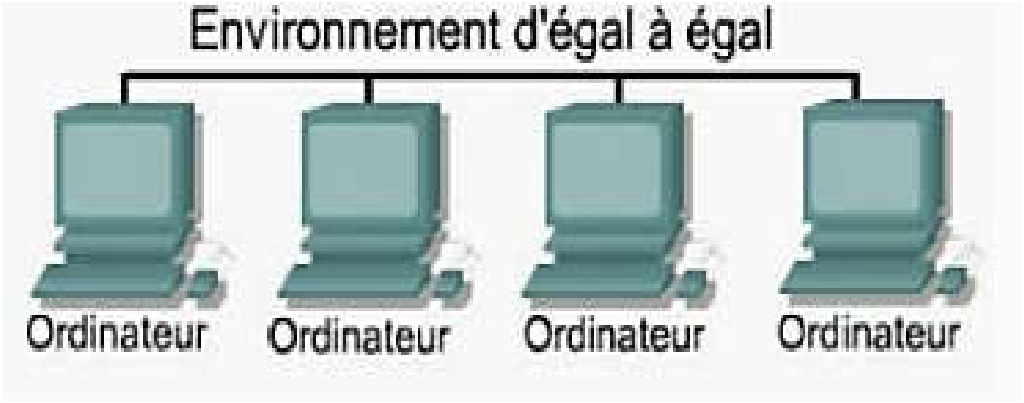

Figure I.5 Architecture poste à poste

- **Réseaux à serveur dédier (client /serveur)**

C'est un réseau informatique où des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont desprogrammes fournissant des données telles que l'heure, des fichiers, une connexion, Dans un environnement purement Client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est un des principaux atouts de ce modèle.

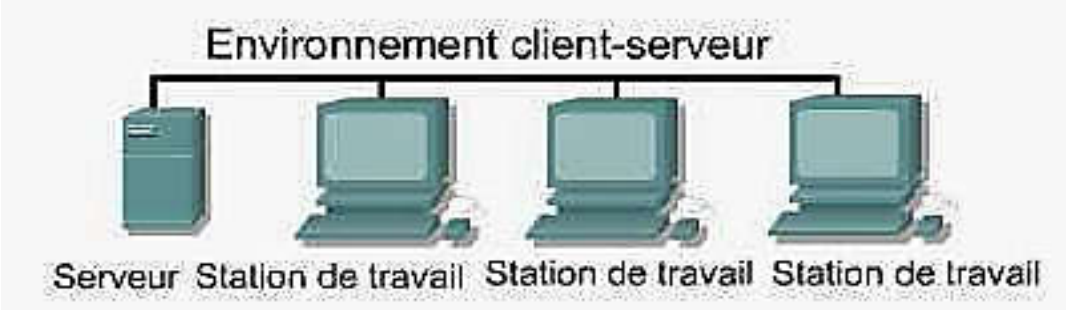

Figure I.6 : Architecture client /serveur.

I.5 Les médiums de transmissions

Les supports de transmission sont nombreux. Parmi ceux-ci, on distingue : les supports métalliques, non métalliques et immatériels. Les supports métalliques, comme les paires torsadées et les câbles coaxiaux, sont les plus anciens et les plus largement utilisés ; ils transportent des courants électriques. Les supports de verre ou de plastique, comme les fibres optiques, transmettent la lumière, tandis que les supports immatériels des communications sans fil propagent des ondes électromagnétiques et sont en plein essor.

Technologie	Type	**Débit ou bande passante**	**Remarque**
Fils métalliques	Paire torsadée	1 Gbits/s pour 100 m ‹ 1 Mbits/s pour 1 Km	Sensible au bruit
	Câble coaxial	10 Mbits/s pour 1Km	Très employé
Fibre optique	Multi-mode à saut d'indice	400 MHz pour 1 km	Faible atténuation 1 répéteur /10 km
	Multi-mode à gradient d'indice	500 MHz pour 1 km	
	Monomode	1 GHz pour 1 km	
Ondes radioélectriques ou électromagnétiques	Infrarouge	1 Mbits/s pour 1 m	Petite distance (10m)
	Satellite géostationnaire	3-10 GHz	Latence 260 ms
	Faisceau terrestre	2-40 GHz	

Tableau I.1 : Les déférents supports de transmission

I.6. Les matériels d'interconnexion

L'interconnexion de réseaux peut être locale : les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard (répéteur, routeur, etc…) suffit à réaliser physiquement la liaison. L'interconnexion peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc…

- **La carte réseau**

La carte réseau (appelée aussi carte d'interface réseau) en anglais **(NIC**) Network Interface Card. Elle s'agit d'une carte connectée sur la carte mère de l'ordinateur et qui permet de l'interfacer au support physique permettant de transmettre l'information.

- **Les concentrateurs**

Un concentrateur (hub) est un élément permettant de connecter le trafic provenant de plusieurs hôtes, et de régénérer le signal. Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports.

Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé: répéteur multi ports.

- **Les commutateurs**

Les commutateurs (switcher) sont similaires aux ponts, mais ils offrent une connexion plus directe entre les ordinateurs sources et destinations. Lorsqu'un commutateur reçoit un paquet de données, il crée une connexion interne séparée, ou segmentée, entre deux de ces ports, et ne transmet le paquet de données qu'au port approprié de destination, en fonction des informations qui figurent dans l'entête de chaque paquet. Cette connexion est ainsi isolée des autres ports et permet aux ordinateurs sources et destinations d'accéder à la totalité de la bande passante d'un réseau.

- **Les routeurs**

Un routeur est un périphérique qui joue le rôle de pont ou du commutateur, mais qui propose un plus grand nombre de fonctionnalités. Lorsqu'il transmet des données entre différents segments du réseau, le routeur examine l'en-tête de chaque paquet pour déterminer le meilleur itinéraire par lequel acheminer le paquet.

- **Les répéteurs**

Un répéteur (repeater) est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne

travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.

- **Les ponts**

Les ponts sont des dispositifs matériels permettant de relier des réseaux travaillant avec le même protocole. Le pont travaille également au niveau de la couche 2 du modèle OSI, c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont. Ainsi le pont permet de segmenter un réseau en conservant au niveau du réseau local les trames destinées aux autres réseaux. Cela permet de réduire le trafic sur chacun des réseaux et augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être écoutées sur l'autre bout.

- **Les passerelles**

Les passerelles permettent à des architectures de réseau différent de communiquer entre elles. Une passerelle peut réassembler différemment les données reçues d'un réseau pour permettre à chaque réseau de comprendre les données reçues d'un réseau ayant une architecture diffèrent.

Une passerelle permet de relier deux systèmes qui n'utilisent pas :

- ✓ La même architecture ;
- ✓ Le même ensemble de règles de communication ;
- ✓ La même structure de format de donnée ;

I.7 Modèle OSI

Le modèle OSI (Open Système Interconnexion). Il permet à des systèmes hétérogènes de s'interconnecter et d'échanger des informations. Il propose donc la manière dont deux éléments communiquent, en décomposant les différentes opérations à effectuer en 7 étapes. Ainsi le modèle OSI se compose de 7 couches, et les protocoles utilisés sont repartis selon ces couches.

Ce modèle définit précisément les fonctions associées à chaque couche. Chacune d'entre elles se comporte comme un prestataire de service pour la couche immédiatement supérieure. Pour qu'une couche puisse envoyer une commande ou des données au niveau équivalent du correspondant, elle doit constituer une information et lui faire traverser toutes les couches inférieures, chacune d'elles ajoutant un en-tête spécifique à ce qui

devient une sorte de train. À l'arrivée, cette information est décodée, la commande ou les données sont libérées.

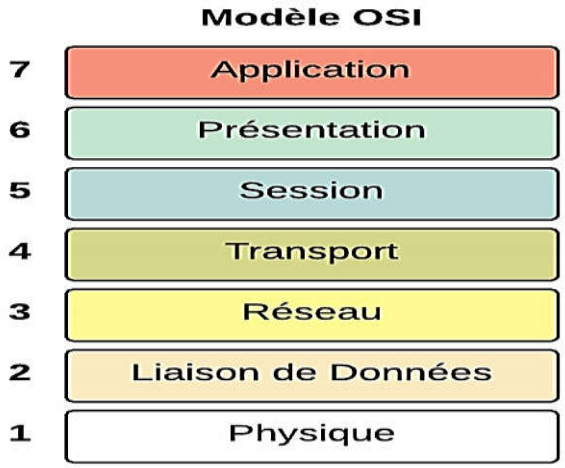

Figure I.7 : Les sept couches du Modèle OSI

I.7.1 Rôle des couches

1) Couche physique (1) :

Elle se charge de l'adaptation du signal aux différents supporte de transmission, elle a comme rôle de gérer les types de transmission (synchrone ou asynchrone). Ainsi elle s'occupe de la modulation et de la démodulation. Enfin l'unité d'échange est le bit.

2) Couche liaison de données (2)

Elle définit les règles d'émission et de réception des données à travers la connexion physique de deux systèmes. Elle intervient aussi dans la détection et la correction des erreurs s'occupe de la réémission s'il ya eu lieu et détermine la méthode d'accès au support. En outre l'unité d'échange est la trame.

3) Couche réseau (3)

Elle assure l'acheminement des données en assurant le routage (choix du trajet) des paquets de données. Ainsi router les données vers un autre nœud en cas de surcharge. Enfin cette dernière assure la translation d'adresse logique en adresse physique l'unité d'échange est le paquet.

4) Couche transport (4)

Les services non pris en compte par d'autres couches sont assurés par cette couche (contrôle d'erreurs, routage).Elle permet aussi le multiplexage de plusieurs flux de données sur le même support. Cette dernière elle a comme rôle de segmenter les messages en paquets numérotés en émission et reconstitution des messages en plaçant les paquets dans l'ordre en réception.

5) Couche session (5)

Cette couche permet l'ouverture ou la rupture d'une session de travail entre deux systèmes distant et assure la synchronisation du dialogue. En outre elle définit le mode de transmission (half-duplex, full-duplex). Enfin cette dernière définit la liaison entre deux programmes d'application et gère le dialogue.

6) Couche présentation (6)

Cette couche intervient dans la transcription des données dans un format compréhensible par les deux systèmes (formatage, codage, compression, cryptage et décryptage de données). Elle permet la mise en forme des données pour quelles soient accessible aux utilisateurs.

7) Couche d'application (7)

Elle offre des services utilisables sur le réseau parmi ces services on trouve :

- ✓ Transfert de fichier FTP
- ✓ Messagerie ou courrier électronique (POP, SMTP)
- ✓ Lecture de page internet (HTTP)
- ✓ Accès a distance (Telnet)

I.7.2. Communication entre couche

Chaque couche assure une fonction bien précise pendant la transmission des données. Il s'agit en effet, de diviser pour mieux régner. La couche N utilise la couche N-1 et fournit des services à la couche N+1.

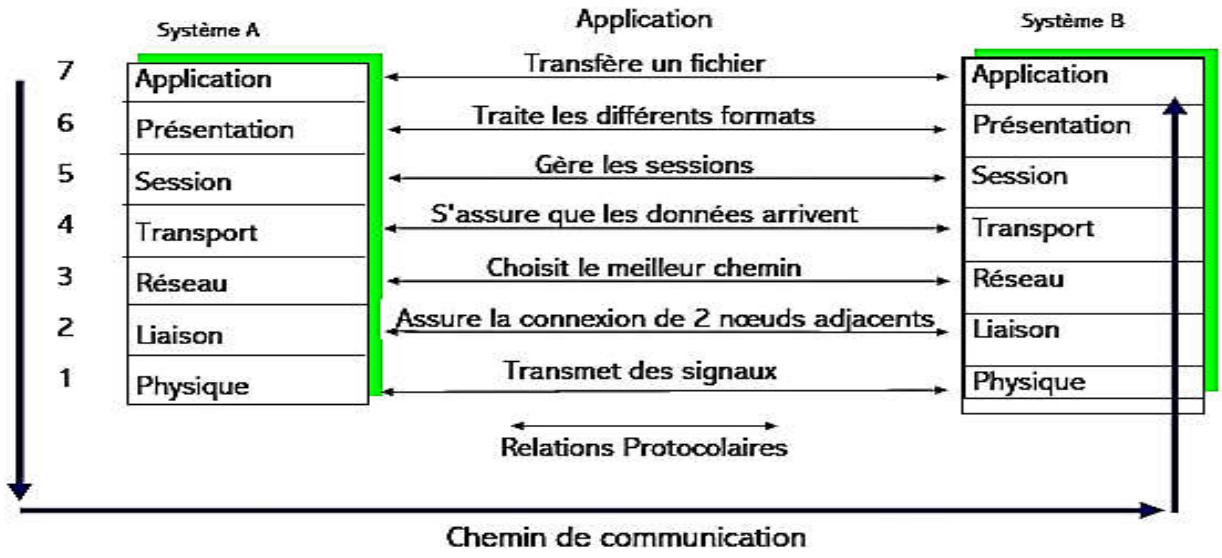

Figure I.8 : Le Modèle OSI et les 7 couches

I.7.3 Encapsulation

Lorsqu'une couche réseau veut dialoguer avec sa couche homologue, elle n'a pas d'autres choix que de faire redescendre l'information en ajoutant des consignes pour la couche du destinataire. Ainsi, l'en-tête et les données d'une couche N vont devenir les données de la couche N-1. Cette couche N-1 va construire un entête (des consignes). Cet en- tête et ces données vont devenir les données de la couche N-2.

On parle alors d'encapsulation. Comme si l'on plaçait des données dans une boite avec des consignes pour cette boite. Cette boite et ces consignes sont ensuite placées dans une plus grande boite avec nouvelles consignes, etc.

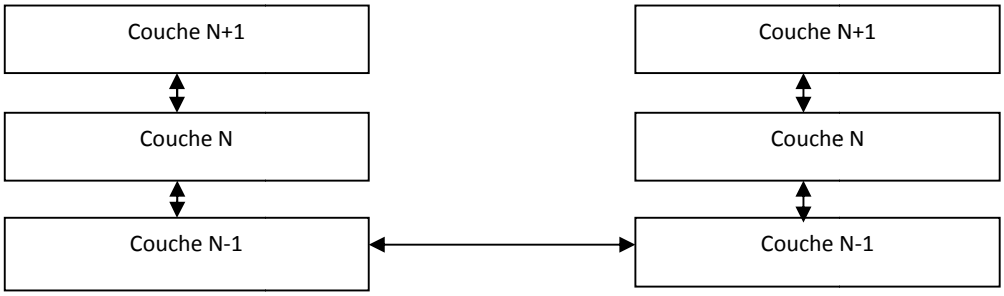

Figure I.9 : Encapsulation de données

I.8.Modèle TCP/ IP

I.8.1. Description du modèle TCP/IP

Le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) réunit les deux protocoles TCP et IP.Il s'agit donc d'une suite de protocoles associée au domaine d'Internet pour lequel elle facilite le transfert de données. Présenté simplement, le protocole TCP/IP est un standard de communication entre deux processus.

Il détermine et fixe les règles inhérentes à l'émission et à la réception de données sur un réseau. L'association des deux protocoles permet d'apporter des garanties de fiabilité dans le Transfert des données.

La famille de protocoles TCP/IP est ce que l'on appelle un modèle en couche, se rapproche en cela du modèle OSI, à la différence que TCP/IP est organisé en seulement 4 couches au lieu des 7 du modèle OSI.

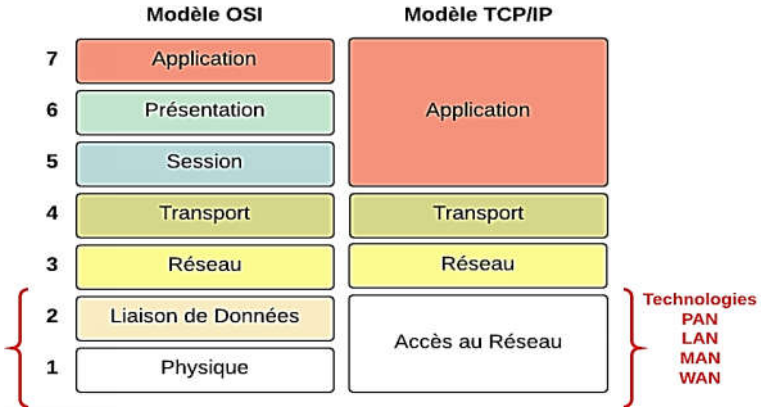

Figure I.10 : Présentation du modèle OSI et TCP/IP

I.8.2 Rôle des couches

On distingue 4 couches qui sont :

1) Couche accès réseaux : On lui donne aussi le nom couche d'hôte-réseaux, cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches physiques et liaisons de données du modèle OSI.

2) Couche Internet : Le rôle de cette couche consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol).L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche. Pensez au système postal. Lorsque vous postez une lettre, vous ne savez pas comment elle arrive à destination (il existe plusieurs routes possibles), tout ce qui vous importe c'est qu'elle arrive à bon port.

3) Couche Transport : La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP (Transmission Control Protocol) , fournit d'excellents moyens de créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé.

4) Couche Application : Cette couche gère les protocoles de haut niveau, les questions de représentation, le code et le contrôle du dialogue. Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

Chaque couche de ce modèle nous offre des services et la figure suivante nous montre les différents services proposés par chaque couche N.

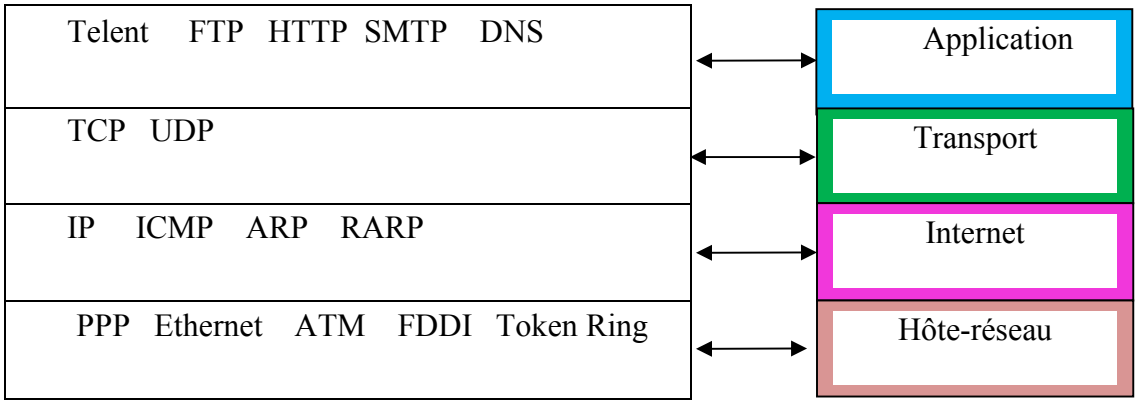

Tableau I.2 services de chaque couche du modèle TCP

I.8.3 Le protocole IP

Le protocole IP a été conçu pour réaliser l'interconnexion de réseaux informatiques et les communications entre systèmes. Le protocole IP est un protocole sans connexion non fiable qui est principalement chargé de l'adressage et du routage des paquets entre les ordinateurs mis en réseau, ainsi qu', il s'occupe de la fragmentation des données.

I.8.3.1 L'adressage IP

Chaque composant impliqué dans une communication réseau doit posséder une adresse IP codée sur 32 bits, Permettant d'identifier un réseau unique et une machine particulière connectée sur ce réseau.

Une adresse IP est codée sur quatre octets représentés conventionnellement par quatre IP est composée d'un identificateur réseau suivi d'un identificateur machine.

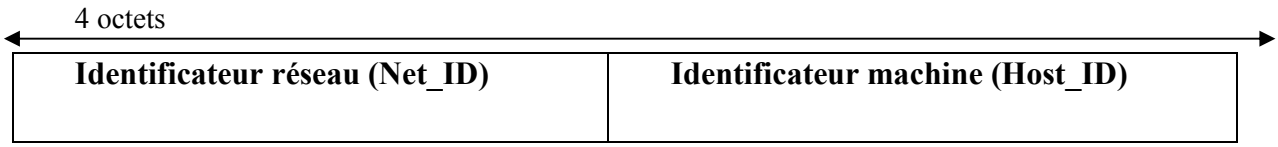

Figure I.11 : Structure général de l'adresse IP.

a. Classes d'adressage

La répartition des octets entre Net_ID et host_ID a généré des classes d'adresses IP, et ces dernières sont distinguées par les premiers bits de poids fort du champ Net_ID.

- **Classe A**

Cette classe est caractérisée par le premier bit de Net_ID qui égal à zéro et un espace d'adressage compris entre les adresse 1.0.0.1.et 126.255.255.254.

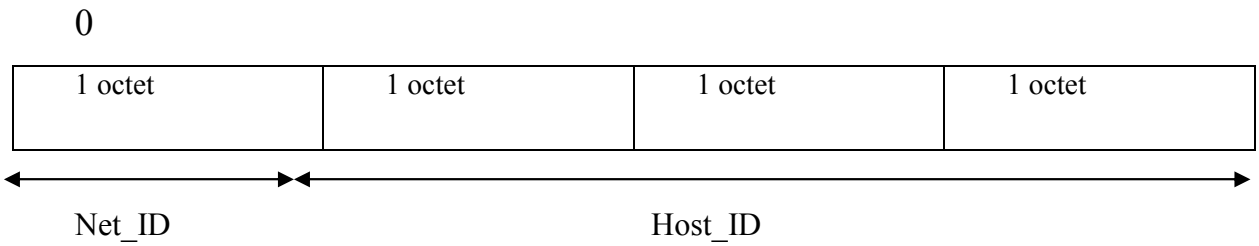

Figure I.12 Classe A.

➢ Classe B

La classe B est caractérisé par les deux premiers bits Net_ID qui sont respectivement égaux à 10 et une plage d'adresse qui s'étale de 128.0.0.1 jusqu'à 191.255.255.254

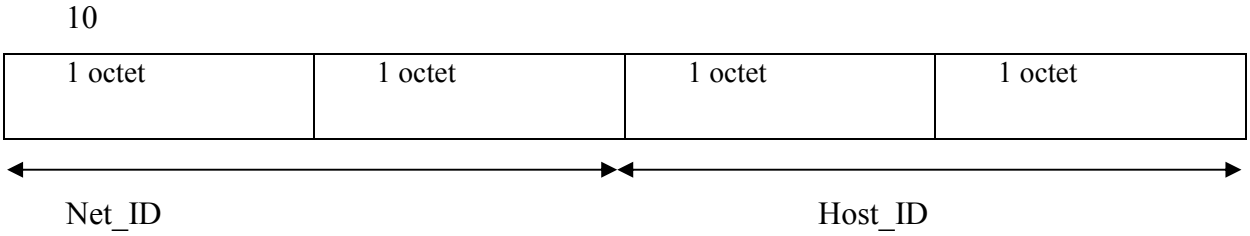

Figure I.13 Classe B.

➢ Classe C

Cette classe est caractérisée par les trois premiers bits Net_ ID qui sont respectivement égaux à 110 et une plage d'adresse comprise entre les adresses 192.0.0.1 et 123.255.255.254.

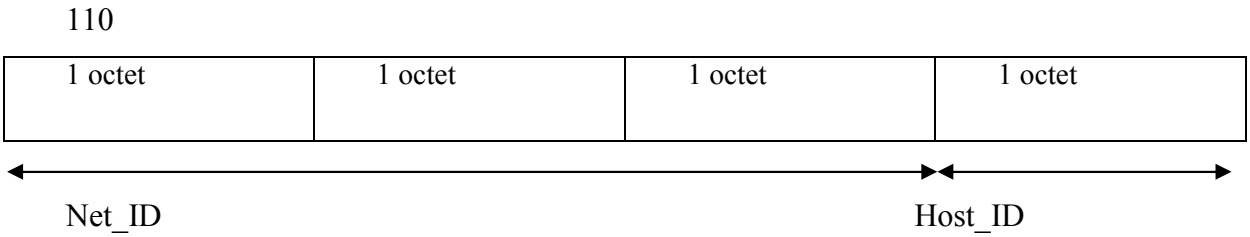

Figure I.14: Classe C.

On trouve aussi des adresses dites non routable, car ces adresses sont utilisés à un usage interne. Elles ne sont en théorie jamais routées sur l'internet

I.8.4 Masque réseau

Le masque servant à faire la séparation en deux parties sur une adresse IP, il est donc indissociable de celle-ci. Une adresse seule ne voudra rien dire puisqu'on ne saura pas quelleest la partie réseau et quelle est la partie machine. De la même façon, un masque seul n'aura pas de valeur puisqu'on n'aura pas d'adresse sur laquelle l'appliquer. L'adresse IP et le masque sont donc liés l'un à l'autre, même si l'on peut choisir l'un indépendamment de l'autre.

Des masques différents sont associés aux classes A, B et C qui sont généralement standard qui peuvent être modifié en fonction des besoins en capacité réseau/hôtes.

Il contient des « 1 » aux emplacements des bits consacrés a la partie réseau, et des « 0 » dans l'emplacement réservé a la partie hôte.

classe	plage	masque	adresse IP	capacité
A	0.0.0.0 – 127.255.255.255	255.0.0.0 (/8)	0.x.y.z – 127.x.y.z	2^7 réseaux, 2^{24} hôtes
B	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)	128.0.x.y – 191.255.x.y	2^{14} réseaux, 2^{16} hôtes
C	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)	192.0.0.x – 223.255.255.x	2^{21} réseaux, 2^8 hôtes

Figure I.15 : Masque réseau par défaut.

I.9 Protocole UDP

Le protocole **UDP (**User Datagram Protocol) assure les services attendus de la couche transport du modèle TCP/IP. Tout comme TCP, son rôle est de gérer le fractionnement des paquets et le réassemblage en paquets des segments de données qui transit via IP. Cependant, UDP n'assure aucun autre service supplémentaire : pas de ré ordonnancement, pas de suivi de la communication à l'aide d'accusé de réception, pas de contrôle de flux.

UDP fonctionne en mode non connecté, c'est-à-dire qu'il ne fait que transporter les paquets de manière indépendante, sans assurer la moindre cohérence entre eux.

I.10 Protocole de routage

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau afin d'acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Ce derniers est appliqué dans plusieurs réseaux tels que réseau téléphonique, les réseaux de données électroniques comme Internet, et les réseaux de transports. Sa performance est importante dans les réseaux décentralisés, c'est-à-dire où l'information n'est pas distribuée par une seule source, mais échangée entre des agents indépendants**.**

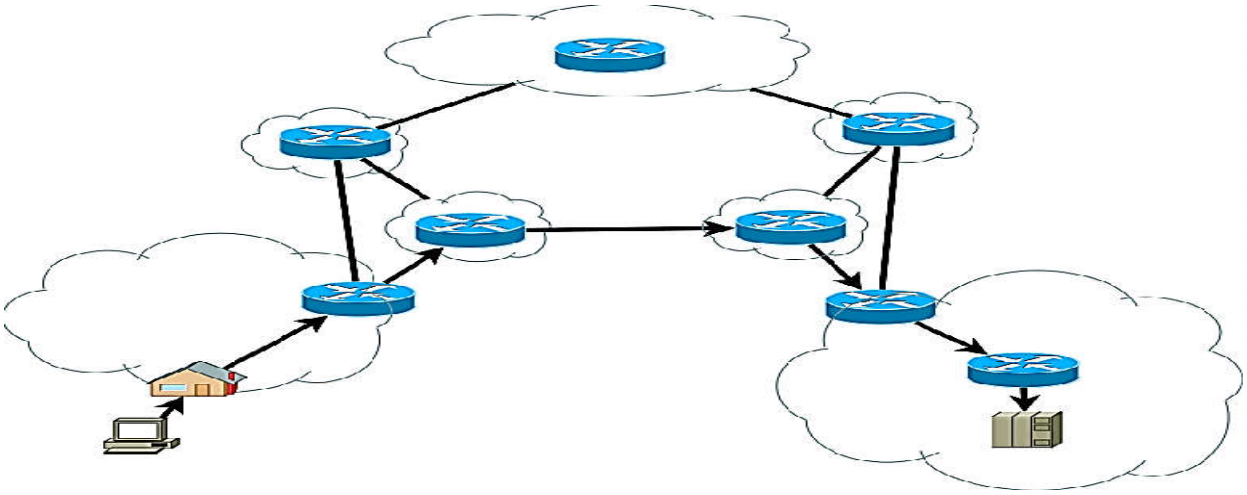

Figure I.16 : Exemple de routage dans un réseau

I.10.1 Le routage IP

Tous les protocoles de routage ont pour objectif de maintenir les tables de routage du réseau dans un état intègre et cohérent. Pour y parvenir, les protocoles diffusent des informations de routage aux autres systèmes du réseau afin de transmettre les modifications des tables de routage. Ces protocoles réceptionnent en contrepartie les informations de routage d'autres systèmes du réseau afin de mettre à jour les tables de routage. [1]

I.10.2 Types de routage

On distingue deux types de routage qui sont :

a. Le routage statique (Non adaptif) : Décisions de routage pré calculéeset chargées initialement dans le routeur. En outre les routes sont fixes, en cas de modification dans le réseau le changement sera fait manuellement.

b. Le routage dynamique (adaptif) : Décisions de routage évoluant selon les modifications de topologie de trafic.

Le dialogue entre routeurs se fait avec ces deux méthodes soit :

- Routage à vecteur de distance (**distance vector**)
- Routage à état de lien (**Link state**)

I.10.3. Méthodes de routage

a. Méthode de routage à vecteur : C'est une méthode itérative par transmission des tables de routage. Chaque routeur transmet sa table de routage initiale à ses voisins immédiats. En suite les tables reçues des ses voisins immédiats seront fusionnées avec sa table. Enfin en cas de modification, transmet la table obtenu ses voisins immédiats. Dans ce cas la convergence n'est pas garantie

b. Méthode de routage de lien : C'est une méthode non itérative par transmission d'état des liaisons. Chaque routeur, transmet l'état de ses liaisons à ses voisins immédiats. Ensuite, il retransmet les informations reçues de ses voisions à ses autres voisions. Enfin calcule sa table de routage. dans ce cas y aura pas de problème de convergence et elle sera garantie.

I.10.4 Table de routage

Une table de routage est une structure de données utilisée par un routeur ou un ordinateur en réseau et qui associe des préfixes à des moyens d'acheminer les datagrammes vers leur destination. Cette dernière se réside en RAM, et elle est constituée des éléments suivant :

- Méthode de routage**:** type de protocole qui a appris la route
- Réseau et masque: destination
- Distance administrative**:** préférence d'une route par un protocole sur un autre. chaque protocole a sa valeur par défaut
- Valeur de métrique**:**valeur d'une route sur une autre parmi toutes celles apprises par protocole de routage
- Via la prochaine interface (passerelle)
- Interface de sortie du routeur.

Le tableau ci-dessous, un exemple à quoi ressemble la table de routage :

Adresse destination	Masque	Passerelle	Interface	Métrique
0.0.0.0	0.0.0.0	192.168.0.100	192.168.0.100	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.0.0	192.168.0.100	192.168.0.100	1
192.168.0.100	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.0.1	255.255.255.255	192.168.0.100	192.168.0.100	1

Tableau I.3 : Exemple a quoi ressemble une table de routage

I.10.5 Les protocoles de routage

Tous les protocoles de routage ont pour objectif de maintenir les tables de routage du réseau dans un état intègre et cohérent. Pour y parvenir, les protocoles diffusent des informations de routage aux autres systèmes du réseau afin de transmettre les modifications des tables de routage. Ces protocoles réceptionnent en contrepartie les informations de routage d'autres systèmes du réseau afin de mettre à jour les tables de routage. [1]

I.10.5.1 Les protocoles de routage interne IGP

- **IGP (interior Gateway protocol)** est un protocole de routage dynamique entre routeurs d'un même système autonome, c'set à dire dont la gestion dépend d'une administration unique. Ce dernier privilège la fiabilité et les chemins les plus courts pour une transmission rapide. [4]

Parmi les protocoles les plus utilisés, citons principalement :

- **OSPF (Open Shortest Path First)** : Protocole de routage à état des liens fondé sur le calcul des chemins les plus courts et sur une architecture hiérarchique constituée de zones OSPF [1]. Par contre ce protocole est considérablement plus complexe que le protocole RIP. Il gére deux niveaux d'hiérarchie, ce qui permet de l'utiliser dans des réseaux de grande taille (une centaine de routeurs). [2]

- **IS-IS (Intermediate System to IntermediateSystems):** C'est un protocole interne de routage. Issu de l'ensemble des protocoles OSI (Open Systems Interconnexion), il fournit un support pour la mise à jour d'informations de routage entre de multiples protocoles.

Le routage IS_IS utilise deux niveaux hiérarchiques de routage. La topologie de ce dernier est découpée en aires de routage de niveaux 1 ou 2. Les routeurs de niveau 1 connaissent la topologie dans leur aire, incluant tous les routeurs de cette aire. Ce pendant, ces routeurs de niveau 1 ne connaissent ni l'identité des routeurs, ni les destinations à l'extérieur de leur aire. Ils routent tout le trafic vers les routeurs interconnectés au niveau 2 dans leur aire. Les routeurs de niveau 2 connaissent la topologie réseau du niveau 2 et savent quelles adresses sont atteignables pour chaque routeur. Les routeurs de niveau 2 n'ont pas besoin de connaître la topologie à l'intérieur d'une aire de niveau 1. Seuls les routeurs de niveau 2 peuvent échanger les paquets de données ou les informations de routage directes avec les routeurs externes situés en dehors de leur aire de routage. [1]

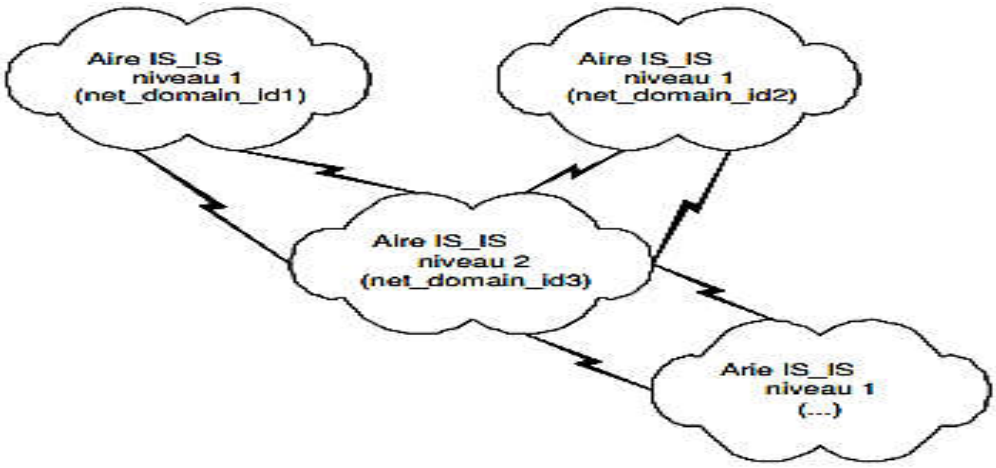

Figure I.17 : Topologie de routage des aires IS-IS

- **RIP (Routing Information Prtocol)** : Est un protocole de routage dynamique de type IGP destiné à être a utilisé sur des réseaux peu étendus. Il fonctionne sur la base de nombre de routeurs intermédiaires sur la route pour joindre une destination donnée ; cette information est appelée métrique, et elle est codée sur 4 bits : 1 pour la route la courte (seul le routeur courant doit être traversé), 15 pour la route le plus longue, 16 étant réservé pour signaler une route infinie. Ce dernier fonctionne de manière à détecter la route optimale pour joindre une destination, soit donc celle proposant la métrique la plus petite. [4]

I.10.5.2 Les protocoles de routage externe EGP

Les protocoles EGP sont conçus pour gérer le routage externe d'un réseau avec des objectifs de convergence et d'optimisation de nouvelles routes injectées dans les tables de routage du réseau. Généralement, le nombre d'entrées dans les tables de routage est souvent important. Par exemple, un routeur qui comporterait l'ensemble des routes actuelles d'Internet compterait près de 100 000 entrées. Parmi les protocoles EGP utilisés de nos jours, c'est le protocole de routage BGP qui s'est imposé. [1]

➢ **BGP (Border Gateway protocol) :** Ce protocole est destiné à assurer le routage entre plusieurs ASs (Autonome Système). Il assure la propagation de route à l'échelle internationale. Il est utilisé plus particulièrement pour l'échange d'informations de routage entres les Ass du réseau internet. Quand ce dernier est utilisé entre différents Ass, il est connu sous le nom de BGP Externe (EBGP), et s'il est utilisé à l'intérieur d'un même AS pour échanger des routes, dans ce cas il est appelé BGP Interne (IBGP). [3]

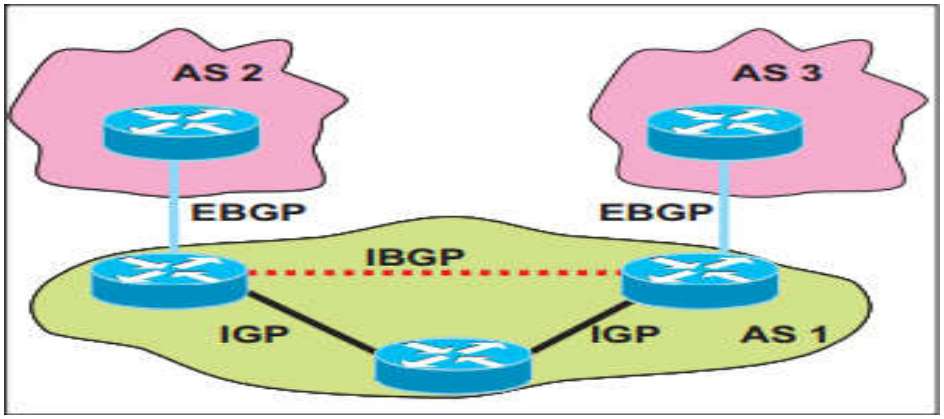

Figure I.18 : Routage BGP

I.11 Les protocoles réseaux

❖ **DNS (Domaine Name Service) :** Est une base de données utilisée sur les réseaux IPpour transposer les noms d'ordinateurs en adresse IP.

❖ **Protocole ICMP (Internet Control Message Protocol) :** Est un protocole qui permet le contrôle des erreurs de transmission. En effet, comme le protocole IP ne gère que le transport des paquets **et** ne permet pas l'envoie de message d'erreur, c'est grâce a ce protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau.

❖ **DHCP (Dynamic Host Configuration Protocol) :** Est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut.

❖ **FTP (File transfert Protocol) :** permet de transférer des fichiers d'une machine à une autre.L'utilisation de FTP depuis un poste client pour aller chercher ou déposer un fichier sur un serveur nécessite de la part de l'utilisateur de se connecter avec un nom et un mot de passe. Donc si l'utilisateur n'est pas reconnu la connexion ne sera pas établie.

❖ **HTTP (Hyper Text Transfer Protocol) :** Est le protocole de communication de web permettant d'échanger des documents hyper textes contenant des données sous la forme de texte, d'image fixes ou animées et de sons. Tout client web communique avec le port80 d'un serveur http.

❖ **TFTP (Trivial File transfer Protocol ou protocole simplifié de transfert de fichiers) :** Est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP.**TFTP** reste très utilisé pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare-feu, etc..) ou pour démarrer un PC à partir d'une carte réseau.

❖ **ARP (AdressResolution Protocol) :** son rôle est de mettre en place un mécanisme de restitution d'une adresse MAC à partir d'une adresse IP dans le cadre d'un réseau où le support est partagé comme le réseau Ethernet par exemple.

❖ **RARP (Reverse AddressResolution Protocol) :** est un protocole permettant à un équipement d'obtenir son **adresse IP** en communiquant son adresse Ethernet à un serveur RARP, RARP s'effectuera au Boot de la machine qui gardera ensuite en mémoire son adresse IP. Après avoir obtenue son adresse IP, la machine peur récupérer les fichiers de configuration. D'autres mécanismes existent pour qu'un équipement (avec ou sans disque) obtienne son adresse IP dynamiquement.

❖ **SNMP (**Simple Network Management Protocol**) :** est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et dediagnostiquer des problèmes réseaux et matériels à distance.

❖ **Le protocole VTP** (VLAN Trunking Protocol) : est un protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques Cisco. Le VTP permet d'ajouter, renommer ou supprimer un ou plusieurs Vlans sur un seul switch (serveur) qui propagera cette nouvelle configuration à l'ensemble des autres switchs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des Vlans sur l'ensemble d'un réseau local.

❖ **Mode trunk :** est une configuration d'une liaison, généralement entre deux switches mais pas uniquement, permettant d'y véhiculer le trafic de plusieurs VLANs.

I.12 Discussion :

Ce chapitre est consacré à l'étude générale des réseaux informatiques. Les réseaux peuvent être divisés en LAN, MAN, WAN, et réseaux d'interconnexion, chacun d'eux ayant ses caractéristiques propres selon des topologies spécifiques, leurs méthodes d'accès et aussi les méthodes de connexion.il y a aussi l'adressage IP, le routage et les protocoles les plus indispensables et les plus utilisées. Pour les individus les réseaux permettent l'accès à de très nombreuses ressources.

Chapitre II
Sécurité des réseaux Informatiques

II.1 Préambule

La continuité de l'activité de l'Entreprise appelle à la continuité de son système d'information. Cette continuité ne peut être assurée que par la mise en place de moyens de protection permettant d'apporter un niveau de sécurité adapté aux enjeux spécifiques de l'Entreprise. [1]. Afin d'assurer la sécurité du réseau, des moyens techniques et des solutions de prévention sont alors déployés. En outre ces derniers doivent prendre en compte la formation et la sensibilisation de tous les acteurs sur les risques encourus qui ne cessent d'être dirigées contre les entreprises. Ainsi une bonne politique de sécurité doit être fondée sur la collaboration de l'ensemble des employés et l'utilisation d'équipements et techniques qui répondent aux exigences du système tout en assurant le blocage d'attaques informatiques de tout genre.

L'objectif de ce chapitre est de présenter les faiblesses les plus couramment exploitées par les attaques et de détailler le mécanisme de ces attaques, et pour ensuite montrer les techniques de parade susceptible afin de contrer ces attaques.

II.2 Définition de la Sécurité informatique

La sécurité informatique est l'ensemble de moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs

II.3 Critères de la sécurité

La sécurité informatique vise généralement cinq principaux critères :

- ✓ **L'intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- ✓ **La confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- ✓ **La disponibilité**, permettant de maintenir le bon fonctionnement du système d'information
- ✓ **La non répudiation**, permettant de garantir qu'une transaction ne peut être niée ;
- ✓ **L'authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

Figure II.1 Critères de sécurité

II.4 Politique de sécurité

Une politique de sécurité est l'ensemble des lois, des règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique. [1]

Une politique de sécurité réseau peut se développer dans les trois directions suivantes :

- **Une politique de sécurité physique :** Elle détaille par exemple les objectifs et règles de sécurité des équipements réseau afin de faire face aux menaces comme le feu, les catastrophes naturelles.
- **Une politique de sécurité administrative :** Elle détaille par exemple les objectifs et règles de sécurité des procédures de gestion du réseau afin de faire face aux événements de congestion du réseau.
- **Une politique de sécurité logique :** Elle détaille par exemple les objectifs et règles de sécurité de configuration des accès des équipements réseau afin de faire face aux accès non autorisés, attaques.

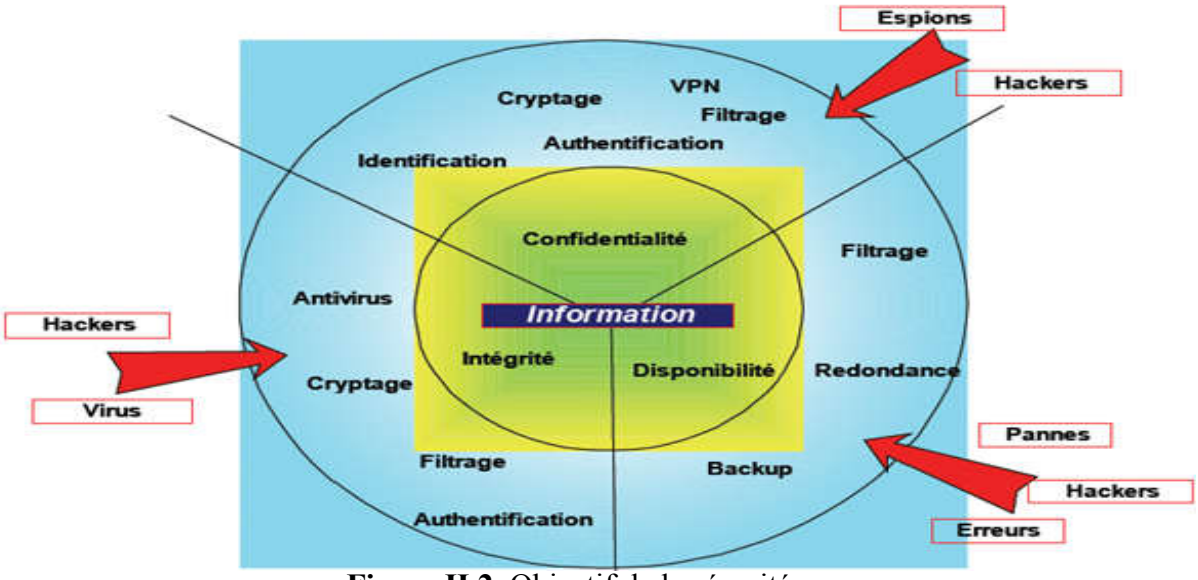

Figure II.2. Objectif de la sécurité

II.5 Les types de menaces

➢ **Menaces accidentelles:**ce sont celles qui existent sans qu'il y ait préméditation, exemples, défaillance de systèmes, bévues opérationnelles et bugs dans les logiciels.

➢ **Menaces intentionnelles:**une menace intentionnelle est une action exécutée par une entité pour violer la sécurité de l'information et l'utilisation non autorisée des ressources. Les menaces intentionnelles peuvent être passives.

➢ **Menaces passives:**les menaces passives sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne change. Il est très difficile de détecter ce type de menaces car elles sont inoffensives par apport aux fonctions normales du système. L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication (surveillance de réseau) est un une concrétisation d'une menace passive.

➢ **Menaces actives:** les menaces actives ou attaques envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou le fonctionnement du système. Les menaces actives sont, contrairement aux menaces passives, plus faciles à détecter si des précautions appropriées on été prises au préalable.

Les exemples d'attaques sont la destruction, la modification, la fabrication, l'interruption ou l'interception de données. Le résultat d'une attaque est soit une

divulgation de l'information (violation de l'intégrité de l'objet) ou un déni de service (violation de la disponibilité)

II.6 Les attaques informatiques

II.6.1 Les types d'attaques

Les hackers utilisent plusieurs techniques d'attaques. Ces attaquespeuvent être regroupées en trois familles différentes :

a.Les attaques directes :C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. La plupart des "script kiddies" utilisent cette technique. En effet, lesprogrammes de hack qu'ils utilisent ne sont que faiblement paramétrables, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

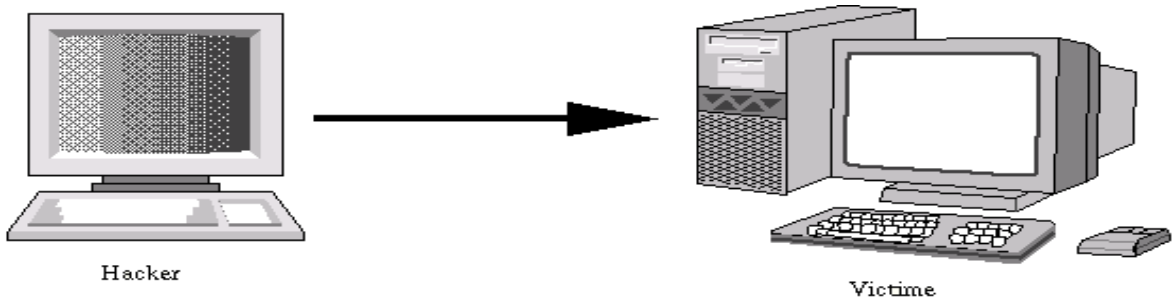

Figure II.3 Attaque directe

b. Les attaques indirectes par rebond : Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) du hacker.
- Éventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer.

Le principe en lui-même, est simple : Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où leterme de rebond.

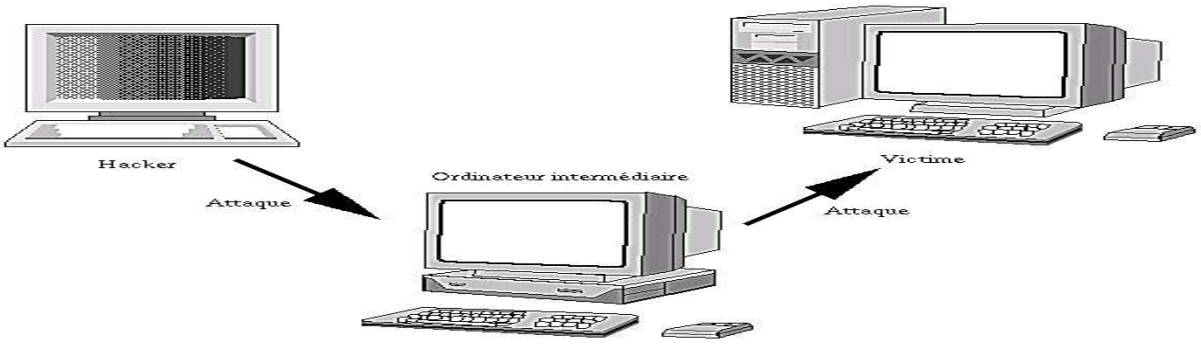

Figure II.4 Attaque indirecte par rebond

c. **Les attaques indirectes par réponse :** Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaqueà l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée àl'ordinateur victime.

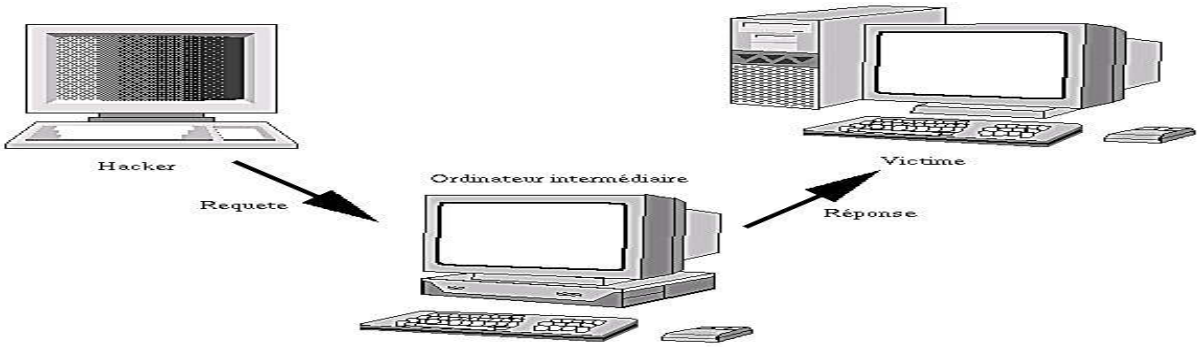

Figure II.5 Attaque indirect par réponse

II.6.2 Les techniques d'attaques

II.6.2.1 Les attaques d'accès

Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.

a. Le sniffing: Cette attaque est utilisée par les pirates informatiques pour obtenir des mots de passe. Grâce à un logiciel appelé renifleur de paquets (sniffer), on peut intercepter toutes les paquets qui circulent sur un réseau même ceux qui ne nous sont pas destinés. Par exemple, lors d'une connexion grâce à « telnet » le mot de passe de l'utilisateur va transiter en clair sur le réseau. Il est aussi possible de savoir à tout moment quelles pages

web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Cette technologie n'est pas forcement illégale car elle permet aussi de détecter des failles sur un système.

b. Porte dérobée: Lorsqu'un pirate informatique arrive à accéder à un serveur à l'aide d'une des techniques présentées dans cette section, il souhaiterait y retourner sans avoir à tout recommencer. Pour cela, il laisse donc des portes dérobées (backdoor) qui lui permettra de reprendre facilement le contrôle du système informatique.

c. L'ingénierie sociale:C'est une méthode pour obtenir des informations sur un système ou des mots de passe. Elle consiste surtout à se faire passer pour quelqu'un que l'on n'est pas (en général un des administrateurs du serveur que l'on veut pirater) et de demander des informations personnelles Elle consiste surtout à se faire passer pour quelqu'un que l'on n'est pas (en général un des administrateurs du serveur que l'on veut pirater) et de demander des informations personnelles.

d. Le craquage de mots de passe: Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

e. Man-in-the-midle: L'intrus est positionné au milieu d'une communication entre deux parties dans le but de l'espionner ou de la modifier .Un intrus peut fournir des services de point d'accès wifi ou de passerelle réseau pour centraliser les communications à son niveau. La victime peut se connecter et utiliser normalement le réseau sans savoir que le flux passe par une tierce personne

II.6.2.2 Les attaques virales

Une attaque de type « modification » consiste, pour un attaquant à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information.

Pour se faire une grande variété de programmes malveillants existe et on trouve :

a. Les virus :C'est un code (programme) malveillant qui s'attache à un autre programme dans le but d'exécuter une fonction non souhaitée sur un ordinateur, du fait qu'un virus se

greffe à un programme légitime, son activation se produit grâce à l'utilisateur qui lance le programme infecté,peut rester inactif pendant un certain temps et ne s'activer qu'après une période de temps. Ilpeut être inoffensif comme il peut exécuter des opérations dangereuse (effacement de fichiers, arrêts de services, …etc.)

b. Les vers : Un ver est un code autonome particulièrement dangereux qui se réplique de façon indépendante en exploitant les vulnérabilités du réseau.Contrairement aux virus, les vers n'ont pas besoin de programme hôte pour se répliquer, ni de la participation de l'utilisateur pour s'activer. Ils peuvent se répondre rapidement sur le réseau.

La majorité des vers utilisent trois composants pour effectuer une attaque ;

- ✓ **Exploitation d'une vulnérabilité :** Le ver s'installe en exploitant une faille d'un système vulnérable (pièce jointe d'un mail, cheval de Troie …etc.)
- ✓ **Propagation :** Après son installation en mémoire, le ver se réplique et localise de nouvelles cibles
- ✓ **Action :** Exécution de codes malveillants

c. Cheval de Troie : C'est une application qui exécute autre chose que ce que son utilisateur pense exécuter. Ils est d'apparence écrite pour une fonction légitime, elle effectue des traitements cachés à l'insu de l'utilisateur. Les chevaux de Troie peuvent causer des dommages immédiats, fournir un accès distant à la machine ou effectuer de l'espionnage (envoie de tous les caractères tapés par l'utilisateur pour retrouver des mots de passes)

II.6.2.3 Les attaques par saturation (déni de service)

Les attaques par saturation sont des attaques informatiques qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes.

Il existe différentes attaques par saturation on site :

a. Le flooding: Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.

b. Le TCP-SYN flooding: Le TCP-SYN flooding est une variante du flooding qui s'appuie sur une faille du protocole TCP. En effet, on envoie un grand nombre de demande de connexions au serveur (SYN) à partir de plusieurs machines. Le serveur va envoyer un grand nombre de paquet SYN-ACK et attendre en réponse un paquet ACK qui ne viendra jamais.

c. UDP Flooding: Le trafic UDP est prioritaire sur TCP, le but es donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP.

d. Le smurf : Le smurf est une attaque qui s'appuie sur le ping et les serveurs de broadcast. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcast. Il le fera suivre à toutes les machines qui sont connectées qui renverront chacune un « pong » au serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter.

e. Packet fragment: Cette attaque utilise une mauvaise gestion de la défragmentation au niveau ICMP. Exemple : ping of death. La quantité des données est supérieure à la taille maximum d'un paquet IP.

f. Le débordement de tampon: Cette attaque se base sur une faille du protocole IP. On envoie à la machine cible des données d'une taille supérieure à la capacité d'un paquet. Celui-ci sera alors fractionné pour l'envoi et rassemblé par la machine cible. A ce moment, il y aura débordement des variables internes. Suite à ce débordement, plusieurs cas se présentent : la machine se bloque, redémarre ou ce qui est plus grave, écrit sur le code en mémoire**.**

II.6.2.4 Les attaques de répudiation

La répudiation est une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passé.

a. L'IP spoofing: c'est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque

sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.

b. DNS Spoofing: Elle consiste à fournir de fausses réponses aux requêtes DNS, c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine, a fin de rediriger, à leur insu, des internautes vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut envoyer ses identifiants en toute confiance. Il existe deux techniques pour effectuer cette attaque :

- **Empoisonnement du cache DNS :** L'empoisonnement du cache DNS ou pollution de cache DNS (DNS cache poisoning) est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse. Une fois que les serveurs DNS a été empoisonné, l'information est mise dans un cache, rendant ainsi vulnérable tous les utilisateurs de ce serveur. Ce type d'attaque permet, par exemple, d'envoyer un utilisateur vers un faux site dont le contenu peut servir à de l'hameçonnage (dans le cas du DNS) ou comme vecteur de virus et autres applications malveillantes.
- **DNS ID Spoofing :** Lors d'une requête pour obtenir l'adresse IP à partir d'un nom, un numéro d'identification est placé dans la trame afin que le client et le serveur puissent identifier la requête. L'attaque consiste ici à récupérer ce numéro puis, envoyé des réponses falsifiées au client avant la réponse des serveurs DNS
- **ARP Spoofing :** Lorsqu'un système désire communiquer avec ses voisins sur un même réseau (incluant la passerelle d'accès à d'autres réseaux), des messages ARP sont envoyés afin de connaître l'adresse MAC des systèmes voisins et d'établir ainsi une communication avec un système donné. Sachant que chaque système possède localement une table de correspondance entre les adresses IP et MAC des systèmes voisins, la faiblesse d'authentification du protocole ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne. Le système du pirate reçoit donc tout le trafic à destination de la passerelle. Il lui suffit d'écouter ou de modifier passivement le trafic et de router ensuite les paquets vers leur véritable destination. [5]

II.6.2.5 Les attaques permettant de modifier le routage réseau

Dans les premiers grands réseaux, les tables de routage étaient statiques et donc maintenues à jour par des techniciens de bout en bout. De nos jours, les mises à jour des tables de routage et le calcul du meilleur chemin sont automatiquement propagés sur le réseau par les protocoles de routage. IGP (Interior Gateway Protocol) et EGP (Exterior Gateway Protocol) sont les deux grandes familles de protocoles de routage dans les réseaux IP. Un réseau de routage est découpé généralement en systèmes autonomes, dits AS (Autonomous System). Dans un système autonome, le protocole de routage utilisé est de type IGP. Pour les échanges de routage entre systèmes autonomes différents, le protocole de routage utilisé est de type EGP. Sachant que toute attaque ou perturbation du routage peut impacter directement la disponibilité du réseau et de ses services, il est primordial de considérer les protocoles de routage comme des éléments-clés de la sécurité d'un réseau. D'autant qu'il est aussi possible de détourner du trafic par le routage à des fins de vol d'information. [5]

II.7 Mécanismes de sécurité

II.7.1 logiciels antivirus

La plupart des ordinateurs sont dotés d'un logiciel antivirus pré intégré capable de détecter les principales menaces virales s'il est régulièrement mis à jour et correctement entretenu.

Avec des milliers de nouveaux virus générés chaque mois, il est crucial que la base de données des virus soit tenue à jour. La base de données des virus est l'enregistrement du logiciel antivirus qui permet d'identifier les virus connus lorsqu'ils surviennent.

La politique de sécurité du réseau doit mentionner que tous les ordinateurs du réseau doivent être tenus à jour et théoriquement qu'ils doivent tous être protégés par le même système d'antivirus (entre autres, afin de réduire au maximum les frais de maintenance et de mise à jour).

II.7.2 cryptographie

Les données qui peuvent être lues et comprises sans mesures spéciales sont appelées texte clair. Le procédé qui consiste à dissimuler du texte clair de façon à cacher sa substance est appelée cryptographie ou chiffrement. Le chiffrement des données fut

inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage. Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui repose sur un codage à deux clés, une privée et l'autre publique.

❖ **Le cryptage symétrique :** il s'agit de clés utilisées pour chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète

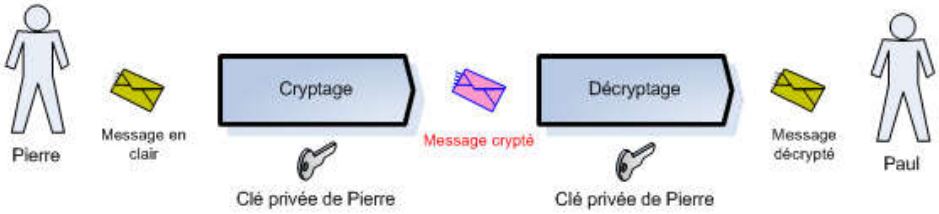

Figure II.6 cryptage symétrique.

❖ **Le cryptage asymétrique** : il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement

✓ Une première clé, visible, appelé clé publique est utilisée pour chiffrer un texte en clair.

✓ Une deuxième clé, secrète, appelée clé privée est connue seulement par le destinataire, qui est utilisé pour déchiffrer un texte.

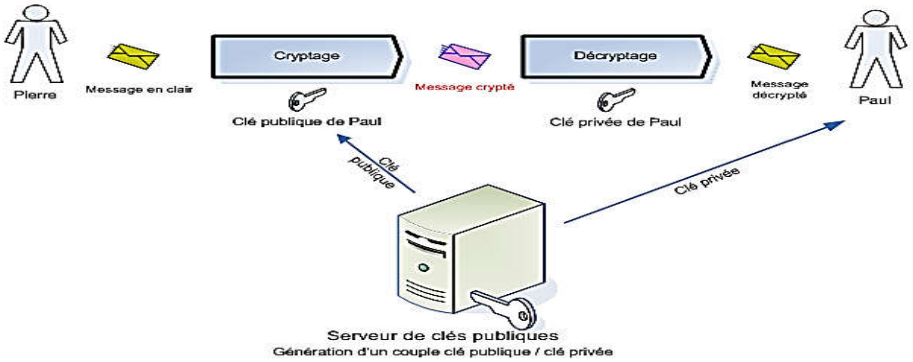

Figure II.7 cryptage asymétrique

II.7.3 la signature

Dans toute transaction professionnelle, les deux parties doivent offrir une garantie de leurs identités. La signature numérique et le certificat sont des moyens d'identification de l'émetteur du message.

II.7.3.1 la signature numérique

L'un des principaux avantages de la cryptographie de clé publique est qu'elle offre une méthode d'utilisation des signatures numériques. Celles-ci permettent au destinataire de vérifier leur authenticité, leur origine, mais également de s'assurer qu'elles sont intactes. Ainsi, les signatures numériques de clé publique garantissent l'authentification et l'intégrité des données. Elles fournissent également une fonctionnalité de non répudiation, afin d'éviter que l'expéditeur ne prétende qu'il n'a pas envoyé les informations. Ces fonctions jouent un rôle tout aussi important pour la cryptographie que la confidentialité, sinon plus.

Une signature numérique a la même utilité qu'une signature manuscrite. Cependant, une signature manuscrite peut être facilement imitée, alors qu'une signature numérique est pratiquement infalsifiable. De plus, elle atteste du contenu des informations, ainsi que de l'identification du signataire.

II.7.3.2 certificats numériques

Lors de l'utilisation des systèmes de cryptographie de clé publique, les utilisateurs doivent constamment vérifier qu'ils cryptent vers la clé du bon utilisateur, ce qui constitue un problème. Dans un environnement où le libre-échange de clés via des serveurs publics est sécurisé, toute attaque menée par une personne intermédiaire, encore appelée un intercepteur, représente une menace éventuelle. Dans ce type d'attaque, une personne place une fausse clé comportant le nom et l'ID utilisateur du destinataire. Les données cryptées (et interceptées) vers le détenteur réel de cette clé erronée sont dorénavant entre de mauvaises mains.

II.7.4 Proxy

Le serveur proxy est un dispositif matériel et logiciel permettant de contrôler, sécuriser et surveiller les accès à Internet des utilisateurs dans un réseau.
Il permet notamment :

- ✓ de gérer les droits d'accès au Web par profil utilisateur.

- ✓ de surveiller les accès Internet à travers l'historique de navigation de chaque utilisateur.
- ✓ de sécuriser le réseau local.

II.7.5 Un pare-feu

Un pare-feu est un composant réseau qui permet non seulement de concentrer l'administration de la sécurité en des points d'accès limités au réseau d'entreprise mais aussi de créer un périmètre de sécurité, par exemple entre le réseau intranet de l'entreprise et le réseau Internet.

Une architecture à base de pare-feu offre l'avantage de concentrer les efforts de sécurité sur un unique point d'entrée. Grâce à des mécanismes de filtrage en profondeur ainsi qu'à des fonctions de journalisation des événements, les pare-feu sont en outre des éléments cruciaux pour les investigations de sécurité.

Les principaux concepts de pare-feu sont le filtrage de paquets, pour filtrer les paquets de la couche réseau (IP, etc.), le filtrage à mémoire, pour filtrer les paquets de manière dynamique en adaptant les règles de filtrage, la passerelle de niveau circuit, pour filtrer les paquets en gérant le concept de session, et la passerelle de niveau applicatif, pour filtrer jusqu'aux protocoles des couches applicatives. [5]

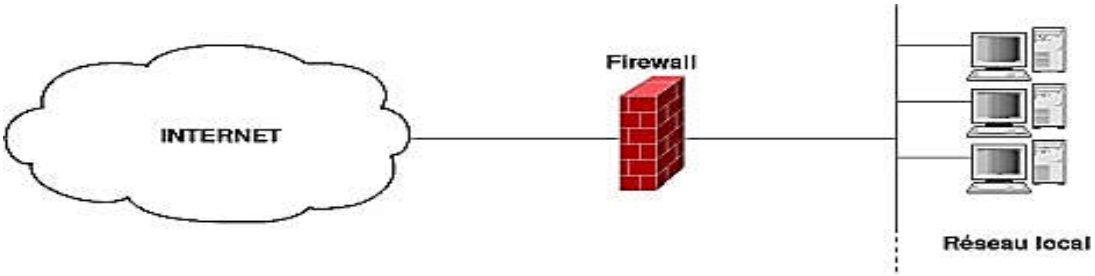

Figure II.8 Pare-feu

II.7.6 zone démilitarisée (DMZ)

Est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.

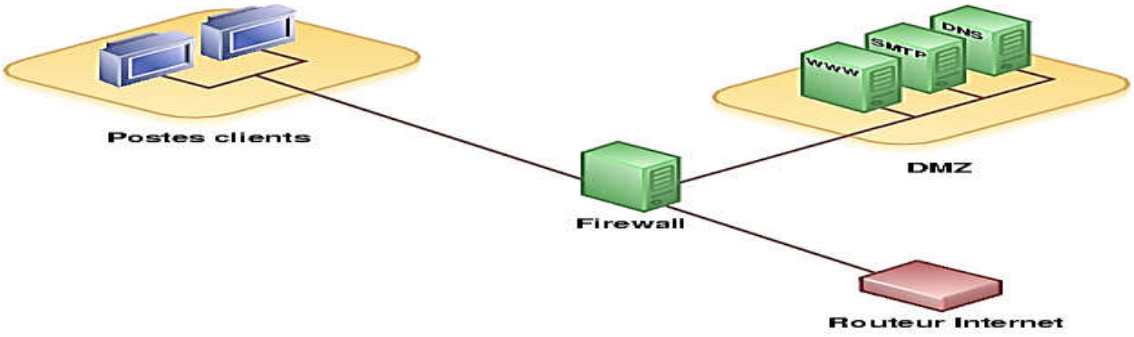

Figure II.9 Réseau d'une utilisation de DMZ avec un pare-feu

II.7.7Radius

Ce protocole repose sur le principe des 3A : Authentication (Authentification) Authorization (Autorisation) Accounting (Comptabilisation).

- Authentification : Le protocole permet d'effectuer une authentification distante, centraliser les données d'authentification et gérer les connexions des utilisateurs vers des services distants.
- Autorisation : Le protocole vérifie les droits attribués à un utilisateur.
- Comptabilisation : Le protocole est en mesure de journaliser l'activité d'un utilisateur sur le réseau pour effectuer entre autres une future facturation.

Ce protocole a trouvé sa réputation auprès des fournisseurs d'accès internet qui l'utilisent pour identifier les clients couplé à un serveur LDAP. Il est également employé pour gérer l'authentification sur des points d'accès WIFI. Il repose sur la couche UDP. En effet, Radius est un protocole dit « sans état » ce qui permet de simplifier la mise en œuvre du serveur puisque celui-ci n'attend pas d'accusé de réception.

II.7.8 Les VLANs

Les réseaux locaux virtuels (Virtual LAN), s'agit d'un dispositif de couche 2 (liaison de donnée). Ils permettent d'améliorer la sécurité d'un réseau local en cloisonnant le trafic réseau par la réservation à chaque équipe ou entité fonctionnelle d'un réseau privé virtuel, et en limitant ainsi la promiscuité des données. Une application assez répandue et commode de ce procédé consiste, sur un campus ou au sein d'une entreprise, à créer pour

accueillir les ordinateurs portables des visiteurs extérieurs un VLAN où ils seront confinés, ce qui évitera qu'ils puissent accéder aux serveurs internes. [6].

Il existe 3 types différents de VLAN :

- **VLAN de niveau 1 ou VLAN par port** : on y définit les ports du commutateur qui appartiendront à tel ou tel VLAN. Cela permet entre autres de pouvoir distinguer physiquement quels ports appartiennent à quels VLAN.
- **VLAN de niveau 2 ou VLAN par adresse MAC** : on indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN.
- **VLAN de niveau 3 ou VLAN par adresse IP** : même principe que pour les VLAN de niveau 2 sauf que l'on indique les adresses IP (ou une plage d'IP) qui appartiendront à tel ou tel VLAN

II.7.9 Les VPNs (Virtual Private Network)

Un VPN (Virtual Private Network)s'agit d'établir un canal chiffré entre deux nœuds quelconques de l'Internet, ces nœuds pouvant eux-mêmes être des routeurs d'entrée de réseaux. On aura ainsi établi une sorte de tunnel qui, à travers l'Internet, reliera deux parties éloignées l'une de l'autre du réseau d'une même entreprise pour donner l'illusion de leur contiguïté. Mais le chiffrement permet aussi d'établir un VPN personnel pour un utilisateur, par exemple entre son ordinateur portable et le réseau local de l'entreprise. [6]

Voici les VPN que nous pouvons mettre en place sur un réseau dédié :

- **PPTP:** Facile à mettre en place, mais beaucoup d'inconvénients liés à la lourdeur du protocole de transport GRE, le matériel réseau (routeur ADSL, wifi, doit être compatible avec le PPTP)
- **Ipsec :** Plus efficace que le PPTP en termes de performance, mais aussi très contraignant au niveau de la mise en place
- **Open VPN :** La Rolls des VPN

II.7.10 IDS (Intrusion Détection System)

S'agit d'un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement de réagir à cette tentative.

II.7.11 IPS (Intrusion Prevention System)

Une fonctionnalité intégrée de plus en plus dans les pare-feu. C'est un outil similaire aux IDS, permettant de prendre des mesures afin de diminuerles impacts d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues etinconnues.

II.8 Les protocoles de sécurité

II.8.1 Le protocole SSL

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur le TCP/IP, (HTTP et FTP, etc..).

Le protocole SSL permet non seulement de fournir les services de d'authentification du serveur mais également les services de confidentialité et d'intégrité.

Le principe d'une l'authentification du serveur avec SSL est le suivant :

- Le navigateur du client fait une demande de transaction sécurisée au serveur.
- Suite à la requête du client, le serveur envoie son certificat au client.
- Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- Le client choisit l'algorithme.
- Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
- Le navigateur vérifie que le certificat délivré est valide.
- Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

II.8.2 Le protocole SSH

Le protocole **SSH** (Secure Shell) est un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

II.8.3 Le protocole IPsec (IPSecurity)

IPsec est un protocole destiné à fournir différents services de sécurité. Il propose ainsi plusieurs choix et options qui lui permettent de répondre de façon adaptée aux besoins des entreprises, particuliers, etc…

IPsec s'insère dans la pile de protocole TCP/IP, au niveau d'IP. Cela signifie qu'il agit sur chaque paquet IP reçu ou émis et peut soit le laisser passer sans traitement particulier, soit le rejeter, soit lui appliquer un mécanisme de sécurisation.

Le placement d'IPsec au niveau IP, c'est-à-dire au niveau réseau, présente l'avantage de le rendre exploitable par les niveaux supérieurs, et donc d'offrir un moyen de protection unique pour toutes les applications.

Le réseau IPv4 étant largement déployé et la migration vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6.

Les principales fonctions que peut assurer le protocole IPsec sont :

- Authentification des extrémités.
- Confidentialité des données échangées.
- Authenticités des données.
- Intégrité des données échangées

- Protection contre les écoutes et l'analyses de trafic.
- Contrôle d'accès

II.8.4 Les ACLs

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées au trafic circulant via une interface de routeur.

Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (InternetworkPacket Exchange).

Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau. Les listes d'accès filtrent le trafic réseau en commandant aux interfaces d'un routeur d'acheminer ou de bloquer des paquets routés [8].

Figure II.10 Les ACLs

II.8.5 NAT (Network Adress Translation)

C'est un mécanisme permettant de simplifier la gestion de l'adressage IP utilisée pour se connecter à l'extérieur tout en conservant les adresses IP, cette croissance rapide aurait épuisé la réserve existant d'adresses IP. Pour enregistrées dans les réseaux privés. Lorsqu'un paquet est routé par un équipement de réseau (routeur ou pare-feu) vers des réseaux externes, une adresse IP publique routable est attribuée par la passerelle NAT à l'adresse source, c'est-à-dire l'adresse réseau interne privée (non routable). L'adresse publique de la réponse est ensuite retraduite en l'adresse interne privée. Cela, permet de

sécurisé, en empêchant de voir les adresses IP privées du réseau interne, les requêtes sembleront ainsi parvenir de la passerelle NAT.

II.8.6 TELNET (Terminal NETwork protocol)

Est un protocole qui offre la possibilité d'émuler un terminal à distance. C'est-à-dire qu'il permet à un utilisateur de se connecter à distance sur une machine, et de travailler sur celle-ci de la même manière que s'il était connecté en local sur cette machine.

II.9 Discussion

Dans ce chapitre on a évoqué que les attaques réseau reposent sur un ensemble de faiblesses de sécurité touchant différents domaines comme les protocoles réseau, les implémentations des piles réseau et les systèmes d'exploitation des systèmes réseaux. De fait que ces derniers peuvent avoir un impact direct et un indirecte sur un réseau. Pour faire face à ces attaques, de nombreux mécanismes de sécurité ont été élaboré pour répondre à un ensemble d'exigences de sécurité. Par conséquent, dans le cas de la sécurité informatique, la maintenance préventive doit être appliquée d'une manière continue dans une entreprise.

Chapitre III

Etude et présentation de la carte de supervision Cisco « WS-SUP720-3B »

III.1 Préambule

L'information a atteint une importance non négligeable dans le fonctionnement de l'entreprise, quelle que soit sa taille, son activité et sa situation géographique. Autrefois centralisée des gros systèmes informatique propriétaires, et accessible localement depuis des terminaux différents, donc l'information va désormais voyager partout au sein de l'entreprise. Afin d'assurer le bon fonctionnement du réseau et l'acheminement et le transfert de données en toute fiabilité et sécurité la famille de produit Cisco Catalyst 6500 fournit des services sécurisés et convergeant pour le commutateur d'étage comme pour le commutateur de cœur, pour les centres de données, et l'accès au WAN, et cela grâce au moteur de supervision Cisco « ws-sup720-3b » qui définit le standard pour les commutateurs multicouches et la livraison d'application dans le campus d'entreprise et les réseaux commutés.

Dans ce chapitre on s'intéressera à l'étude du moteur de supervision Cisco ws-sup720-3b qui est utilisé au sein du centre de calcul de l'Université de Mouloud Mammeri de Tizi-Ouzou et les différents services proposés par ce dernier.

III.2 Présentation du Cisco Série Ctalyst 6500

Les séries Cisco Catalys 6500 définissent la nouvelle norme pour les communications IP et la livraison d'applications dans les réseaux de campus d'entreprise et de fournisseurs de services en maximisant la productivité des utilisateurs et en améliorant le contrôle opérationnel et offre des services sécurisés, convergents et de bout en bout. Ce dernier offre une protection de l'investissement sans précédent et offre des performances évolutives et une densité de port à travers plusieurs configurations de châssis et des interfaces réseau LAN, WAN et métropolitaine (MAN). Disponible dans les châssis de 3, 6, 9 et 13 emplacements, ces commutateurs disposent d'une gamme inégalée de modules de services intégrés, y compris la sécurité du réseau multi-gigabit, le changement de contenu, les modules d'analyse de réseau. Ces derniers offre une grande cohérence opérationnelle qui optimise l'utilisation de l'infrastructure informatique et renforce le retour sur investissement. De 48 ports à 576 ports 10/100/1000 ou de câblages Ethernet 10/100 à 400 millions de paquets par seconde (mpps). Avec de nombreuses fonctionnalités, la nouvelle génération Catalyst 6500 Séries Supervisor Engine 720 intègrent 11 nouveaux circuits intégrés (ASIC) spécifiques à l'application.

Figure III.1 Commutateur Cisco Catalyst 6500

III.3 Présentation du moteur de supervision cisco « ws-sup720-3b »

Les cartes de supervision 1A et les cartes de supervision 2, largement déployées, sont un complément à la carte de supervision SUP720 destinés aux locaux techniques d'étages, les réseaux de distribution ou de cœur de petite taille, le centre de données et les configurations de l'accès WAN. Les cartes de supervision de la famille Catalyst 6500 permettent l'intégration parfaite des services avancés tels que la sécurité, la voix et la gestion de contenu dans un réseau convergeant réduisant ainsi le coût total d'acquisition.

Le Catalyst 6500 Séries équipé de la carte de Supervision sup720 définit le standard pour les commutateurs multicouches et la livraison d'application dans le campus d'entreprise et les réseaux commutés. Ce moteur de supervision combine des liaisons de liaison haute densité, la virtualisation du système et un débit accru avec des performances évolutives et un ensemble de fonctionnalités IP enrichi. Ce dernier fournit des services nouveaux et avancés sur le protocole IP, et elle fournit aussi le support des nouvelles interfaces gigabits et 10 gigabits haute performance. En outre, il supporte les 3 générations d'interface et de modules de services Catalyst 6500, permettant une augmentation de la densité de ports et de configurations des services de module sur le châssis Catalyst 6500. Le moteur de supervision sup720 du Catalyst 6500 intègre une matrice de commutation 720 Gbps de haute performance avec un nouveau moteur de routage et de transfert (MSFC), y compris une carte Policy Feature Card de 3e génération (PFC3) dans un seul module.

Ce dernier est construit sur l'architecture Cisco Express Forwarding (CEF) qui a fait ses preuves, en supportant le transfert centralisé (CEF), le transfert distribué (dCEF) et, maintenant, le CEF accéléré (aCEF) pour fournir une plateforme très évolutive et rentable qui est idéale pour les environnements du réseau fédérateur et de centre de données hautes performances.

Le moteur de supervision « ws-sup720-3b » fournit la performance évolutive, l'intelligence, et le large choix de fonctionnalités pour répondre aux besoins des déploiements des entreprises et opérateurs en télécommunications et construire des solutions de commutation modulaires, résilientes, évolutives, sécurisées et multicouches.

Figure III.2 Carte de supervision **<Cisco ws-sup720-3b>**

III.3.1Caractéristiques du panneau avant de la carte

La figure suivante (Figure) nous montre la face avant de la carte de supervision Cisco (ws-Sup720-3b) :

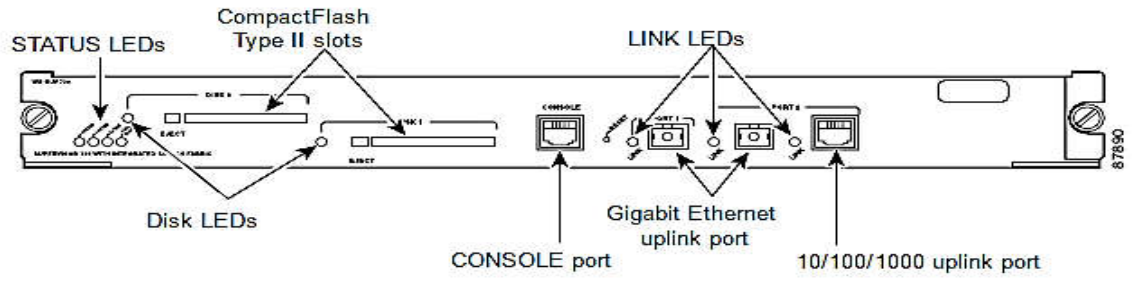

Figure III.3: La face avant de la carte de supervision (ws-Sup720-3b).

Le tableau suivent décrit la fonctionnalité de chaque élément de la carte WS-Sup720-3B :

Fonctionnalité	Description
Interrupteur RESET	Le commutateur RESET permet de réinitialiseret de redémarrer le commutateur.
Port CONSOLE	Il s'agit d'un port 10/100/1000 utilisant un connecteur RJ-45. Permet d'accéder au commutateur localement (avec un terminal de console) ou à distance (avec un modem)
DISK 0 et DISK 1 slot	Deux emplacements PCMCIA sont disponibles. Les machines à sous PCMCIA permettent une carte PC flash à installer en fournissant une mémoire flash supplémentaire. L'utilisation de ce flash mémoire pour stocker et exécuter des images logicielles ou pour servir de périphérique (entré /sortie).
Ports Uplink (PORT 1 et PORT 2)	La carte de supervision dispose de trois ports de liaison montante: • Deux ports de 1000BASE-X SFP • Un port 10/100 / 1000BASE RJ-45. Seuls deux ports peuvent être Actif à la fois.

Tableau III.1 fonctionnalité de chaque port de la face avant de la carte

Les voyants sur le panneau avant du moteur de supervision montrent l'état de processeur et les autres composants installés sur le routeur, Le tableau (III.2) énumère les fonctions des LEDs.

Voyant	Couleur	Description
Statuts	Vert	Tous les tests diagnostiques ont réussi: le module est opérationnel (séquence d'initialisation normale).
	Orange	Le module est en phase d'amorçage ou de tests de diagnostic (séquence d'initialisation normale). Une surchauffe s'est produite. (Un seuil mineur a été dépassé pendant la surveillance de l'environnement).
	Rouge	Les tests diagnostiques ont échoué ; le module n'est pas opérationnel. (La défaillance s'est produite pendant la séquence d'initialisation). Une surchauffe s'est produite. (Un seuil majeur a été dépassé pendant la surveillance de l'environnement).

Tableau III.2 Signification des Voyants du moteur de supervision

III.4 L'architecture de la carte de supervision « ws-sup720-3b »

Le moteur de supervision « ws-sup720-3b » du Catalyst 6500 intègre une matrice de commutation 720 Gbps de haute performance avec un nouveau moteur de routage et de transfert de 3^{éme} génération (MSFC3), y compris une carte Policy FeatureCard de 3^{éme} génération (PFC3) dans un seul module.

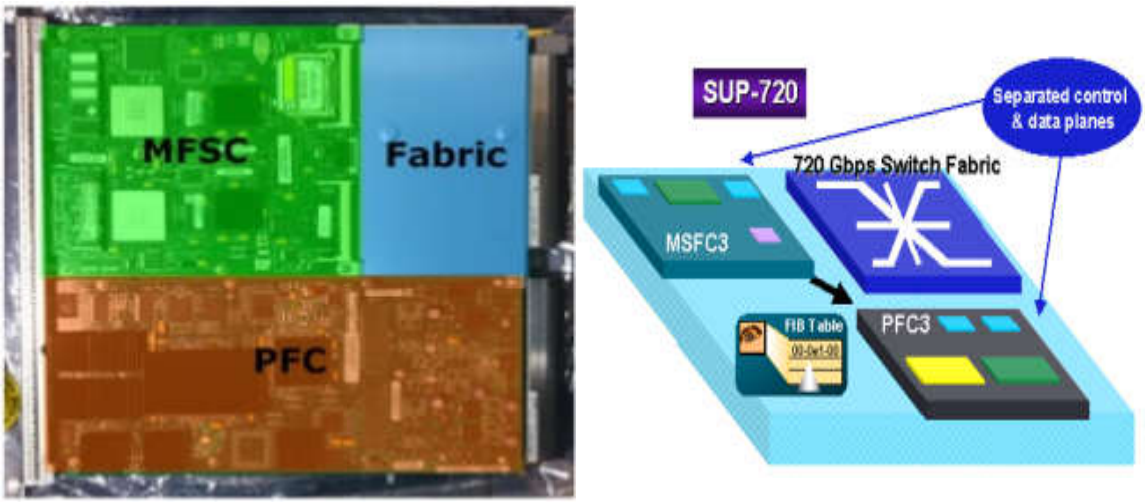

Figure III.4 Schéma représentatif des différents blocs de la carte

III.4.1 Multi-layer Switch Feature Card 3 (MSFC3)

Le **Multilayer Switch Feature Card 3** est le moteur de commutation de couche 3 qui se trouve sur le moteur de supervision en tant que carte fille. Le MSFC est une partie intégrante du moteur supervision, fournissant une haute performance, une commutation multicouche et une intelligence de routage. Sur la carte fille MSFC, le processeur d'itinéraire (RP) est situé sur le MSFC lui-même. Équipé d'un processeur haute performance, le MSFC exécute des protocoles de couche 2 sur processeur de commutation (SP) et des protocoles de couche 3 sur le processeur de routage (RP). Il s'agit notamment du support du protocole de routage, des protocoles de couche 2, et il inclut aussi :

- ✓ Support du protocole de routage : comprenant BGP4, IS-IS, OSPF, RIP, et plus
- ✓ Protocoles traditionnels comprenant IP, IPX, Appletalk, DECnet, OSI, CLNS.
- ✓ Services multimédia : Multidistribution Indépendamment du Protocole (PIM) (Dense Mode et Sparse Mode), et snooping Cisco Group Management Protocol (CGMP) et Internet Group Management Protocol (IGMP)
- ✓ Services de sécurité : liste d'accès, encryptions, serrure et clef

Le MSFC construit la table de Base d'Information de Transfert (FIB) CEF dans le logiciel et télécharge ensuite cette table vers le matériel (ASICs) sur le PFC et DFC (si présent) qui prend les décisions de transfert pour le trafic unicast et multicast IP. Cette approche, utilisant le Cisco Express Forwarding, sépare les plans de contrôle et de données, permettant des possibilités de transfert de paquets très évolutives allant jusqu'à

500Kpps. En outre, cette dernière est équipée aussi de 2 SDRAM de (512 Mo) et aussi de 2 Bootflash de (64Mo)

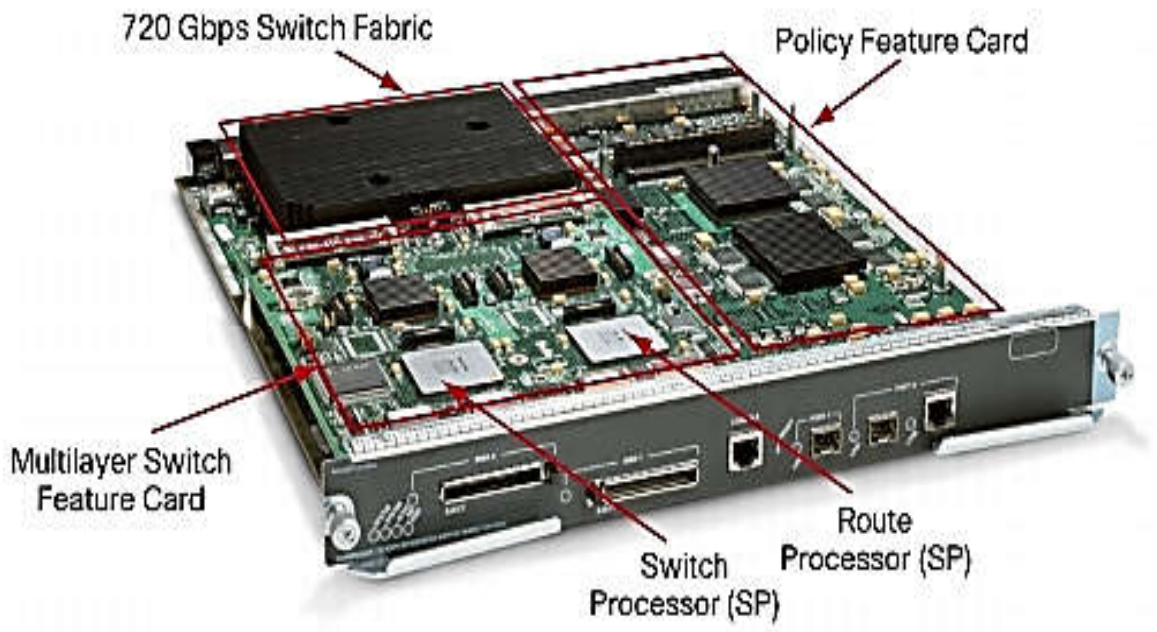

Figure III.5 Partie intégrée MSFC3

III.4.2 Policy Feature Card 3 (PFC3)

La carte de supervision «ws-sup720-3b » comporte une carte Policy Feature Card fournissant la protection et la flexibilité additionnelles d'investissement en supportant une gamme de fonctions accélérées par matériel. Le PFC3 pour le moteur de supervision supporte la fonction de routage et pont, la Qualité de Service (QoS) et de réplication des paquets Multicast. Le PFC identifie et classifie le trafic appliquant les politiques de Qos ou de sécurité défini par l'administrateur réseau au travers d'ACL. Le PFC permet d'interdire les applications non autorisées sur le réseau. La PFC3 de ce dernier réalise le transfert de paquets grâce à son circuit intégré (ASIC). Dans des configurations de transfert distribuées, un composant ASIC situé sur un module d'interface (carte fille DFC3) permet au module d'interface de prendre des décisions de transfert de paquets localement. Après que le PFC3 ou le DFC3 prenne la décision de transfert pour le module d'interface, il transfert les paquets avec les politiques au niveau des couches 2-4 défini par l'administrateur.

En plus du transfert de paquets, le PFC3A propose un traitement matériel pour les fonctions suivantes :

- Rôle du moteur PFC3 dans la couche 2 :

  1. Les recherches d'adresse MAC de couche 2.
  2. Examiner les en-têtes de paquets pour déterminer si cette opération de commutation sera une opération de couche 2 ou de couche 3. Si cela va être une opération de couche 3, il remettra le paquet au moteur Layer 3 pour un traitement ultérieur.

- Rôle du moteur PFC Layer 3

  1. Collection des statistiques NetFlow.
  2. Transmission par matériel des paquets étiquetés IPv4, IPv6 et MPLS.
  3. Le mécanisme QoS pour la classification ACL, le marquage des paquets et la police (limitation des taux).
  4. Mécanisme de sécurité pour valider les règles ACL contre les paquets entrants.
  5. Maintien des entrées et des statistiques de l'adjacence.
  6. Maintenance des compteurs ACL de sécurité.

Figure III.6 CartePFC3

III.4.3 Matrice de commutation

Le moteur de supervision sup720 comporte une matrice de commutation de 720Gbps. Cette matrice à large bande passante permet au Catalyst 6500 séries de supporter des configurations d'agrégation gigabit Ethernet et 10 gigabit Ethernet de haute densité. En intégrant une matrice de commutation avec la fonction de surveillance, ce dernier élimine

le besoin d'un module de matrice de commutation séparé qui utiliserait un slot. Au final, des modules d'interface ou de services additionnels peuvent être déployés, ayant pour résultat une plus grande densité de port système du Catalyst 6500 et/ou réduisant le besoin de sécurité externe, de gestion de contenu, d'analyse de réseau ou de passerelles voix. L'efficacité du port est encore augmentée dans les configurations haute disponibilités qui exigent des cartes de supervisions redondantes et des matrices de commutation, sauvegardant deux slots pour les modules d'interface ou les modules de services qui exigeraient autrement deux modules de matrice de commutation.

III.4.3.1 Architecture du module de matrice de commutation

La matrice de commutation intégrée du moteur de supervision est composée de 18 canaux fournissant 720Gbps de bande passante au châssis du Catalyst 6500 séries. Chaque canal dispose d'une connexion dédiée de 20Gbps en entrée et 20Gbps en sortie (total de 40Gbps par calculs usuels de l'industrie). La matrice de commutation de la carte de supervision utilise une architecture dont les performances ont été augmentées par 3 pour supporter le transfert de paquets efficace pour les trafics unicast, broadcaste et multicast. La bande passante simple ou double canal dédiée est fournie à chaque slot du châssis.

III.4.3.2 Disponibilité élevée

Deux moteur de supervision « ws-sup720-3b » peuvent être configurés dans un système fournissant une configuration redondante de disponibilité élevée de la matrice de commutation permettant au système en cas de panne de basculer sur la matrice de commutation de la seconde carte de supervision et assurant la protection pour des applications critiques (Figure III.7).

Une fois installé dans une configuration redondante, le temps d'indisponibilité entre les matrices de commutation est de quelques secondes et la bande passante de système totale reste de 720. Ce dispositif de disponibilité élevée réduit au minimum l'impact des pannes sur des applications critiques dans différents environnements de réseau. Dans une configuration avec une simple de matrice de commutation avec des modules supportant le bus et la connexion à la matrice, en cas de panne le système peut basculer sur le bus de 32-Gbps de la carte de supervision, fournissant une plateforme fortement disponible pour héberger les applications critiques.

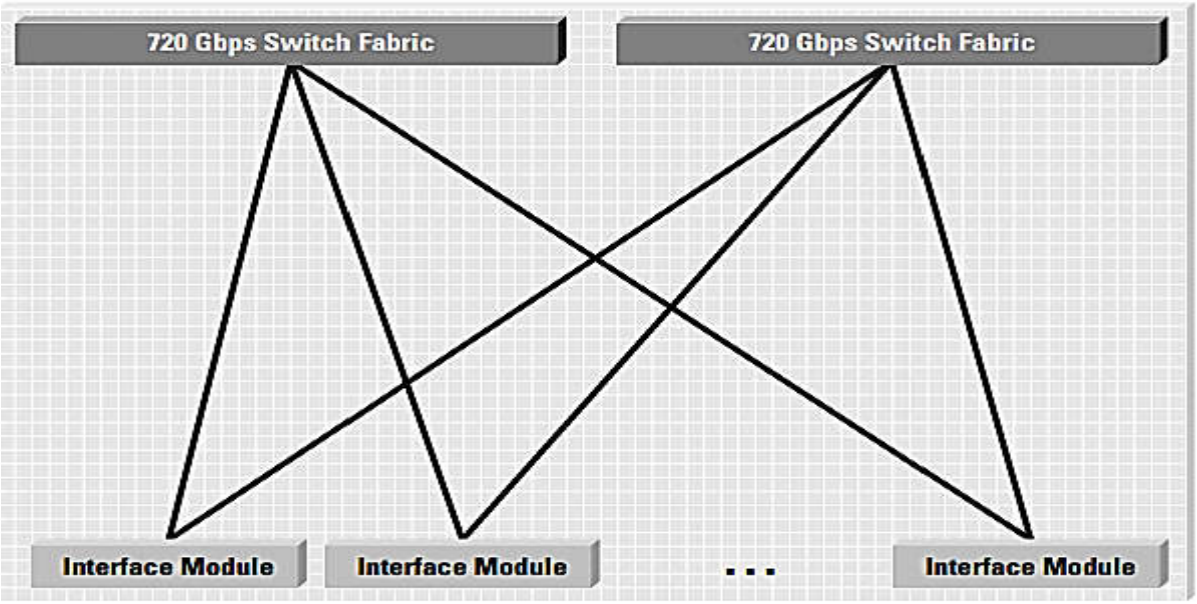

Figure III.7 Configuration redondante du moteur de supervision sup720

III.5 Comment fonctionne le Cisco Express Forwarding (CEF) ?

Le Cisco Express Frowarding (CEF) est une technologie Couche 3 qui fournit une évolutivité de transfert et d'exécution accrus pour gérer plusieurs flux de trafic de courte durée communs dans les réseaux d'entreprise et de fournisseur d'accès d'aujourd'hui. Pour rencontrer les besoins des environnements gérant de grandes quantités de types de trafic à flux courts, basés sur le Web, ou fortement interactifs, CEF transfert tous les paquets de manière matérielle, et maintient son taux de transfert complètement indépendant du nombre de flux traversant le commutateur.

Sur le Cisco Catalyst 6500 séries, le moteur de transfert Couche 3 CEF est situé sur le PFC3 de la carte de supervision : ce même dispositif exécute le transfert Couche 2 et 3 basé sur le matériel, vérifie les ACLs, s'occupe de la politique et du marquage de la QoS, et collecte de statistiques NetFlow.

En utilisant la table de routage que le logiciel Cisco IOS construit à partir des interfaces configurées et les protocoles de routage, l'architecture CEF créé des tables CEF et les télécharge dans le moteur de transfert matériel avant que tout trafic d'utilisateur soit envoyé à travers le commutateur. L'architecture CEF place seulement les préfixes de routage dans ses tables CEF (la seule information qu'elle requiert pour prendre des décisions de transfert Couche 3) se fondant sur les protocoles de routage pour faire le choix de l'itinéraire.

En exécutant une consultation de simple table CEF, le commutateur transfert les paquets rapidement et indépendamment du nombre de flux transitant par le commutateur.

III.5.1 Cisco Express Forwarding distribué (dCEF)

Avec le transfert distribué CEF (dCEF), les moteurs de transfert situés sur les modules d'interface prennent des décisions de transfert localement et en parallèle, permettant au Cisco Catalyst 6500 Series de réaliser les taux de transfert les plus élevés de l'industrie. Avec le dCEF, le transfert se produit sur les modules d'interface en parallèle et permet d'atteindre 400Mpps de performance globale.

En utilisant le même ASIC que le PFCx central, les DFCs situés sur les modules d'interface transfèrent les paquets entre deux ports, directement ou à travers la matrice de commutation, sans impliquer la carte de supervision. Avec le DFC, chaque module d'interface a un moteur de transfert dédié complet avec toutes les tables de transfert. Le transfert dCEF fonctionne comme ceci:

- Comme dans le transfert CEF standard, les PFC3 centraux situés sur le moteur de surveillance et les moteurs DFC situés sur les modules d'interface sont chargés avec la même information CEF dérivée de la table de transfert avant qu'un trafic utilisateur arrive au commutateur.
- Pendant qu'un paquet arrive à un module d'interface, son moteur DFC inspecte le paquet et utilise l'information dans la table CEF (y compris Couche 2, Couche 3, ACLs, et QoS) pour prendre une décision de transfert complètement basée sur le matériel pour ce paquet.
- Le moteur dCEF gère tout le transfert basé sur le matériel pour le trafic sur ce module, y compris le transfert Couche 2 et Couche 3, les ACLs, la politique et marquage QoS et NetFlow.
- Puisque les DFCs prennent toutes les décisions de commutation localement, la carte de supervision est libérée de toutes les responsabilités de transfert et peut exécuter les autres fonctions basées sur le logiciel y compris le routage, l'administration et les services réseau.

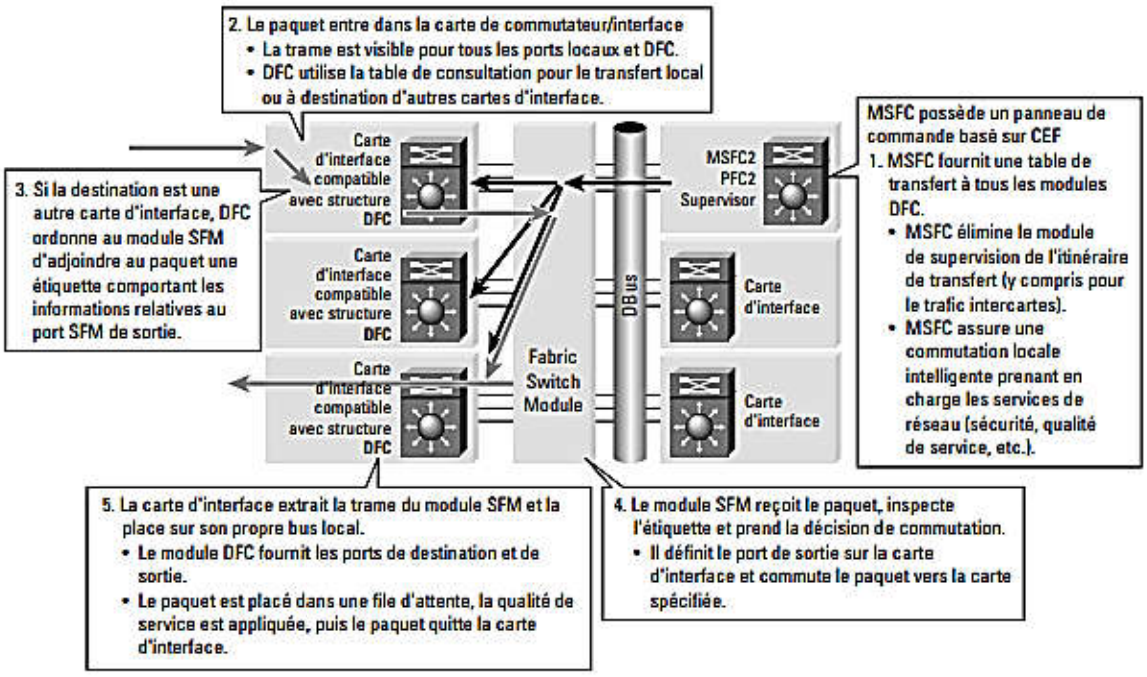

Figure III.8 Flux de paquet Cisco Express Forwarding distribué

III.5

La technologie de transfert express accéléré de Cisco (aCEF) utilise 2 moteurs de transfert travaillant ensemble avec un rapport maître-esclave pour accélérer les flux de trafic à taux élevés à travers le commutateur — un moteur central CEF situé sur le PFC3 du moteur de supervision et une carte fille moteur aCEF distribué supporter sur divers modules d'interface CEF720 (WS-X67xx), prévus pour une future disponibilité.

Le PFC3 central prend la décision initiale de transfert, avec le moteur aCEF stockant le résultat et prenant localement les décisions de transfert de paquets. Le transfert aCEF fonctionne comme suit :

- Comme dans le transfert standard CEF, le PFC3 central est chargé avec les informations de commutation nécessaire avant qu'un trafic utilisateur arrive au commutateur.
- Pendant que le trafic arrive sur un module d'interface CEF720 équipé d'une carte fille aCEF, le moteur aCEF inspecte le paquet, et constatant qu'aucune information spécifique sur le transfert de paquets n'existe, consulte le PFC3 central.
- Le PFC3 prend une décision de transfert basée sur le matériel pour ce paquet (y compris Couche 2, Couche 3, ACLs, et QoS).
- Le moteur aCEF stocke les résultats de décision de transfert et prend des décisions de transfert localement pour les paquets suivants basés sur l'historique du flux de paquet.

- Le moteur aCEF gère le transfert Couche 2 et la Couche 3 basé sur le matériel IPv4 et IPv6, les ACLs, le marquage QoS et NetFlow.
- Le PFC3 central traite toutes les décisions de transfert que le moteur d'interface module CEF ne peut pas gérer.

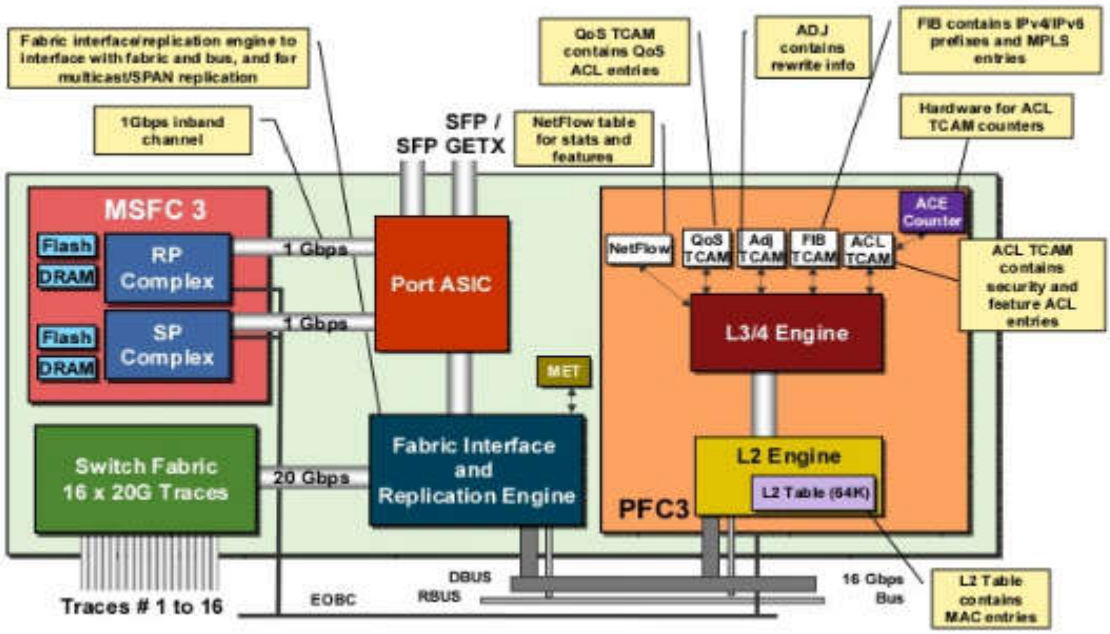

Figure III.9 Architecture du moteur de supervision « ws-sup720-3b »

III.6 Scénarios de déploiements du moteur de supervision sup720

Avec une large gamme d'interfaces, de modules de services, de configurations de châssis/slot aussi bien qu'un ensemble évolutif de carte de surveillance, les Catalyst 6500 peuvent être déployés n'importe où dans le réseau. Le figure suivante dépeint le Catalyst 6500 avec les cartes de surveillance déployées dans un réseau commuté où le Catalyst 6500 a été choisi pour l'accès, le cœur, la distribution, le centre de données, l'accès WAN et l'accès métropolitain.

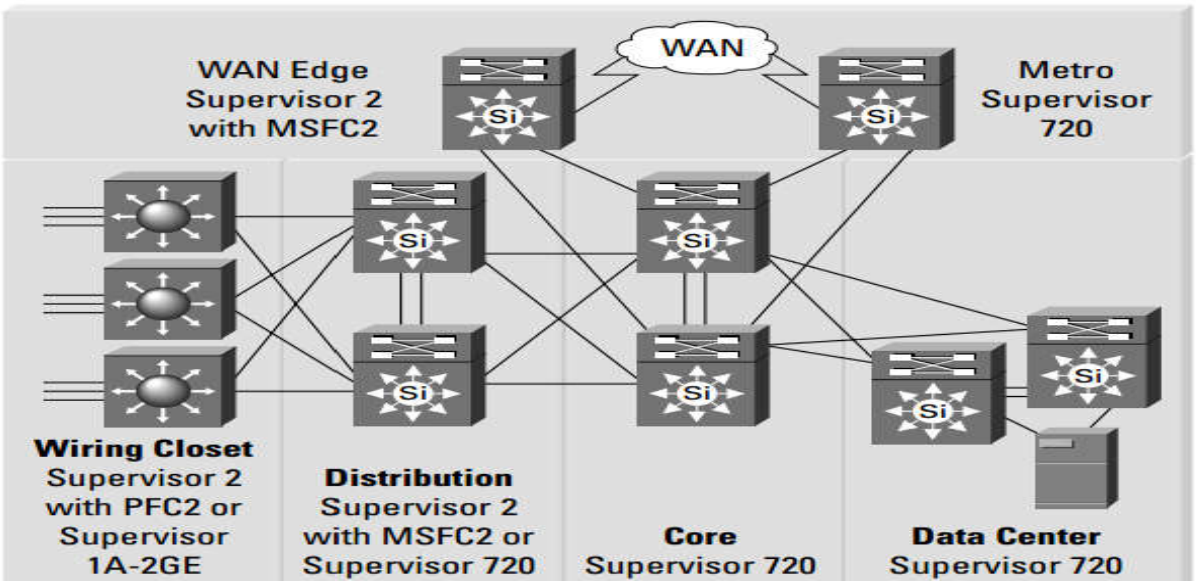

Figure III.10 Scénarios de déploiements des moteurs de supervision sup720

Le tableau suivant nous montre les déploiements recommandés pour le sup720 et autre moteur de supervisions :

Les moteurs de supervisions	Déploiements recommandés
Moteur de supervisionsup720	Cœur de réseau, distribution et centres de données d'entreprise.
Moteur supervision 2 Dispositif tactique carte 2 (PFC2) Dispositif de commutation multicouche carte 2 (MSFC2)	Distribution, centres de données et accès WAN d'entreprise.
Moteur de supervision 2 PFC2	Locaux techniques d'étages et centre de données.
Moteur de supervision 1A PFC MSFC2	Distribution et cœur de réseau.
Moteur de supervision 1A PFC	Locaux techniques d'étage.
Moteur de supervision 1A 2GE	Locaux techniques d'étage.

Tableau III.3 Scénarios de déploiementsdu moteur de supervision

III.7 Dispositifs fournit par le moteur de supervision sup720

Le moteur de supervisionsup720 fournit les dispositifs suivants :

a. Haute disponibilité : Ce dernier peut être déployé dans des configurations avec redondance de cartes de supervision dans tous les châssis de la gamme Cisco Catalyst 6500 Séries. Ces configurations permettent la synchronisation des états de protocole entre les cartes de supervision primaire et redondante, offrant une indisponibilité de réseau inférieur à 3 secondes, et maximise le temps de fonctionnement du réseau en permettant la permutation des cartes de supervision. Les dispositives important de haute disponibilité incluent :

- Redondance du moteur de supervision : support des protocoles HSRP, VRRP, et Uplink Fast
- Reconvérgence rapide : Reconvergence inférieur à 3 secondes au niveau 2, Unicast et Multicast IP Couche 3
- Extraction à chaud : supporte l'extraction à chaud des cartes de supervision

b. Performance évolutive et prévisible : La carte de supervision « ws-sup720-3b » fournit une performance évolutive : jusqu'à 400 Mpps avec une bande passante de 720 Gbps qui est requise dans des cœurs de réseau de forte concentration, les centres de données, et des environnements de calcul GRID avec de l'agrégation de liens multi-gigabit. Cette carte utilise l'architecture de routage Cisco Express Forwarding, qui permet une commutation à grande vitesse même avec des services avancés Couche 2-4 et ce jusqu'à 400 Mpps de performance de transfert.

c. Gestion du trafic avec services avancés : Il traite le trafic en respectant les règles de Qualité de Service (QoS) et sécurité au niveau des couches 2-4, y compris l'application des listes de contrôle d'accès (ACL), en tant qu'élément de son processus de transfert pour protéger et sécuriser le contenu. Ces dispositifs de gestion de trafic manipulent efficacement les réseaux convergés qui transportent aussi bien les applications critiques, celles dites temps-réel, et les applications multimédia qui nécessitent davantage de bande passante.

Outils avancés de QoS (Qualité de Service) : classification, marquage de paquet et contrôle de la congestion basée sur les informations d'en-tête de la Couche 2-4

Limitation de bande passante par utilisateur. Attribution des flux dans les files d'attente (scheduling) : weighted round robin (WRR) basé sur la gestion des files d'attente en entrée et sortie. Limitation de bande passante : Flux capté par flux ou par groupe de flux avec une granularité très fine.

d. Outils de gestion complète : Il nous fournit un ensemble complet d'outils de gestion pour fournir la visibilité et le contrôle exigés sur le réseau.

- Gestion par port console : administration de la carte de supervision et la carte MSFC3 hors bande depuis un terminal local ou un terminal à distance relié par modem au port console ou port auxiliaire.
- Gestion in-band:gestion par les protocoles SNMP, Telnet, BOOTP, TFTP.
- Analyseur de Port Commuté (SPAN) : permet la gestion et la surveillance de trafic commuté à l'aide d'un analyseur.
- Analyseur de Port Commuté à distance (RSPAN) : permet la gestion centralisée et la surveillance par redirection de trafic au travers de lien de type trunk entre les éléments actifs du réseau
- Capture du trafic VLAN avec liste de contrôle d'accès : dirige le trafic vers un port d'analyse réseau ou de détection d'intrusion en utilisant une ACL.

e. Sécurité avancée : Les possibilités de sécurité avancées de la carte de supervisions peuvent réduire la menace des attaques malveillantes du réseau tout en permettant l'authentification, l'autorisation, et la comptabilité (AAA). Avec le support de 32000 entrées ACL et des dispositifs avancés tels que la sécurité des ports, le moteur sup720 offre un ensemble inégalé de possibilités pour la sécurité du trafic au niveau des couches 2-4 :

- Sécurité de la Couche 2 : inclut private VLAN, AAA, IEEE802.1x, et sécurité des ports pour aider l'architecte réseau a correctement partitionné et contrôlé les ressources du réseau.
- Les filtres matériels au niveau des Couches 2-4 : peuvent travailler sur carte de supervision et en même temps sur les modules de services optionnels intégrés pour inspecter chaque paquet transféré et pour permettre ou refuser tous les flux de trafic selon les règles de l'administrateur réseau. Le taux limitant la fonctionnalité peut également être employé pour la protection contre des attaques de déni-de-service.

f. Transfert avancé de la Couche 2-4 : Le moteur de supervisionsup720 fournit les dispositifs avancés au niveau des Couches 2-4 que les concepteurs de réseau exigent pour établir des architectures de réseau avancées :

- MPLS :est un mécanisme de transport de données basé sur la commutation d'étiquettes ou "labels", qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie.
- Encapsulation de Routage Générique (GRE) : support de manière matériel des tunnels GRE pour le trafic IP.
- Traduction d'Adresses de Réseau (NAT) : Traduit des adresses pour le trafic d'entrée et d'arrivée au niveau matériel, permettant une séparation propre entre les réseaux internes et externes

III.8 Discussion

On présentant la carte de supervisions cisco « ws-sup720-3b » sa nous a permis de découvrir les différents blocs qui constituent le moteur de supervision et le rôle de chaque bloc dans la gestiond'un réseau. Adapté pour le déploiement dans la distribution, le noyau et dans le centre de données la carte de supervision « ws-sup720-3b » offre des améliorations significatives dans un réseau, on supportant matériellement les différents protocoles de routage adopté dans un réseau et on apportant des améliorations dans la sécurité élaborée dans le réseau et offre un ensemble inégalé de possibilités pour la sécurité du trafic.

Dans le chapitre suivant on passera a la configuration de cette même carte et présenter les différentes étapes qui nous permettra la configuration de cette dernière.

Chapitre IV

Configuration du moteur

De Supervision sous GNS3

IV.1 Préambule

Dans cette partie, on s'intéressera à la configuration de notre moteur de supervision Sup720 et à son rôle dans la gestion d'un réseau. Cette carte est utilisée uniquement comme routeur dans le réseau géré par le Centre des Systèmes et Réseaux d'information, de Communication, de Télé-enseignement et enseignement à Distance Ex Centre de Calcul de l'université de Mouloud Mammeri de Tizi-Ouzou (UMMTO).

Compte tenu de la sensibilité du réseau de l'UMMTO, nous avons effectués une simulation en utilisant le simulateur GNS3 combiné avec Vmware. Nous avons pris l'exemple de deux architectures. La première topologie pour donner les configurations de base de cette carte telle qu'elle est utilisée par le centre de calcul. Ensuite, nous avons optés pour une deuxième afin de montrer une autre utilité de cette carte qui est la sécurité.

IV.2 Présentation du GNS3

GNS3 est un simulateur d'équipements Cisco. Cet outil permet de charger de véritable IOS Cisco et de les utiliser en simulation complète sur un simple ordinateur. GNS3 permet d'avoir un routeur Cisco virtuel sur son ordinateur. Ce simulateur ne fournit pas d'IOS. Toutefois, afin de mettre en œuvre les différentes plateformes, des images système sont disponibles pour téléchargement.

La version que nous avons utilisée est 1.3.13. Celle-ci possède 4 routeurs qui sont :

- C2600
- C3600 (3620, 3640, 3660)
- C3700 (3725, 3745)
- C7200

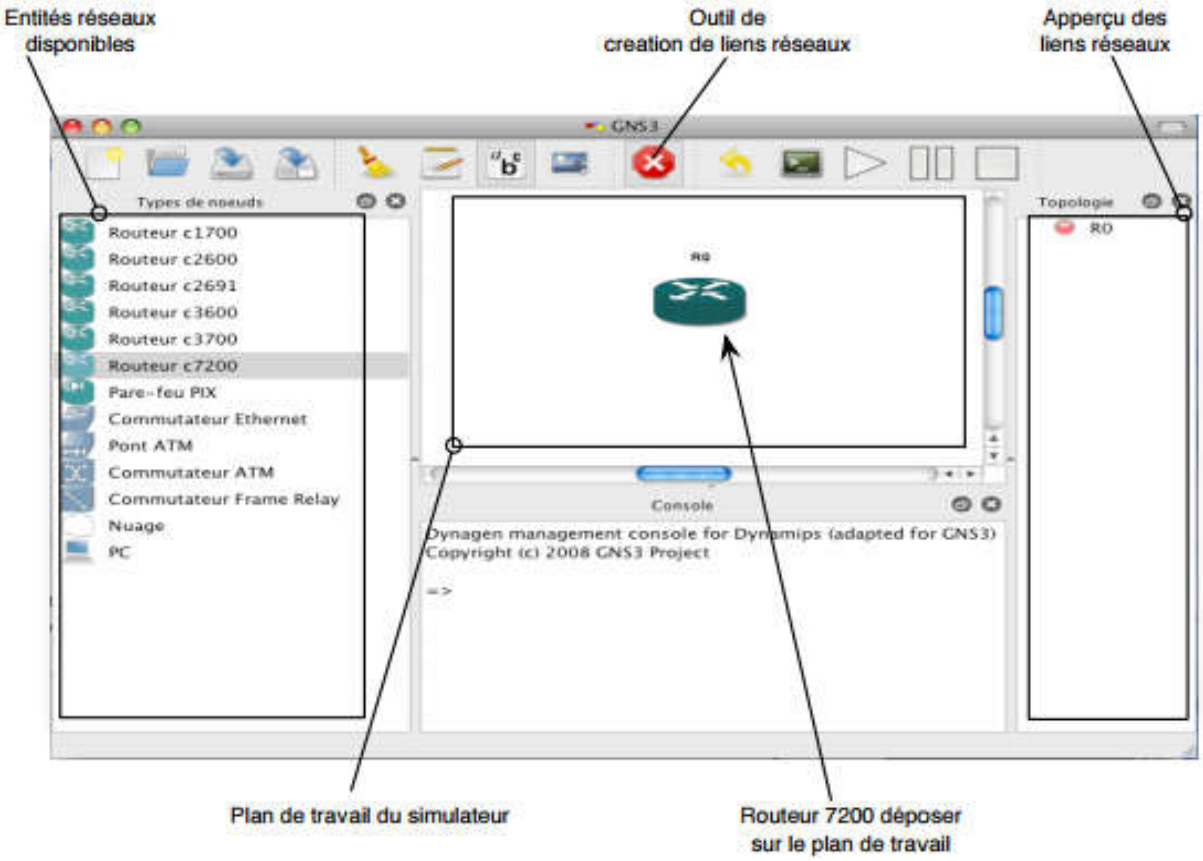

Figure VI.1 détails de la fenêtre du simulateur

Le modèle de la carte de supervision Cisco ws-sup720-3b n'est pas disponible sur notre simulateur GNS3. A cet effet, nous avons optés pour le c7200 car les caractéristiques de ce dernier sont similaires à sup720.

IV.3 Présentation du VMware Workstation

VMware Workstation est un logiciel permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte.

IV.4 Architecture du réseau 1

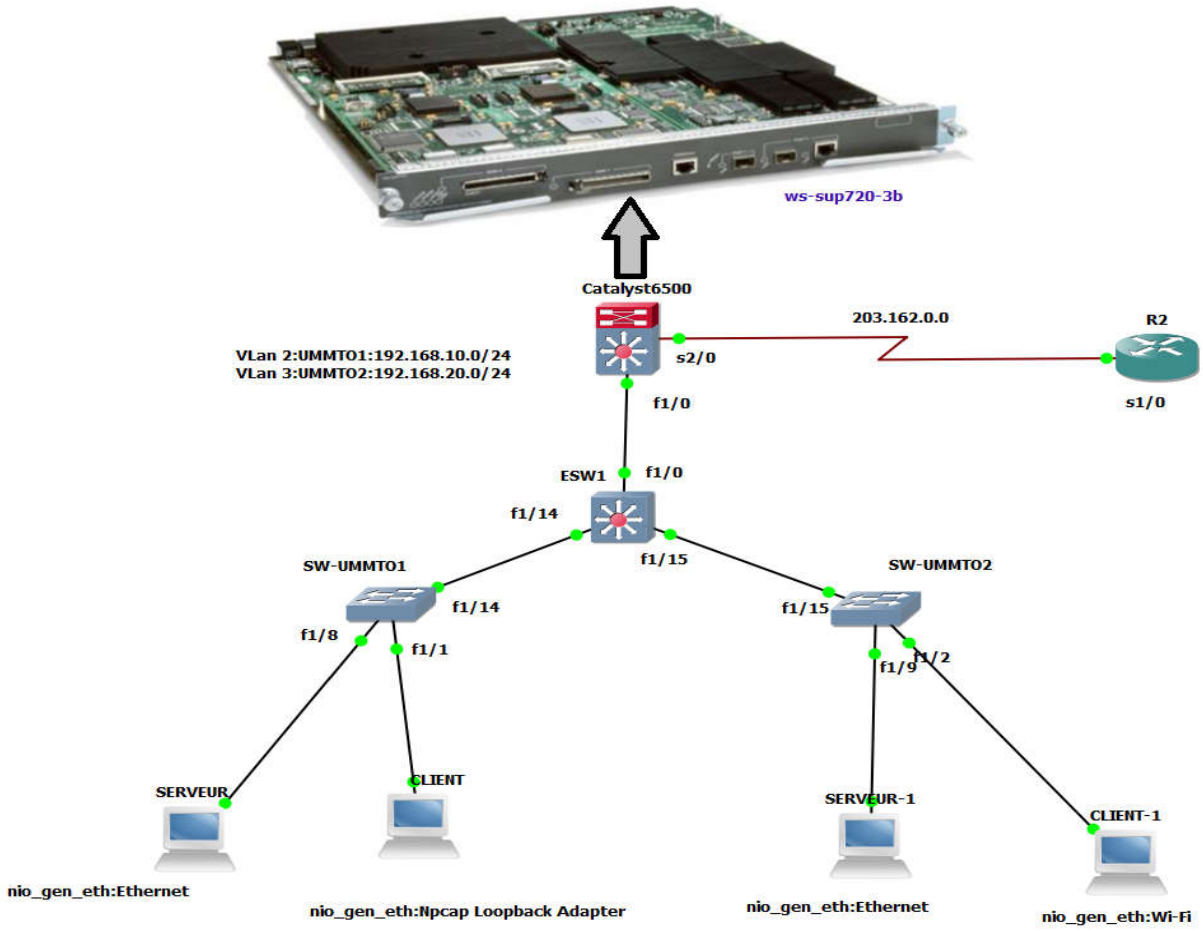

Figure IV.2topologie de notre réseau avec le routeur C7200 catalyst6500

Cette première topologie réseau est constituée des équipements suivant :

-Le routeur C7200 est le cœur du réseau qui représente le catalyst 6500 est utilisé pour la distribution d'adresses IP, et pour limité l'accès et la gestion des interfaces des Vlans. Un routeur R2 est utilisé pour prendre en charge l'accès à distance dans le réseau (accès Telent). Un Switch principale pour la configuration des vlans. 2 Switchs (ummto1/ummto2) secondaire qui sont reliées à des machines. 2 machines utilisées comme des clients. 2 machines utilisées comme des serveurs.

Afin de comprendre l'importance de la carte de supervision, nous l'avons remplacé par un routeur simple qui est le C1700. Au cours de sa configuration nous avons constaté les insuffisances suivantes :

- Une faible mémoire de stockage.
- Manque de ports et d'interfaces (console, Ethernet, VTY)
- Commutation de parquets non fiable
- Pas de contrôle de flux
- Nous ne pourrons pas le configurer autant que serveur DHCP ni appliquer les vlan vpn, IPsec, ACL etc….

Ces inconvénients montrent que nous ne pouvons pas remplacer cette carte par un routeur simple.

Dans cette première architecture (Figure IV.2), nous avons utilisés un serveur DHCP, des ACLs et la gestion du trafic de circulation des informations sur le moteur supervision Cisco. Dans le but de distribuer les adresses IP automatiquement et les liste Contrôle d'accès qui permettent de filtrer les paquets IP et la circulation du trafic.

IV.4.1 Configuration de base des routeurs et switchs

Pour se faire on suit les différentes commandes qui nous permettra la configuration les étapes de cette dernière sont les suivantes :

IV.4.1.a Configuration Catalyst 6500 :

1.Configuration de l'interface sérielle vers R2 nous lui avons attribuer une adresse ip

2.Création et Configuration de l'interface virtuelle FastEthernet 1/0.2 et 1/0.3.

3. configuration la route par default sur le Router Catalyst 6500 en utilisant l'interface série 2/0

Les étapes de configuration seront illustrées dans la figure ci-dessous :

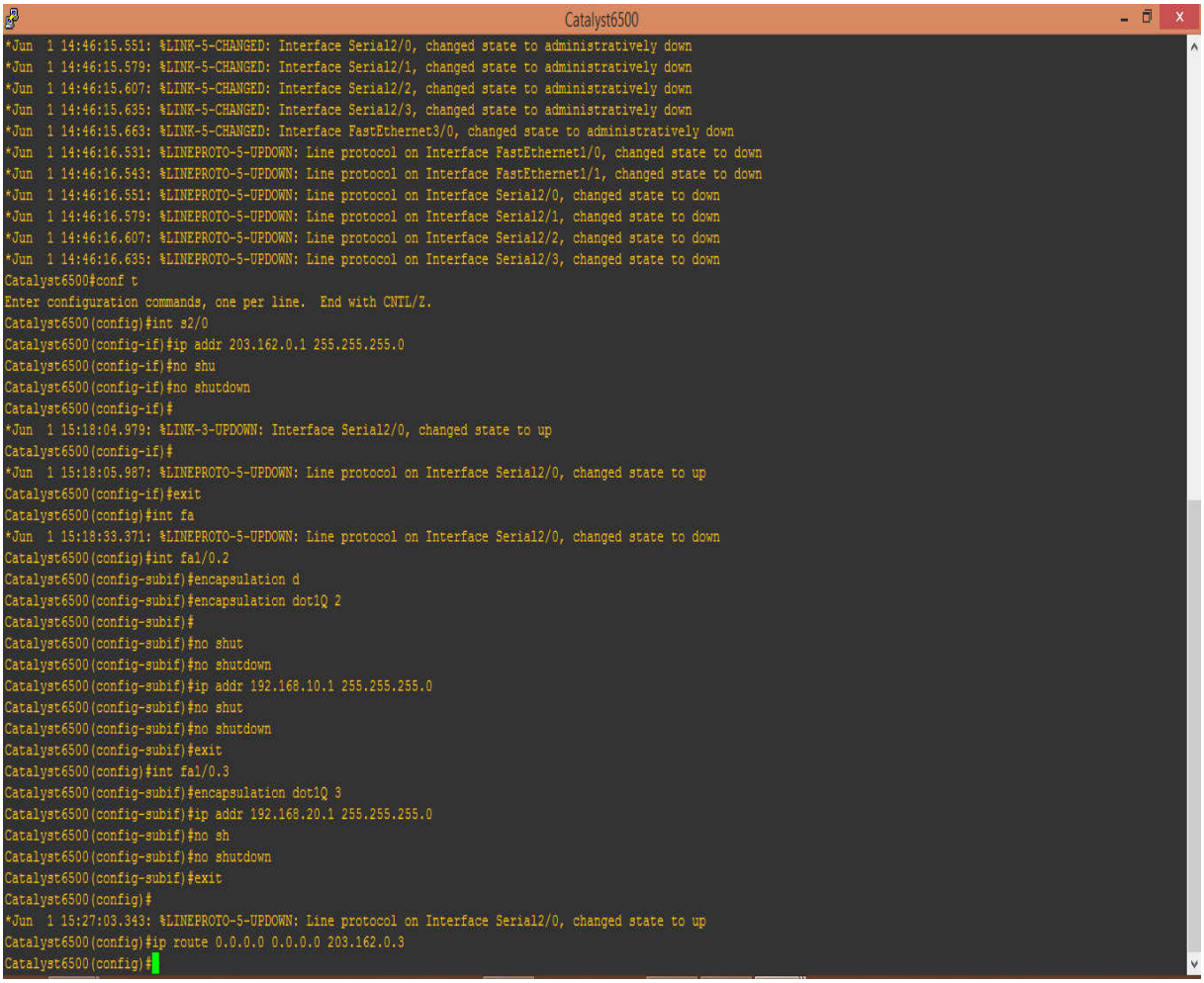

Figure IV.3 Les étapes de configuration sur catalyst6500

IV.4.1.b Configuration pool DHCP.

1. L'activation du serveur dhcp (dynamic Host Configuration Protocol).

2. On configure ensuite:

   - ✓ Le nom du pool.
   - ✓ Le réseau concerné.
   - ✓ Le nom du domaine.

3. attribution du DNS et la durée du bail au client.

Les adresses qui ne seront pas attribuées par le serveur dhcp sont: de 192.168.2.1 à192.168.2.99.

Pour réaliser la configuration on ne prendra qu'un seul exemple ummto1 pour ensuite procéder de la même manière pour la configuration sur ummto2 et la figure ci-dessous montre les différentes étapes de configuration et les étapes de configuration sont représentées par la figure ci-dessous

```
Catalyst6500#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Catalyst6500(config)#service dhcp
Catalyst6500(config)#ip dhcp pool ummto1
Catalyst6500(dhcp-config)#networek 192.168.2.0 255.255.255.0
                          ^
% Invalid input detected at '^' marker.

Catalyst6500(dhcp-config)#network 192.168.2.0 255.255.255.0
Catalyst6500(dhcp-config)#domain-name base1
Catalyst6500(dhcp-config)#dns-server 192.168.1.1
Catalyst6500(dhcp-config)#lease 0 8
Catalyst6500(dhcp-config)#exit
Catalyst6500(config)#ip dhcp ex
Catalyst6500(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.99
Catalyst6500(config)#exit
```

Figure IV.4 Les étapes de configuration le serveur DHCP sur catalyst6500

IV.4.1.cConfiguration d'ACL (Access Contrôle List)

Autoriser le vlan2 (ummto1) et le vlan3 (ummto2) de se communiquer entre euxet interdire la communication de tout autre vlan inconnu.

```
Catalyst6500#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Catalyst6500(config)#access-list 1 permit 192.168.10.0 0.0.0.255
Catalyst6500(config)#access-list 1 permit 192.168.20.0 0.0.0.255
Catalyst6500(config)#access-list 1 deny any
Catalyst6500(config)#int fa1/0.2
Catalyst6500(config-subif)#ip access-group 1 out
Catalyst6500(config-subif)#exit
```

Figure IV.5 Les étapes de configuration ACL sur catalyst6500

Nous utilisons la commande<< show access-list>> pour afficher la liste d'accès les résultats l'affiche la figure ci-dessous :

```
Catalyst6500#show access-list 1
Standard IP access list 1
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
    30 deny   any
```

Figure IV.6 Les résultats de la configuration ACL sur catalyst6500

IV.4.1.c Configuration du routeur R2 :

1. Configuration de la liaison sérielle vers Catalyst 6500
2. Les commandes suivantes permettent de définir un mot de passe facultatif mais recommandé sur la ligne console 0 et les lignes VTY 0 à 4.Pourpour prendre en charge l'accès a distance dans le réseau.
3. Configuration de la route statique on a opté pour un routage statique

La figure IV.7 nous permettra de montrer les etapes de configuration

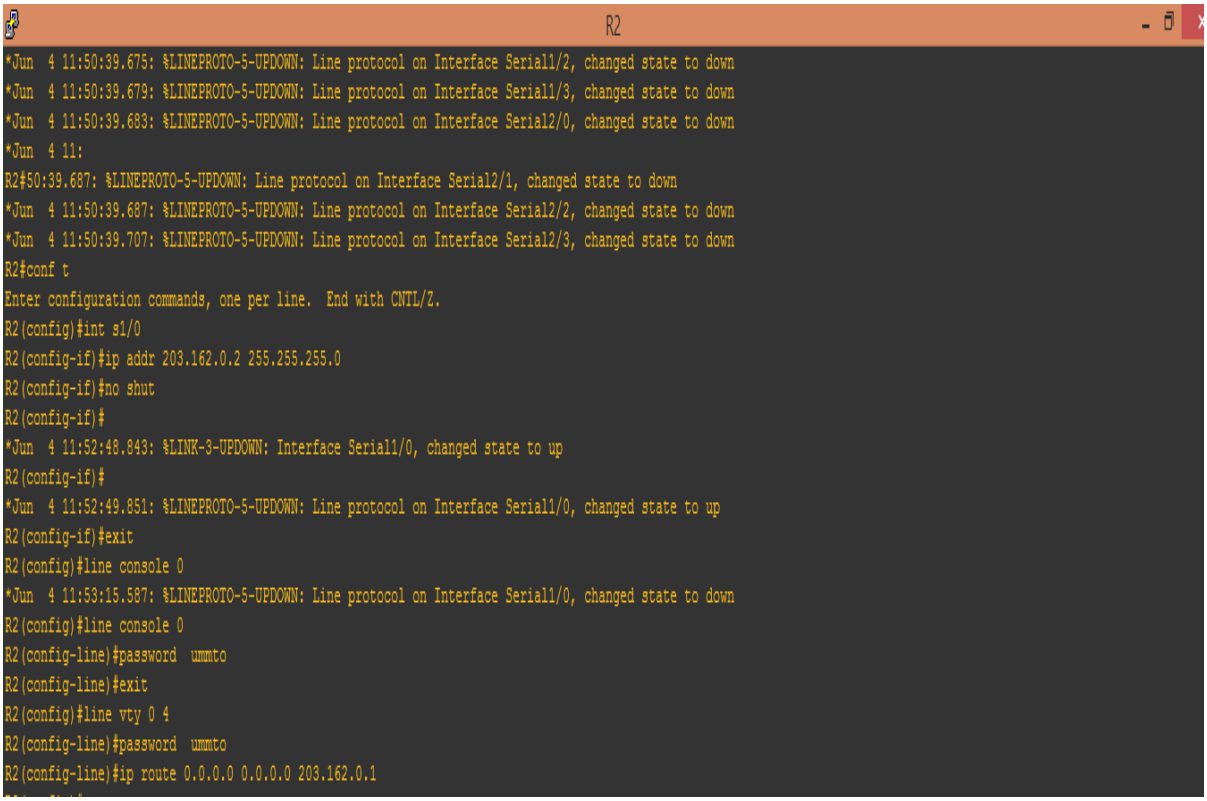

Figure IV.7 Les étapes de configuration sur R2

IV.4.2 configuration des VLANs

IV.4.2.a configuration duswitch1

1. Configuration du switch en monde VTP (Vlan trunk protocole)
2. Configuration de l'interface FastEthernet 1/0
3. Configuration de l'interface FastEthernet 1/14 et 1/15 en mode access et trunk
4. Créations des VLAN(2,3), avec la commande « vlandatabase »
   - ✓ Nom du vlan 2 : ummto1
   - ✓ Nom de vlan 3 : ummto2

Comme le montre la figure suivante :

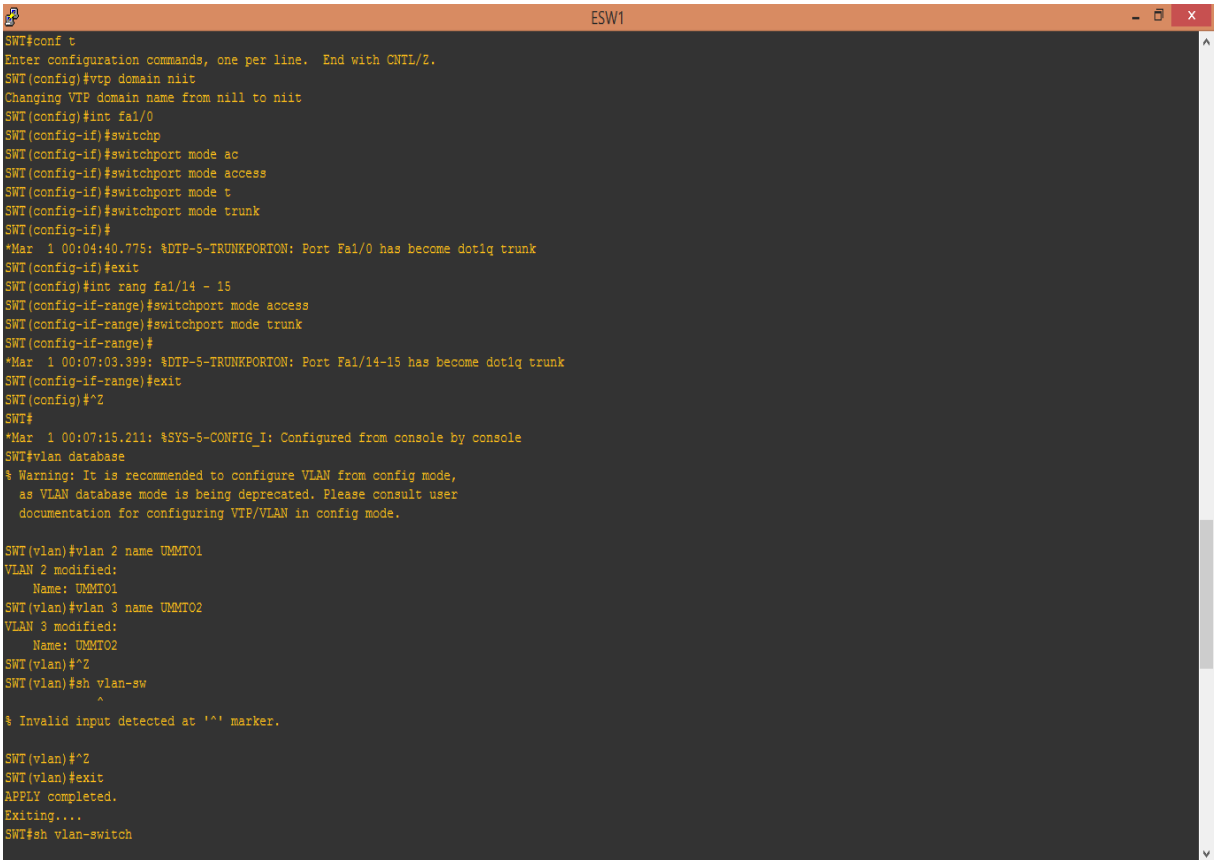

Figure IV.8 Les étapes de configuration du switch 1

On utilise la commande « show vlan-switch » pour afficher les VLAN et les interfacesaffectera chaque Vlans, les résultats sont représentés par la figure ci-dessous :

```
SWT#sh vlan-switch

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa1/0, Fa1/1, Fa1/2, Fa1/3
                                                   Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                   Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                   Fa1/12, Fa1/13, Fa1/14, Fa1/15
2    UMMTO1                              active
3    UMMTO2                              active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

Figure IV.9Résultat de la de configuration du switch 1

IV.4.2.b configuration DHCP par VLAN

Les routeurs peuvent utiliser le Dynamic Host Configuration Protocol (DHCP) pour permettre l'affectation automatique des configurations IP sur les différents postes. Ici nous avons utilisé une configuration DHCP par VLAN.

1- Configuration les vlan2et vlan3.
2- Deuxièmes nous allons indiquer le sous-réseau et le masque du pool d'adresses DHCP.
3- Spécification de l'adresse IP du switch par défaut pour un client DHCP.
4- nous avons Indiqué les adresses IP que le serveur DHCP ne doit pas attribuer aux clients DHCP.

Toutes les étapes de configuration sont illustrées dans la figure qui suit :

```
SWT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWT(config)#int vlan 2
SWT(config-if)#
*Mar  1 00:41:41.295: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
SWT(config-if)#ip addr 192.168.10.2 255.255.255.0
SWT(config-if)#exit
SWT(config)#int vlan 3
SWT(config-if)#
*Mar  1 00:43:03.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up
SWT(config-if)#ip addr 192.168.20.2 255.255.255.0
SWT(config-if)#exit
SWT(config)#ip dhcp pool vlan_UMMTO1
SWT(dhcp-config)#net
SWT(dhcp-config)#netw
SWT(dhcp-config)#network 192.168.10.0 255.255.255.0
SWT(dhcp-config)#default-r
SWT(dhcp-config)#default-router 192.168.10.1
SWT(dhcp-config)#exit
SWT(config)#ip dhcp exc
SWT(config)#ip dhcp excluded-address 192.168.10.1 192.168.10
% Incomplete command.

SWT(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
SWT(config)#ip dhcp pool vlan_UMMTO2
SWT(dhcp-config)#network 192.168.20.0 255.255.255.0
SWT(dhcp-config)#default-router 192.168.20.1
SWT(dhcp-config)#exit
SWT(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.9
SWT(config)#
```

Figure IV.10 Les étapes de la de configuration DHCP par VLAN sur le switch 1

IV.4.2.c Configuration du switch UMMTO1

1. Configuration du switch-UMMTO1 en mode VTP client.
2. Configuration du switch-UMMTO1 en mode access
3. Configuration du port fa1/1 en mode access au vlan 2

4. Configuration du port fa1/8 en mode access au vlan 3

Pour réaliser la configuration on ne prendra qu'un seul exemple switch-UMMTO1 pour ensuite procéder de la même manière pour la configuration du switch UMMTO2. Dans la figure suivante nous permettra de visualiser les étapes de configurations.

```
*Mar  1 00:08:29.283: %SYS-5-CONFIG_I: Configured from console by console
SW-UMMTO1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-UMMTO1(config)#vtp domain projet
Domain name already set to projet.
SW-UMMTO1(config)#vtp mode client
Device mode already VTP CLIENT.
SW-UMMTO1(config)#int fa1/14
SW-UMMTO1(config-if)#switchport mode access
SW-UMMTO1(config-if)#exit
SW-UMMTO1(config)#int rang fa1/1 - 7
SW-UMMTO1(config-if-range)#switchport mode access
SW-UMMTO1(config-if-range)#switchport access vlan 2
SW-UMMTO1(config-if-range)#exit
SW-UMMTO1(config)#int rang fa1/8 - 13
SW-UMMTO1(config-if-range)#switchport access vlan 3
SW-UMMTO1(config-if-range)#exit
SW-UMMTO1(config)#^Z
```

Figure IV.11 Les étapes de la de configuration du switch-ummto1

On utilise la commande « show vlan-switch» pour afficher les VLAN et les interfaces affecter au vlan 2,3 comme la figure ci-dessous le montre les interfaces Vlans sont activées

VLAN	Name	Status	Ports
1	default	active	Fa1/0, Fa1/1, Fa1/8, Fa1/14 Fa1/15
2	UMMTO1	active	Fa1/2, Fa1/3, Fa1/4, Fa1/5 Fa1/6, Fa1/7
3	UMMTO2	active	Fa1/9, Fa1/10, Fa1/11, Fa1/12 Fa1/13

Figure IV.12Résultat de la de configuration du switch-ummto1 et switch-ummto

IV.5 Configuration d'un VPN IPSec

Dans cette partie on va réaliser un VPN IPsec entre deux moteurs de supervision Cisco. Le but d'un VPN est d'authentifier et de chiffrer les données transmises où seul le routeur final pourra lire les données. On détaillera dans un premier temps la configuration de base que l'on doit faire sur les différents équipements avant de configurer le VPN.

IV.5.1 La deuxième architecture

Afin de donner l'une des applications supplémentaire de notre carte de supervision qui est la sécurité, nous l'avons utilisé dans le réseau suivant.

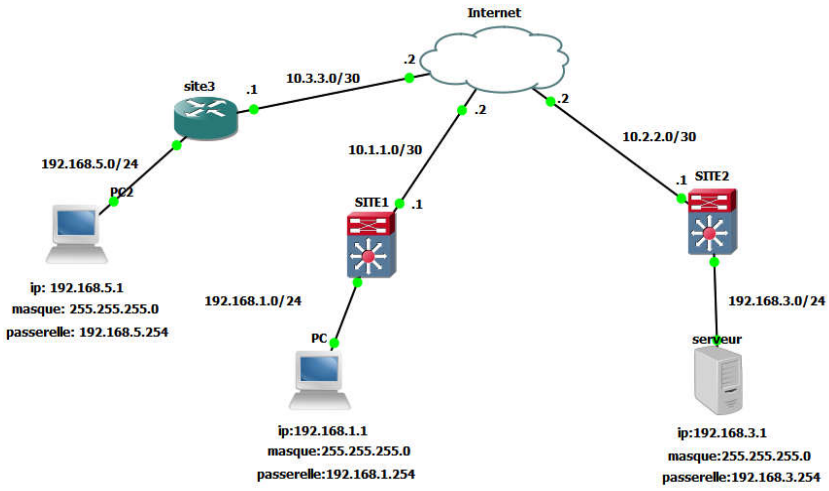

Figure IV.13architecture du réseau

Dans cette topologie nous avons proposé trois sites qui sont connecté a un réseau public (Internet) et les site1 et le site 2 sont connectés au réseau grâce à des catalyst6500 et le site 3 est connecté via un simple routeur comme la figure le montre (IV.13)

IV.5.2 Configuration de base des routeurs

Pour se faire on suit les différentes commandes qui nous permettra la configuration les étapes de cette dernière sont les suivantes :

1. configuration des interfaces de chaque routeur
2. on va leur allouer des adresses IP
3. configuration du routage RIP
4. sauvegarde de la configuration

Pour réaliser la configuration on ne prendra qu'un seul exemple **catalyst du site 1** pour ensuite procéder de la même manière pour la configuration des autres routeurs (routeur internet, catalyst du Site 2, routeur du site 3).

Figure IV.14 Les étapes de configuration sur catalyst du Site1

Les résultats de la configuration nous les montre la figure ci-dessous :

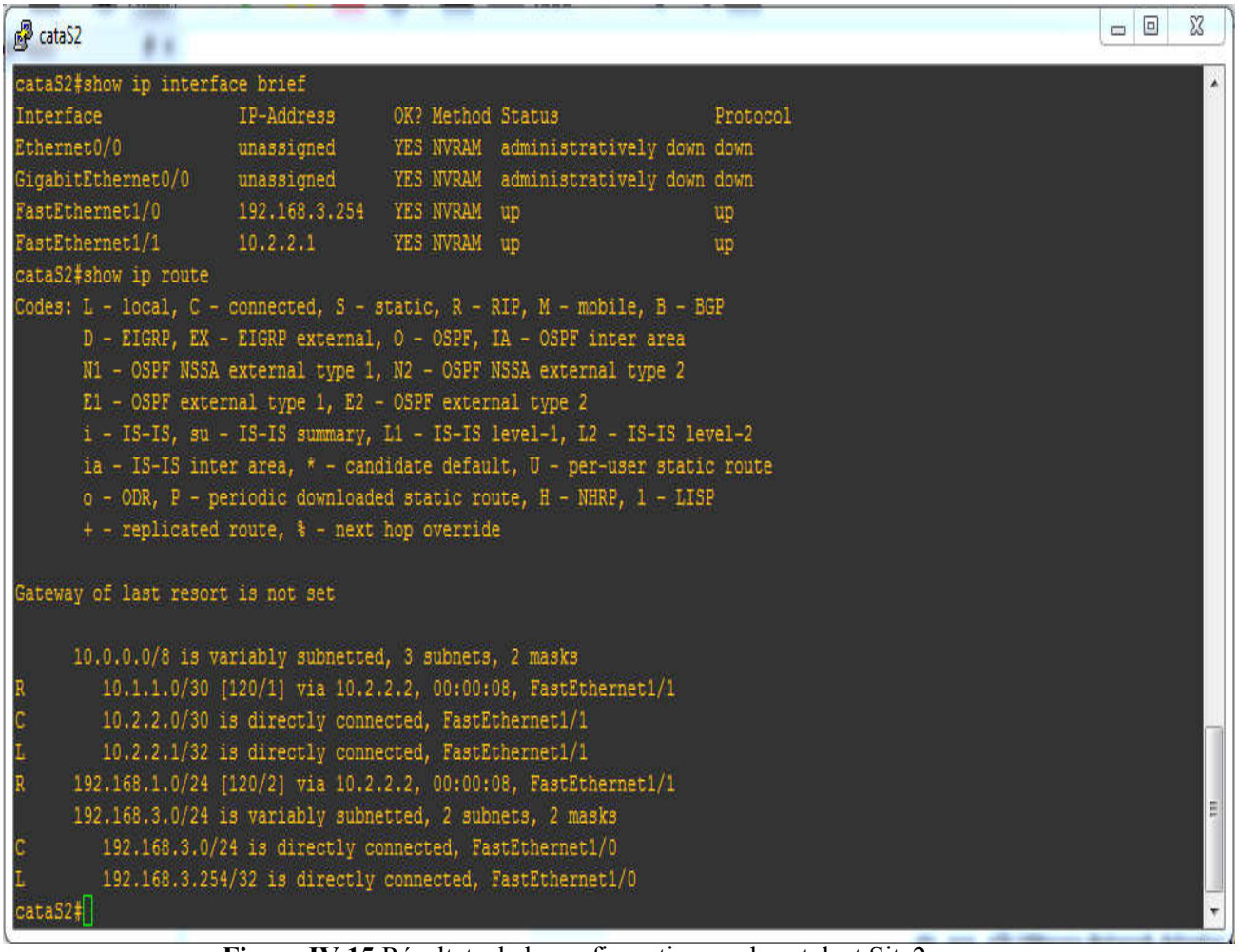

Figure IV.15 Résultats de la configuration sur le catalyst Site2

IV.5.3 Configuration des ordinateurs et serveur

Pour la configuration de notre ordinateur et le serveur, nous avons utilisés des machines virtuelles sous VMware. Nos machines seront dotées du système d'exploitation Windows XP. Ensuite des cartes réseaux des machines virtuelles et leurs adresses IP seront configurées.

Le principal objectif de VMware dans notre simulation il nous permettra de créer des machines virtuelle que nous utiliserons dans notre réseau et il va nous permettre d'essayer la connectivité du réseau et la distribution des adresses IP pour ces machines.

Dans notre topologie nous sommes limites seulement a trois machines virtuelles car la capacité des mémoires de nos machines nous a pas permit de générer trop de machine et ne

supportait pas trop de machines car nous avons rencontré des problèmes lors de la compilation des configurations.

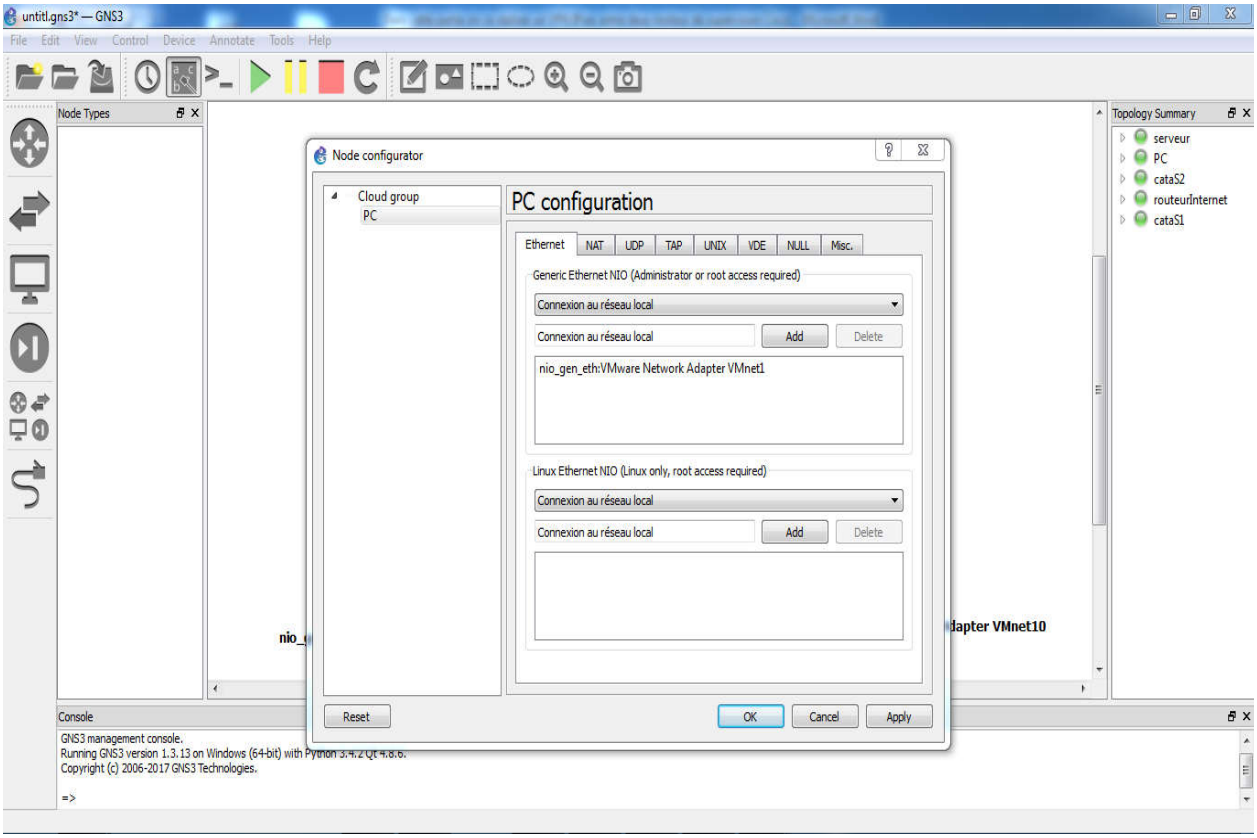

Figure IV.16instauration d'une carte réseau sur le PC

L'attribution des adresses IPs pour le serveur et le PC se fait comme suit :

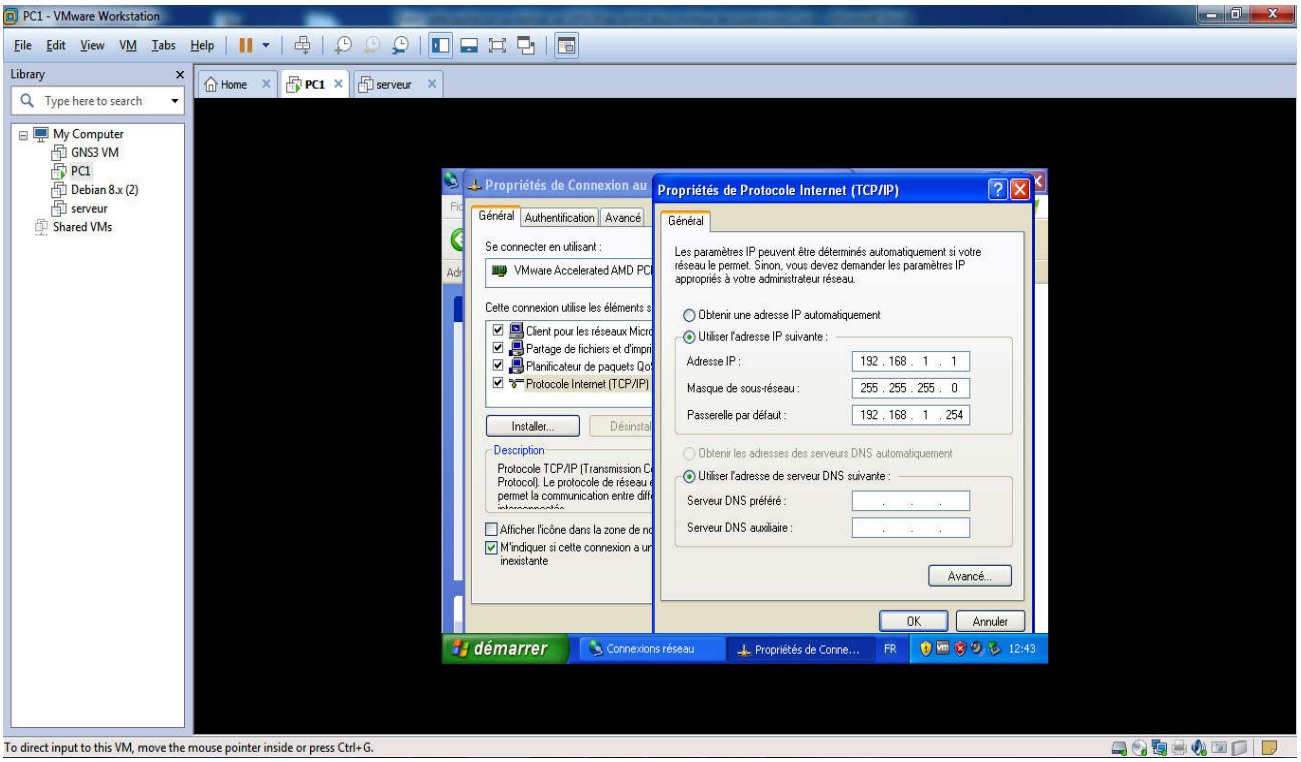

Figure IV.17 Attribution d'adresse IP au PC dans notre machine virtuelle

Pour configurer le serveur on procédera encore de la même manière que la précédente.

IV.5.4 Test de connectivite de notre architecture

Pour le test de la connectivité de notre on se servira des machines généré grâce a VMware et pour se faire nous allons pinger le serveur depuis notre PC les résultats du ping sont représente par la figure ci-dessous

```
PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=27ms TTL=125
Reply from 192.168.3.1: bytes=32 time=23ms TTL=125
Reply from 192.168.3.1: bytes=32 time=26ms TTL=125
Reply from 192.168.3.1: bytes=32 time=19ms TTL=125

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 27ms, Average = 23ms
```

Figure IV.18 Test de fonctionnement du réseau

Le test est réussi car nous constat que la totalité des paquets sont arrivés a destination du serveur donc ya une requête la configuration est réussi.

IV.5.5 Configuration du VPN (Virtual Private Network)

Pour la configuration du VPN il suffit juste de configurer le Catalyst du Site1 et celui du site2.comme le montre figure suivante

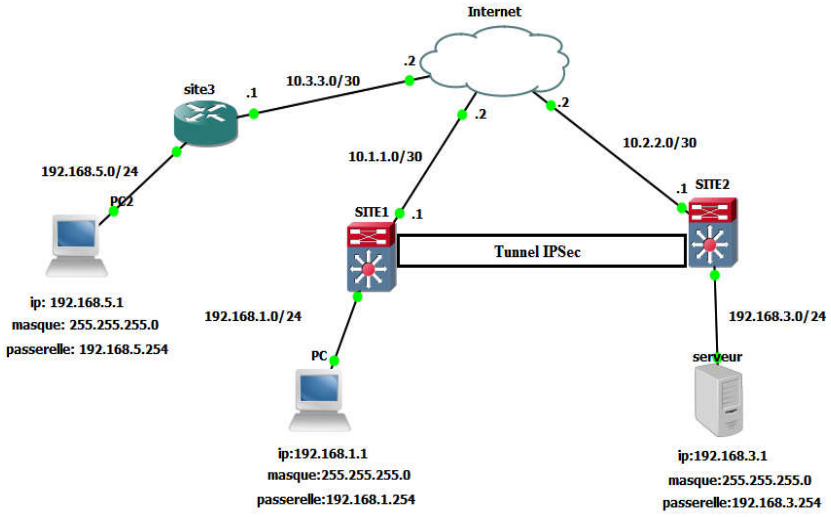

Figure IV.19 Le tunnel IPSec

Pour commencer la configuration on s'intéressera à la configuration du Catalyst du Site 2 pour ensuite procède de la même méthode pour la configuration du catalyst du Site 1et le tunnel sera configurer entre le site1 et le site2 toute en montrant les différentes étapes de la configuration.

Les étapes de configurations sont les suivantes :

1. Activer la fonction de cryptographie
2. Création de stratégie de négociation de clés et d'établissement de la liaison VPN
   - Pre-sharee (PSK)
   - aes 256 (protocole de chiffrement)
   - sha (Protocole de hachage)
   - Group 5 (deffiehelman)
   - lifetieme 3600 (durée de vie)
   - creation de clé pré-partagé
3. Création de la méthode de cryptage transform-set
   - la durée de vie de la Clé de cryptage

4. Cette étape consiste à créer une ACL qui va déterminer le trafic autorisé.
5. Dans cette dernière étape nous configurons la crypto map qui va définir le chemin qu'emprunte notre tunnel avec : la politique IPSec, la crypto ACL, le transform-set pour la politique IPSec et l'adresse IP du routeur distant avec lequel on veut communiquer.
6. Enfin nous devons appliquer la crypto map sur l'interface de sortie du catalyst de chaque site.

Les étapes de configuration seront représentées dans la figure(IV.20) et la figure (IV.21)

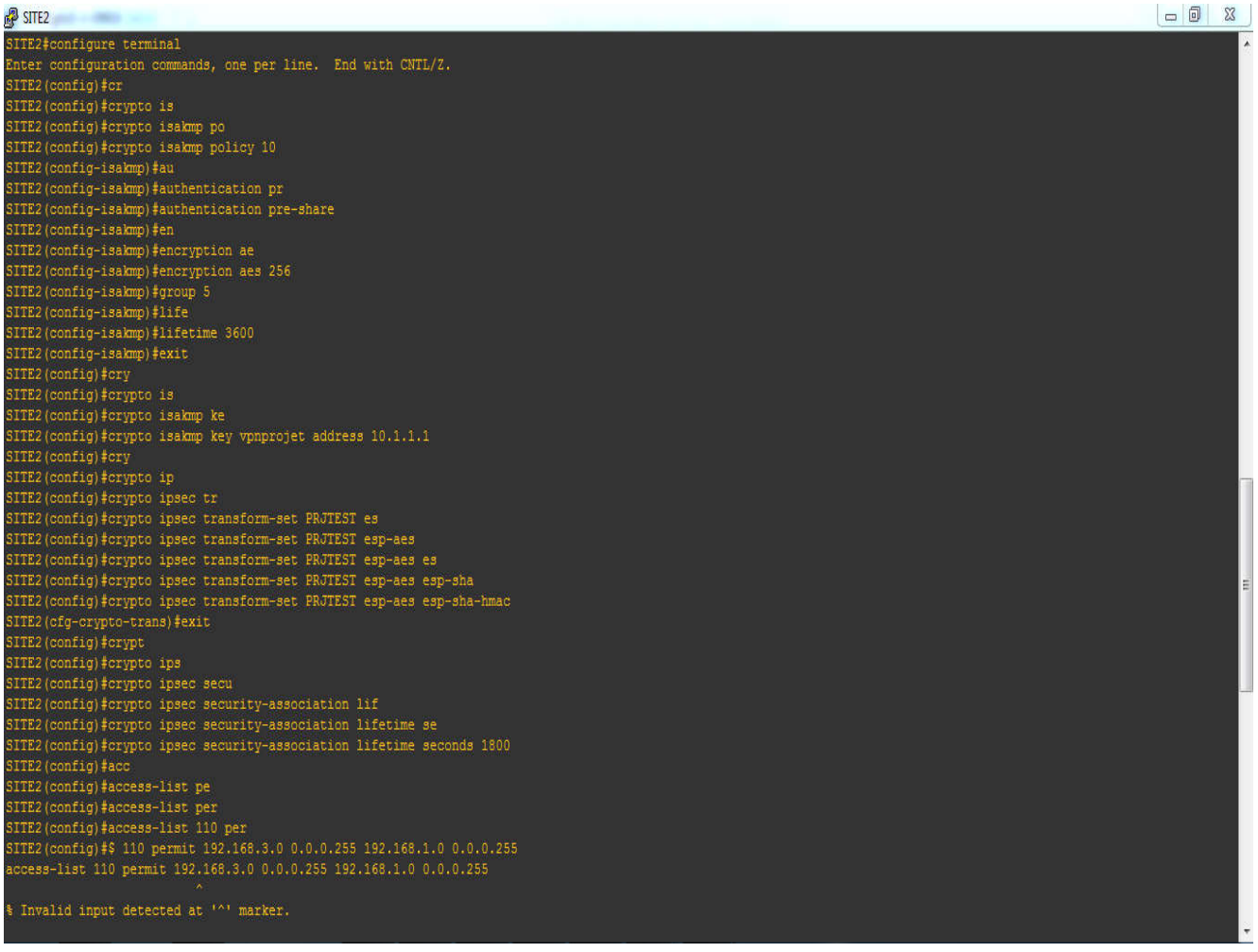

Figure IV.20 Les Étapes de configuration du VPN sur catalyst Site2 (Etapes 1)

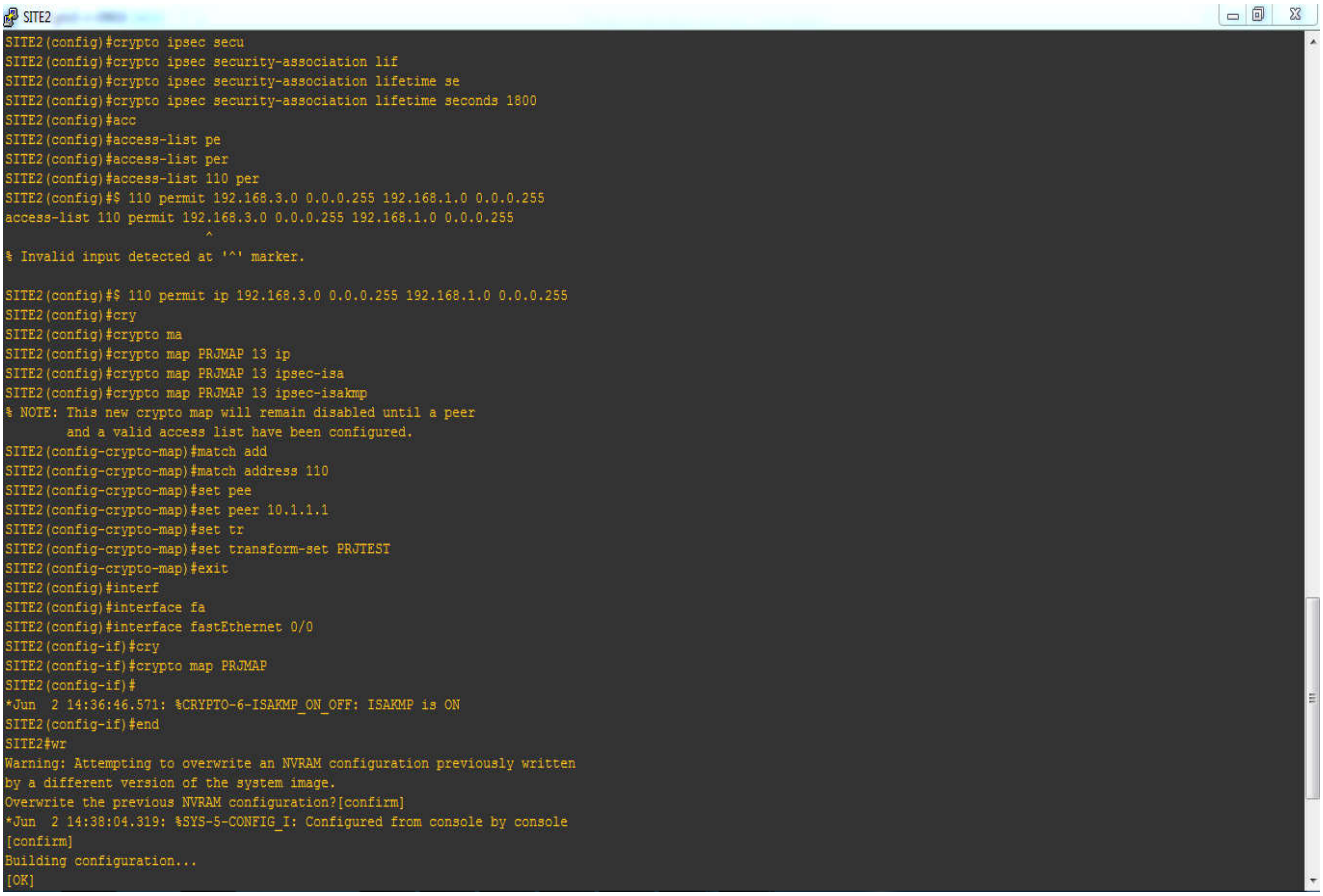

Figure IV.21 Les Étapes de configuration du VPN sur catalyst Site2 (étapes 2)

IV.5.6 Vérification des résultats

Ensuite on passera à la vérification des résultats de la configuration :

✓ vérification des informations retournées par le VPN sur le catalyst du site 2 comme le montre la figure ci-dessous

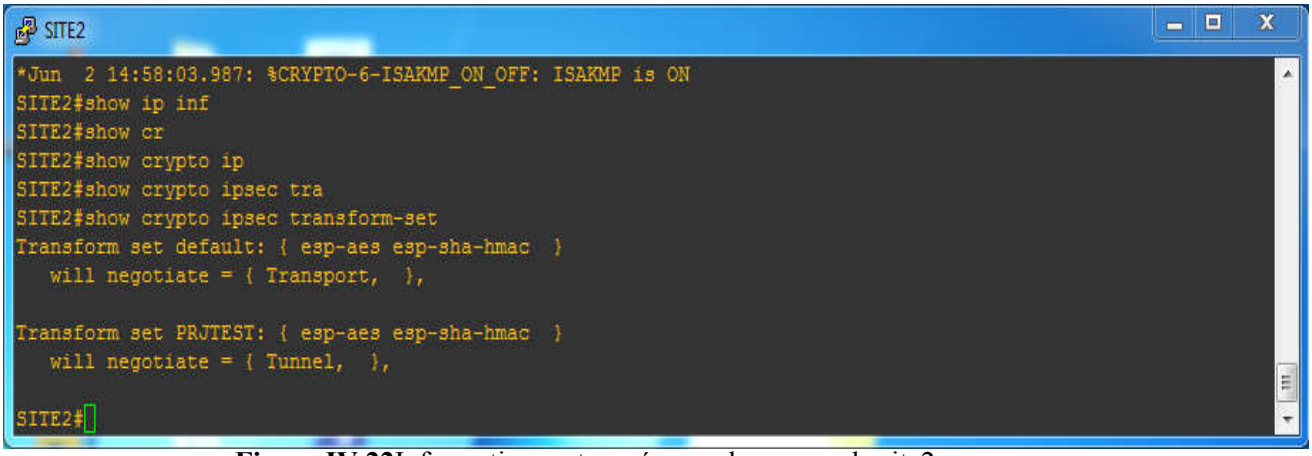

Figure IV.22 Informations retournées par le vpn sur le site2

Sur la figure (IV.22) on montre quel algorithme de hachage et de cryptage qui sont utilisé pour protéger le trafic. Dans notre cas 256 AES algorithme de cryptage et SHA algorithme de hachage ont été choisi

✓Vérification du MapVpn les résultats obtenus sont représenté par la figure ci-dessous

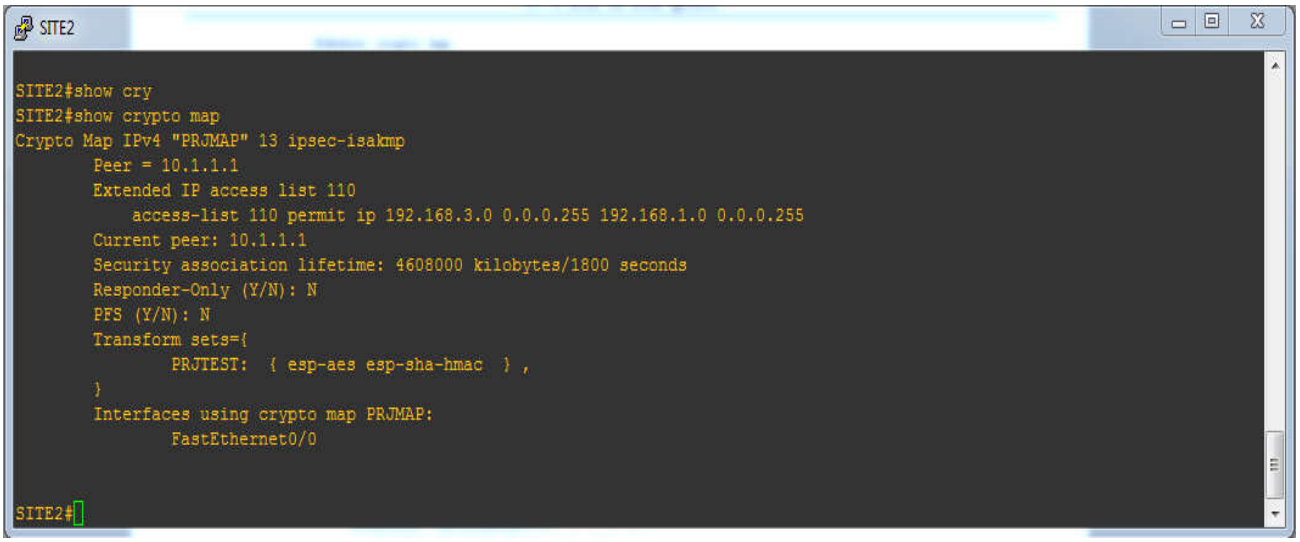

Figure IV.23 Informations du MapVpn sur le site2

Les noms de carte « PRJMAP » CRYPTO_MAP ont une entrée 110 utilisant ISAKMP pour négocier IPsec. Cette entrée de carte cryptographique devrait correspondre au trafic spécifié par la liste d'accès 110 et effectuer les paramètres définis dans le profil ISAKMP. La façon de protéger le trafic est définie dans le jeu de transformation Dans notre cas, 256AES et SHA ont été choisis. Lors de la négociation IKE, les paquets doivent être envoyés à pair 10.1.1.1. Dans ce la cas l'interface qui est activé est l'Interface 0/0

✓ Les résultats des opérations d'IPsec nous les montre la figure ci-dessous

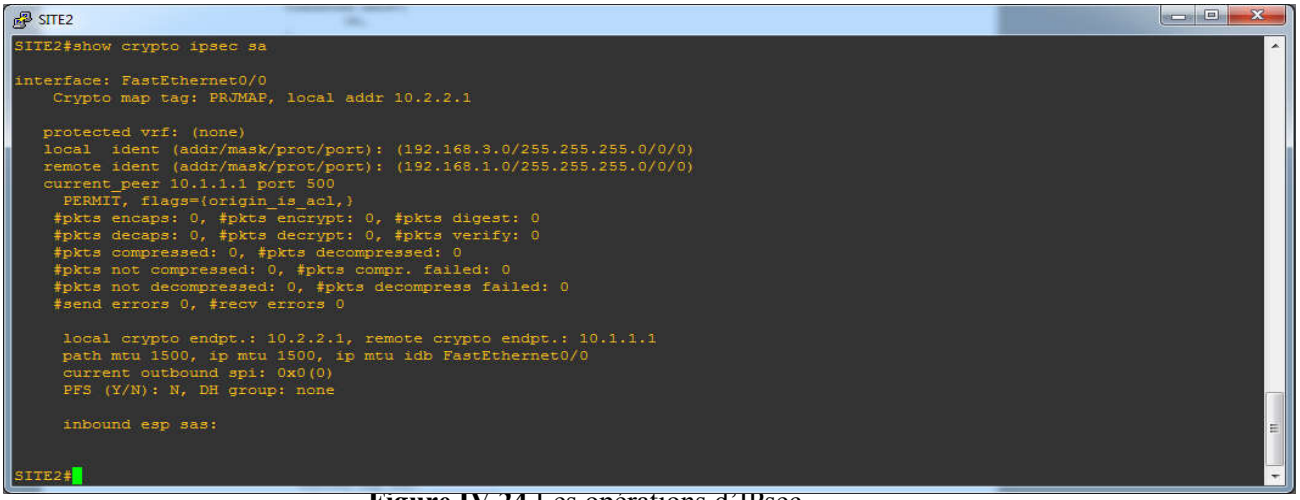

Figure IV.24 Les opérations d´IPsec

La figure ci-dessus montre le statut des SA d'IPsec et nous offre Des informations cruciales à rechercher et ce que le trafic a protégé. Dans notre cas le trafic entre le 192.168.3.0/24 réseau local (site2) vers le réseau distant (site1) 192.168.1.0/24, et l'interface distante qui est protégé 10.1.1.1.

La figure (IV.25) montre les résultats des tests sur le routeur du site 3

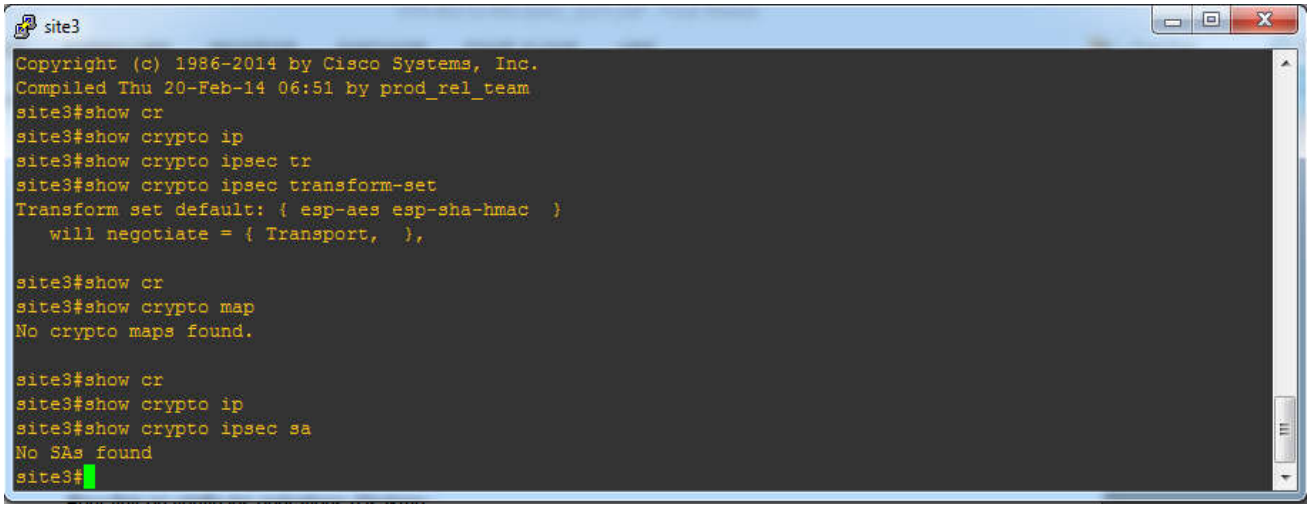

Figure IV.25 Résultats des tests sur le routeur du site3

Le tunnel IPsec n'est pas instauré dans le Routeur du site 3 et on constat d'après les résultats précédents ce dernier est instauré entre le site 1 et le site 2

IV.6 Discussion

Après toutes les configurations effectuées et ses résultats obtenus dans les deux topologies évoquées auparavant, nous pouvons dire que ce moteur de supervision a la capacité d'être utilisé comme un routeur performant mais un routeur ne pourra pas remplacer la carte de supervision. Grâce à la deuxième topologie, nous avons montrés le rôle de sécurité que peut apporter ce moteur dans un réseau. En effet, il possède plusieurs protocoles de sécurité (Vpn , ACL,…) que les routeurs n'ont pas.

Conclusion

Le réseau informatique est au cœur de l'entreprise, quelle que soit son secteur d'activité. On peut donc facilement comprendre la place que comprend un réseau au sein d'une entreprise. En effet, ce dernier doit pleinement fonctionner afin de garantir la bonne activité de l'organisme.

Dans notre projet, nous avons simulés deux réseaux contenant le moteur de supervisions Cisco « WS-sup720-3B ». A cet effet, nous avons utilisés le GNS3 afin de simuler le segment du réseau de l'université qui utilise cet équipement. Nous avons configuré les VLANs et le serveur DHCP. Cette première simulation nous a permis de comprendre les étapes de configurations ainsi que les commandes nécessaires. Nous avons montré cet équipement est utilisé dans le réseau de l'université de Tizi-Ouzou comme routeur très performant.

Dans la deuxième topologie proposée, nous nous sommes intéressés à une autre configuration utilisant un routage dynamique basé sur la création d'un tunnel VPN IPsec entre deux sites. Ainsi, nous avons montrés une nouvelle fonctionnalité de ce moteur de supervision. En effet, ce moteur de supervision ne joue pas uniquement le rôle d'un routeur mais peut être utilisé comme outil de sécurité.

Comme perspectives, il est nécessaire d'implémenter la deuxième architecture afin d'exploiter au maximum le moteur de supervision Cisco « WS-sup720-3B ».

Bibliographie

- [1] : Cédric LLORENS, Mesure de la sécurité « logique » d'un réseau d'operateur de télécommunication, thèse doctorat, Ecole National supérieur des télécommunications, Paris tech, 2005, 153 pages.
- [2] : Abdelaziz BABAKHOUYA, Sécurité de Routage, Magistère, Université A/Mira Bejaia, 2005, 91page
- [3] : Afef KOTTI-ABDLMOULAH, Etude, évaluation et amélioration des méthodes

  d'ingénierie de trafic : mise en œuvre d'une infrastructure d'établissement de LSPs supportant la différenciation de services dans les réseaux IP/MPLS, Doctorat, école supérieure des communications de Tunis, 2011,189 pages.
- [4].Céderic LLORENS, Tableaux de Bord de la sécurité réseau, (3éme édition), aout 2010
- [5]Cédric LLORENS, Tableau de bord de la sécurité réseau, 2éme Edition, Édition EYROLLES, 569 pages
- [6] Laurent BLOCH, Sécurité informatique Principes et Méthode, Édition EYROLLES, 276 pages
- [7]Document, les Listes de contrôle d'accès, Office de la Formation Professionnelle et de la Promotion du Travail, Royaume du Maroc, 2014, 14 pages
- [8] Stéphane GILL, Type d'attaques Informatique, 2013
- Nicolas BAUDOIN, NT Réseau IDS et IPS, Saint Etienne, 2003

Site Web:

- https://www.securiteinfo.com/attaques/hacking/typesattaques.shtml
- https://www.securiteinfo.com/conseils/introsecu.shtml
- http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper09186a00800c8441.html
- Cisco support community, Understanding MSFC, PFC and DFC roles in Catalyst 6500 Series Switch
- Wikipedia
- http://www.memoireonline.com/03/17/9694/m_Implantation-dun-systeme-de-gestion-des-utilisateurs-et-monitoring-des-taches-dans-un-reseau-d32.html
- http://wawadeb.crdp.ac-caen.fr/iso/tmp/ressources/ssh/ssh.php3.html
- http://www.axn-informatique.com/moteur-de-recherche.html
- Cisco Catalyst 6500/Cisco 7600 Series Supervisor Engine 720 Data Sheet
- CISCO CATALYST 6500 SERIES SUPERVISOR ENGINE 720, Data-sheet