République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté de Technologie
Département Automatique, Télécommunication et Électronique

Mémoire de fin d'étude
Pour l'obtention du Diplôme de Master Recherche
Spécialité
Télécommunication
Thème

Développement des Méthodes de Sécurité des Réseaux Mobiles

Réalisé par :
M^{lle} BOUCHOUCHA Lydia
M^{lle} TOUCHI Ibtissam

Soutenu devant le jury composé de :

Président	M^{r} ***BERRAH***
Promoteur	M^{r} ***KHIREDDINE*** **A/Karim**
Co-promotice	M^{me} ***MEZHOUD*** **Naima**
Examinateur	M^{r} ***SABI***

Promotion 2014/2015

REMERCIEMENT

*Louange à notre Seigneur **ALLAH** qui nous a dotés de la merveilleuse faculté de raisonnement. Louange à notre Créateur qui nous a incités à acquérir le savoir. C'est à lui que nous adressons toute notre gratitude.*

Ce travail n'aurait sans doute jamais eu lieu sans le concours volontaire ou involontaire de tous ceux qui nous ont formés, soutenus, encouragés et aidés.

A travers ce modeste travail, nous tenons à remercier vivement notre promoteur « M^{r} KHIREDDINE K.» pour toutes les commodités, les conseils judicieux, et la confiance qu'il nous a témoigné et aisances qu'il nous a apportés durant notre étude et la réalisation de ce projet.

Nous exprimons notre gratitude à notre co-promotrice « M^{me} MEZHOUD N.» pour la qualité de son encadrement, sa rigueur et sa disponibilité, ses remarques fructueuses et ses directives précieuses, qui ont contribué efficacement à l'avancement de ce travail.

Nous exprimons notre profonde gratitude à monsieur le président de jury et les membres des jury de nous avoir honoré en acceptant d'examiner et d'évaluer ce travail.

Nos remerciements les plus distingués s'adressent à «M^{r} CHALOUAH » enseignant à l'INSIM de BEJAIA qui nous aidé dans la mise en œuvre de notre partie pratique en fournissant les logiciels nécessaire à notre simulation et les conseilles directives.

Nos remerciements les plus vifs s'adressent aussi à «M^{r} BEKHOUCH » qui s'est totalement mis à notre disposition afin d'amener ce travail à bout durant notre stage à ATM de BEJAIA.

Nous remercions également « M^{r} OMAR M.» chef département Informatique à l'université de BEJAIA & « M^{r} BOUBKER S.» enseignant à l'université de BEJAIA ; pour leur conseilles et leur aide à la rédaction de ce mémoire.

DÉDICACES

Je rends grâce à dieu de m'avoir donné le courage et la volonté ainsi que la conscience d'avoir pu terminer mes études

Je dédie ce projet de fin d'étude, aux personnes qui me sont les plus chères :

A mes Parents pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance. Et pour leurs patiences, leurs soutien dans les moments les plus difficiles, partagé mes joies et mes peines, qui se sont toujours sacrifiés à mes dépends.

A mon Fiancé Hichem qui ma toujours encouragé pour allez de l'avant, aidé, soutenu dans mes réussites et mes défaites.

A mon Frère Sif et ma Sœur Kounouz pour leurs encouragements, amours et soutiens continus pendant toute ma formation.

A toute ma Famille, en particulier mes oncles Amokrane et Riad qui ont toujours été à mes cotés pour m'encourager et me conseiller le long de mon parcours, Sans oublié ma très chère cousine Kahina.

A la mémoire d'un être très cher à mon cœur qui a été mon exemple toute ma vie, et qui restera dans nos cœur à jamais mon oncle TIGHILT Djafer que ton âme repose en pais.

A mes amis(es) et collègues, spécialement ma très chère amie Loubna qui a toujours été à mes cotés et soutenue.

La vie n'est qu'un éclair, Et un jour de réussite est un jour très cher.

Lydia

DÉDICACES

Je dédie mon projet de fin d'études à toutes les personnes que j'aime :

À mon père qui a combattu toute sa vie pour me procurer tout ce d'ont j'avais besoin, celui qui m'a soutenu tout au long de mon parcours et qui était toujours un très bon exemple pour moi.

À ma mère qui m'a noyé avec ses sentiments, celle qui ma supportée, soutenu et encouragé le long de mon parcours et grâce à elle que j'ai trouvé le chemin de la réussite.

À ma très chère sœur « Sasa » qui a été toujours à mes coté surtout dans les moments les plus difficile pour me soutenir, encouragée et qui a toujours cru en moi.

À mes deux chèrs frères «Salah Et Mouloud » pour tout les précieux conseilles et l'aide qu'ils ont su me donner et qui m'ont permis d'arriver là où je suis.

À mes adorables sœur « Hassina Et Bania » qui ont toujours été derrière moi pour me guider dans la bonne direction.
À mes neveux Yanis, Silyane et Lina.

À la mémoire de mes chères grandes mères qui sont toujours dans mon cœur, que dieu le tout puissant l'accueille dans son vaste paradis.

À toute ma familles spécialement à les filles de mes tantes : Nassma, Nassima, loubna et bassma, Sans oublié ma chère Nadine que je considère comme ma sœur.

E nfin, mes dédicaces sont destinées à tous ceux que j'aime et qui m'ont soutenu, aidé, encouragé durant toute ma formation.

Ibtissam

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

ABRÉVIATION

3DES	Triple Data Encryption Standard
3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AGW	Access Gateway
AH	Authentication Header
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication and key Management Field
AMPS	Advanced Mobile Phone Service
AMRF	Accès Multiple par Répartition en Fréquence
AMRT	Accès Multiple par Répartition dans le Temps
APN	Access Point Name
ARP	Address resolution protocol
ASN	Access Service Network
AT	Access Terminal
ATM	Asynchronous Transfer Mode
AUC	AUthentification Center
AUTN	Authentication token
AV	Authentication Vector
BGP	Border Gateway Protocol
BSC	Base Station Controller
BTS	Base Transceiver Station
CA	Certificate Authority
CDMA	Code Division Multiple Access
CK	Cipher Key
CN	Core Network
CS	Circuit Switched
CSN	Connectivity Service Network
DDOS	Distributed Denial Of Service
DES	Data Encryption Standard
DNS	Domain Name System
DOS	Denial Of Service
EDGE	Enhanced Data rate for GSM Evolution
EIR	Equipment Identity Register
EK	Ephemeral Key
EPC	Evolved Packet Core
ESP	Encapsulation Security Payload
ETSI	Europeen Telecommunication Standard Institue
E-UTRAN	Evolved UMTS Terrestrial Radio Access Netwrok
FDD	Frequency Division Duplex

GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communication
HDLC	High-Level Data Link Control
HLR	Home Location Register
HMAC	Hached Message Authentification Code
IETF	Internet Engineering Task Force
IK	Integrity Key
IKE	Internet Key Exchange
IKi	Intermediary Key level 1
IMEI	International Mobile Equipment Identification
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version4
IPv6	Internet Protocol Version6
IS-95	Interim Standard 95
ISAKMP	Internet Security Association Key Management Protocol
ITU	Union International des Télécommunications
L2TP	Layer 2 Tunneling Protocol
LA	Location Area
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MAC	Message Authentication Code
MAP	Mobile Application Part
MAPSec	MAP Security
MCC	Mobile Country Code
MD5	Message Digest 5
ME	Mobile Equipement
MNC	Mobile Network Code
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Station Identification Number
MT	Mobile Termination
NAMPS	Narrowband Analogue Mobile Phone Service
NBAP	Node B Application Part
NMT	Nordic Mobile Téléphone

NSP	Network Service Provider
NSS	Network Sub System
NSS	Network Sub System
OMC-N	Centre d'exploitation et de maintenance réseau
OMC-R	Centre d'exploitation et de maintenance
OSI	Open Systems Interconnection
OSS	Operation Sub-System
PCU	Packet Control Unit
PDP	Packet Data Protocol
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PPTP	Point-to-point tunneling protocol
PS	Packet Switched
PSK	Phase-shift keying
RAB	Radio Access Bearer
RAND	Random number
RC4	Rivest Cipher 4
RES	Response
RNC	Radio Network Controller
RRC	Radio Ressource Control
RSA	Rivest, Shamir and Adleman
SA	Security Association
SCCP	Signalling Connection Control Part
SDLC	Synchronous Data Link Control
SEAL	Software Encryption Algorithm
SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm
SIM	Sucriber Identity Module
SK	Session Key
SQN	Sequence Number
SS7	Signalling System no. 7
SSH	Secure Shell
TACS	Total Access Communications System
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TDMA	Time division multiple access
TE	Terminal Equipement
TMSI	Temporary Mobile Subscriber Identity
TRAU	Transcoder and Rate Adapter Unit
TRC	TRansCoder

TTA	Telecommunications Technology Association
TTC	Telecommunications Technology Committee
UE	User Equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS Integrated Circuit Card
UMB	Ultra Mobile Broadband
USIM	UMTS Integrated Circuit Card
UTRA	UMTS Terrestrial Radio Access
UTRAN	Universal Terrestrial Radio Access Network
UUI	Unsecured ULE Information
VLAN	Virtual LAN
VLR	Visitor Location Register
VLS	Vendor Specific Location Server
VPN	Virtual Private Network
VRID	Virtual Router Redundancy Protocol
VRRP	Virtual Router Redundancy Protocol
WCDMA	Wideband Code Distributed Multiple Access
WiMAX	Worldwide Interoperability for Microwave Access
XRES	Expected Response

INTRODUCTION GÉNÉRALE

La communication est l'une des richesses les plus fondamentales de toute société organisée. Pour cela, les télécommunications ont subit en l'espace de deux décennies des évolutions et bouleversements profonds. Dans le panorama des systèmes de télécommunications, les réseaux mobiles ont connu un essor sans précédent ces dernières années en termes de recherche, investissements, de revenus et d'abonnées.

Il s'agit d'une part du déploiement de plusieurs générations successives des réseaux de télécommunications, essentiellement dédiés à la téléphonie puis plus orienté vers le multimédia.

Afin de permettre une compatibilité et la création de ces nouveaux services multimédias et d'offrir aux usagers une itinérance à l'échelle mondiale. Il est devenu nécessaire d'effectuer un saut technologique et de franchir le pas vers un premier réseau mobile basé sur la commutation de paquets qui est le réseau de troisième génération spécifiquement le réseau UMTS.

L'introduction des technologies UMTS qui offrent à l'usager une panoplie de services non seulement la voix, mais aussi le transport de données et principalement l'accès au réseau internet ou de manière générale, les réseaux TCP/IP.

Le réseau mondial TCP/IP qui est devenu le moyen le plus adéquat pour accéder et diffuser l'information et divers applications ont permis aux réseaux mobiles de transmettre des données à des distances lointaines à l'importe quel endroit, à tout moment.

L'inconvénient majeur qu'on rencontre dans ce type de réseau est que les données transmises sont soumise à des attaques telles l'écoute des paquets IP sur le réseau mobile.

La sécurité des réseaux mobiles est vaste, car elle englobe celui de l'accès radio, de l'infrastructure des réseaux, des terminaux, et des applications. La solution de sécurité est mise en œuvre par la réalisation des différents mécanismes et fonctions de sécurité jusqu'à la création d'un réseau privée virtuel.

Un VPN est une liaison pour une transmission des données sécurisé entre deux sites distants via le réseau IP et cela grâce à un principe de tunneling. Il existe plusieurs protocoles de sécurité pour la mise en œuvre d'un VPN, on se focalise sur le protocole IPSecurity.

Dans ce contexte l'objectif de notre mémoire, se base sur la mise en œuvre de la sécurité d'un réseau mobile et de définir une architecture qui permet à des clients fixes et mobiles de transmettre leurs données en toute sécurité via le réseau internet. Cette suggestion, est mise en

œuvre en utilisant le tunnel VPN sous le protocole IPSec.

La répartition de notre mémoire suit la logique suivante :

Le premier chapitre sera consacré à la présentation des différentes normes (générations) des réseaux mobiles. Il constitue la base nécessaire à la compréhension des évolutions des réseaux cellulaires de la première à la cinquième génération, en mettant l'accent sur le réseau de troisième génération qui est le sujet de notre projet.

Le second chapitre est dédié à la manière dont les réseaux mobiles (2G & 3G) sont sécurisés. On a abordé les différents mécanismes et procédures de sécurité pour remédier à des différentes attaques sur les réseaux mobiles.

Le troisième chapitre concerne l'étude de la transmission de données dans le domaine de commutation de paquet du réseau UMTS, et les attaques informatiques que subissent ces dernières, lors de sa connexion à ce réseau. A fin de remédier à ces risques, on a présenté une gestion de protection stratégique basé sur la réalisation d'un réseau privé virtuel en utilisant un protocole internet sécurisé IPSecurity.

Le quatrième chapitre présente l'architecture du réseau UMTS lorsqu'on est connecté au réseau TCP/IP et les attaques qui peuvent être fatal pour les entreprises connectées à ce réseau. Pour remédier à ce fait, on a simulé notre solution en utilisant un simulateur PACKET TRACER. Ce dernier, nous a permis la mise en œuvre d'un VPN sous le protocole IPSec.

On termine par une conclusion générale et des perspectives.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX MOBILES

1.1 Introduction :

Les réseaux hertziens concernent l'ensemble des systèmes de communication qui utilisent les voies hertziennes. Ces réseaux se présentent sous forme de réseaux cellulaires, c'est-à-dire d'un ensemble de zones géographiques, appelées cellules, avec des antennes situées au centre.

Les réseaux mobiles font partie de la famille des réseaux hertziens cellulaires, en permettant le passage d'une cellule à une autre sans couper la communication. Les communications entre les utilisateurs mobiles se développent rapidement et représentent un énorme marché pour cette décennie.

Cinq générations de réseaux mobiles se sont succédées, qui se distinguent par la nature de la communication transportée :

1G :communication analogique ;
2G :communication numérique sous forme de circuit ;
3G :communication sous forme de paquet ; sauf pour la parole ;
4G :communication multimédia sous forme de paquet de haut débit ;
5G :communication multimédia et service du Cloud [1] .

Dans ce chapitre, nous expliquerons brièvement les caractéristiques de chaque générations et éventuellement leurs architectures. Neaumoin, le réseau UMTS sera detaillé puisqu'il est le sujet principale de notre étude.

1.2 Evolution des réseaux mobiles :

1.2.1 Réseaux de première génération 1G :

Les réseaux mobiles de première génération, qui font appel à la transmission analogique des communications vocales, ont été constituées d'appareils relativement volumineux.
Les standards utilisés pour cette génération sont les suivants [2] :

- Le service téléphonique mobile avancé AMPS a recours à la technique AMRF dans la bande de fréquences des 800-900MHz (et depuis peu dans la bande des 1800-2000MHz).
- Le service téléphonique mobile analogique à bande étroite NAMPS, qui permet de coupler le traitement vocal avec la signalisation numérique, ce qui multiplie par trois sa capacité.
- Le système téléphonique mobile nordique NMT fonctionne au début dans la bande des 450MHz puis dans la bande des 900MHz par suite de contraintes en matière de capacité.
- Le système de communication à accès total TACS a été conçu à partir du système AMPS pour fonctionner à la fois dans la bande des 800MHz et dans celle des 900MHz.D'autres parties de la bande des 900MHz sont souvent utilisées pour la version dite étendue (ETACS).

1.2.2 Réseaux de deuxième génération 2G :

1.2.2.1 GSM (Global System for Mobile) :

Présentation :

GSM est la première norme de la téléphonie cellulaire qui est pleinement numérique [1]. C'est la référence mondiale pour les systèmes radio mobiles. Le réseau GSM offre à ses abonnés des services qui permettent la communication de stations mobiles de bout en bout à travers le réseau.

La téléphonie numérique améliore également la sécurité des transmissions de la voix qui est le service le plus important du GSM et des données à faibles débits.

Le système GSM fait appel à la technique TDMA et fonctionne dans les bandes de fréquences des 900, 1800 et 1900 MHz [3].

Architecture du réseau GSM :

L'architecture du réseau GSM (cf.Figure 1.1) est divisée en quatre sous ensembles[3] :

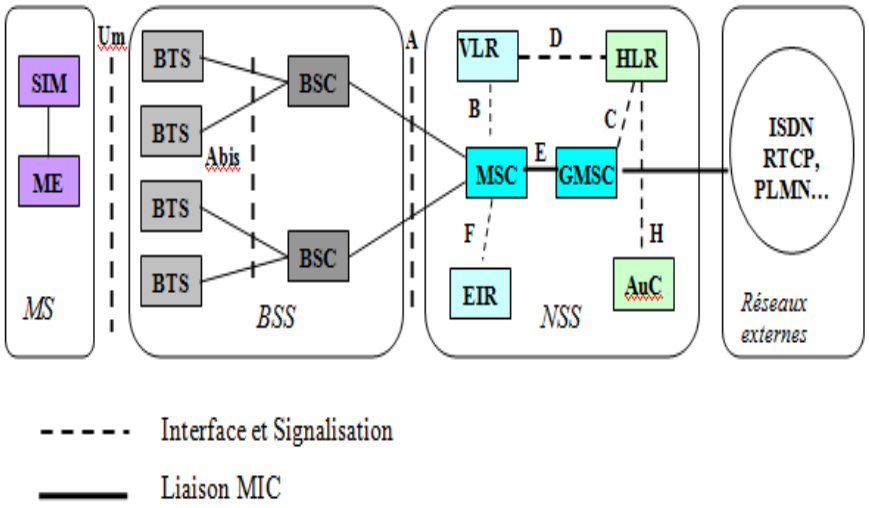

FIGURE 1.1 – Architecture du réseau GSM

1. Sous système radio BSS :

   C'est l'ensemble des constituants du réseau d'accès qui gère l'échange et la transmission des données par voie hertzienne.Le BSS est principalement constitué de deux éléments [4] :
   - La station de base BTS : c'est l'équipement de transmission radio du réseau GSM.
   - Le contrôleur de stations de base BSC : c'est un équipement qui peut contrôler une ou plusieurs BTS.
2. Sous système réseau NSS :

   Le NSS est constitué de commutateurs et des bases de données des utilisateurs qui sont :

- Commutateur de service mobile MSC : Ce commutateur gére la gestion des appels et tout ce qui est lié à l'identité des abonnés,leur enregistrement et leur localisation.
- Commutateur d'entrée de service mobile GMSC : Ce commutateur est chargé d'acheminer les appels du réseau fixe à un usager GSM.
- Registre des abonnés locaux HLR : est une base de données contenant les informations relatives aux abonnés gérer par l'opérateur.
- Registre des abonnés visiteurs VLR : est une base de données temporaire des informations liée aux abonnés visiteurs.
- le centre d'authentification AUC : mémorise pour chaque abonné une clé secrète dite IMSI de l'abonné utilisée pour authentifier les demandes de services et assure le chiffrement de la communication.
- Registre d'identification d'équipement EIR : c'est une base de données annexe contenant les identités des terminaux (IMEI).

3. Sous-système d'exploitation et de maintenance OSS :
   Les éléments constituants les deux sous réseaux précédent sont reliés à distance, via X25, au centre d'exploitation et de maintenance. Dans un réseau GSM, l'OSS comporte un OMC-R et un OMC-N.
4. La station mobile :
   La station mobile désigne un terminal équipé d'une carte SIM. Chaque terminal reste muni d'une identité particulière IMEI.

Les interfaces GSM :

Un certain nombre d'interfaces ont été normalisées pour le réseau GSM par l'ETSI. Chaque interface désignée par une lettre, comme il est indiqué dans le tableau 1.1 [5] :

Interfaces	Equipements	Protocoles	fonction
A	MSC-BSC	SS7	Etablissement et libération des communications
Abis	BSC-BTS	LAPD	Activation et désactivation des ressources radio
B	MSC-VLR	MAP	Echange de mise à jour de LA
C	MSC-HLR	MAP	Intérogation d'un HLR pour joindre un abonné mobile
E	MSC-MSC	SS7	Gestion de Handover
F	MSC-EIR	MAP	Vérification de l'identité du términal
H	HLR-AUC	MAP	Echange des informations de chiffrement et d'authentification
Um(radio)	BTS-MS	LAPDm	Gére les communications entre le mobile et les BTS

TABLE 1.1 – Interfaces du réseau GSM

1.2.2.2 GPRS(General Packet Radio Service) :

Présentation :

Le GPRS représente une évolution majeure du GSM. Par l'utilisation de la commutation de paquets et l'augmentation des débits [6]. Il ouvre la porte aux applications mobiles multimédias et il permet la transition en douceur vers la troisième génération.

Le GPRS a la possibilité d'allouer 8 times slots d'une porteuse GSM à un instant donné à un utilisateur, ce qui lui permet d'afficher un débit crête de 8 x 21.4 kbit/s soit 171.2 kbit/s [7], moyennant l'utilisation d'un codage canal défini spécialement pour ce service.

Architecture du réseau GPRS :

Le réseau GPRS et le réseau GSM fonctionnent en parallèle (cf.Figure 1.2), le premier est utilisé pour le transport des données, et le second pour les services de la voix. Tous les deux utilisent les mêmes équipements BSS.

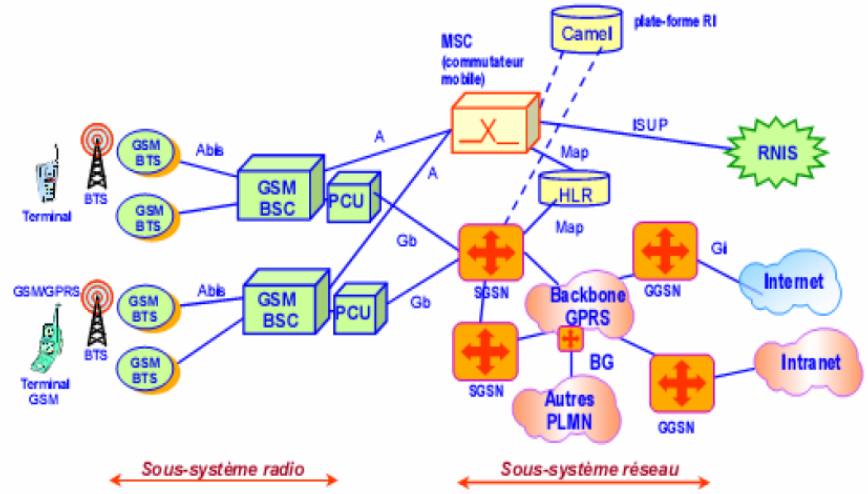

FIGURE 1.2 – Architecture du réseau GPRS

Les éléments propres au GPRS sont :

- Le SGSN est un routeur de paquets relié à un ou plusieurs BSS.
- Le GGSN est un routeur de paquets relié à un ou plusieurs réseaux de données.
- Le PCU assure la compatibilité entre la transmission de données en mode paquets et la transmission radio GSM.

1.2.2.3 EDGE (Enhanced Data rate for GSM Evolution) :

EDGE permet à ces utilisateurs favorisés de bénéficier des transmissions plus efficaces, en augmentant le trafic offert dans la cellule. Il permet d'affranchir cette limite, moyennant

l'introduction d'une nouvelle modulation (8PSK) [8], de nouveaux schémas de codage et la généralisation du principe de l'adaptation de lien (link adaptation).

La norme EDGE propose des débits presque trois fois plus important que le GPRS ; allant jusqu'à 43.2 kbit/s par time slot GSM [4].

EDGE et le GPRS (cf.Figure 1.3) permettent ensemble de « doper » le réseau GSM/GPRS afin d'offrir à l'utilisateur les moyens de transmettre des données à des débits très loin des 9,6 kbit/s du GSM (jusqu'à 384 Kbit/s).

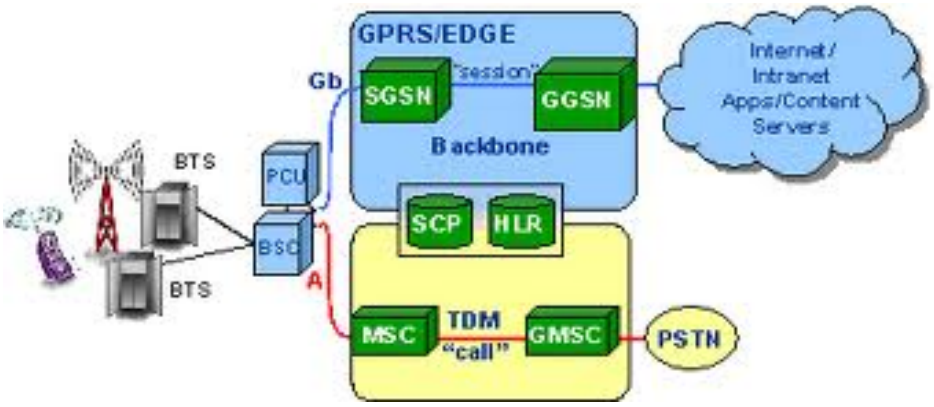

FIGURE 1.3 – Architecture du réseau EDGE

1.2.3 Réseaux de troisième génération 3G :

Les systèmes de télécommunications mobiles de troisième génération fournissent toute une gamme de services de télécommunications aux utilisateurs fixes et mobiles, situés dans une variété d'environnements autour de la bande de fréquences de 2 GHz.Elle améliore les réseaux précédents par une qualité du service rendu au moins comparable à celle fournie par les réseaux fixes.

Un autre objectif des réseaux de troisième génération est de rendre les services fixes et mobiles compatibles pour former un service transparent de bout en bout pour les utilisateurs.

L'UMTS n'est qu'une des cinq normes de la famille IMT 2000,où il est applé le WCDMA-2OOO.

1.2.3.1 Etude du réseau UMTS :

Présentation :

L'UMTS représente une évolution dans les services et les vitesses de transfert de la deuxième génération à la troisième génération[9]. Elle constitue une voie royal pour le développement des produits et des services multimédias.

En parallèle au développement de l'internet qui propose désormais des services spécialisés (e-banking, achat, jeux, information diverse), les opérateurs, poussés par cette vague, mettent en place des services permettant l'accès à ce nouveau média par l'intermédiaire de la téléphonie mobile.

Cependant de nouveaux protocoles plus performants sont indispensables pour proposer une nouvelle gamme de services à haut débit allant de l'Internet au téléchargement de musique ou de film. C'est ce qu'apporte l'UMTS.

Architecture matérielle du réseau UMTS :

L'architecture générale d'un réseau UMTS(cf. Figure 1.4) est composée de trois domaines qui sont reliés par des interfaces tel que Uu et Iu [7].

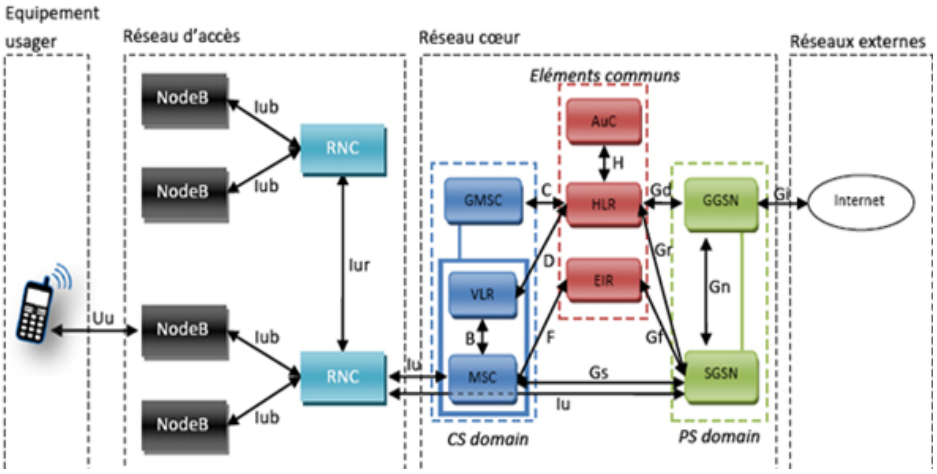

FIGURE 1.4 – Architecture du réseau UMTS

Les trois domaines sont définits comme suit :

Domaine de l'équipement de l'usager UE :

L' équipement usager (cf. Figure 1.5) est utilisé pour désigner la station mobile dans un réseau UMTS.Il est assuré par :

- L'équipement mobile ME : est chargé de la transmission radio et des procédures associées sur l'interface radio Uu. Il est encore divisé en deux parties [9] :
  La terminaison mobile (MT) assure la transmission de l'information vers le réseau UMTS à travers l'interface radio et il est utilisé comme modem. L'equipement Terminal(TE) qui peut être par exemple, un ordinateur portable.
- USIM : C'est une application qui permet à l'abonné d'accéder aux services souscrits [9]. Elle gère également les informations associées à la souscription de l'abonné, les procédures d'authentification et de chiffrement. L'USIM réside dans une carte à puce (smart card) appelée UICC.

  Des informations permettent l'identification de l'UICC sont :

- Le répertoire des applications ;
- L'IMSI qui permet au réseau d'identifier l'abonné de manière unique. Ce numéro n'est pas connu de l'utilisateur.
- le(s) MSISDN(s) ;
- Les clés de chiffrement.

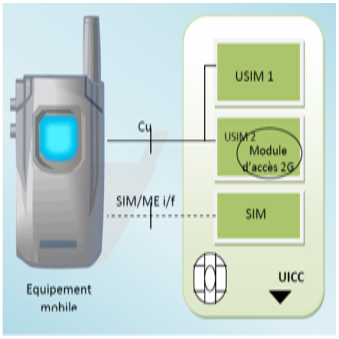

FIGURE 1.5 – La structure de l'équipement usager

Domaine du réseau d'accès UTRAN :

Le réseau d'accès UTRAN (cf. Figure 1.6) est doté de plusieurs fonctionnalités (Sécurité, Mobilité, Gestion des ressources radio, Synchronisation).Sa fonction principale est le transfére des données générées par l'usager.

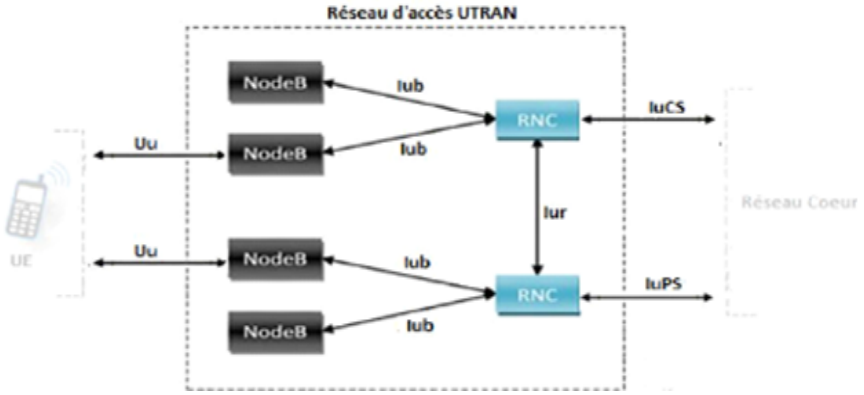

FIGURE 1.6 – Architecture de l'UTRAN

Il est composé de deux entités [10] liées à travers des interfaces de communication :

- Node B :
  Le Node B est un ensemble de stations de base et de contrôleur de site qui sont chargés de gérer la macro-diversité. Chaque station de base gère une cellule ou plusieurs cellules

[11] (cf. Figure 1.7) . Son rôle principal est d'assurer les fonctions de réception et de transmission radio pour une ou plusieurs cellules du réseau d'accès de l'UMTS.

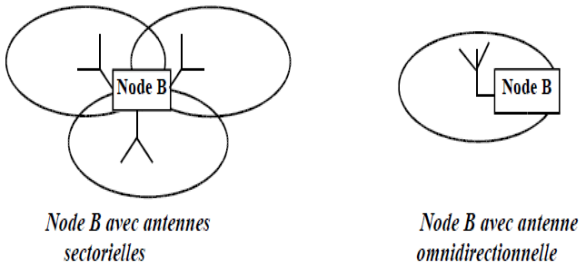

FIGURE 1.7 – Implémentation possible du Node B

– RNC :
Le RNC est un contrôleur de Node B qui est l'équivalant du BSC dans le réseau GSM.Comme il s'interface avec le réseau pour la transmission en mode paquet et en mode circuit.
Son rôle principal est le routage des communications entre les NodeBs et gère les ressources radio en utilisant le protocole RRC. Il peut avoir deux modes de fonctionnement [2] (cf. Figure 1.8) :
Le Serving RNC (SRNC) : permet de gérer la signalisation associée, prendre les décisions de handover, gérer le contrôle de puissance...
Le Drift RNC (DRNC) : permet de gérer d'autres cellules extérieures au SRNC également utilisées par le mobile, et de transférer les données de manière transparente entre le mobile et le SRNC.

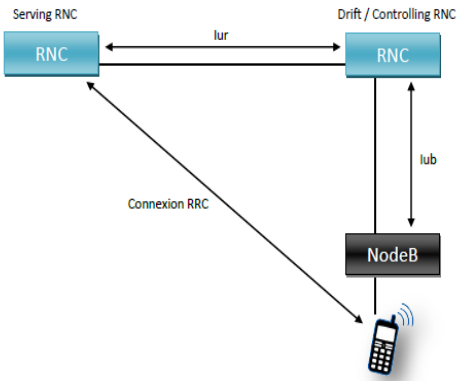

FIGURE 1.8 – Représentation graphique de l'exemple de communication

Le contrôle de la mobilité par le handover :

Les réseaux WCDMA utilisent une technique de handover différente que celle du GSM. Elle est appelée soft handover (cf. figure 1.9).

FIGURE 1.9 – Le soft handover dans le réseau UMTS

Les procédures suivirent durant le soft hadover (cf. Figure 1.10) :

- Si le mobile se trouve dans une zone de couverture commune à deux secteurs adjacente d'un même node B, les communications empruntent simultanément deux canaux radioélectriques.
- Si le mobile se trouve dans une zone de couverture commune à deux nodes B :
  Dans le sens montant, le signal transmis par le mobile, utilisant le code de brouillage C_s, est reçu par déférents NodeB pour être ensuite retransmis vers le SRNC. Ce dernier attribut la ressource radioélectrique et procéde à la sélection entre les deux signaux provenant du node B et du DRNC, qui effectue un transit sur l'interface Iu_r.
  Dans le sens descendant, les NodeB engagent le soft handover de transmettre simultanément les mêmes informations usager en direction du mobile. Chaque NodeB utilise les codes de brouillage C_{s1}, C_{s2} propres à chaque cellule.

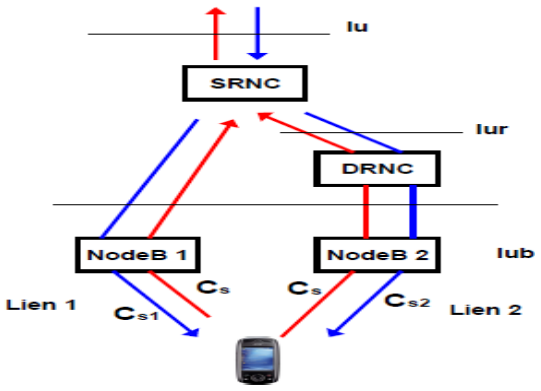

FIGURE 1.10 – Les liens radio entre le réseau et le mobile

Domaine du réseau cœur : CN

Le réseau cœur est la partie du système chargée de la gestion des appels. Il permet aux abonnées de communiquer à l'intérieur d'un même réseau de la téléphonie mobile. Il

assure l'interconnexion de ce dernier avec des réseaux externes, fixes ou mobiles. Il fournit les logiciels d'applications qui permet, tout en garantissant la sécurité des échanges, le maintien de la communication, même lorsque l'utilisateur est itinérant.

L'architecture du réseau cœur de l'UMTS (cf.Figure1.2.2.1) est constituée des élements et des interfaces comme suit[8] :

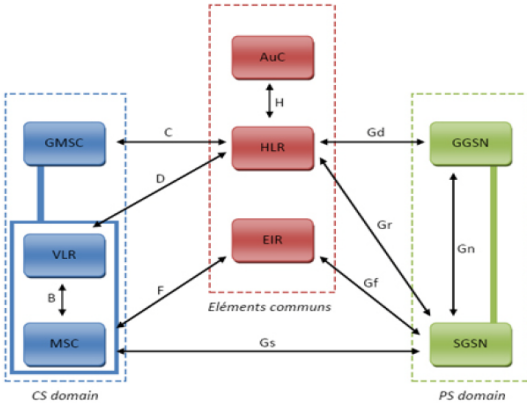

FIGURE 1.11 – Architecture du réseau cœur

- Le domaine CS :comprend tous les services liés à la téléphonie. Il est assuré par les equipements suivants : le MSC et le VLR, qui réalisent les mêmes fonctions que dans le GSM.
- Le domaine PS :comprend tous les services liés à la commutation de paquets. Ces services sont assuré par :
  Le SGSN : c'est un commutateur de données et de signalisation.
  Le GGSN : il joue le rôle d'une passerelle vers les réseaux à commutation de paquets extérieurs (Internet public, un intranet privé, etc..).
- Les éléments communs :
  Le réseau UMTS utilise les équipements du sous systéme réseau (NSS) du réseau GSM pour gérer ces bases de données qui sont le HLR, AuC et l'EIR.
- Les interfaces de communication du réseau cœur :
  Plusieurs types d'interfaces de communication coexistent au sein du réseau UMTS. Elles sont présentées dans le tableau 1.2 :

Intérfaces	Extrémités	Fonctions
C	GMSC-HLR	Informations sur les abonnés lors d'une communication entrante
D	VLR-HLR	Authentification et mise à jour de localisation
F	MSC-EIR	Vérifier que l'UE n'est pas dans la liste noire
Gf	SGSN-EIR	Verifier l'identité du terminal
Gr	SGSN-HLR	Authentification et mise à jour de localisation
Gd	GGSN-HLR	Information sur les abonnés lors d'une communication entrante
B	MSC-VLR	Recherche des identificateurs et localisation des abonnés
Gs	MSC-SGSN	Interaction des domaines PS et CS
Gn	GGSN-réseau externe	Routage des paquets vers les réseaux externes

TABLE 1.2 – Interfaces du réseau cœur de l'UMTS

Les différentes interfaces ouvertes disponibles : Les interfaces ouvertes permettent d'avoir une connexion entre les différents élements du réseau (cf.Tableau 1.3)

Intérfaces	Localisation	Fonctions
Uu	UE-UTRAN	Accéder à la partie fixe du système
Iu_{CS}	UTRAN-CN	Etablissement/Libération des communications
Iu_{PS}	UTRAN-CN	Transport des données
Iu_r	RNC-RNC	Soft handover/Gestion des ressources
Iub	Node B-RNC	Contrôle/Transmission du trafic
C_u	USIM-Terminal	Gestion de fichier/Echange de donnée/Commande de sécurité

TABLE 1.3 – Interfaces ouvertes du réseau UMTS

Organisation fréquentiel du réseau UMTS :
Les bandes de fréquences allouées pour l'IMT 2000 sont 1885-2025 MHz et 2110-2200 MHz (cf.Figure1.12) :

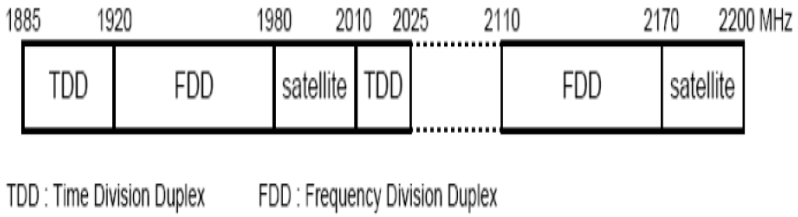

FIGURE 1.12 – Allocation fréquentielle en UMTS

Organisation temporelle du réseau UMTS :

L'organisation temporelle du réseau UMTS (cf.Figure1.13) est basée sur une super-trame de 720 ms, comportant elle-même 72 trames de 10 ms. Chaque trame de 10 ms est divisée en 15 slots de 667 µs.

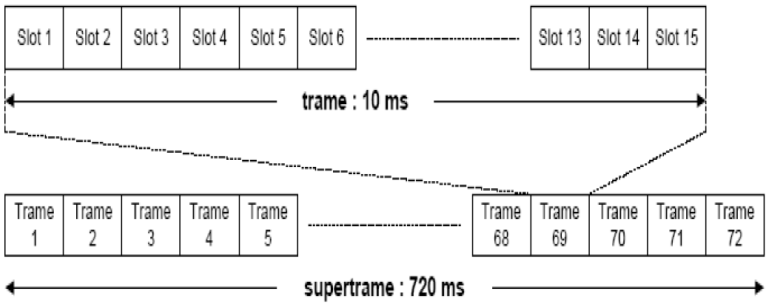

FIGURE 1.13 – Structure de trame de l'UMTS

Le duplexage dans le réseau UMTS :

Dans la norme UMTS, on distingue deux voies de communication entre l'UE et la station de base (le Node B) (cf.Figure 1.14) :

- la voie montante ou UL (Up Link), où l'UE transmet vers la station de base.
- la voie descendante ou DL (Down Link), où la station de base transmet vers l'UE.

La norme UMTS propose deux techniques pour la gestion de ces deux voies à savoir : le duplexe fréquentiel FDD et le duplexe temporel TDD.

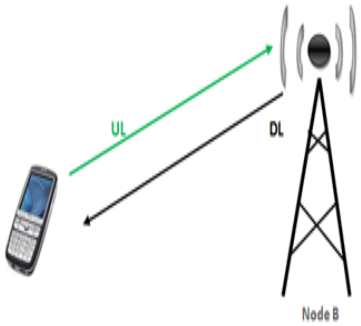

FIGURE 1.14 – Duplexage dans l'UMTS

Architecture en couches de l'UMTS :

L'architecture en couches du réseau UMTS (cf.Figure 1.15) est basée sur l'interface radio, qui s'est faite à l'aide d'une pile de protocoles classées en 3 couches correspondantes aux couches du modèle OSI.

La couche physique :

Elle réalise les fonctions de bas niveau de traitement radio fréquence, de codage, d'étalement de spéctre, de brouillage, de contrôle de puissance, de synchronisation et d'exécution du soft-handover.

La couche liaison de données :

Elle assure le passage des canaux logiques utilisés dans les couches superieures aux canaux physiques à travers des sous-couches suivantes :

- La couche MAC :permet le multiplixage de plusieurs flux sur un même canal de tranport [7]qui peuvent concerner le même utilisateur ou différents utilisateurs.
- La couche RLC :Elle fournit le service de transfert de donnée, de contrôle et du trafic entre le mobile et le RNC [5].

La couche accès réseau :

Elle est constituée de trois couches [12] qui sont definies comme suit :

- La couche PDCP : fournit le service de transfert des communications par paquets en s'appuyant sur des services offerts par la couche RLC.
- La couche BMC : assure du côté de l'UTRAN le service de diffusion de messages utilisateur sur l'interface radio. Du côté du mobile, elle assure la livraison des messages diffusés à l'utilisateur de la couche.
- La couche RRC : est «la tour de contrôle » de l'interface radio, elle gère la signalisation entre l'UTRAN et les mobiles.

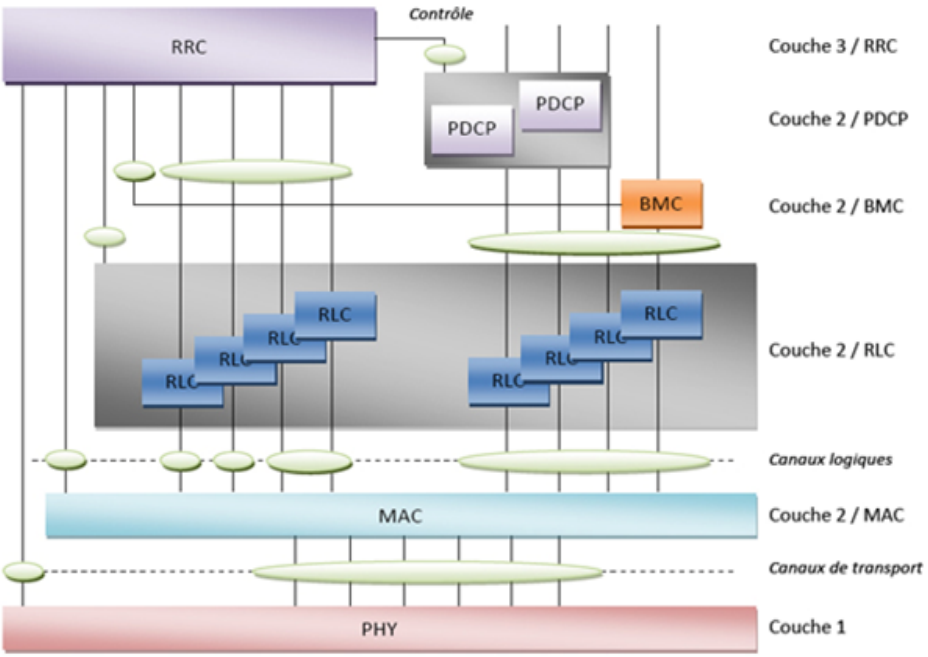

FIGURE 1.15 – Vue en couches de l'UMTS

La couverture de l'UMTS :

La couverture globale de l'UMTS (cf. Figure 1.16) s'organise en une structure cellulaire hiérarchisée qui assurera l'itinérance mondiale. Au sommet de la hiérarchie se trouve les satellites qui assurent une couverture sur l'ensemble de la planète.

Le réseau radio terrestre s'occupe de la couverture terrestre selon une répartition hiérarchisée pico, micro et macro-cellule. La composante satellitaire sert pour le roaming mondial et pour compléter la couverture assurée par l'UTRAN. Les pico-cellules sont conçus pour la couverture des bâtiments c'est-à-dire en environnement *indoor*, les microcellules pour les zones urbaines et suburbaines denses et les macro-cellules assurent la couverture en environnement rural.

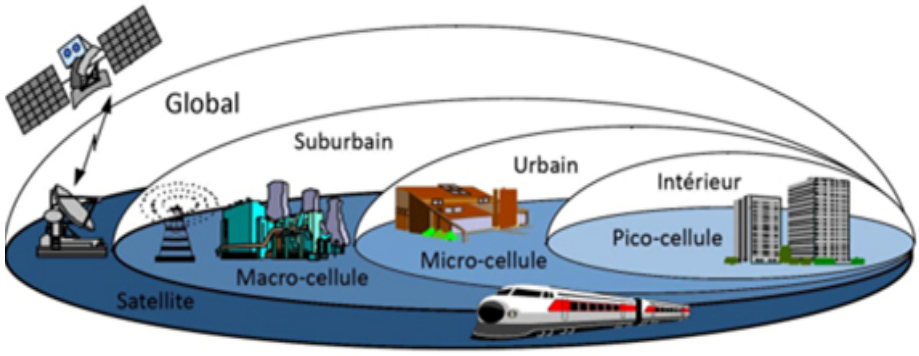

FIGURE 1.16 – Couverture de l'UMTS

1.2.4 Réseaux de quatrième génération 4 G :

La 4G vise à améliorer l'efficacité spectrale et la gestion du nombre de mobiles dans la même cellule. Elle vise à rendre le passage entre les réseaux transparent pour l'utilisateur en lui évitant l'interruption des services durant le transfert intercellulaire, et à basculer l'utilisation vers le tout-IP.

Les trois technologies supposées pour une validation 4G sont [13] :

- Long Term Evolution (LTE).
- WiMAX version 802.16m.
- Ultra Mobile Broadband (UMB) .

1.2.4.1 Long Term Evolution : LTE :

Présentation :

La technologie LTE, s'appuis sur un réseau de transport à commutation de paquet IP. Elle n'est pas prévue de mode d'acheminement pour la voix autre que la VoIP, contrairement à la 3G qui transporte la voix en mode circuit.

Les réseaux LTE sont des réseaux cellulaires constitués de milliers de cellules radio qui utilisent les mêmes fréquences hertziennes. Ces dernière ont une largeure pouvant varier de 1,4 MHz à 20 MHz, permettant ainsi d'obtenir un débit binaire théorique pouvant atteindre 300 Mbit/s en « downlink ».

Architecture du réseau LTE :

La technologie LTE est caractérisée par son architecture qui comporte les éléments suivants [13] (cf. Figure 1.17) :

- Le réseau d'accès E-UTRAN : La conception de ce réseau a connu l'intégration des stations eNode Bs avec des liaisons en fibre optique.
- Réseau Coeur EPC : Il utilise une technologie « *full IP* » c'est-à-dire basées sur les protocoles internet pour la signalisation.

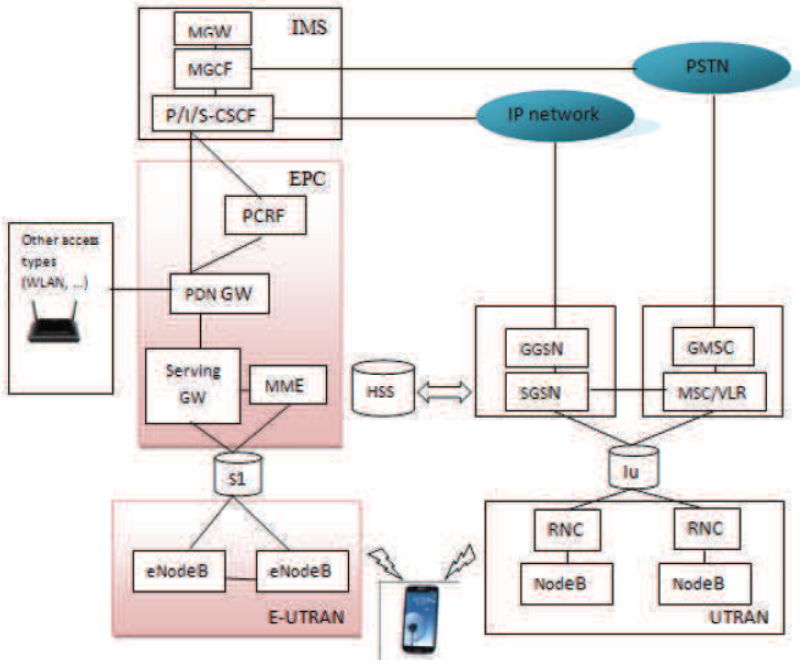

FIGURE 1.17 – Architecture du réseau LTE

1.2.4.2 Le WIMAX :

Présentation :

Le WiMAX est une solution hertzienne des réseaux WMAN. C'est une technologie qui permetd'aporter un haut débit par voie radio et une efficacité en termes de coût.

L'objectif du réseau WIMAX est de fournir une connexion Internet à haut débit sur une zone de couverture de plusieurs kilomètres. Il possède l'avantage de permettre une connexion sans fil entre une station de base et des milliers d'abonnés sans la nécessité des lignes visuelle directe.Il existe deux types de WIMAX : fixe et mobile [13].

Architecture du réseau WIMAX mobile :

La technologie WIMAX mobile (cf. Figure 1.18) est caractérisée par son architecture qui comporte les éléments suivants :

- Les BSs sont connéctés à un réseau appelé ASG-GW utilisé comme passerelle pour gérer le racordement des BSs avec le réseau IP, et assure l'interconnexion CSN.
- Les SSs sont des stations clients peuvent représenter un seul utilisateur, comme elles peuvent former un réseau sans fil ou filaire.
- Le sous système radio (ASN) : C'est le réseau d'accès radio du WIMAX, il regroupe un ou plusieurs passerelles et des stations de base BS. L'ASN assure la couverture radio et la gestion des fonctionnalités d'accès MAC.
- Le CSN : C'est un ensemble de fonctionnalités assurant la connectivité IP aux stations d'abonnés WIMAX. Il regroupe des passerelles pour l'accès Internet, des routeurs, des serveurs et des « proxy » de sécurité ainsi que des bases de données.

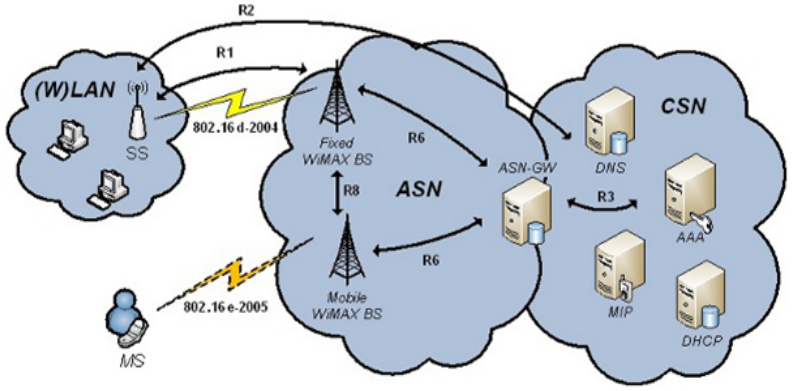

FIGURE 1.18 – Architecture du réseau WIMAX mobile

1.2.4.3 Réseau Ultra Mobile Broadband : UMB

Présentation :

L'UMB est le nom commercial de la prochaine version de la famille CDMA. Elle propose par l'évolution de ces versions qui se base sur l'amélioration des débits ; un réseau tout-IP et dispose des passerelles permettant l'interconnexion avec les réseaux de la famille 3GPP.

Architecture du réseau UMB :

Les éléments du réseau et les interfaces qui forment l'architecture de l'UMB sont (cf. Figure 1.19) :

- AT : c'est le périphérique sans fil compatible avec l'UMB.
- AGW : c'est un routeur qui présente le premier point de rattachement au réseau IP.
- SRNC : il est responsable du maintien de la référence de la session avec l'AT.

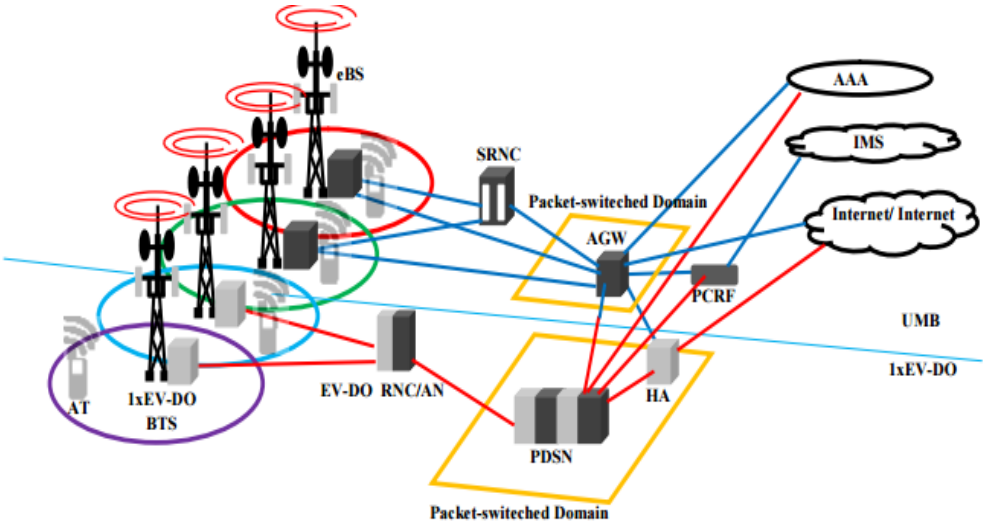

FIGURE 1.19 – Architecture du réseau UMB

1.2.5 Réseaux de cinquième génération 5G :

Ces derniers temps,on entend parler de la cinquième génération. Cette technologie de base a un but pas différente de la quatrième génération mais les différences sont architecturales qui sont définit comme suit [1] :

L'introduction de Cloud :

Il joue un rôle important pour prendre en charge le contrôles des réseaux mobiles. Il apporte une puissance de calculer et de récupérer l'information. Il permet aussi de prendre des décisions tenant compte d'un très grand nombre de paramètres. On peut parler du Cloud distribué ou local.

Utilisation fort de la virtualisation :

L'idée principale de la virtualisation est de partager des équipements du réseau entre plusieurs opérateurs et plus généralement entre les utilisateurs. Elle peut permettre la coexistence de réseaux hétérogène puisque les réseaux sont isolés les uns des autres.

Les plates formes d'altitude :

C'est la partie la plus visible de cette génération, car il utilise deux plates forme d'altitude :

- les plates forme à haute altitude, où on la trouve dans une position stratosphérique de l'ordre de 18 à 22 km dont la couverture se compte en centaine de kilomètre carrés.
- les plates formes de basse altitude peuvent se positionner de quelque dizaines de mètre de hauteur jusqu'à plusieurs kilomètres, la couverture étant de quelque kilomètres carrés.

  L'avantage de ces plates-formes provient d'une capacité de communication pouvant couvrir un million de personnes avec un haut débit et un matériel de l'ordre de 20

tonnes.

L'architecture du réseau de la cinquième génération est présentée sur la Figure 1.20 :

FIGURE 1.20 – Architecture de la cinquième génération

1.3 Conclusion :

On souhaite qu'à travers ce chapitre, on a arrivé à donner une vue générale sur l'évolution des générations des réseaux mobiles de la première à la cinquième génération.

On a spécifié notre étude sur le réseau de troisième génération l'UMTS, qui vient offrir un service de communication en mode circuit et en mode paquet, en se basant sur les réseaux GSM et GPRS. Les services offert par le réseau UMTS, permet de faire un pas géant vers un monde qui converge vers tous IP et les services multimédia.

Le réseau UMTS comme tous les réseaux mobiles, est soumis à des intrusions et des attaques au niveau du réseau et son infrastructure. A ce sujet vient la nécessité de protéger le réseau et les données transmises, en implémentant des algorithmes et des fonctions de sécurité. C'est ce qu'on développera dans le chapitre suivant.

CHAPITRE 2

LES MÉTHODES DE SÉCURITÉ DANS LES RÉSEAUX MOBILES

2.1 Généralités sur la sécurité des réseaux mobiles :

2.1.1 Introduction :

La sécurité est une fonction incontournable des réseaux mobiles. Elle consiste à éviter que des curieux puissent lire ou modifier les messages destinés à d'autre, ou des individus qui essaient d'utiliser des services en ligne auxquels ils ne sont pas autorisée à accéder. C'est pour cela qu'un ensemble des moyens sont mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

La sécurité a pour but d'assurer que les ressources matérielles et logicielles d'une organisation soient uniquement utilisées dans le cadre prévu.

Globalement, on peut deviser la sécurité en deux parties : la sécurité à l'ouverture de la session et la sécurité lors du transport de l'information.

2.1.2 Les objectifs de la sécurité :

Le terme «sécurité » recouvre des objectifs, qui sont définit comme suit[14] :

La confidentialité : est une exigence importante dans la sécurité du réseau. Elle permet d'assurer qu'une communication reste privée entre un émetteur et un destinataire. La cryptographie des données est la seule solution fiable pour assurer la confidentialité des données.

Authentification : consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être et permet un contrôle d'accès à des ressources uniquement aux personnes autorisées.

Non répudiation de l'information : est de garantir qu'aucun des correspondants ne pourra nier la transaction. Il permet par exemple de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.

Intégrité : c'est d'assurer qu'aucune modification n'a eu lieu entre l'émetteur et le destinataire au cours de la transmission. C'est un très bon complément à la confidentialité.

Disponibilité : est d'offrir une assurance aux entités autorisées d'accéder aux ressources réseaux avec une qualité de service adéquate et en toutes circonstances.

2.1.3 Les attaques dans les réseaux mobiles :

En raison de l'architecture massive d'un réseau cellulaire, il existe une variété d'attaques qui peuvent atteindre l'infrastructure d'un réseau ; qu'on peut définir comme suit :

– Deni de service (DOS) : C'est l'attaque la plus nocive qui peut réduire et nuire à l'infrastructure en entier. Ceci est provoqué par l'envoi des données excessives au

réseau. Plus le réseau peut manipuler ces données, il en résulte, que les utilisateurs ne pourront plus accéder aux ressources du réseau.

- Deni de service distribué (DDOS) : Il peut être difficile de lancer une attaque de DOS de large echelle à partir d'un centre d'un serveur simple. Un certain nombre de serveurs peuvent être utilisés pour lancer une attaque [15].

- Blocage de canal [15] : C'est une technique employée par les attaquants pour bloquer le canal de transmission sans fil et de nier l'accès à tous les utilisateurs légitimes dans le réseau.
- Accés non autorisée : Si une méthode d'authentification appropriée n'est pas déployée alors un attaquant peut gagner une liberté d'accès au réseau.

- Espionage des communications [15] : Si le trafic n'est pas chiffré, alors l'attaquant peut écouter et capter la communication. En suite, il va procéder à l'arrêt de la communication.

- Rejeu du message : Si la voie de transmission n'est pas sûre, un attaquant peut intercepter le message et le modifier puis le renvoyer à sa destination.

- Détournement de session : Un utilisateur malveillant peut détruire une session déjà établie et peut agir comme une station de base.

2.1.4 Politiques et mécanismes de sécurité :

Comme le but de la sécurité est la protection des informations échangées entre les sites distant et l'accès au réseau. Une politique de sécurité est définie et mise en place par un ensemble de règles qui doivent contrôler et assurer que seules les personnes autorisées ont accès à l'information. Parmi ces mécanismes, on peut citer :

2.1.4.1 Cryptographie / Chiffrement :

La cryptographie est la science d'écriture et de lecture de messages codés. En effet, elle joue un rôle essentiel dans toutes les communications sécurisées ; en chiffrant un message dit « texte clair » en un deuxième dit « texte crypté » à l'aide d'une clé et des algorithmes conçus à ce fait [16] (cf. Figure 2.1). Les textes originaux sont restitués à partir de ceux qui sont codées. Cette opération inverse est nommée décryptage/déchiffrement.

Il existe deux types de cryptographie :

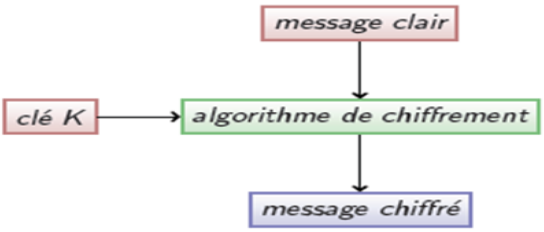

FIGURE 2.1 – Mécanisme de cryptographie

Cryptographie symétrique :

La cryptographie à clé secrète est basé sur une clé partagée entre les deux parties communicantes (cf.Figure 2.2).

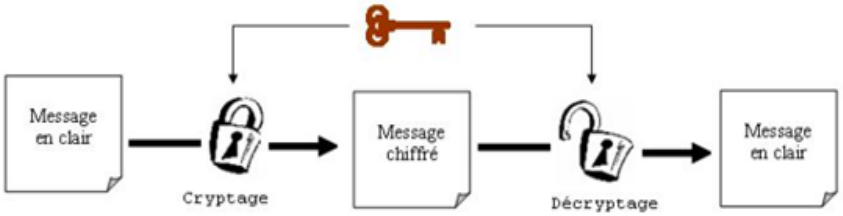

FIGURE 2.2 – Cryptographie symétrique

Cette même clé sert à crypter et décrypter les messages. Ces algorithmes peuvent être classés en deux types [16] :

– Le chiffrement symétrique par flot :
  Les algorithmes de chiffrement par flot, traitent les données bit par bit. Dans la plupart des cas, il s'agit d'un générateur de nombres pseudo-aléatoires, avec lequel une opération simple est effectuée entre sa sortie et le texte clair (cf. Figure 2.3). L'opération effectuée est généralement un XOR ou une addition modulo N. Elles sont considérées moins robustes, mais plus rapides que les algorithmes de chiffrement par bloc. L'algorithme le plus connu est le RC4 .

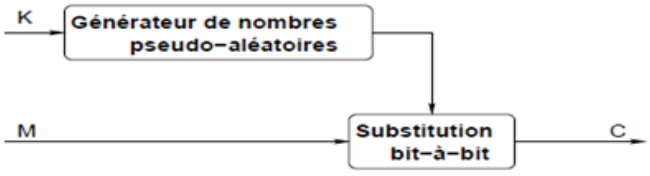

FIGURE 2.3 – Chiffrement symétrique par flot

– Le chiffrement symétrique par bloc :

Un algorithme de chiffrement par bloc (cf.Figure 2.4), décompose le texte clair en blocs de taille identique (64 bits, 128 bits) et chiffre les blocs les uns après les autres avec une clé secrète.

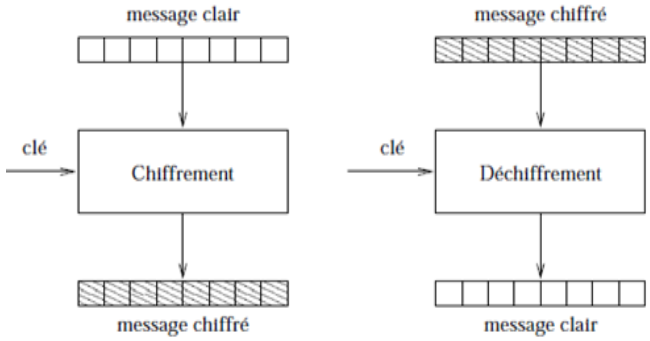

FIGURE 2.4 – Chiffrement / déchiffrement symétrique par bloc

Les algorithmes de chiffrement par bloc les plus connu sont :

L'algorithme DES : c'est une clé secrète utilisée pour chiffrer à l'émission et déchiffrer a la réception. Elle se base sur un algorithme de 56 bits (cf. Figure 2.5) ; travaillant sur des blocs de données de 64 bits à la fois et nécessite 16 étapes d'itérations.

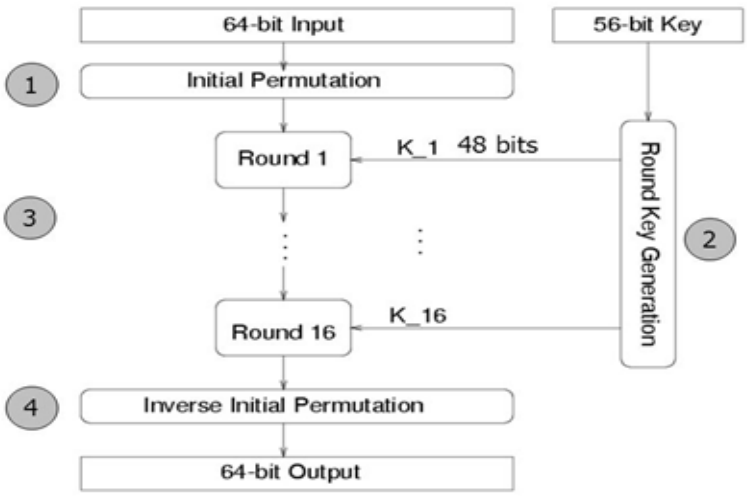

FIGURE 2.5 – L'algorithme DES

Le DES est remplacé par le triple DES qui travaille avec deux clés de 56 bits et effectue le chiffrement en trois phases(cf. Figure 2.6) :

– La première phase consiste à chiffrer les données avec la première clé ;
– La seconde phase effectue un déchiffrement avec la seconde clé ;
– La troisième phase effectue un nouveau chiffrement avec la première clé.

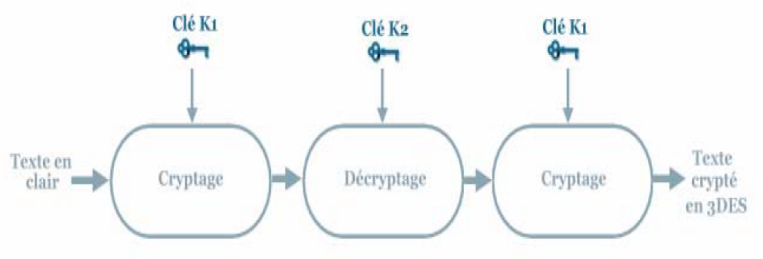

FIGURE 2.6 – L'algorithme de 3DES

*L'algorithme AES (Rijndael) :*c'est un algorithme qui opère sur des blocs de texte de 128 bits, trois tailles de clés sont possibles 128, 192 et 256 bits. Pour une clef de 128 bits, l'AES effectue 10 itérations d'une fonction.

La cryptographie asymétrique :

La cryptographie asymétrique (cf. Figure 2.7) est basée sur deux clés différentes qui sont générées par le récepteur[16] :

– une clé publique diffusée à tous les nœuds servant au chiffrement de données qu'ils vont émettre au récepteur.
– une clé privée maintenue secrète chez le récepteur servant pour le déchiffrement de ces données à la réception.

Le point fondamental sur lequel repose la sécurité du chiffrement asymétrique est l'impossibilité de déduire la clé privée à partir de la clé publique. Lesalgorithme de chiffrement asymétrique les plus connus sont :DH et RSA [16].

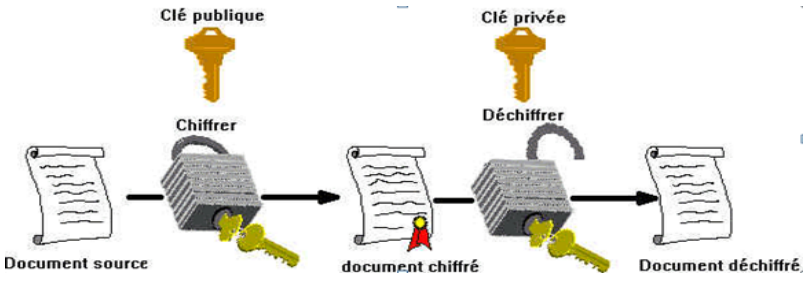

FIGURE 2.7 – Cryptographie asymétrique

Le protocole de Diffie-Hellman-Merkle :

C'est le premier système de cryptographie à clé publique (plus connu sous le nom de Diffie-Hellman ou DH). Cette méthode fut employée dans les protocoles Internet tels que le *Secure Socket Layer* et *Internet Protocol Security*. L'algorithme s'étale sur 4 étapes pour générer les quatre paramètres communiqués [17].

Toute personne espionnant l'opération (c'est-à-dire possédant les quatre paramètres communiqués) ne pourra calculer la clé secrète. Cependant un inconvénient de la méthode DH est qu'il ne permet pas de signer des documents. C'est pour cette raison que Diffie-Hellman est souvent associé à DSS qui permet de signer les documents.

L'algorithme RSA :
C'est un algorithme de chiffrement à clé publique, qui utilise la quasi-impossibilité d'effectuer la fonction d'inversion d'une fonction puissance. Il tient sa sécurité du problème de factorisation des grands nombres premier.
L'algorithme se déroule en trois étapes qui sont : la création de clés, le chiffrement puis le déchiffrement [17].

2.1.4.2 Mécanisme d'authentification :

L'authentification a pour objectif de vérifier l'identité des processus communicants. Il utilise deux mécanismes qui sont :

La signature électronique :
Elle est définie comme des « données ajoutées à un message », ou transformation cryptographique d'un message (cf.Figure 2.8), permettant à un destinataire :
- D'authentifier l'auteur d'un document électronique.
- De garantir son intégrité.
- D'assuré la non-répudiation.

La signature électronique est basée sur l'utilisation conjointe d'une fonction de Hachage (génère un nombre qui constitue l'empreinte numérique du message), et de la cryptographie asymétrique.

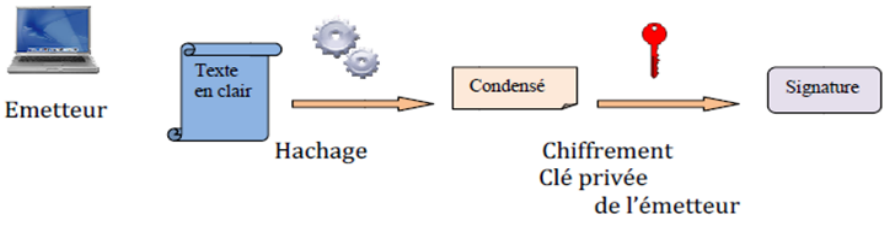

FIGURE 2.8 – Signature d'un message

Certificats électroniques :
Un certificat est un élément d'information qui prouve l'identité du propriétaire et l'intégrité des clés publiques. Les certificats sont signés et transmis de façon sécuritaire par un tiers de confiance appelé autorité de certification CA.

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité, ainsi que de révoquer éventuellement des certificats avant cette date

en cas de compromission de la clé (ou du propriétaire).

La structure des certificats est normalisée par le standard X.509 de l'UIT, qui définit les informations contenues dans le certificat.

2.2 Sécurité dans le réseau GSM :

Les procédures de sécurité misent en place par le GSM protègent à la fois l'utilisateur des écoutes frauduleuses ou d'usurpation d'identité et le réseau d'utilisations abusives.

D'où ce système se manifeste par les éléments de sécurité suivants :

- Authentification d'un abonné,
- Confidentialité de l'abonné,
- Confidentialité de la localisation.

2.2.1 Les algorithmes de sécurité dans le réseau GSM :

Trois types d'algorithmes sont utilisés dans les protocoles de sécurité et de confidentialité des données GSM :

2.2.1.1 Algorithme A_3 :

Cet algorithme est utilisé pour l'authentification d'un utilisateur du réseau [18]. Il fournit une réponse SRES à partir d'un nombre aléatoire envoyé par le réseau. Pour la détermination du SRES, l'algorithme A_3 utilise aussi la clé d'authentification K_i.

- Du coté mobile, l'algorithme A_3 est enregistré dans la carte SIM.
- Du coté du réseau, il est obtenu dans l'AuC qui correspond juste à une subdivision du HLR.

Les deux paramètres utilisés par l'algorithme A_3 ont les formats suivants :

- Longueur de K_i : 128bits.
- Longueur du nombre aléatoire (RAND) : 128 bits.
- Le résultat de l'algorithme (SRES) à une longueur de 32 bits.

2.2.1.2 Algorithmes A_5 :

Cet algorithme est implémenté dans le mobile, il est utilisé dans les processus de cryptage et de décryptage [18].

- Pour le cryptage, l'algorithme A_5 produit toute les 4.615ms une séquence de 114 bits de cryptage / décryptage (BLOCK) qui sont additionnés modulo 2 avec les 114 bits du texte en clair.
- Le décryptage est accompli du coté du MS avec le premier bloc de 114 bits produit par l'algorithme A_5 et l'encryptage est accompli avec le second bloc.

L'algorithme A_5 doit avoir le format suivant :

- Longueur de K_c : 64 bits.

– Longueur de COUNT : 22 bits.
– Longueur de chaque bloc : 114 bits.

L'algorithme A_5 doit produire un bloc1 et bloc2 en un temps plus court que la durée d'une trame (4.615ms).

2.2.1.3 Algorithme A_8 :

Du coté de la station mobile, l'algorithme A_8 est contenu dans la carte SIM [18]. Du coté du réseau, l'algorithme A_8 est co-localisé avec A_3.

Les deux paramètres en entrée (RAND,K_i) et le paramètre de sortie (K_c) de A_8 doivent avoir les formats suivants :
– Longueur de K_i :128 bits.
– Longueur du paramètre RAND : 128 bits.
– Longueur de K_c : 64 bits.

La figure 2.9 représente la procédure du chiffrement et d'authentification :

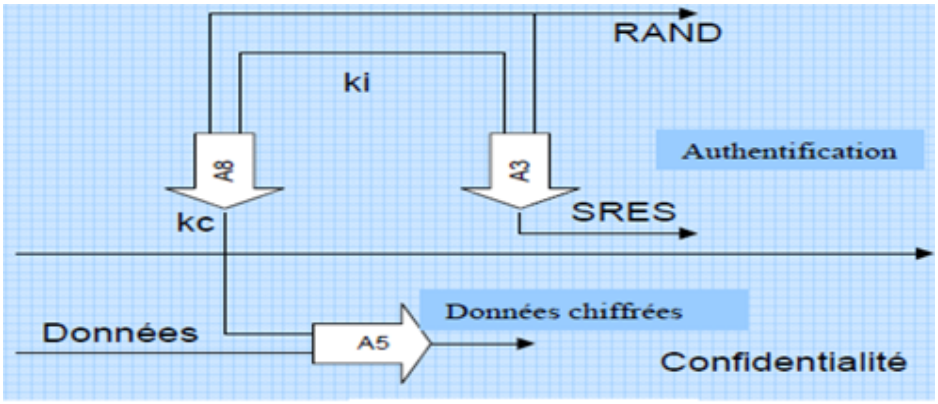

FIGURE 2.9 – Procédure du chiffrement et d'authentification

2.2.2 Faiblesses de la sécurité 2G :

En dépit des mesures de sécurités mises en place, on observe quelques failles et faiblesses de la sécurité du GSM , qui sont :
– Clé secrète trop petite (54 bits).
– Algorithmes de chiffrement fragiles .
– Apparition de cellules virtuelles qui permettent l'écoute en temps réel.
– L'intégrité des données n'est pas assurée.
– Le réseau d'origine ne contrôle pas l'utilisation des vecteurs d'authentification AV par le réseau de service ; en plus, il n'a aucune information à leur propos.

Cette sécurité ne suffit pas pour les informations sensibles de l'entreprise. Il faut utiliser d'autres outils de sécurité que nous apportent les méthodes de sécurité des réseaux 3G.

2.3 Sécurité dans le réseau UMTS :

Les évolutions de la sécurité portée sur l'UMTS est basé sur les problèmes et les risques connus dans le système de deuxième génération (GSM). Trois grands principes de sécurité ont été pris en compte quand les protocoles de la sécurité 3G ont été développés : garder le plus possible les principes de la sécurité 2G, de l'améliorer et offrir de nouveaux services.

La sécurité de l'UMTS doit tenir compte de la diversité des fournisseurs et des offerts de services. Les services de la voix sont moins importants que ceux des données. Ceci implique un risque accru d'attaques actives surtout lors de leur utilisation qui est très sensible.

2.3.1 Les attaques et menaces principales :

Un réseau étant constitué d'un ensemble d'équipements informatiques, il est particulièrement sensible aux attaques. Dans le cas de l'UMTS, la vulnérabilité est renforcée par l'aspect immatériel de l'interface radio (cf. Figure 2.10). Les différents scénarios d'attaques sont rassemblés en plusieurs types, selon que le pirate attaque [19] :

- Le déni de service ;
- usurpation d'identité ;
- attaque cryptographiques.

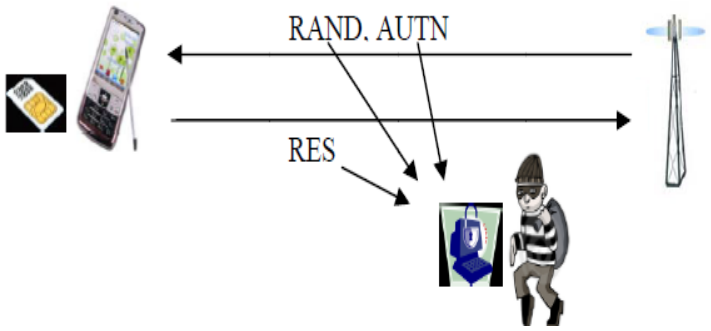

FIGURE 2.10 – Attaque sur la voix radio

Un ensemble de mécanismes ont été spécifiés pour empêcher ou, plus modestement, rendre plus difficile les différents types d'attaques. Cependant, la sécurité n'est pas que l'affaire de protocoles mais aussi d'architecture et de gestion du réseau. En particulier pour les éléments devant être mis à jour ou reliés à des réseaux extérieurs (cf. Figure 2.11).

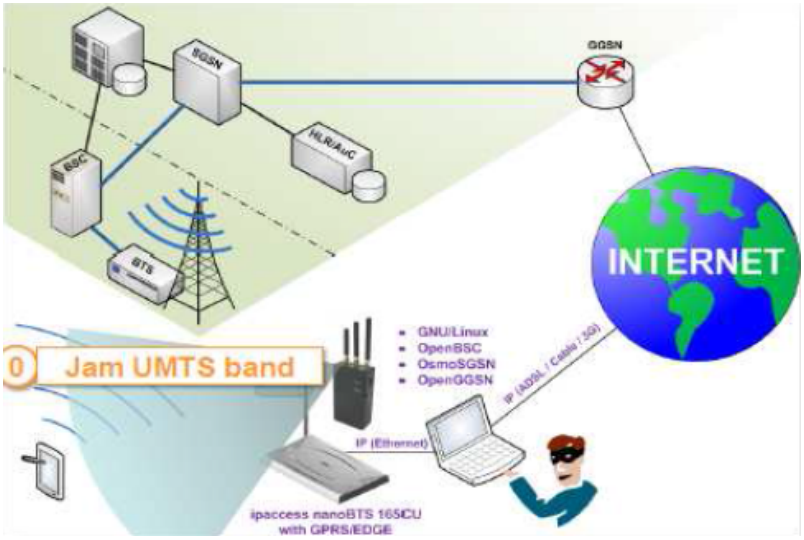

FIGURE 2.11 – Attaque sur les réseaux extérieurs

2.3.2 Architecture de sécurité du réseau UMTS :

Le réseau UMTS se repose sur deux aspects, physique qui se base sur le concept domaine et logique (protocoles) sur le concept en couche. Le transfert des communications se fait entre ses domaines, la où les informations doivent être protéger et sécuriser de toute attaques malveillante.

La conception globale de la sécurité de UMTS est composée de 5 catégories[20](cf. Figure 2.12), que nous allons présenter ci-dessous.

2.3.2.1 Sécurité du domaine utilisateur :

La sécurité du domaine utilisateur est réalisée avec un secret partagé entre l'USIM et un utilisateur authorisé, elle porte deux aspects :

- Authentification Utilisateur-USIM : elle utilise le code PIN pour but de limiter l'accès à l'USIM et des utilisateur non autorisés.
- Authentification USIM-ME : elle a pour but de limiter l'accès à l'EM pour les USIMs qui ne sont pas autorisés.

2.3.2.2 Sécurité au niveau accès réseau :

Cette catégorie de sécurité protège la liaison radio entre l'utilisateur et le reste du réseau UMTS. Les spécifications techniques de 3GPP définissent des aspects de sécurité à ce niveau qui sont :

- Confidentialité de l'identité de l'usager ;
- Authentification réciproque réseau-utilisateur ;
- Confidentialité et Intégrité des données.

2.3.2.3 Sécurité du domaine réseau :

Le système de sécurité pour le domaine réseau, offre la sécurisation des messages envoyés sur le réseau IP et sur le réseau de signalisation pour les réseaux téléphoniques.

Les réseaux IP sont sécurisés avec l'IPSec. Le standard UMTS utilise l'IPSec-ESP en mode tunnel permettant la sécurisation des messages IP entre les passerelles IP. La distribution et l'échange des clés sont réalisées avec l'IKE.

La sécurité sur le réseau SS7 est offerte par l'MAPSec. Le protocole de sécurité pour le MAP est la partie du protocole SS7 spécifique pour la téléphonie mobile. Chaque message MAPSec consiste en un en-tête MAP et un corps de message protégé.

2.3.2.4 Sécurité du domaine application :

Cet aspect de la sécurité UMTS permet le développement des applications de sécurité sur la carte UICC, pour le transfert de données avec un degré de sécurité choisi par le réseau ou le fournisseur d'application.

2.3.2.5 Visibilité et configuration de la sécurité :

Les spécifications techniques de l'UMTS donnent des suggestions vis-à-vis de la visibilité et de la possibilité de configuration des services de sécurité par l'utilisateur tels que :

- Indication de chiffrement au niveau réseau d' accès : la propriété que l'utilisateur est informé si le chiffrement est utilisé pour la communication avec le RNC.
- Annulation ou activation de l'authentification USIM-Utilisateur : la propriété que l'utilisateur est capable de contrôler si l'authentification USIM-Utilisateur est activé ou non.
- Acceptation ou rejet des appels non chiffrés : l'utilisateur doit pouvoir contrôler s'il veut établir des appels quand le réseau n'a pas activé la procédure de chiffrement.

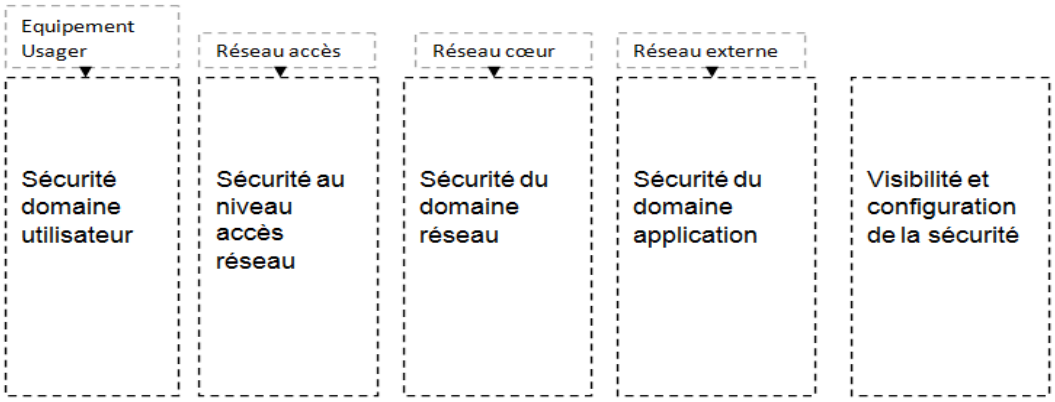

FIGURE 2.12 – Architecture de sécurité du réseau UMTS

2.3.3 Protocole AKA :

Le protocole AKA a été conçu afin de sécuriser l'accès aux réseaux mobiles, plus précisément le réseau UMTS. Cette procédure est une évolution de la procédure de sécurité du GSM.

La procédure d'authentification et d'établissement des clés entre le réseau UMTS et le client est basée sur une clé secrète K, connue seulement par l'USIM et l'AuC du réseau d'origine.

La partie « authentication » du protocole AKA permet de vérifier l'identité de l'usager, alors que la partie « Key Agreement » permet de générer des clés qui sont utilisées pour le chiffrement du trafic de l'usager dans le réseau d'accès et aussi pour la protection de l'intégrité des messages de signalisation [20].

2.3.3.1 Vecteur d'authentification AV :

La procédure AKA est basée sur un ensemble de paramètres appelé vecteur d'authentification AV. Ce vecteur est généré par le réseau d'origine et il est envoyé au réseau de service dans le but de réaliser la procédure AKA.

Six fonctions de sécurité :$f_0, f_1, f_2, f_3, f_4 et f_5$ sont utilisées pour générer ces vecteurs. Chaque vecteur AV est composé des éléments suivants [20] :

1. RAND : une valeur aléatoire générée par la fonction f_0. Il est envoyé en clair sur la voie radio et utilisé comme entrée pour toutes les autres fonctions de sécurité de f_1 à f_5.
2. XRES : c'est la réponse attendue par le réseau qui est généré par la fonction $f_2$comme suit : XRES=f_2 (RAND, K), où la clé K n'est pas connu par le réseau du service.
3. Les clés de chiffrements et d'intégrité CK et IK : c'est deux clés de chiffrement sont générées respectivement par les fonctions f_3 et f_4, comme suit : CK =f_3(RAND, K) et IK=f_4(RAND, K).
4. La clé d'anonymat AK : Ceci commence par un nouveau numéro de séquence SQN_{he} et d'une nouvelle variable RAND. L'AUC utilise un compteur SQN_{he} différent pour chaque utilisateur. La valeur envoyé est chiffré avec la clé d'anonymat AK : AK=f_5(RAND, K) .
5. Message MAC :c'est la partie du jeton AUTN qui va être vérifié par l'USIM pour authentifier le réseau. Cette valeur est obtenu en utilisant un champ de gestion d'authenticité AMF, qui est utilisé pour envoyer des informations relatives aux algorithmes utilisés :MAC=f_1(K, AMF , SQN_{he}).
6. Message AUTN : c'est la concaténation des trois valeurs (SGN_{he}, XOR, AK), AMF, MAC. Il est envoyé par le réseau de service à l'utilisateur ; pour que ce dernier puisse authentifier le réseau de service, et avoir les informations sur certaine aspect de sécurité.

La génération des éléments du vecteur d'authentification AV est présentée sur Figure 2.13.

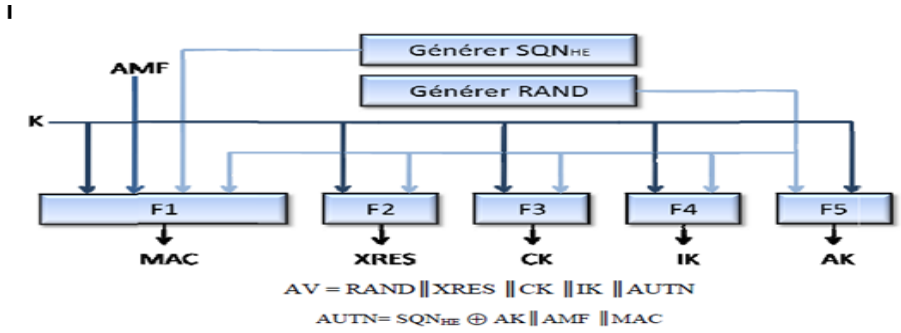

FIGURE 2.13 – Vecteur d'authentification

2.3.4 Fonctions de sécurité :

Il y a neuf fonctions de sécurité qui sont utilisées par l'UMTS [19]. Ces fonctions sont divisées en deux catégories :

2.3.4.1 Fonctions utilisées par la procédure AKA :

La procédure AKA utilise sept fonctions f_1 ,f_1*, f_2,f_3, f_4 ,f_5 et f_5*, dont (f_1*, f_5*) qui sont pour la resynchronisation, en cas de perte de synchronisation entre la clé ME et les clés du réseau (cf. Tableau 2.1).

Fonction	Type	Données d'entrée	Données de sortie
f_0	Génération de variable aléatoire		RAND
f_1	Fonction d'authentification du réseau	K, SQN,RAND,AMF	MAC
f_1*	message de resynchronisation	K, SQN,RAND,AMF	MAC
f_2	authentification de l'utilisateur	K,RAND,AMF	RES
f_3	clé de chiffrement dérivée	K,RAND,AMF	CK
f_4	clé de calcul de dérivation	K,RAND,AMF	IK
f_5	clé anonyme de chiffrement dérivée	AK	K,RAND,AMF
f_5*	message de resynchronisation	K,RAND,AMF	AK

TABLE 2.1 – Les fonctions de bases de MILENAGE [19]

2.3.4.2 Fonctions utilisées pour le chiffrement et l'intégrité :

L'ETSI SAGE a développé deux jeux d'algorithmes de chiffrement et d'intégrité :

1. UIA_1 et UEA_1 utilisant l'algorithme KASUMI :

   L'algorithme de chiffrement KASUMI constitue le noyau des algorithmes UIA_1 et UEA_1. C'est un algorithme de chiffrement par bloc de 64 bits utilisant 8 séries Feistel et une clé secrète de taille 128 bits.

   La Figure 2.14 montre comment est réalisée la fonction de chiffrement f_8, en utilisant l'algorithme KASUMI pour le chiffrement des données.

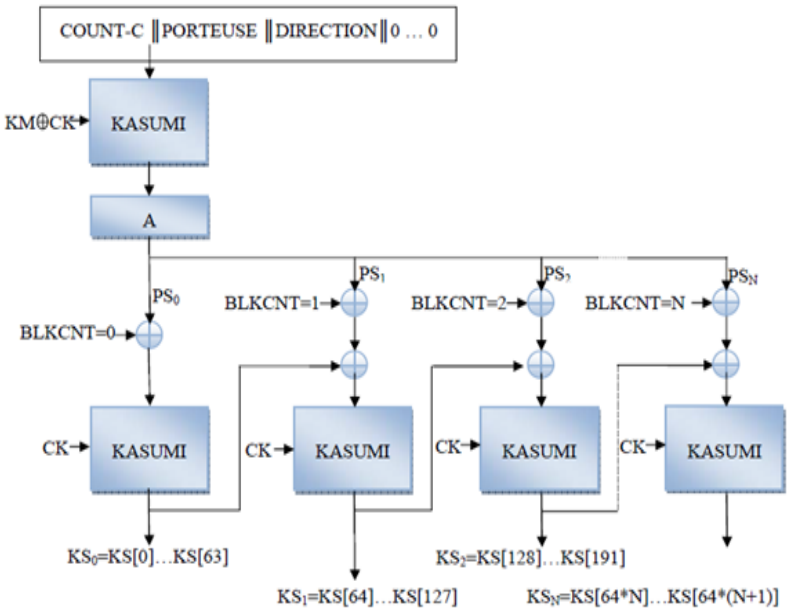

FIGURE 2.14 – Fonction de chiffrement $f_8$utilisant l'algorithme KASUMI [20]

La Figure 2.15 montre comment est réalisée la fonction d'intégrité f_9, en utilisant l'algorithme KASUMI pour le chiffrement des données :

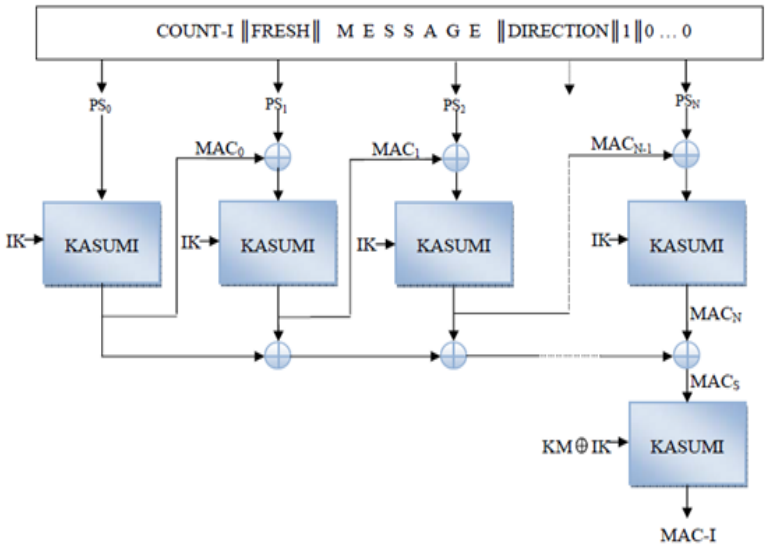

FIGURE 2.15 – Fonction d'intégrité f_9 utilisant l'algorithme KASUMI [20]

2. UIA_2 et UEA_2 utilisant l'algorithme SNOW 3G :

   L'algorithme SNOW 3G est un algorithme de chiffrement par flux utilisant une clé de 128 bits et une variable d'initialisation de 128 bits. Il est basé sur l'algorithme SNOW 2.0. Il a subi des modifications pour devenir plus robuste contre la cryptanalyse algébrique et les attaques de type distinguées.

   La Figure 2.16 montre comment est réalisée la fonction de chiffrement f_8, en utilisant l'algorithme SNOW 3G.

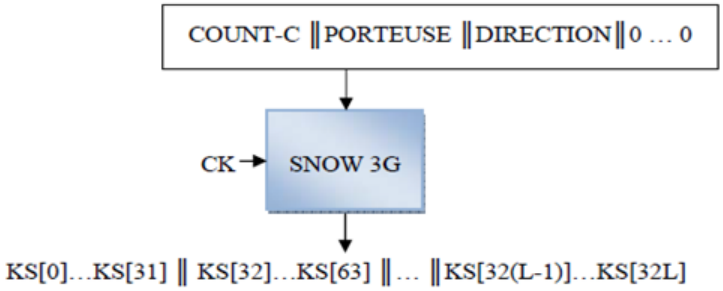

FIGURE 2.16 – Fonction de chiffrement $f_8$utilisant l'algorithme SNOW 3G [20]

La Figure 2.17montre comment est réalisée la fonction d'intégrité f_9,en utilisant l'algorithme SNOW 3G.

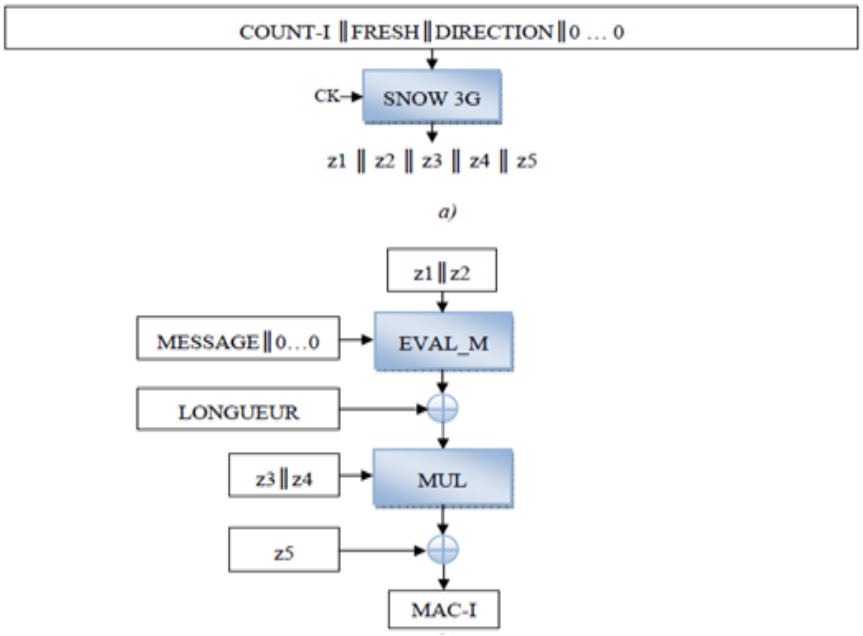

FIGURE 2.17 – Fonction d'inégrité f_9 utilisant l'algorithme SNOW 3G[20]

2.3.5 Procédure de sécurité du réseau UMTS :

Les trois procédures de sécurité proposées par la norme UMTS sont :

2.3.5.1 Procédure d'authentification :

L'authentification joue un rôle important dans la sécurité des réseaux UMTS. Cette procédure permet au réseau de vérifier l'identité de l'abonnée, et permet également au mobile d'authentifier le réseau par une vérification de la validité des informations transmises par le réseau. Elle permet au mobile de générer les clés IK et CK de chiffrement et d'intégrité, par un mécanisme d'authentification.
L'authentification repose sur des éléments qui doivent être tenues secrets :

- La clé K, qui est spécifique à chaque usager. Elle n'est connue que par la carte USIM et l'AuC ;
- Les algorithmes f_1, f_2 et f_5.

La procédure d'authentification est exécutée par le réseau à chaque demande d'accès du mobile, qu'il s'agisse de l'inscription initiale au PLMN, d'une réponse à un message de *paging* ou d'un appel initié par l'usager du mobile.

La figure 2.18 présente le déroulement de la procédure d'authentification effectuée par le SGSN pour le domaine PS.

Mécanisme d'authentification :

Il existe deux mécanismes d'authentification qui sont :

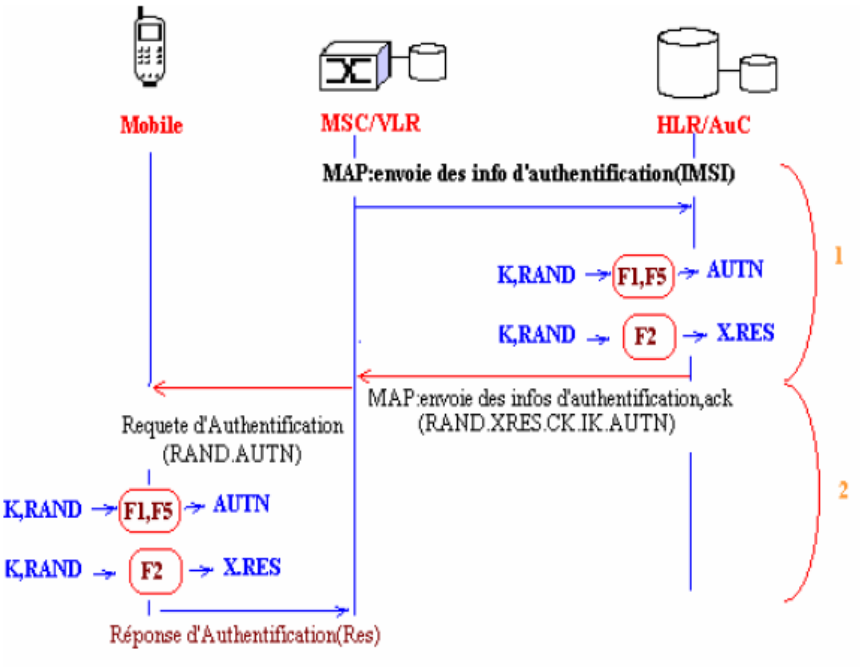

FIGURE 2.18 – Le déroulement de procédure d'authentification

Authentification de l'abonné :

L'authentification de l'abonné reprend le même principe que dans GSM. Un algorithme d'authentification « à sens unique » est utilisé pour calculer, à partir d'un nombre aléatoire RAND et de la clé K, un résultat (cf. Figure 2.19).

Si XRES = RES c'est le cas d'un abonné authentifié. Sinon, toutes les demandes de services sont rejetées.

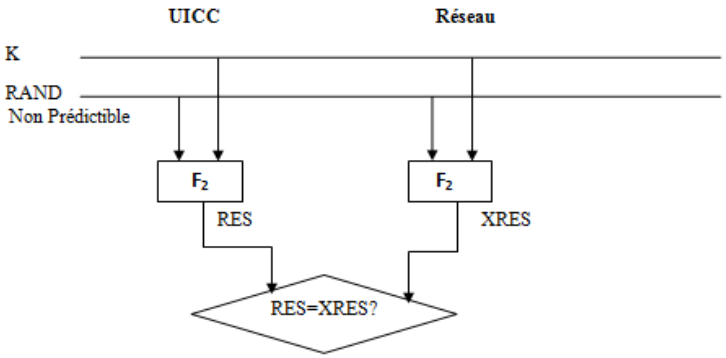

FIGURE 2.19 – Principe d'authentification de l'abonnée

Authentification mutuelle :

Le système GSM utilisait seulement le mécanisme d'authentification du réseau. Pour contrer, les attaque connu dans le GSM , l'UMTS repose sur l'authentification mutuelle (c'est-à-dire du mobile par le réseau et du réseau par le mobile) et sur un mécanisme

de compteur.

L'authentification du réseau repose sur les mêmes principes que l'authentification du mobile, le nombre aléatoire est le même (RAND), l'algorithme est différent mais du même type, le résultat est appelé MAC.

La carte USIM calcule de son côté, à partir du RAND, le code d'authentification appelé XMAC.

Si XMAC = MAC, alors elle renvoie la valeur RES. Sinon, elle refuse la demande d'authentification. Pour réduire encore le risque de « fausse authentification », on utilise un principe de compteur.

Pour éviter les problèmes de désynchronisation, la valeur de SQN est transmise sur la voie radio mais sous forme chiffrée, la clé étant calculée à partir de RAND et de K.

Si le terminal détecte que le SQN envoyé par le réseau ne correspond pas au SQN attendu, il indique au réseau un problème de désynchronisation.

La figure 2.20 représente la procédure de l'authentification mutuelle :

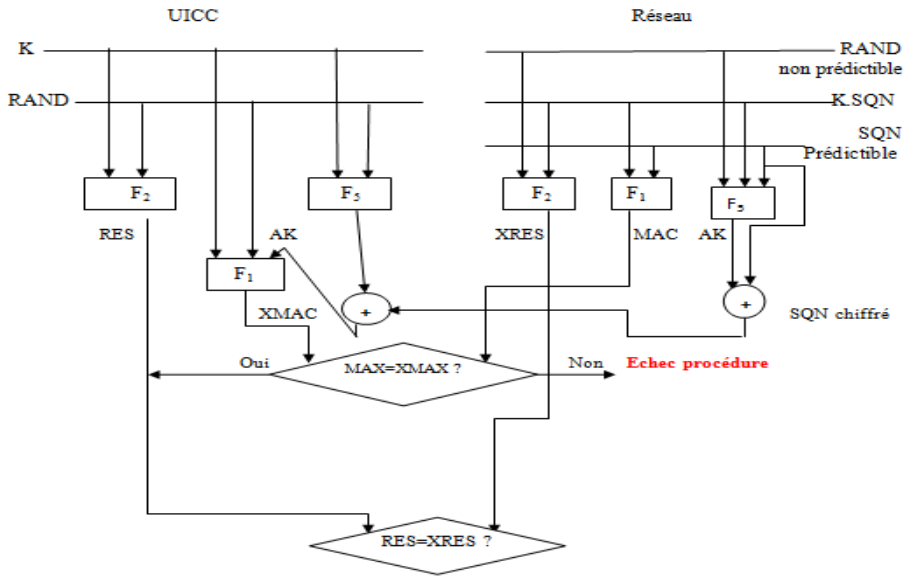

FIGURE 2.20 – L'authentification mutuelle

2.3.5.2 Procédure de chiffrement :

Le chiffrement permet d'assurer la confidentialité des données usager échangées entre le mobile et le réseau dans les deux sens de transmission. Le chiffrement s'applique indépendemment aux domaines PS et CS du réseau cœur.

Mécanisme de chiffrement :

Le chiffrement des données est réalisé par :

- la couche RLC lorsque le protocole RLC est utilisé en mode acquitté ou non acquitté (mode UM et AM)
- la couche MAC lorsque le RLC est utilisé en mode transparent.

Chaque bloque MAC ou RLC est simplement chiffré par l'émetteur à l'aide d'une addition bit à bit (ou exclusif) entre les bits du bloc de données et les bits du bloc KSB (Keystream Block).

Le bloc KSB est généré par l'algorithme f_8, qui utilise les paramètres suivants :

- La clé de chiffrement CK ;
- Un compteur COUNT-C, qui est un numéro de séquence variant au cours du temps ;
- Une information de longueurs, *LENGTH*, permettant à l'algorithme f_8 de générer des blocs KSB de même longueur que les blocs de données à chiffrer ;
- Les paramètres *DIRECTION* et *BEARER*, utilisés pour éviter que les blocs KSB des différents canaux de transport utilisés soient identiques. Ce qui affaiblirait la protection apportée.

La figure 2.21 représente le mécanisme de chiffrement :

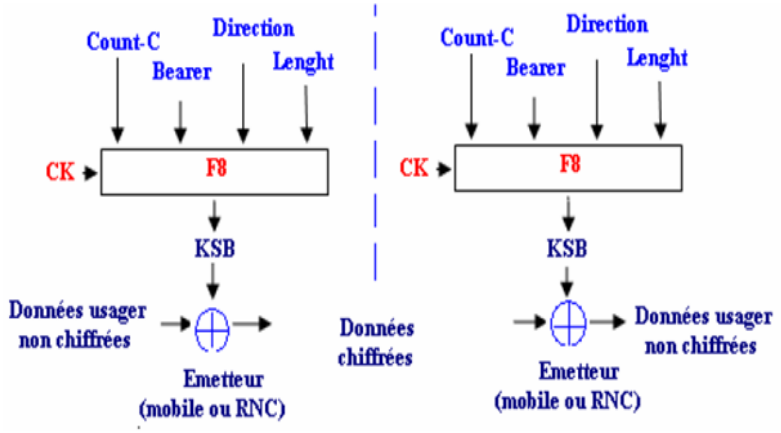

FIGURE 2.21 – Le mécanismes de chiffremnt

2.3.5.3 Procédure d'intégrité :

La procedure est nouvelle par rapport au GSM, s'applique à la signalisation échangée entre le mobile et le réseau. Elle permet à l'entité réceptrice d'authentifier l'émetteur et de s'assurer que le message reçu n'a pas été altéré ou falsifié au cours de la transmission.

Mécanisme d'intégrité :

L'intégrité fonctionne suivant un mécanisme assez similaire (cf.Figure 2.22).

L'algorithme f_9 génère un code MAC à partir du message à émettre par les entrées suivantes :

- IK .
- COUNT-I : un compteur de séquences sur 32 bits.
- MESSAGE : est le message qui est protégé.
- *FRESH* : une valeur aléatoire établie par le réseau, chaque fois qu'une liaison de sécurité est établie avec un UE. Ensuite elle est utilisée par le réseau et l'UE afin

d'éviter l'utilisation des anciens codes MAC-I.

– *DIRECTION* : un bit qui indique le sens du message (voix montante ou descendante). Ce paramètre est utilisé pour éviter l'utilisation des mêmes paramètres d'entrée pour les deux voies.

Le code MAC est ensuite accolé au message avant d'être transmis. Le côté qui envoie le message, calcule le code MAC-I et l'ajoute au message.

A la réception du message, un code XMAC est généré à l'aide de la même méthode que celle employée par l'émetteur et comparé avec le code MAC reçu. En cas d'échec, le message est considéré comme non valide et détruit par le récepteur.

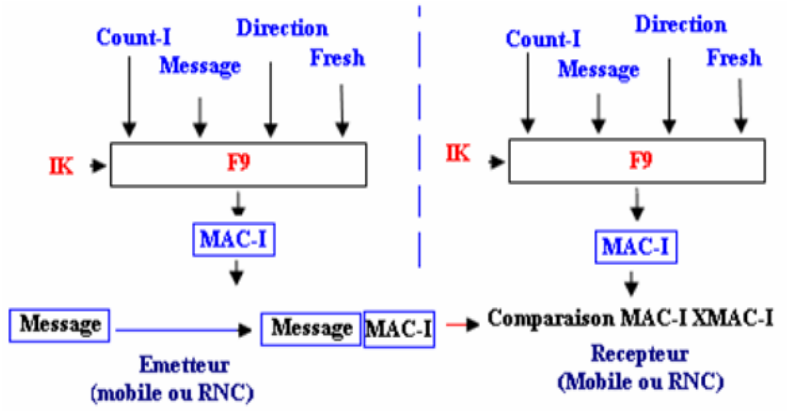

FIGURE 2.22 – Le mécanismes d'intégrité

2.4 Conclusion :

La sécurité du réseau UMTS a nettement évolué par rapport aux réseaux de deuxième génération, tout en conservant l'élément clé du GSM qu'est l'utilisation d'une carte à puce pour l'authentification et la génération des clés. Les progrès des technologies et des techniques de cryptographie ont permis d'avoir un systéme robuste et fiable.

Ces évolutions importantes ont permis de contrebalancer la fragilité croissante des systèmes dont l'architecture est de plus en plus ouverte, dans lesquels on trouve de plus en plus d'interfaces que peuvent tenter les pirates pour perturber le réseau soit en écoutant les communications ou en volant les informations.

De ce fait est alors née la sécurité du domaine PS ; auquel nous nous intéresserons particulièrement dans le chapitre suivant.

CHAPITRE 3

SÉCURITÉ DES DONNÉES DANS LE DOMAINE PS DU RÉSEAU UMTS :

3.1 Introduction :

Le réseau UMTS a donné plus d'importance à la transmission des données que pour la voix. Pour cela, il possède un mode de commutation de paquet qui permet une intégration naturelles des protocoles Internet (TCP/IP ou UDP /IP).

L'hétérogénéité des piles protocolaires traversées par les paquets destinées, ou en provenance d'un mobile UMTS durant une connexion à Internet, nécessite la mise en place des différentes sortes de routage au sein du réseau. L'explication des techniques de routage, la résolution des adresses, et de sécurité demeurent donc indispensable pour comprendre l'accès à Internet via le réseau UMTS.

A fin d'intégrer les services de sécurité appropriés, le système permet la création d'un tunnel de communication sécurisé et basé sur des protocoles de protection robuste afin de remédier aux attaques informatiques que subiront les données en se connectant aux réseaux public.

3.2 Transport de données dans le domaine PS du réseau UMTS :

3.2.1 Notion du PLMN dans L'UMTS :

Le PLMN est défini dans la norme, comme un réseau de télécommunication qui est constitué d'un réseau cœur et un réseau d'accès, installé et gère par un opérateur.

Chaque PLMN dispose d'une identité, composée de deux champs [2] : le MMC et le MNC. Les MMC sont attribues par l'ITU ,afin d'éviter qu'un même code ne soit utilisé par deux pays différents. En revanche, l'attribution du MNC est laissée à l'appréciation des organismes de régulation de chaque pays.

Une fois le PLMN et la cellule d'accueil sélectionnés, le mobile va tenter de s'inscrire auprès du PLMN choisi pour chaque domaines du réseau cœur.

Dans les spécifications de l'UMTS, cette procédure porte le nom de :
- *IMSI attach* pour l'inscription au domaine CS ;
- *UMTS GPRS attach* pour l'inscription au domaine PS.

Les principaux protocoles misent en œuvre dans la procédure d'inscription sont les suivants :
- Le protocole GMM, entre le mobile et le SGSN, pour l'inscription au domaine PS.
- Le protocole MM, entre le mobile et le MSC/VLR, pour l'inscription au domaine CS.
- Le protocole MAP entre les différents nœuds du réseau cœur.

L'inscription dans domaine PS :
Le déroulement de la procédure de l'inscription est composé de trois phases principales (cf. Figure 3.1 et 3.2) :

1. Une fois la connexion RRC établie entre le mobile et le RNC, la demande d'ins-

cription est émise par le mobile à destination du SGSN, via le RNS.

2. Avant l'inscription du mobile, le SGSN doit procéder à certaines vérifications, sur la validité de l'identité de l'usager (et plus précisément de l'IMSI stocké dans la carte USIM) et l'identité du terminal. Une fois les vérifications des identités effectuées, le SGSN peut procéder à l'inscription du mobile auprès du réseau.

   Pendant cette phase et afin de protéger les échanges ultérieurs de signalisation entre le mobile et le réseau, le chiffrement entre les interfaces de l'UTRAN est activé.

   La figure 3.1représente les deux phases de l'inscription :

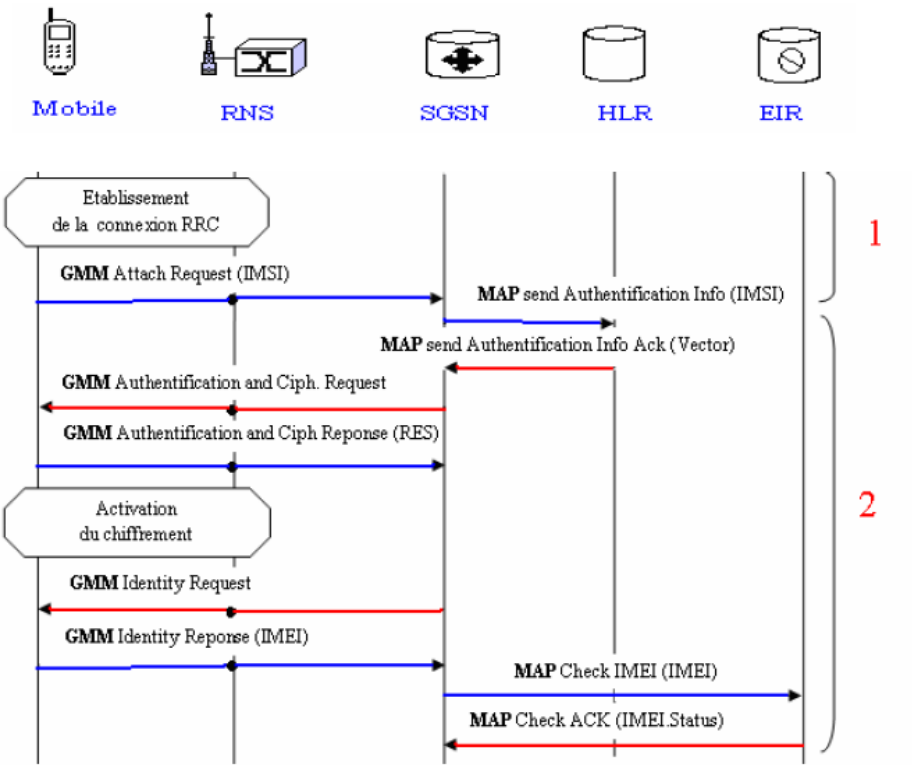

FIGURE 3.1 – L'inscription dans domaine PS (phase 1 et 2) [10]

3. La dernière opération (cf. Figure 3.2) effectuée est l'allocation d'une identité temporaire : Le P-TMSI, c'est cette identité qui sera utilisée dans les échanges ultérieurs entre le mobile et le réseau.

Le déroulement de la procédure d'inscription au domaine CS est quasiment identique à la procédure d'inscription PS. À la fin de l'inscription, une identité spécifique au domaine CS est allouée au mobile : le TMSI.

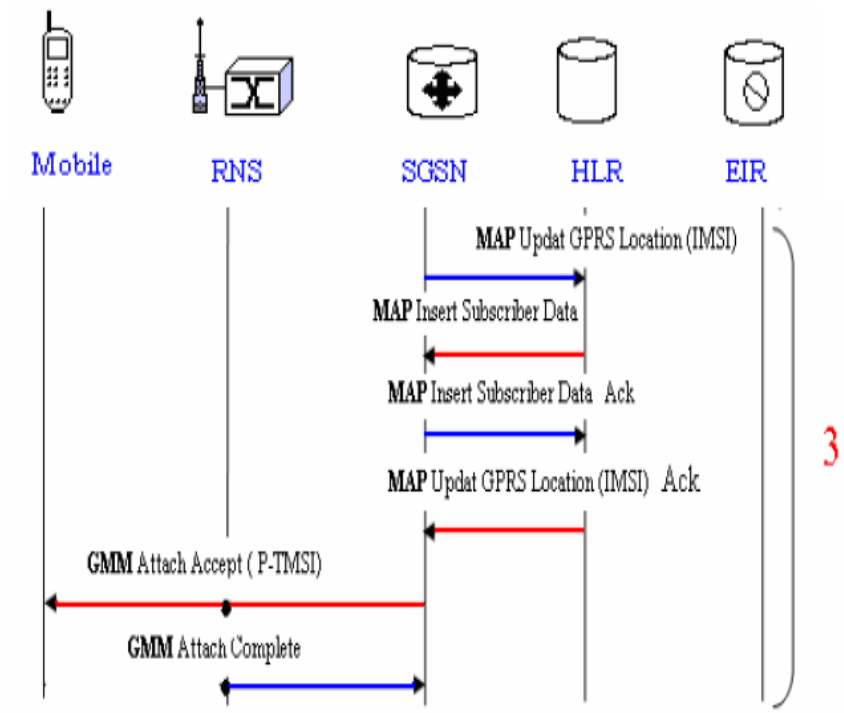

FIGURE 3.2 – L'inscription dans domaine PS (phase3) [10]

L'inscription combinée CS/PS :

Afin de diminuer les échanges de signalisation mobile-réseau, la norme offre la possibilité d'effectuer simultanément les inscriptions CS et PS ; si l'interface optionnelle Gs entre le SGSN et le MSC/VLR est supportée par le réseau (cf. Figure 3.3).

La phase initiale de la procédure d'inscription combinée est identique à celle de l'inscription PS. Une fois le mobile inscrit dans la base de données du SGSN(1), le SGSN transmet la demande d'inscription du mobile au MSC/VLR.

Le MSC/VLR informe le SGSN du succès de l'inscription CS par le message *Location Update Accept*, qui contient l'identité temporaire de l'usager au sens CS (le TMSI).

À la fin de la procédure d'inscription, le mobile se voit donc allouer simultanément les deux identités temporaires TMSI et P-TMSI pour chaque domaines.

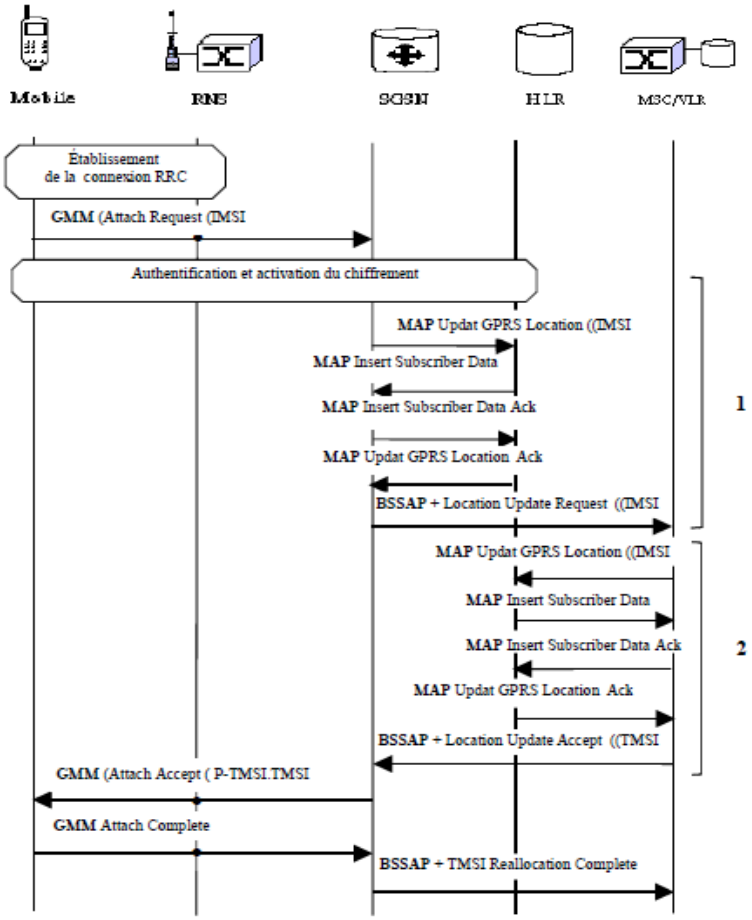

FIGURE 3.3 – La procédure d'inscription combimée CS / PS [10]

3.2.2 Notion de contexte PDP :

Le contexte PDP est une particularité du domaine PS. Il regroupe l'ensemble des informations permettant la transmission des données usager entre le mobile, le réseau UMTS et le réseau de commutation de paquet externe (Ex : Internet).

Le contexte PDP contient principalement les données suivantes :

- La qualité de service associée à la communication, qui est en fait représentée par les attributs du RAB alloué par l'UTRAN ;
- L'APN , qui est l'identifiant du réseau PDP externe auquel le mobile souhaite accéder ;
- L'adresse PDP du terminal ; dans le cas d'un réseau externe Internet, il s'agit d'une adresse Ipv4 ou Ipv6.

3.2.2.1 Mécanisme d'établissement d'un contexte PDP :

Phase 1 d'établissement d'un contexte PDP :

Si le terminal mobile veut activer un contexte PDP, il établit une connexion avec le SGSN à travers le RNC (cf. Figure 3.4). Pour se faire, le terminal envoit une requête d'établissement de connexion vers le RNC en utilisant le protocole RRC.

Dans le cas échéant le RNC envoi une réponse de réalisation de la connexion « *connection setup* », et le terminal lui acquitte avec « *connection setup complete* ».

Dans ce cas le mobile envoie la demande d'activation du PDP au RNC. Avant que la demande soit acheminée au SGSN, le RNC doit activer une connexion avec le SGSN par le protocole SCCP qui se fait en deux phases (demande et réponse).

Le RANAP donc initialise un message de la demande vers le SGSN. Dans ce cas commence la phase la plus importante qui consiste à créer ce qu'on appel le tunnel entre le SGSN et GGSN.

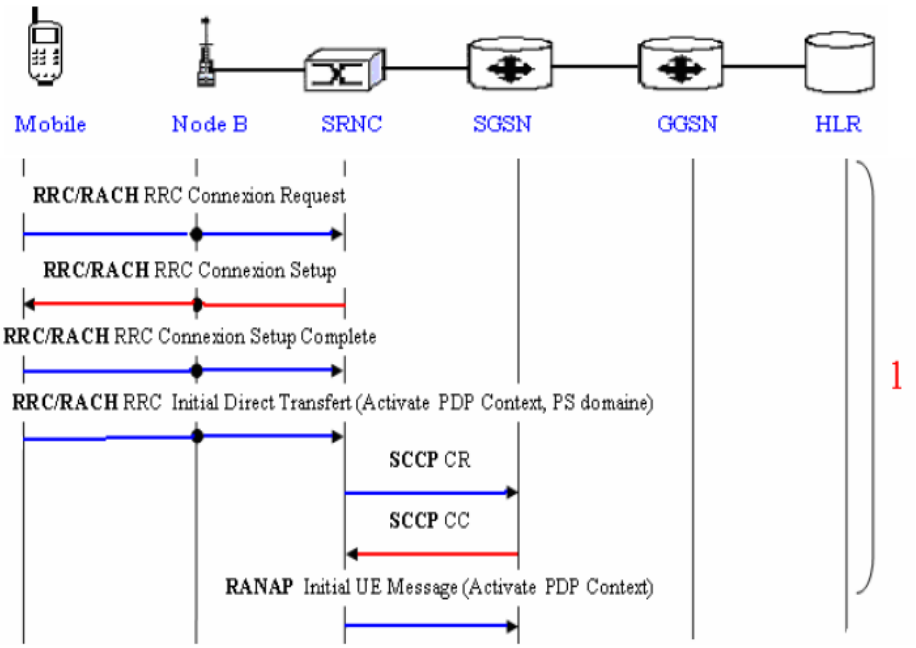

FIGURE 3.4 – Etablissement d'un contexte en mode paquet (phase1)[10]

Requête PDP :

C'est une requête envoyée du SGSN vers le GGSN demandant le début du tunneling, en lui fournissant le MSISDN de l'usager, le type du PDP, la qualité de service requise et les options de configuration.

Phase 2 d'établissement d'un contexte PDP :

Répose PDP :

Ce message doit être envoyé du GGSN vers le SGSN comme réponse de création du contexte PDP. Plusieurs types de réponses peuvent avoir lieu. Parmi ces réponses on cite :

- « *Request accepted* » : requête acceptée.
- « *No ressources availables* » : pas de ressources disponibles ou valides.
- « *All PDP adress are occupied* » : toute les adresses PDP sont occupées.

Dans le cas où la réponse est positive, c'est-à-dire « *Request accepted* » ; le contexte est considérer évidemment comme crée ; et des réponses au paramètres, sollicitées dans la requêtes, seront envoyées vers le SGSN.

Le contexte est donc crée, le SGSN va rendre la réponse au RANAP à sa demande d'initialisation en lui envoyant une requête d'attribution. Ce dernier va à son tour informer le terminal de la création du contexte suivant les étapses suivante (cf. Figure 3.5) :

- Il va premièrement établir la connexion avec le NBAP au niveau du Node B , pour pouvoir mettre en place le support radio (*Radio Bearer*) avec le RRC.
- Après que le support radio soit mis en place un chemin virtuel est crée (en deux phase, demande et réponse) entre le RNC et le Node B.
- Une réponse (à la requête d'attribution) est rendue au SGSN (avec le porotocole RANAP), pour que ce dernier termine définitivement la procédure d'activation du contexte PDP,en envoyant au terminal réponse finale d'acceptation.

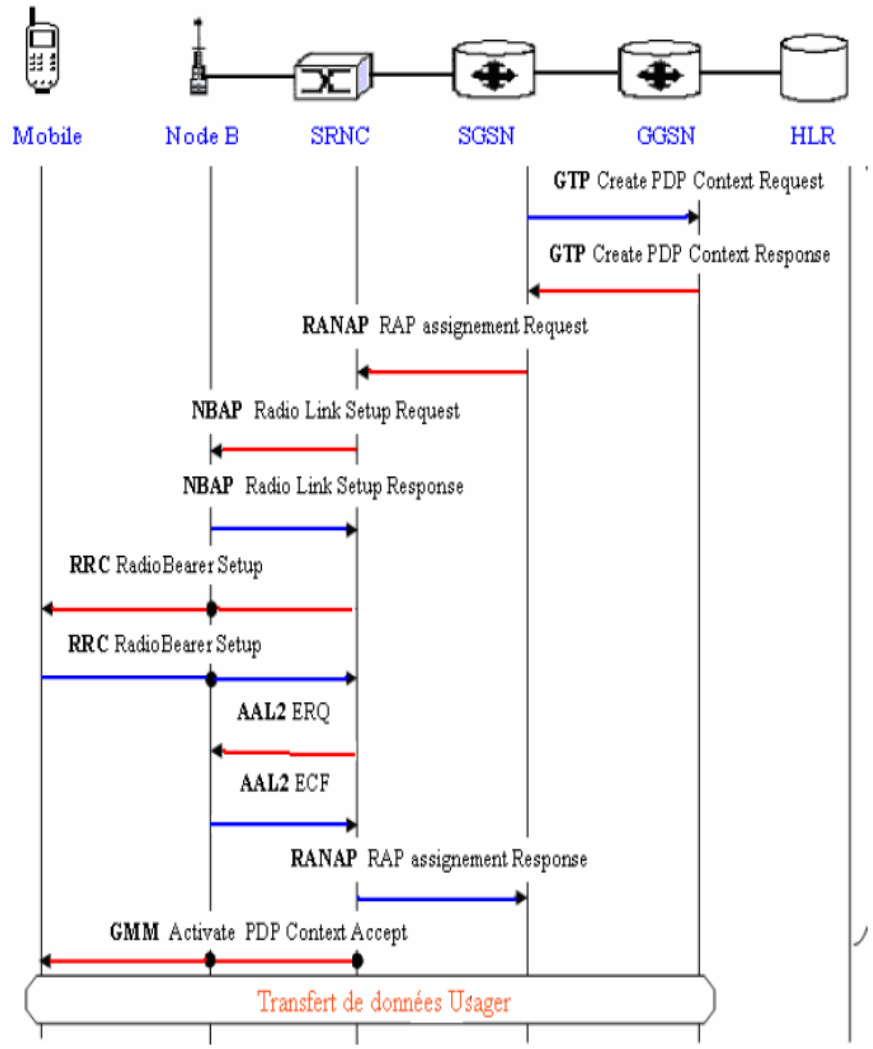

FIGURE 3.5 – Etablissement d'une connexion en mode paquet (phase 2)

3.2.3 Routage de paquet dans l'UMTS :

Suivant le type de données à transporter, la gestion du transport des données est différente.

Commençant par détailler les trames relatives à la voix. La couche PDCP n'est pas utilisée dans ce type de transport. Les couches MAC et RLC sont employées en mode transparent, c'est-à-dire qu'il n'y a pas de segmentation, ni de multiplexage.

En revanche, le transport d'un paquet IP, le mécanisme est différent. Ce type de paquet NPDU (Network PDU) provient du réseau cœur de l'UMTS à destination du réseau d'accès UTRAN.

Tout d'abord, l'en-tête de la N-PDU est compressé par la couche PDCP. La couche RLC segmente le PDU ainsi compressée. Un en-tête est alors rajouté à la RLC-PDU par la couche MAC lors du multiplexage.

Le figure 3.6 présente l'encapsulation des paquets qui arrivent au réseau cœur de l'UMTS :

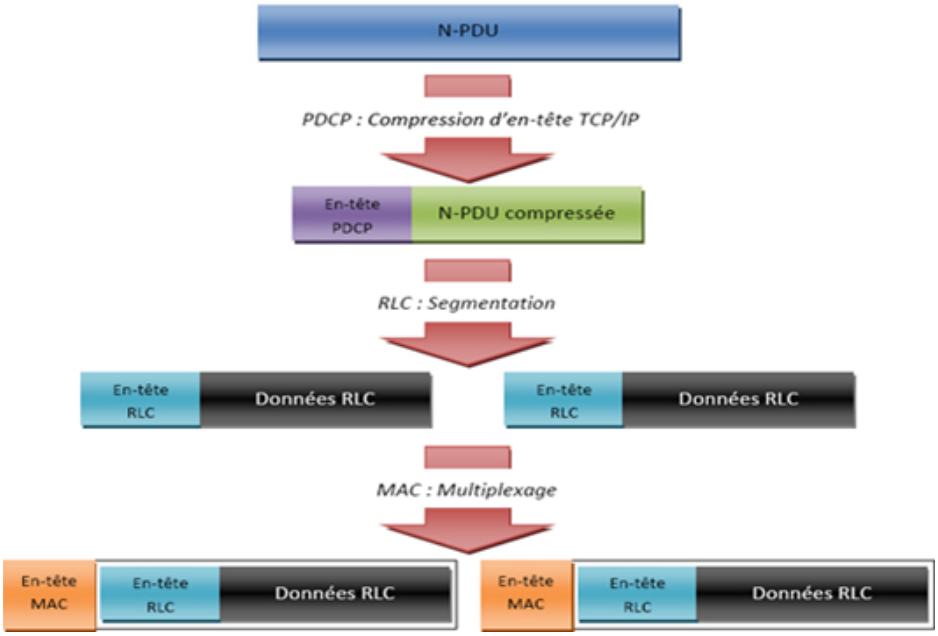

FIGURE 3.6 – Encapsulation des paquets à l'arrivée au réseau cœur

3.2.3.1 Résolution d'adresses :

Pour cette section, il est nécessaire de rappeler quelques notions des adresses. L'ESI est l'adresse MAC non pas l'adresse IP pour un terminal qui utilise le protocole IP dans la couche3.

Dans le CN, l'ESI correspond à une adresse MAC qui est unique et gravée dans l'interface de l'équipement du réseau.

Dans l'UMTS (en mode paquets) l'ESI correspond à l'IMSI. Dans un réseau IP fixe, lors de chaque transfert de données, un lien est établi entre l'addresse IP et l'addresse MAC de l'équipement correspondant. Pareillement dans le tunneling, dans le Backbone, un lien doit être établi entre l'addresse IP et le TEID [10].

Dans le cas d'un paquet provenant de l'extérieur du réseau, est destiné à un terminal mobile, l'adresse IP est convertie en un TIED ; dans le GGSN dans le cas où le contexte PDP est déjà créé ; et cela va permettre de router le paquet à travers le réseau.

3.2.3.2 Le point d'accès :

Le point d'accès est le point de connexion externe du réseau de l'opérateur. C'est l'utilisateur qui indique le point d'accès avec lequel la connexion devra être établie.

Lors de la requête de création du contexte PDP, le GGSN vérifie avec le HLR si le point d'accès est déjà défini ou pas. Ensuite, si le point d'accès est valide, une information est passée du HLR vers le GGSN indiquant si le mobile est permis d'avoir accès à ce point d'accès ou pas.

L'APN est une information utilisée par le GGSN pour différencier les accès vers les réseaux de données externes qui utilise le même type du PDP. Il est envoyé du GGSN vers le SGSN et le mobile pour identifier le réseau qui veut solliciter.

L'APN contient un nom logique qui identifie le point d'accès. L'en-tête GTP qui définit l'APN est présenté sur la figure 3.7.

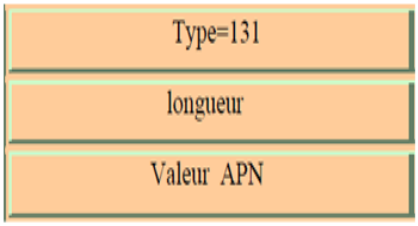

FIGURE 3.7 – Format de l'en-tête GTP

3.2.3.3 Sélection d'adresses IP :

L'adresse IP du mobile peut être allouée par le réseau d'opérateur et cela en activant un contexte PDP, ou par le réseau externe que le mobile veut solliciter. L'utilisateur doit sélectionner dans un menu le type du service vers lequel il veut avoir accès, Internet par exemple ou son propre réseau Intranet. Une requête est envoyée alors vers le SGSN à travers l'UTRAN.

- Le SGSN doit localiser le GGSN adéquat pour router les données que le mobile veut transmettre vers le réseau externe.
- Le SGSN doit donc consulter le DNS de cet opérateur pour repérer le GGSN en question.

– Le DNS va retourner l'adresse IP du GGSN où la connexion (point d'accès) est localisée.

Le GGSN peut avoir un nombre de point d'accès (cf.Figure 3.8)avec différents réseaux externes. A ce moment le SGSN peut véhiculer la requête PDP vers le GGSN.

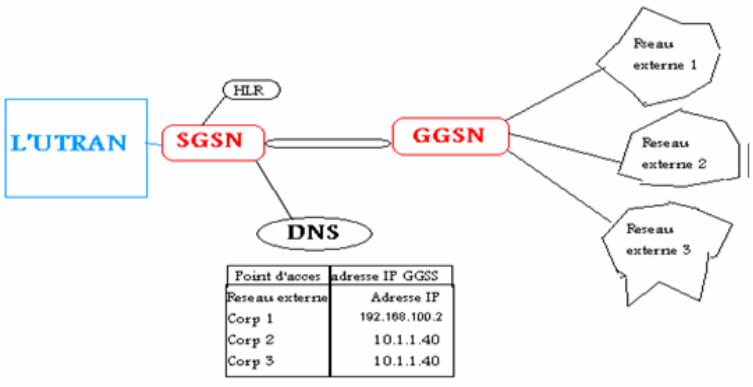

FIGURE 3.8 – Les points d'accés

3.2.4 Acheminement des paquets vers le mobile :

Supposant que l'application de l'utilisateur connecte au point d'accès Internet. Si l'utilisateur sollicite une page Web, il doit donc envoyer une requête au serveur approprié. Le serveur va répondre avec cette page, et l'adresse IP destination sera l'adresse à partir du quelle la requête a été envoyée.

L'adresse IP doit être routée donc à travers l'Internet jusqu'au GGSN. Il doit à son tour la router vers le mobile. Il va chercher une correspondance entre cette adresse et le tunnel déjà activé.

N.B : Si le mobile change de cellule, ou strictement le SGSN, un autre tunnel sera créé entre le nouveau SGSN et GGSN sans avoir à changer l'adresse IP.

Supposant que le tunnel est localisé ; donc l'IMSI est connu. Le SGSN exécute les étapes suivantes :

1. Le tunnel transfert le paquet IP vers le SGSN. Une fois le paquet atteint le SGSN, il sera enlevé du tunnel.
2. Le SGSN va donc résoudre l'adresse IP en P-TMSI (PacketTMSI). Le SGSN contient une base de données de correspondance P-TMSI.
3. L'IMSI, qui est utilisée pour identifier vers quel mobile doit-il envoyer la réponse.

Contrairement au tunnel utilisé dans le GPRS du GSM, dans l'UMTS le tunnel est raccordé jusqu'à l'UTRAN ou l'en-tête GTP est écartée au niveau du relais. C'est au réseau d'accès radio (UTRAN) d'identifier le mobile par des identités temporaires de la cellule et du réseau d'accès.

La figure 3.9 illustre le format du transport du paquet IP dans le réseau UMTS :

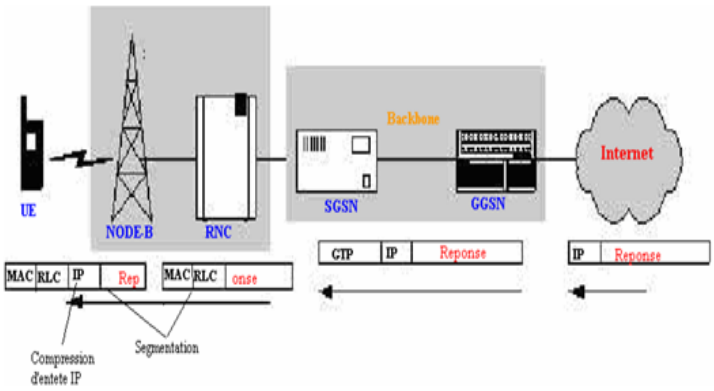

FIGURE 3.9 – Transport de paquet dans le réseau UMTS

Cas où aucun contexte n'est activé :

Dans le cas où un paquet IP, destiné à un mobile, arrive au GGSN, et qu'aucun contexte PDP n'est activé (c'est le cas où le mobile possède une adresse IP statique). Pour pouvoir acheminer ce paquet vers le mobile correspondant, le GGSN va exécuter les procédures suivantes :

1. Il va envoyer une requête vers le HLR pour demander son IMSI.
2. Le HLR va répondre avec l'IMSI et l'adresse du SGSN sur lequel le mobile est attaché.
3. Dés que ces informations soient reçues, le GGSN va envoyer une requête de notification vers le SGSN qui porte l'IMSI du mobile, l'APN, le type du PDP et l'adresse PDP.
4. Le SGSN doit donc envoyer au SGSN une réponse (*Notification Response Message*) pour l'informer qu'il va essayer de trouver le mobile.
5. Dans le cas où le mobile est trouvé, le SGSN envoie une requête vers le mobile lui demandant d'initier une activation du contexte PDP indiqué.
6. A ce moment, le mobile commence la procédure d'activation du contexte PDP.

3.2.5 Protocole VRRP :

Le VRRP est un protocole de communication inter routeur ou inter serveur qui permet d'organiser des élections et de remplacer un serveur défaillant en cas de panne d'un serveur principal dénommé serveur primaire.

Les routeurs ou les serveurs communiquant en VRRP peuvent avoir un ou plusieurs VRID. Ce dérenier n'est, en fait, qu'un groupement d'une ou plusieurs adresses IP virtuelles. Il ne peut y avoir qu'un seul serveur principal d'un VRID à la fois, les autres , s'ils sont configurés sur le même VRID, des backups attendent d'être éventuellement élus en cas de panne du principal.

La figure 3.10 représente une défaillance d'une liason entre SGSN et GGSN :

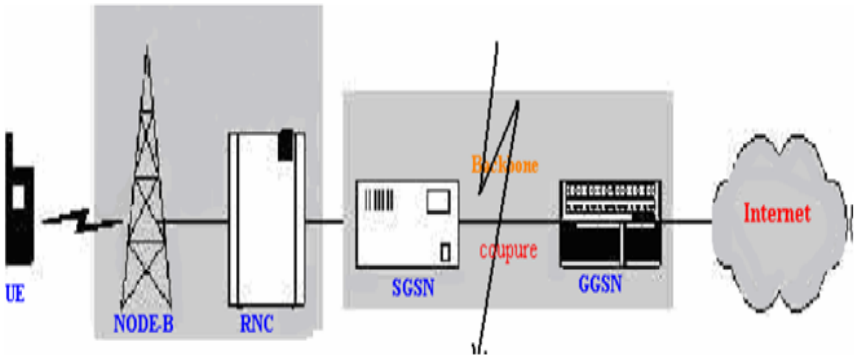

FIGURE 3.10 – Coupure de liaison entre SGSN & GGSN

Quand l'ancien serveur principal revient à nouveau, il reprend sa place et les autres serveurs redeviennent des backups du VRID. La communication inter serveur s'effectue par une adresse de multicast. Le serveur principal doit émettre toutes les secondes un paquet VRRP sur l'adresse de groupe multicast afin que les backups soient prévenus que le serveur principal fonctionne parfaitement bien.

Lors du réglages d'une adresse IP d'un VRID sur une interface d'un serveur, ce même serveur se doit de changer l'adresse MAC de son interface par une adresse MAC de VRRP normalisé.

Ce serveur envoie des paquets ARP, afin de forcer la remise à jour des caches ARP des DNS se trouvant sur le même segment réseau.

Si cette mise à jour n'est pas faite, le SGSN et le DNS ne connaîtront pas la nouvelle adresse MAC s'il y a changement d'autorité de serveur d'une adresse IP ; et le serveur fraîchement élu ne pourra pas communiquer avec les machines du même réseau physique.

Le protocole VRRP ne fait pas partie de la spécification UMTS ni GPRS, mais c'est une solution recommandée par le 3GPP pour assurer le secours du GGSN.

La figure 3.11 illustre le cas d'un rétablissement d'une liaison GGSN-SGsN

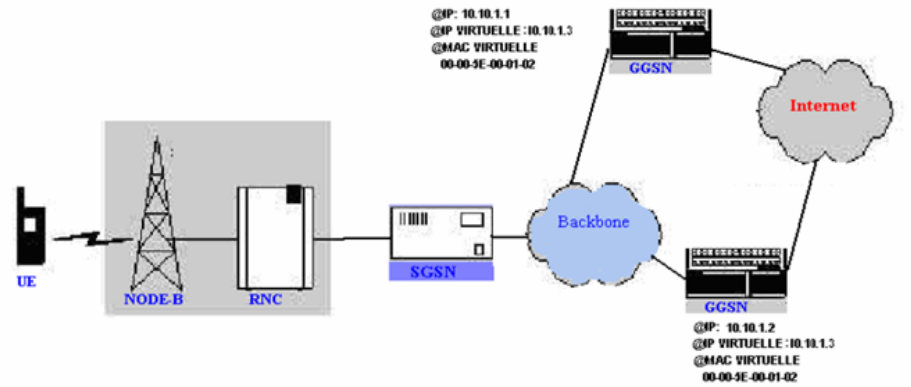

FIGURE 3.11 – Rétablissement d'une liaison GGSN-SGSN

3.2.6 Mise à jour de la zone de routage pour le domaine PS :

La gestion de la mobilité comme déjà vu, est une fonction essentielle des réseaux cellulaires. Afin de localiser les usagers dont le mobile est en mode veille, le réseau est découpé en zone géographiques, appelées zone de localisation (LA) pour le domaine circuit, et zone de routage (RA) pour le domaine paquet.

Les étapes de mise à jour du RA sont comme suit :

1. Une fois la connexion RRC est établie entre le mobile et le réseau d'accès, la demande de mise à jour de RA est émise à destination du nouveau SGSN qui peut déterminer la référence de l'ancien SGSN grâce à l'identifiant de l'ancienne RA fourni par le mobile.
2. L'ancien SGSN est interrogé par le nouveau en vue de récupérer la véritable identité du mobile (IMSI) et le contexte VA permettant d'authentifier ce dernier. Le nouveau SGSN peut alors authentifier le mobile à inscrire et passer en mode chiffré. Le chiffrement permet de sécuriser les informations émises sur l'interface radio entre le mobile et le réseau, en particulier le nouveau P-TMSI, qui sera alloué ultérieurement à l'abonné.

   Ces deux étapes sont représentées sur la figure 3.12 :

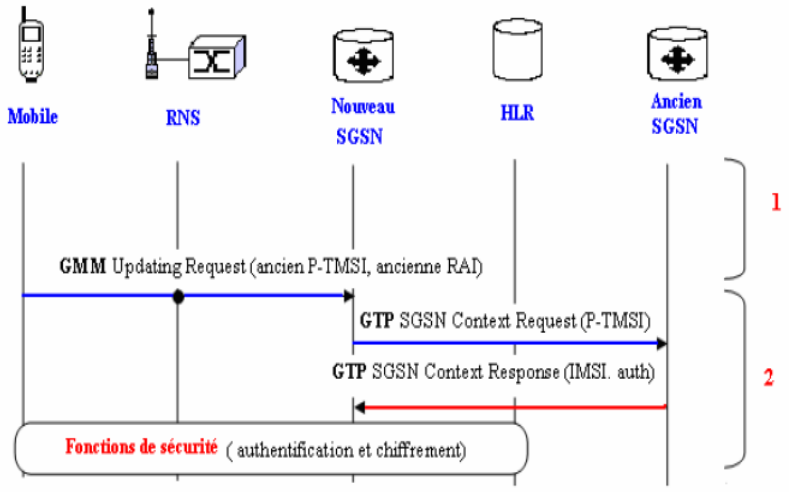

FIGURE 3.12 – Les deux premiere étapes de la mise à jour du RA

3. Une fois les informations récupérées, le nouveau SGSN informe le HLR du changement de RA du mobile. A son tour, le HLR va informer l'ancien SGSN, qui supprimera de sa base de données l'enregistrement correspondant à l'abonné. Au cours de cette phase, le HLR fournit au nouveau SGSN les informations relatives aux services souscrits par l'abonné.

4. Le mobile est informé du succès de la procédure de la mise à jour de RA. Une nouvelle identité temporaire P-TMSI lui est allouée par le nouveau SGSN.
5. La procédure étant terminée, le SGSN demande au réseau d'accès de libérer la connexion mobile-réseau et les ressources utilisées.

Ces trois dernière étapes sont présentées sur la figure 3.13.

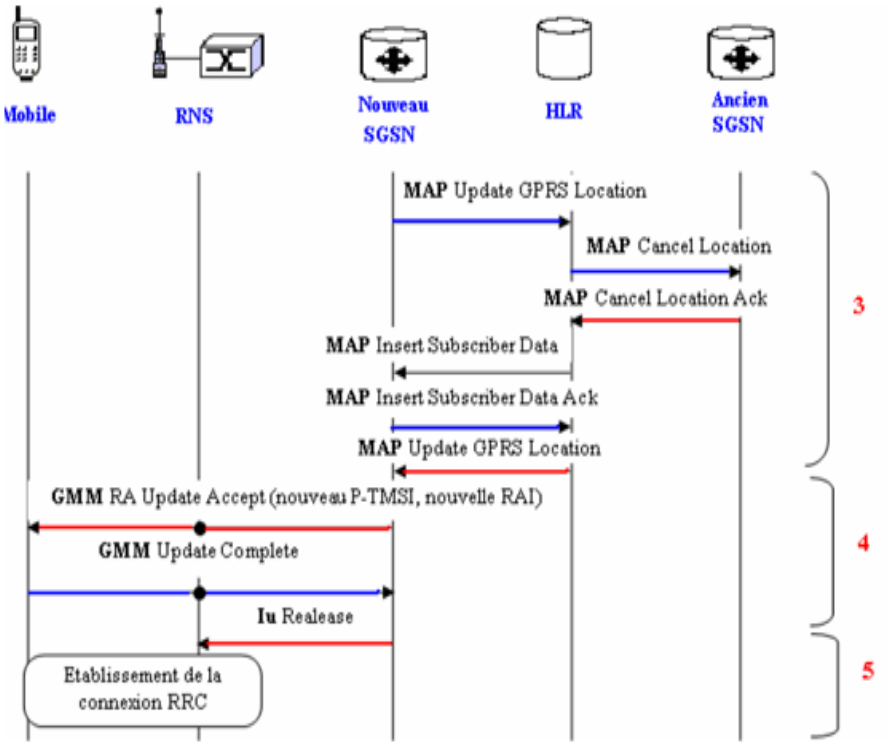

FIGURE 3.13 – Les trois dernière étapes de la mise à jour du RA

3.3 Sécurité des données dans le domaine PS :

Comme nous avons vu dans la section précédente que le transport de données dans le réseau UMTS nécessite toute une étude et divers protocoles. La transmission de ces données du réseau UMTS vers des réseaux extérieurs (Internet) représente un inconvénient, car ces données sont soumissent à des attaques de types informatique.

Dans le but de remédier à ces attaques, il se doit d'utiliser des mécanismes et des protocoles afin d'assurer leur sécurité.

3.3.1 Les attaques informatiques :

Les attaques informatiques constituent l'un des fléaux de notre civilisation moderne. Par conséquent, aucune des entreprises ne peuvent ignorer ces risques et se

croire à l'abri des telles épreuves. Sachant que ces attaques ont des buts précis qui visent des mécanismes de sécurité dans les réseaux.

Il existe quatre catégories d'attaques [14] (cf.Figure 3.14) :

(a) Interruption : C'est une attaque portée à la disponibilité . Elle a pour but de prendre le contrôle d'une ressource. Par exemples la coupure d'une ligne de communication.

(b) Interception : C'est une attaque porté à la confidentialité. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur .Par exemple, dans le cas d'une écoute téléphonique dans le but de capturer les données sur un réseau.

(c) Modification : C'est une attaque portée à l'intégrité. Par exemple, modifier le contenu du message transmis sur un réseau et changer les valeurs dans un fichier de données.

(d) Fabrication : C'est une attaque portée à l'authentification. Il peut s'agir de l'insertion de faux message dans un réseau ou d'ajout d'enregistrement à un fichier. Cette catégorie peut avoir pour but désinformé l'utilisateur.

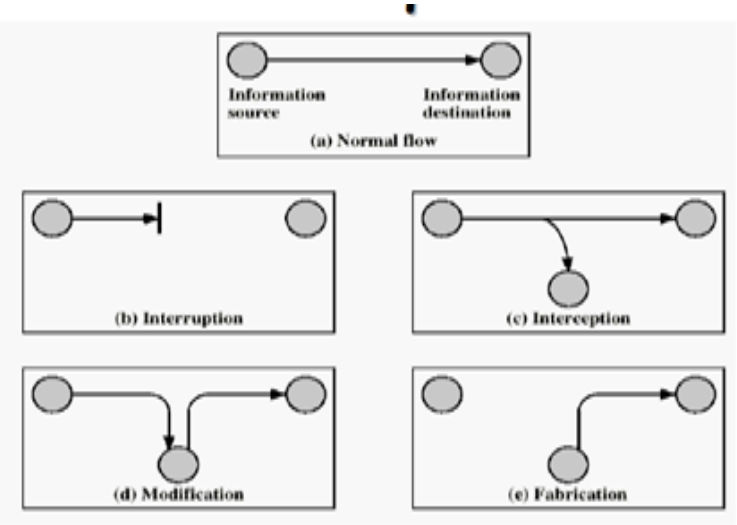

FIGURE 3.14 – les catégorie des attaques informatiques

Quelques exemples d'attaques informatiques :

Il existe plusieurs types d'attaques informatiques qui peuvent attiendre le réseau, on peut citer :

Contamination par un VIRUS : c'est un petit programme écrit pour modifier le fonctionnement d'un ordinateur sans l'accord de l'utilisateur. Un virus doit remplir deux critères : il doit s'exécuter et se reproduire.

Contamination par un VERS : est un programme autonome, une fois installé sur la machine ; tente de se reproduire sur d'autre machines, provoquant une saturation des mémoires.

Contamination par SPYWARE : c'est un logiciel qui collecte des informations d'une machine et les envoie à l'insu de l'utilisateur sans son consentement.

Cheval de Troie : c'est un morceau de code qui s'attache à un fichier, puis il s'exécute à un moment donné, provoquant la destruction de fichiers [6].

SPAM : c'est l'envoi massif de courrier électronique à des destinataires ne l'ayant pas sollicité.

Snifer (analyseur réseau) : est un dispositif permettant d'écouter le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent.

3.3.2 Sécurisation des données par création d'un VPN :

Le VPN est un réseau privé virtuel au sein d'une infrastructure d'unréseau publique.il permet d'interconnecter des sites distant réservés à un groupe d'usager, afin d'échanger des données de manière crypté de bout à l'autre bout du tunnel (cf. Figure 3.15). D'où vient, l'appellation, le principe de tunneling qui consiste à créer un chemin virtuel après avoir identifié l'émetteur et le destinataire [33].

L'implémentation des VPN dans les entreprises permet :
- La confidentialité et l'intégrité de l'information ;
- L'authentification des postes ;
- La protection du client VPN ;
- La gestion de la qualité de service et des délais ;
- La gestion des pannes.

FIGURE 3.15 – Présentation du réseau privé virtuel

3.3.2.1 Catégorie de VPN :

Les deux grandes catégories (topologies) du réseau VPN sont[33] :

Les VPN Site à site :

Ce type de VPN est créé lorsque les dispositifs de raccordement des deux côtés de la connexion VPN sont conscients de sa configuration à l'avance. Le VPN reste statique, et les hôtes internes n'ont pas connaissance qu'il existe. Frame Relay, ATM, GRE et les VPN MPLS sont des exemples de VPNs site à site.

Dans ce type de VPN, les hôtes envoient et reçoivent du trafic TCP /IP via une passerelle VPN, qui peut être un routeur, pare-feu, concentrateur.

Un VPN d'accès à distance :

Ce type de VPN est créé lorsque les informations VPN ne sont pas mises en place de façon statique, mais peuvent changer dynamiquement. Dans un VPN d'accès à distance, chaque hôte a généralement un logiciel client VPN. Chaque fois que l'hôte tente d'envoyer le trafic destiné au VPN, son logiciel client encapsule et crypte le trafic avant de l'envoyer par Internet à la passerelle VPN à la périphérie du réseau cible.

3.3.2.2 Les protocoles du VPN :

Les protocoles utilisées dans le cadre du VPN sont deux types, suivant le niveau de couche OSI auquel ils travaillent :

- Les protocoles de la couche 2 comme le PPTP et L2TP.
- Les protocoles de la couche 3 comme IPSec, GRE et MPLS.

Nous limiterons notre étude au protocole de couche 3 du VPN qui est le protocole IPSec.

3.3.3 Application du protocole IPsec dans un VPN :

L'IPsec est un standard IETF qui définit la manière dont un VPN peut être configuré en utilisant le protocole d'adressage IP. C'est un système de normes ouvertes qui énonce les règles pour les communications sécurisées.

L'IPsec n'est pas lié à un cryptage spécifique, ni à l'authentification, ni aux algorithmes de sécurité, ou à des mécanismes de gestion des clés. Mais il repose sur des algorithmes existants pour le mettre en œuvre. Il fonctionne à la couche réseau, et assure la protection et l'authentification des paquets IP entre les dispositifs IPsec participants (pairs).

En conséquence, il peut protéger pratiquement tout le trafic de l'application, car la protection peut être mise en œuvre de la couche quatre à la couche sept (modèle OSI).

Toutes les implémentations d'IPsec ont un en-tête de couche trois en texte clair, donc il n'y a aucun problème avec le routage. Comme il fonctionne aussi sur tous les protocoles de couche deux, comme Ethernet, ATM, Frame Relay, SDLC, et HDLC [33].

3.3.3.1 Architecture du protocole IPSec :

L'architecture IPSec (cf. Figure 3.16)se compose de cinq blocs constitutifs[W3].

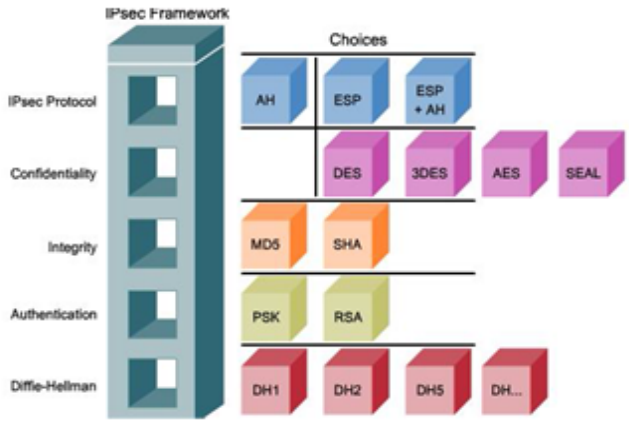

FIGURE 3.16 – Présentation du protocole IPSec

(a) Le premier bloc représente le protocole IPsec, les deux principaux protocoles qui permettent de sécuriser les communications sont AH et ESP [24].

Authentification du Header AH :

Il réalise l'authentification (cf. Figure 3.17) en appliquant une fonction de hachage unidirectionnelle à clé secrète partagée au paquet pour créer une table de hachage ou condensé de message. Le hachage est combiné avec le texte puis transmis[33].

Le récepteur détecte des changements dans n'importe quelle partie du paquet qui se produisent pendant le transport ; en effectuant la même fonction de hachage unidirectionnelle sur le paquet reçu et en comparant le résultat à la valeur du condensé de message que l'émetteur fourni.

La fonction du AH est appliqué à l'ensemble du paquet, à l'exception de tous les champs d'en-tête IP qui changent pendant le transport.

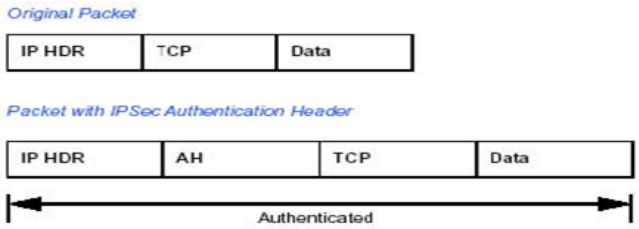

FIGURE 3.17 – Le mécanisme AH

Encapsulation Security Payload (ESP) :

Il peut assurer la confidentialité et l'authentification [33]. Il assure la confidentialité en effectuant le chiffrement sur le paquet IP qui permet de dissimuler la charge utile des données, l'identité de la source et la destination finale. Il fournit l'authentification pour le paquet IP interne et à l'en-tête ESP. L'algorithme par défaut pour IPsec est DES 56 bits.

ESP peut également assurer l'intégrité et l'authentification [33]. En premier lieu, la charge utile est cryptée. Ensuite, cette charge cryptée est envoyée à travers un algorithme de hachage, HMAC-MD5 ou HMAC-SHA-1.

La Figure 3.18 représente le mécanisme ESP.

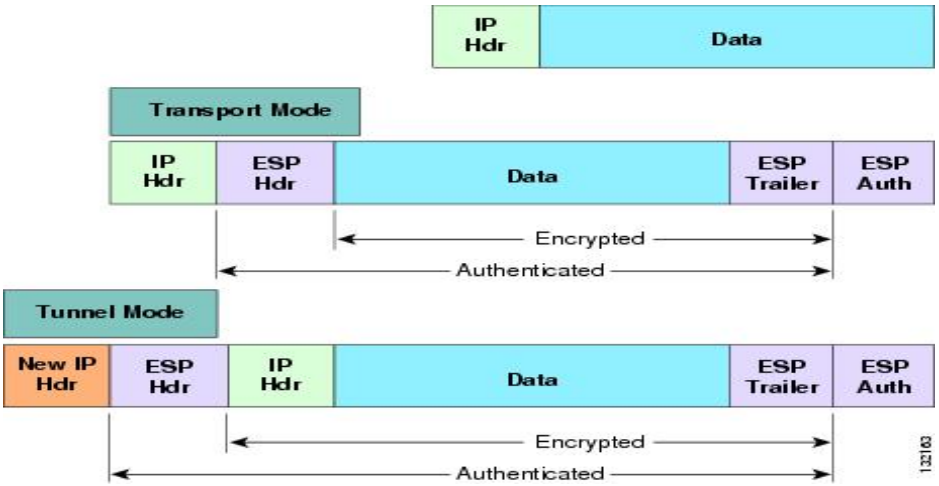

FIGURE 3.18 – Le mécanisme ESP [21]

(b) Le second bloc(cf. Figure 3.19) représente une type d'algorithme de confidentialité :

Il utilise un algorithme de chiffrement tels que DES, 3DES, AES ou SEAL [33]. Le choix dépend du niveau de sécurité requis.

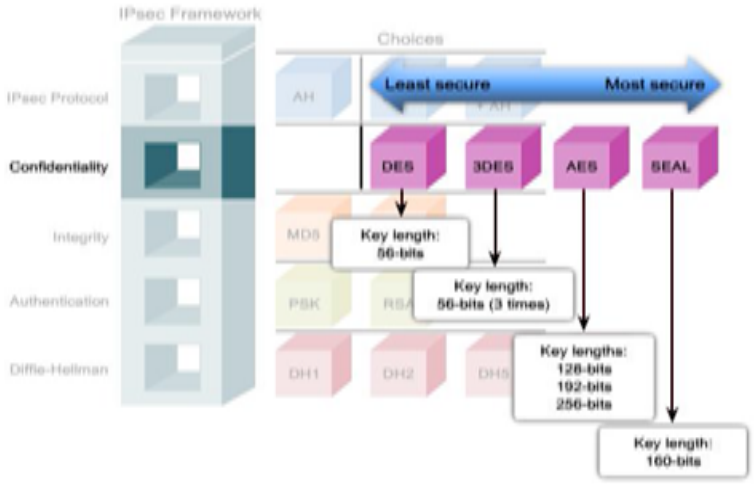

FIGURE 3.19 – Les algorithmes de chiffrement selon leurs clés

(c) Le troisième bloc représente l'intégrité qui peut être implémenté en utilisant l'algorithmes MD5 ou SHA (cf .Figure 3.20).

Les données sont transportées sur l'Internet public. Potentiellement, ces données peuvent être interceptées et modifiées. Une méthode permettant de prouver l'intégrité des données est nécessaire pour garantir que le contenu n'a pas été modifié sont les codes d'authentification de message haché HMAC.

Il ya deux algorithmes HMAC courants [33] :

- HMAC-Message Digest 5 (HMAC-MD5) :
  Il utilise une clé partagée secrète de 128 bits. Le message de longueur variable et la clé secrète partagée de 128 bits sont combinées et exécutées par l'algorithme de hachage HMAC-MD5. La sortie est une table de hachage de 128 bits.

- HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1) :
  Il utilise une clé secrète de 160 bits. Le message de longueur variable, et la clé secrète partagée de 160 bits sont combinées et exécutées par l'algorithme HMAC-SHA-1. La sortie est un hachage de 160 bits.

  Le HMAC-SHA-1 est considéré comme cryptographiquement plus forte que HMAC-MD5.

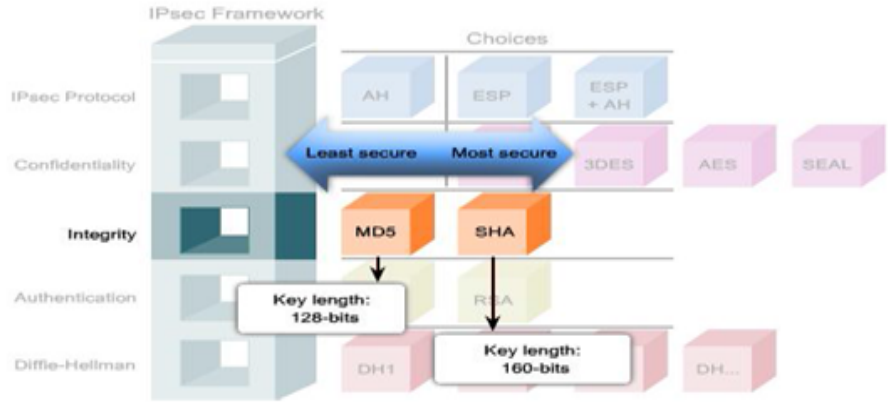

FIGURE 3.20 – Les algorithmes d'intégrité et leurs clés

(d) Le quatrième bloc représente l'authentification (cf. Figure 3.21). Le dispositif à l'autre extrémité du tunnel VPN doit être authentifié avant que le chemin de communication ne soit considéré comme sûr.

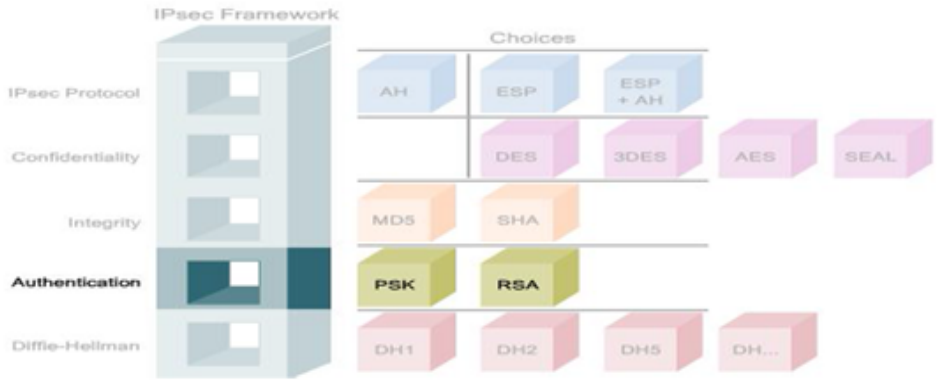

FIGURE 3.21 – Présentation des algorithmes d'authentification

Il existe deux principales méthodes de configuration de l'authentification :

Clés pré-partagées (PSK) :

Une valeur d'une clé secrète prépartagée est entrée dans chaque homologue manuellement afin de l'authentifier [33]. A chaque extrémité, le PSK est combinée avec d'autres informations pour former la clé d'authentification. Chaque paire doit authentifier son homologue opposé avant que le tunnel ne soit considéré comme sûr.

Signatures RSA :

L'échange de certificats numériques authentifie les pairs. Le dispositif local crée un hachage et le chiffre avec sa clé privée. Le hachage cryptée est joint au message à une extrémité éloignée et tient lieu la signature.

A l'extrémité opposée, la valeur de hachage cryptée est décryptée à l'aide de la clé publique de l'extrémité locale. Si le hachage déchiffré correspond au hachage recalculée, la signature est authentique. Chaque pair doit authentifier son homologue opposé avant que le tunnel soit considéré comme sûr.

(e) Le cinquième bloc représente les groupes d'algorithmes DH (cf. Figure 3.22) :
Le Diffie-Hellman (DH) : C'est une méthode d'échange de clé publique. Il fournit aux deux pairs un moyen d'échanger des clés secrètes partagées qu'ils doivent être les seuls à connaitre , même s'ils communiquent sur un canal non sécurisé.

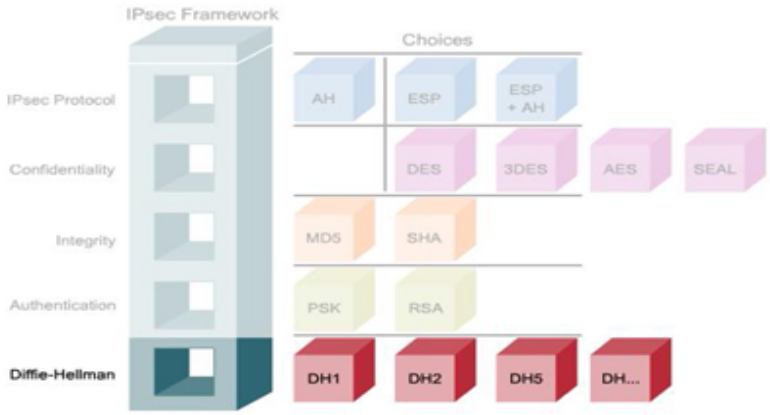

FIGURE 3.22 – Présentation du groupe d'algorithmes DH

3.3.3.2 Associations de sécurité SA :

Une SA est un bloc constitutif de base du protocole IPSec [22]. Les associations de sécurité sont maintenues dans une base de données SA, qui est établie par chaque dispositif.

Un VPN possède des entrées SA définissant les paramètres de chiffrement IPsec ainsi que les paramètres d'échange de clés [24].

3.3.3.3 Mode opératoire d'IPsec :

Il existe deux modes d'utilisation d'IPSec [22] : le mode transport et le mode tunnel. La génération des datagrammes sera différente selon le mode utilisé comme

il est représenté sur la figure 3.23.

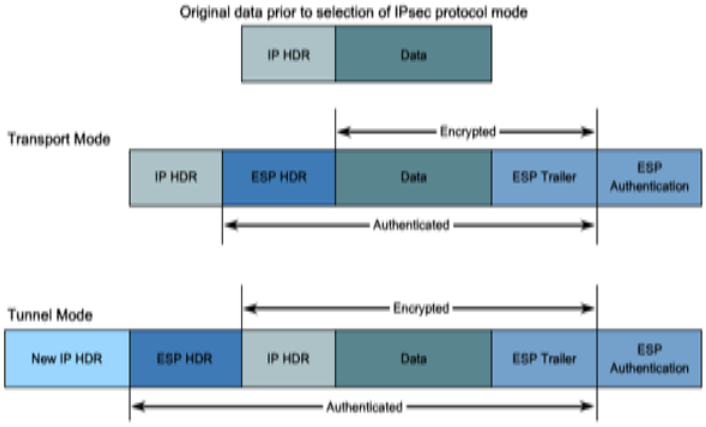

FIGURE 3.23 – Présentation des modes selon le datagramme

Mode Transport :

Ce mode est utilisé pour créer une communication entre deux hôtes qui supportent IPSec. Une SA est établie entre les deux hôtes. Les en-têtes IP ne sont pas modifiées, les protocoles AH et ESP sont intégrés entre cette en-tête et l'en-tête du protocole transporté. Ce mode est souvent utiliser pour sécuriser une connexion Point-à-Point.

Mode Tunnel :

Ce mode est utilisé pour encapsuler les datagrammes IP dans IPSec. La SA est appliquée sur un tunnel IP, ainsi les en-têtes IP originaux ne sont pas modifiés et un en-tête propre à IPSec est crée.

Ce mode est souvent utilisé pour créer des tunnels entre les réseaux LAN distant. Effectivement, il permet de relier deux passerelles étant capable d'utiliser IPSec sans perturber le trafic IP des machines du réseau qui ne sont donc pas forcément prête à utiliser le protocole IPSec.

3.3.3.4 Gestion des clés du chifferement

IPSec utilise des clés de cryptage pour assurer les services d'authentification, d'intégrité et de chiffrement. La distribution manuelle et automatique des clés est acceptée.

Le niveau le plus bas de gestion est la gestion manuelle dans laquelle une personne configure manuellement chaque système en tapant des informations et des données de gestion de SA relatives à la communication sécurisée avec d'autres systèmes.

Le protocole de gestion automatisé des clés sélectionnées par défaut pour être employé avec IPsec est L'IKE.

L'IKE est un protocole hybride qui permet de réaliser l'echange des clés (clés authentifiée) et de négocier les services de sécurité pour d'autres protocoles comme les protocoles de routage (par exemple RIPv2) [27].

L'IKE provient les trois protocoles suivants [31] :

1. ISAKMP est la structure qui permet l'echange des clés et l'etablissement des SA [25]. Le protocole ISAKMP permet à des entité homologue de couche de communication différentes de sélectionner et de négocier les fonction de sécurité propre à une configuration particuliere.

   D'autre part ISAKMP intégre un mécanisme visant à contrecarrer les attaques de deni de service dans lesquelles les serveurs sont inondés par des faux messages de requettes.

2. *Oakley* décrit une série des types d'échanges de clés appelés modes et détaille les services que chacun d'eux fournit pour les clés.

3. SKEMI décrit une technique de transmission des clés qui permet l'anonymat, la répudiation et le renouvellement rapide des clés.

L'IKE crée un tunnel authentifié sécurisé entre deux entités et négocie ensuite l'association de sécurité pour IPsec. Cela est réalisé en deux phases [31] :

- Dans la phase 1 : les deux correspondants ISAKMP établissent un tunnel sécurisé et authentifié par lequel ils peuvent communiquer. Ce canal est appelé la SA-ISAKMP.
- Dans la phase 2 du processus IKE, les associations de sécurité sont négociées au nom des services tels que AH ou ESP de IPsec.

L'IPSec utilise une clé partagée différente de celle qu'utilise IKE. Elle peut être produite en employant Diffie-Hellman ou en renouvelant le secret partagé dérivé de l'échange original.

La figure 3.24 représente un flot de données partager par l'IPsec :

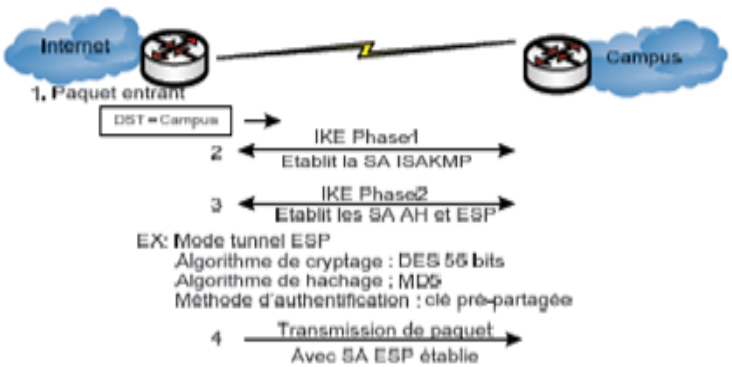

FIGURE 3.24 – Création d'un flot de données partager par l'IPsec

3.4 conclusion :

On souhaite bien qu'à travers ce chapitre, on est arrivé à donner une vue générale du processus d'établissement de la connexion à Internet, ou plus généralement d'une communication en mode paquet ; ainsi que les différentes sortes de routage que vont subir les paquets, en destination ou en provenance d'un mobile, au sein du réseau UMTS.

L'étude de la sécurité du domaine paquet dans le réseau UMTS demeure primordiale, sachant que les données deviennent de jour aprés jour la cible de diverses attaques. De ce fait, nous avons décrit les attaques informatiques les plus envisageables dans le réseau UMTS basé sur le réseau IP. Nous avons noté qu'il convient d'appliquer certaines techniques et de suivre quelques recommandation qui améliorent la sécurité des données dans le domain PS en créant un réseau privé virtuel basé sur le protocole IP Security.

Dans le chapitre suivant, nous proposerons une solution améloirée pour une sécurisation fiables de la transmission des données via le domaine PS du réseau UMTS.

CHAPITRE 4

SIMULATION DE LA SÉCURITÉ DES DONNÉES DU RÉSEAU UMTS SOUS PACKET TRACER :

4.1 Introduction :

Comme nous avons vu dans le chapitre précédent diverses solutions ont été proposées pour la sécurisation du réseau UMTS contre les attaques. L'objectif principal de ce chapitre est de présenté notre solution pour la sécurisation des données transmises via le domaine PS du réseau UMTS, en destination des réseaux extérieures.

Nous commençons d'abord par une description de la topologie utilisée, ensuite nous discutrons de l'environnement du simulateur utilisé pour l'implémentation de la solution de sécurité proposée qui consiste à créer un réseau privé virtuel basé sur le protocole IPSec .

Enfin, nous analyserons la performance de notre topologie avec les différentes simulations.

4.2 L'environnement de la simulation :

La politique de la sécurité est la priorité de chaque operateur. A ce fait, chacun d'eux utilisent des équipements différents pour assurer ce service. Comme dans le cas de l'opérateur MOBILIS, qui utilise des équipements ERICSON.

Durant notre stage au niveau de l'entreprise ATM.MOBILIS de BEJAIA, on a pu comprendre le principe de l'architecture du réseau de troisième génération l'UMTS, ainsi que les équipements qui assurent son fonctionnement. Le stage nous a également pérmis de comprendre l'évolution du réseau GSM vers le réseau UMTS, tout en permettant la coexistence des deux réseaux qui est assuré par des équipements ERICSON, plus exactement par la M-MGw et le MSC-server.

A ceci s'ajoute, qu'on a pu voir l'importance de la politique de la sécurité au niveau des équipements et au niveau du réseau. On a été témoin d'une installation d'une licence de sécurité au niveau du DUW (Digital Unit WCDM) qui est un module du Node B(cf. Figure 4.1).

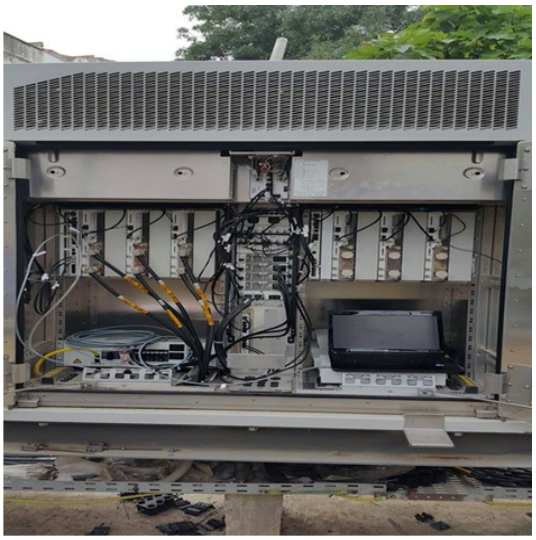

FIGURE 4.1 – L'installation d'une licence de sécurité sur le DUW du node B

Vu que les paquets sont soumis à des risques d'attaques au niveau des réseaux extérieurs. L'idée de notre projet est la sécurisation de transfert de ces paquets de l'usager (cas des entreprises privées équipées des USIM de 60GB/s) via le domaine de commutation de paquet (cf. Figure 4.2) qui consiste a :

- Empêcher la divulgation de données confidentielles,
- Empêcher la modification des données non autorisées ;
- Empêcher l'écoute des paquets ;
- Empêcher le Vol d'information.

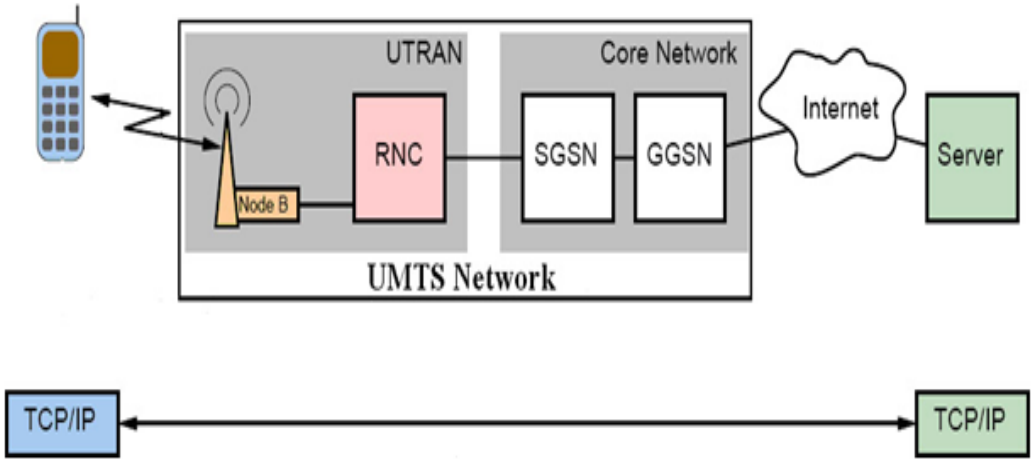

FIGURE 4.2 – Acheminement de donnée via UMTS

Connaissant l'importance de cet acte. Nous n'avons pas pu appliquer notre proposition de sécurité qui consiste à créer un réseau privé virtuel sous le protocole IPSec sur les équipements de l'entreprise, pour des raisons de confidentialité. On a fait appel à un simulateur réseau qui est PACKET TRACER.

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, d'être configurés avec des adresses IP et les services de sécurité suivants :

- La politique de mot de passe : les routeurs et les commutateurs présente plusieurs types et niveaux d'accès (telnet, ligne virtuel, mode enable .. .). Chacun d'eux est protégé par un mot de passe.
- La politique d'exploitation : pour chaque routeur et commutateur, on doit lui définir une politique d'exploitation (protocoles utilisés).
- Le chiffrement des mots de passe.

– La sécurisation de transfert des paquets.

L'avantage principale de ce simulateur est qu'il utilise les équipements CISCO, qui sont compatible à ceux d'ERICSON, car ils sont soumis aux conditions exigées par ISO (International Organization for Standardization).

4.3 Méthode développée pour l'amélioration de la sécurité UMTS :

Afin de répondre aux objectifs de sécurités cités précédemment, nous proposons une nouvelle structure du réseau (cf. Figure 4.3), qui consiste à créer un réseau privé virtuel basé sur le protocole IP Security entre deux GGSN sur deux sites différents.

L'avantage de cette solution est qu'elle est totalement transparente pour les utilisateurs, puisqu'elle donne l'impression d'avoir un réseau en continu.

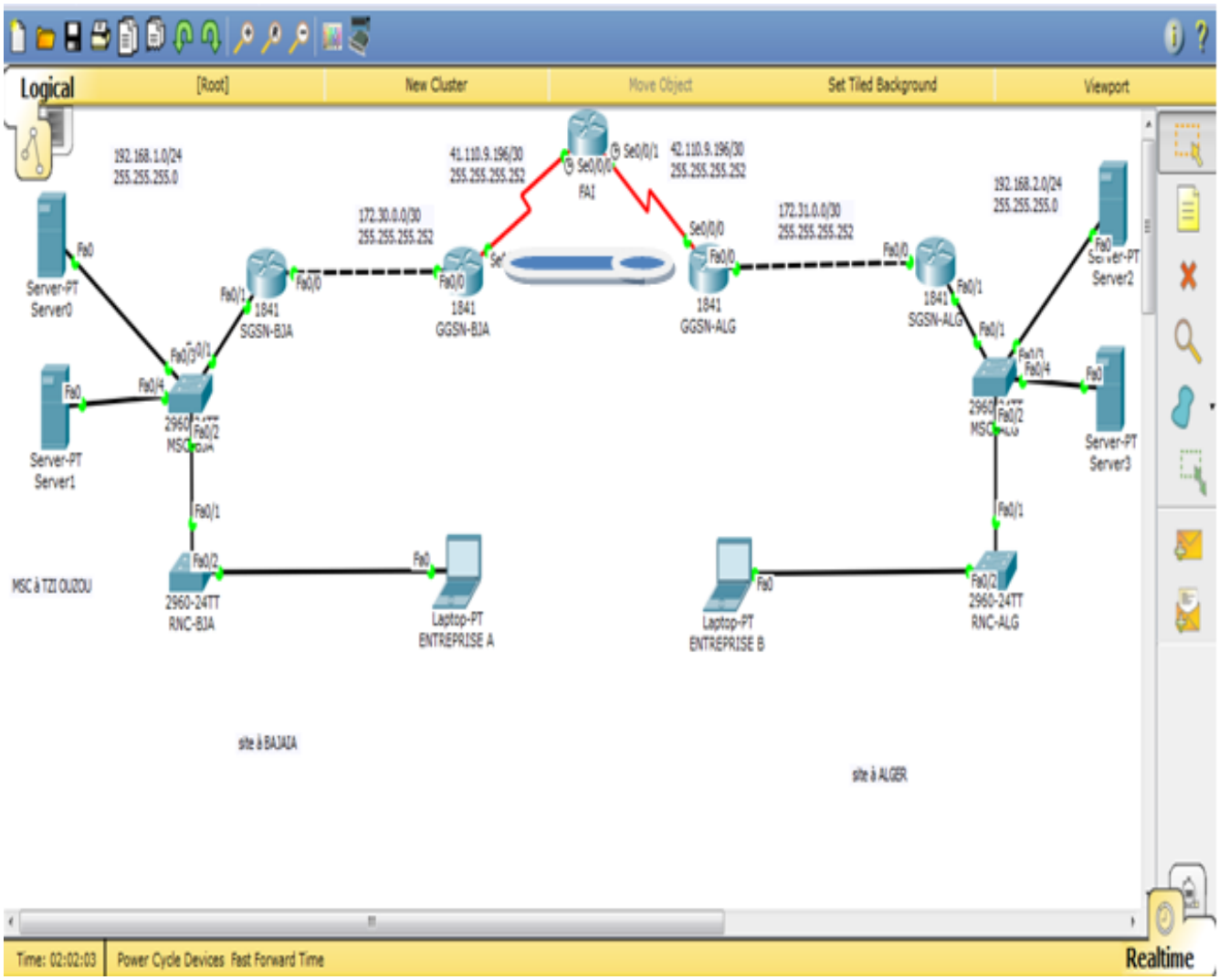

FIGURE 4.3 – Architecture proposée pour un réseau UMTS

4.4 Réalisation du réseau :

Afin de réaliser notre solution de sécurité, on doit d'abord réaliser une architecture du réseau UMTS. Pour cela, on doit faire les étapes suivantes :

- Création de la topologie ;
- Etude de l'adressage IP et de la configurée sur chaque équipement ;
- Configurations des routeurs et switchs ;
- Configurations des parametre de base de la sécurité (les mots de passes et les modes d'accès) sur les equipemets ;
- Configuration de la connexion SSH.

4.4.1 La topologie utilisée :

L'architecture du réseau UMTS présentée sur la figure 4.4, est inspirée de l'architecture réel du réseau UMTS.

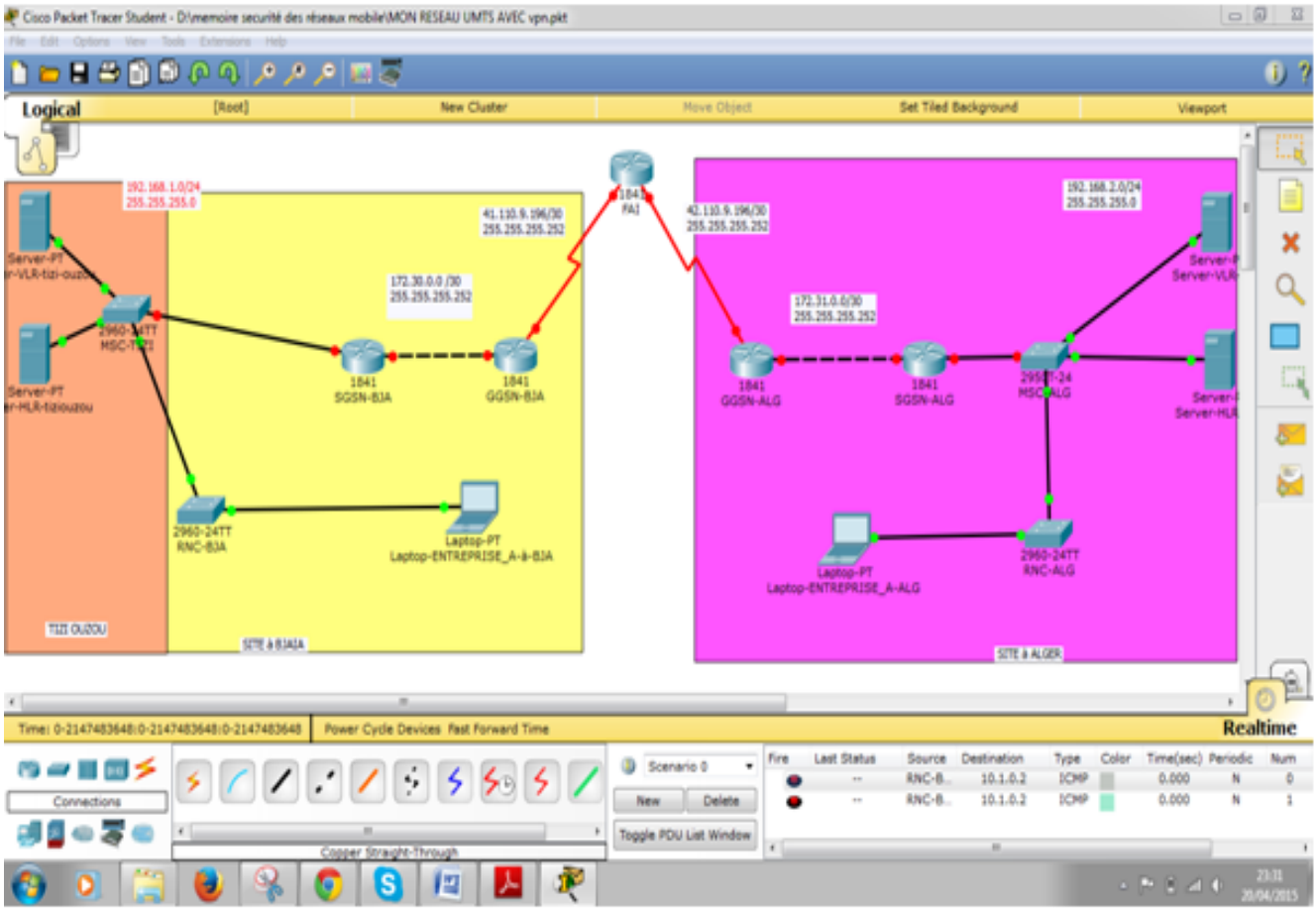

FIGURE 4.4 – L'architecture du réseau UMTS sous Packet Tracer

Au niveau accès réseau (EM-RNC) est présenté sous forme d'une liaison *fastethernet*, afin de simplifier la configuration de notre réseau, mais son architecture réel est présentée sur la figure montrée sur la figure 4.5.

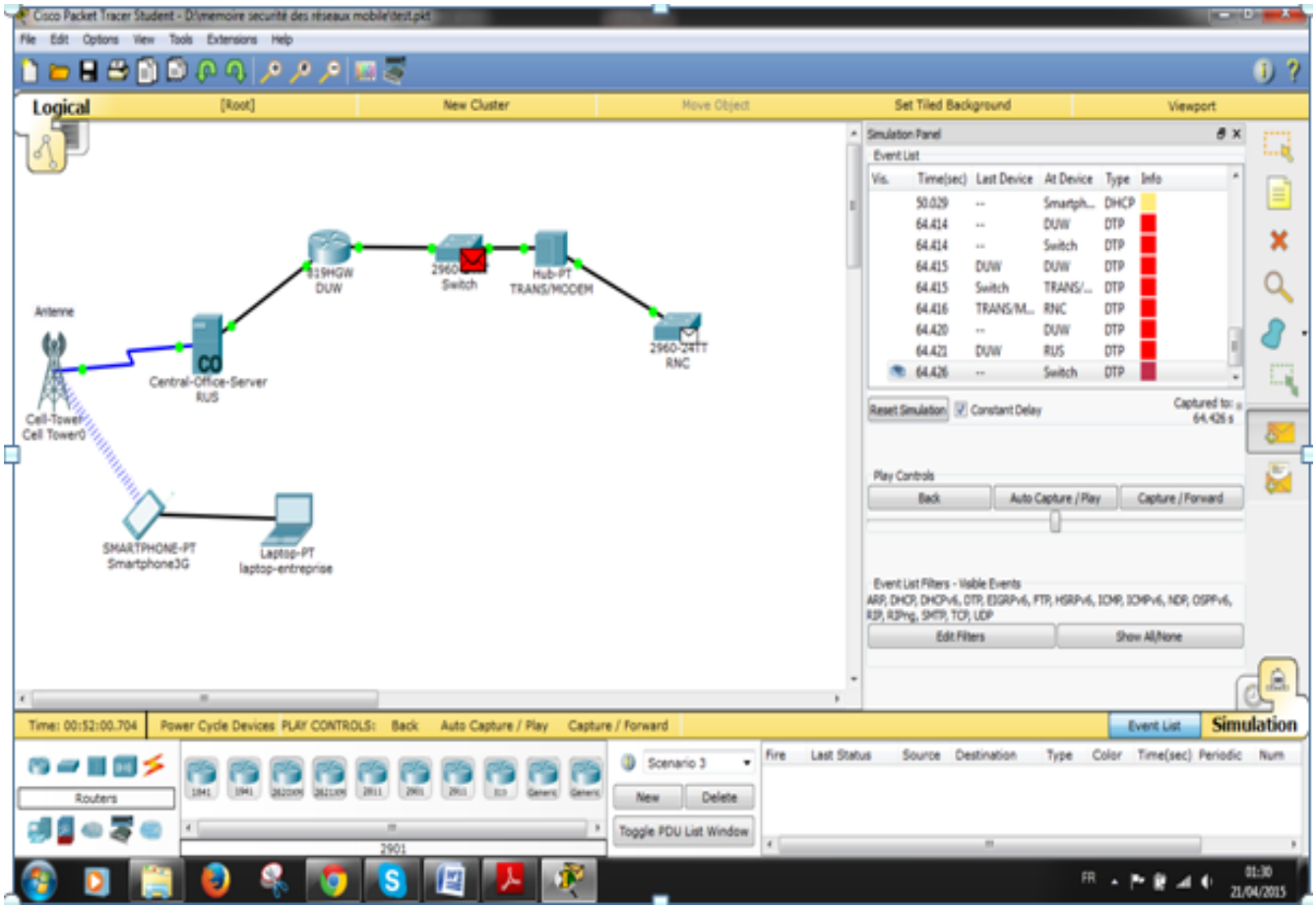

FIGURE 4.5 – L'architecture du réseau UMTS sous Packet Tracer

Table d'adressage IP :

Le choix des adresses n'est pas arbitraire. Cette procédure doit être faite avec délicatesse. Elle est soumise à des exigences ; par exemple , il ne faut pas avoir un conflit d'adressage, ou gaspillement des adresses. Les adresses IP à utiliser doivent être similaires à un cas d'une entreprise.

Afin d'éviter le probléme de gaspillement des adresses, on a procédé au calcul des sous réseaux qui peut étre fait par un calcul manuel ou en utilisant une calcularice d'adresse IP. On présente sur la figure 4.6 un exemple de calcule d'adresse d'un sous réseau avec la calculatrice d'adresse IP. Cette calculatrice nous a aporté beaucoup de résultats soit en affichant les adresses IP à utiliser, le masque sous réseau, le nombre d'hotes...

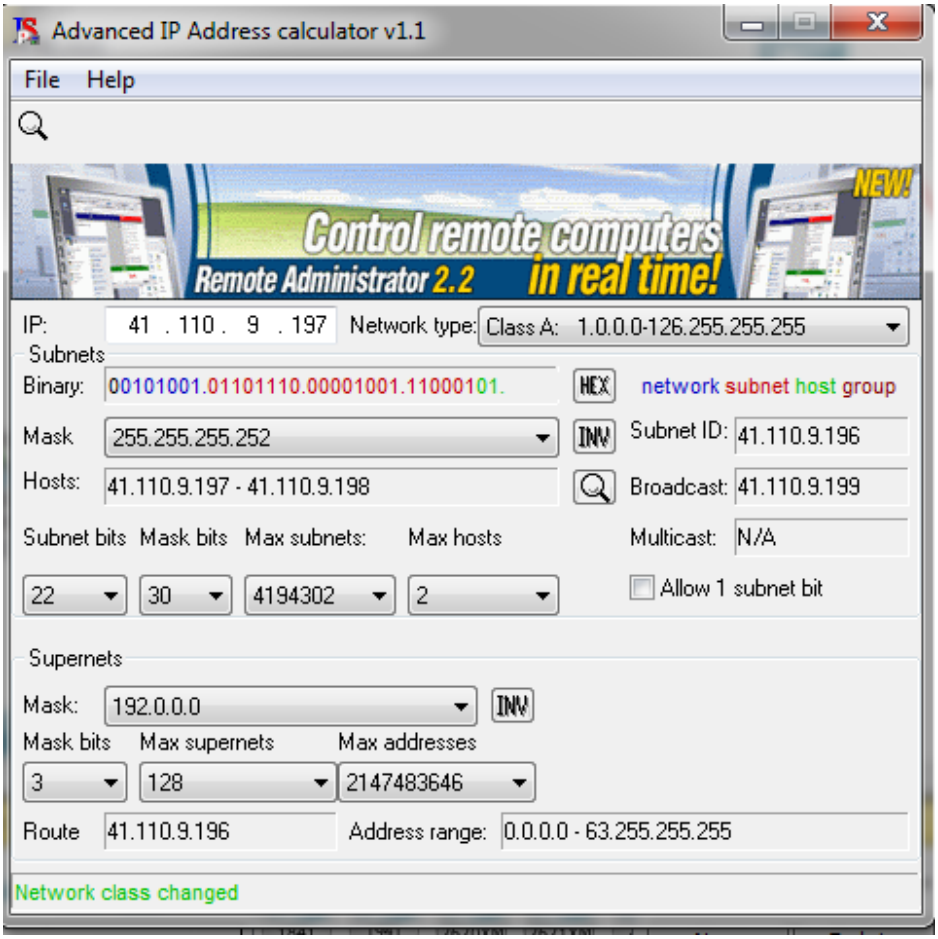

FIGURE 4.6 – Calcul d'une adresse d'un sous réseau

En tenant compte de toute les concidérations expliquées ; nous avons calculé et présenté les résultats dans le tableau 4.1 ;

Périphériques	Interface	Adresse IPV4	Masque sous réseaux	Passerelle
R :FAI	S0/0/0	41.110.9.197	255.255.255.252	
	S0/0/1	42.110.9.197	255.255.255.252	
R :GGSN-BJA	S0/0/0	41.110.9.198	255.255.255.252	
	Fa0/0	172.30.0.1	255.255.255.252	
R :SGSN-BJA	Fa0/0	172.30.0.2	255.255.255.252	
	Fa0/1	192.168.1.1	255.255.255.0	
R : GGSN-ALG	S0/0/0	42.110.9.198	255.255.255.252	
	Fa0/0	172.31.0.1	255.255.255.252	
R : SGSN-ALG	Fa0/0	172.31.0.2	255.255.255.252	
	Fa0/1	192.168.2.1	255.255.255.0	
S : MSC-TIZI OUZOU	VLAN1	192.168.1.4	255.255.255.0	192.168.1.1
S : RNC-BJA	VLAN1	192.168.1.3	255.255.255.0	192.168.1.1
S : MSC-ALG	VLAN1	192.168.2.3	255.255.255.0	192.168.2.1
S : RNC-ALG	VLAN1	192.168.2.4	255.255.255.0	192.168.2.1
PC : entreprise BJA		192.168.1.30	255.255.255.0	192.168.1.1
PC : derection ALG		192.168.2.30	255.255.255.0	192.168.2.1
Serveur HLR-TIZI OUZOU		192.168.1.29	255.255.255.0	192.168.1.1
Serveur VLR-TIZI OUZOU		192.168.1.29	255.255.255.0	192.168.1.1
Serveur HLR-ALG		192.168.1.28	255.255.255.0	192.168.2.1
Serveur VLR-ALG		192.168.1.29	255.255.255.0	192.168.2.1

TABLE 4.1 – Table d'adressage

4.4.2 Configuration de base du réseau :

Afin que notre réseau fonctionne comme un cas réel et pérmetre le transfert des données à des distances lointaines, il faut procéder à des configurations et la mise en sérvice des équipements utilisés (routeurs, commutateurs, les serveurs, les ordinateurs et configurations des routes d'echange de paquets).

4.4.2.1 Configuration des routeurs :

Configuration de base des routeurs :

Pour une configuration initiale d'un périphérique réseau, on utilise un câble *console* (cf. Figure 4.7). L'avantage d'utiliser un port de *console* est que le périphérique est accessible même si aucun service réseau n'a été configuré.

Le port *console* peut également être utilisé lorsque les services réseau ont échoué ou lorsque l'accès à distance au périphérique Cisco IOS est impossible [33].

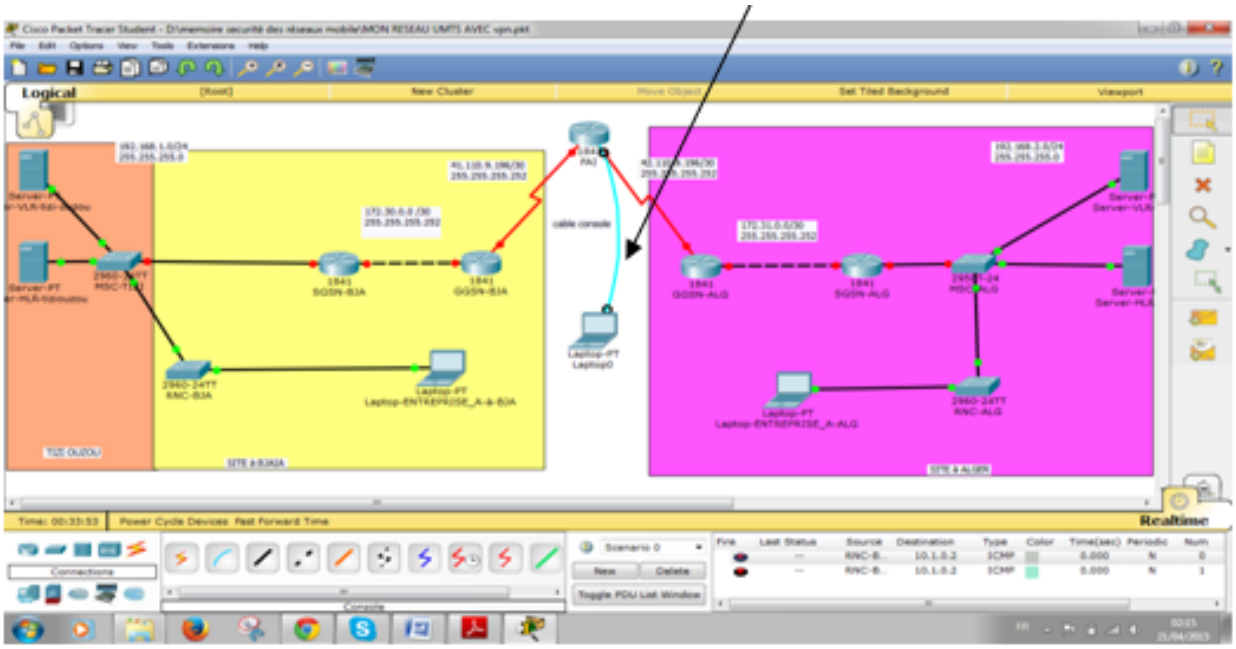

FIGURE 4.7 – L'accès au routeur avec un câble *console*

Etape 1 : Configuration du nom du routeur :
Il permet d'attribué un nom à un routeur.

Router(config)#hostname FAI FAI(config)#

Etape 2 : Configuration du mot de passe *enable* :
Les mots de passe *enable secret* sont utilisés pour empêcher l'accès au mode privilègié.Il est crypté en utilisant un puissant algorithme MD5.
La commande suivante permet de définir les mots de passe *enable* :

FAI(config)#enable secret mobilis

Etape 3 : Configuration du mot de passe de l'accès *console* :
Les commandes suivantes permettent de définir un mot de passe facultatif mais recommandé sur la ligne *console* :

FAI(config)#line console 0
FAI(config-line)#PASsword mobilis
FAI(config-line)#login

Etape 4 : Configuration de mot de passe des lignes *VTY* :

Pour qu'un utilisateur puisse accéder à un routeur à distance via *telnet*. Un mot de passe doit être défini sur une ou plusieurs lignes du terminal virtuel (vty).

Les commandes suivantes permettent de définir un mot de passe sur les lignes *VTY* :

FAI(config)#line vty 0 4
FAI(config-line)#password mobilis FAI(config-line)#login

Etape 5 : Chiffrer les mots de passes :

Il est parfois préférable que les mots de passe ne soient pas affichés en texte clair dans les résultats des commandes *show running-config* ou *show startup-config*.

La commande suivante permet de crypter les mots de passes :

FAI(config)#service password-encryption

Etape 6 : Configurez une bannière *MOTD* :

La bannière *MOTD* affiche tous les terminaux connectés à la connexion et permet de transmettre des messages destinés à tous les utilisateurs du réseau (pour les avertir, par exemple, d'un arrêt imminent du système)[31]. La bannière *MOTD* apparaît avant la configuration de la bannière de connexion.

FAI(config)#banner motd #ATTENTION ROUTEUR SECURISEE#

Etape 7 : Désactiver la recherche DNS :

Désactivation de la résolution DNS empêche la conversion du nom d'hôte de type DNS en adresse. Cette commande est activée par défaut.

La commande suivante permet de désactiver la recherche DNS :

FAI(config)#no ip domain-lookup

Etape 8 : Configuration des interfaces du routeur *(serial/ fastethernet)* :

Cette configuration permet d'attribuer à chaque interface de l'équipement des adresses IP, comme est montre dans la configuration suivante :

FAI(config)#interface serial 0/0/0
FAI(config-if)#ip address 41.110.9.198 255.255.255.252
FAI(config-if)#clock rate 128000
FAI(config-if)#no shutdown
FAI(config)#interface serial 0/0/1
FAI(config-if)#ip address 42.110.9.197 255.255.255.252
FAI(config-if)#clock rate 128000
FAI(config-if)#no shutdown

Etape 9 : Enregistrer la configuration en cours dans le fichier de configuration initial :

Apres la configuration des équipements, on doit enregistrer les configurations effectuées selon la commande suivante :

FAI#copy running-config startup-config

Remarque : La configuration des quatre routeurs se fait de la même façon, sauf au niveau de la configuration des interfaces qui vont être configurés selon le tableau 4.1.

Configuration du routage dynamique sur les routeurs :

Les protocoles de routage[23](Voir l'Annexe) déterminent le meilleur chemin, ou la meilleure route, vers chaque réseau [33]. Cette route est alors ajoutée à la table de routage. L'un des principaux avantages des protocoles de routage dynamique est l'échange d'informations de routage entre les routeurs lors de la modification de la topologie.

Le tableau 4.2représente les adresses des routes configurées sur les routeurs de notre réseau ; apres avoir déterminé les adresses de la partie réseau de chaque réseau utilisé selon le tableau 4.1 et la calsse des adresses :

Les routeures	les routes statiques
SGSN-BJA	172.30.0.0 192.168.1.0
GGSN-BJA	41.0.0.0 172.30.0.0
SGSN-ALG	172.31.0.0 192.168.2.0
GGSN-ALG	42.0.0.0 172.31.0.0
FAI	41.0.0.0 42.0.0.0

TABLE 4.2 – Les routes statiques des routeurs utilisées

Exemple d'une configuration du routage dynamique sur le routeur SGSN-BEJ (cf. Figure4.8) :

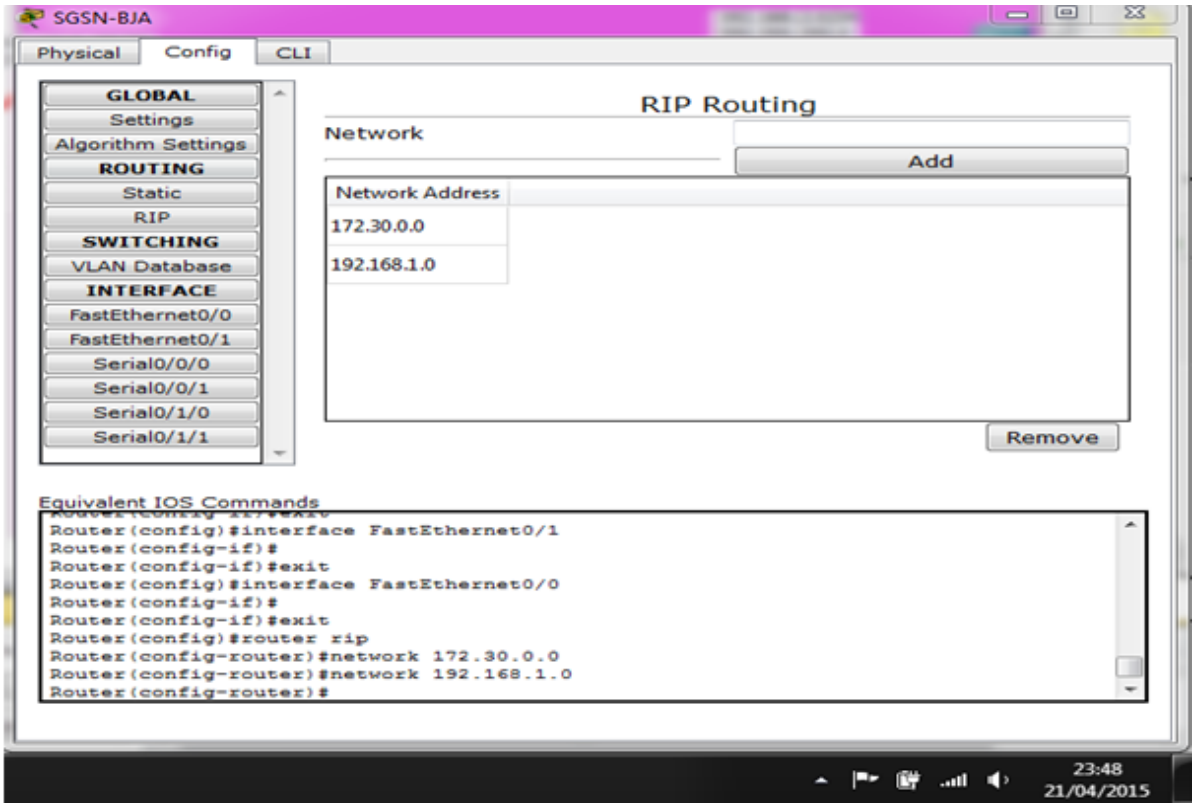

FIGURE 4.8 – Configuration des routes sur SGSN-BJA

Configuration des routeurs pour un accès SSH :

Le protocole *Secure Shell (SSH)* fournit une connexion à distance en utilisant des services réseau plus sécurisés [33]. SSH fournit une authentification par mot de passe plus résistante et emploie un chiffrement lors du transport des données de la session.

Pour réaliser cette configuration, il faut suivre les étapes suivantes :

Etape 1 : Configurer le domaine du périphérique :

GGSN-BJA(config)#ip domain-name mobilis.dz

Etape 2 : Configurer la clée de chiffrement :

Le protocole SSH utilise les clés RSA pour le chiffrement de ces données tous en choisissant le nombre de bit nécessaire :

GGSN-BJA(config)#crypto key generate rsa
GGSN-BJA(config)#crypto key gHow many bits in the modulus [512] : 1024

Etape 3 : Configurer un nom d'utilisateur de base de données locale :

Pour un accès SSH, l'administrateur doit identifier un nom d'administrateur et un mot de passe comme suit :

GGSN-BJA(config)#USErname ADMIN SEcret mobilis

Etape 4 : Activez SSH sur les lignes VTY :

GGSN-BJA(config)#line vty 0 4
GGSN-BJA(config-line)#transport input SSH
GGSN-BJA(config-line)#login local
GGSN-BJA(config-line)#end

4.4.2.2 Configuration des commutateurs :

Configuration de base des commutateurs :

Pour une configuration de base des commutateurs ; elle se fait de la même façon que les routeurs avec un câble *console* et on procéde à faire toutes les étapes citées précédemment pour une gonfiguration de base. Sauf dans ce cas, on ne va pas configurer le routage dynamique mais on procède à la configuration des VLANs.

Etape 1 :configuration du mode bidirectionnelle et la vitesse entre deux commutateurs :

Les communications bidirectionnelles simultanées améliorent les performances d'un réseau LAN commuté [31]. Elles augmentent la bande passante réelle, car les deux extrémités de la connexion transmettent et reçoivent simultanément des données.

Les commandes de cette configuration est comme suit :

MSC-TIZI(config)#interface fastEthernet 0/2
MSC-TIZI(config-if)#duplex full
MSC-TIZI(config-if)#speed 100

Etape 2 :configuration du VLAN par défaut :

MSC-TIZI(config)#INTERface VLAN 1
MSC-TIZI(config-if)#ip address 192.168.1.4 255.255.255.0

Etape 3 : configuration de la passerelle :

MSC-TIZI(config)#IP DEFAult-gateway 192.168.1.1

Remarque : La configuration pour une connexion SSH fait avec la même procédure que celle des routeurs.

La configuration des quatre commutateurs se fait de la même façon, sauf au niveau de la configuration des interfaces qui vont être configurés selon le tableau 4.1.

4.4.2.3 Configuration de bases des ordinateurs et serveurs :

Dans cette configuration, on a attribué à chaque ordinateur une adresse IP, un masque sous réseau, et une adresse passerelle selon le tableau 4.1.

Exemple d'une configuration des adresses IP sur l'ordinateur de la dérection à ALG (cf. Figure 4.9) :

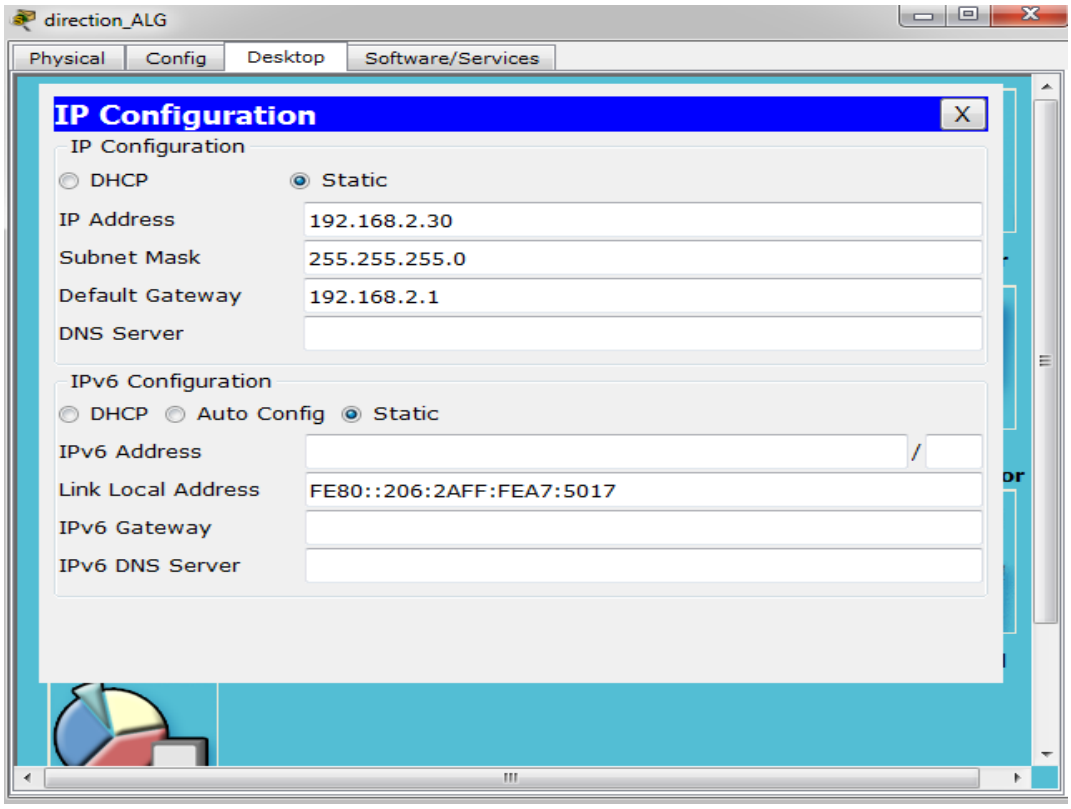

FIGURE 4.9 – Configuration de l'adresse IP sur l'ordinateur de la dérection ALG

Remarque : La configuration des quatres serveurs se fait de la même façon, sauf au niveau de la configuration des interfaces qui vont être configurés selon le tableau 4.1.

4.4.3 Les résultats des configurations de bases :

Apres avoir configuré notre réseau, on vérifie la connectivité entre les différents équipements du réseau.

4.4.3.1 Vérification dans le mode *REALTIME* :

D'apres la figure 4.10, on remarque que les LED sont devenu vert qui signifie que notre réseau a été configurer et qu'il représente aucun conflit d'adressage.

De plus, en faisant un *ping* entre ces équipements a été réussi, où il s'affiche un commentaire *successful* dans la fenêtre *TOGGLE PDU*.Cela signifie que la trame arrive sur chaque éléments du réseau.

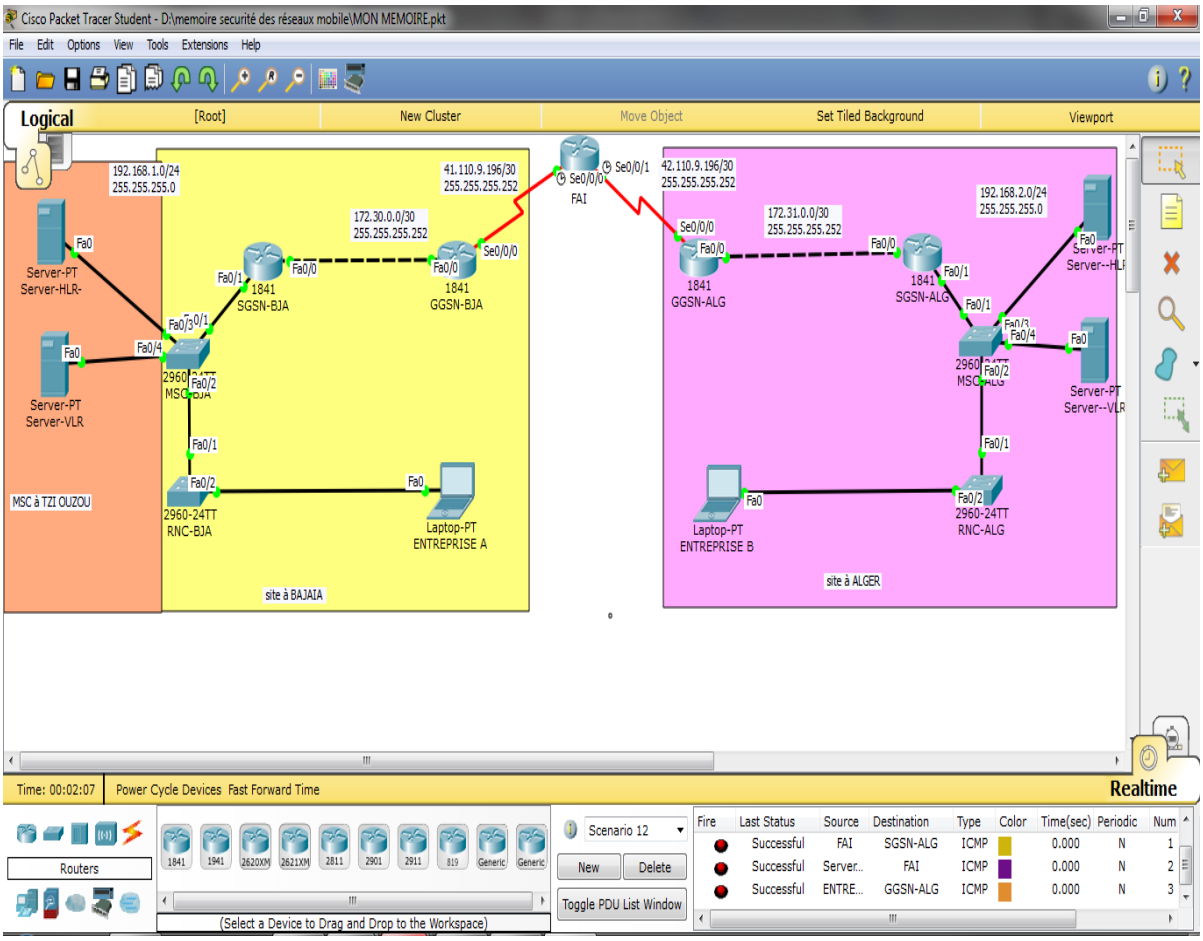

FIGURE 4.10 – Le réseau UMTS aprés la configuration de tout les équipements

4.4.3.2 Vérification en mode *SIMULATION* :

Dans cette partie, on visualise sur la figure 4.11 que les paquets sont échangés entre les équipements du réseau, ce qui signifie que les routes et les équipements ont êté bien configurées. On remarque aussi que les protocoles de routages sont activés comme le cas du protocole RIPv2, ainsi que le cache ARP.

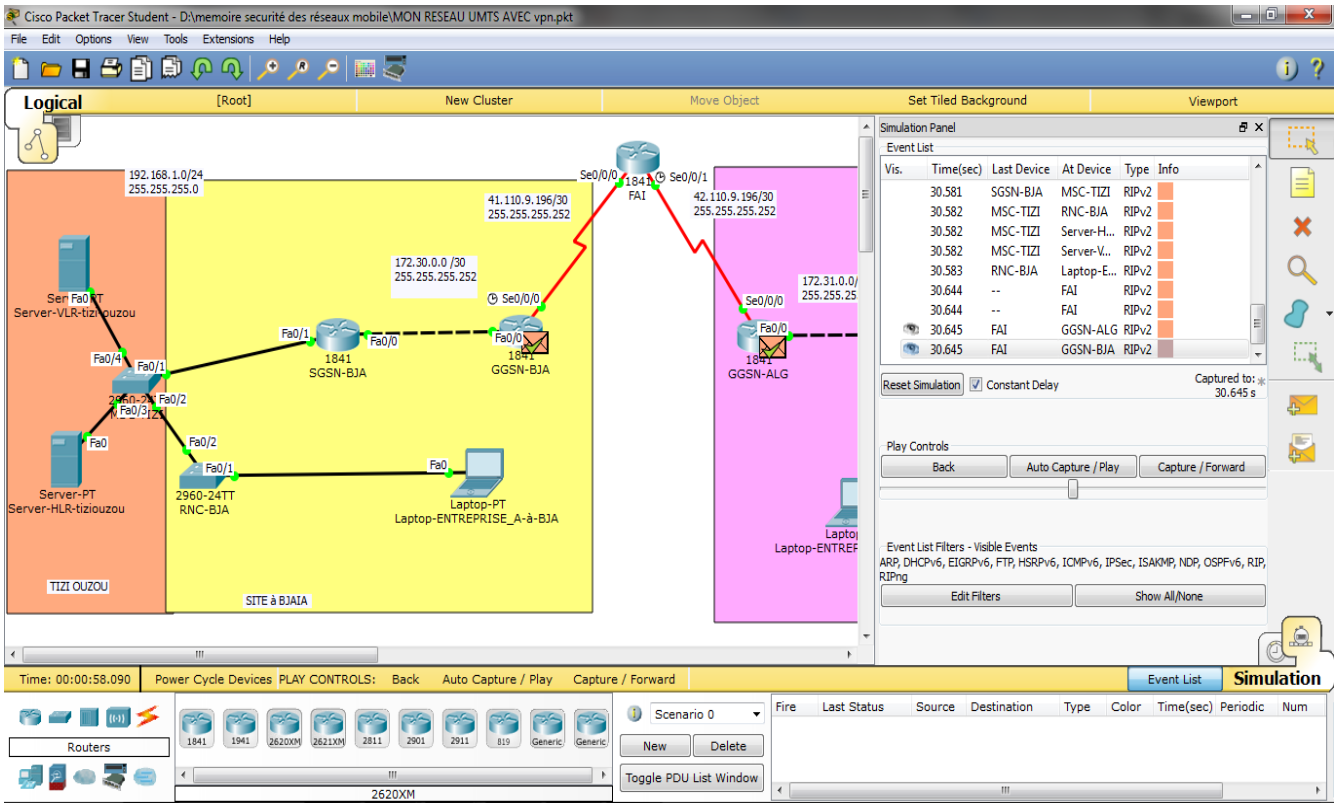

FIGURE 4.11 – Le réseau UMTS en mode simulation

4.4.3.3 Vérification des configurations des mots de passes :

Comme le montre la figure 4.12, on constate que les mots de passe ont été bien configurés et chiffrés pour l'accés *console*, les lines VTY et auxiliaires.

4.4.3.4 Vérification de la connectivité entre les 2 entreprises :

On constate que les deux entreprises communiquent entre elle,comme le montre La figure 4.13 montre que les deux entreprises communiquent entre elles, c'est-à-dire, lors de l'envoie des paquet d'une entreprise à une autre, le paquet arrive sans aucun probleme, aucune pérte d'information, et la durée du transfert ne depasse pas la limite maximum qui est de 26ms :

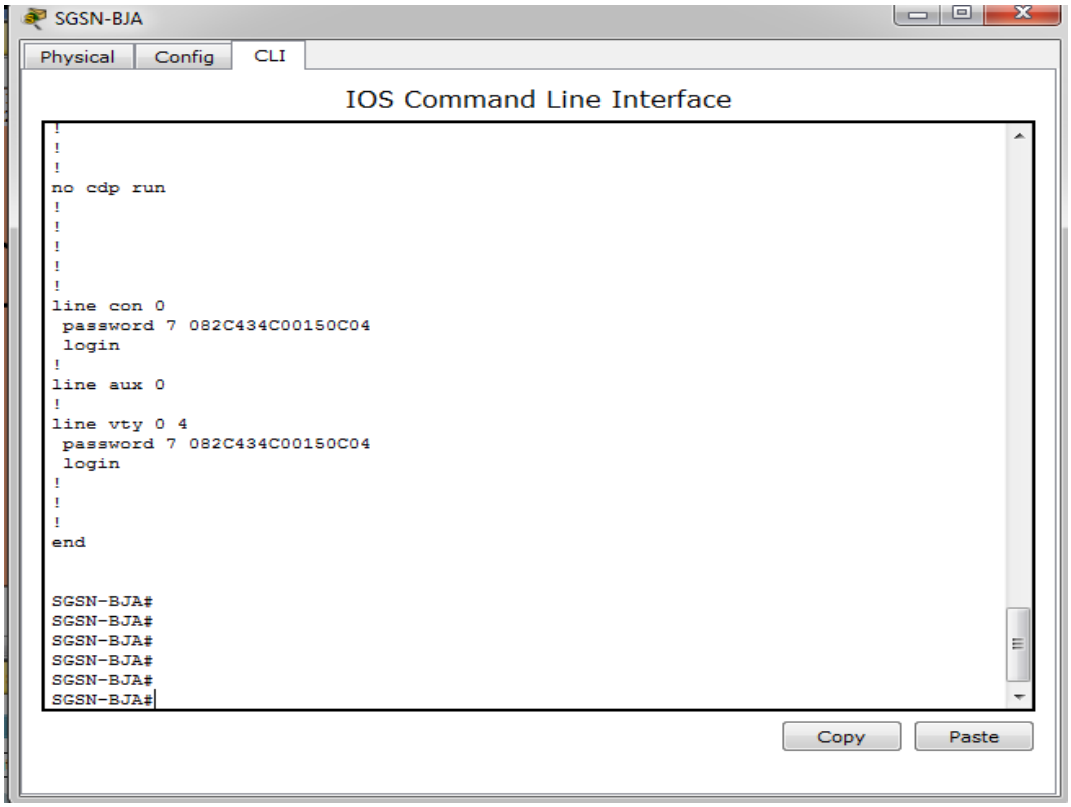

FIGURE 4.12 – Vérification des configuration des mots de passe

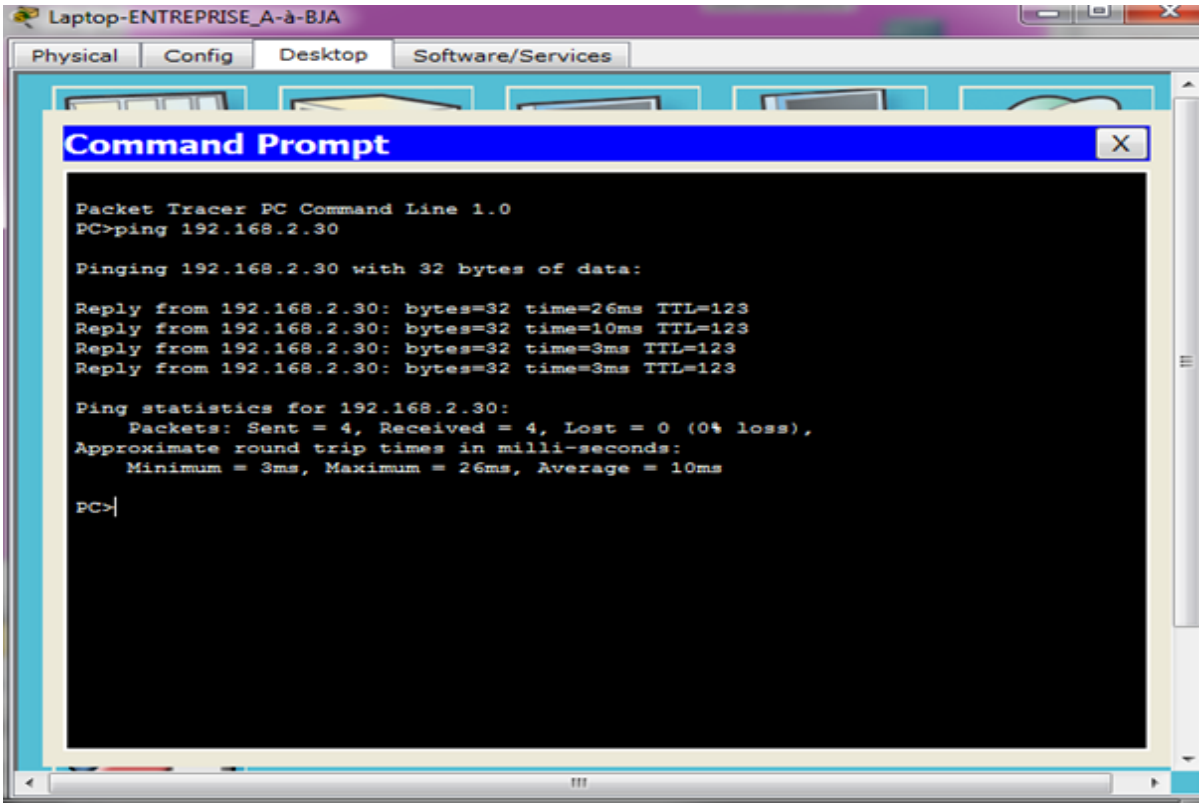

FIGURE 4.13 – Connectivité réussie entre les entreprises

4.5 La mise en œuvre de la solution de sécurité : Configuration du VPNIPSec

Voici les différentes étapes afin de configurer la solution de sécurité basé sur la création d'un VPN sous le protocole IP Security sur les routeurs GGSN-BJA et GGSN-ALG :

- Définir les règles de sécurité ISAKMP.
- Configurer les « *transform set* ».
- Configurer une ACL qui spécifiera quel trafic peut/doit emprunter le VPN.
- Configurer une « *crypto-map* »
- Appliquer la « *crypto-map* » sur l'interface
- Configurer une ACL sur l'interface « *outside* »

Définir une règle de sécurité ISAKMP :

Nous devons d'abord activer le moteur « isakmp »en utilisant la commande suivante :

GGSN-BJA(config)#crypto isakmp enable

Configuration des paramètres du VPN :

Cette étape consiste à configurer les règles IKE sur les deux routeurs. Les règles IKE précisent le type d'encryptions et de découpage à utilisé ainsi le type d'authentification. Comme le montre les commandes suivantes :

GGSN-BJA(config)#crypto isakmp policy 10
GGSN-BJA(config-isakmp)#encryption AES 256
GGSN-BJA(config-isakmp)#authentication pre-share
GGSN-BJA(config-isakmp)#group 5
GGSN-BJA(config-isakmp)#encryption 3des
GGSN-BJA(config-isakmp)#Hash Md5
GGSN-BJA(config-isakmp)# lifetime 3600
GGSN-BJA(config-isakmp)#EXIT

Explication :

- encryption AES 256 / encryption 3des : type d'endcryptage sur 256 bit.
- authentication pre-share : Précise qu'aucun certificat d'autorité ne sera utilisé.
- group 5 : Spécifie l'identifiant Diffie-Hallman.
- Hash Md5 : Précise le type de découpage.
- lifetime 3600 : c'est la durée de vie de l'échange de clé. Nous utiliserons 3600 secondes pour 1 heure. (Par défaut 86400 secondes, une journée).

Configuration des *transform-set* :

Une « *transform-set* » est une combinaison d'algorithmes et protocoles de sécurité «compatibles»[31]. Les routeurs essaieront de trouver la meilleure combinaison possible

selon les configurations et capacités de chaque point de chute du VPN en se basant sur les « *transform-set* » disponibles.

GGSN-BJA(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac

Association de la sécurité :
C'est le délai pour renégocier les clés de chiffrement, s'il y a pas d'échange de clés.

GGSN-BJA(config)#crypto ipsec security-association lifetime seconds 1800

Configuration de la clé de partage :
Sur un routeur, on configure la clé qui correspond au partenaire IPsec , comme suit :

GGSN-BJA(config)#crypto isakmp key mobilis address 42.110.9.198

Configuration des ACL :
Elles permettent d'autoriser le trafic entre les sites distants.

GGSN-BJA(config)#access-list 101 Permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

Configuration du « *crypto map* » :
Le « *crypto map* » permet d'associé l'access-list, le trafic ; et la destination :

GGSN-BJA(config)#CRYpto map mobilis_map 10 ipsec-isakmp
GGSN-BJA(config-crypto-map)#set peer 42.110.9.197
GGSN-BJA(config-crypto-map)#Set Transform-set 50
GGSN-BJA(config-crypto-map)#SEt Security-association LIfetime Seconds 900
GGSN-BJA(config-crypto-map)#Match Address 101
GGSN-BJA(config-crypto-map)#exit

Configuration sur les interfaces de sortie :
Pour que les fonctions précédentes puissent fonctionner. Il faut assigner la carte de criptage sur l'interface WAN du routeur, comme il est montré dans la configuration suivante :

GGSN-BJA(config)#INterface serial 0/0/0
GGSN-BJA(config-if)# CRypto map mobilis_map

Remarque :
Toutes ces configurations doivent etre configurées sur l'autre routeur GGSN-ALG . mais avac une légere difference au niveau de l'aderessage qui vont être comme suit :

- La configuration de la clé de partage qui va être sous l'adresse suivante : 41.110.9.198.
- La configuration des ACL pour l'autorisation du trafic qui : de 192.168.2.0 0.0.0.255 vers 192.168.1.0 0.0.0.255.

– La configuration du *crypto map* où on défini l'ensemble des paires 41.110.9.197.

4.5.1 Simulation et Résultats des configurations :

4.5.1.1 Em mode simulation :

On remarque que dés le lancement de la simulation (cf. Figure 4.14), le moteur ISKAMP s'active le premier puis l'aplication du protocole sur l'interface des deux routeurs, qui signifie qu'il y a une négociation des fonctions de sécurité configurées.

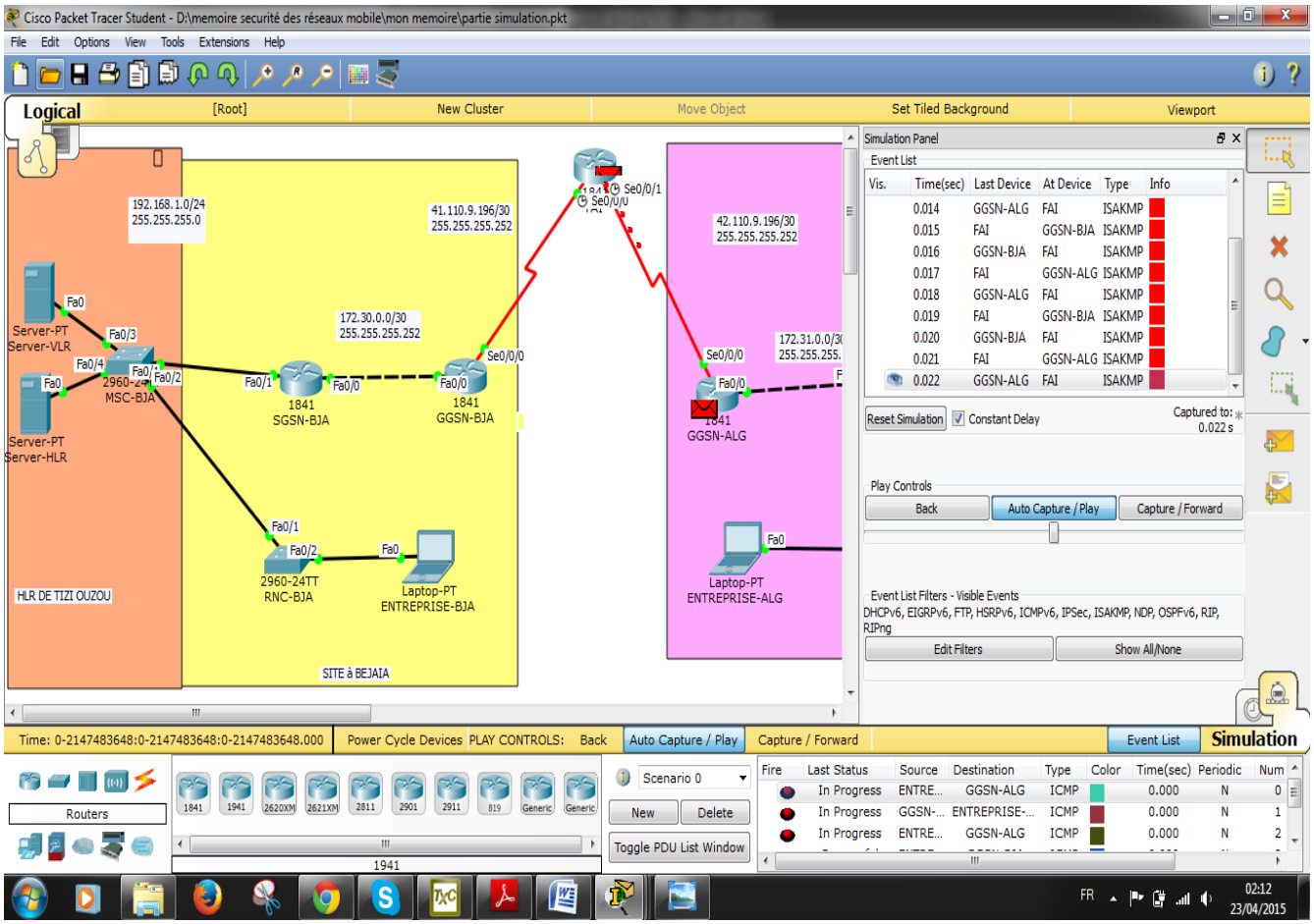

FIGURE 4.14 – L'activation de ISKAMP

On voit sur la figure 4.15 le lancement du protocole IPSec entre les deux routeurs, comme est montré sur la fenêtre *simulation panel*. Son activation dure une tres petite période de temps qui arrive à 2.877s.

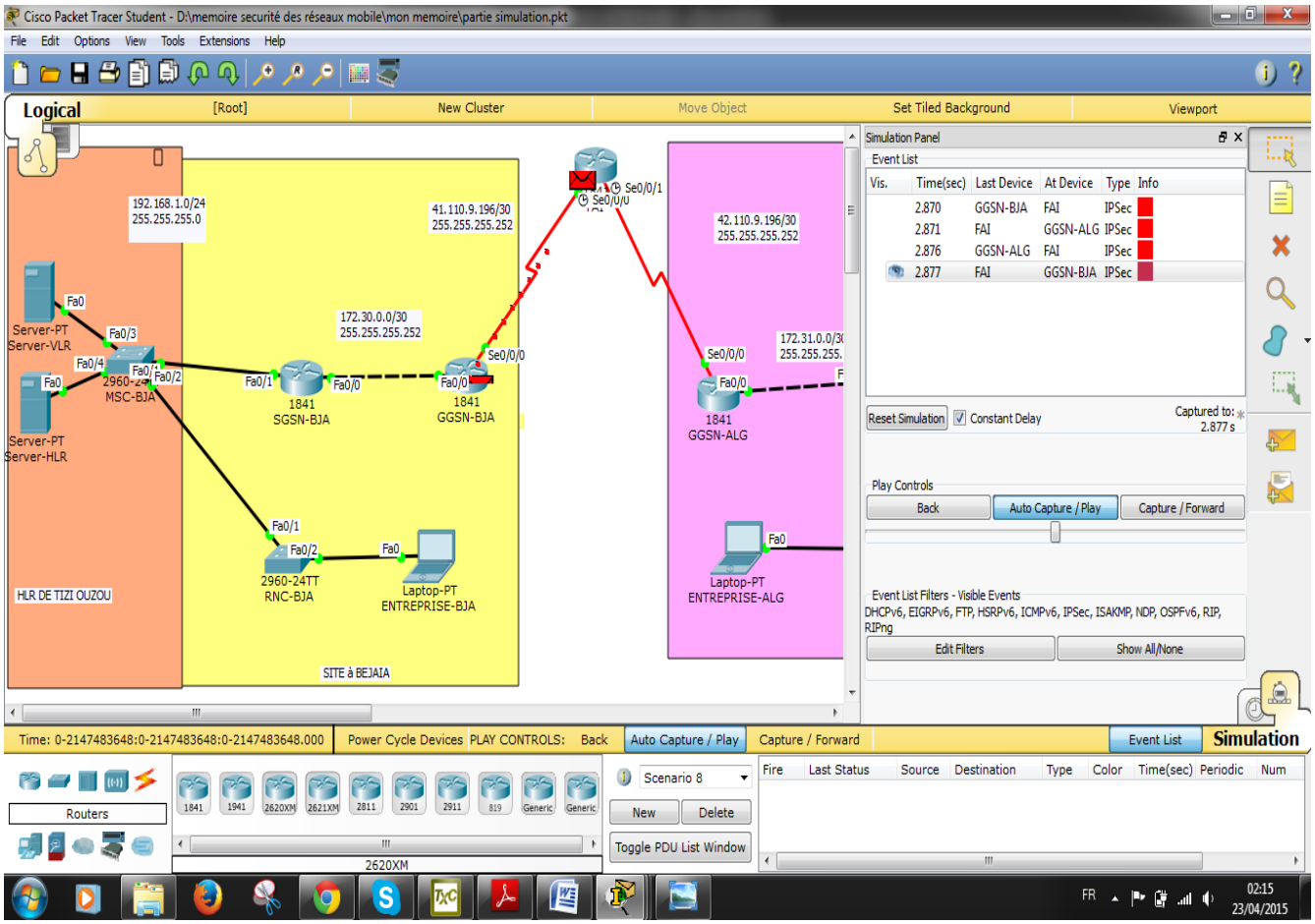

FIGURE 4.15 – L'activation du protocole IPSec

4.5.1.2 Rélisation d'un ping :

Selon ces résultats (cf. Figure 4.16), la communication n'est pas coupée. Le paquet est arrivé à l'entreprise distante durant une petite période du temps de 2ms moins que celle d'une configuration sans VPN et sans perte d'information.

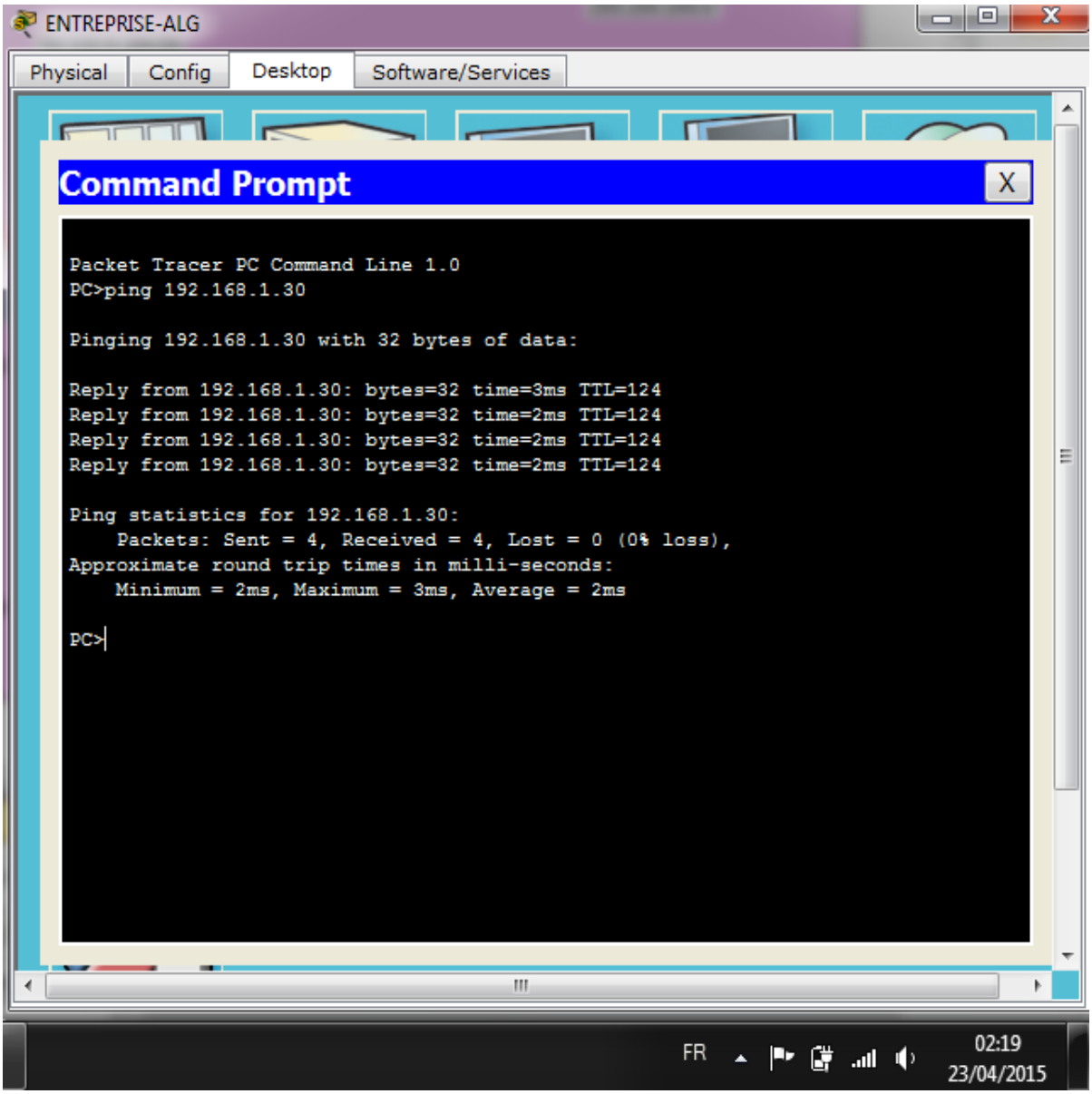

FIGURE 4.16 – Réalisation du ping

4.5.1.3 Vérification du *MAP* du VPN :

On constate que les interfaces ont été bien configurées, ainsi les acces-list.

La figure 4.17 montre que l'accés est permi pour le transfert des paquets de ce réseau (BJA) vers l'autre réseau distant (ALG) en spicifiant l'interface de réception qui est 42.110.9.198. A ce ci s'ajout , qu'elle nous montre que l'ensemble de paires est avctivé, l'accés des listes est valide, le transfert entre les sites est pérmis en spécifiant l'interface d'échange.

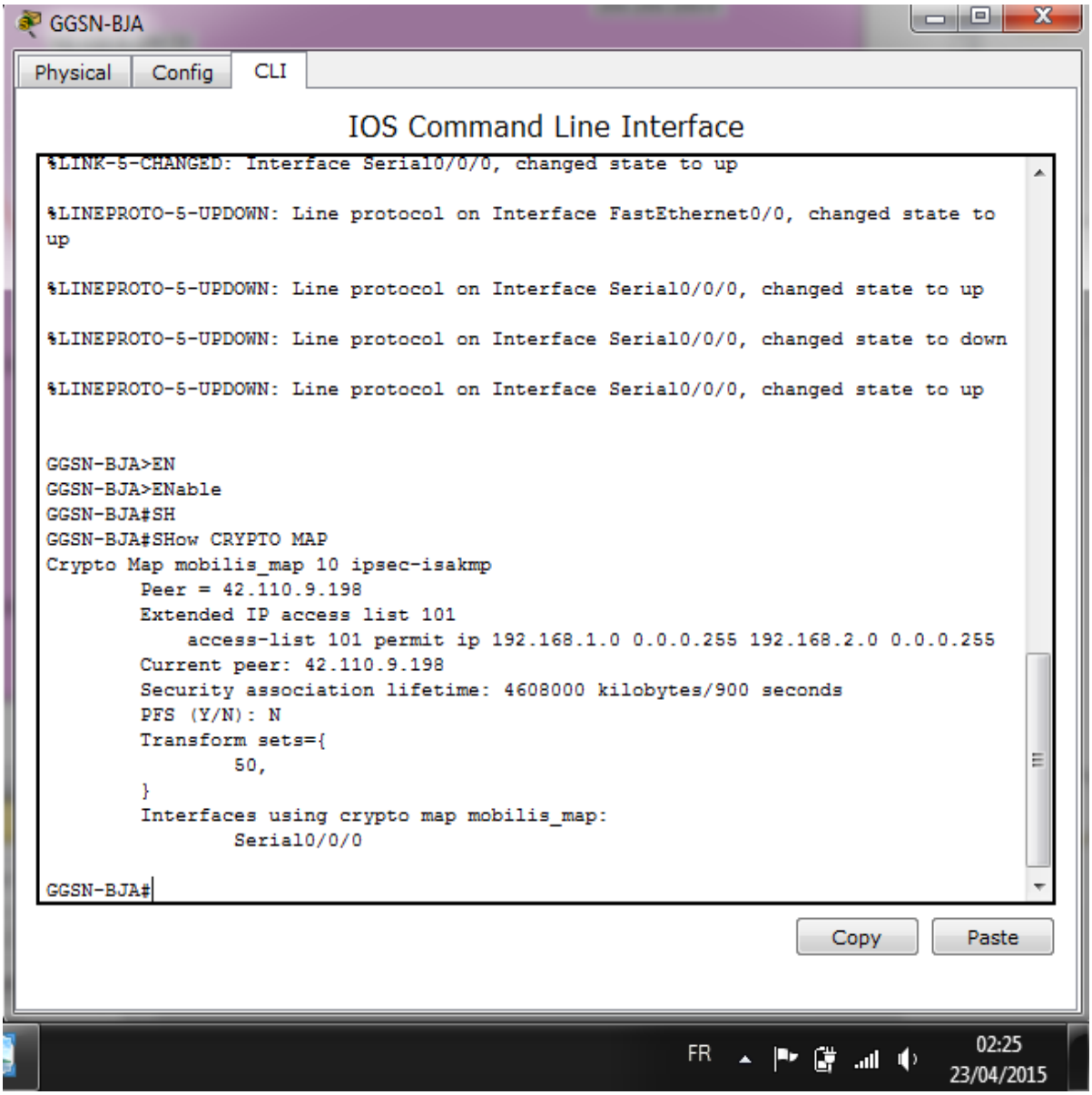

FIGURE 4.17 – Le map VPN sur le routeur GGSN-BJA

La figure 4.18 montre que l'accés est permis pour le transfert des paquets de ce réseau (ALG) vers l'autre réseau distant (BJA) en spicifiant l'interface de réception qui est 42.110.9.198. A ce ci s'ajoute, qu'elle nous montre que l'ensemble de paires sont activés, l'accés des listes est valide, le transfert entre les sites est pérmis en spécifiant l'interface d'échange.

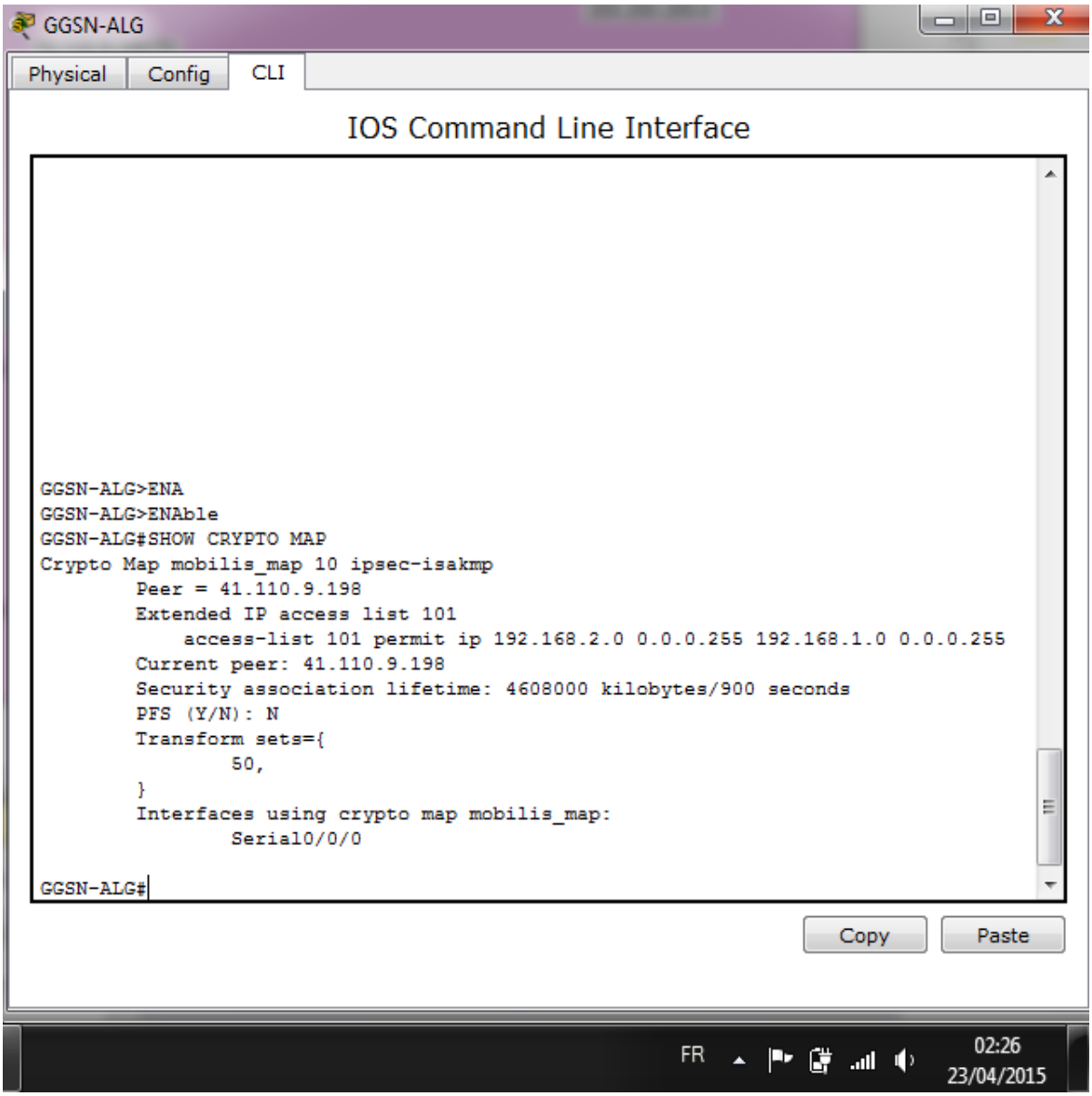

FIGURE 4.18 – Le map VPN sur le routeur GGSN-ALG

4.5.1.4 Verification des opérations IPSec :

On remarque aussi que les opérations de IPSEC sont bien activées, les algorithmes de cryptage fonctiones et le mode TUNNEL est activé sur le routeur GGSN-BJA (cf. Figure 4.19).

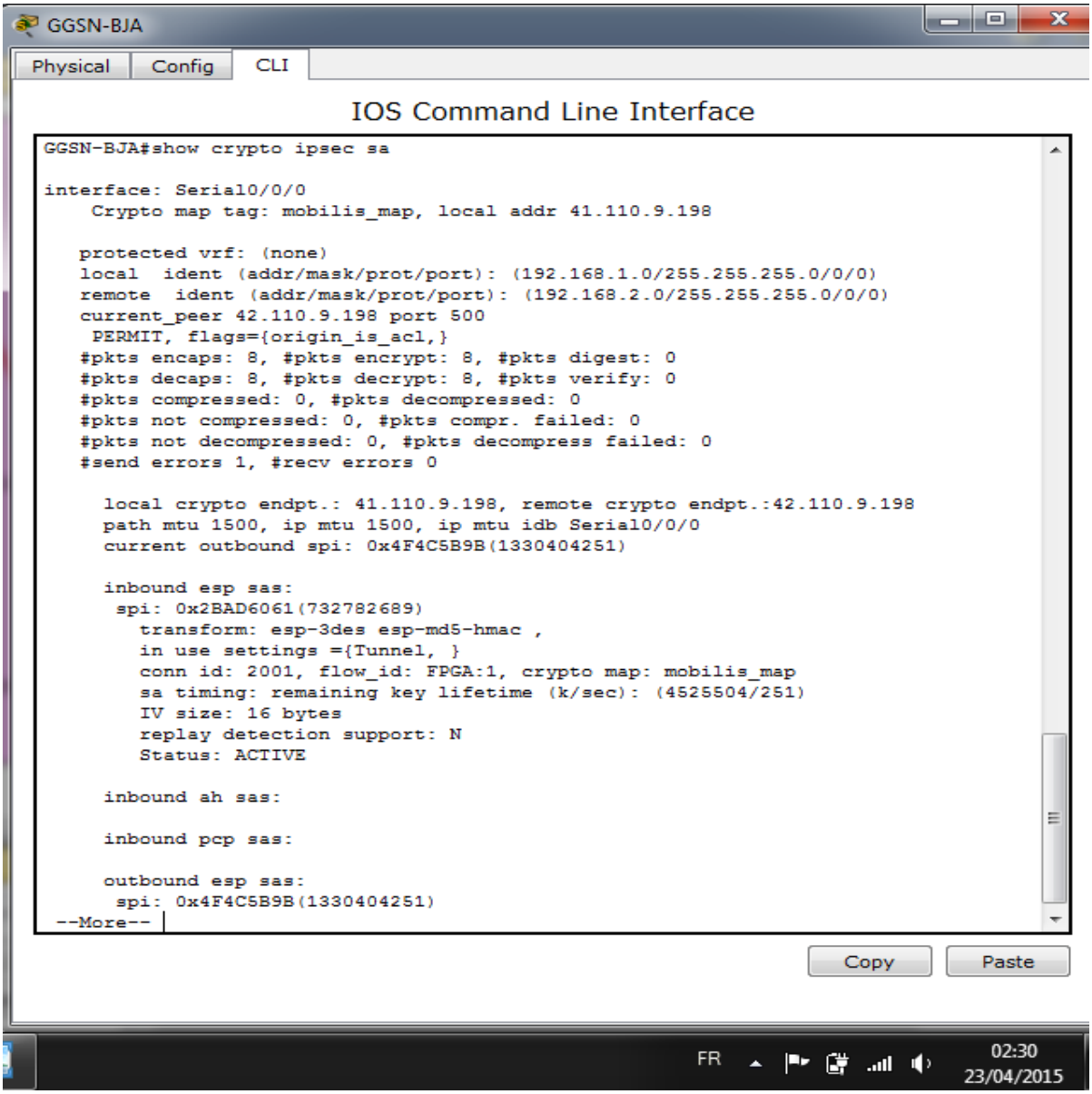

FIGURE 4.19 – L'activation de IPsec et les algoritme de cryptage sur le routeur GGSN-BJA

On remarque aussi que les opérations de IPSec sont bien activées, les algorithmes de cryptage fonctiones et le mode TUNNEL est activé sur le routeur GGSN-ALG (cf. Figure 4.20).

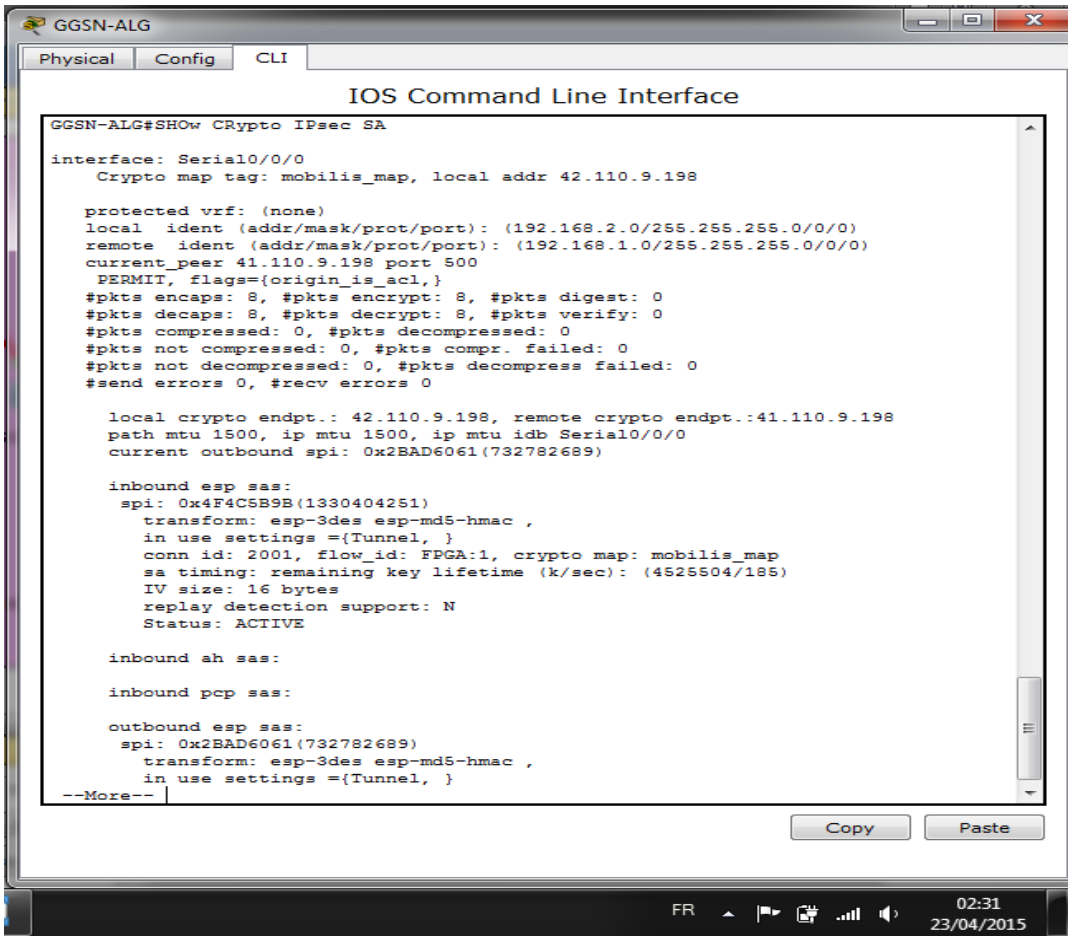

FIGURE 4.20 – L'activation de IPsec et les algoritme de cryptage sur le routeur GGSN-ALG

4.5.1.5 Verification des opérations d'ISAKMP :

On constate aussi que les opérations ISAKMP sont activées, entre l'adresse source et destination.

Comme il est montrée sur l figure 4.21 le tunnel entre le réseau 41.110.9.198 et le réseau 42.110.9.198 est activée.

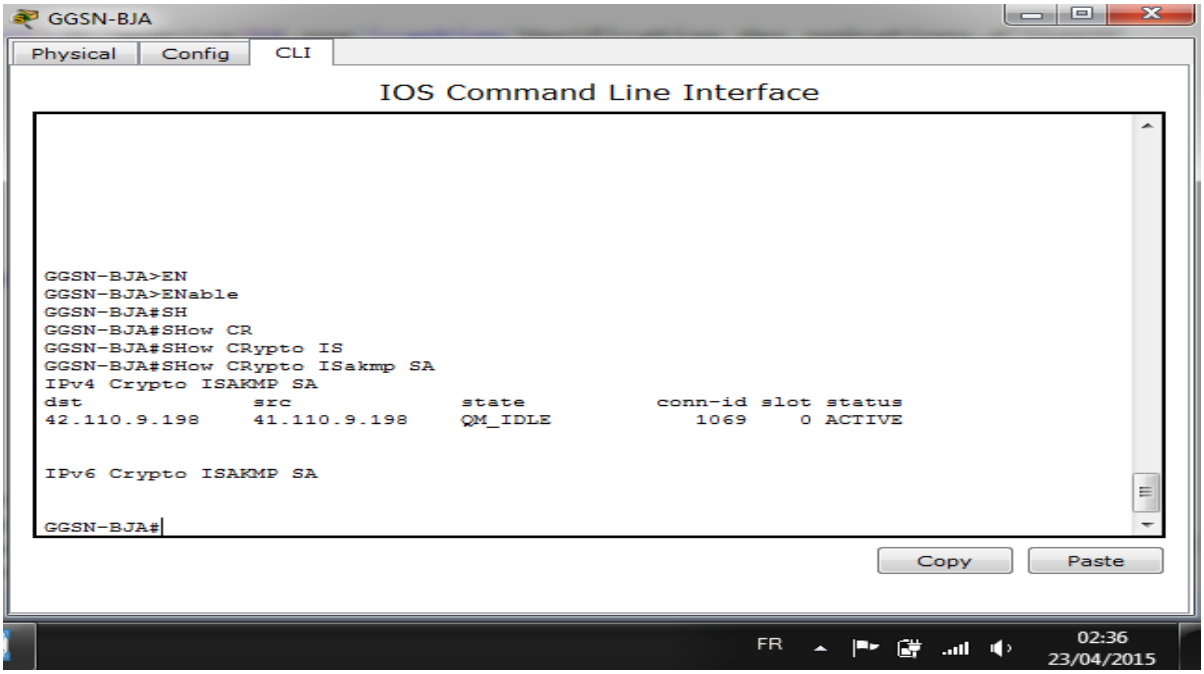

FIGURE 4.21 – Verification des opérations d'ISAKMP sur le routeur GGSN-BJA

La figure 4.22 montre que le tunnel entre le réseau 42.110.9.198 et le réseau 41.110.9.198 est activée.

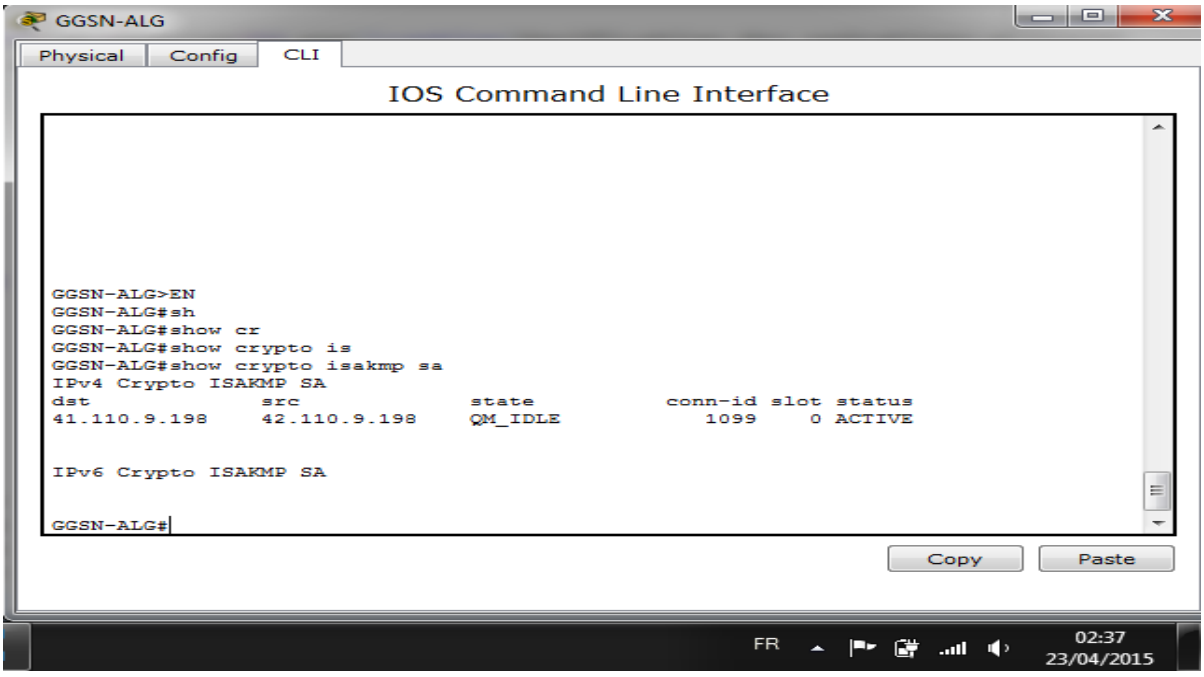

FIGURE 4.22 – Verification des opérations d'ISAKMP sur le routeur GGSN-ALG

Commentaires :

D'aprés nos configurations et notre simulation sur les équipements CISCO , spétialement au niveau des routeurs , où on a configuré le même module IPSEC et ISAKMP. Notre réseau a donné un fonctionnement normal sans signaler aucune erreur lors de la transmission de paquets.

Donc on peut dire que notre configuration d'un tunnel VPN sous le protocole IPSEC a été bien realisée.

4.6 Conclusion :

Dans ce chapitre, nous avons exposé notre thématique, et essayé de porter une solution en définissant les exigences de sécurité à prendre en compte et les différents protocoles de sécurité à appliquer pour réaliser un réseau sécurisé.

L'IOS dans le simulateur a offert diverses commandes permettant de répondre à ces besoins ; principalement les ACL (Access Control List) qui nous ont permis de filtrer des paquets suivant des critères définis ainsi les différentes commandes qui ont permis d'implémenter notre stratégie de sécurité qui est basé sur la creation d'un réseau privé virtuel sous le protocole IPSecurity .

CONCLUSION GÉNÉRALE

Dans ce projet de fin d'étude, nous nous sommes motivées par le fait d'avoir l'opportunité d'étudier la sécurité des réseaux mobiles, où on s'est focalisé sur l'objectif de la création d'un réseau VPN sous le protocole IPSec pour se protéger contre les menaces au niveau des réseaux TCP/IP. Notre motivation centrale est la sécurité des données dans le réseau UMTS.

A fin de développer notre idée, on a fait une projection sur la sécurité des réseaux informatiques qui interfacent les attaques et les risques qui peuvent atteindre notre réseau cellulaire lorsqu'il est connecté au réseau public IP.

La méthodologie adaptée dans ce travail, consiste à montrer la migration progressive des protocoles de la seconde génération à la troisième génération de la sécurité des échanges.

L'authentification mutuelle d'un terminal et du réseau opérateur basé sur l'utilisation des algorithmes de chiffrement, d'authentification et génération des clés de sécurité les plus robustes, font partie des améliorations rentables. Toutes fois, la couverture des protocoles de cette génération au niveau du territoire demeure inférieure lors qu'il s'agit d'une connexion au réseau Internet.

L'inconvénient présenté dans ce mémoire est que les données transmises dans le réseau UMTS suivent une architecture bien définit en passant par le réseau public IP, pour arriver à son destinataire. A ce niveau la, elles sont soumises à des risques d'attaques et d'intrusions.

Dans le but de remédier à ces intrusions, nous avons implémenté notre solution de sécurité, après avoir exploité toute l'architecture du réseau UMTS pour la transmission des données. Cette solution qui consiste à implémenter et à créer un tunnel VPN en utilisant le protocole IPSecurity, qui garantie la communication entre les sites distants via le réseau IP sécurisé.

Grâce à l'ensemble d'outils de conception et de mesure de PACKET TRACER, nous avons pu développer notre suggestion et la valider par une simulation. Celui-ci nous a permis d'avoir une collection de données prouvant que notre réseau est sécurisé en lui appliquant le protocole IPSec intégré dans le VPN. Il nous a montré qui est un système

très complet et qui peut répondre à beaucoup de besoins en matière de sécurité et de s'adapter à de nombreuses situations.

Au terme de ce travail, nous estimons que nos efforts ont été récompensés par des résultats assez intéressants, qui nous ont permis de nous imprégner de connaissances techniques nouvelles sur la technologie de transmission de données dans le réseau mobile UMTS.

Ce travail ouvre de nombreuses perspectives aussi bien au niveau des propositions des systèmes de sécurisation de l'UMTS et au niveau d'amélioration de sécurité au certains composants.

La première perspective consiste à sécuriser la transmission au niveau de l'IMSI. L'envoie de l'identité permanente IMSI en claire lors de la première connexion RRC (lorsque le mobile est allumé) ou lors d'une panne du VLR. Ceci permet à un attaquant de connaître l'identité de l'abonné et donc d'ouvrir la voie à différentes attaques.

La seconde perspective consiste a créer un réseau privé virtuel entre l'équipement usager et le cœur du réseau, qui permet de définir le tunnel de transmission des données.

La dernière perspective concerne la sécurisation de la voix qui consiste à crées le réseau privé virtuel au niveau du domaine commutation de circuit.

BIBLIOGRAPHIE

[1] PUJOLLE Guy , *Les Réseaux* , Eyrolles, 2014.

[2] KECHKOUCHE.M, *Etude des services et applications offerts par UMTS*, mémoire d'ingéniorat, ITO d'Oran, 2013/2014.

[3] JOACHIN Tisal, *Le Réseau GSM*, DUNOD, 2003.

[4] LESCUYER Pierre, *Réseaux 3G : principe, architecture et services de l'UMTS*, DUNOD, 2006.

[5] PEREZ André, *Architecture des réseaux mobiles GSM/GPRS/UMTS /HSPA /ESP /NGN /IMS*, Lavoisier, Edition 2011

[6] PEREZ Andre , *Architecture des réseaux de télécommunication*, Lavoisier, 2002.

[7] LAGRANGE Xavier, TABBANE Sami et JOLIVET Paul, *Principe et évolutions de l'UMTS*, Chapitre 2, Lavoisier, Edition 2005

[8] ABDOUL.R et MAHAMA.S, *Optimisation des réseaux GSM pour la migration vers l'UMTS*, Mémoire d'ingéniorat, ITO d'Oran, juin 2005.

[9] JAVIER Sanchez et MAMADOU Thioune, *UMTS*, Lavoisier, Edition 2004.

[10] BENCHAMA. A et BENSAID .K, *L'utilisation de lUMTS Pour l'accès à l'internet*, Mémoire d'ingénieur d'état, ITO ,2005/2006.

[11] ERICSON *WCDMA System Overview*,LZU1085418, Ericsson AB 2014

[12] CHIKER. S CHIKH .Y *Gestion de la Mobilité et des Appel dans un Réseau Terrestre et Satellitaire de l'UMTS* , Mémoire d'ingénieur d'état, ITO, 2005-2006 .

[13] BCHINI. T, *Gestion de la Mobilité, de la Qualité de Service et Interconnexion de Réseaux Mobiles de Nouvelle Génération* , Thèse de doctorat de l'université de TOULOUSE, 10/06/2010.

[14] ALPHA.D, *Installation et configuration d'un site FTP sécurisé, cas INSIM Bejaia*, Thése d'ingénieur d'état, INSIM BEJAIA, 2012/2013.

[15] http ://www.cse.wustl.edu/ jain/cse574-06/ftp/cellular$_s$ecurity.pdf

[16] BARTHELEMY Pierre & ROBERT Rolland, *Cryptographie*, Lavoisier 2005.

[17] HALAL. A. et EL ABED, *ryptographie RSA sur FPGA* , Mémoire d'ingénieur d'état, ENP d'Alger, Juin 2008.

[18] BOUTIOUTA. A, *Sécurité et Gestion de la Mobilité dans le Réseau GSM*,Mémoire d'ingénieur d'état, ITO d'Oran, 2004/2005.

[19] JOLIVET Paul, *Principe et évolutions de l'UMTS* , Chapitre 10, Lavoisier, Edition 2005.

[20] CARAGATA.D, *Protocoles de communications sécurisées par des séquences chaotiques. Applications aux standards de communications IP via DVB-S, et l'UMTS* , Thèse doctorat, HALL, 23 Jan 2015.

[21] MOUHRI.O ABDELLATIF. Y,*Architecture des réseaux VPN*, mémoire d'ingéniorat, ITO d'Oran juin 2006.

[22] ARCHIER Jean-Paul, *Les VPN : fonctionnement, mise en œuvre et maintenance des réseaux privés virtuels*, ENI, 2010.

[23] DORDOIGNE José, *Réseaux informatique Notion fondamentales*, Eyrolles,2009.

[24] NOUREDDINNE .K e et YOUNSI.N. *Etude générale sur la sécurité des systèmes d'information*, Thése d'ingénieur d'état, ITO d'Oran 2011/2012 .

[25] MAUGHAND, SCHERTLER. M et TURNER.J, *Internet security association and key management protocol (ISAKMP)*, rec2408, 1998.

[26] CORVALAN Rafel,CORVALAN Ernesto, LE CORVIC Yoann,*Les VPN Principe, Conception et déploiement des Réseaux Privés Virtuels*,DUNOD, 2003.

[27] GHERNAOUTI Solange, *Sécurité informatique et réseaux cours avec plus de 100 exercices corrigés* , DUNOD, 2013.

[28] BLOCH Laurent, WOLFHUGEL Christophe , *Sécurité informatique Principe et Méthode à l'usage des DSI, RSSI et administrateurs*, Eyrolles ,2009

[29] BAASSOU .C, *Dimensionnement et caractérisation des réseaux mobiles*, Thése de Magister, Université de BATNA, 2011/2012.

[30] BELLILI. Y, *Mise en place d'une politique de sécurité des routeurs Cisco 1900*, Mémoire d'ingénieur d'état, INSIM BEJAIA, 2013.

[31] CHALOUAH. A, *Sécurité des réseaux Administration des réseaux VPN, cas EPB-BEJAIA* , Séminaire Octobre 2014

[32] LUDOVIC Mé , YVES Dewarte et RAFIK Molva, *Sécurité des systèmes d'informations* , Lavoisier, Edition 2006 .

[33] https ://www.netacad.com.

ANNEXE

Routage et adressage IP :

L'adreesage IP :

L'adressage est l'une des fonctions principales des protocoles de couche réseau [23]. Il permet de mettre en œuvre la transmission de données entre des hôtes situés sur un même réseau ou sur des réseaux différents. La version 4 (IPv4) et la version 6 (IPv6) du protocole IP fournissent un adressage hiérarchique pour les paquets qui transportent les données. Elles peuvent être configurer de manière statique ou dynamique.

L'adressage IP se décompose en deux parties : un numéro de réseau logique, et une adresse d'hôte sur le réseau logique.

L'adresse IP version 4 (IPv4) :

Une adresse IP de version 4 est représentée avec 4 octets[23]. Ce dernier est affiché et séparé par un point, exemple : 192.168.1.9. Suivant le premier octet on peut définir le nombre d'octet utilisé pour l'adresse du réseau, et le nombre d'octet pour l'adresse de l'hôte.

On utilise un masque de sous réseau pour distinguer la partie de l'adresse IP correspondant au réseau, de la partie identifiant le nœud.

Pour identifier un hôte de manière unique, trois classes d'adresses (cf. Figure 4.23) sont été définies comme suit :

1. La classe A :

   Le premier octet est compris entre 1 et 126 bits [23]. Les 7 bits sont attribués pour le numéro du réseau et 24 bits pour identifier l'hôte avec un masque du réseau de 255.0.0.0.

2. La classe B :

   Le premier octet varie de 128 à 191 bits [23]. Les 14 bits permettent de coder un nu-

méro de réseau et 16 bits pour le numéro de l'hôte avec un sous réseau de 255.255.0.0.

3. La classe C :

   Elle est identifiée par un premier octet variant de 192 à 223bits [13]. Les 21 bits sont utilisés pour le réseau et 8 bits pour l'hôte avec un masque de réseau de 255.255.255.0.

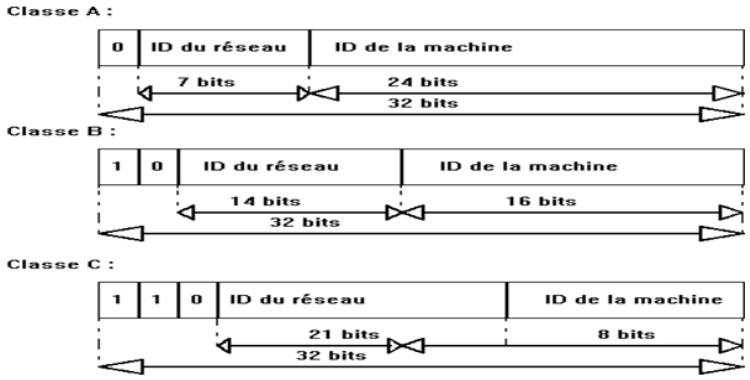

FIGURE 4.23 – Les classes de l'adressage IPv4

La segmentation en sous réseau :

L'élaboration, la mise en œuvre et la gestion d'un modèle d'adressage IP garantissent un fonctionnement optimal des réseaux. Cela devient d'autant plus important lorsque le nombre de connexions d'hôtes à un réseau augmente alors on rencontre une pénurie d'adresse ; c'est pout se fait on a appliqué la stratégie de segmentation du réseau.

La segmentation du réseau consiste à sous-diviser un réseau qui permet d'ajouter un niveau hiérarchique, pour obtenir trois niveaux : un réseau, un sous réseau, et un hôte. Le fait d'ajouter un niveau hiérarchique permet de créer des sous-groupes supplémentaires dans un réseau IP, qui facilitent l'acheminement rapide des paquets et le filtrage efficaces en réduisant le trafic « local ».

L'adresse IP version 6 (IPv6) :

L'IPv6 est conçu pour être le successeur de l'IPv4. L'IPv6 possède un plus grand espace d'adressage 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales [W3]. Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique (cf. Figure 4.24) ; pour un total de 32 valeurs hexadécimales

Routage de paquet :

Les réseaux permettent de communiquer, de collaborer et d'interagir de diverses manières. Ils sont utilisés pour accéder aux pages Web, échanger de communications par le biais des

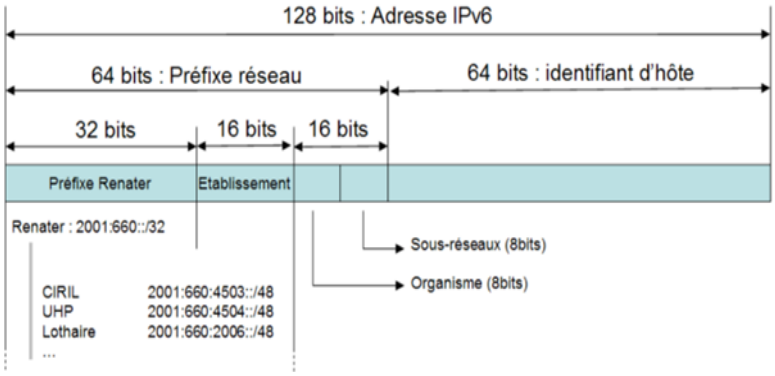

FIGURE 4.24 – L'adressage IPv6

téléphones IP, participer à des conférences vidéo, s'affronter dans le cadre de jeux interactifs, achats sur Internet, suivre des cours en ligne et bien plus encore.

La fonction des commutateurs Ethernet sur la couche liaison de données et la couche 2 permet de transmettre des trames Ethernet entre les périphériques d'un même réseau. Cependant, lorsque les adresses IP source et de destination se trouvent sur des réseaux différents, la trame Ethernet doit être envoyée à un routeur.

Le but d'un routeur est de relier un réseau à un autre. Le routeur est responsable de la transmission de paquets à travers différents réseaux. La destination du paquet IP peut être un serveur se trouvant dans un autre pays ou un serveur de messagerie situé sur sur réseau local.

Le routeur utilise sa table de routage pour déterminer le meilleur chemin à utiliser pour transférer un paquet. Les routeurs doivent transmettre ces paquets rapidement. Ils obtiennent des informations sur les réseaux distants, soit dynamiquement, en utilisant des protocoles de routage, soit manuellement, en utilisant des routes statiques. Dans de nombreux cas, les routeurs utilisent une combinaison de protocoles de routage dynamique et de routes statiques.

Routage statique :

Les routes statiques sont très courantes et ne nécessitent pas le même niveau de traitement et de charge que les protocoles de routage dynamique.

Un administrateur réseau peut configurer manuellement une route statique pour accéder à un réseau spécifique. Les routes statiques ne sont pas mises à jour automatiquement et elles doivent être reconfigurées manuellement à chaque modification de la topologie du réseau. Une route statique ne change que lorsque l'administrateur la reconfigure manuellement.

Les types suivants de routes statiques IPv4 et IPv6 seront abordés :

- Route statique standard.
- Route statique par défaut.
- Route statique récapitulative.
- Route statique flottante.

La figure 4.25 illustre une configuration d'un routage statique :

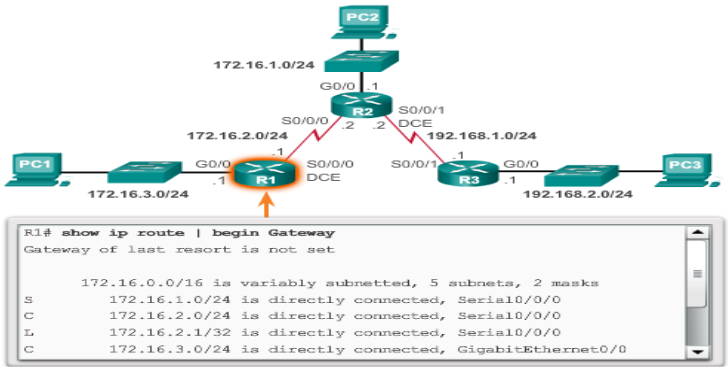

FIGURE 4.25 – Configuration d'un routage statique sur un routeur CISCO

Routage dynamique :

Les routes distantes sont automatiquement acquises via un protocole de routage dynamique. Les protocoles de routage permettent aux routeurs de partager de manière dynamique des informations sur les réseaux distants et d'ajouter automatiquement ces informations à leurs propres tables de routage.

Un protocole de routage est un ensemble de processus, d'algorithmes et de messages qui sont utilisés pour échanger des informations de routage et construire la table de routage en y indiquant les meilleurs chemins choisis par le protocole. La fonction des protocoles de routage dynamique inclut les éléments suivants :

- Découverte des réseaux distants ;
- Actualisation des informations de routage ;
- Choix du meilleur chemin vers les réseaux de destination ;
- Capacité à trouver un nouveau meilleur chemin si le chemin actuel n'est plus disponible.

L'un des principaux avantages des protocoles de routage dynamique est l'échange d'informations de routage entre les routeurs lors de la modification de la topologie.

Les protocoles de routage dynamique sont :

Le protocole RIP : C'est l'un des tout premiers protocoles de routage. Il a deux versions : la version 1 du protocole RIP (RIPv1) puis âpres la mis à jour pour prendre en compte la croissance de l'environnement réseau, devenant ainsi RIPv2.

Le protocole OSPF et IS-IS : sont des protocol de routage advances.

Les protocoles IGRP et Enhanced IGRP :sont des protocoles qui s'adaptent également bien aux réseaux de plus grande taille.

Le protocole BGP : C'est désormais utilisé entre les fournisseurs d'accès Internet (FAI).

La figure 4.26 suivante représente une vérification du routage dynamique :

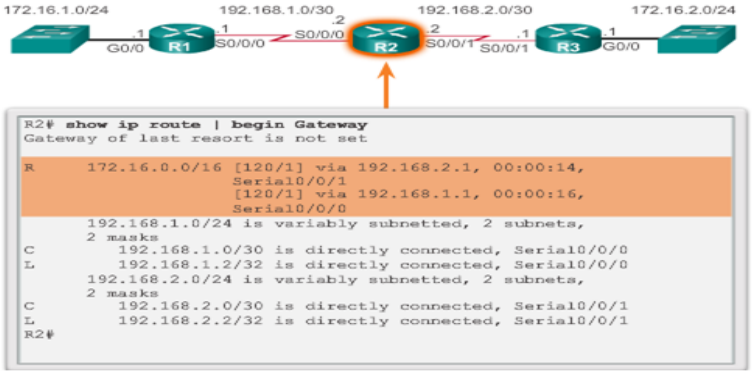

FIGURE 4.26 – Vérification d'un routage dynamique sur un routeur CISCO