MODELO TEÓRICO PARA LA IMPLEMENTACIÓN DE UNA VPN A TRAVÉS DE UNA RED GSM CON GPRS

Dennis Alexandra Marín Marín

Jaime Ignacio Montoya Giraldo

Monografía para optar el título de Especialista en Ciencias Electrónicas e Informática con énfasis en Telemática

UNIVERSIDAD DE ANTIOQUIA

FACULTAD DE INGENIERÍA

Departamento de Electrónica

Medellín, 6 de mayo de 2005

Tabla de contenidos

[3] **MVPN: Móbile VPN**

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

Gustavo Adolfo Orozco Arroyave, Analista Senior de Datos, Gerencia de Planeación de Red de Colombia Móvil S.A. E.S.P., por sus valiosos aportes.

INTRODUCCIÓN

La creciente popularidad de los computadores portátiles, los Asistentes Personales Digitales (PDA - Personal Digital Assistant) y los teléfonos celulares demuestran que las personas están ansiosas por utilizar la tecnología móvil. Las aplicaciones de la computación móvil aumentan cada día, no sólo por las necesidades de un mercado globalizado sino también por las posibilidades que traen consigo los avances tecnológicos. Dentro de las principales aplicaciones se tienen el servicio al cliente, ventas directas, manejo de pacientes, personal móvil en oficinas, manejo de sucursales, grupos de trabajo, etc. accediendo desde sitios antes inimaginables: Aeropuertos, aviones, cafés, hoteles, centros de convenciones, la oficina del cliente, la casa y trenes los cuales se han convertido en una extensión de la oficina. Es así como en la actualidad es fácil encontrar personas intentando conectarse en línea con su portátil cuando se encuentran lejos de la oficina o lugar de trabajo, para lo cual la opción más fiable es buscar una línea telefónica o un punto de conexión a la red en caso de encontrarse en sitios con la infraestructura adecuada.

La masificación del uso de Internet así como el impresionante crecimiento de la telefonía móvil permitía vislumbrar un mercado que combinara ambas innovaciones: la telefonía inalámbrica y los servicios de transmisión de datos. El desempeño actual de los sistemas de transmisión de datos por la red celular han convertido en una realidad la posibilidad de los usuarios móviles para acceder al sistema de información de su empresa, a servicios como correo electrónico, transmisión de imágenes y todas las posibilidades que brinda el estar conectado con Internet, pero ahora desde un dispositivo que nos permite movilidad.

La movilidad es en la actualidad un tema de preocupación de las empresas y en el cual tienen centrada gran parte de su atención. La necesidad de utilizar sistemas de información únicos, de compartir información de forma más ágil, las nuevas modalidades de trabajo con empleados operando desde fuera de la empresa, entre otros, hacen que este tema cobre cada vez más importancia.

Sin embargo, una vez identificadas las posibilidades que tienen las empresas de conectarse a Internet desde dispositivos móviles y desde allí a los sistemas de información corporativos, surge una nueva preocupación y es la seguridad, la cual se debe garantizar no sólo desde el punto de vista de las transacciones sino desde la perspectiva de la información del negocio dada la alta competencia y la globalización del mercado.

Las *Redes Privadas Virtuales* (VPN - Virtual Private Networks) plantean una solución que permite conectar un dispositivo móvil con la Red Local (LAN - Local Área Network) de una empresa creando un camino físico que proporciona mecanismos de autenticación, encriptación y el uso de túneles para las conexiones.

Actualmente las VPN son muy usadas utilizando protocolos que operan sobre medios cableados como Frame Relay, RDSI, ADSL, el sistema telefónico convencional, pares aislados de cobre entre otros, pero pocas son las implementaciones que usan tecnologías inalámbricas.

En el proyecto se realizará un estudio teórico para implementar una VPN móvil que permita conectar un dispositivo móvil que utilice GSM / GPRS como medio físico de acceso con una Red de Área Local (LAN).

En la primera parte del documento se hará una revisión de la arquitectura de GSM y su integración con GPRS, luego se introducirá el tema de las VPNs y finalmente se describirá la arquitectura de una VPN utilizando la infraestructura de GPRS.

2. REDES GSM (Global System for Mobile Communication)

2.1 Evolución de los sistemas de telefonía móvil

La telefonía celular es una de las aplicaciones de las telecomunicaciones de más rápido crecimiento. Esta representa un incremento continuo en el porcentaje de nuevos suscriptores alrededor del mundo. En la actualidad la telefonía móvil cuenta con más de 1.6 mil millones de suscriptores en todo el mundo. Se ha pronosticado que los sistemas celulares digitales se convertirán en el mecanismo universal de telecomunicaciones. Los pronósticos indican que para finales de 2006 la telefonía móvil contará con más de 1.8 mil millones de suscriptores y para finales de 2007 esta cifra habrá superado los 2000 millones (Ver Figura 1).

Países	2002	2003	2004	2005	2006	Cto. 02/06 (%)
Alemania	59.244	63.663	66.510	69.779	72.532	5,2
Dinamarca	4.208	4.513	4.732	4.922	5.143	5,1
España	**33.076**	**35.746**	**36.149**	**36.539**	**37.074**	**2,9**
Finlandia	4.562	4.654	4.811	5.013	5.263	3,6
Francia	36.850	39.596	43.523	47.458	51.282	8,6
Italia	51.999	54.057	55.179	55.833	56.610	2,1
Noruega	3.560	3.710	3.893	4.109	4.358	5,2
Reino Unido	49.473	50.954	52.590	54.382	56.513	3,4
Suecia	7.937	8.444	8.497	8.551	8.644	2,2
Suiza	5.706	5.967	6.279	6.617	6.970	5,1
Otros países(*)	72.358	79.260	84.843	89.509	94.095	6,8
Europa Occ.	328.973	350.563	367.006	382.710	398.485	4,9
Europa Este	75.541	97.330	111.275	119.328	124.958	13,4
Total Europa	**404.514**	**447.894**	**478.281**	**502.039**	**523.443**	**6,7**
EE.UU.	141.211	157.549	180.664	207.033	233.900	13,4
Japón	73.541	80.444	88.230	96.018	103.626	9,0
Resto Mundo	529.001	655.784	770.277	871.013	950.332	15,8
Total Mundo	**1.148.267**	**1.341.671**	**1.517.452**	**1.676.103**	**1.811.301**	**12,1**

Fuente: EITO 2004; (*) Otros países: Países europeos como Turquía, Resto [illegible]

Figura 1. Evolución en el número de usuarios de Telefonía móvil

El concepto de servicio celular se refiere al uso de transmisores de baja potencia en el cual las frecuencias pueden ser reutilizadas dentro de un área geográfica. La idea de un sistema de radio basado en celdas fue formulada en estados Unidos en los laboratorios Bell al comienzo de la década de 1970. Sin embargo, los países nórdicos fueron los primeros en introducir servicios celulares para uso comercial con el NMT (Nordic Mobile Telephone) en 1981.

En los Estados Unidos, los sistemas celulares comenzaron con el lanzamiento del sistema AMPS (Advanced Mobile Phone Service) en 1983. El estándar AMPS fue adoptado por Asia, América latina, y los países Oceánicos, creando un gran mercado potencial para los celulares en el mundo.

Al comienzo de la década de 1980, la mayoría de los sistemas de telefonía móvil eran analógicos y no digitales, como los nuevos sistemas actuales. Una dificultad con los sistemas analógicos fue su incapacidad de manejar las necesidades de crecimiento de abonados de forma que permitiera conservar un equilibrio en los costos. Como resultado de esta incapacidad de la tecnología análoga, se le dio la bienvenida a la tecnología digital. La ventaja de los sistemas digitales sobre los sistemas analógicos incluye la facilidad de hacer señalización, niveles de interferencia más bajos, integración de la transmisión y la conmutación, y un incremento de la capacidad para ajustarse a cambios en la demanda.

2.2 Arquitectura de red GSM

A lo largo de la evolución de las telecomunicaciones celulares, se han desarrollado varios sistemas, lo cual no ha favorecido la estandarización. Esto ha presentado muchos problemas, principalmente relacionados con la compatibilidad entre los sistemas, especialmente con la tecnología de radio digital. El estándar GMS está orientado a resolver este problema.

El Sistema Global para la comunicación Móvil (GSM) es un estándar globalmente aceptado para la comunicación digital celular. GSM es el nombre de un grupo de estandarización conformado en 1982 con el fin de crear un estándar de telefonía móvil dirigido a Europa que formulara especificaciones para los sistemas móviles de radio celular operando en la banda de los 900 MHz.

Entre 1982 y 1985 se mantuvieron discusiones para decidir entre un la construcción de un sistema análogo o un sistema digital. Después de muchas pruebas de campo se decidió por adoptar un sistema digital para GSM. La siguiente tarea fue decidir entre una solución de banda angosta o de banda ancha. En mayo de 1987 se eligió TDMA de banda angosta.

Tabla 1. Evolución de la telefonía móvil

Año	Sistema Móvil
1981	Nordic Mobile Telephone (NMT) 450
1983	American Mobile Phone System (AMPS)
1985	Total Access Communication System (TACS)
1986	Nordic Mobile Telephone (NMT) 900
1991	American Digital Cellular (ADC)
1991	Global System for Mobile Communication (GSM)
1992	Digital Cellular System (DCS) 1800
1994	Personal Digital Cellurar (PDC)
1995	PCS 1900 – Canada
1996	PCS – United States

La red GSM

GSM proporciona recomendaciones y no requerimientos. Las especificaciones de GSM definen en detalle los requerimientos de las interfaces y de funcionalidad pero no trata el tema del hardware. La razón es limitar lo menos posible a los diseñadores y hacer posible a los operadores comprar equipos a diferentes proveedores. La red GSM está dividida en tres grandes sistemas: el *Sistema de Conmutación* (SS – Switching System), el *Sistema de Estación Base* (BSS – Base Station System), y el *Sistema de Operación y Soporte* (OSS – Operation and Support System). En la figura 2 se muestran los elementos de la red GSM.

2.2.1 Sistema de conmutación (SS)

El SS es el encargado de llevar a cabo el proceso de llamadas y de las funciones relacionadas con el suscriptor. Este sistema incluye las siguientes unidades funcionales:

- **Home Location Register (HLR):** El **HLR** es una base de datos usada para el almacenamiento y administración de las suscripciones. La **HLR** es considerada la base de datos más importante, ya que almacena permanentemente los datos de los suscriptores, incluyendo el perfil de servicio del suscriptor, información de la ubicación y el estado de actividad. Cuando un individuo se suscribe con un operador, este es registrado en la base de datos **HLR** del operador.
- **Mobile Services Switching Center (MSC)**: El **MSC** lleva a cabo las funciones de conmutación telefónica del sistema. Este controla las llamadas hacia y desde otro teléfono o sistema de datos. También se encarga de la facturación, las interfaces de red, funciones comunes de señalización, entre otras.
- **Visitor Location Register (VLR):** El **VLR** es una base de datos que contiene la información temporal de los suscriptores que son requeridos por el MSC para poder prestarle el servicio a los suscriptores visitantes. La **VLR** siempre está integrada con el MSC. Cuando un dispositivo móvil (teléfono o PC) se encuentra en un área cubierta por un MSC diferente al que pertenece, la VLR conectada a ese MSC solicita los datos del dispositivo a la HLR. Posteriormente, si el dispositivo móvil hace una llamada, la VLR tendrá la información necesaria para configurar la llamada sin tener que preguntarle cada vez a la HLR.
- **Authentication Center (AUC**): La unidad llamada AUC proporciona parámetros de autenticación y encriptación que permite verificar la identidad del usuario y asegura la confidencialidad para cada llamada. El AUC protege a los operadores de la red frente a diferentes tipos de fraude que se presentan en el mundo de la telefonía celular.
- **Equipment Identity Register (EIR):** El **EIR** es una base de datos que contiene información de la identidad del equipo móvil previniendo el robo de llamadas, llamadas no autorizadas, o estaciones móviles defectuosas. El AUC y el EIR son implementados como nodos independientes o como nodos combinados AUC / EIR.

2.2.2 Sistema de estación base (BSS)

El BSS se encarga de realizar todas las funciones relacionadas con el sistema de radio, el BSS se compone de Estaciones Controladoras Base (BSCs – Base Station Controllers) y de Estaciones Transmisoras / Receptoras Base (BTSs – Base Transceiver Stations)

- **Base Station Controllers (BSC):** Los **BSCs** proporcionan todas las funciones de control y los enlaces físicos entre el MSC y el BTS. Este es un suiche de alta capacidad que permite funciones de manejo, configuración de datos de la celda, y control de los niveles de potencia de radio frecuencia (RF) en las BTSs. Un MSC puede servir a un número determinado de **BSCs**.
- **Base Transceiver Stations (BTS):** Los **BTSs** manejan la interfaz de radio hacia el dispositivo móvil. Un BTS se compone del equipo de radio (transmisores, receptores y antenas) necesario para prestar el servicio en cada una de las celdas de la red. Un grupo de **BTSs** es controlado por un BSC.

2.2.3 Sistema de operación y soporte (OSS)

El *Centro de Operación y Mantenimiento* (OMC – Operation and Maintenance Center) está conectado a todos los equipos en el SS y al BSC. La implementación de un OMC se denomina el *Sistema de Operación y Soporte* (OSS). El **OSS** es la unidad funcional que le permite al operador de la red monitorear y controlar el sistema. Una función importante del **OSS** es proporcionar una perspectiva general de la red y soporte a las actividades de mantenimiento requeridas.

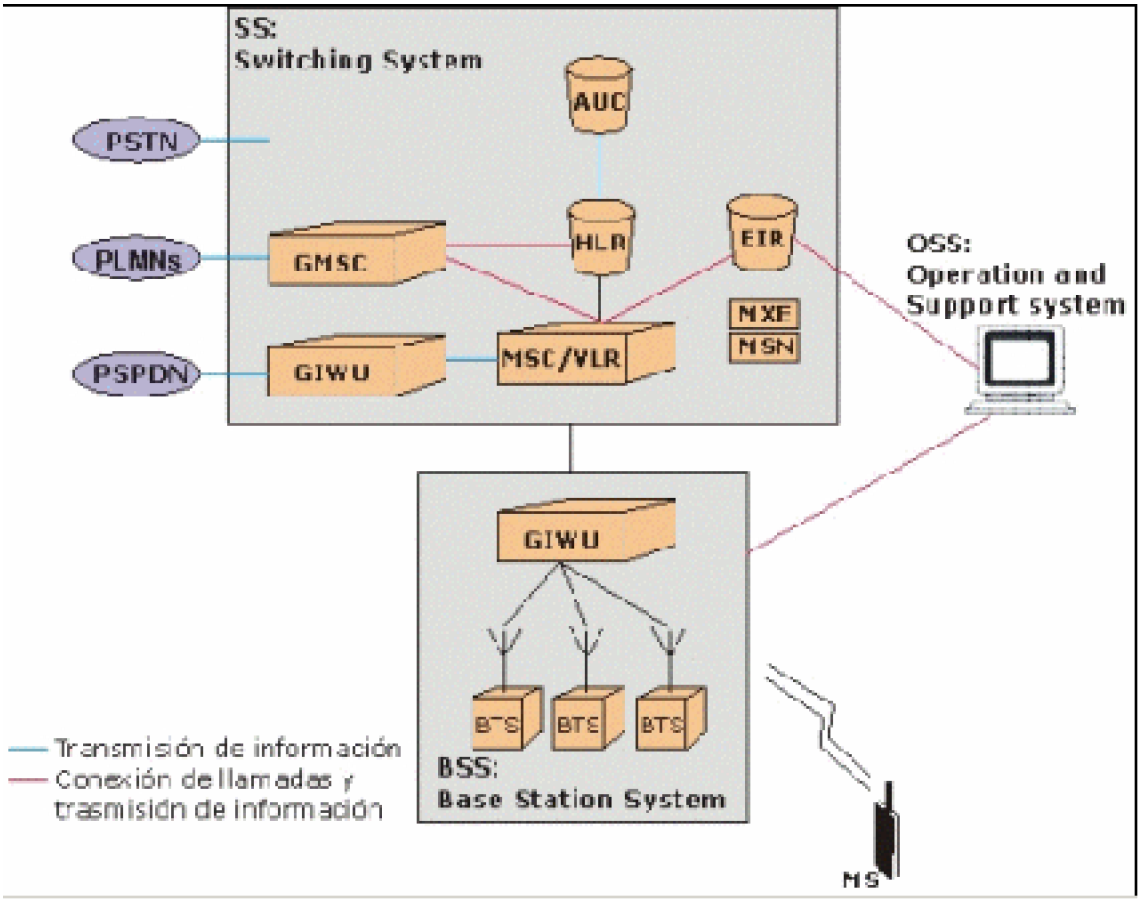

Figura 2. Sistemas de la Red GSM

2.2.4 Elementos funcionales adicionales

Otros elementos que también se muestran en la Figura 2 son los siguientes.

- **Message Center (MXE)** El Centro de Mensajes (MXE – Message Center) es un nodo que proporciona integración a los servicios de voz, fax e intercambio de mensajes. Específicamente, el MXE maneja el servicio de mensajes cortos de texto, broadcast a toda la celda, correo de voz, fax, correo electrónico y notificaciones.
- **Mobile Service Node (MSN)** El Nodo de Servicio Móvil (MSN – Mobile Service

Node) es un nodo que maneja los servicios de la red móvil inteligente. Algunos de estos servicios son:

- Convertidor genérico de números: Con este servicio un suscriptor podrá marcar un número genérico como *27 y este será convertido en un número de 10 dígitos correspondiente para facilitar la marcación.
- Identificador de llamada: Es un servicio que permite identificar el nombre del suscriptor que llama. Este nombre puede ser tomado de una base de datos disponible en el servicio de telefonía convencional con el fin de unificar la identificación en el dispositivo fijo y en el dispositivo móvil.
- Detección de la ubicación: Con este servicio, el suscriptor podrá usar sólo el número de su dispositivo móvil, con el que podrá ser localizado en la oficina, en la casa, etc. De acuerdo con su ubicación geográfica. Además con este servicio, el sistema detectará la ubicación del dispositivo móvil y si éste se encuentra en un lugar sensible al uso de dicho dispositivo como un teatro o un hospital, la llamada será transferida al buzón de mensajes.
- Identificador virtual de llamadas: Con este servicio el suscriptor podrá recuperar un listado completo de las llamadas recibidas mientras su dispositivo móvil se encontraba apagado, la fecha, hora, la identificación de quien llamó y el número de llamadas que realizó.

· **GSM Interworking Unit (GIWU)** La Unidad de Interoperabilidad de GSM (GIWU – GSM Interworking Unit) consiste en elementos de hardware y software que proporcionan una interfaz entre varias redes para la comunicación de datos. A través de GIWU los usuarios pueden alternar entre voz y datos durante la misma llamada, esto funciona a través de un esquema de conmutación de circuitos y no de paquetes. El hardware del GIWU está físicamente ubicado en el MSC / VLR. Sin embargo es necesario aclarar que este modo de operación no es soportado actualmente por todos los dispositivos puesto que ha entrado en obsolescencia.

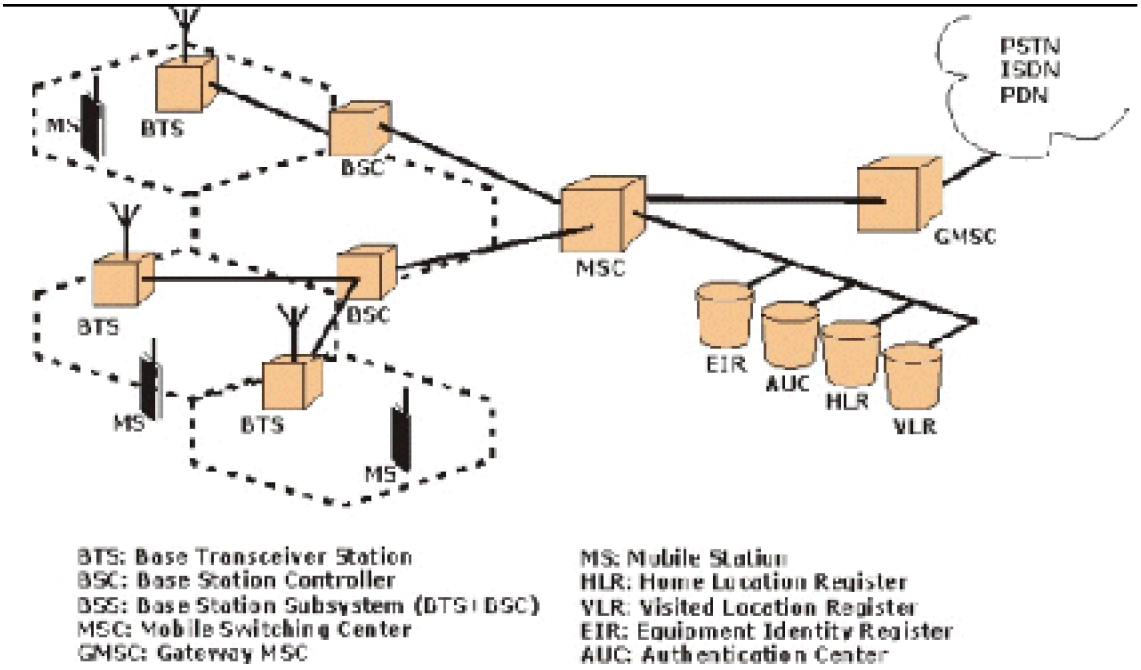

Figura 3. Arquitectura de la Red GSM

3. GPRS - GENERAL PACKET RADIO SYSTEM

El Sistema General de Paquetes sobre Radio (GPRS - General Packet Radio System) es un servicio de valor agregado de datos que permite enviar y recibir información a través de una red de telefonía móvil.

3.1 Conmutación de paquetes

GPRS introduce una interfaz al aire basada en paquetes en una red GSM basada en conmutación de circuitos. GPRS permite al usuario utilizar un servicio de datos basado en paquetes. Para complementar la arquitectura de una red basada en conmutación de circuitos haciendo que ésta permita hacer conmutación de paquetes haría necesaria una actualización mayor de la red. Sin embargo, como se verá más adelante, el estándar GPRS lo hace de una forma muy elegante, haciendo que el operador de la red sólo tenga que adicionar una pareja de nodos en la infraestructura de la red y actualizar el software de algunos de los elementos existentes.

Con GPRS, la información se divide en paquetes diferentes pero relacionados antes de ser transmitidos y posteriormente son reensamblados en el lugar de destino. El ejemplo más común de una red de paquetes es Internet, en el cual la información es

dividida en paquetes, transportados independientemente a un destino y posteriormente reensamblada.

3.2 Arquitectura y funciones de la red GPRS

Para integrar GPRS con la arquitectura de una red GSM existente, se introduce una nueva clase de nodos llamados Nodos de Soporte de GPRS (GSN – GPRS Support Nodes). Los GSNs son responsables de repartir y enrutar los paquetes entre las estaciones móviles y las Redes de Datos basadas en transmisión de Paquetes (PDN – Packet Data Networks) externas.

Los GSNs son dos y se enumeran a continuación:

- El SGSN (Serving GPRS Support Node)
- El GGSN (Gateway GPRS Support Node)

Las responsabilidades de este par de nodos son complementarias. En líneas generales el SGSN se encargará de gestionar la movilidad y de mantener el enlace lógico entre la MS y la red, por su parte el GGSN es el que proporciona el acceso a las redes externas como Internet.

Además se deben introducir los siguientes elementos:

- Actualización de software a nivel del BTS.
- Nuevo hardware en el BSC. Este hardware se denomina Unidad de Control de Paquetes (PCU - Packet Control Unit) y es la encargada de manejar la comunicación de paquetes.
- La red troncal GPRS o backbone, la cual es basada en IP y cuenta con un grupo de servidores que ofrecen, entre otros, los siguientes servicios a la red:
  - DNS (Domain Name Service): Servidor de nombres de dominio, mediante el cual se traduce un nombre de dominio a una dirección IP.
  - DHCP (Dynamic Host Configuration Protocol): Protocolo de configuración dinámica de hosts, con el cual se hace la asignación dinámica de direcciones IP.
  - SNMP (Simple Network Management Protocol): Es un protocolo usado para realizar tareas de administración es una red.
  - NTP (Network Time Protocol): Protocolo que permite mantener actualizada la hora en los diferentes equipos de la red, lo cual es de vital importancia para el manejo de la facturación y el manejo de políticas de administración.
  - AAA (Authentication, Authorization, and Accounting): Es un servidor que autentica y autoriza usuarios y almacena los perfiles de usuario. El AAA puede almacenar las direcciones IP de las MS y recolectar información de facturación desde otros componentes de la red.

3.2.1 Serving GPRS Support Node (SGSN)

El SGSN se encarga de la entrega de paquetes desde y hacia las estaciones móviles que se encuentren dentro de su área de servicio. Dentro de sus tareas también se encuentra el enrutamiento de paquetes, gestión de la movilidad, cifrado de información, autenticación de los usuarios y las funciones de carga. Cualquier SGSN de la red puede prestar servicio a un usuario GPRS.

El flujo de información se dirige desde el SGSN al BSC y desde allí al dispositivo móvil a través de una BTS.

El SGSN puede ser visto como un MSC que reparte paquetes a las estaciones móviles que se encuentren dentro de su área de servicio. El SGSN envía solicitudes al HLR para obtener los datos correspondientes al perfil de los suscriptores GPRS (como el Identificador Internacional del Suscriptor Móvil (IMSI - Internacional Mobile Subscriber Identity)), también utiliza el HLR para mantener información de la ubicación del usuario (como la celda y el VLR actual).

El SGSN también detecta nuevas estaciones móviles GPRS en su un área de servicio, se encarga de procesar el registro de nuevos suscriptores, controla la autenticación, autorización y la admisión de estaciones móviles, envía y recibe paquetes desde y hacia las estaciones móviles

El SGSN está conectado al BSS por medio de un enlace Frame Relay con el PCU en el BSC.

El SGSN y la gestión de la movilidad

- La gestión de la movilidad está basada en los mismos principios que en MSC/VLR. El SGSN tiene asociado un registro de ubicación que hace lo mismo que el VLR, pero en sí mismo éste no es un elemento lógico de la red.
- El SGSN lleva a cabo las funciones de conexión / desconexión de un dispositivo móvil.
- Se encarga de la interacción con el MSC / VLR y el HLR.
- Para la interacción con una PDN como IP, el SGSN asigna las direcciones IP, sigue los movimientos del usuario al cambiar de BSS, garantiza la seguridad de la conexión y el enrutamiento de paquetes.

Enrutamiento

- Enruta los datos hacia el GGSN cuando se requiere una conexión a la red externa.
- Todos los paquetes enviados entre 2 MS’s de la misma red, viajan a través de GGSN.
- El SGSN se encarga de la conmutación del tráfico hacia el BSS y los elementos de la red que establecen la interconexión con PDNs externas. Por lo tanto un SGSN también lleva a cabo las labores de un enrutador ordinario de paquetes desde la red

hacia el dispositivo móvil, sin embargo se aclara que este dispositivo no hace enrutamiento hacia redes externas como Internet.

- El Servidor de Nombres de Dominio (DNS – Domain Name Service) está lógicamente asociado con el SGSN.
- Los recursos de radio son asignados por la BTS quien es la que maneja la interfaz directa con el dispositivo móvil.
- El proceso de control de la admisión incluye la determinación de la Calidad del Servicio.

Administración de enlaces lógicos

- La administración de los enlaces lógicos se realiza entre el SGSN y el dispositivo móvil, independiente del sistema de acceso de radio. Un enlace lógico entre el SGSN y el dispositivo móvil se puede mantener aún cuando no existan recursos físicos en uso. La administración de los enlaces lógicos incluye establecimiento, mantenimiento y liberación.
- Conversión de protocolos entre el backbone IP y los protocolos que usan el BSS y la MS.

Facturación

- Recolección de estadísticas de tráficos y de datos para el cobro.

Seguridad

- La funcionalidad de la seguridad de GPRS es equivalente a la seguridad existente en GSM. El SGSN lleva a cabo los algoritmos de autenticación y de cifrado de información configurando procedimientos basados en los mismos algoritmos, claves, y criterios existentes en GSM. Sin embargo GPRS utiliza un algoritmo de cifrado de información optimizado para la transmisión de paquetes de datos.

3.2.2 Gateway GPRS Support Node (GGSN)

El Nodo de servicio de Gateway GGSN se comporta como una interfaz entre el backbone de la red GPRS y las PDNs externas. El GGSN se encarga de convertir los paquetes GPRS que llegan del SGSN en el protocolo de manejo de paquetes (PDP – Packet Data Protocol) apropiado (por ejemplo IP o X25) y los envía a la PDN correspondiente. En el otro sentido, las direcciones PDP de los paquetes que llegan se convierten en las direcciones GSM del usuario destino. Los paquetes redireccionados se envían al SGSN responsable. Para poder realizar el redireccionamiento, el GGSN almacena en su HLR la dirección del SGSN actual del usuario y la información de su perfil. El GGSN también lleva a cabo recolección de información para la facturación, funciones de carga y de autenticación.

Como su nombre lo indica, GGSN actúa como un gateway entre la red GPRS y la

una Red Pública de Datos como IP y X.25. GGSN también se conecta con otras redes GPRS para permitir roaming. El SGSN permite el enrutamiento de paquetes desde y hacia el área de servicio del SGSN para todos los usuarios en esa área de servicio.

En general existe una relación de muchos a muchos entre los SGSNs y los GGSNs. Un GGSN es la interfaz con una red de paquetes externa para muchos SGSNs. Un SGSN puede enrutar sus paquetes por diferentes GGSNs para llegar a diversas PDNs.

3.2.3 Packet Control Unit (PCU)

La PCU es responsable de la asignación de capacidad por demanda. Ésta decide qué recursos de radio se deben asignar dinámicamente para ser usados en conmutación de paquetes y en conmutación de circuitos. El BSC se encarga de gestionar los recursos de radio asignados para el uso en la conmutación de circuitos, mientras que el PCU gestiona los recursos de radio para el tráfico de GPRS. Este incluye además, el control de acceso al canal, la segmentación y reensamble de paquetes, entre otros. El PCU puede ser ubicado después del SGSN como una unidad independiente, o puede ir después o dentro del armario del BSC o en el sitio del BTS.

3.2.4 Channel Codec Unit (CCU)

La CCU se encarga de implementar los nuevos esquemas de codificación, control de potencia y procedimientos avanzados de control de tiempo. Al principio la mayoría de los operadores sólo usaban esquemas de codificación CS-1 y CS-2, porque podían ser implementados con una actualización del software del BTS. Los esquemas de codificación CS-3 y CS-4, sin embargo, requieren modificaciones del BTS y además no se consiguen en el mercado, ya que los fabricantes decidieron construir hasta CS-2 y de ahí pasar a soportar EDGE.

Tabla 2. Radio de transferencia para cada codificación

Codificación del Canal	Ratio por TimeBlock	Máxima transferencia con los 8 time-slots
CS-1	9.05 kb/s	72.4 kb/s
CS-2	13.4 kb/s	107.2 kb/s
CS-3	15.6 kb/s	124.8 kb/s
CS-4	21.4 kb/s	717.2 kb/s

3.2.5 Otros elementos que conforman la red GPRS

- DNS (Domain Name Server): Convierte los nombres a direcciones IP’s.
- APN (Access Point Name): Es un elemento de la red, definido por los estándares de GPRS, el cual es usado por la red para identificar una PDN que es accesible desde

un GGSN de la red GPRS

- Border Gateway: gateway que provee un túnel directo entre redes GPRS, a través de Redes Públicas Móviles (PLMN - Public Land Mobile Network).
- Charging Gateway (CG): los datos generados por los GGSN y SGSN pasan al CG la procesa y envía al CCB.
- Customer Care and Billing (CCB): Es el encargado del cobro por la información transmitida. Se basa en los datos que le pasa el CG.

3.2.6 Definición del contexto PDP

PDP (Packet Data Protocol): Es utilizado para comunicar paquetes de datos sobre una red de paquetes de datos, por ejemplo TCP/IP sobre Internet.

Contexto PDP: El dispositivo móvil y la red deben negociar un grupo de parámetros que soportan el flujo del tráfico de datos a y desde el dispositivo móvil. Entre los parámetros que deben ser configurados son: el identificador de la red de paquetes de datos externa con la que se comunica el dispositivo móvil, una dirección PDP reconocida en la red (por ejemplo una dirección IP), la dirección del GGSN, Calidad del servicio (QoS - Quality of Service), etc. El grupo de estos parámetros juntos es llamado Contexto PDP. Cada uno de los parámetros puede cambiar durante la vida del contexto de acuerdo a como el dispositivo móvil se mueva a través de la red. Un dispositivo móvil puede tener varios contextos activos al tiempo así como configurar y mantener sesiones simultáneamente en más de una red.

Activación del contexto PDP:

Se debe activar el contexto PDP entre el dispositivo móvil, el SGSN y el GGSN, para que el dispositivo móvil pueda transferir datos.

El usuario inicia este procedimiento el cual es similar a autenticarse en una red destino deseada.

El usuario inicia el proceso de autenticación utilizando una aplicación en el dispositivo móvil. El dispositivo móvil requiere los recursos de radio suficientes para soportar el procedimiento de activación del contexto. Una vez los recursos de radio son localizados, el dispositivo móvil envía el requerimiento de activación de contexto al SGSN. Este mensaje incluye información clave a cerca de la dirección IP estática del usuario, la calidad del servicio necesaria para este contexto, el APN (Access Point Name) de la red externa a la cual se va a conectar, la identificación del usuario y algunos parámetros de configuración IP necesarios (por ejemplo parámetros de seguridad).

Luego de recibir el mensaje de la activación del contexto PDP, el SGSN chequea el registro de suscripción del usuario para determinar si el requerimiento es válido. Si el requerimiento es válido, el SGSN envía una consulta que contiene el APN requerido al servidor DNS (Domain Name Service). El servidor DNS utiliza el APN para determinar la dirección IP del último GGSN que proveerá la conectividad requerida con la red externa. La dirección IP del GGSN es retornada al SGSN.

El SGSN utiliza la dirección IP del GGSN para hacer el requerimiento del túnel de conexión al GGSN. Luego de recibir este requerimiento, el GGSN completa el establecimiento del túnel y retorna una dirección IP que será comunicada al dispositivo móvil. El GGSN asocia el túnel a la conexión con la red externa.

Al finalizar este procedimiento, una conexión virtual es establecida entre el dispositivo móvil y el GGSN. El GGSN además tiene una asociación entre el túnel y la interfaz física hacia la red externa.

3.2.7 Creación de túneles GTP (GPRS Tunneling Protocol)

GTP es el encargado de transportar los paquetes del usuario y sus señales relacionadas entre los nodos de soporte de GPRS (GSN's). Los paquetes GTP contienen paquetes IP o X.25 del usuario.

Por debajo de él, los protocolos estándares TCP o UDP se encargan de transportar los paquetes por la red. Los paquetes de datos del usuario son llevados por el backbone del GPRS a través de paquetes GTP. Cuando llega un paquete de una red externa al GGSN, es encapsulado en un paquete GTP y luego es enviado al SGSN. El flujo de paquetes GTP dentro del backbone del GPRS es completamente transparente para el usuario (el usuario tiene la sensación de que está conectado directamente, a través de un enrutador GGSN a una red externa). En la comunicación de datos, este tipo de flujo virtual de paquetes GTP es llamado túnel. Por lo que se dice que el SGSN y el GGSN están estableciendo un túnel para transportar los paquetes del usuario. El protocolo GTP es el encargado de esto. Por lo tanto lo que se transmite entre el SGSN y el GGSN son paquetes GTP.

Los paquetes IP son utilizados en el backbone del GPRS para llevar los paquetes GTP. Por lo tanto un paquete GTP contiene el paquete original del usuario, por ejemplo un paquete TCP/IP que contiene una parte de la información del correo electrónico, es llevado dentro del paquete GTP. El paquete GTP es llevado a través del backbone del GPRS utilizando IP y TCP o UDP.

El encabezado del paquete GTP, incluyendo la identificación del túnel (TID), permite que el GSM receptor se entere quién es el usuario que envió el paquete. El TID contiene información del usuario, incluyendo el IMSI, por ende el TID es la etiqueta que le dice al SGSN y al GGSN de quién es el paquete que está dentro del paquete GTP.

Desde el punto de vista del usuario y de la red externa, los paquetes GTP que contienen los paquetes de los usuarios pueden ser transmitidos entre GSN's utilizando cualquier tecnología, por ejemplo ATM, X.25 o Frame Relay. La tecnología escogida para el backbone de GPRS es IP. Todos los elementos de la red que están conectados al backbone GPRS deben poseer una dirección IP. Las IP utilizadas en el backbone son transparentes a las Estaciones Móviles (MS – Mobile Station) y a las redes externas, y son llamadas direcciones IP privadas. Por lo tanto los paquetes de los usuarios son llevados a través del núcleo del GPRS entre SGSN y GGSN utilizando IP privadas del backbone del GPRS.

3.2.8 Funciones de alto nivel en GPRS

Algunas de las principales funciones de alto nivel requeridas por GPRS son:

- Network Access Control Function (NACF)
- Se refiere a los procedimientos que permiten a los usuarios emplear los servicios de la red (por ejemplo, autenticación y autorización, control de admisión, tarifación, etc.)
- Packet Routing and Transfer Functions (PRTF)
- Se refiere a los procedimientos para determinar la ruta que siguen los paquetes de datos, así como a la transmisión de los mismos (por ejemplo, traducción de direcciones, compresión, etc.
- Radio Resource Management Functions (RRMF)
- Se encarga de la asignación y el mantenimiento de los recursos del canal radio. La asignación de frecuencias de GSM se comparte entre los servicios de conmutación de circuitos y de GPRS.
- Mobility Management (MM) Functions
- Teniendo en cuenta que GPRS posee un sistema inalámbrico para el transporte de información, éste debe introducir el concepto de Gestión de la Movilidad (MM – Mobility Management) de las estaciones, hablando de estaciones móviles como cualquier dispositivo móvil capaz de enviar y recibir datos, que le permita al sistema disponer de un medio eficiente y confiable y de procedimientos adecuados para la transmisión y recepción de datos entre dos hosts. De no ser así, existiría un formato de recepción de datos incompleto y no estructurado en ambos extremos, lo cual disminuiría la eficiencia del sistema y aumentaría su complejidad. La MM se encarga de seguir la situación / estado de cada uno de las MS dentro y fuera de su PLMN.

Con relación a la MM, un usuario GPRS se puede encontrar en uno de tres estados posibles. Cada estado describe un tipo de funcionalidad e información almacenada. La información se denomina *MM context* y es almacenada en el MS y en el SGSN (Ver Figura 4). Estos estados son:

- Estado IDLE (Inactivo):

En este estado, el suscriptor no se encuentra registrado en la MM de GPRS y por lo tanto resulta no alcanzable. La MS y el contexto SGSN no mantienen una ubicación o información de enrutamiento válida para el suscriptor.

No se realizan los procedimientos de MM.

La MS lleva a cabo los procesos de selección y reselección de la PLMN y de la celda GPRS.

No es posible la transmisión de datos hacia y desde el suscriptor móvil, tampoco el paging del suscriptor.

La MS es vista como no alcanzable. Para establecer el MM context en la MS y en el SGSN, la MS deberá llevar a cabo el procedimiento de conexión. El Procedimiento de conexión, informa al SGSN de su presencia, lo cual actualiza las bases de datos para garantizar su visibilidad en la red.

Estado STANDBY (en espera):

En este estado, el suscriptor está registrado en el GPRS MM. El MS y el SGSN tienen establecido un MM context asociado al IMSI del usuario. La MS solo puede recibir una llamada o una señalización. No es posible hacer transmisión y recepción de datos. El MS puede activar o desactivar un PDP context.

En cualquier momento la MS puede llevar a cabo la selección y reselección de la celda GPRS, o entrar en una nueva área de enrutamiento, esto se hace al nivel de red local. Los procedimientos de MM se ejecutan para informar al SGSN sobre el cambio de área de enrutamiento y sobre cambios de celda.

De esta manera, en el estado STANDBY el SGSN contiene toda la información del área de enrutamiento de la MS. Para un SGSN iniciar la comunicación con la MS, le envía una solicitud. Si el flag PPF [1] está en Clear, se completa la solicitud. La MS pasa a estado READY y se establece la conexión. Para controlar el tiempo de conexión de la MS con el SGSN se usa un timer. Si el timer expira, el SGSN ejecuta el procedimiento de desconexión con el fin de devolver al suscriptor al estado IDLE. El procedimiento de desconexión es exactamente opuesto al procedimiento de conexión. Este hace que la MS no pueda acceder a la red.

Estado READY (listo):

Se refiere a la información de ubicación en el SGSN MM context e indica la celda donde se encuentra la MS. La MS puede enviar y recibir Paquetes de Datos (PDU – Protocol Data Unit) en algún PDP, así como desactivar un contexto PDP o activar uno nuevo.

La MS puede enviar PDUs en algún PDP. En el estado READY, el SGSN también recibe actualizaciones desde la MS indicando el cambio de área de enrutamiento y la selección y reselección de celdas.

Aún cuando no se han asignado recursos de radio a un suscriptor, el MM context permanece en el estado READY, así no se estén transmitiendo datos. El estado READY esta controlado por un timer. Cuando el timer expira, el dispositivo móvil va al estado STANDBY.

[1] PPF (Paging Proceed Flag) : Es un flag, que si esta en “on”, esto indica que se pueden enviar mensajes Paging GPRS o Paging CS al dispositivo móvil, y si está en “off”, indica que se debe detener el paso de estos mensajes.

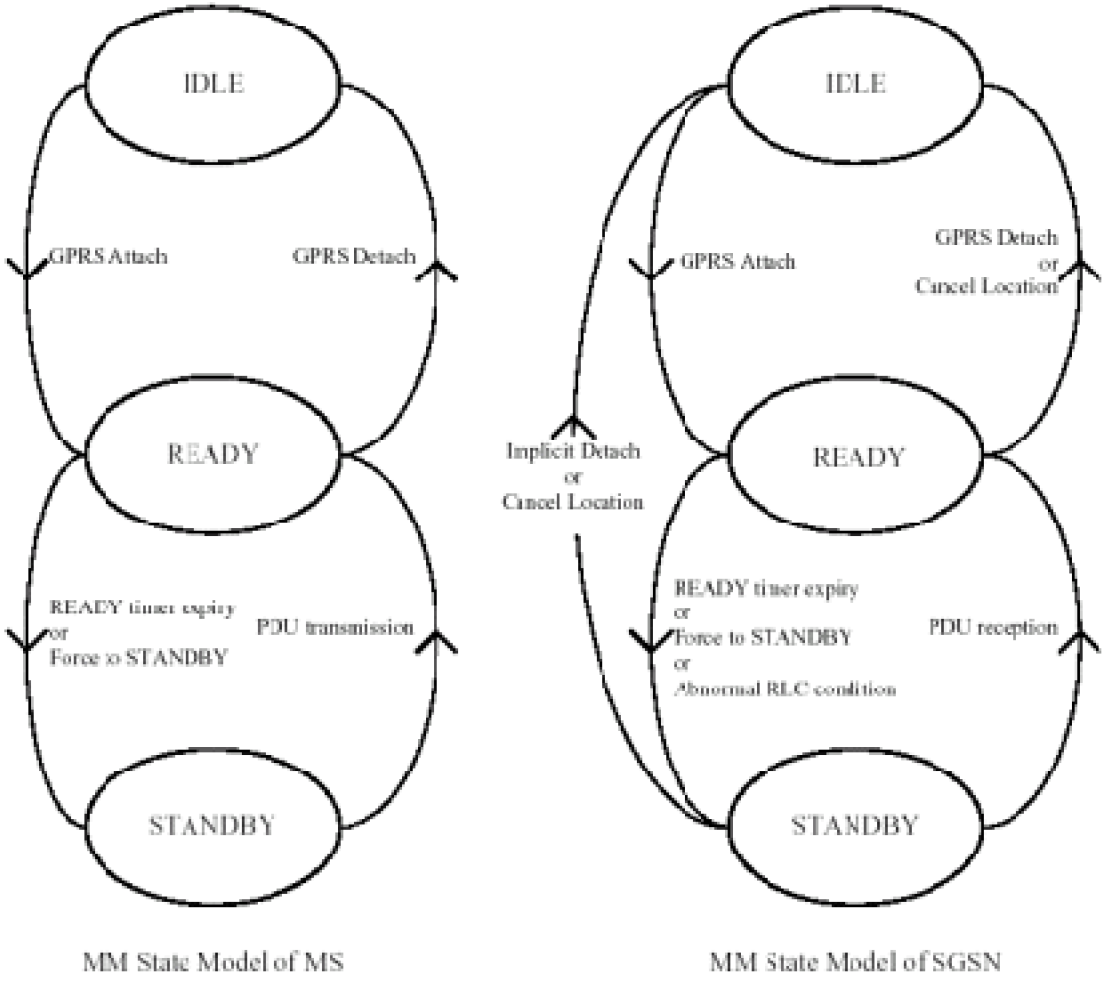

Figura 4. Gestión de la Movilidad (Estados)

3.2.9 Interfaces

GPRS especifica 9 interfaces adicionales a las que especifica GSM, todas ellas comienzan con la letra “G”. La figura 5 muestra los elementos básicos de la red GSM y GPRS y las interfaces entre ellos, las cuales se describen a continuación:

Gb

La interfaz Gb conecta el BSC con el SGSN, en otras palabras, transporta el tráfico y la señalización entre la red de Radio GSM y el backbone GPRS.

Cuando un paquete de usuario llega al SGSN, debe ser transmitido a la MS GPRS. El enlace lógico entre la MS GPRS es manejado por medio de la interfaz Gb. Para que la transmisión física pueda ser llevada a cabo, el SGSN debe estar conectado con el BSS (PCU). El PCU recibe instrucciones de la calidad del servicio con la que el paquete del usuario debe ser transmitido a la interfaz de aire. Esta información también es enviada por la interfaz Gb del SGSN al BSS (PCU).

Gn

La interfaz Gn es usada sólo cuando el SGSN y el GGSN se encuentran en la misma PLMN. Utiliza TCP/IP.

Gr

La interfaz Gr permite al SGSN solicitar información del suscriptor al HLR cuando éste se encuentra en su área de servicio.

Gi

La interfaz Gi es el punto de referencia entre PDNs externas y la red GPRS. El operador de la red y el ISP externo pueden acordar una tecnología de transmisión en la capa 1 y 2 para la conexión de ambas redes. Por ejemplo se puede usar el protocolo X.25 y el protocolo IP.

Gp

La interfaz Gp es usada cuando el SGSN y el GGSN están ubicados en diferentes PLMNs. Esta interfaz es basada en IP.

Gs

Es la interfaz entre el SGSN y el MSC/VLR y puede ser usada para ejecutar procedimientos comunes como la actualización de la ubicación. Por ejemplo, si un suscriptor se mueve del área de servicio de un SGSN hacia otra, se deben actualizar ambos registros de ubicación y la información del enrutamiento. Si esta interfaz no existe, los procedimientos de actualización de la ubicación pueden hacerse a través de la interfaz de aire. Pero si la interfaz existe, se puede iniciar un procedimiento para la actualización del enrutamiento, y el SGSN informa al MSC/VLR que se debe iniciar una actualización de la ubicación. El uso de esta interfaz permite ahorrar recursos de la interfaz de aire.

Gd

La interfaz Gd comunica el SGSN con el gateway SMS (SMS-GMSC/SMS-IWMSC), esta basada en el snack de protocolos SS7 y permite que una red GPRS pueda enviar mensajes SMS largos.

Gc

Es la interfaz entre el GGSN y un HLR. En el caso de que esta interfaz no exista, la solicitud puede ser enviada al SGSN principal, el cual a su vez transfiere la solicitud al HLR usando la interfaz Gr. La información de enrutamiento es enviada por el HLR hacia el SGSN, el cual la entrega al GGSN.

Gf

Es la interfaz entre un SGSN y un EIR. Ya que el EIR no es de obligatoria implementación tanto en GSM como en GPRS, esta interfaz tampoco es obligatoria.

Tabla 3. Resumen de las interfaces en GPRS

Interfaz	Nodos
Gb	SGSN -- BSS
Gn	SGSN -- GGSN
Gr	SGSN -- HLR
Gi	GGSN – PDNs externas
Gp	SGSN -- GGSN en diferentes PLMNs
Gs	SGSN -- MSC/VLR
Gd	SGSN – SMS-GMSC/SMS-IWMSC
Gc	GGSN – HLR
Gf	SGSN -- EIR

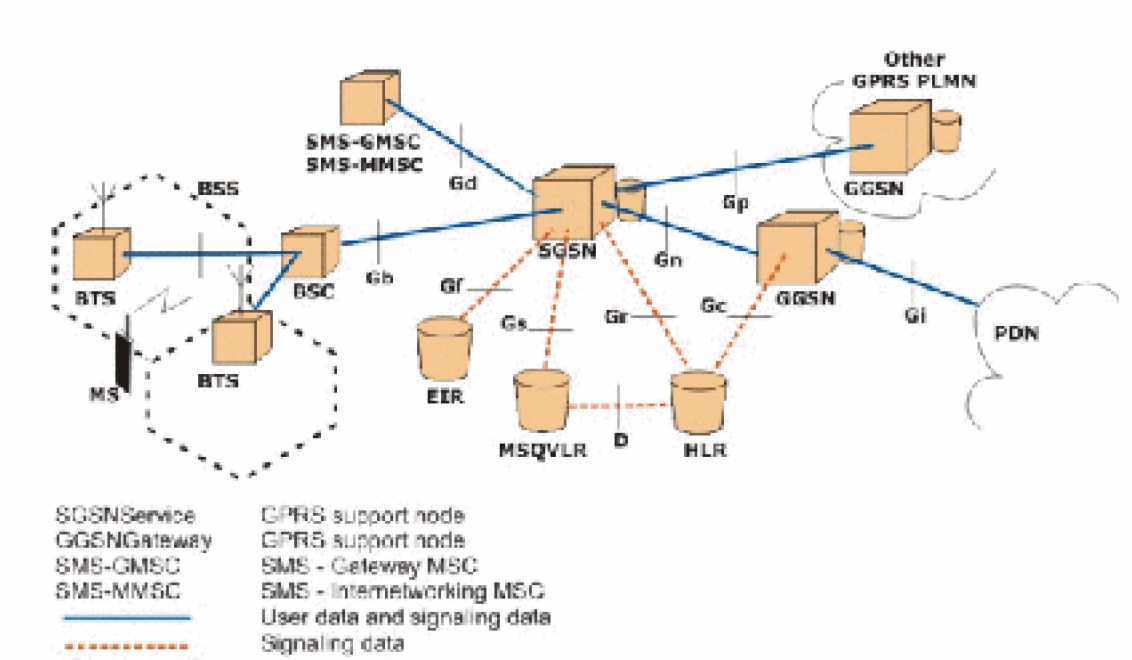

Figura 5. Arquitectura de la red GPRS

3.2.10 Dispositivo Móvil GPRS (Mobile Station – MS)

Los MS, que se encuentran del lado del cliente, requieren de una tecnología que les permita manejar tráfico de conmutación de paquetes sobre la interfaz de aire. GPRS define tres clases diferentes de MS.

Clase A

Los MS Clase A pueden manejar simultáneamente servicios GSM basados en conmutación de circuitos y servicios GPRS basados en conmutación de paquetes. También manejan simultáneamente la señalización y el control de GSM y GPRS. En esta clase no hay degradación para ninguno de los dos servicios. Se usa 1 Time-Slot para GSM y 1 o más para GPRS.

Clase B

Los MS Clase B pueden manejar simultáneamente la señalización de GSM y GPRS, pero sólo puede ser transmitido tráfico GSM o GPRS en un momento dado. Si por ejemplo, un suscriptor recibe una llamada basada en conmutación de circuitos mientras baja información de Internet, GPRS interrumpe la transmisión de datos. Tan pronto como termine la llamada de voz, la descarga de información continúa, siempre y cuando aún exista el enlace lógico entre el MS y la red GPRS (Uno de los dos está suspendido mientras el otro está activo). En esta clase sólo GPRS debe sufrir degradación de QoS.

Clase C

Los MS Clase C no pueden manejar simultáneamente GSM y GPRS. Si un dispositivo móvil está conectado a una llamada GSM, no está disponible para manejar tráfico GPRS, y viceversa. La elección de GSM o GPRS se hace manualmente.

Tabla 4. Clasificación de dispositivos móviles según la cantidad de slots

Clase	Download	Upload	Max.slots
1	1dl	1ul	2
2	2dl	1ul	3
3	2dl	2ul	3
4	3dl	1ul	4
5	2dl	2ul	4
6	3dl	2ul	4
7	3dl	3ul	5
8	4dl	1ul	5
9	3dl	2ul	5
10	4dl	2ul	5
11	4dl	3ul	5
12	4dl	4ul	5

La segunda columna se refiere a cuántos canales están reservados para efectuar descargas de la red al terminal (Download), la tercera las descargas del terminal a la red (Upload), y por último el número máximo de Time-Slots que pueden estar activos al mismo tiempo.

4. GENERALIDADES DE LAS VPN'S

Una de las necesidades más importantes de toda organización, es la de poder compartir información, y más aún, si se trata de organizaciones que poseen sedes en diferentes zonas y /o secciones que no se encuentran en el mismo entorno físico.

Inicialmente, las compañías con diferentes sedes, tenían redes LAN independientes en cada una de ellas, pero con el paso del tiempo, la información crece cada vez más y por consiguiente, la administración de esta, se hace cada vez más dispendiosa; debido a esto, las compañías se han visto en la necesidad de que sus redes LAN trasciendan mas allá del ámbito de la oficina, de que su información esté centralizada y sea más fácil de mantener, dada esta necesidad, las grandes organizaciones empezaron a implementar sistemas de acceso remoto entre sus sedes y / o secciones a través de líneas dedicadas, a muy altos costos, privilegio del que se veían privadas las organizaciones menor tamaño y con recursos técnicos y económicos más escasos.

Las últimas alternativas de comunicación, como ADSL, han hecho que la desventaja operativa desaparezca, permitiendo ya a pequeñas y medianas empresas disponer de su propia red de comunicación privada. Ahora, las centrales y tiendas o sucursales disponen de su propia red de comunicación privada. Ahora, pueden intercomunicarse y compartir información de forma sencilla y segura, con inversiones muy inferiores a las de hace muy poco tiempo.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras sin pensar en la seguridad de la información; pero Internet no es seguro, por lo tanto las VPN usan protocolos especiales

que permiten encriptar información y permitir únicamente a la persona autorizada desencriptar esa información con un identificador que comprueba que la transmisión se ha hecho desde una fuente confiable.

Una Red Virtual Privada (VPN - Virtual Private Network) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la Figura 6, la idea es que la red pública sea “vista” desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

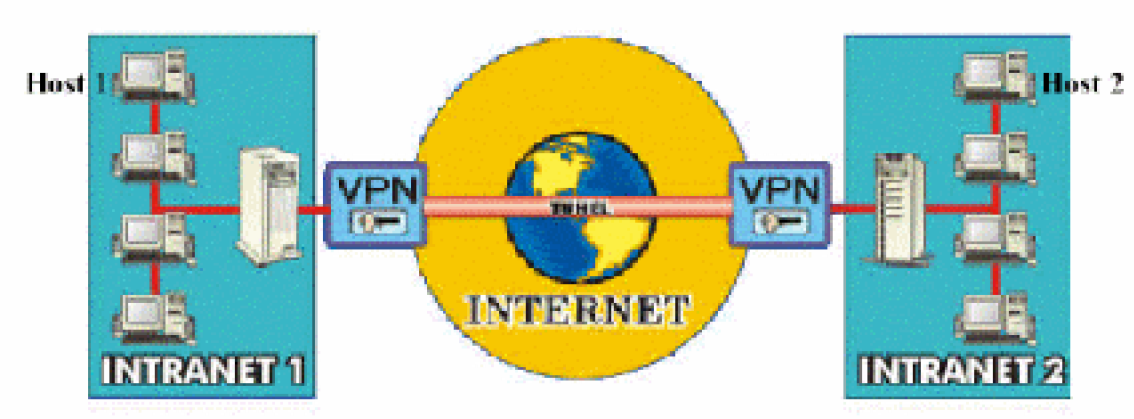

Figura 6. Esquema de una VPN

Las VPN’s también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN, a este tipo de implementación se le conoce como VPN móvil (MVPN) . Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo **túneles** virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autenticación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

Al emplear el término “túnel”, se hace necesaria una definición de este término dada su importancia dentro de las redes privadas virtuales:

El principio de funcionamiento para el proceso de túnel es el siguiente: para enviar un paquete IP al Host2, el Host1 construye el paquete que contiene la dirección IP del Host2, lo inserta en un marco ethernet dirigido al enrutador multiprotocolo que enlaza la intranet 1, y lo pone en el ethernet. Cuando el enrutador multiprotocolo recibe el marco, retira el paquete IP, lo inserta en el campo de carga útil del paquete de capa de red de la WAN, y dirige este último a la dirección de la WAN del enrutador multiprotocolo que enlaza con la intranet2. Al llegar ahí, el enrutador retira el paquete IP y lo envía al Host2 en un marco ethernet.

La WAN puede visualizarse como un gran túnel que se extiende de un enrutador multiprotocolo a otro. El paquete IP simplemente viaja de un extremo del túnel al otro. Sólo el enrutador multiprotocolo tiene que entender los paquetes IP y WAN.

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. La tecnología de túneles -Tunneling- es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama "encapsulación, a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado -encapsulación-, ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autenticación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.

El uso de la encriptación en la conexión VPN puede ser necesario en aquellos casos en los que la información que se vaya a pasar por el túnel sea sensible y requiera privacidad. La conexión encriptada VPN requiere de bastantes recursos tanto en el servidor del túnel como en el ordenador cliente de VPN a parte de requerir la instalación de software especial en el cliente.

Existen muchas aplicaciones y programas que ya hacen dicha encriptación y el encriptar el túnel VPN no nos aporta seguridad adicional. Aplicaciones tales como el

correo seguro leído por medio de una interfaz web seguro o una conexión ssh a una máquina multiusuario son suficientemente seguros para no requerir la encriptación adicional, a parte que al encriptar entre el servidor de la aplicación y el cliente de la misma la conexión es absolutamente segura en todo su recorrido, mientras que en una conexión VPN segura la encriptación sólo tiene lugar entre el servidor de túnel y el cliente VPN y la conexión entre el servidor de túneles, y el servidor de la aplicación se realiza sin encriptación.

4.1 Características de las VPN’s

Una VPN consiste en dos máquinas (una en cada "extremo" de la conexión) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos ordenadores son encriptados por el protocolo Punto a Punto (PPP - Point to Point Protocol), un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) a través de un dispositivo PPTP.

Las VPN’s permiten:

- La administración y ampliación de la red corporativa al mejor costo-beneficio.
- La facilidad y seguridad para los usuarios remotos de conectarse a las redes corporativas.

Los requisitos indispensables para esta interconectividad son:

- Políticas de seguridad.

- Requerimiento de aplicaciones en tiempo real.
- Compartir datos, aplicaciones y recursos.
- Servidor de acceso y autenticación.
- Aplicación de autenticación.

Características que deben garantizar todas las VPN:

- **Confidencialidad**: previene que los datos que viajan por la red sean leídos correctamente.
- **Integridad**: asegura que los datos de origen corresponden a los de destino.
- **Autentificación**: asegura que quien solicita la información exista.
- **Control de acceso**: restringe el acceso a usuarios no autorizados que quieran infiltrarse en la red.

4.2 Protocolos utilizados para implementar VPN's

Han sido implementados varios protocolos de red para el uso de las VPN. Estos protocolos intentan cerrar todos los huecos de seguridad inherentes en VPN.

4.2.1 PPTP - Point-to-Point Tunneling Protocol

Es un protocolo de la capa 2 del modelo OSI (enlace), que encapsula paquetes PPP en datagramas IP para ser transportados sobre una red pública IP, como Internet. Es una especificación de protocolo desarrollada por varias compañías.

Normalmente, se asocia PPTP con Microsoft, ya que Windows incluye soporte para este protocolo. Los primeros inicios de PPTP para Windows contenían características de seguridad demasiado débiles para usos serios. Por eso, Microsoft continúa mejorando el soporte PPTP. La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. Sin embargo, el principal inconveniente de PPTP es su debilidad por elegir una única encriptación y autenticación estándar: dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

El protocolo de túnel punto a punto PPTP utiliza una conexión TCP, por el puerto 1723, para el mantenimiento del túnel y tramas PPP en tramas IP encapsuladas mediante **Encapsulación de enrutamiento genérico** GRE "Generic Routing Encapsulation" para los datos del túnel. Las cargas, partes de datos útiles, de las tramas PPP encapsuladas se pueden cifrar o comprimir. El uso de PPP proporciona la capacidad de negociar los servicios de autenticación, cifrado y asignación de dirección IP. Actualmente este protocolo, aunque muy popular en el mundo de Microsoft, esta siendo sustituido por el L2TP.

Partes de un PPTP

El túnel lleva datagramas entre PAC y PNS. Muchas sesiones son multiplexadas sobre un mismo túnel:

PAC (PPTP Acces Concentrator).- es un concentrador de acceso PPTP. Es un dispositivo que asocia una o más líneas capaces de soportar PPP (Point to Point Protocol) y el manejo del protocolo PPTP. PAC necesita solamente TCP/IP para pasar sobre el tráfico de una o más PNS.

PNS (PPTP Network Server).- Es el servidor para red de PPTP. Sirve para operar sobre computadoras de propósito general y plataformas de servidores. PNS dirige la parte del servidor del protocolo PPTP mientras PPTP confía completamente TCP/IP y es independiente de la interfaz de Hardware, el PNS puede usar cualquier combinación de hardware de interfaz IP, incluyendo dispositivos LAN y WAN.

PPTP esta implementado para PAC y PNS. Existen actualmente relacionados muchos PAC y PNS, un PAC puede proveer servicio a muchos PNS.

PPTP usa una forma parecida a GRE (Generic Routing Encapsulation) para llevar los paquetes PPP de usuario. Permite a bajo nivel controlar la congestión y flujo que va a llevarse a través de los túneles usados para llevar los datos de usuarios entre PAC y PNS.

Este mecanismo permite la eficiencia del uso del ancho de banda disponible para los túneles y evita retransmisiones innecesarias y desbordamiento en los buffers.

PPTP requiere el establecimiento de un túnel para cada comunicación PNS-PAC. Este túnel es usado para llevar todos los paquetes PPP de sesión de usuario participando un par determinado de PNS y PAC. Una llave está presente en el encabezamiento GRE indicando a cual sesión en particular pertenece el paquete PPP. De esta manera los paquetes PPP son multiplexados y demultiplexados sobre un túnel simple entre el PNS y PAC dado. El valor a usar en el campo de la llave es establecido por la llamada, estableciendo el procedimiento mediante el cual toma el control de la conexión. El encabezamiento GRE también contiene la secuencia de información que ha sido usada para desempeñar algún nivel de control de congestión y detección de errores sobre el túnel. Luego la conexión de control es usada para determinar la tasa y los parámetros de almacenamiento temporal que han sido usados para regular el flujo de paquetes PPP para una sesión particular sobre el túnel.

4.2.2 L2F Layer 2 Forwarding

L2F es un protocolo de transmisión que permite a un servidor encapsular el tráfico de una conexión telefónica convencional en PPP y transmitirlo sobre enlaces WAN a un servidor L2F. Este servidor desencapsula los paquetes y los inyecta a la red. En contraste con PPTP y L2TP, L2F no tiene un cliente definido. L2F es una tecnología propuesta por Cisco.

4.2.3 L2TP Layer Two Tunneling Protocol

El principal competidor de PPTP en soluciones VPN fue L2F. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP. L2TP existe en el nivel de **enlace** del modelo OSI. Al igual que PPTP, L2TP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

El escenario típico L2TP, cuyo objetivo es la creación de marcos PPP entre el sistema remoto o cliente LAC (L2TP Access Concentrator) y un LNS (L2TP Network Server) ubicado en una LAN local.

Un LAC es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto son locales o a través una conexión PPP.

Un LNS actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

L2TP sobre IP utiliza el puerto UDP 1701 e incluye una serie de mensajes de control L2TP para el mantenimiento del túnel. L2TP. También utiliza UDP para enviar tramas PPP encapsuladas en L2TP como datos del túnel. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, aprovechan la seguridad IPSec estándar mediante el modo de transporte IPSec para obtener una fuerte protección de integridad, reproducción, autenticidad y privacidad.

L2TP se diseñó específicamente para conexiones cliente a servidores de acceso a redes, así como para conexiones entre gateways. Mediante su utilización del protocolo PPP, L2TP gana compatibilidad multiprotocolo para protocolos como IPX y Appletalk.

El L2TP soporta dos modos de túneles, el modo Obligatorio y el Voluntario.

Túnel Obligatorio L2TP

1. El usuario remoto inicializa una conexión PPP a un ISP

2. El ISP acepta la conexión y el enlace PPP se establece

3. El ISP solicita la autentificación parcial para saber el nombre de usuario

4. El ISP mantiene una lista de todos los usuarios admitidos, para servir el final del túnel LNS

5. El LAC inicializa el túnel L2TP al LNS

6. Si el LNS acepta la conexión, el LAC encapsulara el PPP con el L2TP, y entonces enviará a través del túnel

7. El LNS acepta estas tramas, y las procesa como si fueran tramas PPP.

8. El LNS la autentificación PPP para validar al usuario y entonces asigna una dirección IP

Túnel Voluntario L2TP

1. El usuario remoto tiene una conexión a un ISP ya establecida

2. El cliente L2TP (LAC), inicializa el túnel L2TP al LNS

3. Si el LNS acepta la conexión, LAC encapsula con PPP y L2TP, y lo manda a través del túnel

4. El LNS acepta estas tramas, y las procesa como si fueran tramas normales de entrada

5. el LNS entonces usa la autentificación PPP para validar al usuario y asignarle una IP

4.2.4 IPSec - Internet Protocol Security

IPSec es una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPSec existe en el nivel de **red** en OSI, para extender IP con el propósito de soportar servicios más seguros basados en Internet.

En la siguiente sección se hará un estudio más detallado del protocolo IPSec ya que el escenario VPN basado en IPSec, es el preferido por los operadores inalámbricos.

4.3 EL PROTOCOLO IPSec

IPSec es un protocolo de seguridad “de extremo a extremo”: toda la funcionalidad e inteligencia de la conexión VPN reside en los puntos extremos; es decir, en un enrutador o en la computadora terminal.

El protocolo IPSec definido en el RFC 2401 [1], especifica un conjunto de extensiones que proveen servicios de seguridad en la capa de red. La tecnología de IPSec está basada en un estándar de tecnologías criptográficas que habilitan una muy fuerte integridad de los datos y garantizan privacidad. Dado que el protocolo IPSec asegura conectividad en la capa de red, garantiza seguridad para cualquier aplicación que la use. Los servicios de seguridad que ofrece son: integridad independiente de la conexión, autenticidad de los datos de origen, confidencialidad (encriptación) y protección a repeticiones durante el flujo de tráfico.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende la validación del remitente de los datos.

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

Los servicios de seguridad que ofrece IPSec se consiguen mediante:

Dos protocolos de seguridad de tráfico: AH – Authentication Header, que confiere integridad de los datos, y ESP – Encapsulating Security Payload, que confiere integridad y confidencialidad de los datos.

Un protocolo de gestión de clave criptográfica: el denominado “Intercambio de claves por Internet” (IKE- Internet Key Exchange), que se utiliza para negociar las conexiones IPSec.

4.3.1 Protocolos de seguridad de tráfico

Cabecera autenticación AH: asegura la autenticidad y la integridad de los datos incluyendo campos invariantes de la cabecera (direcciones origen y destino, por ejemplo)

Cabecera de encapsulado de seguridad ESP: protege la autenticidad, confidencialidad e integridad de los datos (no incluye cabecera).

La diferencia más importante entre los protocolos AH y ESP, es que AH protege partes del encabezado IP, como las direcciones de origen y destino y ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al encabezado.

Los protocolos AH y ESP pueden ser aplicados solos o combinados. Cada uno de ellos soporta dos modos de uso: modo transporte y modo túnel. En el modo transporte los protocolos proveen protección para los protocolos que están en capas superiores; en modo túnel, los protocolos son aplicados a paquetes IP encapsulados en otros.

El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los encabezados de seguridad son antepuestos a los de la capa de transporte, antes de que el encabezado IP sea incorporado al paquete. En otras palabras, AH cubre el encabezado TCP y algunos campos IP, mientras que ESP cubre la encriptación del encabezado TCP y los datos, pero no incluye ningún campo del encabezado IP.

El modo de túnel es usado cuando el encabezado IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un enrutador. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el encabezado IP entre los extremos, agregando al paquete un encabezado IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del enrutador.

El protocolo IPSec en modo túnel, permite definir un túnel entre dos enrutadores. Un

enrutador IPSec consistiría normalmente en un enrutador de acceso o un firewall en el que esté implementado el protocolo IPSec. Los enrutadores IPSec están situados entre la red privada del usuario y la red compartida del operador.

Los túneles IPSec se establecen dinámicamente y se liberan cuando no están en uso. Para establecer un túnel IPSec, dos enrutadores deben autenticarse y definir los algoritmos de seguridad y las claves que utilizarán para el túnel. El paquete IP original es encriptado en su totalidad e incorporado en encabezamientos de autenticación y encriptación IPSec. Se obtiene así la carga útil de un nuevo paquete IP cuyas direcciones IP de origen y destino son las direcciones IP públicas de los enrutadores IPSec. Se establece así la separación lógica entre los flujos de tráfico de la VPN en una red IP compartida. Seguidamente, se utiliza un enrutamiento IP tradicional entre los extremos del túnel.

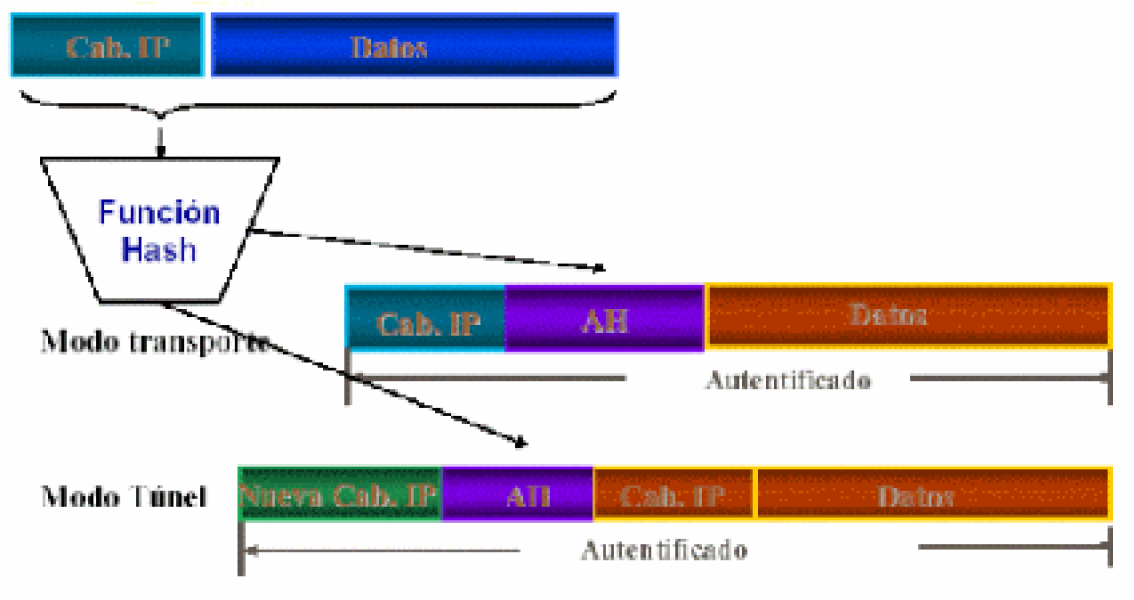

Figura 7. Modo túnel en modo transporte. Ejemplo con AH

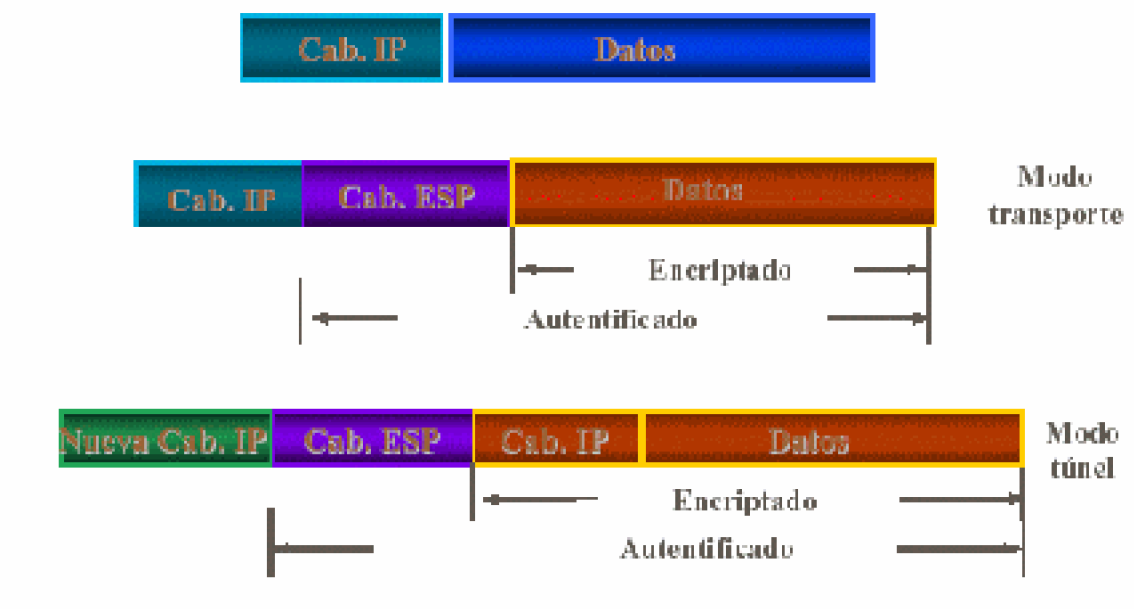

Figura 8. Modo transporte en modo túnel. Ejemplo con ESP

Ejemplo AH y ESP: Como ESP no puede autenticar la cabecera IP más exterior, es muy útil combinar una cabecera AH y ESP:

Figura 9. AH – ESP modo transporte

Figura 10. AH - ESP modo túnel

4.3.2 Protocolo de gestión de clave criptográfica IKE

4.3.2.1 Asociaciones de seguridad (SA – Security Associations)

Una SA es la relación entre dos o más entidades que describe cómo las entidades utilizarán los servicios de seguridad para comunicarse de forma segura. Esta relación está representada por un grupo de información que puede ser considerada un contrato entre las entidades.

El contenido de una SA variará para cada conexión, y puede incluir claves de autenticación o cifrado, algoritmos específicos, tiempos de vida de las claves, direcciones IP.

Una SA indica a un dispositivo IPSec cómo procesar paquetes IPSec entrantes, o cómo generar paquetes IPSec salientes.

Los dispositivos IPSec insertan un campo en el encabezado de IPSec para asociar un cierto datagrama a la SA adecuada en las máquinas que los procesen.

4.3.2.2 Funcionamiento de IKE

Los enlaces seguros de IPSec son definidos en función de Asociaciones de seguridad (SA's).

Partes del tráfico pueden estar sujetas a varias SA, cada una de las cuales aplica cierta transformación.

Al establecer una SA entre dos hosts, ellos deben primero adicionar una política de compatibilidad y algoritmos criptográficos. Deben además compartir un mecanismo seguro para determinar una clave sobre un canal inseguro. El método por defecto de IPSec para una negociación de claves segura es el protocolo IKE. Este permite que diversos tipos de autenticación, métodos y grupos de estándares criptográficos sean utilizados.

IPSec reside en la capa de red, por el contrario el protocolo IKE pertenece a la capa de aplicación.

IKE provee determinación de clave de seguridad a través del intercambio DH (Diffie-Hellman).

Intercambio Diffie-Hellman para transmisión de datos entre A y B

Se elige un numero primo **n** y un entero **x** (Estos números pueden ser públicos eso no debilita el método.)

Luego el PC **A** toma en secreto un numero **a** al azar

Luego A calcula: (**x^a)** mod **n** y le envía ese número al PC **B**

El PC **B** toma en secreto un numero **b** al azar

Luego **B** calcula: (**x^b)** mod **n** y le envía ese numero al PC **A**

El PC **A** ahora calcula **(x^b)^a mod n**

El PC **B** ahora calcula **(x^b)^a mod n**

El resultado de los pasos A y B es el mismo y esa sería la clave secreta que utilizan ambos PC's.

IKE consiste de dos fases, la primera crea una ISAKMP [2] SA o IKE SA, utilizando un intercambio DH. El propósito de esta fase es establecer un canal bidireccional seguro. El establecimiento de una ISAKMP SA debe ser siempre el primer paso de una transacción con IPSec.

Luego, en la segunda fase Los nodos IPSec negocian por el canal establecido:

- Algoritmo de cifrado
- Algoritmo hash

[2] ISAKMP: Internet Security Association and Key Management Protocol Marco conceptual para la autenticación y el intercambio de claves. Define formatos de datos, la mecánica del protocolo de intercambio de claves y la negociación de una SA. Independiente de cualquier tecnología de claves.

- Método de autenticación.

A través de una ISAKMP SA se pueden establecer múltiples IPSec SA's .

IKE proporciona tres métodos de autenticación para establecer una relación de confianza entre los equipos:

- La autenticación Kerberos 5.0 la proporciona el dominio de Windows 2000 que sirve como Centro de distribución de claves Kerberos versión 5.0 (KDC). Éste proporciona una cómoda implementación de comunicaciones seguras entre equipos de Windows 2000 que son miembros de un dominio o a través de dominios con relación de confianza.
- Las firmas de clave pública o privada que utilizan certificados son compatibles con algunos sistemas de certificados, incluidos los de Microsoft, Entrust, VeriSign y Netscape. Esto forma parte del RFC 2409. [2]
- Las contraseñas, llamadas claves de autenticación compartidas previamente, se utilizan estrictamente para establecer relaciones de confianza entre equipos. Esto forma parte del RFC 2409.

Una vez configurados con una política IPSec, los equipos homólogos negocian mediante IKE para establecer una asociación de seguridad principal para todo el tráfico que se desarrolla entre los dos equipos. Esto implica realizar la autenticación mediante uno de los métodos anteriores y generar una clave maestra compartida. Los sistemas utilizan entonces IKE para negociar otra asociación de seguridad para el tráfico de la aplicación que intentan proteger en ese momento. Esto trae consigo la generación de claves de sesión compartidas. Sólo los dos equipos conocen ambos conjuntos de claves. Los datos intercambiados mediante la asociación de seguridad se encuentran muy bien protegidos contra modificaciones o interpretaciones por parte de atacantes que pudieran actuar en la red.

5. IMPLEMENTACIÓN DE UNA VPN SOBRE GPRS

La creciente demanda de acceso móvil a intranets corporativas a través de la infraestructura GPRS, requiere la provisión de autenticidad, confidencialidad e integridad de los servicios. Los más importantes mecanismos de seguridad, tales como VPN's e IPSec, fueron originalmente concebidos para dirigirse a problemas de seguridad en redes fijas. Sin embargo, la aumentada movilidad de usuarios / dispositivos y la nueva tendencia de la integración entre móviles y redes fijas han introducido un nuevo mundo de escenarios de seguridad que no fueron previstos.

Aunque hay algunas criticas con respecto a IPSec, se admite comúnmente que este es el mejor protocolo de seguridad IP disponible hoy [3]. Este facilita la encriptación transparente y la protección de integridad tanto de paquetes Ipv4 como Ipv6 y la autenticación entre las entidades que se comunican. Es especialmente utilizado para la implementación de VPN's y para acceso de usuarios remotos a redes privadas. Una gran ventaja de IPSec es que los arreglos de seguridad pueden ser manejados sin necesidad de cambios en los computadores de usuarios individuales. Adicionalmente, IPSec es empleado bajo la capa de transporte (TCP / UDP), así que es transparente para los usuarios finales y sus aplicaciones. Finalmente, otra fortaleza de IPSec es su flexibilidad, la cual simplifica su instalación y funcionamiento a través de cualquier red IP existente.

Por otro lado, la desventaja principal de IPSec es su complejidad. Este contiene demasiadas opciones y demasiada flexibilidad, esto hace que existan muchas formas de

hacer lo mismo, por lo que algunos argumentan que la dificultad para analizar la seguridad de un sistema aumenta con su complejidad [22]. Adicionalmente el protocolo IKE ofrece muchas opciones para un gran número de escenarios, en lugar de dirigirse a un número de necesidades más limitadas de una forma más simple lo que lo hace también muy complicado de manejar.

Desafortunadamente, el desarrollo de servicios VPN utilizando el protocolo IPSec no está libre de problemas, especialmente sobre las redes móviles GPRS. Exceptuando la configuración de los protocolos IPSec e IKE, el principal problema identificado es la incompatibilidad entre la traducción de direcciones de red (NAT - Network Address Translation) e IPSec (debido al cambio que hace NAT en el campo IP Origen del paquete fuente).

NAT toma un paquete IP que sale de una red y reemplaza la dirección origen privada con una dirección origen pública permitiendo a hosts con direcciones privadas acceder a Internet, y el proceso contrario para un paquete entrante. En IPSec, el protocolo AH protege la integridad del encabezado IP (donde se encuentran las direcciones IP origen y destino) agregando un campo que permite verificar la integridad del paquete, posteriormente al pasar por el NAT, el paquete IP cambia su dirección origen, lo cual hará que falle la verificación de integridad del mismo, salvo que se utilice IPSec en modo túnel y el NAT se haga antes, o en el mismo dispositivo donde se hace el túnel IPSec.

En la actualidad algunos dispositivos NAT permiten que un Gateway VPN pase a través de ellos, lo cual se denomina IPSec Passthrough.

De la misma manera, existe otra alternativa denominada NAT Traversal (NAT-T) que permite que varios clientes VPN salgan con NAT, mediante la encapsulación de IPSec en un segmento UPD.

5.1. Escenario End– to – End

5.1.1 Arquitectura de una MVPN [3] sobre GPRS

El escenario se desarrolla para un usuario móvil que establece una conexión segura a la Intranet corporativa de una organización, como se muestra en la Figura 7.

Los pasos que se siguen para la conexión son:

El dispositivo móvil hace presencia conectándose a la red GPRS, la cual establece un enlace lógico entre la estación y el SGSN.

Para enviar y recibir datos, el dispositivo móvil activa su dirección PDP, la cual la introduce al correspondiente GGSN, y el intercambio con redes de datos externas puede empezar.

[3] **MVPN: Móbile VPN**

Con los dos primeros pasos: la conexión a la red y la activación del contexto PDP (Sección 3.2.6), el dispositivo móvil adquiere una dirección IP, gracias a esto en el tercer paso, se crea un túnel GTP entre el SGSN y el GGSN, adicionalmente, se configura la ruta física entre el GGSN, SGSN y el dispositivo móvil.

El usuario móvil inicia una sesión entre él y el Security Gateway (SG) de la red LAN.

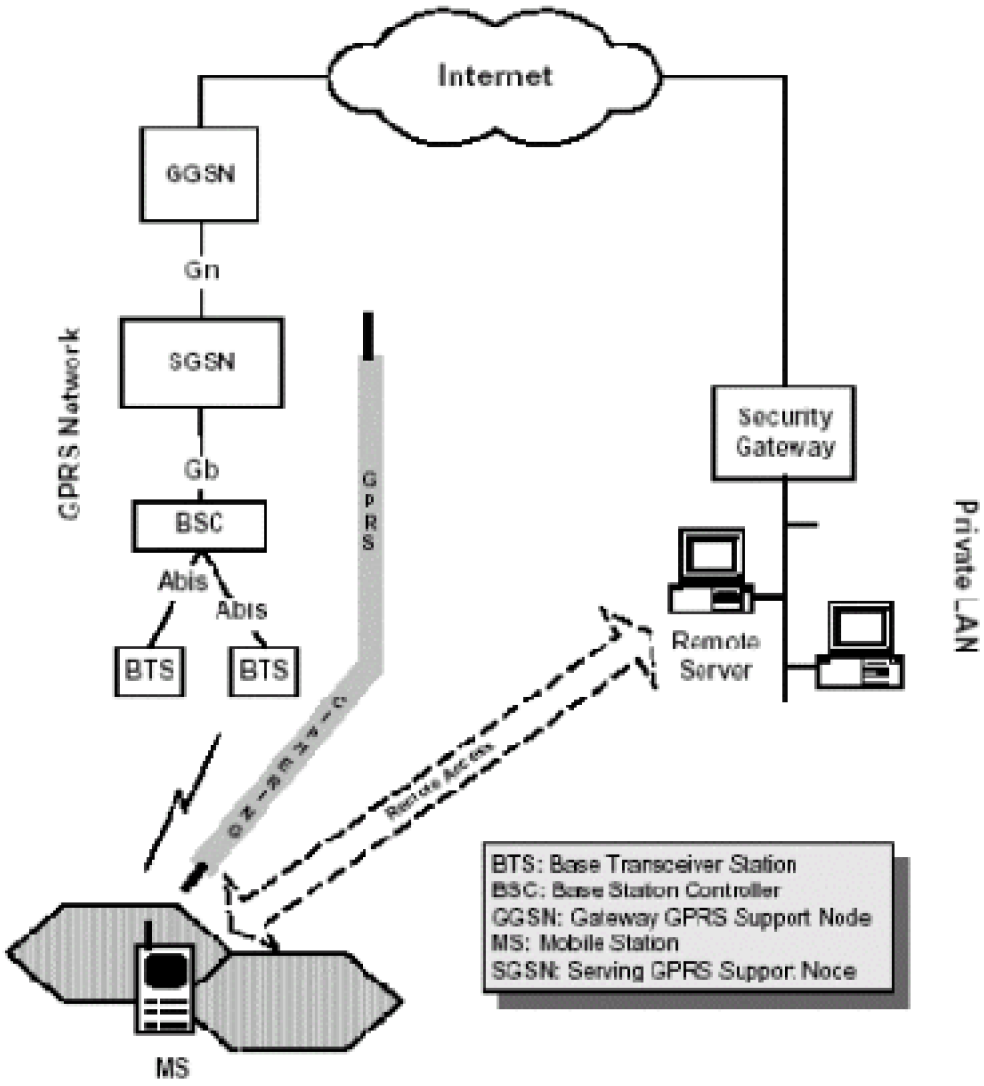

Figura 11. Arquitectura de una VPN sobre GPRS

5.1.1.1 Sesión entre el Security Gateway y la red LAN

El Security Gateway (SG) es un dispositivo posicionado entre Internet o la red pública y la red privada. Este funciona como un proxy que brinda servicios de seguridad a los nodos de la red privada protegidos por él.

Para el establecimiento de la VPN entre el dispositivo móvil y el SG, se negocia la sesión IPSec a través del protocolo IKE. Como se mencionó en la sección 4.3.2.2, IKE tiene dos fases:

· FASE 1

Durante la primera fase, se inicia una asociación de seguridad (SA) ISAKMP [4] , en modo agresivo (AM). La negociación en Modo agresivo de IKE es una opción para acelerar la transacción de IKE, usando claves precompartidas para establecer la SA, sacrificando ligeramente la seguridad. Es más, el método de autenticación usado en AM, no tiene en cuenta la dirección IP de quien inicia la negociación. Así, el protocolo IKE es operacional en un ambiente de red móvil donde pueden ser usadas direcciones IP dinámicas.

En la Figura 8, se observan los pasos para la negociación en modo agresivo:

El dispositivo móvil envía al SG un mensaje que contiene: una cookie [5] (número de 64 bit generado aleatoriamente para prevenir ataques), el dato ISAKMP SA, la mitad de la clave Diffie Hellman, una marca de tiempo (número largo entre 4 y 2048 bits) y la identificación de los datos.

El Security Gateway SG, responde con un mensaje que contiene: la respuesta al cookie, la respuesta ISAKMP SA, la mitad de la clave Diffie Hellman, una marca de tiempo, su identidad y la clave HASH, la cual contiene información de autenticación del SG.

Finalmente, en un tercer mensaje, el dispositivo móvil transmite su información de autenticación a SG junto con la respuesta al cookie.

[4] ISAKMP: Internet Security Association and Key Management Protocol Marco conceptual para la autenticación y el intercambio de claves.

[5] Una "cookie" es una pequeña cantidad de información que un servidor de la Red almacena en su navegador. Es útil para que su navegador recuerde cierta información que posteriormente su servidor leerá

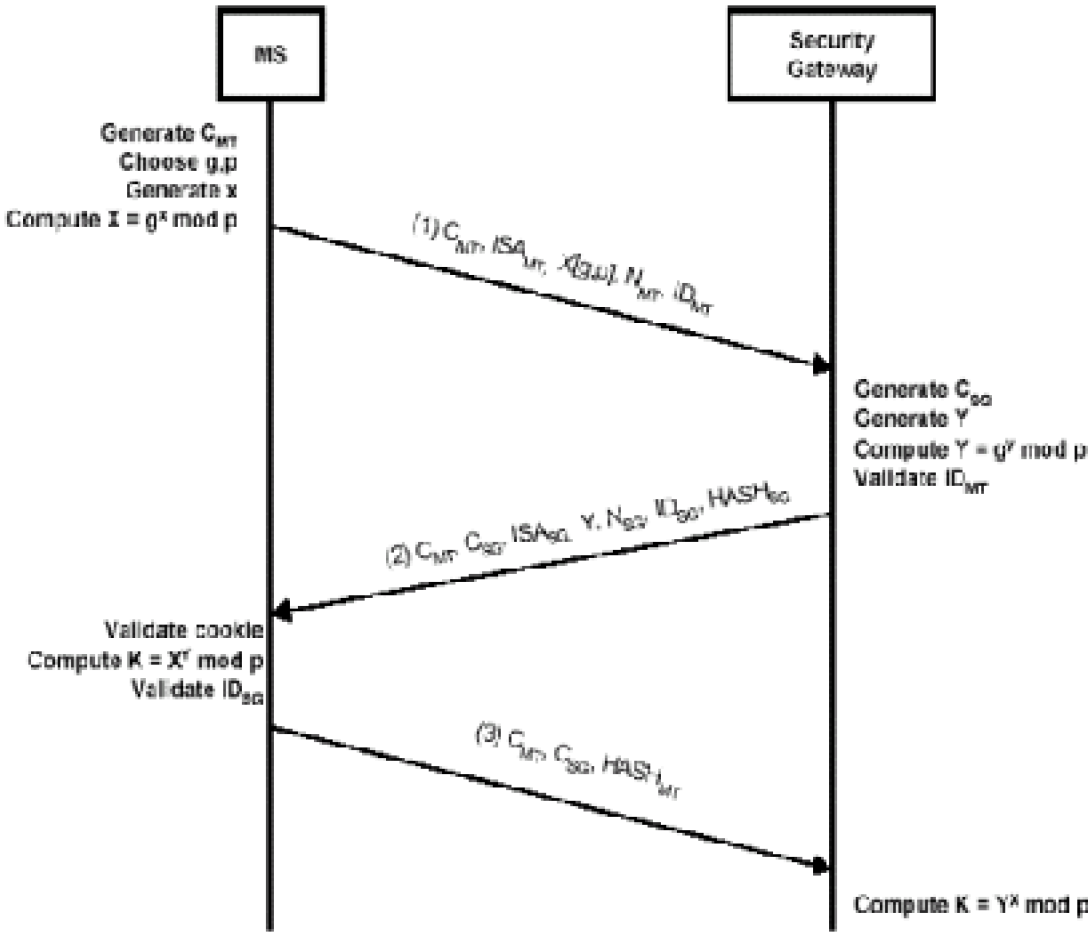

Figura 12. Negociación de la SA ISAKMP en modo agresivo

La autenticación entre el dispositivo móvil y el SG está basada en un método de clave pre-compartida, ya que esta es la forma más simple de autenticación comparada con la firma digital y la encriptación de clave publica, y se ajusta mejor al escenario móvil. El cálculo de la autenticación se realiza basado en la identificación contenida en el payload del paquete, la cual es estática y no en la dirección IP la cual puede variar.

Habiendo establecido una asociación de seguridad ISAKMP entre la MS y el SG, las partes han acordado:

El algoritmo de encriptación para proteger los datos.

El algoritmo Hash para reducir los datos a ser firmados

El método de autenticación para firmar los datos

El intercambio Diffie – Hellman

Una función opcional seudo–aleatoria utilizada para codificar ciertos valores durante

el intercambio de claves con propósitos de verificación.

- FASE 2

Luego de completar con éxito la primera fase, comienza la segunda fase de IKE: negociación en modo rápido (quick mode), con ésta se pretende establecer una asociación de seguridad IPSec (IPSec SA) entre la MS y el SG. Todos los paquetes que pertenecen a la fase 2 son encriptados utilizando la asociación de seguridad ISAKMP preestablecida.

En la Figura 9 se observan las transacciones entre la MS y el SG en modo rápido (quick mode):

La MS transmite las cookies (C_{MS} , C_{SG}), su solicitud de asociación de seguridad IPSec (SA_{MS}), su marca de tiempo (N_{MS}), la mitad de la clave Diffie Hellman (DH), y la identidad de la MS y del SG (ID_{MS}, ID_{SG} respectivamente). Adicionalmente a esto, la MS autentica el mensaje con una clave HASH (1).

El SG transmite las cookies, su respuesta IPSec SA, su marca de tiempo, la mitad de la clave DH y las identidades MS y SG. El SG, también autentica el mensaje con una clave HASH (2).

La MS autentica la transacción con una clave HASH (3). Luego de este dialogo entre la MS y el SG, se establece una IPSec SA, la cual contiene todos los parámetros necesarios para una comunicación segura.

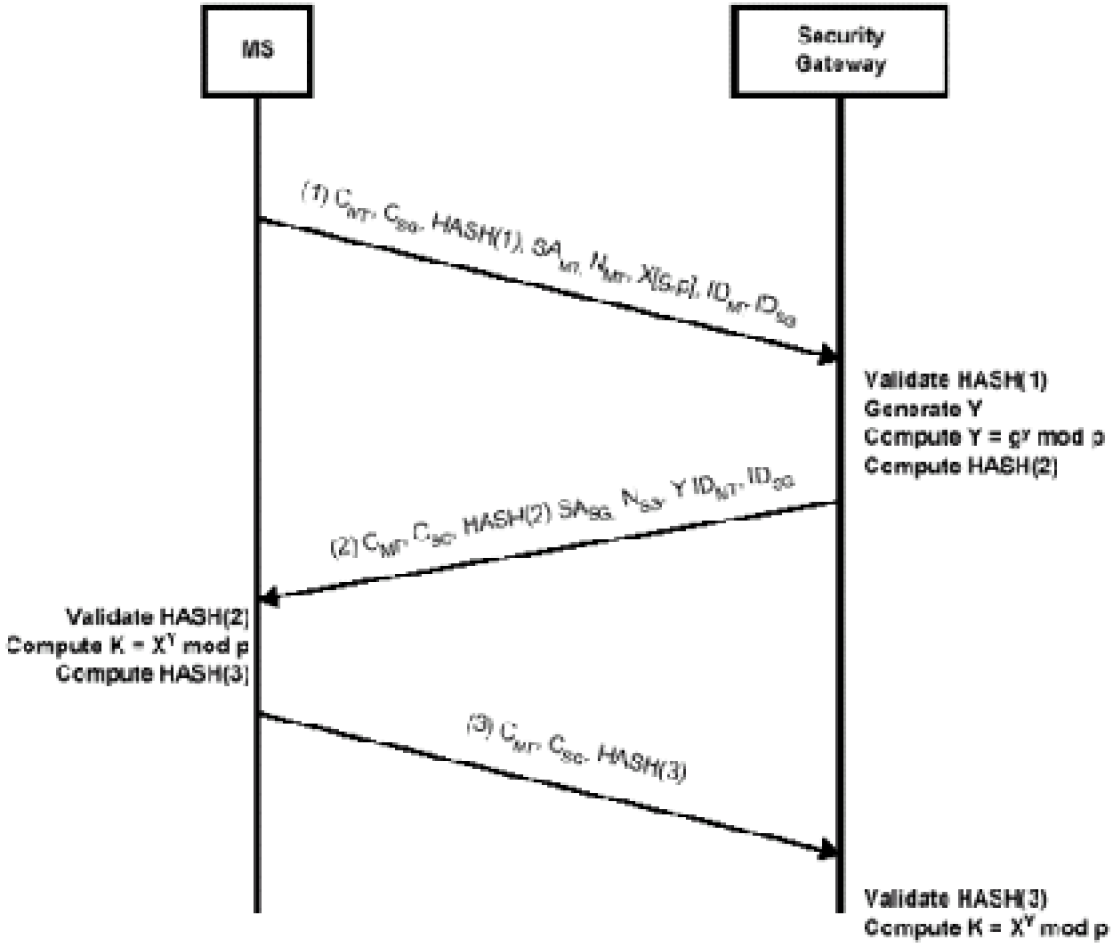

Figura 13. Negociación de la SA IPSec (Modo rápido)

- Esta asociación tiene las siguientes especificaciones:
- El índice de parámetro de seguridad
- La dirección IP destino
- El identificador del protocolo de seguridad, en este caso ESP
- El modo en el que operara el protocolo IPSec, en este caso, modo transporte.
- El algoritmo de encriptación utilizado en ESP y las claves que utiliza.
- Cómo se desempeña la autenticación
- Cuantas veces son cambiadas estas claves
- El tiempo de vida de la propia asociación de seguridad
- La dirección fuente de la asociación de seguridad SA.

Dado que la SA es usada solo en una dirección, para la comunicación bidireccional entre la MS y el SG, se requieren dos SA's.

5.1.2 Operación de IPSec

Habiendo establecido un par de SA IPSec entre la MS y el SG, se ha puesto en funcionamiento un canal que permite el intercambio seguro de información entre estos dos nodos. El dispositivo móvil GPRS que está ubicado en una red pública móvil (PLMN), ahora puede enviar y recibir paquetes IP a y desde un servidor remoto conectado a una LAN privada a través de Internet.

El empleo del protocolo ESP es considerado una gran ventaja en esta arquitectura ya que ESP puede brindar muy buena protección de integridad. Además, el protocolo IPSec es configurado en modo transporte puesto que uno de los puntos de terminación de la VPN que es la MS, es muy difícil de operar en modo túnel.

El SGSN al que la MS esta registrada, encapsula a través del GTP los paquetes IP ya encriptados que provienen de la MS, examina el contexto PDP y los enruta al interior del backbone GPRS para ser entregados al GGSN apropiado. El GGSN desencapsula los paquetes GTP, y aplica NAT sobre ellos. Así, los paquetes son re enviados a la red pública IP y posteriormente entregados al SG de la red privada.

Una vez que el SG recibe los paquetes protegidos IP, éste termina el túnel IPSec, desencripta los paquetes y los envía al host destino dentro de la LAN. Dado que se utilizó NAT, el SG cambia dirección destino en el encabezado IP. El empleo de NAT dentro del SG no tiene impacto sobre la operación IPSec, ya que IPSec está localizado en el espacio de direcciones públicas y así la combinación de IPSec con NAT es viable sin problemas de incompatibilidad.

Sin embargo, el servidor remoto de la red LAN privada envía paquetes IP a la MS, el SG recibe estos paquetes, cambia su dirección IP fuente (NAT), y los mapea a la asociación de seguridad apropiada. Los paquetes encriptados son llevados a través de la red IP y son enrutados hasta el GGSN que sirve el área de cobertura en la que se encuentra la MS. La dirección IP de la MS, que ha sido asignada por el GGSN, tiene el mismo prefijo de red que el de la dirección IP del GGSN. Este encapsula los paquetes IP entrantes y a través de un túnel los lleva al interior de la GPRS hasta entregarlos al SGSN. El SGSN desencapsula los paquetes y los entrega a la MS.

5.1.3 Consideraciones en el escenario End – to – End

5.1.3.1 Consideraciones al utilizar el protocolo GTP

La comunicación entre GGSNs y SGSNs, esta basada en túneles IP. [4]. Esto significa que los paquetes IP estándar, tan pronto como alcanzan un nodo GSN, son encapsulados en nuevos paquetes IP y enrutados como corresponde. GTP es una parte integral de la tecnología GPRS y opera de manera transparente para servicios VPN. Un problema que puede resultar de utilizar GTP en el escenario VPN es la encapsulación duplicada del paquete IP original (IPSec y GTP) para la transmisión segura sobre la red GPRS, ya que esto introduce basura que consume recursos valiosos y puede causar problemas de eficiencia en la red y degradación del desempeño.

5.1.3.2 Consideraciones al utilizar NAT

Generalmente, el uso de NAT es un poco problemático, cuando se usa con IPSec porque IPSec oculta el direccionamiento privado mediante la encriptación, por lo cual no es posible su posterior traducción, o experimentan violaciones de integridad debido a la manipulación de NAT a las direcciones IP protegidas.

En este escenario particular de VPN, hay dos puntos donde NAT puede ser aplicado: SG y GGSN. El SG en la LAN privada combina la funcionalidad de IPSec y NAT en el mismo dispositivo. Hasta el momento, la forma más sencilla de evitar problemas es ubicar el punto final de IPSec en el espacio de direcciones públicas (NAT antes de IPSec) y de esta manera la coexistencia de IPSec con NAT no provoca problemas de incompatibilidad.

Por otro lado, el NAT en el GGSN toma lugar entre los puntos de terminación de la VPN (MS y SG), y contrario a lo mencionado anteriormente, el número de incompatibilidades potenciales puede aumentarse. [5, 6, 7]

- Incompatibilidad entre la autenticación IPSec y NAT.
- Incompatibilidad entre el checksum (campo de verificación de integridad de información) de TCP y NAT.
- Incompatibilidad entre los identificadores de dirección IKE y NAT.

ESP emplea un algoritmo de mensaje resumido para la autenticación de paquetes, pero a diferencia de AH, el hash creado no incluye los campos del encabezado del paquete. Esto permite al nodo GGSN modificar el encabezado IP original sin experimentar fallas de integridad con IPSec.

Cuando TCP se involucra en la transmisión de datos, entonces se origina un problema de incompatibilidad entre TCP y NAT. Porque NAT modifica el paquete TCP, este debe además recalcular el checksum utilizado para verificar la integridad. Si NAT actualiza el checksum del paquete TCP, entonces la autenticación ESP fallará. Si NAT no actualiza el checksum, la verificación TCP fallará. Por consiguiente, el checksum del paquete TCP debería ser desactivado. En otras palabras ESP puede pasar a través de NAT en modo transporte con los campos checksum de los paquetes TCP deshabilitados o ignorados por el receptor. Esto es mejor que nada, ya que el tráfico IPSec es autenticado y protegido en su integridad usando una encriptación fuerte, las modificaciones al paquete pueden ser detectadas antes del chequeo de los campos checksum de TCP. Así que la verificación del checksum sólo proporciona aseguramiento contra errores cometidos en el proceso interno.

Otra solución al problema de incompatibilidad podría ser el uso de encapsulación UDP. En este esquema, los paquetes son encapsulados en UDP antes de que sean enviados. El receptor descarta el encabezado IP y la encapsulación UDP pasando por alto algunos cambios que pudieron haber sido hechos por NAT.

Más allá de las soluciones mencionadas, la IETF está definiendo una alternativa para NAT llamada Realm-Specific IP (RSIP) [8, 9] que puede ser más amistosa con IPSec.

Con RSIP, el payload de IP fluye desde la fuente al destino sin modificaciones que puedan perjudicar a IPSec. Para lograr esto, el host encapsula el paquete original con

direccionamiento privado en un paquete exterior. Esta encapsulación puede ser realizada utilizando cualquier protocolo estándar de “tunneling”. Al recibir el paquete, el enrutador RSIP, desencapsula el paquete y lo enruta a través de la red pública hacia el destino que enlaza a la red privada con Internet.

Finalmente, a cerca de la incompatibilidad entre los identificadores de dirección IKE y NAT, el escenario propuesto de VPN emplea IKE en AM porque este utiliza identificación de datos en vez de direcciones IP para la autenticación en el nodo final. El mismo método de autenticación también debería ser utilizado durante el modo rápido (quick mode) de la negociación IKE, para eliminar los problemas de incompatibilidad entre el direccionamiento de IKE y NAT.

5.1.3.3 Implicaciones de la movilidad

El usuario puede moverse libremente dentro del área de cobertura de la red GPRS, manteniendo conectividad a la red y provisión del servicio VPN. La tarea principal de la gestión de la ubicación es guardar huella de la ubicación actual del usuario, así los paquetes que llegan pueden ser enrutados a su dispositivo móvil (MS).

Cuando la MS se mueve a un área de enrutamiento (RA), esta es asignada al mismo SGSN, este ya ha almacenado el perfil de usuario necesario y asigna un nuevo paquete temporal con la identidad del suscriptor móvil (P-TMSI) al usuario.

Desde que el contexto de enrutamiento no cambie, la VPN entre la MS y el SG permanece igual.

En caso de que una nueva área de enrutamiento (RA) esté administrada por un SGSN diferente al anterior, el nuevo SGSN entiende que la MS ha cambiado a su RA y requiere que el anterior envíe el contexto PDP del usuario. Después, el nuevo SGSN informa al GGSN involucrado, el HLR y opcionalmente el MSC/VLR sobre el nuevo contexto de enrutamiento del usuario. Sin embargo, la VPN opera sobre la capa 3 y ninguno de los parámetros de seguridad, que están contenidos dentro de la asociación de seguridad de IPSec, ha sido cambiado.

Por consiguiente, la VPN opera transparentemente sin tener en cuenta el movimiento de la MS y los procedimientos de GMM (GPRS Mobility Management).

5.2. Escenario basado en red

5.2.1 Arquitectura de una MVPN sobre GPRS

5.2.1.1 Arquitectura

El escenario se desarrolla para un usuario que intenta establecer una conexión remota y segura a una LAN corporativa accediendo a través de una infraestructura GPRS como se

presenta en la Figura 10.

La red estándar GPRS no ofrece por si sola una solución adecuada para el objetivo propuesto, a pesar de que el cifrado de la interfaz de aire que se extiende hasta el SGSN es seguro en el escenario básico, el tráfico IP viaja desencriptado desde el SGSN hasta el SG. El backbone de la red GPRS utiliza además un firewall y direccionamiento IP privado para restringir el acceso no autorizado a ella.

Para establecer un intercambio seguro entre la MS y el servidor remoto, se realiza una VPN sobre la red pública Internet. Para el establecimiento de ésta, se utiliza un modelo iniciado por el cliente, que satisface muy bien a los usuarios móviles.

Se asume que el GGSN y el SG utilizan NAT.

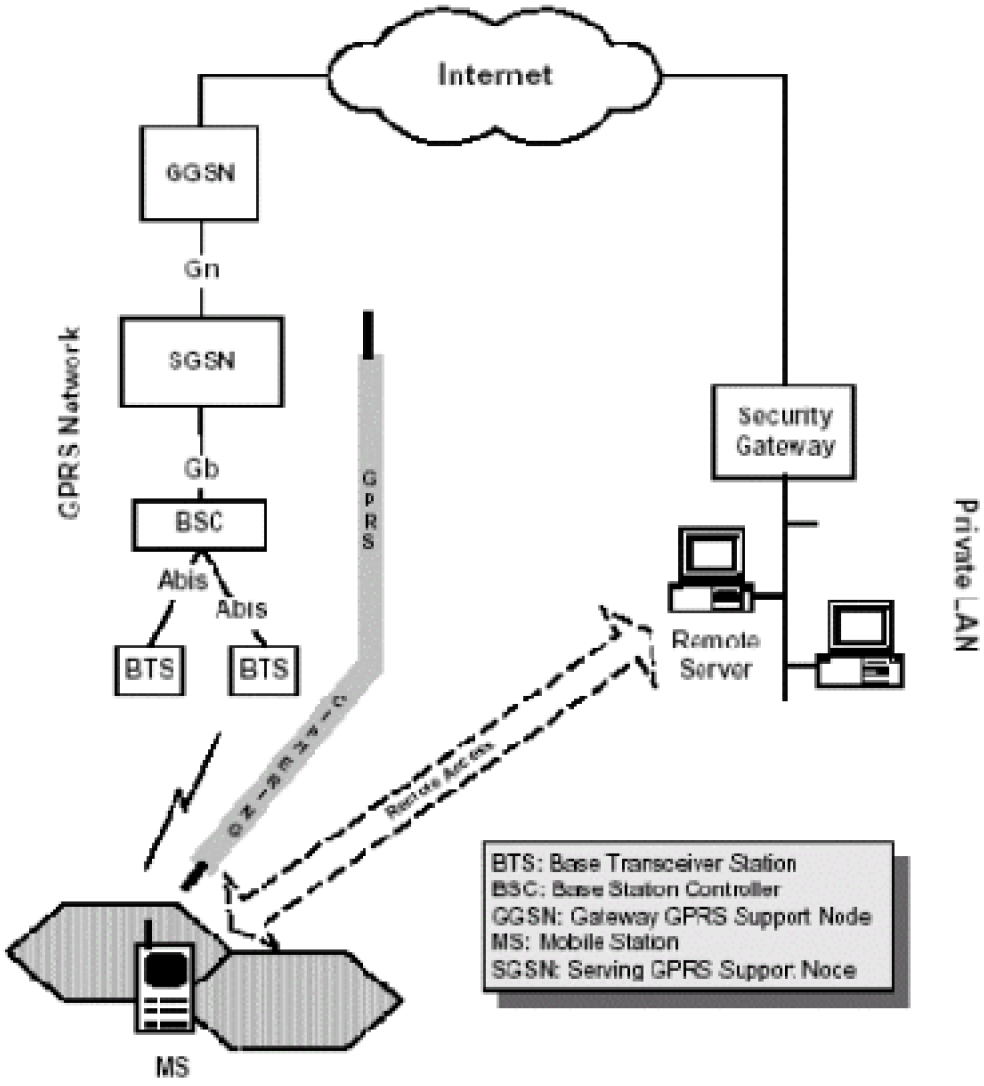

Figura 14. Arquitectura de red

5.2.1.2 Mejoras a la red GPRS

La propuesta para el desarrollo de una VPN basada en red, coloca la funcionalidad de IPSec tanto en la MS como en el GGSN, y en consecuencia, requiere de unas mejoras a la infraestructura existente como se ilustra en la Figura 11

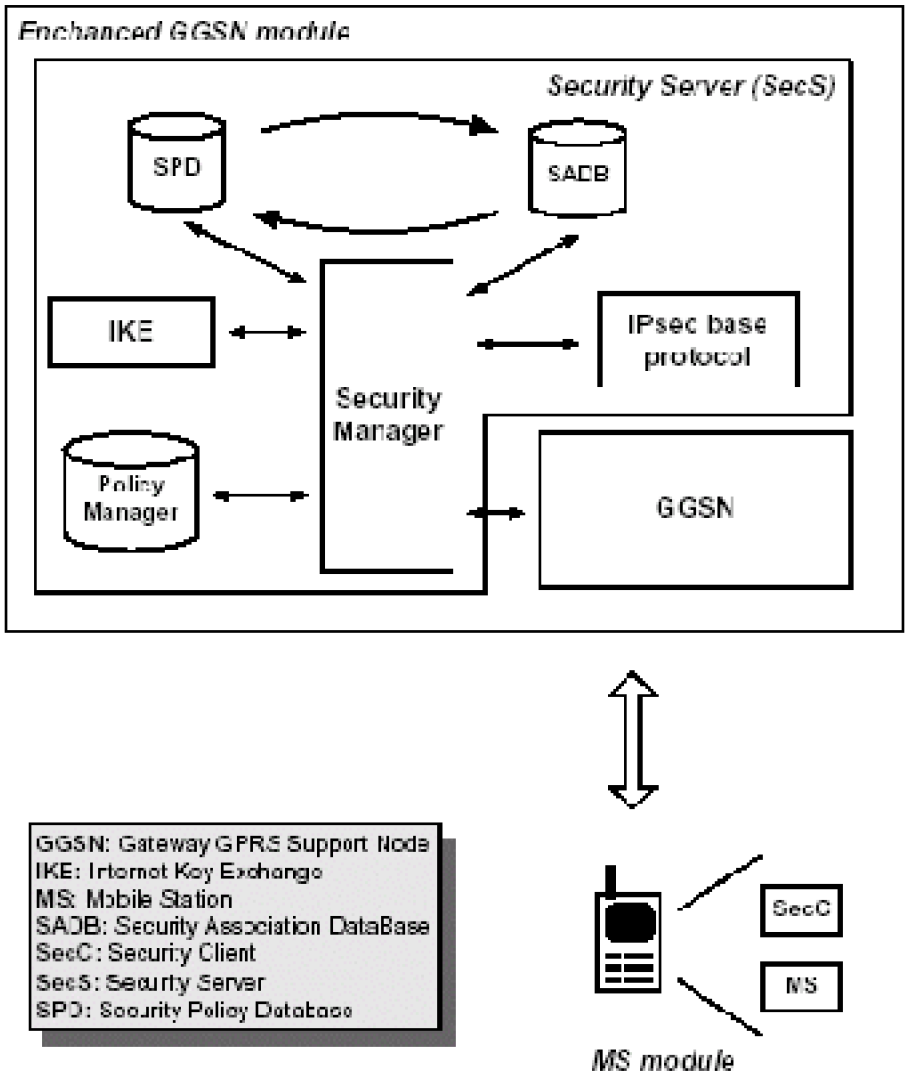

Figura 15. Mejoras a la red GPRS

El dispositivo móvil MS debe ser mejorado con un módulo de seguridad cliente (SecC), el cual es utilizado para realizar peticiones de servicios a la VPN y definir las preferencias de usuario

El GGSN debe incorporar un módulo Servidor de Seguridad (SecS), que establece, maneja y controla la VPN entre el GGSN y el SG al Intranet corporativo a favor del usuario móvil.

SecS comprende la implementación de un framework modificado para adaptar el esquema de VPN iniciada por el cliente y la provisión de un servicio de seguridad en un ambiente móvil GPRS. El principal componente funcional del SecS es el Administrador de seguridad (SM – Security Manager), el cual juega un papel central ya que permite la

administración de submódulos del SecS y facilita la configuración de la VPN. El SM mantiene las políticas de seguridad de las bases de datos, maneja las peticiones de los usuarios y reporta errores.

IKE autentica pares IPSec, negocia servicios de seguridad y genera claves compartidas dinámicamente. Este provee determinación de clave segura a través del intercambio Diffie – Hellman.

El administrador de políticas (PM – Policy Manager) contiene las políticas de seguridad de la red, que especifican el grupo de usuarios permitidos para tener servicios de seguridad y el tipo de servicios permitidos. Este se comunica con el HLR para conseguir el perfil de los usuarios. Los contenidos del PM son utilizados para configurar la base de datos de políticas de seguridad (SPD), y la base de datos de Asociaciones de Seguridad (SADB).

SPD es la base de datos de las políticas primarias, utilizada por el SecS para decidir sobre el manejo de tráfico en la red, tal como encriptación, desencriptación, autenticación, descarte, aceptación y modificación. SPD contiene una lista ordenada con las entradas de las políticas, cada una de las cuales define un grupo de trafico IP abarcado por esta entrada de la política y es identificado por uno o más selectores. El SM es responsable de llenar los contenidos de esta base de datos y compartirlos con otros submódulos SecS.

La SADB mantiene los contenidos de todas las asociaciones de seguridad activas utilizadas por el SecS para el formato de IPSec. El SM es el responsable de llenar el contenido de cada entrada en la SADB.

El protocolo IPSec procesa la autenticación y la encriptación definidas en el framework IPSec. Este maneja todas las funciones en la capa de red tales como fragmentación y máxima unidad de transferencia. Y asegura que el tráfico que pasa a través de la red GGSN es seguro y autorizado, proporcionando capacidades de firewall.

5.2.1.3 Gestión de la seguridad

Cuando un usuario móvil desea establecer una conexión remota segura a través del SG, usa el SecC para solicitar una SA IPSec del SecC de la empresa. El SecC se encarga de negociar la SA IPSec usando el protocolo IKE en uno de los lados del SecC.

Durante la fase I se realiza una negociación SA ISAKPM en modo agresivo. El AM de la negociación IKE es una opción que se puede definir para aumentar la velocidad de la transacción IKE sacrificando ligeramente la seguridad. Además, el método utilizado en AM no toca la dirección IP del iniciador. De este modo, el protocolo IKE está operando en un esquema basado en proxy, donde la VPN no se establece directamente por el iniciador, y en un ambiente de red móvil donde se puede estarse usando direccionamiento IP dinámico.

El mecanismo de autenticación de los extremos de la VPN está basado en el método de clave compartida, ya que es considerado como la forma más simple de autenticación, comparado con las firmas digitales de clave pública y métodos de encriptación de la autenticación, y encaja mejor en el escenario de una VPN móvil basada en red. La autenticación se basa en el campo ID (Identification Data) que es estático, en lugar de la

dirección IP que puede variar.

Para iniciar la negociación de la SA IPSec, el SecC dirige un mensaje al SecC que incluye la dirección IP del SG remoto, la solicitud de la SA IPSec (SAMS), la clave pre – compartida y los datos de identificación del suscriptor móvil. Una vez recibe el mensaje, el SecC verifica los privilegios del suscriptor móvil y las capacidades de la red móvil para proporcionar servicios VPN preguntándole al PM. Adicionalmente el SecC busca una SA ISAKMP entre el SecC y el SG a nombre de un usuario particular. Si dicha SA existe, el SecC procede con la fase 2. Si no, el SecC primero genera una cookie (CSecC), la mitad de la clave Diffie- Hellman (DH), la hora actual (NSecC), y luego, las envía juntas con los datos de la SA ISAKMP (ISASecC) y los datos de identificación de la estación (IDMS) hacia el SG (mensaje 2). El SG contesta con un mensaje 3, el cual contiene un par para la cookie, al igual que la respuesta de la SA ISAKMP, la mitad de la clave Diffie-Hellman, la hora actual, su identificación y el HASHSG, el cual contiene la información de la autenticación del SG. Finalmente, el SecC transmite un mensaje 4 con la información de autenticación de la MS (HASHMS) hacia el SG junto con un par para la cookie. Teniendo establecida la SA ISAKMP entre el SecC y el SG, a nombre de la MS, las partes han acordado:

- El algoritmo de encriptación.
- El algoritmo hash para señalización.
- El método de autenticación para señalización.
- El intercambio Diffie- Hellman

Después de haber completado la fase 1, se lleva a cabo la fase 2 IKE para establecer la SA IPSec (Ver figura 8). Todos los paquetes pertenecientes a la fase 2 son enripiados usando la SA ISAKMP preestablecida. En el mensaje 1, la SecS transmite la cookie al SG (CSecS, CSG), la solicitud de la SA IPSec (SAMS), su hora actual (NSecS), la mitad de la clave Diffie Hellman y la identidad del MS y el SG (IDMS, IDSG) respectivamente. Adicionalmente, la SecS autentica el mensaje con una función hash.

En el mensaje 2 el SG transmite la cookie, su SA IPSec de respuesta, su hora actual, la mitad de la clave Diffie-Hellman, y las identidades de la MS y el SG. El SG también autentica el mensaje con una función Hash.

En el mensaje 3, la SecS responde con un par para la cookie y autentica la transacción con una función Hash.

Para finalizar este diálogo, la SecS envía un mensaje 4 informando al SecS sobre el éxito de la creación de la SA IPSec. Como una SA IPSec se una en una sola dirección, para establecer una comunicación bidireccional entre el SecS y el SG se requieren dos SAs.

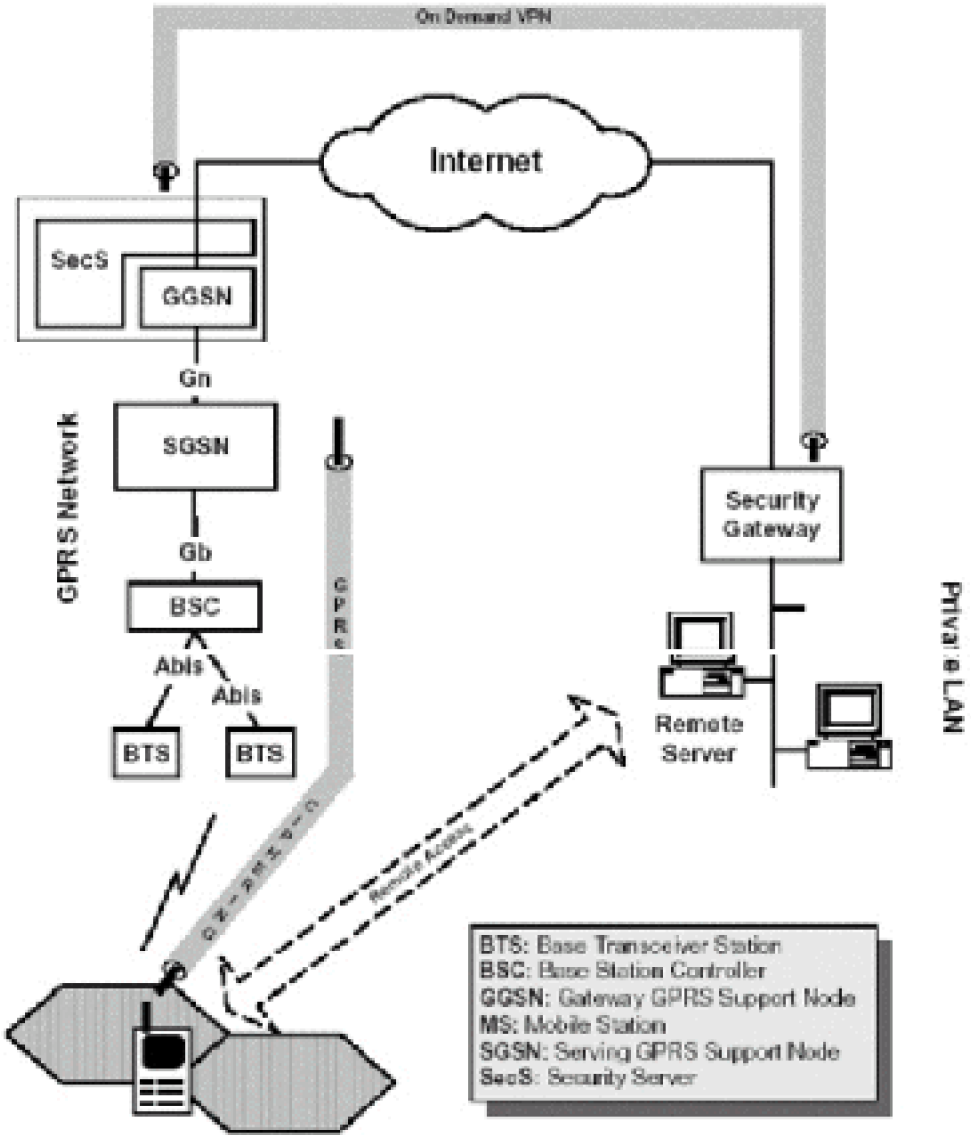

Figura 16. Esquema de la VPN basada en red

5.2.2 Operación de la VPN

Habiendo establecido un par de Asociaciones de Seguridad (SA's) entre el SecS y el SG, se ha iniciado un canal bidireccional privado que permite intercambio seguro de datos sobre la red pública Internet. El protocolo IPSec es configurado en modo túnel en los dos puntos finales de la comunicación, el GGSN y el SG, en este escenario particular ambos son Enrutadores. Además el empleo del protocolo ESP es considerado de gran ventaja en esta arquitectura, dado que puede proporcionar confidencialidad y protección a la integridad de los datos.

Cada paquete que sale está sujeto a ser procesado por el protocolo IPSec, que determina si aplicará protección de IPSec o no. Además el protocolo IPSec asegura que el datagrama IP está autorizado para pasar o si debe ser rechazado, a través de los servicios de firewall. Para decidir qué servicio será permitido, el IPSec interactúa con el

SPD. El procesamiento de salida en el SPD compara los valores de los campos selectores contra el SPD para buscar una entrada igual en el SPD. En efecto, estos selectores son usados para filtrar el tráfico de salida con el fin de mapearlo en una SA particular. Cada SA tiene una entrada en la SADB que define los parámetros de seguridad asociados a ella. Note que si una entrada SPD no está apuntando a una SA activa, entonces el SecS la crea y la enlaza con una entrada en el SPD.

En caso de que se esté aplicando procesamiento IPSec, el paquete IP original es encriptado y autenticado. El modo túnel permite encriptación y autenticación de los protocolos de las capas superiores (por ejemplo los segmentos TCP) incluyendo el encabezado original IP.

Para tráfico de entrada, antes de realizar cualquier procesamiento IPSec, se reensamblan los fragmentos IP. Cada datagrama IPSec protegido es identificado por la aparición del valor ESP en el campo “next protocol” de IP. Con el fin de determinar la SA de IPSec que se ha de aplicar, se debe buscar en la SADB. Si la búsqueda de la SA falla, entonces el paquete es eliminado y se reporta error. De lo contrario, si se encuentra la SA, el protocolo IPSec realiza el procesamiento (desencapsula, autentica y desencripta el paquete). Luego, el hace coincidir los selectores de los paquetes internos con aquellos contenidos dentro de la SA, y encuentra la política de entrada contenida en el SPD. Finalmente, este chequea si se ha aplicado el procesamiento IPSec requerido y reenvía el paquete original IP a su destino.

5.2.3 Implicaciones de la movilidad

La MS puede moverse libremente dentro del área de cobertura de GPRS, manteniendo la conectividad a la red, gracias a los procedimientos de administración de movilidad. Con tal de que el MS permanezca bajo el mismo GGSN, su movimiento no tiene impacto en el desarrollo del la VPN basada en red. De lo contrario, la VPN no puede ser utilizada, y deberá establecerse otra VPN desde el nuevo GGSN. . Esto sólo ocurre en el escenario de VPN basada en red, en el escenario end – to – end, la gestión de la movilidad es distinto, ver sección 5.1.3.3

6. ESCENARIO DE EVALUACIÓN VPN SOBRE GPRS

6.1 Características de un dispositivo móvil

Las siguientes son las restricciones que tiene un dispositivo móvil y que deben tenerse en cuenta en el esquema de VPN sobre GPRS:

- Bajo poder de procesamiento de CPU
- Potencia limitada de la batería
- Capacidad limitada de memoria
- Ancho de banda
- Pequeño tamaño de la pantalla
- Capacidad de entrada limitada
- Restricciones de sistema operativo

A continuación se presentan las ventajas y desventajas de dos de los posibles escenarios de VPN sobre GPRS, ya que estos son los más comúnmente utilizados.

6.2 Ventajas del escenario GPRS basado en red

La ventaja principal del esquema de seguridad propuesto tiene que ver con el hecho de que un suscriptor móvil inicia el establecimiento de una VPN entre el GGSN y el SG de la LAN corporativa, utilizando una funcionalidad de negociación de claves compleja, encriptación y desencriptación externa a la funcionalidad de la infraestructura de la red móvil. Los servicios VPN dinámicos iniciados por los clientes son adecuados para los usuarios móviles que requieren acceso a redes remotas, desde cualquier lugar, en cualquier momento. Los usuarios finales deciden cuando y desde donde establecer una VPN haciendo uso de la infraestructura vulnerable de una red pública protegiendo la transferencia de datos sensibles.

Además, el esquema de seguridad propuesto es compatible con la opción de intercepción legal, la cual requiere acceso a los datos que atraviesan la red móvil.

Un objetivo adicional es minimizar el costo de configuración y computacional de los dispositivos móviles, comparado con el esquema convencional entre usuarios finales. Más específicamente, el uso de IPSec impone costo computacional al host que implementa dicho protocolo. Estos costos se encuentran asociados con la memoria requerida para el código y las estructuras de datos IPSec, el número de mensajes que se intercambian en la negociación de la seguridad, y el cómputo de verificación de la integridad, encriptación y desencriptación, los cuales son adicionales en el modo por paquetes [10]. Considerando las restricciones impuestas por la naturaleza del dispositivo móvil (baja capacidad de procesamiento de la CPU, potencia de batería limitada, y capacidad limitada de memoria), con el esquema propuesto los suscriptores móviles pueden tomar ventajas significativas dejando la operación y administración de las VPNs a los operadores de la red móvil. Los operadores de la red tienen una experiencia sólida en la administración y mejores recursos para crear, ofrecer y administrar servicios VPN que se originen desde el suscriptor móvil. Ellos pueden ofrecer servicios de seguridad a un menor costo, consolidando los servicios sobre una infraestructura común. Esto permite la utilización de módulos de hardware aceleradores para ganar velocidad y un uso más eficiente de la implementación de IPSec. Además, la implementación basada en red puede evolucionar continuamente para atender los nuevos requerimientos de los usuarios finales, y permite a los operadores de la red desarrollar estrategias de seguridad integradas.

Las adiciones requeridas por la red para proveer servicios de seguridad pueden ser integradas en el GGSN existente, soportando la funcionalidad de la red GPRS existente. La VPN basada en red opera de manera transparente con respeto a la administración de la red GPRS, la gestión de la movilidad y funciones de enrutamiento, y posteriormente, puede ser usada como una característica adicional del estándar GPRS. Al proporcionar una iniciación dinámica de los servicios de VPN basados en red, el operador de la red móvil tiene la oportunidad de atraer nuevos usuarios. Reducir el costo de operación y mantenimiento permite servicios VPN rápidos y efectivos, y elimina la necesidad de

conocimiento técnico especializado del lado del usuario final. La estación final simplemente inicia el establecimiento de la VPN, y no es necesario realizar tareas de seguridad del lado del usuario. Generalmente, en este escenario, la configuración de la SA es transparente al usuario móvil.

Adicionalmente, GPRS utiliza procedimientos específicos de cifrado y autenticación, los cuales son optimizados para transmisión de paquetes de datos sobre la interfaz de radio, entre el MS y el SGSN. Por otro lado, a diferencia del escenario entre usuarios finales, este esquema utiliza servicios de seguridad proporcionados por el estándar GPRS, y permite la aplicación de la encriptación duplicada (encapsulación de paquetes) sobre la costosa y escasa interfaz de radio.

Además, el montaje de una VPN basada en red, no tiene un impacto negativo en la eficiencia del acceso a los recursos de radio, ya que este esquema utiliza el estándar de GPRS (autenticación y procedimientos de cifrado, los cuales están optimizados para transmisión de datos sobre interfaz de radio).

Finalmente, comparado con el esquema estático soportado actualmente por GPRS, este esquema permite prestar servicios VPN por demanda, los cuales están disponibles para todo un conjunto de suscriptores móviles. Esto también es compatible con los firewall de frontera de la red, los cuales son responsables del filtrado de paquetes, control de acceso, y NAT. El uso de NAT no tiene impacto en la operación de la VPN, debido a que el IPSec está localizado en el espacio público de direcciones, y de esta manera la combinación de IPSec con NAT es posible sin problemas de compatibilidad [11].

6.3 Desventajas del escenario GPRS basado en red

La consideración más grande en el esquema propuesto es que el establecimiento de la VPN y su operación no están directamente bajo el control del usuario final. Este esquema de seguridad que ya se usa en las redes terrestres alambradas, asume que los suscriptores móviles corporativos, confían en el operador de la red móvil.

En orden a proporcionar servicios VPN efectivamente, la infraestructura de red GRPS existente debe ser ampliada. Específicamente, la MS requiere la introducción del módulo liviano SecC que inicia el establecimiento de la VPN y expresa las preferencias del usuario final. Además, el GGSN requiere la incorporación del SecS, el cual es responsable para el establecimiento y operación de la VPN. Sin embargo, las mejoras que hacen referencia al core de la red GPRS, requieren una inversión del operador móvil, y con esta funcionalidad se espera que aumente la señalización y la carga de trabajo en la red.

Finalmente, cuando una MS se mueve a una nueva área de enrutamiento, la cual es asignada a un nuevo GGSN, la VPN basada en red que ha sido establecida por el anterior GGSN, no es operacional ya. En este caso, la MS tiene que iniciar el establecimiento de una nueva VPN desde el nuevo GGSN.

6.4 Ventajas del escenario VPN sobre GPRS End – to – End

Desde el punto de vista de los usuarios, las conexiones VPN end – to – end proporcionan la mejor seguridad. El tráfico es encriptado en el cliente VPN y desencriptado en el SG de la red corporativa, así, el tráfico permanece encriptado durante toda la conexión. La autenticación está en manos de los suscriptores móviles.

Las mejoras de seguridad requeridas tienen un mínimo impacto sobre la infraestructura de red existente. Más específicamente, los nodos SGSN y GGSN de la red GPRS y los enrutadores IP intermediarios no requieren mejoras adicionales o modificaciones que soporten este escenario de VPN específico. Los cambios necesarios están limitados a la seguridad de los puntos finales (MS y SG). Por consiguiente, esta configuración no adiciona carga de datos de señalización sobre la red móvil.

El suscriptor móvil puede acceder a Internet desde cualquier GGSN disponible, y hasta ahora, puede seleccionar el acceso más barato. Además, el flujo de tráfico de usuario es encriptado todo el camino desde la MS hasta el SG, lo que significa que este es cargado como tráfico de datos normal.

Adicionalmente, cualquier restricción de flujo es impuesta al tráfico encriptado. Todo el tráfico que tiene servicios de seguridad aplicados, pasa a través de la seguridad de los dos puntos finales, sin tener en cuenta las rutas intermedias que pueden seguir. Esto permite que el tráfico encriptado sea tratado de acuerdo con las políticas de red, como los mecanismos de enrutamiento para evitar la congestión, sin afectar los procesos de encriptación.

Finalmente, como una consecuencia de la transparencia de la operación de una VPN sobre una red móvil, los mecanismos tales como el GTP y el GMM no causan ningún problema de incompatibilidad.

6.5 Desventajas del escenario VPN sobre GPRS End – to – End

La principal desventaja del esquema de VPN propuesto, deriva del hecho de que cada dispositivo móvil debe tener el software apropiado (IPSec) para aplicar la política de seguridad requerida.

El uso de IPSec impone costos computacionales en los hosts que implementan estos protocolos. Estos costos están relacionados con la memoria necesaria para la codificación IPSec y las estructuras de datos, y el chequeo de la integridad de valores en la computación, encriptación y desencriptación. Considerando las restricciones antes

mencionadas, impuestas por la naturaleza de los dispositivos móviles (Baja capacidad de procesamiento, capacidad de batería limitada y capacidad de memoria limitada), puede percibirse que la integración de IPSec en la MS es un poco complicada. La sobrecarga computacional de aplicar IPSec a la MS será manifestada por el incremento de la latencia [6] , y posiblemente, por la reducción del rendimiento.

Otro problema esencial es que el usuario debe estar consciente de cuándo se requiere encriptación. El software de la estación final puede necesitar que el usuario tome decisiones y configure la política de seguridad apropiada. Generalmente, en este escenario la configuración de la SA puede no ser transparente para el suscriptor móvil.

El uso de IPSec además impone costos de utilización de ancho de banda en la transmisión de datos debido al aumento en el tamaño del paquete desde la adición de los encabezados ESP. [1]. Se prevé que el incremento de la demanda de ancho de banda no afectará notablemente la infraestructura de Internet, sin embargo, esto tendrá una influencia significativa sobre la interfaz de radio. Además, GPRS emplea autenticación específica y procedimientos de cifrado, los cuales son optimizados para la transmisión de paquetes de datos sobre la interfaz de radio, entre la MS y el SGSN. Por consiguiente el esquema VPN fina a fin propuesto duplica la encriptación (encapsulación de paquetes) sobre la costosa interfaz de radio, el cual incrementa el costo de la comunicación y disminuye la eficiencia de los accesos a la red.

Finalmente, el escenario end – to – end tiende a causar problemas cuando se utiliza NAT, que es el caso en la mayoría de la VPN's de acceso remoto. Las soluciones tradicionales con IPSec no permitirán NAT por algunas razones mencionadas en la sección 5.

[6] Latencia es una expresión que expresa cuanto tiempo tarda un paquete de datos en salir de un punto de la red y llegar a otro

7. COMPARACIÓN DE LOS ESCENARIOS END – TO – END Y BASADO EN RED Y CONCLUSIONES

- Se puede concluir que, cuando la seguridad es la preocupación principal, la solución VPN end-to-end VPN es una buena opción.
- Una solución alternativa a la VPN end – to – end podría ser una VPN basada en red. Bajo este acercamiento, la funcionalidad de la VPN es delegada a los nodos GSN y por consiguiente las desventajas del esquema VPN end – to –end pueden confinarse. Sin embargo la VPN basada en red pone la funcionalidad de IPSec dentro del core GPRS de la red, y así, introduce una carga extensa en él. Adicionalmente, la consideración más grande es que el funcionamiento de la VPN no está directamente bajo el control del usuario final.
- De todo lo visto, se puede deducir que ambos, el esquema end – to – end y el esquema basado en red, soportan el desarrollo de una VPN dinámica iniciada por el cliente. Sin embargo el esquema end – to – end proporciona los mejores servicios de seguridad desde el punto de vista del cliente, minimiza las mejoras que requieren hacerse en la red, así como la carga de señalización, y no exige a los interesados en la comunicación, confiar en el operador de la red móvil. Por otra parte, el esquema basado en red, minimiza el envolvimiento del usuario móvil y su terminal en el

desarrollo de la VPN, no tiene impacto en los escasos recursos de radio, es compatible con la presencia de NAT y la opción de intercepción legal, y finalmente, proporciona servicios de seguridad más eficientes a más bajo costo.

- Con respecto al esquema de VPN basado en red. Confiando en una secuencia de mecanismos de protección concatenados (Cifrado GPRS y desarrollo de la VPN), es posible proporcionar acceso remoto seguro a los usuarios móviles, sin necesidad de un túnel extra que sobre cargue el enlace de radio o la implementación de intensos algoritmos de encriptación en la MS. El desarrollo de la VPN está basado en el framework de seguridad IPSec, el cual facilita servicios de seguridad transparentes a cualquier aplicación que utilice la red. Para la inicialización de la VPN y los procedimientos para convenir claves, se propone un esquema de proxy con el protocolo IKE, el cual permite a los usuarios móviles iniciar una VPN, mientras desplaza la negociación compleja de claves a la infraestructura de red. De esta forma, los servicios por demanda de la VPN, están disponibles para todos los suscriptores GPRS y usuarios que se encuentren en la red. Las mejoras necesarias para proporcionar los servicios de seguridad pueden ser integradas en la infraestructura de red existente, y por lo tanto, el esquema de seguridad propuesto puede ser utilizado como una característica adicional de GPRS.

Tabla 5. Comparación entre esquemas end to end y basado en red

Característica	end to end	Basado en red
Servicios de VPN dinámica iniciada por el cliente	□	
Seguridad end – to – end	□	
Minimiza mejoras sobre la red	□	
No exige confianza de terceros en el operador	□	
Compatibilidad con intercepción legal		□
Minimiza el impacto en la MS		□
Configuración transparente de la SA para el usuario final		□
No tiene impacto en los recursos de radio		□
Compatible con NAT		□
Bajo costo de la VPN		□

BIBLIOGRAFÍA

[1] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, Nov. 1998.

[2] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409, Nov 1998.

[3] C. Xenakis, E. Gazis and L. Merakos, “Secure VPN Deployment in GPRS Mobile Networks”, 2002.

[4] C. Perkins, “IP Encapsulation within IP” RFC 2003, Mayo 1996

[5] Phifer, L., "IP Security and NAT: Oil and Water?" ISP-Planet, Junio 15, 2000 Disponible desde http://www.isp-planet.com/technology/nat_ipsec.html

[6] Bernard Adoba, “IPSec-NAT, Compatibility Requirements” Internet Draft (work in progress) draft-ietf-ipsec-nat-reqts-00.txt, Junio 2001.

[7] Nicolas Gabriel, “VPN and Firewall Traversal”, Nov. 2000.

[8] Phifer, L., "Realm-Specific IP for VPNs and Beyond" ISP-Planet, June 23, 2000 available from http://www.isp-planet.com/technology/rsip.html

[9] Borella M., Grabelsky D., Lo J., Taniguchi K., Realm-Specific IP:Protocol Specification“ Internet Draft (work in progress) draft-ietf-nat-rsipprotocol-07.txt, Julio 2000.

[10] GSM 03.60, GPRS, Service Description, 1998.

[11] L. Phifer, “The Trouble with NAT”, Cisco publications, The Internet Protocol Journal, Vol. 4, Dec. 2000.

[12] C. Xenakis and L. Merakos, “DYNAMIC NETWORK-BASED SECURE VPN DEPLOYMENT IN GPRS”, 2002.

[13] R. Kopeikin and S. Sommars,” Wireless GPRS Access to Virtual Private Networks For Carriers and ESPs”, 2000

[14] S. Aust, D. Proetel, A. Könsgen, C. Pampu and C. Görg, “Design Issues of Mobile IP Handoffs between General Packet Radio Service (GPRS) Networks and Wireless LAN (WLAN) Systems” , 2002.

[15] Dung Chang, “Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services”, Enero 2002.

[16] Georgios Karagiannis, “QoS in GPRS”, Diciembre 2000.

[17] NetScreen Technologies Inc, “GPRS Security Threats and Solutions”, Marzo 2002.

[18] C. Bettstetter, H. Vögel, and J. Eberspächer, Technische Universität München. GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols, and Air Interface. 1999

[19] Peter Schefczik. Performance Simulation for the General Packet Radio Service, GPRS. Lucent Technologies/Global Wireless Systems Research. Germany

[20] Iñigo Sedano . Tutorial de GPRS. Junio 203

[21] John Scourias. University of Waterloo. Overview of GSM: the Global System for Mobile Communications. Marzo 1996

[22] N. Ferguson and B. Schneier. A cryptographic evaluation of IPsec. Enero 2000. Disponible en: http://www.counterpane.com/ipsec.html