République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique
Université **A**. **M**ira de **B**éjaia
Faculté de **T**echnologie
Département de **G**énie **E**lectrique

Mémoire de fin de cycle

En vue de l'obtention du Diplôme de master électronique

Option : Télécommunication

Thème :

Sécurité du réseau GSM-1800 avec IPSEC

Réalisé par :

M^elle^ BENAMARA Megdouda

Promoteur :

M^r^ KHIREDDINE A/K

2011-2012

Remerciements

*Je tiens à remercier **DIEU** qui m'a accordé la santé, la possibilité ainsi que la volonté d'entamer et de continuer mes études.*

*Je remercie profondément mon promoteur, **Mr Khireddine** pour le soutien et l'aide qu'il m'a présenté pour la réalisation de ce document.*

Je remercie également l'ensemble de jury d'avoir accepter d'examiner et d'évaluer mon travail.

*Mes remerciements s'adressent à tous le personnel de l'entreprise **MOBILIS**, pour l'accueil, l'aide, et conseils qui m'ont apportés tout au long de mon stage.*

Mes remerciements vont plus particulièrement à ma famille et à mes amis qui ont su me soutenir et m'encourager tout au long de mes études.

Dédicace

A la mémoire de « yemma azizou »

A mes grands-mères « yaya djoudjou » et « yemma el-djida »

A mes très chers parents

A mes sœurs

A mes frères

A toute la famille BENAMARA

A mes copines de chambre

A mes amis en particulier Mounira

A toute la promotion télécom 2011/2012

A toute personne chère à mes yeux

Table de matière

Table des figures

Liste des tableaux

Liste des abréviations

ACL : Acces Contrôle List

AH : Authentication Header

AuC : Authentification Center

BSC : Base Station Controler

BSS : Base Station Subsystem

BTS : Base Transceiver Station

CEPT : Conférence Européenne des administrations des Postes et Télécommunications

CEPT : Conférence Européenne des administrations des Postes et Télécommunication

DCN :Data Communication Network

EIR : Equipement Identification Register

ESP : Encapsulating Security Payload

FTP : File Transfert Protocol

GSM :Global System for Mobile communications

HLR : Home Location Register

IMSI : International Mobile Subscriber Identity

IOS : Inter network Operating System

IP : Internet Protocol

IPSec : Intenet Protocol Security

L2TP : Layer 2 Tunneling Protocol

LAN : local area network

M S : Mobile Station

MAC : Medium Access Control

MSC : Mobile-services Switching Center

MSISDN : Mobile Subscriber Integrated Services Digital Network

NSS : Network Switching Subsystem

NVRam : Non Volatile Random Access Memory

PPTP : Point to Point Tunneling Protocol

ROM : Read Only Memory

SA : Security Association

SMS : Short Message Service

SMTP : Simple Mail Transport protocol

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

VLR : Visitor Location Register

VPN : Virtual Private Network

WAN : Wide Area Network

Les réseaux de télécommunications ont pris un essor important dans le monde. Aujourd'hui, ce sont des systèmes que nous utilisons quotidiennement (utilisation de la téléphonie par exemple). Les besoins se multiplient, la complexité de ces systèmes augmente. On demande aux réseaux de télécommunications d'être efficaces, robustes, surs et toujours disponibles.

Durant ces dernières années, les réseaux radio mobiles ont eu une expansion sans précédent en termes de capacité et en nombre d'abonnés. La norme GSM, Global System for Mobile communication, représente de nos jours le système de télécommunications mobile le plus étendu et le plus répandu à travers le monde.

Dans notre pays (Algérie), la norme de téléphonie mobile utilisée est le GSM 1800-1900 et ses services sont offert aux usagers via trois grands opérateurs soient MOBILIS, NEDJMA et DJEZZY. La gestion du réseau des BSC (monitoring, alarmes) de chacun d'eux est rendue possible par le réseau DCN (data communication network), qui n'est autre qu'un réseau de routeurs (donc réseau informatique) reliés entre eux par des liens de transmission de type E1 assurant la communication et l'échange d'informations entre les différents BSC.

Les réseaux informatiques sont devenus indispensables à la bonne marche des entreprises. La croissance accélérée de ces réseaux qui sont aujourd'hui de plus en plus ouverts sur Internet, pose néanmoins un problème majeur : il en découle un nombre croissant d'attaques qui peuvent aboutir à de graves conséquences professionnelles en menaçant l'intégrité, la confidentialité et la disponibilité de l'information.

Avec l'intégration des réseaux DCN entre les stations BSC afin d'assurer la gestion de ces dernières, les exigences en terme de sécurité deviennent de plus en plus indispensable pour le réseau GSM, et ne peut se limiter à la sécurisation de l'interface radio Um. Pour cela, nous aborderons une nouvelle technologie de sécurisation des réseaux informatique qui est le VPN.

Le VPN (Virtuel Private Network), est une liaison sécurisée entre deux sites d'une organisation via un réseau public. Il permet d'envoyer et de partager des données entre des sites distants grâce à un principe de tunneling dont chaque extrémité est identifiée ; les données transitent après avoir été chiffrées. C'est la méthode utilisée pour faire transiter des informations privées sur un réseau public. Cette technique assure donc l'authentification des deux parties, l'intégrité des données et le chiffrement de celles-ci.

Pour se communiquer au travers du VPN, plusieurs protocoles peuvent être utilisés [1]: le PPTP (point to point tunneling protocol), le protocole L2TP (layer 2 tunneling protocol) et enfin le protocole IPSEC que nous allons utiliser.

Etant donné que la plupart des entreprises déploient des équipements réseaux de marque CISCO, les routeurs de cette marque ont été la cible de plusieurs attaques basées sur l'exploitation frauduleuse des protocoles réseaux, ainsi que les failles liées à leurs configurations.

L'utilisation matérielle des VPN consiste à déléguer le tunneling au matériel mis en place en sortie d'entreprise, à savoir les routeurs qui sont des équipements d'interconnexion de réseaux informatiques permettant d'assurer le routage d'informations entre deux réseaux et de déterminer le chemin qu'un paquet de données va emprunter.

L'objectif de ce travail est de répondre à l'ensemble des besoins de sécurité des stations de commande BSC de GSM (cas Mobilis) du fait que ces équipements sont interconnectés à travers les routeurs du réseau DCN. Pour cela, nous allons proposer une solution de sécurisation de l'interface en utilisant le tunneling IPSEC entre les routeurs de type CISCO.

Ce mémoire est devisé en deux grandes parties :

La première partie examine d'un point de vue théorique, les concepts mis en œuvre.

- ✓ Le premier chapitre constitue une introduction au réseau GSM, on exposant son architecture physique, sa gestion ainsi que sa sécurité.
- ✓ Le second chapitre qui est le cœur du projet, traite les technologies de sécurité des réseaux : la cryptographie et le VPN ainsi que la solution IPSEC mis en place sur le marché afin de mieux sécuriser les réseaux d'entreprise.

- ✓ Le troisième chapitre parlera sur les routeurs et le routage dans les réseaux.

La seconde partie est consacrée à l'implémentation d'une solution de sécurisation du réseau GSM en configurant un tunnel VPN IPSEC entre les routeurs de deux BSC.

En fin, notre mémoire, s'achèvera par une conclusion générale résumant les grands points qui sont présentés dans ce mémoire ainsi qu'une annexe.

I.1 Introduction

Le réseau GSM (Global System for Mobile communications) constitue au début du 21ème siècle le standard de téléphonie mobile le plus utilisé. Il s'agit d'un standard de téléphonie dit de seconde génération.

L'énorme succès qu'elle a connue cette génération des réseaux de télécommunication revient au fait qu'elle répondait aux besoins des usagers dont on peut citer la mobilité des services, la voix, l'itinérance et la messagerie.

Dans un réseau GSM, le territoire est découpé en petites zones appelées cellules [2]. Chaque cellule est équipée d'une station de base fixe munie de ses antennes installées sur un point haut.

Ce chapitre propose une vue d'ensemble du réseau GSM, son architecture, sa gestion ainsi que sa sécurité.

I.2 historique

L'histoire de la téléphonie mobile (numérique) débute réellement en 1982. En effet, à cette date, le Groupe Spécial Mobile, appelé GSM, est créé par la Conférence Européenne des administrations des Postes et Télécommunications (CEPT) afin d'élaborer les normes de communications mobiles pour l'Europe dans la bande de fréquences de 890 à 915 [MHz] pour l'émission à partir des stations mobiles et 935 à 960 [MHZ] pour l'émission à partir de stations fixes [3]. Il y eut bien des systèmes de mobilophonie analogique (MOB1 et MOB2, arrêté en 1999), mais le succès de ce réseau ne fut pas au rendez-vous.

Les années 80 voient le développement du numérique tant au niveau de la transmission qu'au niveau du traitement des signaux. Ainsi, en 1987, le groupe GSM fixe les choix technologiques relatifs à l'usage des télécommunications mobiles : transmission numérique, multiplexage temporel des canaux radio, chiffrement des informations ainsi qu'un nouveau codage de la parole. Il faut attendre 1991 pour que la première communication expérimentale par GSM ait lieu. Au passage, le sigle GSM change de signification et devient Global System for Mobile communications et les spécifications sont adaptées pour des systèmes fonctionnant dans la bande des 1800 [MHz].

I.3 Différences entre le GSM 900 et le GSM1800

Les spécifications de la norme GSM 1800 sont similaires à celles du GSM 900 pour bien des aspects [4]. Il y a principalement quatre domaines où les différences sont évidentes.

I.3.1 Fréquences radio

- GSM 900 : 890-915 MHz (montant) et 935-960 MHz (descendant) ;
- GSM 1800 : 1710-1785 MHz (montant) et 1805-1880 MHz (descendant).

I.3.2 Classes de mobiles

La norme GSM 1800 cherche à faciliter la mise sur le marché de terminaux portatifs de très faible encombrement, ce qui a conduit à des puissances d'émission crête différentes :

- GSM 900 : 5 classes de terminaux, de 800 mW à 20 W ;
- GSM 1800 : 2 classes de terminaux, 250 mW (classe 2) et 1 W (classe 1).

I.3.3 Taille des cellules

- GSM 900 : de 1 km (environ) à 35 km ;
- GSM 1800 : jusqu'à 8 km.

Le tableau I.1 illustre la différence entre les trois catégories de GSM.

	GSM 900	GSM 1800	GSM 1900
Fréquence d'émission du terminale vers la station de base	890-915MHZ	1710-1785MHZ	1850-1910MHZ
Fréquence d'émission de la station de base vers le terminal	935-960MHZ	1805-1880MHZ	1930-1990MHZ
Bande de fréquence disponible	25+25MHz	75+75MHz	60+60MHz
Mode d'accès	AMRT/AMRF	AMRT/AMRF	AMRT/AMRF
Espacement des canaux radio	200 KHZ	200 KHZ	200 KHZ
Espacement du duplex	45MHz	95MHz	80MHz
Nombre de canaux par sens	124	375	300
Nombre de canaux de parole plein débit	8	8	8
Type de transmission	numérique	numérique	numérique
Débit brut d'un canal radio	270 KBIT/S	270Kbit/s	270Kbit /s
Débit brut d'un canal de phonie à plein débit	22.8Kbit/s	22.8Kbit/s	22.8Kbit/s
Débit d'un codec à plein débit	13Kbit/s	13Kbit/s	13Kbit/s
Type de codage	RTE/LTP	RTE/LTP	RTE/LTP
Type de modulation	GMSK	GMSK	GMSK

Tableau I.1 : Fréquences du GSM

I.4 Architecture du réseau GSM

L'architecture du réseau GSM peut être divisée en trois sous-systèmes [5] :

- Le sous système radio
- Le sous système réseau
- Le centre d'opération et de maintenance

Les éléments de l'architecture d'un réseau GSM sont repris sur le schéma de la figure I.1.

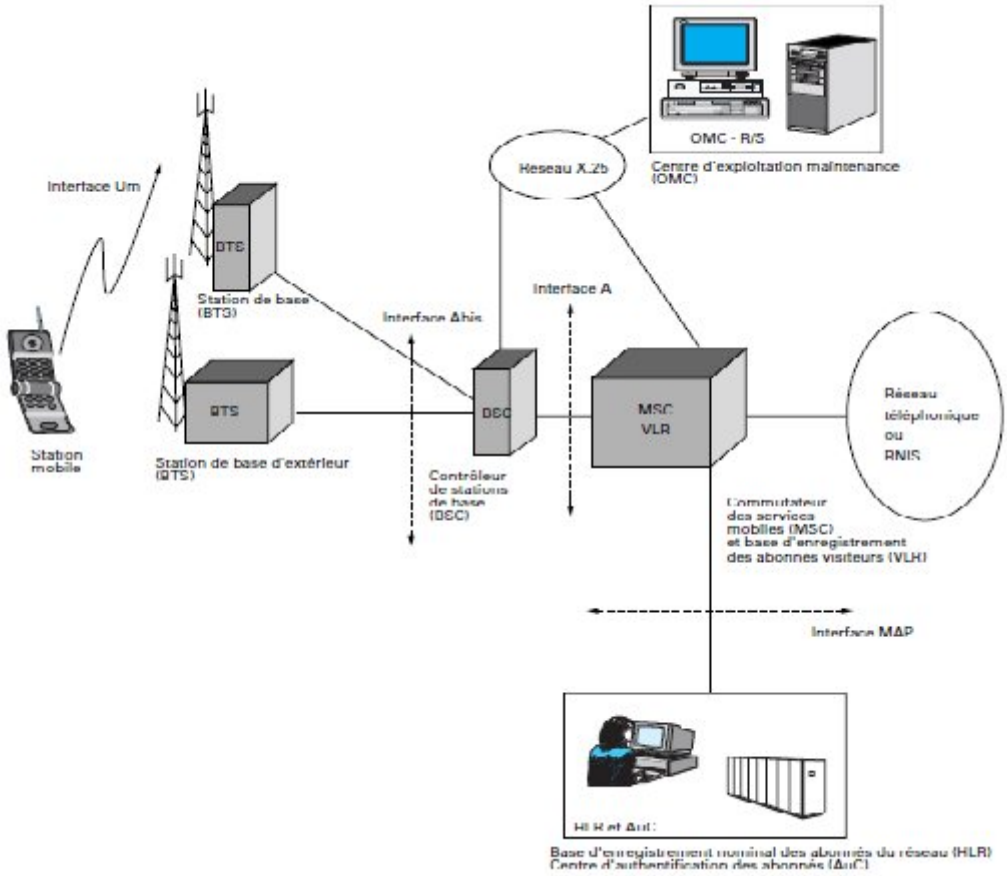


Figure I.1 : Architecture de réseau GSM

I.4.1. Sous système radio

Il est composé de deux entités MS et BSS [6]:

a. L'équipement MS

C'est le terminal utilisé par un abonné de réseau ; chaque abonné possède un téléphone portable et une carte SIM d'identification sur le réseau. Ces derniers sont les deux seuls éléments auxquels un utilisateur a directement accès, ils sont suffisent pour réaliser l'ensemble des fonctionnalités nécessaires à la transmission et à la gestion des déplacements (Tableau I.2).

paramètres	commentaires
Données administratives	
PIN/PIN2	Mot de passe demandé à chaque connexion
PUK/PUK2	Code pour débloquer une carte
langage	Langue choisie par l'utilisateur
Données liée à la sécurité	
Clé Ki	Valeur unique, connue de la seule carte SIM et du HLR
CKSN	Séquence de chiffrement
Données relatives à l'utilisateur	
IMSI	Numéro international de l'abonné
MSISDN	Numéro d'appel d'un téléphone GSM
Données de roaming	
TMSI	Numéro attribué temporairement par le réseau à un abonné
Location updating status	Indiquer si une mise à jour de la localisation est nécessaire
Données relatives au réseau	
Mobile Cuntry Code (MCC), Mobile Network Code (MNC)	Identifiant du réseau mobile de l'abonné
Numéro de fréquence absolue	Fréquences utilisées par PLMN

Tableau I.2 : Liste partielle des informations contenues dans une carte SIM

b. Le sous système radio BSS (Base Station Subsystem)

Le BSS est un ensemble regroupant le BSC et les BTS qui lui sont associés. Il assure :

- ✓ la gestion du canal radio, c'est à dire la configuration des canaux,
- ✓ l'affectation de ces canaux,
- ✓ la supervision de la communication,
- ✓ le timing des messages,
- ✓ le contrôle de la puissance,
- ✓ les sauts de fréquence,
- ✓ le codage du canal,
- ✓ le transcodage de la parole,
- ✓ le handover entre BTS,
- ✓ le processus d'émissions discontinues.

- **La station de Base (BTS)**

La BTS est un ensemble d'émetteurs-récepteurs appelés TRX. Elle a la charge de :

- ✓ la transmission radio : modulation, démodulation, égalisation, codage correcteur d'erreur.
- ✓ La gestion de la couche physique : multiplexage TDMA, saut de fréquence lent, chiffrement.
- ✓ La réalisation de l'ensemble des mesures radio nécessaires pour vérifier qu'une communication en cours se déroule correctement.

Ces mesures ne sont pas exploitées par la BTS mais directement transmises au BSC.

- **La Station de commande BSC**

Le contrôleur de stations de base BSC administre un ensemble de stations de base BTS, il a pour rôle :

- ✓ la gestion du trafic des BTS.
- ✓ Il assure l'allocation de canaux,
- ✓ la gestion du saut de fréquence,
- ✓ le transfert intercellulaire des communications,
- ✓ la gestion de la signalisation sur voie radio.
- ✓ Il assure aussi des fonctions de liaison avec le centre d'exploitation et de maintenance.

I.4.2 Le NSS (Network Switching Subsystem)

Le sous-système réseau NSS prend en charge les fonctions de commutation et de routage. Il est composé des éléments suivants [7] :

a. MSC (Mobile-services Switching Center)

C'est le centre de commutation des appels mobiles (routage des communications). Il gère les procédures de contrôle d'appel ainsi que les procédures de gestion de la mobilité des abonnés (avec le VLR).

b. HLR (Home Location Register)

Le HLR est la base de données centrale contenant toutes les informations administratives relatives aux abonnés d'un réseau donné utilisant deux clés d'entrée :

✓ **IMSI (International Mobile Subscriber Identity)**

C'est un numéro unique alloué à chaque abonné stocké dans la carte SIM et utilisé par le réseau pour la transmission des données de l'abonné.

✓ **MSISDN (Mobile Subscriber Integrated Services Digital Network)**

C'est le numéro d'appel de l'abonné lié à l'IMSI dans le HLR; les appels destinés à l'abonné sont transcrits en numéro d'IMSI ce qui permet sa recherche et l'établissement de la communication.

c. VLR (Visitor Location Register)

Le VLR est une base de données où sont stockées les informations relatives à une région particulière (zone de travail du MSC). Nous y trouvons les mêmes informations que dans le HLR avec en plus l'identité temporaire de l'utilisateur TMSI (Temporary Mobile Subscriber Identity) et sa zone de localisation (ensemble de cellules où se trouve l'abonné).

d. AuC (Authentification Center)

L'AUC est une base de données protégée qui contient une copie de la clé secrète inscrite sur la SIM de chaque abonné. Cette clé est utilisée pour vérifier l'authenticité de l'abonné et pour le cryptage des données envoyées.

e. **L'équipement EIR (Equipement Identification Register)**

L'EIR est une base de données annexe contenant les identités des terminaux (IMEI). Elle peut être consultée lors des demandes de services d'un abonné pour vérifier si un équipement mobile (ME) a ou n'a pas le droit d'accès au système.

I.4.3 Sous Système d'Exploitation et de Maintenance

Ce sous système est composé généralement d'un sous système d'exploitation et de maintenance du BSS, appelé OMC-R et d'un sous système d'exploitation et de maintenance du NSS, appelé OMC-NSS [7] :

a. L'OMC-R

Assure les fonctions d'exploitation et de gestion du BSS, à savoir :

- la gestion des cellules,
- l'affichage des performances du BSS,
- la visualisation des alarmes.

L'OMC-R permet également le paramétrage et l'intégration des nouveaux équipements dans le BSS (déclaration des nouvelles cellules, nouveaux BSC…).

b. **L'OMC-NSS**

Permet la centralisation de l'exploitation technique du sous système réseau. Parmi les principales fonctions de l'OMC–NSS est la visualisation des états de différents organes (software et hardware) composant le sous système réseau.

I.5 Les interfaces d'un système GSM

Les interfaces assurent le dialogue entre les équipements de GSM et permettent leur interfonctionnement comme indique la figure I.2 [8].

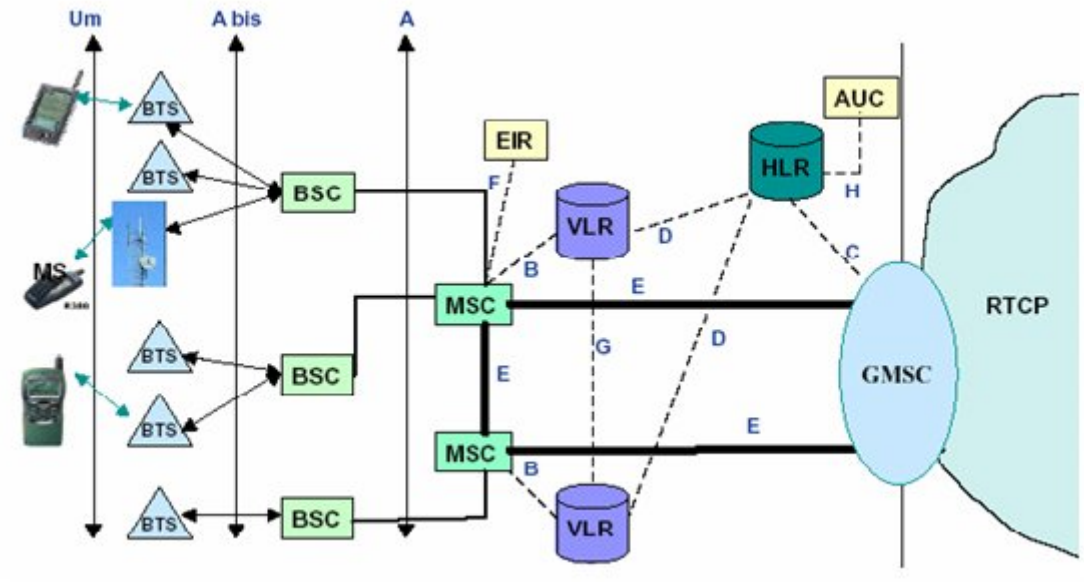


Figure I.2 : Interfaces de GSM

- L'interface Um : C'est l'interface entre les deux entités : le MS (Mobile Station) et le BSS (Base Station Sub-system. On la nomme couramment interface radio ou interface air.
- L'interface Abis : C'est l'interface entre les deux composants du BSS : la BTS (Base Station Transceiver) et le BSC (Base Station Controler).
- L'interface A : C'est l'interface entre les deux sous systèmes BSS (Base Station Sub System) et le NSS (Network Sub System).
- L'interface B relie le MSC et le VLR, elle est utilisée pour l'Échange d'informations usager et mise à jour de zone de localisation. Cette interface est non normalise car les fonctions du MSC et VLR sont souvent intégrées dans un seul équipement.
- L'interface C relie le GMSC et le HLR : Interrogation du HLR pour joindre un abonné mobile.
- L'interface D relie le VLR et le HLR : Le VLR informe le HLR de la localisation du mobile. Le HLR fournit au VLR les informations relatives à l'abonné.
- L'interface E relie entre deux MSC, pour la gestion de handover, et relie le MSC et GMSC pour le transport des SMS.
- L'interface F relie le MSC et le EIR, pour la Vérification de l'identité du terminal.
- L'interface G relie deux VLR : Gestion du changement de zone de localisation.
- L'interface X25 relie le BSC-OMC et le MSC-OMC.

I.6 Gestion du réseau

La gestion d'un système englobe l'ensemble des moyens mis en œuvre pour offrir aux utilisateurs un service de qualité et permettre l'évolution du système en incluant de nouvelles fonctionnalités. Elle vise à optimiser les performances des services pour les utilisateurs et à permettre une utilisation maximale des ressources à un cout minimal.

La gestion de réseau consiste donc à résoudre un ensemble de problèmes fondés sur des ressources communes. Nous présentons une séparation des problèmes selon leur nature par l'utilisation de cinq modèles conceptuels (voir figure I.3) [8].

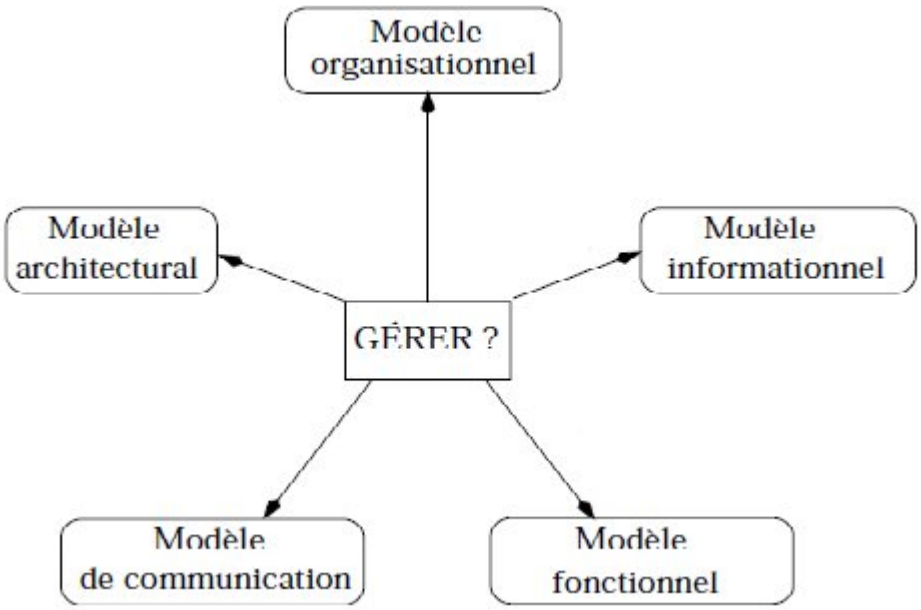


Figure I.3 : Les cinq modèles conceptuels de la gestion de réseau.

Chaque modèle répond à une question sur la gestion.

- ✓ Le modèle informationnel sert à l'identification et à la représentation des éléments à gérer.
- ✓ Le modèle architectural et le modèle de communication décrivent la structure des entités gérées ainsi que la façon dont les outils de gestion peuvent interagir avec ces entités.

L'institut de normalisation UIT-T a élaboré le concept de réseaux de gestion des télécommunications (TMN) (Télécommunication Management Network) pour définir une architecture fonctionnelle d'un système de gestion de réseau souple, complet et évolutif.

La figure I.4 montre l'architecture du TMN.

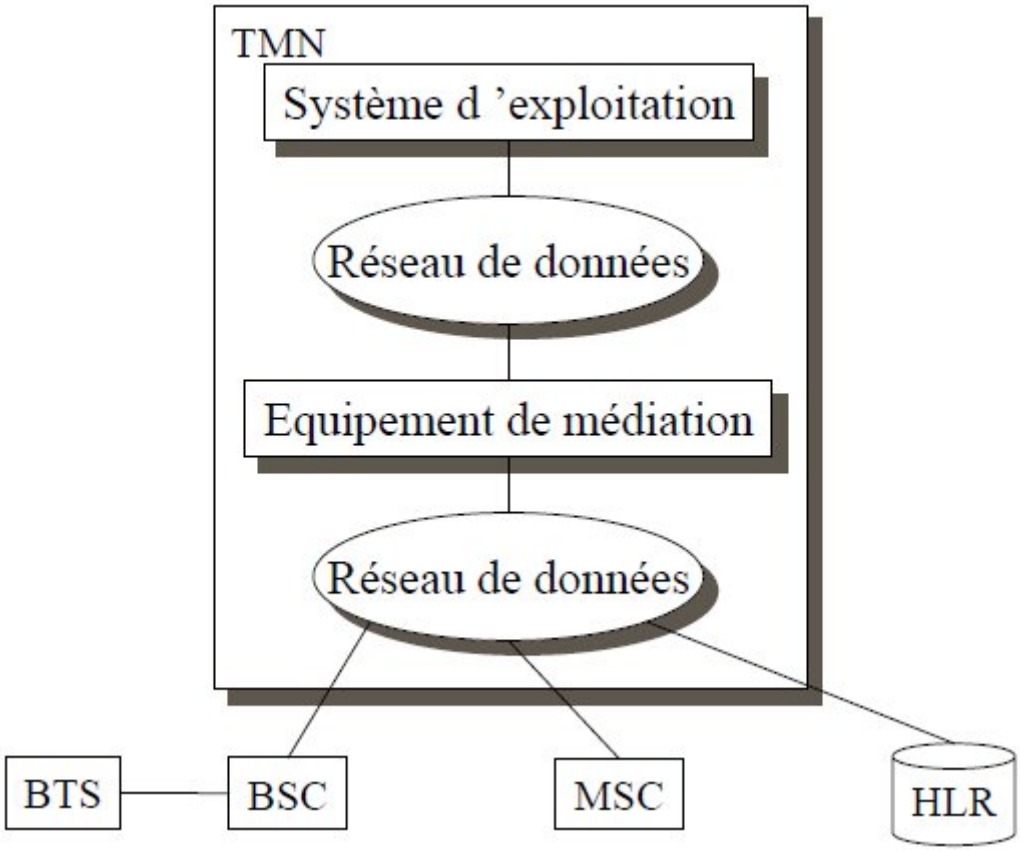


Figure I.4 : Architecture du TMN

Le TMN se compose de [10]:

- l'élément de réseau (NE pour Network Element), il se compose d'un équipement de télécommunications (un groupe ou une partie) et d'un équipement de support exécutant des fonctions de gestion mais considéré comme faisant partie du réseau de télécommunications ;

- le réseau de transmission de données (DCN pour Data Communication Network), il s'agit d'un réseau de communication pour les échanges d'information de gestion entre les éléments de TMN (BSC, MSC, HLR).
- le système de gestion (OS pour Operation System), c'est un centre d'administration qui offre des applications de gestion ;
- la station de travail (WS pour Work Station), elle assure la communication entre l'opérateur humain et les composants du réseau.

✓ Le modèle fonctionnel définit les différentes taches à effectuer par la gestion

✓ le modèle organisationnel décrit les participants de cette gestion et la façon dont leur sont affectées les différentes fonctions de la gestion.

I.7 Sécurité du réseau GSM

Dans le cas du réseau GSM, lors de la transmission radio au travers l'interface Um, deux principaux problèmes peuvent être posé [11]:

✓ Écoute des communications

✓ Accès frauduleux par des mobiles pirates en utilisant des données d'abonnés existantes.

Pour cela, le réseau GSM se manifeste donc par les éléments de sécurité suivants [12]:

✓ Confidentialité de l'identifiant personnel IMSI de l'abonné par utilisation d'un autre identifiant ;

✓ Cryptage(ou chiffrement) des communications ;

✓ Authentification de chaque abonné avant tout accès à un service .

a. Confidentialité de l'identifiant

➢ **I.M.S.I**

Numéro (identité) d'abonné se trouvant dans la SIM d'une part et dans le HLR d'autre part (logique). IMSI n'est connu qu'a l'intérieur du réseau GSM et doit (autant que possible) resté secrète (d'ou l'utilisation de TMSI).

- **L'identifiant T.M.S.I**

C'est l'identifiant temporaire codé sur 4 Octets modifié a chaque changement de zone (gérer par un VLR) [13]. Le TMSI est utilisé pour identifier le mobile appelé ou appelant lors de l'établissement d'une communication. L'IMSI est transmis à la mise sous tension du mobile.

Une fois l'IMSI transmis, les TMSI successives du mobile seront transmises. Ce n'est qu'en cas de perte du TMSI ou lorsque le VLR courant ne la reconnaît pas (par exemple après une panne) que l'IMSI peut être retransmise. En cas d'échec lors de la vérification d'un de ces identifiants, on interdit l'accès aux services.

L'allocation d'une nouvelle TMSI est faite au minimum à chaque changement de VLR, et suivant le choix de l'opérateur, à chaque intervention du mobile. Son envoi à la station mobile a lieu en mode chiffré (figure I.5).

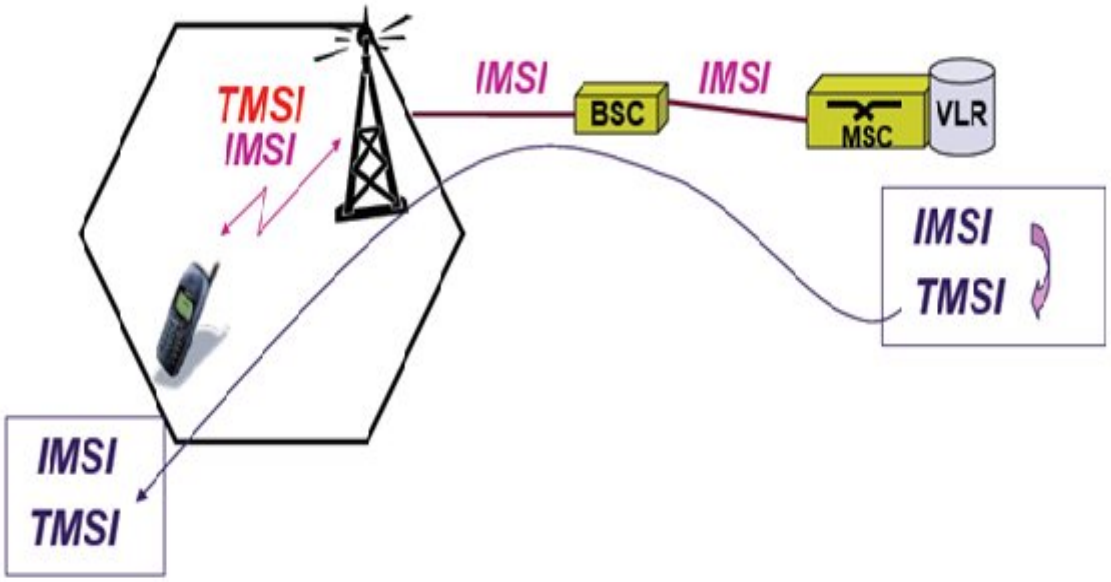


Figure I.5: Procédé de confidentialité de l'IMSI

b. Chiffrement et authentification

Le chiffrement GSM sur la voie radio (interface Um):

Pour assurer la confidentialité de leurs abonnés, les opérateurs ont recours aux éléments suivant (figure I.6):

- ✓ Nombres aléatoire (RAND())
- ✓ une clé appelée Ki pour l'authentification et la création d'une seconde clé Kc (la clé Ki, stockée dans la carte SIM et dans l'AUC coté réseaux, est attribuée lors de l'abonnement avec l'IMSI)
- ✓ un algorithme A3 fournissant le nombre SRES à partir des arguments de RAND et de la clé Ki (construction SRES)

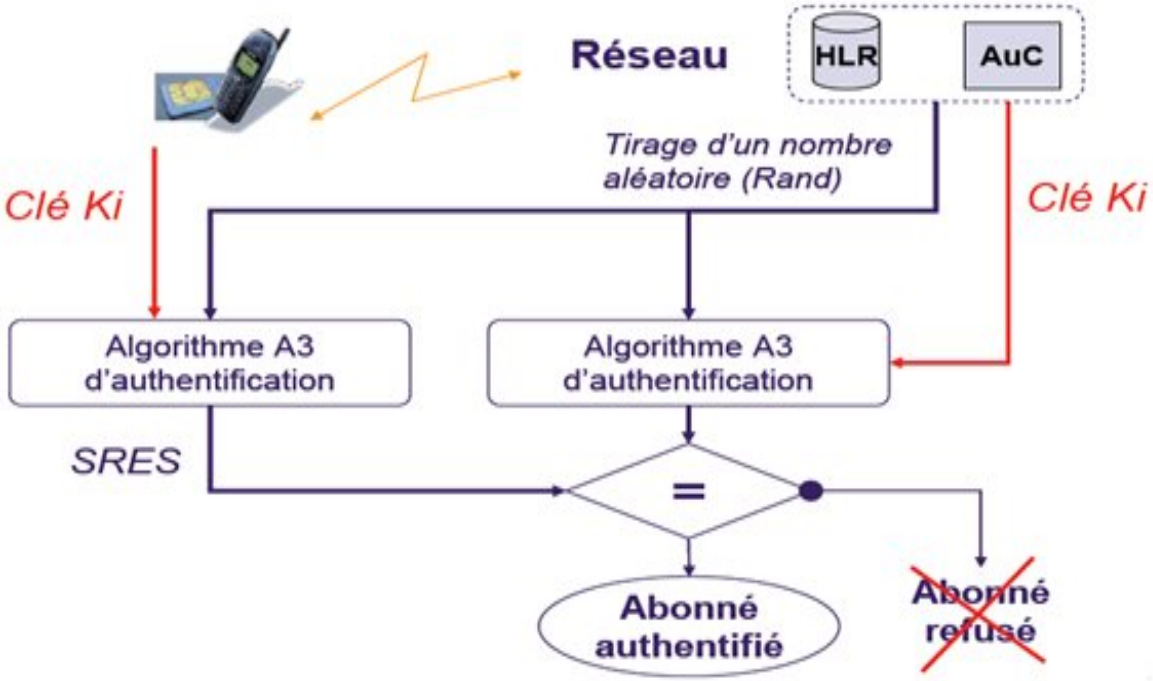


Figure I.6 : Principe d'authentification des abonnés

- ✓ un algorithme A8 pour la détermination de la clé Kc à partir des arguments de RAND et Ki (construction clé Kc), Il est illustré en figure I.7.

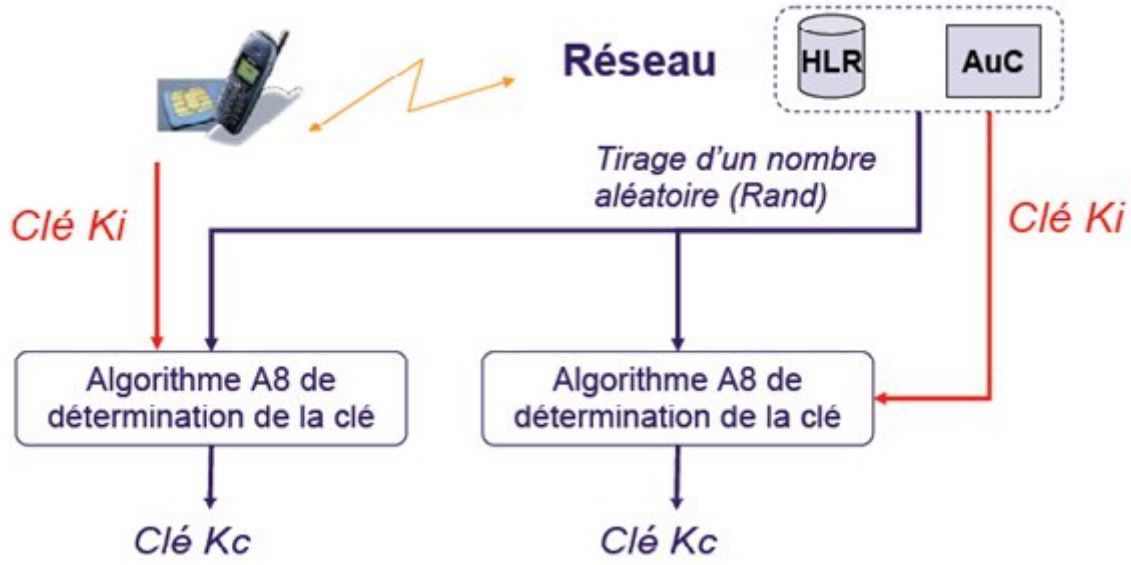


Figure I.7 : Principe de chiffrement

- ✓ un algorithme A5 (figure I .8) pour le chiffrement / déchiffrement des données à partir de la clé Kc (chiffrement a proprement parlé),

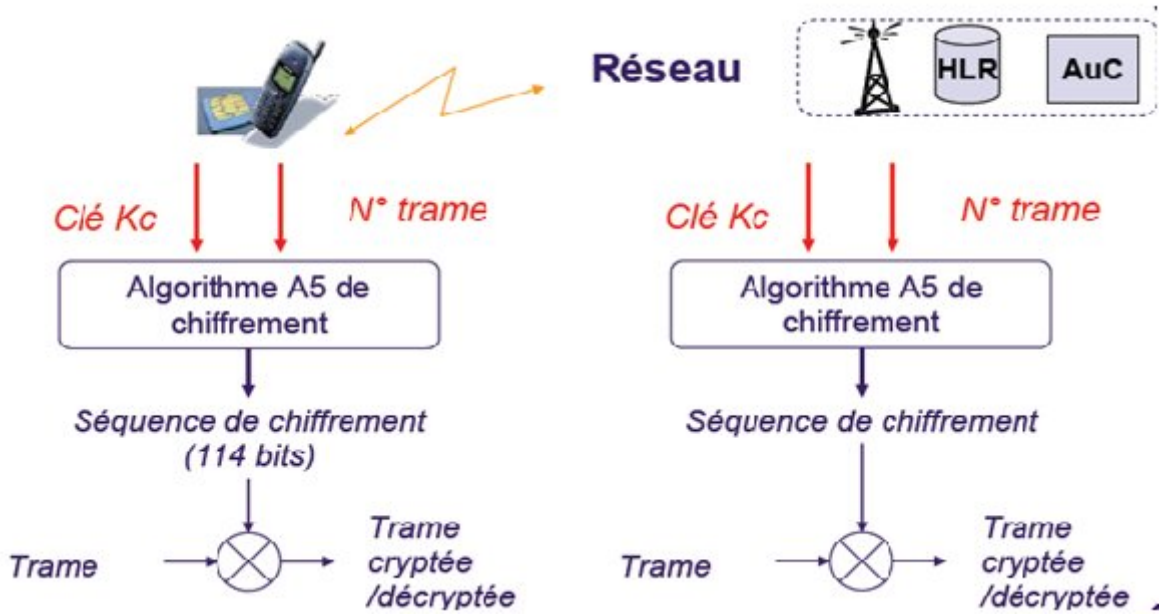


Figure I .8 : Principe de confidentialité des communications avec A5

Les algorithmes A3, A5 et A8 sont quant à eux les mêmes pour tous les abonnés d'un même réseau.

- Le centre d'authentification (AUC) stocke ainsi :
  - ✓ l'algorithme d'authentification A3,
  - ✓ l'algorithme de génération de la clé de chiffrement A8
  - ✓ les clés Ki des différents abonnés du réseau GSM.
- Le HLR stocke les (Kc, RAND, SRES) pour chaque IMSI.
- Dans le VLR les (Kc, RAND, SRES) sont enregistrés pour chaque IMSI avec les couples TMSI - IMSI.
- La BTS quand a elle, stocke l'algorithme de chiffrement A5 pour les données usager et pour les données de signalisation.
- La station mobile contient dans la carte SIM de l'abonné : l'algorithme d'authentification A3, l'algorithme de chiffrement A5, l'algorithme de génération des clés de chiffrements A8, la clé d'authentification individuelle de l'utilisateur Ki, la clé de chiffrement Kc, le numéro de séquence de la clé de chiffrement et le TMSI.

I.8 Conclusion

Dans ce chapitre nous avons présenté une vue d'ensemble sur le réseau GSM, et nous nous sommes amener à déduire que plusieurs mesures de sécurité dans ce réseau ont été prise mais elle reste toujours limiter à l'interface radio.

Le réseau DCN, permet de relier les stations BSC, MSC et HLR (dans le but d'assurer la gestion du GSM), et puisque le DCN est un réseau informatique, des mesures de sécurité devront être prise par l'entreprise afin de garantir la sécurité des donnés que contiennent ces stations.

Les VPN sont présentés comme une clé de sécurité à utiliser par le GSM, pour cela nous nous intéressons dans notre travail, à une étude détailler de cette solution, que nous allons proposer de mettre en œuvre entre les stations de commande BSC du réseau GSM.

Pour s'on faire, nous allons présenter dans le chapitre II, cette technologie récente et efficace de sécurité ainsi que le protocole IPSEC permettant sa mise en œuvre.

II.1 Introduction

L'ouverture des réseaux d'entreprise au monde extérieur, la décentralisation des traitements et des données ainsi que la multiplication des postes de travail accroissent les risques de dénaturation des systèmes et d'altérations des données d'où l'exigence de la sécurité.

Dans ce chapitre, nous allons présenter deux technologies de sécurité informatique qui sont la cryptographie et le VPN ainsi que le protocole IPSEC utilisé pour réaliser les connections VPN.

II.2 Menaces de sécurité courantes

- Vulnérabilité du protocole TCP/IP : Les protocoles http, FTP et ICMP sont intrinsèquement non sécurisés. Les protocoles SNMP, SMTP sont liés à la structure intrinsèquement non sécurisés qui est à la base de la conception du TCP [14].
- Vulnérabilité des équipements réseaux : Les différents types d'équipements réseau tels que les routeurs, les firewalls et switchs ont des faiblesses de sécurité qui doivent faire l'objet d'une détection et d'une protection. Ces faiblesses concernent la protection des mots passe, le manque d'authentification et les protocoles de routage.
- Absence d'une politique de sécurité écrite : Une stratégie de sécurité non écrite ne peut pas être appliquée ni respectée de manière cohérente.
- Vulnérabilité des Systèmes d'exploitation: Tous les systèmes d'exploitation présentent des problèmes de sécurité qui doivent être résolus [15].

II.3 La cryptographie

La cryptographie permet l'échange sûr de renseignements privés et confidentiel. Un texte compréhensible est converti en texte inintelligible (chiffrement), en vue de sa transmission d'un poste de travail à un autre. Sur le poste récepteur, le texte chiffré est reconverti en format intelligible (déchiffrement).

Les techniques de cryptographie sont utilisées pour [16] :

- ✓ assurer la confidentialité des données (algorithme de chiffrement),
- ✓ garantir l'intégrité des données (algorithme de hachage),
- ✓ authentifier l'émetteur des données (algorithme de signature numérique).

La figure II.1 ci-après montre le principe de la cryptographie

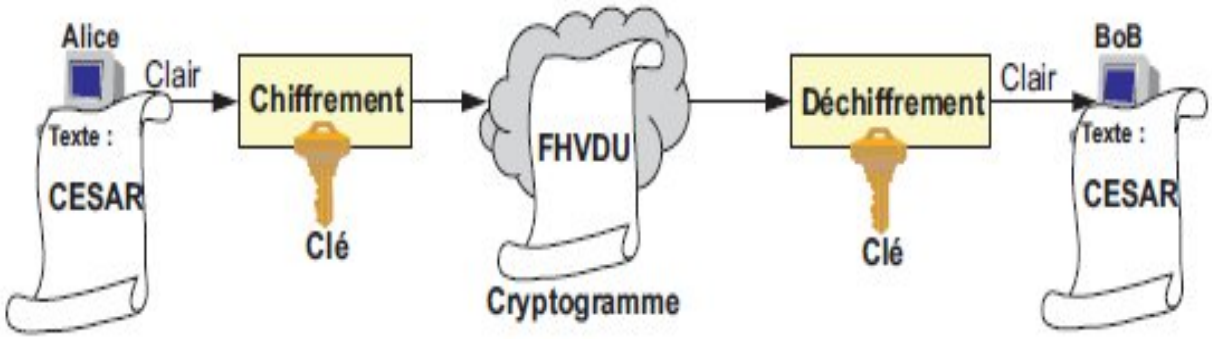


Figure II.1 : Principe de la cryptographie.

II.3.1 Confidentialité des données

Le chiffrement est une technique destinée à rendre les données inintelligibles pour les tiers non autorisés. L'opération de brouillage du texte s'effectue à partir d'une clé (clé de chiffrement) [17]. Le message en clair est codé (chiffré) à l'aide d'une clé de chiffrement ; seul, le cryptogramme (message chiffré) est transmis sur le réseau. Le destinataire du message effectue le décryptage à l'aide d'une clé de déchiffrement.

La figure ci-dessous, présente les différents types de chiffrement :

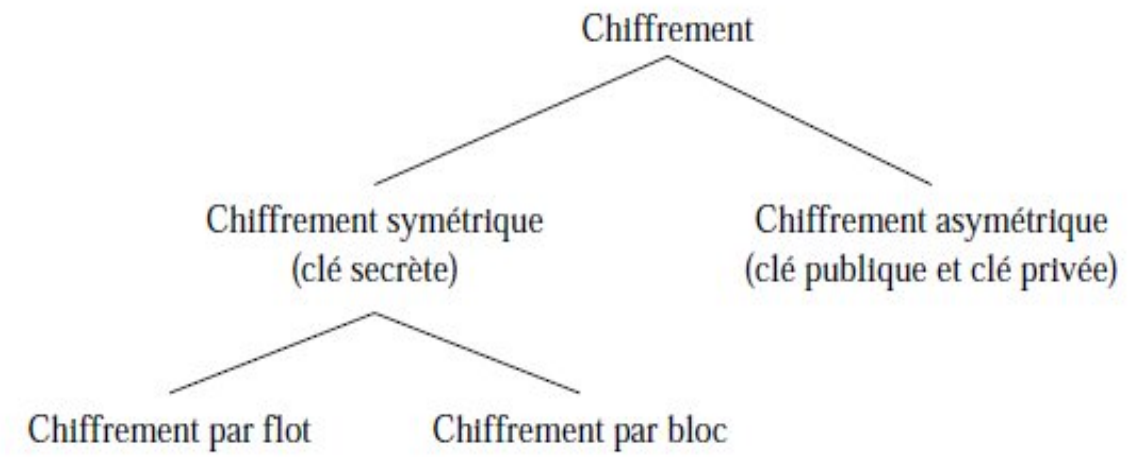


Figure II.2 : Types de chiffrement

a. Les méthodes de chiffrement symétrique

Les systèmes à clés symétriques ou secrètes utilisent une clé de chiffrement et une clé de déchiffrement identique, cette clé est secrète. Ces algorithmes peuvent être classés en deux : chiffrement par flot et chiffrement par bloc [18].

- **Le chiffrement symétrique par flot**

Leur utilisation repose sur un générateur de nombres pseudo-aléatoires et un mécanisme de substitution bit-à-bit (on faisant l'opération « ou exclusif » entre les bits). Ce principe est illustre dans la figure II.3.

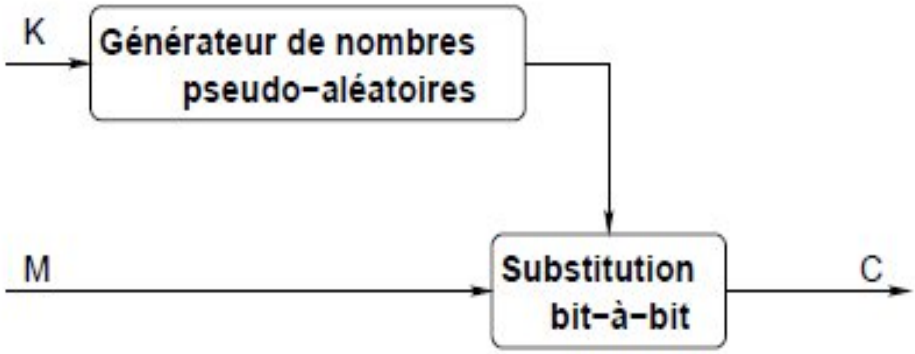


Figure II.3: Chiffrement symétrique par flot

Parmi les exemples les plus connus de chiffrement par flot, on citera LFSR, RC4 et A5/3 (utiliser dans les communications par GSM).

- **Les chiffrements symétriques par blocs**

Dans le cadre de ce chiffrement, le message original est divisé en bloc de taille identique, chaque bloc est manipulé avec la clé secrète. Le processus de chiffrement et déchiffrement par bloc est illustré par la figure II.4

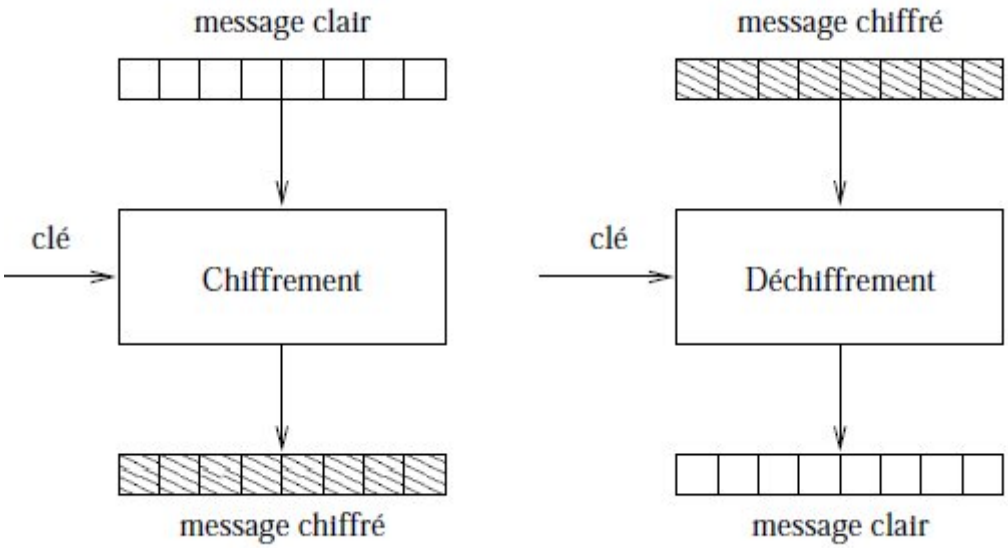


Figure. II.4: Chiffrement et déchiffrement par bloc (Bloc cypher).

Les systèmes classiques comme les DES et AES utilisent le chiffrement par blocs.

- ✓ **Algorithme DES**

Le DES (Data Encryption Standard) est l'algorithme à clé symétrique le plus connu. Il consiste en une suite de substitutions (DES-S) et de transpositions, ou permutations (DES-P), par bloc de 64 bits utilisant une clé de 56 bits (64 bits dont 8 de parité) [19]. A cause de la longueur très courte de la clé (56 bits), le DES est remplacé par le triple DES (3DES, application de 3 DES successivement avec 3 clés indépendantes) [20].

La figure II.5 illustre de manière simple le principe d'un tel code.

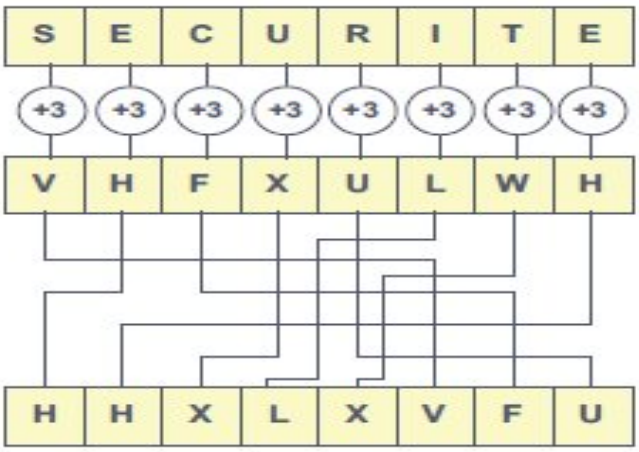


Figure II.5 Principe du DES.

Le protocole de Diffie-Hellman permet de sécuriser l'échange de clé, cette technique est utilisée dans IPSec (IP Secure).

- ✓ **AES (Rijndael)**

Rijndael est le chiffrement à clef secrète qui a été retenu par le NIST (National Institute of Standards and Technology) comme le nouveau standard américain de chiffrement (AES : Advanced Encryption Standard). C'est un code par blocs encodant 128 bits avec des clefs de 128, 192 ou 256 bits [18].

b. Les méthodes de chiffrement asymétrique

Evitant la diffusion de clés, les systèmes à clés asymétriques utilisent deux clés, l'une est connue de tous (clé publique), l'autre n'est connue que de l'un des correspondants (clé secrète). Le message chiffré avec l'une ne peut être déchiffré qu'avec l'autre. Les deux clés sont reliées mathématiquement entre elles, mais l'utilisation de grands nombres rend ce lien pratiquement impossible à retrouver. La figure II.6 illustre ce mécanisme.

Figure II.6 Principe de la cryptographie à clé publique.

II.3.2 Contrôle d'intégrité du message

Pour vérifier l'intégrité d'un message, une fonction dite de hachage (hash) est appliquée au contenu du message.

Le résultat obtenu ou digest (résumé, sceau...) est joint au message à transmettre, il est recalculé par le destinataire. Si le résultat du calcul local est identique au digest reçu, le message n'a pas été altéré (figure II.7).

La fonction de hachage doit garantir qu'il est impossible à partir du digest de retrouver le message initial (non retour arrière ou one-way hash) et qu'il doit être quasi impossible que Deux messages différents ne donnent le même digest (résistance à la collision). Le digest a une longueur de 128 bits (MD2 à MD5, Message Digest X) ou de 160 bits (SHA-1, Secure Hash Algorithm) [18].

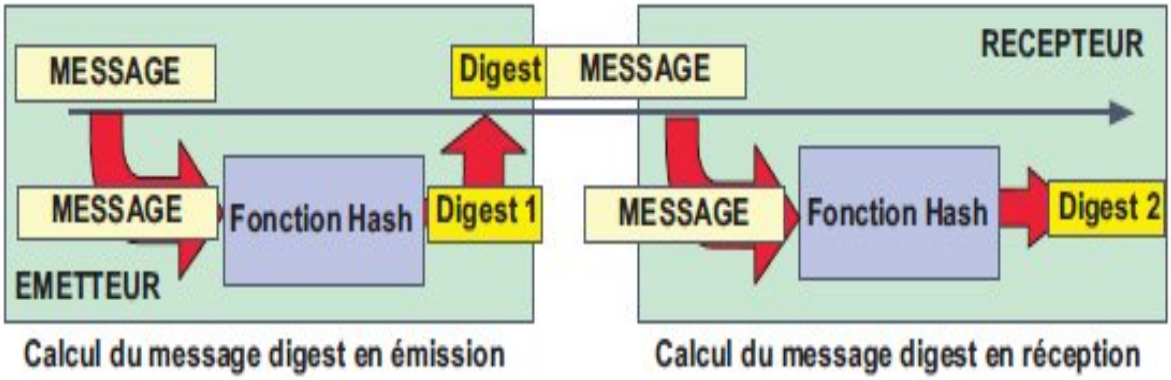


Figure II.7 : Principe de détermination du « digest ».

II.3.3 L'authentification de l'émetteur

Un message chiffré avec la clé publique n'est déchiffrable qu'à l'aide de la clé privée, cela assure la confidentialité mais ne permet pas d'authentifier l'auteur du message. L'authentification de l'émetteur peut être obtenue en chiffrant le message avec la clé secrète et en le déchiffrant avec la clé publique.

II.4 VPN « Virtual Private Network »

II.4.1 Principe général

Un réseau VPN repose sur un protocole appelé « protocole de tunneling » [21]. Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou

aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet [22].

II.4.2 Fonctionnalités des VPN

a. L'Intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières…). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées.

La figure II.8 montre le principe de l'intranet VPN.

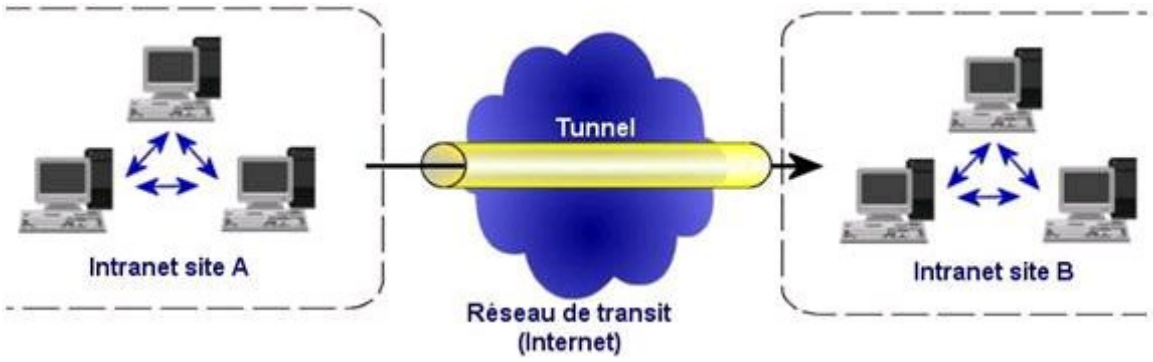


Figure II.8 intranet VPN

b. L'Extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

La figure II.9 montre le principe de l'extranet VPN.

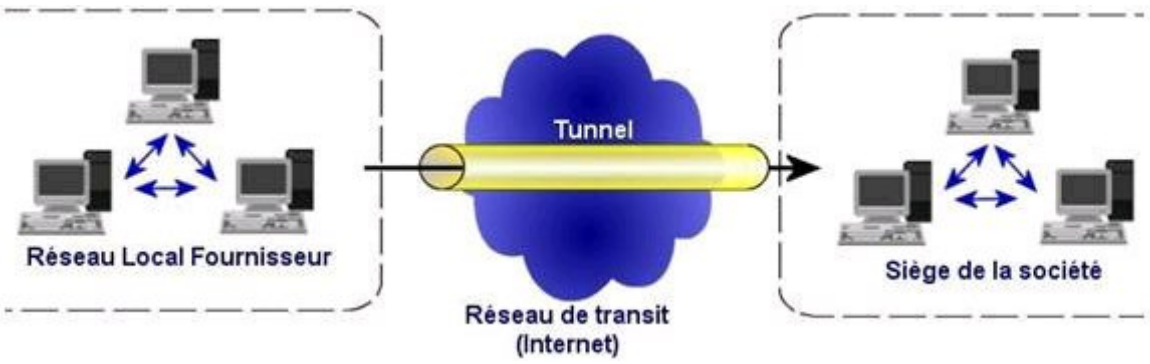


Figure II.9 extranet VPN

II.4.3 Caractéristiques fondamentales d'un VPN

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes:

- ✓ Authentification d'utilisateur : Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel.
- ✓ Gestion d'adresses : Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.
- ✓ Cryptage des données : Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- ✓ Gestion de clefs : Les clefs de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

II.5 L'IPSEC : protocole de réalisation des connections VPN

II.5.1 Notions de base

a. Modèle de référence OSI

L'ISO (international standardisation organisation) a défini un cadre pour la normalisation des systèmes de communication appelé modèle OSI pour l'interconnexion des systèmes ouverts. Son objectif est d'assurer que les protocoles spécifiques utilisés dans chacune des couches coopèrent pour assurer une communication efficace.

L'architecture OSI définit le processus de communication comme un ensemble de sept couches assurant chacune des fonctions bien spécifiques [23].

La figure II.10 montre les différentes couches du modèle OSI.

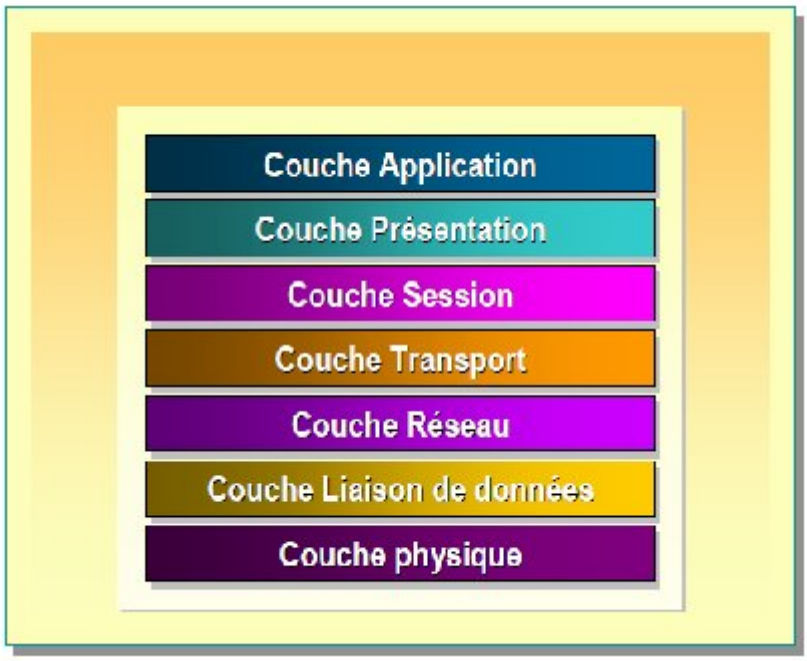


Figure II.10 Description des couches du modèle OSI

Les rôles des différentes couches sont les suivants :

- **La couche physique**
  - Elle se charge de la transmission de bits sur un canal
  - elle met en œuvre les mécanismes de modulation et démodulation des signaux.
- **La couche liaison**

Elle se charge de :

- L'envoi et la réception des trames de données sur une liaison
- la gestion des accès au canal de communication
- l'adressage des interfaces de la liaison (adresses MAC)
- la correction ou la détection d'erreur

- **La couche réseau**

Elle utilise et gère le sous-réseau afin de transmettre des paquets de liaison en liaison en passant par des systèmes intermédiaires (routeurs/commutateurs)

- **La couche transport**

Elle transporte des messages utilisateur provenant de la couche session et s'assurer qu'ils arrivent correctement

- **La couche session**

Elle fourni aux entités de présentation les moyens nécessaires à l'organisation et à la synchronisation de leur dialogue

- **La couche présentation**

Elle facilite l'échange de données entre utilisateurs

- **La couche application**

Elle donne aux processus d'application les moyens d'accéder à l'environnement de communication de l'OSI.

b. Modèle d'architecture de protocole TCP/IP

Il est inspirer du modèle OSI, apparu en 1974, ses couches ont des taches beaucoup plus diverse que les couches du modèle OSI [24].

La figure II.11 présente les différentes couches du modèle TCP/IP.

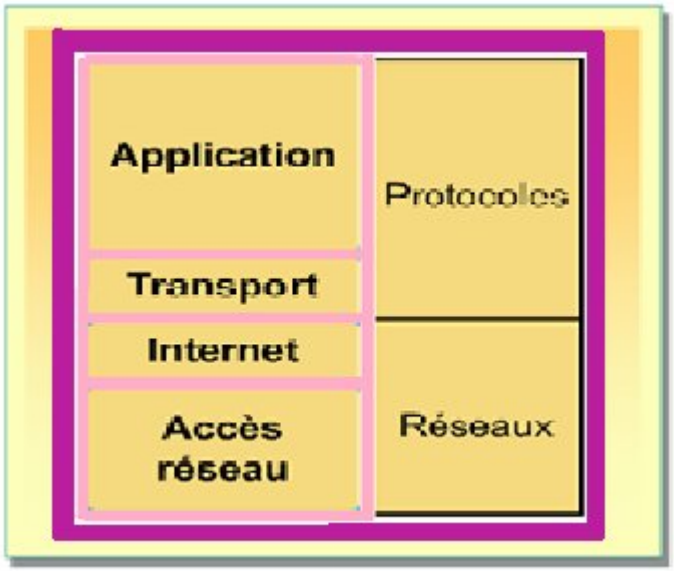


Figure II.11 Structure en couche

Les rôles des différentes couches sont les suivants :

- **Couche application**

La Couche Application englobe les applications standards du réseau [25]:

- ✓ SMTP: "Simple Mail Transport protocol", gestion des mails
- ✓ TELNET: protocole permettant de se connecter sur une machine distante (serveur) en tant qu'utilisateur
- ✓ FTP: "File Transfert Protocol", protocole permettant d'échanger des fichiers via Internet et d'autres moins courants.

- **Couche transport**

- elle assure l'acheminement des données et les mécanismes permettant de connaître l'état de la transmission.
- elle d'identifie les applications qui communiquent.
- La couche transport gère 2 protocoles de livraison des informations [26]:
  - ✓ TCP : assure le contrôle des données, orienté connexion
  - ✓ UDP, non orienté connexion, n'assure aucun contrôle de transmission des données.

- **Couche internet**

La couche internet est chargée de fournir le paquet des données. Elle définit les datagrammes et gère la décomposition /recomposition des segments.

- **Couche Accès réseau**

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

II.5.2 Présentation d'IPSec

Le protocole IPSec est une suite de protocoles désignés pour sécuriser les communications au niveau de la couche réseau [27]. La suite de protocoles est constamment en évolution depuis 1995. IPSec propose deux protocoles de sécurité du trafic IP :

- Authentication Header (AH)
- Encapsulating Security Payload (ESP). Chaque protocole AH ou ESP peut fonctionner en mode transport ou en mode tunnel.

Lors d'une connexion IPSec, une Security Association (SA) est définie. Elle va permettre de déterminer comment les paquets vont être sécurisés : Protocole, type de clé et leur durée de validité.

II.5.3 Principaux composants d'IPSEC

a. Mécanisme AH

Authentification Header est conçu pour assurer l'intégrité et l'authentification des datagrammes IP sans confidentialité. Son principe est d'ajouter aux datagrammes IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme [28]. Le principe est illustré par la figure II.13.

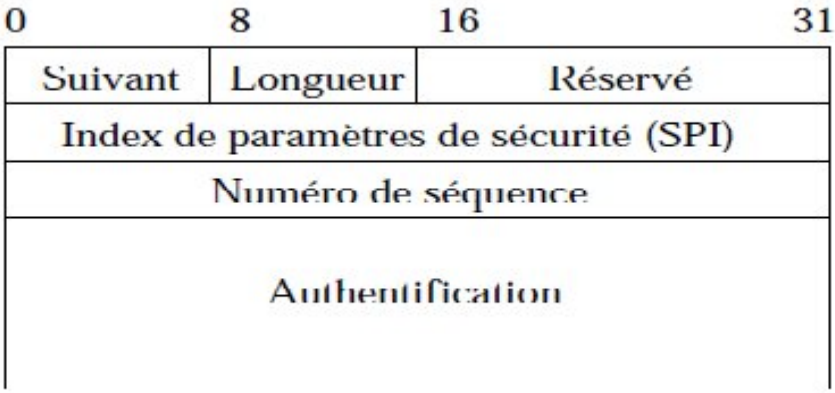


Figure II.13 mécanisme AH

b. Mécanisme ESP

Le mécanisme (Encapsulating security payload) a pour rôle premier d'assurer la confidentialité mais peut aussi assurer l'authenticité des données. Son principe est de générer à partir d'un datagramme IP classique un nouveau datagramme dans lequel les données son chiffrées [29]. Le principe est illustré par la figure II.14.

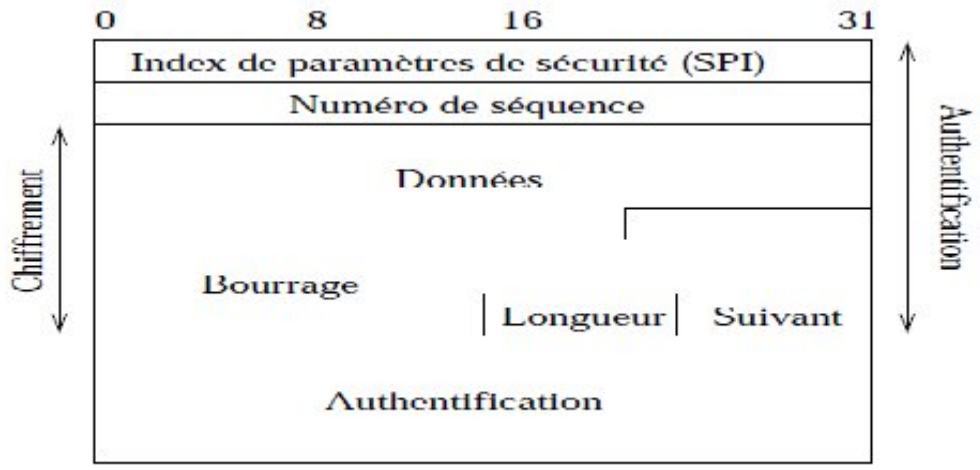


Figure II.14 : mécanisme ESP

c. Association de sécurité

L'association de sécurité peut être considéré comme une structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée, elle est unidirectionnelle, Donc, pour protéger les deux sens d'une communication, il nous faut deux SA, une dans chaque sens; et l'application de deux protocoles de sécurité AH et ESP au trafic amène à parler de paquet de SA [30].

d. Gestion des clés

La gestion des clés de chiffrement est une tache qui intervient lors de la mise en œuvre de solutions basés sur IPSEC pour cela deux alternatives sont utilisées.

- L'une manuelle, utilisé dans le cas des petits environnements statiques
- L'autre automatique, utilise un protocole d'échange de clés, le plus important est ISAKMP/Oakley qui permet de travailler dans les grands environnements

✓ ISAKMP (internet sécurity association and key management protocole) définit les procédures et les formats des paquets pour négocier une SA [31].

✓ IKE (internet key echange) permet de réaliser l'échange de clés (authentifiées) et de négocier les services de sécurité pour une SA [32].

II.5.4 Modes opératoires

Deux modes d'utilisation des services d'authentification et de confidentialité existent.il s'agit des modes dits de transport et de tunnel [33].

a. Le Mode transport

- Assure la protection pour les protocoles de la couche transport (information utile d'un paquet IP)
- ESP chiffre (et optionnellement authentifie) uniquement l'information utile du paquet IP (l'en-tête reste inchangé).
- AH authentifie l'information utile IP et des parties de l'en-tête IP.

La figure II.15 décrit le mode transport.

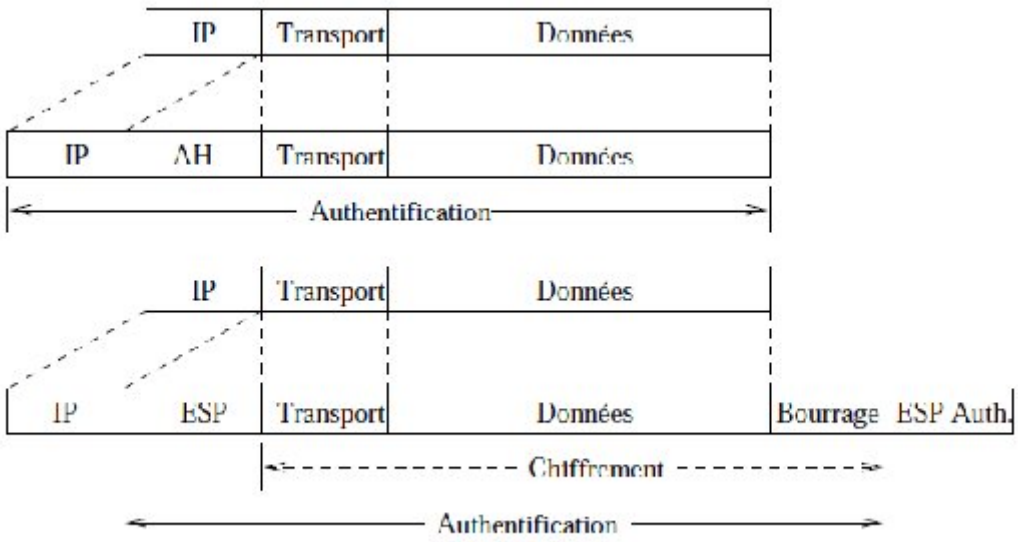


Figure II.15 : Les protocoles Ah et ESP en mode transport

b. Mode tunnel

- Assure la protection du paquet IP tout entier.
- Après l'ajout des champs AH ou ESP le paquet entier est traité comme l'information utile du paquet IP externe.
- Une (ou les deux) extrémité de l'AS doit être une passerelle de sécurité (firewall, passerelle implémentant IPSec, . . .)

La figure II.16 décrit le mode tunnel.

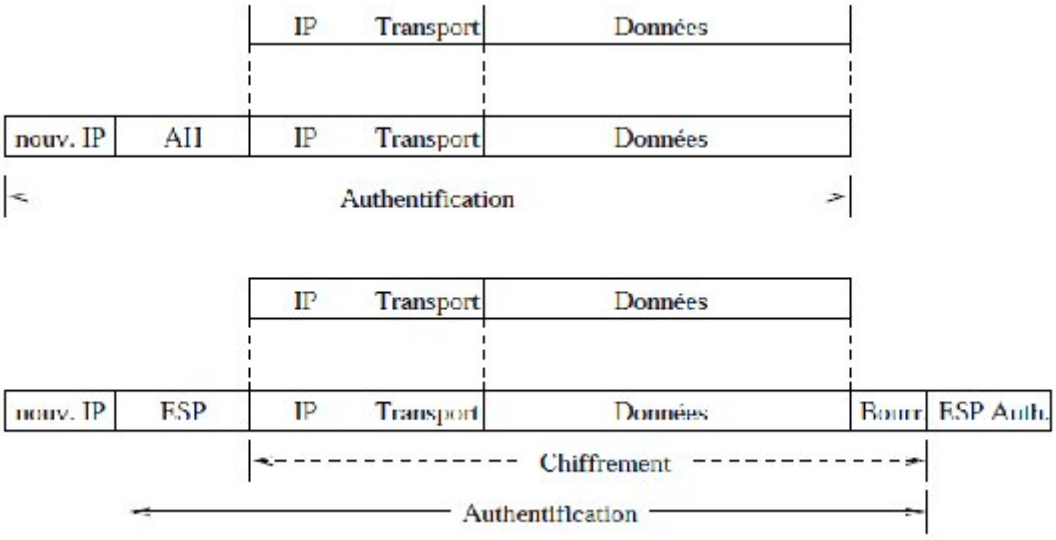


Figure II.16 : description du mode Tunnel

II.5.5 Les services d'IPSec

• Contrôle d'accès
• Intégrité des communications ("Connectionless") ;
• Authentification de l'origine des données ;
• Détection des paquets répétés (rejeu) ;
• Confidentialité (chiffrement) ;
• Confidentialité limitée du volume de trafic.

II.6 Conclusion

La couche trois du modèle OSI, est la couche essentielle de la majeure partie des réseaux d'entreprise et d'internet.

Au cours de ce chapitre, nous avons étudié une mesure de protection adéquate de cette couche qui est VPN à base d'IPSEC. Ce protocole propose

- Des services de sécurité complète (confidentialité, authentification et intégrité),
- il propose aussi différent mécanismes (AH et ESP) et modes de fonctionnement

(transport et tunnel) correspondant au différent niveau de sécurité.

Dans le chapitre III, nous aborderons l'équipement de routage dans les réseaux (le routeur) sur lequel nous allons par la suite implémenter l'IPSEC.

III.1 Introduction

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Un routeur est chargé de recevoir sur une interface des données sous forme de paquets et de les renvoyer sur une autre en utilisant le meilleur chemin possible. Selon l'adresse destination et l'information contenue dans sa table de routage.

Dans ce chapitre, nous allons décrire les procédures à suivre pour connecter et configurer les routeurs. Ces procédures requièrent l'utilisation du système d'exploitation Cisco Inter network Operating System (IOS).

III.2 Rappel sur un routeur

III.2.1Fabricants des routeurs

On site quelques uns [34]:

- **Cisco system** : c'est une entreprise informatique américaine qui vendait à l'origine uniquement du matériel réseau (routeurs et commutateurs Ethernet).mais aujourd'hui, elle offre une gamme importante des produits tel que les VPNs (virtuel private network), les firewalls….etc
- **3com** : elle est crée en 1979 par Robert Metcalfe, c'est une société spécialisée dans les équipements réseau.son sigle signifie computers, communication and compatibilité
- **Nortel** : c'est une entreprise canadienne, active dans le secteur des télécommunications. Elle fournit des matériels, des logiciels et des services pour les réseaux de télécommunication des opérateurs et les réseaux informatiques des entreprises dans plus de 150 pays.

III.2.2 Architecture des routeurs Cisco

Ses principaux composants sont les suivants [35] :

a. Matériel (hard)

Tous Les routeurs Cisco ont une architecture interne qui peut être représenté par la
Figure III.1:

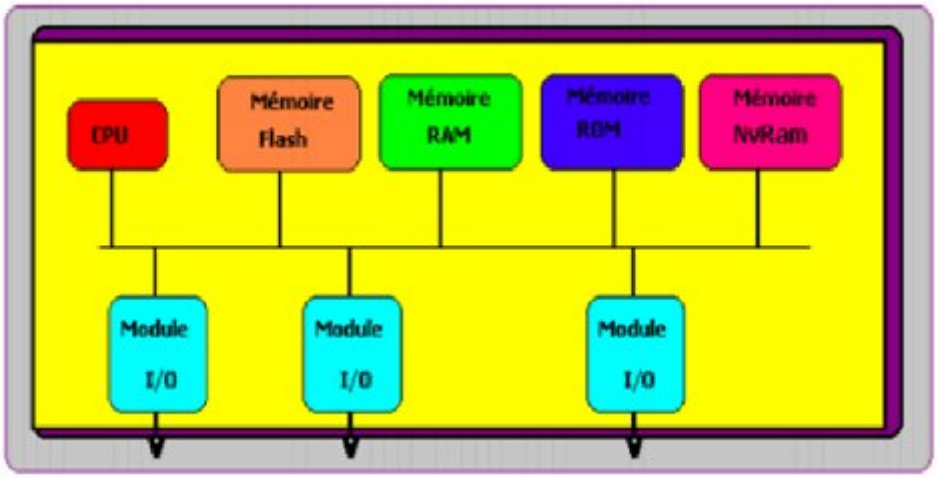


Figure III.1 : Architecture interne d'un routeur Cisco

Ils contiennent :

- Une mémoire **NVRam** (Ram non Volatile) sur laquelle l'administrateur va stocker la configuration qu'il aura mise dans le routeur. Elle contient également la configuration de l'IOS.
- Une **CPU** qui est un microprocesseur avec un BIOS spécial nommé I.O.S. pour Internetwork Operating System, elle exécute les instructions du système d'exploitation.
- Une mémoire **RAM** principale contenant le logiciel IOS, c'est dans laquelle le système d'exploitation maintient les informations durant le fonctionnement.
- Une mémoire **FLASH** sur laquelle on stocke la version courante de l'IOS du routeur.
- Une mémoire **ROM** contient les instructions de démarrage (bootstrap) et est utilisée pour des opérations de maintenance difficiles de routages, ARP, etc
- **Interfaces**

  Elles permettent aux routeurs de se connecter avec l'extérieur. Il possède trois types d'interfaces : LAN, WAN et console / AUX

- ✓ Les interfaces LAN sont en générale des ports Ethernet ou Token Ring standards ;
- ✓ Les interfaces WAN incluent des port séries ;
- ✓ Les ports console / AUX sont des ports séries utilisés pour la configuration initiale du routeur. Ce ne sont pas des ports réseaux. Ils sont utilisés pour les sessions de terminal à partir des ports de communication de l'ordinateur ou via un modem.

La figure III.2 illustre les différentes connexions externes d'un routeur.

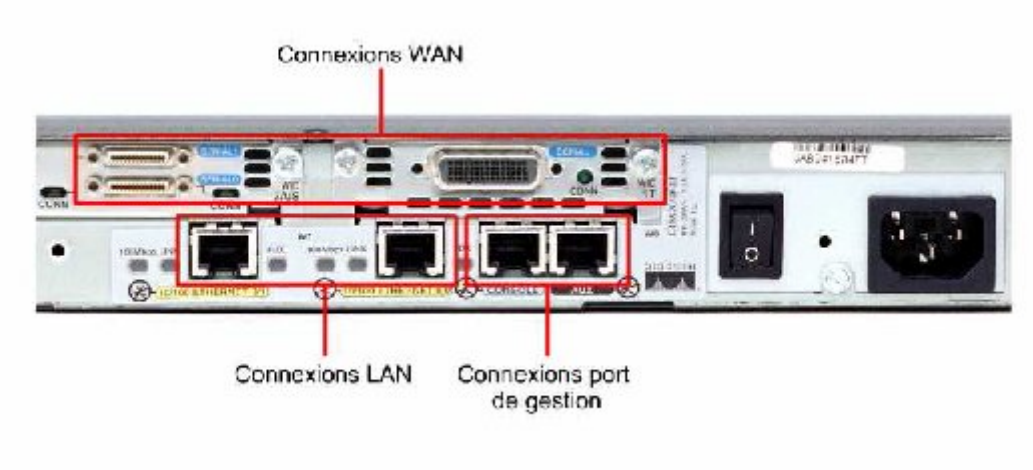


Figure III. 2 : Connexion externe sur un routeur

- **Bus**

Il est utilisé par le microprocesseur pour transférer les instructions et les donnés vers ou depuis les adresses mémoire spécifiées.

- **Alimentation**

Fournit l'énergie pour le fonctionnement des composants internes.

b. Logiciel (soft)

Les routeurs CISCO doivent être équipé d'un système d'exploitation IOS (internet working operating software) pour exécuter les fichiers de configuration qui contiennent les instructions et les paramètres afin de contrôler le trafic entrant et sortant des routeurs.il spécifie aussi toutes les informations pour l'installation et l'utilisation correcte des protocoles de routage et routés sélectionnés sur le routeur.

III.3 Protection du réseau avec le routeur

Les routeurs peuvent jouer un rôle dans la garantie de réseaux. Les routeurs exécutent beaucoup de travaux différents dans des réseaux modernes, les routeurs peuvent être employés selon trois voies fondamentales [36]:

III.3.1 Routeurs Intérieurs

Un routeur intérieur transmet le trafic entre deux ou plusieurs réseaux locaux au sein d'une organisation ou une entreprise. Les réseaux connectés par un routeur intérieur partagent souvent la même politique de sécurité et le niveau de confiance entre eux.
La figure III.3 montre l'utilisation des routeurs intérieurs.

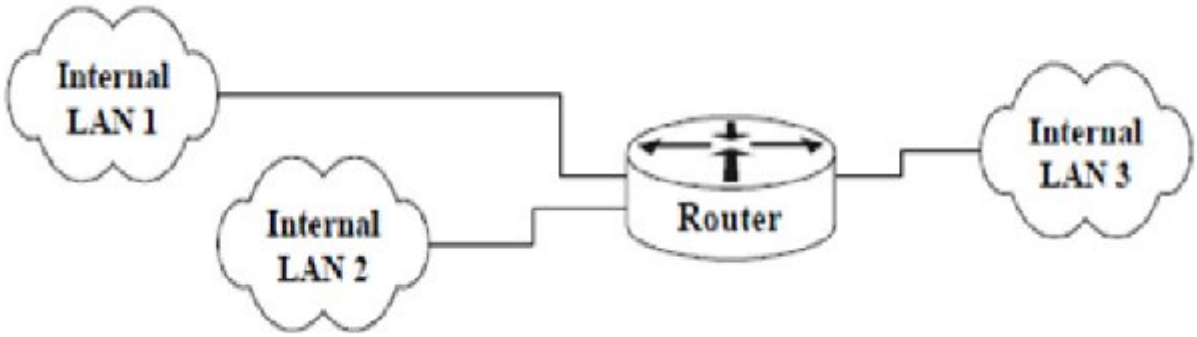


Figure III.3: Routeur reliant les réseaux locaux

III.3.2 Routeurs Backbone

Un routeur Backbone ou un routeur extérieur est celui qui transmet le trafic entre les différents sites d'une entreprise. Généralement, les routeurs de backbone sont conçus et configurés pour acheminer le trafic aussi rapidement que possible.
La figure III.4 montre l'utilisation des routeurs backbone.

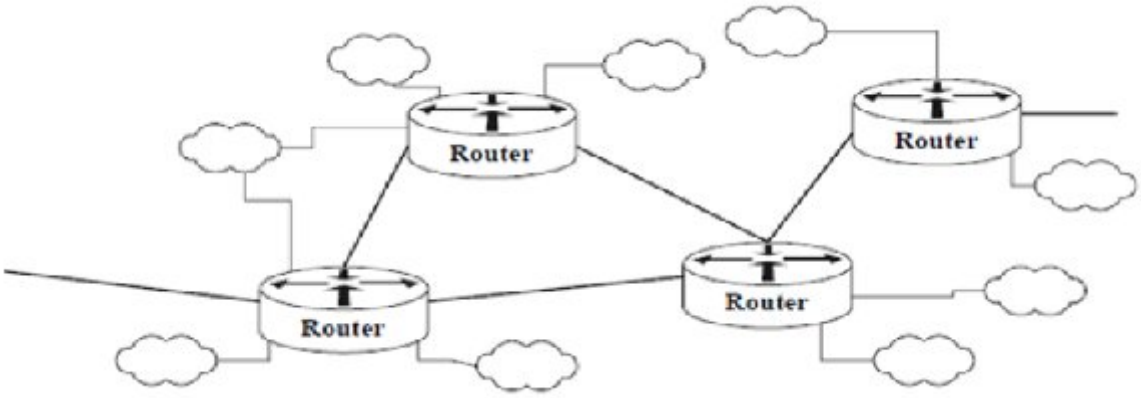


Figure III.4 : Routeur externe reliant différents site

III.3.3 Routeurs frontaux

Un routeur frontal achemine le trafic entre le réseau de l'entreprise et le réseau extérieurs. L'aspect clef d'un routeur de frontière est qu'il présente la partie intermédiaire entre les réseaux internes sécurisés d'une entreprise et des réseaux externes non sécurisés (par exemple l'Internet). Il peut aider à sécuriser le périmètre d'un réseau d'entreprise en appliquant des restrictions au trafic qu'il contrôle. Un routeur de frontière peut utiliser des protocoles d'acheminement, ou il peut dépendre des routes statiques.
La figure III.5 montre l'utilisation des routeurs fontaux.

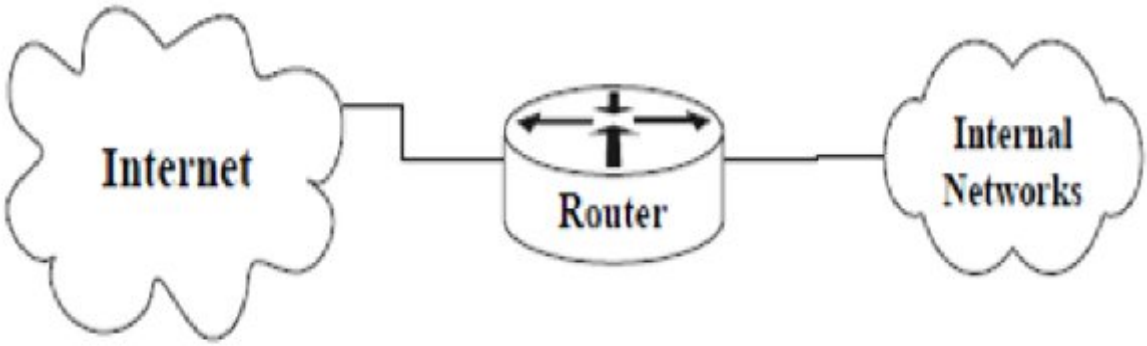


Figure III.5 : Routeur frontal

III.4 Configuration des routeurs

Pour préparer le démarrage et la configuration initiale nous connectons le routeur à un ordinateur comme suit [37]:
Le connecteur RJ-45 du câble à paires inversées (câble console) est connecté au port console du routeur ;
L'autre extrémité du câble à paires inversées est connectée à l'adaptateur RJ-45 à DB-9 ou DB-25, ce dernier est connecté à un PC (figure III.6).
Ensuite nous accédons au programme hyper-terminal à partir de la barre des taches de Windows (menu démarrer-> tous les programmes-> accessoire-> communications- hyper-terminal), puis nous entrons un nom pour la nouvelle connexion, nous sélectionnons le port série sur lequel est connecté le câble console et nous cliquons sur paramètres par défaut puis ok.

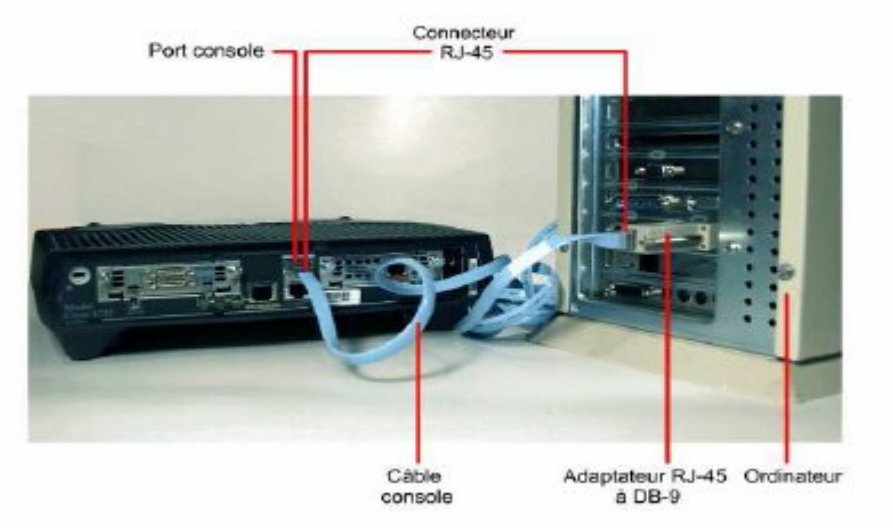
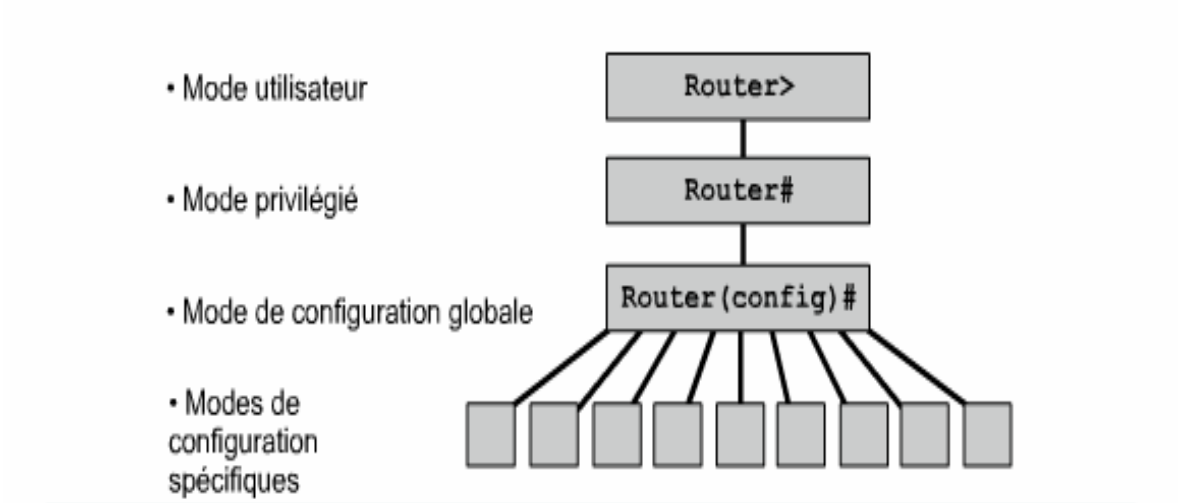


Figure III.6 :Accés au routeur via un ordinateur

III.4.1 Modes de configuration

Le routeur dispose de plusieurs modes de configuration [38] :

- **Mode utilisateur** : c'est un mode de visualisation seule, il est identifié par l'invite >.
- **Mode privilégie** : il permet en plus de la visualisation des paramètres, la configuration du routeur et le changement de paramètres dans la configuration. Il est caractérisé par l'invite # .
- **Mode de configuration globale** : c'est le mode de configuration principal, il permet d'appliquer des instructions de configuration qui affectent l'ensemble du système. Il est caractérisé par l'invite (config)#.



Mode de configuration	Invite
Interface	Router(config-if)#
Sous-interface	Router(config-subif)#
Ligne	Router(config-line)#
Routeur	Router(config-router)#

Figure III.7 : Les principaux modes IOS

III.4.2 Langage de commandes

Pour commencer la configuration du routeur, nous devons passer en mode global ; pour cela, nous introduirons au début dans le mode utilisateur, la commande « enable » pour passer au mode privilégie qui va nous permettre de rentrer en mode globale en tapant le commande « configure terminale ».

Ainsi, nous pouvons attribuer à notre routeur un nom on utilisant la commande « hostname » et un mot de passe en utilisant la commande

a. Configuration du nom d'hôte IOS

En mode d'exécution privilégié, accédez au mode de configuration globale en entrant la commande configure terminal :

- Router# configure terminal

Après exécution de cette commande, l'invite devient :

- Router(config)#

En mode de configuration globale, entrons le nom d'hôte :

- Router(config)#hostname router

Après exécution de cette commande, l'invite devient :

- router(config)#

nous observez que le nom d'hôte apparaît dans l'invite. Pour quitter le mode de configuration globale, nous utilisons la commande exit.

b. Limitation de l'accès aux périphériques avec mots de passe

Les mots de passe présentés ici sont les suivants :

✓ limitation d'accès au périphérique par une connexion console

- router (config)#line console 0
- router (config-line)#password
- router (config-line)#login

✓ Application d'un mot de passe à l'accès Privilégié

Il faut tout d'abord, se connecter en mode privilégié, puis en mode de configuration globale pour effectuer cette manipulation:

- router > enable
- router # configure terminal
- router(config) #

Une fois en mode de configuration globale, Il suffit de taper une seule commande pour appliquer un mot de passe:

- router (config) # enable password mot_de_passe

c. Configuration d'une interface de routeur

Dans le cas ou l'interface est destinée à transmettre des paquets IP, chaque interface connectée doit posséder une adresse IP et un masque de sou réseau

- Router(config-if)ip address <ip address> <net mask>

Les commandes suivantes permettent d'activer et de désactiver respectivement l'interface:

- Router(config-if) #no shutdown
- Router(config-if) # shutdown

d. Création d'access lists

Les access list filtrent le trafic réseau en contrôlant si des paquets routés sont transférés ou bloqués sur les interfaces du routeur. Lors de la création de l'acess list, il faut lui assigner un identificateur unique. Dans la majorité des cas, nous devons utiliser un numéro suivant le type de protocole à filtrer (tableau1) [39].

Protocole	espace
IP	1 à 99
Extended IP Ethernet type code	100 à 199 200 à 299
Ethernet address	700 à 799
Transparent bridging (protocol type)	200 à 299
Transparent bridging (vendor code)	700 à 799
Extended transparent bridging	1100 à 1199
DECnet & extended DECnet	300 à 399
XNS	400 à 499
Extended XNS	500 à 599
Appletalk	600 à 699
Source-route bridging (protocol type)	200 à 299
Source-route bridging (vendor code)	700 à 799
IPX	800 à 899
Extended IPX	900 à 999
IPX SAP	1000 à 1099
VINES	1 à 100

Tableau III.1 : Définition des ACL par numéro

III.5 Le routage

III.5.1 Types de routage

Il existe deus types de routage, soient statique et dynamique [40].

a. Routage statique

Une route statique est le fait de l'administrateur, il faut l'inscrire manuellement dans la table de routage.

Inconvénients

- ✓ Toute modification de topologie requiert l'intervention de l'administrateur.
- ✓ La panne d'un équipement ou d'une interface est une modification de topologie accidentelle, non planifiée.
- ✓ Le temps d'indisponibilité est fonction du délai de prise en compte du défaut par l'administrateur.

Avantage

- ✓ Le routeur n'a pas à consacrer une partie de ses ressources à l'entretien d'un protocole de routage (CPU, mémoire).

b. Routage dynamique

Lorsqu'un réseau atteint une taille assez importante, il est très lourd de devoir ajouter les entrées dans les tables de routage à la main. La solution est le routage dynamique. Cela permet de mettre à jour les entrées dans les différentes tables de routage de façon dynamique.

III.5.2 La table de routage

Routage statique et dynamique peuvent être utilisés conjointement, la table de routage comporte alors [41]:

- ➢ des routes directement connectées :
- ✓ les premières à apparaître dans la table ;
- ✓ leur présence est obligatoire (un routeur sans interfaces n'a pas de sens) ;
- ✓ une route directement connectée n'apparaît que lorsque l'interface correspondante est active.

- des routes statiques ;
- des routes dynamiques.

Seules les routes statiques et dynamiques concernent les réseaux distants (non directement connectés).

La table de routage est stockée en mémoire RAM et doit donc être reconstruite à chaque initialisation de l'équipement.

III.7 Conclusion

Dans ce chapitre, nous avons appris comment accéder aux modes et aux procédures de configuration de base d'un routeur Cisco.

L'étude du routeur ainsi que sa configuration nous a permis de mettre en évidence les différentes failles qui peuvent infecter les routeurs.

Dans la chapitre qui suit, on va configurer une solution de sécurité IPSEC dans les routeurs afin d'avoir des tunnels VPN sécurisé entre les différent BSC de réseau GSM (cas MOBILIS).

IV.1 Introduction

Un réseau de communication est exposé à des menaces tel que : l'écoute, la création, la modification et la destruction non autorisée des données, etc. l'idée de notre projet est de proposer une solution qui rends la communication entre les stations de commande BSC de GSM (entreprise MOBILIS) sécurisée.

Dans ce chapitre, nous allons implémenter notre solution pour cela nous commençons à organiser notre réseau en sous-réseau composer de deux BSC (chaque BSC est représenté par un routeur), ensuite nous configurons l'ACL et le protocole IPSEC sur les routeurs.

IV.2 Etude critique de l'architecture du réseau GSM

Dans l'architecture ci-dessous du réseau GSM, nous pouvons voir des liens de transmission entre différents équipements, ces liens de transmission s'appellent interfaces de GSM.

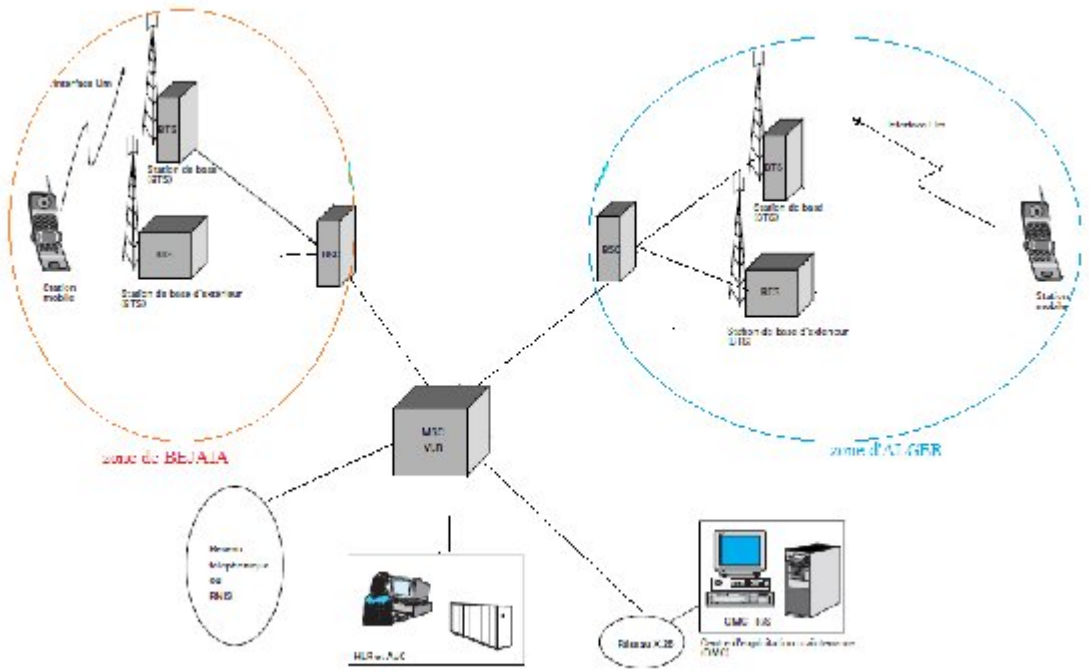


Figure IV.1 : Architecture du réseau GSM

Dans le premier chapitre, nous avons abordé les interfaces de GSM, dans cette partie, nous nous intéresserons à l'interface reliant les BSC, MSC, HLR. Cette interface est une liaison internet rendue possible par le réseau DCN, ce qui fait que l'interface est soumise à des risque d'attaques comme :

- La pénétration d'un réseau,
- Le vol ou détérioration d'informations,
- Les perturbations,
- L'écoute des réseaux,

Les objectifs de la sécurité dans notre cas est :

- empêcher la divulgation de données confidentielles,
- la modification non autorisée de données.

Nous retrouvons ainsi les principes fondamentaux de la sécurité :

- La confidentialité,
- L'intégrité,
- L'authentification,
- Le contrôle d'accès .

IV.3 Méthode d'amélioration de la sécurité du GSM

Pour répondre aux besoins de sécurités cités précédemment, nous proposons une nouvelle structure du réseau GSM (figure IV.2) qui va permettre de relier les différentes stations de commandes BSC de GSM par des tunnels privés IPSEC, pour cela, nous avons choisis deux zone géographiques, soient Bejaia et Alger (nous nous sommes limiter à deux station à cause de la grande taille du réseau GSM dans notre pays).

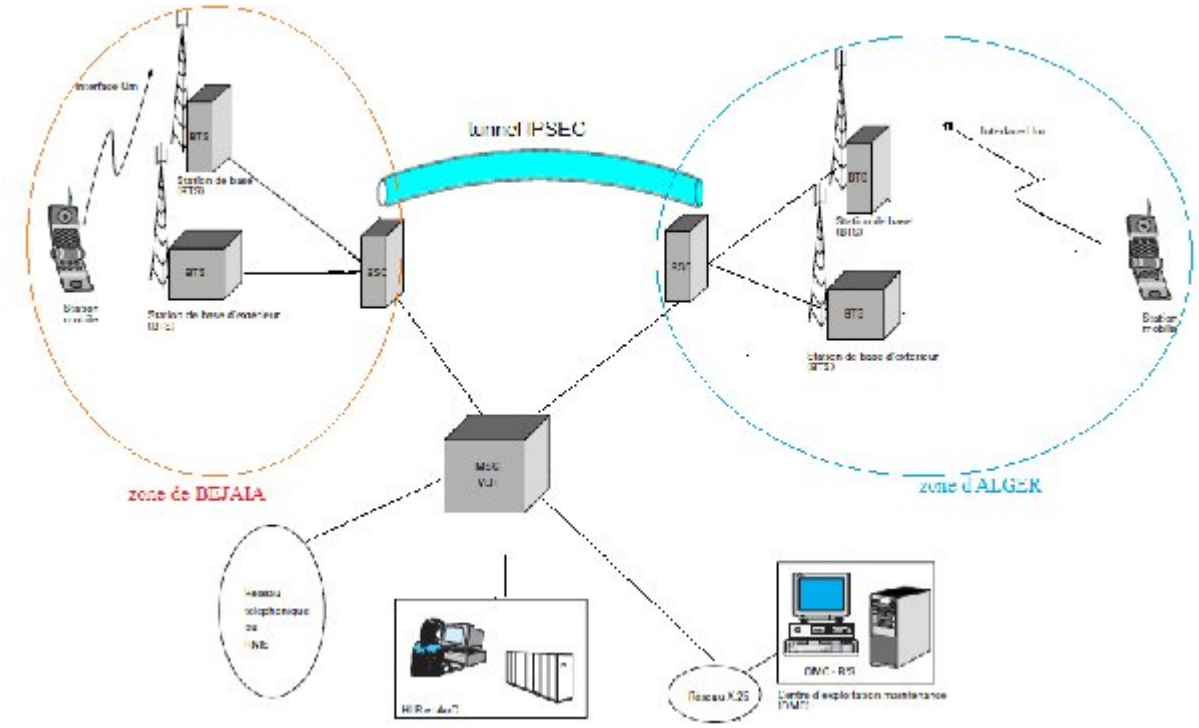


Figure IV.2 : Architecture proposé du réseau GSM

IV.4 La mise en œuvre d'un VPN

La mise en œuvre d'un VPN peut se faire à l'aide de logiciels ou de matériel d'interconnexion de réseau :

- Utilisation de logiciel : Elle consiste à configurer l'IPSEC sous windows, linux.... Etc.
- Utilisation matériel : consiste en fait à déléguer le tunneling au matériel mis en place en sortie d'entreprise, à savoir les routeurs (c'est la méthode que nous allons utiliser par la suite).

L'avantage de cette solution est qu'elle est totalement transparente pour les utilisateurs, puisqu'ils ont l'impression d'avoir un réseau en continu avec une simple gestion des accès classique.

IV.5 Politique de sécurité de routeur

Dans notre cas, la politique de sécurité devrait satisfaire :

- La Politique de mot de passe : Les routeurs présentent plusieurs types et niveaux d'accès (telnet, ligne virtuelle, mode enable, etc.). Chacun de ces accès est protégé par un mot de passe.
- Politique d'exploitation : Le routeur étant en service, il convient de définir une politique d'exploitation. Cette politique doit contenir les commandes de l'IOS de configuration de base des routeurs.

IV.6 Présentation de packet tracer

Packet tracer est un logiciel permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseau sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tel que les routeurs, les switchs ou des ordinateurs.ces équipements doivent ensuite être relié via des connections (fibre, câble).une fois, l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc.

La figure ci-dessous montre un aperçu général de packet tracer :

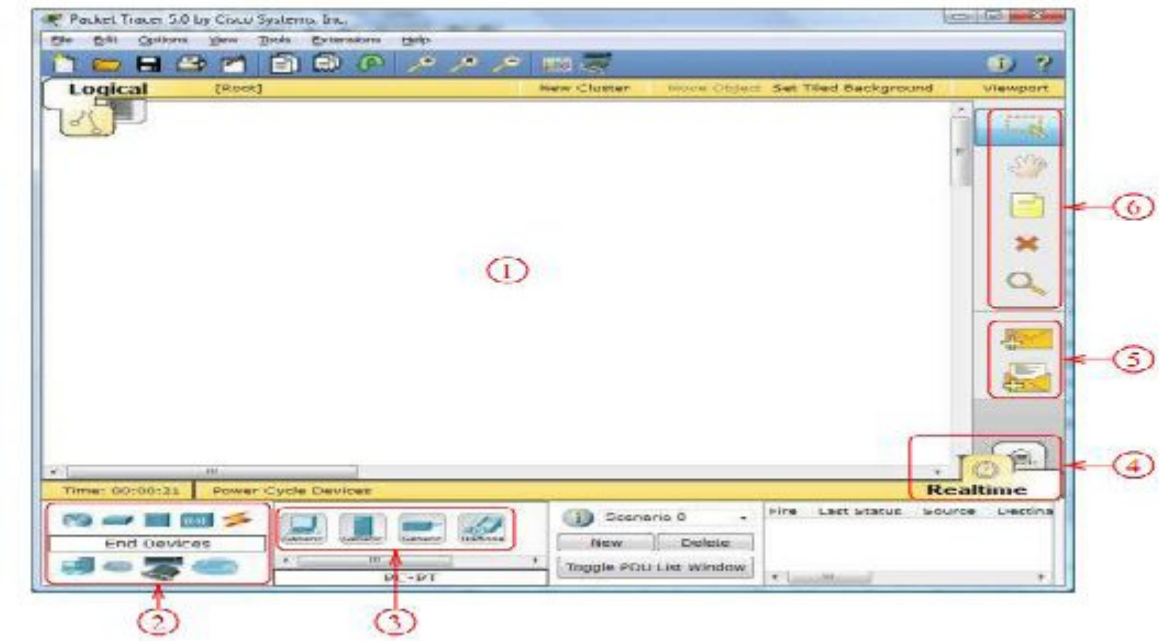


Figure IV.3 : Packet tracer

La zone (1) : est la partie dans laquelle le réseau est construit.les équipements sont regroupés en catégories accessible dans la zone (2).une fois la catégorie sélectionnée, le type d'équipement peut être transmis à la zone(3).la zone (4) permet de passer du mode temps réel au mode simulation.la zone (5) permet d'ajouter les indications dans le réseau. Enfin la zone (6) qui contient un ensemble d'outils :

- Select : pour déplacer ou éditer les équipements.
- Move Layout : permet de déplacer le plan de travail.
- Place note : place des notes sur le réseau.
- Delete : supprime un équipement ou une note.
- Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage).

IV.7 Mise en œuvre de la solution de sécurité

La mise en œuvre de notre solution se limite par la représentation de deux station BSC (routeurs) par le simulateur packet tracer (voir les détails en annexe). La figure suivante est une illustration de notre réseau.

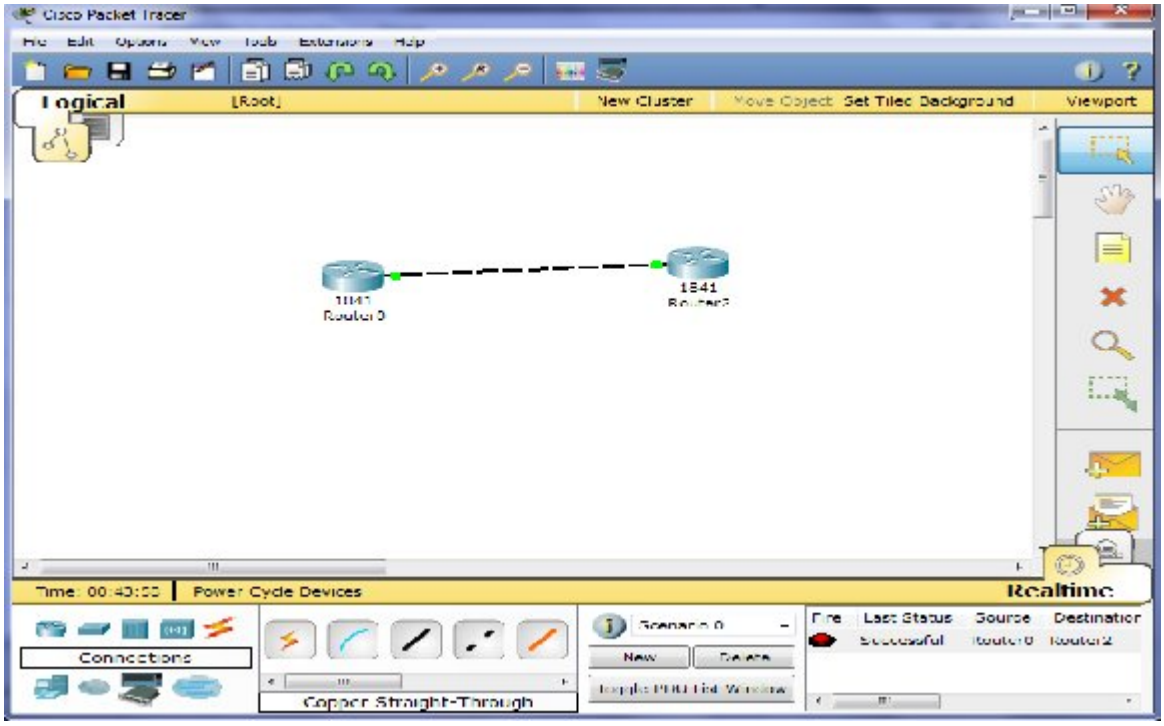


Figure IV.4 : Schéma du réseau

Après avoir installé l'architecture du réseau, nous aborderons les points suivants :

- Configuration des routeurs,
- Configuration des ACLs,
- Configuration du protocole IPSEC

IV.7.1 Configuration du routeur R0 et R2

Pour construire notre réseau sous packet tracer, nous devons sélectionner deux routeur, aprés cela nous cliquons deux fois sur le routeur, une fenêtre comportant trois anglets : physical, config et CLI s'ouvrent.

- Dans l'anglet physical, nous pouvons voir l'interface physique du routeur ainsi qu'une explication du rôle de chaque module du routeur.

La figure ci-dessous montre la fenêtre physical.

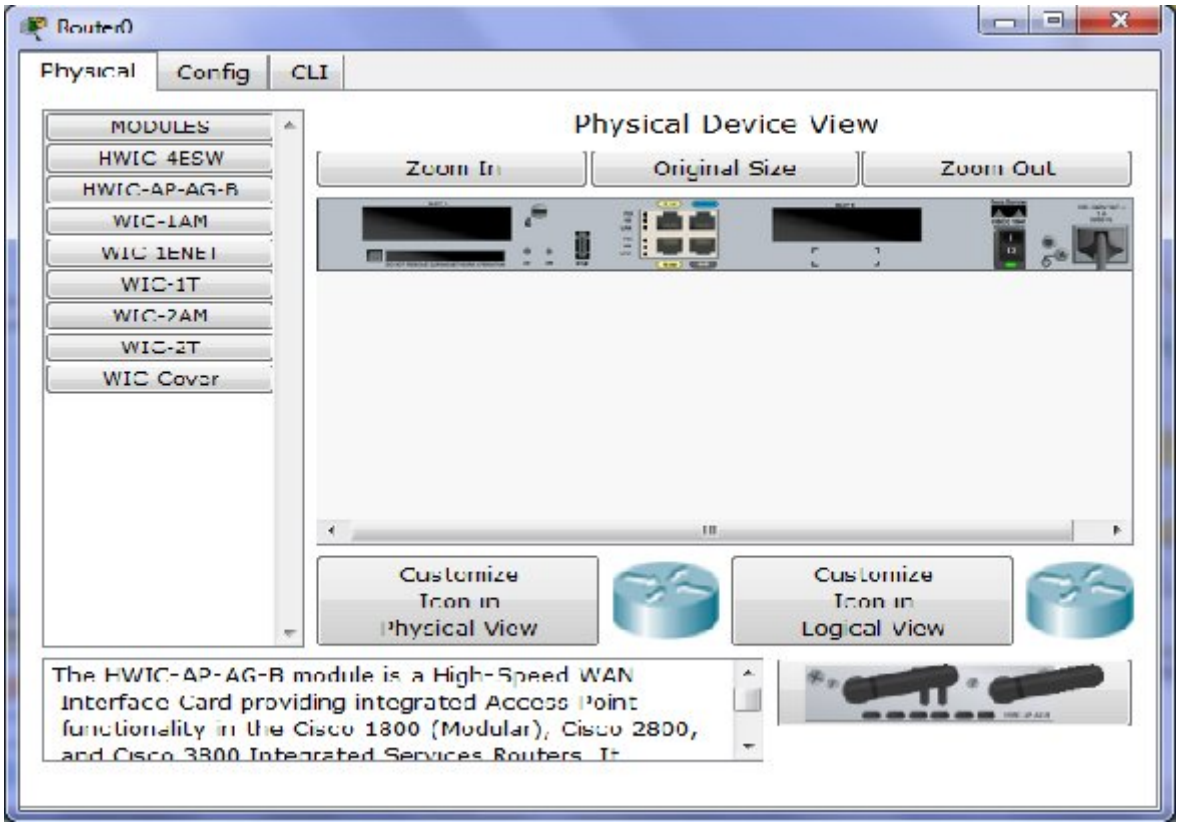


Figure IV.5 : Fenêtre physical

- Dans l'anglet config, nous sélectionnons le « port status » en mode « on » cela signifie que le routeur est allumé, et nous entrerons l'adresse IP dans « IPaddress » et en aura automatiquement un mask qui s'affichera dans « subnet Mask ».

La figure ci-dessous montre l'interface « config » du router0.

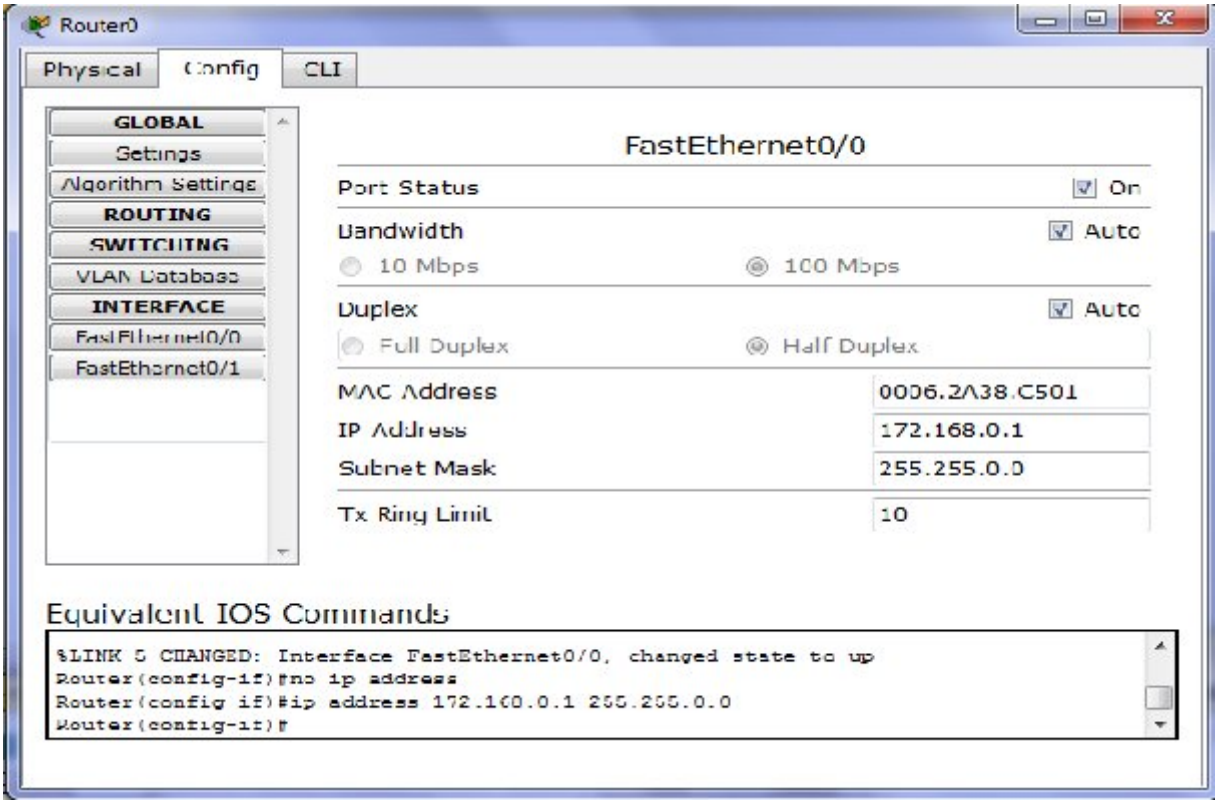


Figure IV.6 : Fenêtre config

- Dans l'anglet CLI, nous pouvons rentrer toutes les commandes de configuration du routeur ou les commande des protocoles que nous voulons configurer dans le routeur.

La figure IV.6 montre l'interface CLI du routeur0.

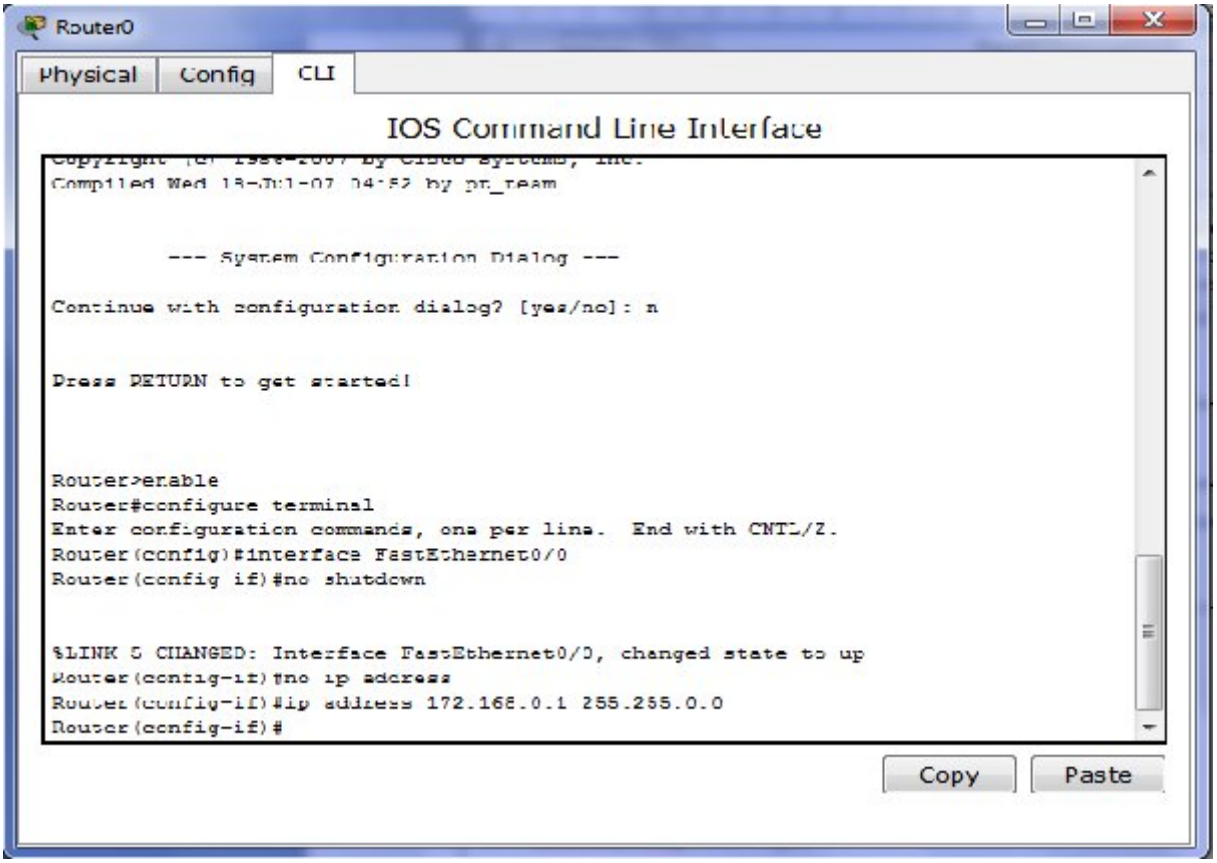


Figure IV.7: Fenêtre CLI

Après avoir rentré dans la fenêtre CLI, nous pouvons rentrer les commandes de configuration des routeurs.

La configuration est présentée comme suit :

```
Router>enable
Router#configure terminal
Router(config)#hostname rout-mobilis
rout-mobilis(config)#line console 0
rout-mobilis(config-line)#password mobilis
rout-mobilis(config-line)#login
rout-mobilis(config-line)#exit
rout-mobilis(config)#enable password mobilis
rout-mobilis(config)#enable secret password
rout-mobilis(config)#service password-encryption
rout-mobilis(config)#exit
```

IV.7.2. Introduction d'une ACL (access list)

Elle définie le trafic à chiffrer :

```
Rout-mobilis(config)#ip access-list extended CHIFFRER
Rout-mobilis (config-ext-nacl)# permit ip 172.168.0.1 255.255.0.0 172.168.0.2
255.255.0.0
```

IV.7.3 Chiffrement en AES

Nous observons ici la configuration des phases du protocole IKE qui est appelé ISAKMP. Les phases d'authentification mutuelle des routeurs sont protégées avec le protocole AES et le protocole de DiffieHellman au niveau 5 [42], les deux routeurs utilisent une même clé prépartagée.

```
Rout-mobilis (config)#crypto isakmp policy 10
Rout-mobilis (config-isakmp)#encr aes
Rout-mobilis (config-isakmp)#authentication pre-share

Rout-mobilis (config-isakmp)#group 5

Router(config-isakmp-policy)# encryption 3des

Router(config-isakmp-policy)# lifetime 43200
```

Voici la clé pré-partagée :
Sur le routeur, nous configurons la clé qui correspond au partenaire IPSec.

```
Rout-mobilis (config)#crypto isakmp key 0 address 172.168.0.1
```

IV.7.4 Association de sécurité

La commande security-association lifetime limite dans le temps la validité de l'association des deux routeurs. Au delà de la limite de 3000 secondes sans échange, les clés de chiffrement sont renégociées.

```
Rout-mobilis (config)#crypto ipsec security-association lifetime seconds 3000
```

IV.7.5 Chiffrement AES et intégrité

Nous choisissons de chiffrer les paquets avec le protocole aes-256 et d'en protéger l'intégrité avec le protocole de hachage sha [43], par défaut le mode tunnel est employé cela signifie que les paquets d'origine (et notamment les adresses IP) seront chiffrés masquant ainsi leur origine et leur destination sur les réseaux locaux

```
Rout-mobilis (config)#crypto ipsec transform-set  myset  esp-aes 256 esp-sha
```

IV.7.6 Commande crypto

Voici la commande qui nomme la fonction IPSec et qui la rattache à la stratégie policy créée au début. Le routeur nous informe que cette commande n'est d'aucune utilité tant qu'un partenaire IPSec ne sera pas déclaré et tant qu'une ACL déterminant le trafic à chiffrer n'aura pas été créé.

```
Rout-mobilis (config)#crypto map VPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

Poursuivons avec les sous commandes de crypto map.

```
Rout-mobilis (config-crypto-map)#set peer 192.168.0.1
Rout-mobilis (config-crypto-map)#set transform-set myset
Rout-mobilis (config-crypto-map)#match address myset
```

Dans cette séquence de commande, nous appelons les fonctions de chiffrement définies auparavant avec la commande crypto ipsec transform-set, cette commande permet de sécuriser les messages chiffrés avec les clés antérieures à une clé compromise grâce à une renégociation par le protocole de DiffieHellman. En clair, si une clé venait à être compromise, un attaquant aurait du mal à déchiffrer les messages émis avec les clés précédentes, car ces dernières ne seraient plus liées entre elles. Enfin, l'ACL nommée myset est appelé. Cette dernière, définit le trafic à chiffrer sur le lien.

```
Rout-mobilis (config)#int f0/0
Rout-mobilis (config-if)#crypto map VPN
```

A cette étape nous avons terminé la configuration d'IPSEC dans le routeur, à présent, lors du lancement de la simulation, les paquets seront cryptés et décrypté en utilisant les différents algorithmes : AES, DES et SHA.

IV.8 Simulation du réseau sous packet tracer

1. Pour lancer le réseau, on envoie un paquet (enveloppe) de l'émetteur vers le récepteur. La figure ci-dessous montre le lancement des paquets.

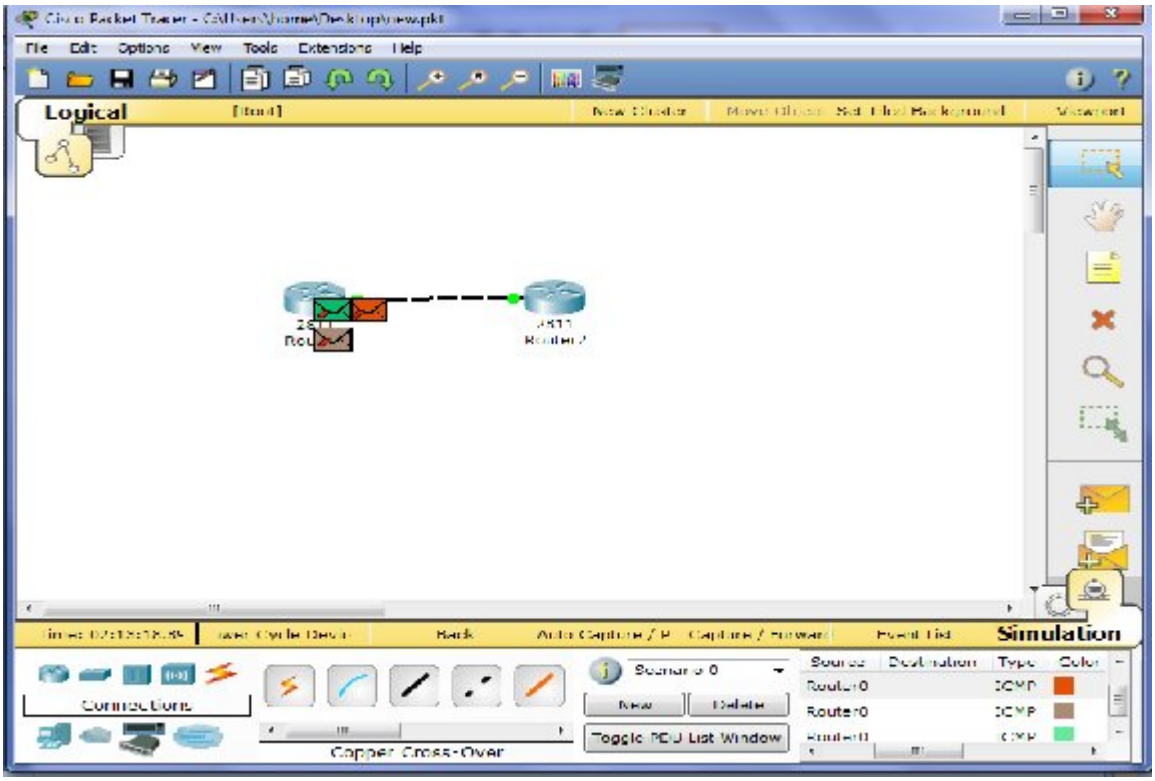


Figure IV.8 : Opération de lancement des packets

2. Après avoir lancé les packets, on rentre dans le mode simulation, nous aurions les résultats de simulation dans une fenêtre « simulation panel » (figure IV.3) qui indique le temps de transmission des paquets, le routeur émetteur et le routeur récepteur, le protocole de routage utilisé.

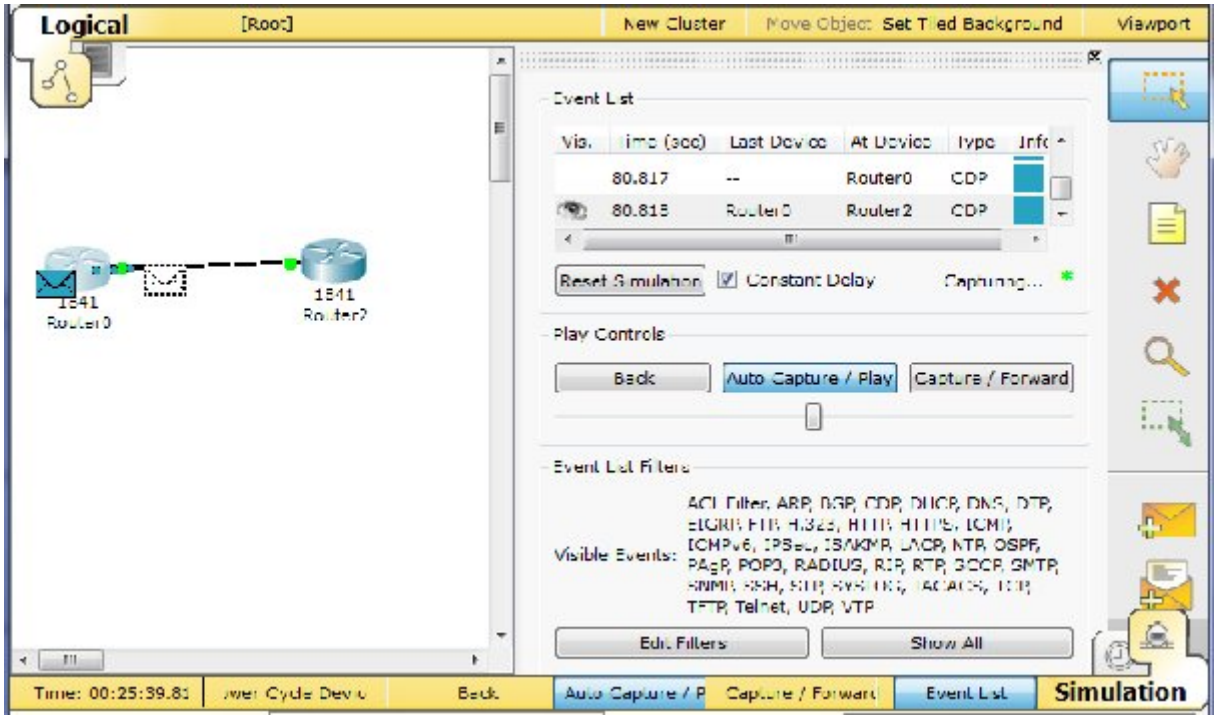


Figure IV.9 : Fenêtre simulation panel

3. On cliquant sur une couleur dans la case « info » de la fenêtre « simulation panel », on aura des informations concernant l'état de la transmission sous model OSI et des détails sur le protocole de routage. (figure IV.4)

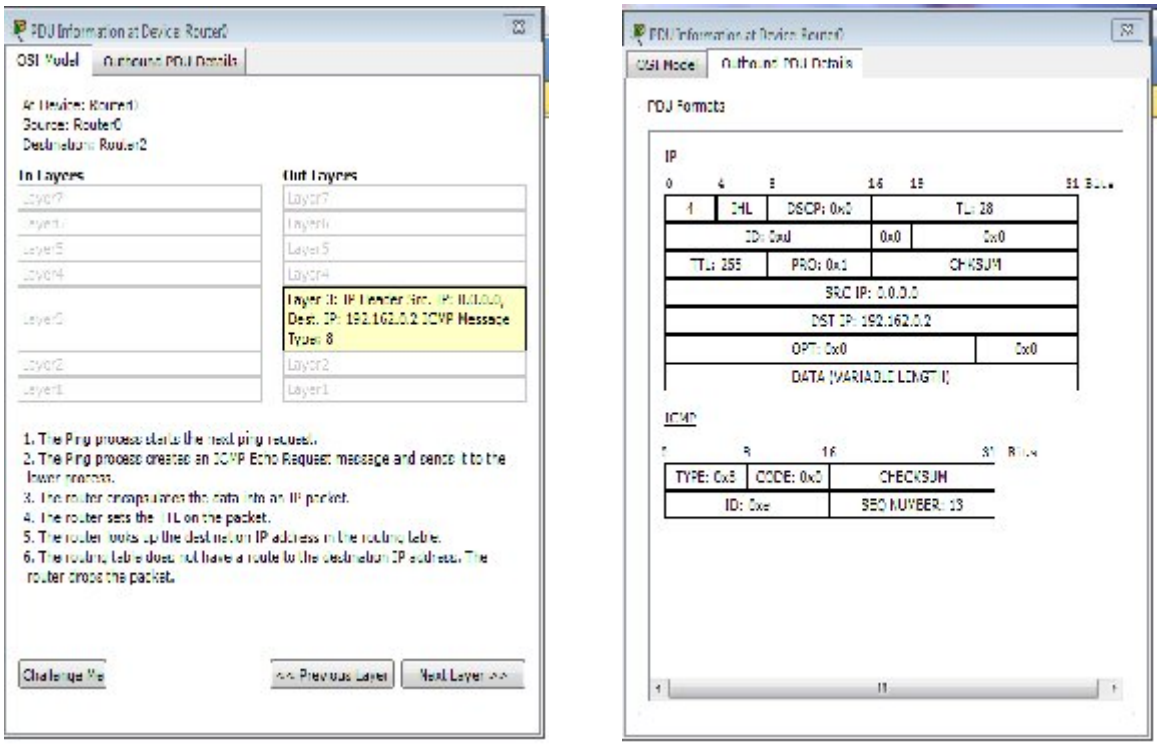


Figure IV.10 : Fenêtre d'informations

Commentaire :

Les deux routeurs Cisco utilisant le même module IPSec, on est sûre de la compatibilité, donc si la connexion ne se fait pas, il s'agit uniquement d'une erreur de configuration. Et puisque la simulation de notre réseau a donner un fonctionnement normale de notre réseau et n'a signaler aucune erreur lors de la transmission des paquets donc notre configuration de l'IPSEC est parfaite.

IV.4 Conclusion

Dans ce chapitre, nous avons exposé notre environnement de travail tout en définissant les exigences de sécurité à prendre en compte.

L'IOS offre diverses commandes permettant de répondre à ce besoin, principalement les ACL (Access Control List) qui permettent de filtrer des paquets suivant des critères définis ainsi que différentes commandes d'implémenter notre solution de sécurité (VPN ipsec).

Le présent projet, est une opportunité pour aborder le domaine le plus important de nos jours, celui de la sécurité des systèmes d'information. Nous avons examiné la sécurité des routeurs CISCO qui présentent la colonne vertébrale de l'infrastructure réseaux de MOBILIS ou tout autre entreprise déployant ce type de routeur, en vu de satisfaire le besoin de la société en matière de sécurité des équipements réseaux.

La méthodologie adoptée dans ce travail consistait à cerner les vulnérabilités qui peuvent se présenter, en étudiant les techniques des attaques sur le réseau. Ces dernières exploitent les vulnérabilités dans les protocoles réseau. Ensuite, établir les procédures de sécurité pour se protéger contre ces menaces au niveau du routeur, pour cela nous avons procédé comme suit :

Dans un premier temps, nous avons présenté les notions de base du réseau GSM, voir son architecture et sa sécurité. Puis nous avons présenté un large panorama sur les technologies de sécurité des réseaux à savoir la cryptographie et les algorithmes utilisés, le VPN et le protocole IPSEC utilisé pour ce genre de connexions. En suite nous avons vue l'équipement d'interconnexion des réseaux, le routeur, qui permet le routage des donnés.

Les suggestions que nous avons vu sur l'architecture du GSM sont l'un des points importants de notre travail, car nous ont dévoiler ses points faible afin d'implémenter notre solution qui sert à organiser l'ensemble des station BSC de GSM dans des sous réseau virtuels en utilisant l'IPSEC , et pour permettre la communication entre eux, nous avons configurer un routeur au niveau de chaque station pour qu'il effectue cette tache.

L'IPsec est un système très complet qui peut répondre à beaucoup de besoins en matière de sécurité et s'adapter à de nombreuses situations. Ces avantages, couplés à la prédominance grandissante du protocole IP, vont certainement faire d'IPsec un acteur important de la sécurité des réseaux informatiques. Il lui manque encore, pour être utilisé à grande échelle, un peu de maturité et surtout un système de gestion centralisée et dynamique des politiques de sécurité.

Les VPN permettent un accès sécurisé à Internet pour les communications offrant les mêmes stratégies et niveaux de sécurité et de performance qu'un réseau privé. Les VPN assurent la sécurité par la transmission en mode tunnel avec cryptage tandis que les routeurs Cisco prennent en charge la sécurisation matérielle des réseaux IP (IPSec), 3DES (Triple Data Encryption Standard) et logicielle AES (Advanced Encryption Standard).

L'IPSEC, DES et 3DES, fournissent des solutions VPN robustes pour garantir la confidentialité des données ainsi que leur intégrité et leur authenticité. Le module de cryptage matériel VPN des routeurs Cisco améliore encore les performances de cryptage VPN.

Toutefois, des améliorations peuvent être apportées à notre travail. Pour une prochaine version, la majeure perspective qui est envisagée sera l'implémentation du protocole LDAP, dans les tunnels VPN que nous avons proposé, qui est uniquement prévu pour gérer l'interfaçage avec un annuaire. Ce dernier va stocker les informations sensibles des stations de commande BSC de GSM, et puisque le GSM constitue la base des réseaux GPRS et UMTS, notre solution est applicable même dans ces générations de télécommunication.

Packet tracer

1. Présentation de packet tracer

Packet tracer est un logiciel permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseau sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tel que les routeurs, les switchs ou des ordinateurs.ces équipements doivent ensuite être relié via des connections (fibre, câble).une fois, l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc.

2. Description générale

La figure ci-dessous montre un aperçu général de packet tracer :

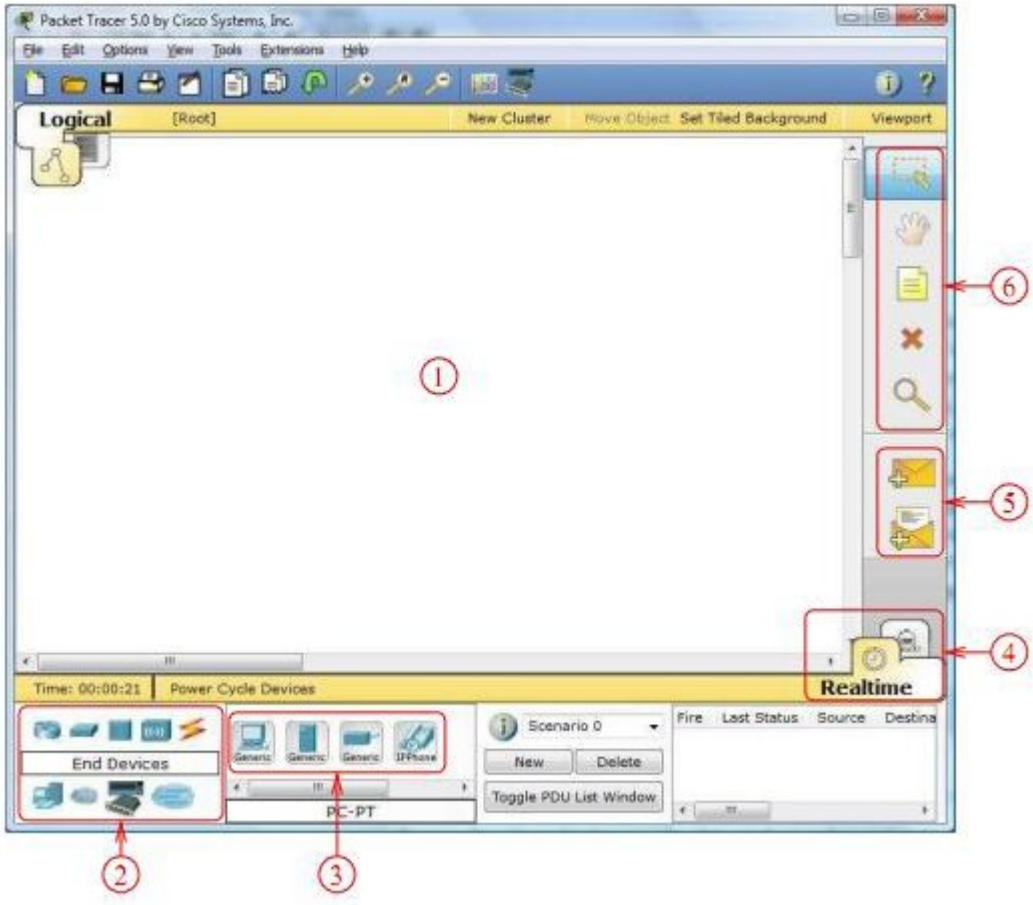


Figure 1 : l'interface du logiciel packet tracer

La zone (1) : est la partie dans laquelle le réseau est construit.les équipements sont regroupés en catégories accessible dans la zone (2).une fois la catégorie sélectionnée, le type d'équipement peut être transmis à la zone(3).la zone (4) permet de passer du mode temps réel au mode simulation.la zone (5) permet d'ajouter les indications dans le réseau. Enfin la zone (6) qui contient un ensemble d'outils :

Select : pour déplacer ou éditer les équipements.

Move Layout : permet de déplacer le plan de travail.

Place note : place des notes sur le réseau.

Delete : supprime un équipement ou une note.

Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage).

3. Construire un réseau

Pour construire un réseau l'utilisateur doit choisir parmi les 8 catégories proposées par packet tracer : les routeurs, les switchs, les hubs, les équipements sans fil, les connections, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin une connexion multi-utilisateurs. Lorsqu'une catégorie est selectionnée, l'utilisateur à alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi.

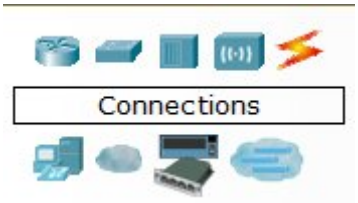


Figure2 : types d'équipements

Figure3 :les différentes connexion proposées

Pour relier deus équipements, il faut choisir la catégorie connections puis cliquer sur la connexion désirée.

4. **Configuration d'un équipement**

Lorsqu'un ordinateur a été ajouter, il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau.une nouvelle fenêtre s'ouvre comportant 3 onglets : physical (aperçu réel de la machine et de ses modules), config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur web).

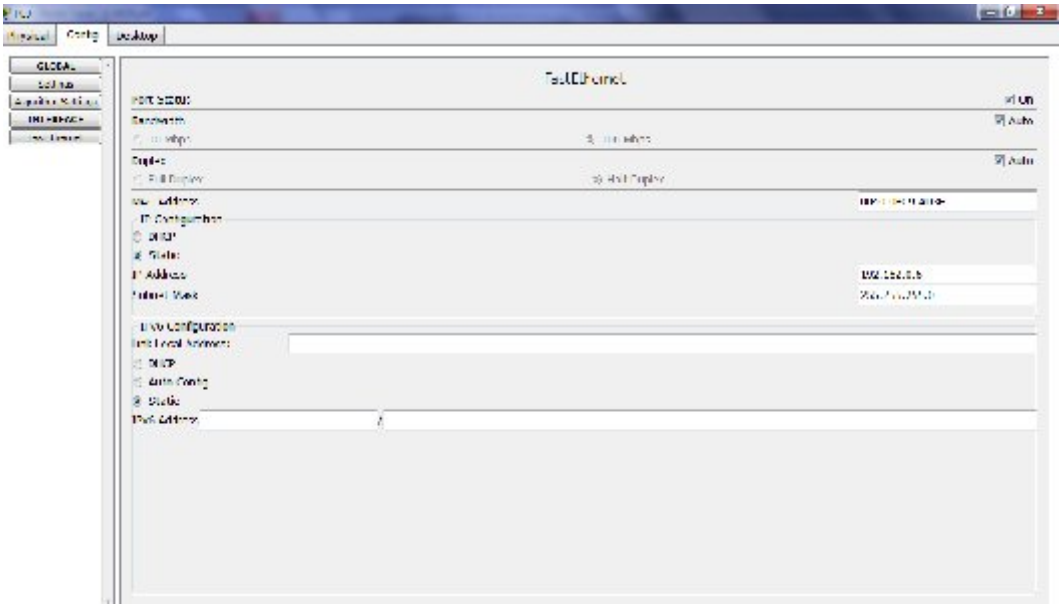


Figure 5 : configuration IP

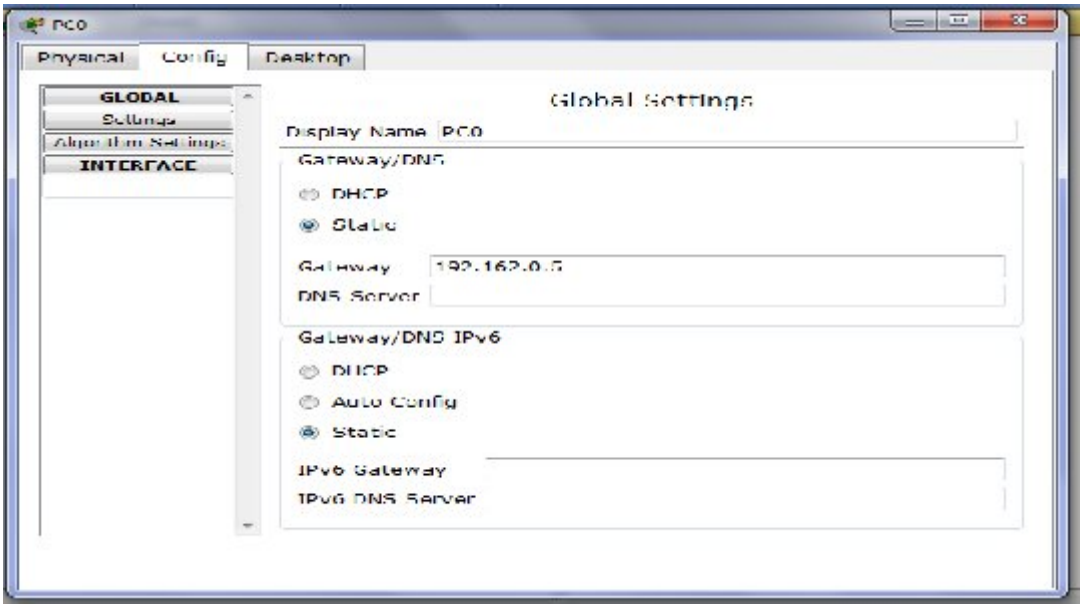


Figure 4 : configuration passerelle et DNS

Dans l'onglet config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquer pour cela sur le bouton Fast Ethernet en dessous du bouton INTERFACE).

5. Mode simulation

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindé en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles.

6. Invite de commandes

Il est possible d'ouvrir une invite de commande sur chaque ordinateur du réseau. Elle accessible depuis Desktop, lorsque nous cliquons sur un ordinateur pour le configurer (mode sélection).cet onglet contient un ensemble d'outils dont l'invite de commande (command prompt) est un navigateur internet (web browser).

L'invite de commande permet d'exécuter un ensemble de commandes relatives au réseau.

La liste est accessible en tapant help. En particulier les commandes Ping et ipconfig sont accessible.si packet tracer est en mode simulation, les messages échangées suite à un appel à la commande ping peuvent ainsi être visualisé.

Bibliographie

[1] Brieuc Jeunhomme, tout sur tunnel IPSEC, 2005

[2] Xavier Lagrange, Performances des réseaux cellulaires, 2000

[3] Étienne Sicard et Sonia Delmas-Benha, Une introduction au GSM, INSA Toulouse - 31077 Toulouse Cedex, Vol. 96 ,2002

[4] Bruno Salgues, les télécoms mobiles GSM-DCS,2ème édition, paris, 2000

[5] Ajay R.Mishra, cellular technologies for emerging markets: 2G, 3G and Beyond, first edition, 2010.

[6] Shahid K.Siddiqui, roaming in wireless network, 2006

[7] Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons ,2G1330 Mobile and Wireless Network Architectures, GSM, GPRS, 2001

[8]Zerihun Abate, GSM networks: protocols, terminology and implementation, artech house, 1998

[9]Arpege, Gestion de réseaux : concepts et outils, Masson, 1992.

[10]N. Simony et S. Znaty, Gestion de réseau et de service : similitude des concepts, spécificités des solutions, InterEditions, Masson, 1997.

[11] Eric Berthomier, Sécurité des Réseaux, Version 1.0.1, 2005

[12] Efort, Sécurité Mobile 2G, 3G et 4G: Concepts, Principes et Architectures, 2010

[13] http://jf.morreeuw.free.fr/security/a3a8.txt.

[14] Solange Ghernaouti-Helie, Sécurité internet, stratégies et technologies, dunod paris 2000

[15] Laurent Bloch, Christophe Wolfhuge, Sécurité informatique Principes et méthode à l'usage des DSI, RSSI et administrateurs 2ème édition, Paris ,2009

[16]D. Stinson, Wiley-Thomson, Cryptographie, théorie et pratique ,1996.

[17]Gilles Zémor, Cours de Cryptographie, CASSINI, 2000.

[18] Jean-Guillaume, Dumas Jean-Louis, Roch Éric, Tannier Sébastien, Varrette, Théorie des codes, Compression, cryptage,

[19] O'Reilly ,Electronic Frontier Foundation, Cracking DES, secrets of Encryption Research, Wiretap Politics and Chip Design , 1999.

[20]P.Barthélemy, R. Rolland, P.Véron, Cryptographie, Hermès Science 2005.

[21] http://www.ietf.org/html.charters/ipsec-charter.html

[22] Benjamin Dexheimer, Roland Dirlewanger, François Morris, Les réseaux privés virtuels. Tutoriel JRES 2003, Lille.

[23] Cyril Pain-Barre, Introduction aux réseaux et modèle OSI, 2009

[24] Jean-Pierre Lips, Réseaux Architecture TCP/IP, ,2009

[25] Jacques Savoy, Réseaux et Internet, 2001

[26] Guy Pujolle, Cours réseaux et télécoms Avec exercices corrigés 3ème édition, 2008

[27] Ghislaine Labouret, IPSEC : présentation technique, paris version 2000

[28] S. Kent, R. Atkinson, IP Authentication Header. November 1998.

[29] Stéphane Natkin, les protocoles de sécurité d'internet, dunod paris 2000

[30] Ghislaine Labouret, Network security with IPSec, 1999

[31] D.Piper.The Internet IP Security Domain of Interpretation for ISAKMP. November 1998.

[32] G.Labouret, Dynamic management of the IPSEC parameters: the IKE protocol, 1999

[33]S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, November 1998

[34] Encylopidie libre, »wikipédia », routeur, http : //www .wikipédia.com

[35] http://www.cisco.com/web/learning/netocad/index.html

[36] Tatouh Nejiba, Saida Djebbi, Sécurisation des routeurs Cisco, 2010

[37] Jean Robert HOUNTOMEY, Introduction aux routeurs CISCO, 2006

[38] Allan Lei wand and Bruce Pinsky, Cisco Router Configuration, Second Edition, 2001

[39] http://www.cisco.com/rout/Configuration_de_routeurs_Cisco.html

[40] Stéphane Gill, Le routage, 2004

[41]Pacon massol, Initiation au routage, 2ème partie, 2002 ;

[42] C. Madson, N.Doraswamy the ESP DES-CBC Cipher Algorithm, 1998.

[43] C. Madson, R. Glenn, the Use of HMAC-SHA-1-96 within ESP and AH. 1998.