ESCUELA POLITECNICA DEL EJERCITO

FACULTAD DE INGENIERIA ELECTRONICA

PROYECTO DE GRADO PARA LA OBTENCION DEL TITULO EN INGENIERIA ELECTRONICA

"SERVICIOS Y SOLUCIONES QUE BRINDA EL PROTOCOLO DE INTERNET MOVIL (MOBILE IP) EN REDES DE TERCERA GENERACION"

FRANCISCO DAVID CHANG BALDEON

SANGOLQUI – ECUADOR

ABRIL 2005

CERTIFICACION

Certificamos que el presente proyecto de grado titulado “Servicios y soluciones que brinda el Protocolo de Internet Móvil (Mobile IP) en redes de Tercera Generación” ha sido desarrollado en su totalidad por el Sr. Francisco David Chang Baldeón con C.I: 060289684-7, bajo nuestra dirección.

Ing. Fabián Sáenz
DIRECTOR

Ing. Flavio Pineda
CODIRECTOR

AGRADECIMIENTO

Doy gracias....

A Dios
Por haberme dado la vida.

A mis Padres
Por haberme enseñado a vivirla correctamente.

A mis profesores
Por su guía siempre oportuna.

DEDICATORIA

Dedico este mi trabajo final de Tesis a Dios el Creador Supremo y Arquitecto del Cosmos, por caminar junto a mi en todos los momentos a lo largo de este camino que hoy no concluye sino que cambia de rumbo.

A mis Padres, por ser los cimientos de quien ahora soy, por su apoyo incondicional y su ejemplo de dedicación y esmero. Por haber sido mi guía y mi consuelo en las horas de debilidad.

A mi familia y mis amigos, por brindarme su apoyo y afecto. A mis compañeros y profesores a lo largo de esta carrera, por sus acertados criterios y enseñanzas.

PROLOGO

En los últimos años las comunicaciones móviles han tenido un gran despliegue tecnológico, cada día existen en el mercado más requerimientos relacionados con Internet Móvil por parte de empresas y personas y por ende más aplicaciones y servicios brindados a través de operadoras celulares en todo el mundo.

Actualmente la movilidad en Internet brindada a través de un terminal móvil como es un teléfono celular es lo que muchas empresas y las personas en general buscan. Es así, como surge la alternativa de realizar un estudio para mostrar las diferentes aplicaciones, servicios y soluciones que se brindan utilizando el Protocolo de Internet Móvil (Mobile IP) en redes de Tercera Generación como UMTS y CDMA2000.

A lo largo de este estudio se presenta una idea clara del actual desarrollo tecnológico, haciendo hincapié en el funcionamiento mismo del Protocolo Mobile IP y de cada uno de sus procedimientos. También se muestra la relación de Mobile IP con IPv4 e IPv6 recalcando la necesidad urgente de la adopción de la nueva versión del Protocolo de Internet para las ya actuales redes 3G y por consecuencia se hace un análisis completo de la versión Mobile IPv6 mostrando sus principales ventajas sobre Mobile IPv4. Se presenta además como Mobile IP se integra con nuevas tecnologías conocidas como de Tercera Generación como son GPRS, UMTS y CDMA2000, demostrando que este protocolo puede trabajar de manera eficiente en cualquier plataforma tecnológica.

Se concluye este trabajo con la presentación de una basta gama de servicios que ya están siendo utilizados en varios países del mundo, así como también diversas aplicaciones que hoy por hoy brinda Mobile IP en el campo de las comunicaciones móviles de ultima generación.

INDICE

CAPITULO I

INTRODUCCION

1.1 ANTECEDENTES

En los últimos años las comunicaciones móviles han tenido un gran despliegue tecnológico, cada día existen en el mercado más aplicaciones y servicios basados en Internet móvil los mismos que son requeridos de forma corporativa e individual para solucionar un sin numero de necesidades.

Como se ha mencionado, actualmente la movilidad en Internet es lo que muchas empresas y las personas en general buscan. Es así, como surge la alternativa de realizar un estudio cuyo objetivo es analizar y dar a conocer las soluciones y los servicios que brinda el protocolo de Internet Móvil o Mobile IP en redes de Tercera Generación, así como un análisis de su funcionalidad y su relación tanto con IPv4 e IPv6.

Con este estudio se intenta proporcionar una idea clara del actual desarrollo tecnológico, que ya está siendo utilizado en nuestro país y el mundo, y sus diversas aplicaciones en el campo de las comunicaciones móviles de última generación.

Como sabemos los protocolos actuales de internetworking (TCP/IP, IPX o AppleTalk) presentan serias complicaciones a la hora de tratar con nodos que presentan cierto grado de movilidad.

La mayoría de las variantes del protocolo IP asumen de manera implícita que el punto al cual se esta conectando un nodo es fijo. Por otro lado la dirección IP de un nodo lo identifica de manera única en la red en la que se encuentre conectado. Cualquier paquete que vaya destinado hacia ese nodo es encaminado en función de la información contenida en la IP del mismo que identifica la red en que esta conectado.

Con esto se deduce que si un nodo móvil se desplaza de una red a otra, manteniendo su dirección IP, no será localizable en su nueva ubicación ya que los paquetes dirigidos hacia ese nodo serán encaminados a su anterior punto de conexión.

Mediante el Protocolo “Mobile IP” se pretende dotar al nodo de cierta libertad para moverse libremente a través de Internet, estando siempre accesible mediante una dirección IP.

1.2 MOVILIDAD EN INTERNET

Actualmente se habla de Internet Móvil, esto pretende proporcionar un grado de movilidad a los diferentes nodos de una red.

Ante las posibles opciones propuestas para lograr la movilidad de los nodos, el IETF (Internet Engineering Task Force) estableció un grupo de trabajo para llegar a la solución, concretando varias metas consideradas deseables.

Las principales metas fueron las siguientes:

1. Todo host móvil debe ser capaz de usar su dirección IP base en cualquier lugar.
2. No se permiten cambios de software en los hosts fijos.
3. No se permiten cambios de software en el router ni en sus tablas.
4. La mayoría de los paquetes para los hosts móviles no deben desviarse en el camino.

5. No se debe incidir en carga extra cuando un host móvil este en su base.

1.3 TIPOS DE MOVILIDAD

Existen diferentes tipos de movilidad estos son:

Movilidad Nómada: No se encuentra activa mientras se está en movimiento.

Movilidad Celular: Se encuentra activa mientras se produce el movimiento.

Micro movilidad: Se presenta en áreas geográficas pequeñas en donde se presentan handoffs frecuentes y de manera rápida. Por ejemplo, entre puntos de acceso de una misma red WLAN.

Macro movilidad: Se presenta en áreas geográficas más grandes, en donde ocurren menos handoffs. Por ejemplo, entre subredes de una organización.

Movilidad Global: Ocurre entre zonas geográficas extensas o entre operadores. Por ejemplo, entre dos redes celulares compatibles entre si.

1.4 RETO DE LA MOVILIDAD EN INTERNET

El principal reto de la movilidad en Internet es mantener una conectividad IP mientras se cruzan los límites de una red local.

Esto es explicado de mejor forma en el siguiente gráfico, aquí se muestra un nodo móvil dentro de una red A, se aprecia que su dirección IP es 171.1.1.1, lo que se desea es pasar de la red A hacia la red D sin cambiar de dirección IP. Esto se lo puede lograr de distintas formas las cuales se presentan a continuación.

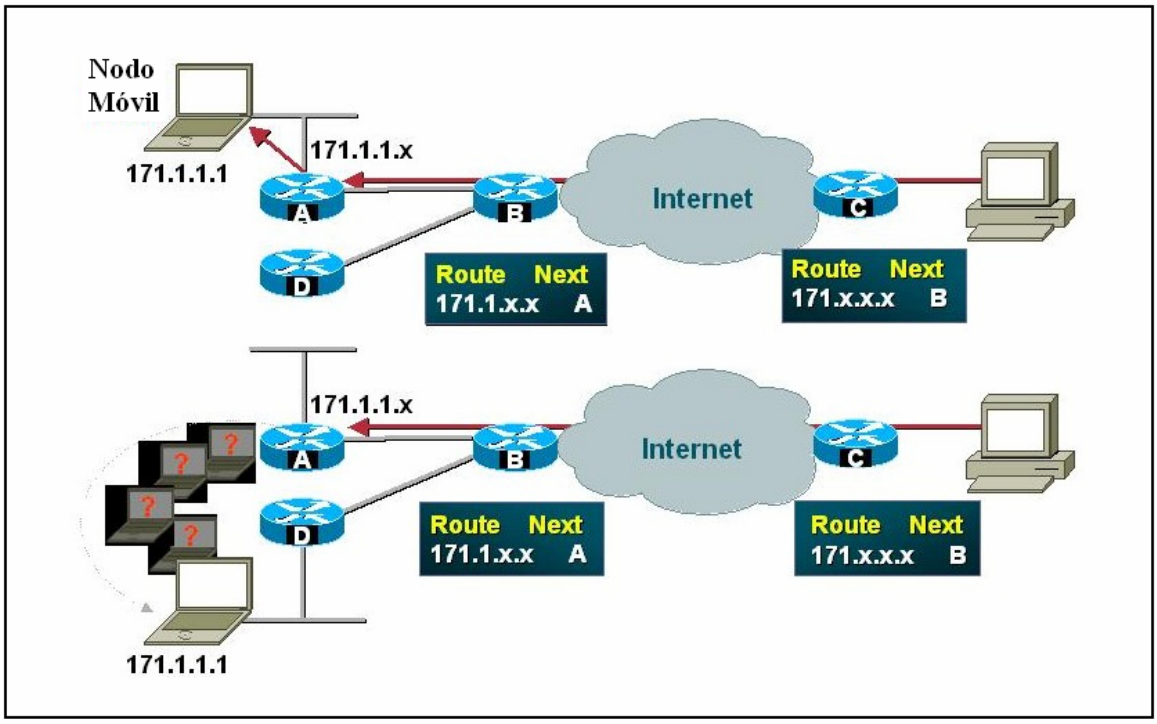

Figura 1. Reto de movilidad en Internet

1.5 SOLUCIONES PARA PROPORCIONAR MOVILIDAD A LAS ESTACIONES DE REDES IP

Para dotar de movilidad a un nodo de la red, aparecen diferentes alternativas algunas de las soluciones que se van a tratar son las siguientes:

- Establecimiento de rutas especificas para terminales con movilidad.
- Cambio de la dirección IP de los terminales y
- Soluciones basadas en realizar cambios a nivel de la capa de enlace.

1. Creación de rutas específicas para nodos con movilidad

La utilización de rutas específicas para los nodos a los cuales se quiere dotar de movilidad implica la reconfiguración de las tablas de enrutamiento de los dispositivos de interconexión de red o Routers para permitir contactar al host móvil en su nueva ubicación.

Esta solución es costosa ya que generaría un gran incremento de tráfico en la red para soportar la movilidad de los nodos. Ya que para ello seria necesario actualizar las tablas de encaminamiento como mínimo de todos los routers entre el enlace local y el nuevo punto de enlace.

Si tenemos en cuenta el número de posibles nodos móviles en una red y la velocidad con la que estos cambian de ubicación, estas actualizaciones de las tablas de enrutamiento podrían llegar a colapsar la red. De lo que se deduce que cuantas menos actualizaciones hagamos en los routers mejor, pero nos encontramos con que se limita las posibilidades de enrutamiento.

2. Cambio de direcciones IP

Consiste en asignar al nodo móvil una nueva dirección IP acorde con su nuevo punto de conexión a la red.

Esta solución no es muy recomendable ya que requiere que a la entrada en una nueva ubicación cambie su dirección IP. Si esta operación no se realiza de manera instantánea, cualquier consulta de la dirección IP del nodo puede ser errónea.

Por otro lado si tenemos en cuenta, como en el caso anterior, la velocidad con la que un nodo móvil puede cambiar su ubicación y por lo tanto su IP, se hará necesario un mecanismo para verificar la actualidad de la dirección IP devuelta por el servidor de nombres de dominio (DNS). El resultado es un gran número de consultas y actualizaciones que generan un alto nivel de trafico en la red.

3. Soluciones a nivel de la capa de enlace

Se va a exponer dos soluciones a nivel de la capa de enlace que pretenden permitir la movilidad de los nodos.

La primera de ellas se basa en el Cellular Digital Packet Data (CDPD), que se trata de un estándar diseñado para transmitir paquetes IP a través de los canales

de radio no utilizados por el servicio de voz en el sistema de telefonía celular norteamericano. El CDPD asigna a cada nodo móvil una dirección fija dentro de su área de cobertura.

La segunda solución se basa en el estándar de IEEE 802.11, realizado por el Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers) para la comunicación de redes de área local inalámbricas.

Ambas soluciones presentan dos inconvenientes. Por un lado las soluciones a nivel de capa de enlace proporcionan movilidad para un solo tipo de medio físico, por lo que habría que buscar una solución para cada uno de ellos. Y por otro lado la movilidad con estas soluciones se encuentra mas o menos limitada geográficamente.

Como se va a presentar en los siguientes capítulos el protocolo Mobile IP es el único capaz de proporcionar movilidad en cualquier tipo de medio y extensión geográfica.

CAPITULO II

PROTOCOLO DE INTERNET MOVIL O MOBILE IP

2.1 INTRODUCCION

La informática y las comunicaciones móviles han ganado importancia debido al aumento de computadoras portátiles y teléfonos celulares así como otros terminales móviles y el deseo de los usuarios de mantenerse siempre conectados a Internet, sin tener que preocuparse de su posición física.

La infraestructura de Internet esta construida en base a una serie de protocolos llamados *La Suite de Protocolos TCP/IP*. Siendo El Protocolo de Transmisión (TCP) y el Protocolo de Internet (IP), los fundamentales. El protocolo IP requiere que la posición de cualquier host, conectado a Internet, sea identificada por una dirección IP única. Esto representa, como ya se ha explicado en el capitulo anterior, uno de los principales retos de movilidad, porque cuando dicho host cambia de posición física, se ve forzado a cambiar su dirección IP. Sin embargo los protocolos de niveles superiores requieren que la dirección IP de un host no cambie. Esto se logra gracias al Protocolo Mobile IP.

2.2 GENERALIDADES

El Protocolo de Internet Móvil o Mobile IP (Mobile Internet Protocol) fue propuesto originalmente por el Dr. John Ioannidis y el Prof. Gerald Maguire Jr. en la Universidad de Columbia. A partir de esto el IETF, creó el "Grupo de trabajo

para Mobile IP" en Junio de 1992, actualmente Mobile IP es un estándar abierto definido por el RFC 2002.

Su diseño se basó desde un comienzo sobre las siguientes premisas mínimas e indispensables:

- El nodo móvil debe ser capaz de comunicarse con los demás nodos aún después de haber cambiado su punto de conexión a Internet.

- Esta comunicación debe efectuarse siempre con una única dirección IP para el nodo móvil que deberá ser su dirección IP en la red de origen, se encuentre donde se encuentre.

- El nodo móvil debe ser capaz de comunicarse con otros nodos que no implementen las funciones de movilidad del protocolo Mobile IP.

- El nivel de seguridad y de privacidad de las comunicaciones de un nodo móvil no debe ser menor que el de cualquier otro nodo fijo.

- El medio entre el nodo móvil y su punto de conexión a Internet será a menudo un enlace inalámbrico. Muy probablemente, el nodo móvil estará alimentado por pilas o baterías, lo que hace importante minimizar el consumo reduciendo al mínimo el número de mensajes de señalización.

El principal objetivo del protocolo IP Móvil es sencillo: permitir el encaminamiento de paquetes IP hacia nodos móviles que pueden cambiar rápidamente su punto de conexión a Internet, cabe mencionar que Mobile IP es escalable para Internet ya que está basado en IP es decir cualquier medio de comunicación que pueda soportar IP puede soportar IP Móvil, este objetivo implica la transmisión de actualizaciones de encaminamientos entre numerosos nodos de la red. Para permitir su uso a través un gran número de enlaces inalámbricos, es muy importante reducir el tamaño y la frecuencia de estas actualizaciones al mínimo posible.

Por otra parte, para que el protocolo IP Móvil pueda ser soportado por el mayor número posible de nodos, se requiere que su implementación de software sea lo más sencilla posible en términos de carga computacional y de memoria. De esta manera, tanto ordenadores portátiles como otros terminales con prestaciones de hardware reducidas, como por ejemplo buscapersonas, teléfonos celulares u organizadores personales puedan gozar de la funcionalidad de este protocolo.

En las redes IP, el enrutamiento esta basado en direcciones IP estacionarias, similar a cómo una carta postal se entrega a una dirección fija en un sobre. Un dispositivo en una red es alcanzable a través de una dirección IP normal que se enruta por la dirección IP asignada a éste dentro de una red. Sin embargo, los problemas ocurren cuando un dispositivo vaga fuera de su red local y no es alcanzable mediante el enrutamiento IP normal.

Esto causa que las sesiones activas del dispositivo sean terminadas o canceladas. IP móvil permite a los usuarios que mantengan la misma IP mientras se encuentran viajando a una red diferente, qué incluso puede ser la de un operador inalámbrico diferente, asegurando así que un nodo móvil pueda continuar la comunicación sin obligarlo a cancelar o cerrar sesiones o conexiones. Esto se logra ya que la movilidad de IP Móvil se realiza en la capa de red en lugar de la capa física.

Operaciones como login remotos, impresión remota, y traslados de archivos son ejemplos de aplicaciones dónde es indeseable interrumpir las comunicaciones mientras un individuo o un nodo vaga por los límites de una red. También, ciertos servicios de red, como licencias de software y privilegios de acceso, están basados en direcciones IP. El cambio de estas direcciones IP puede comprometer estos servicios de red.

2.3 COMPONENTES DE UNA RED MOBILE IP

Una red basada en Mobile IP cuenta con los siguientes componentes:

- Nodo móvil o Mobile Node (MN)

- Agente Local o Home Agent (HA)
- Agente Extranjero o Foreign Agent (FA)
- Care-of Address o Dirección de cuidado

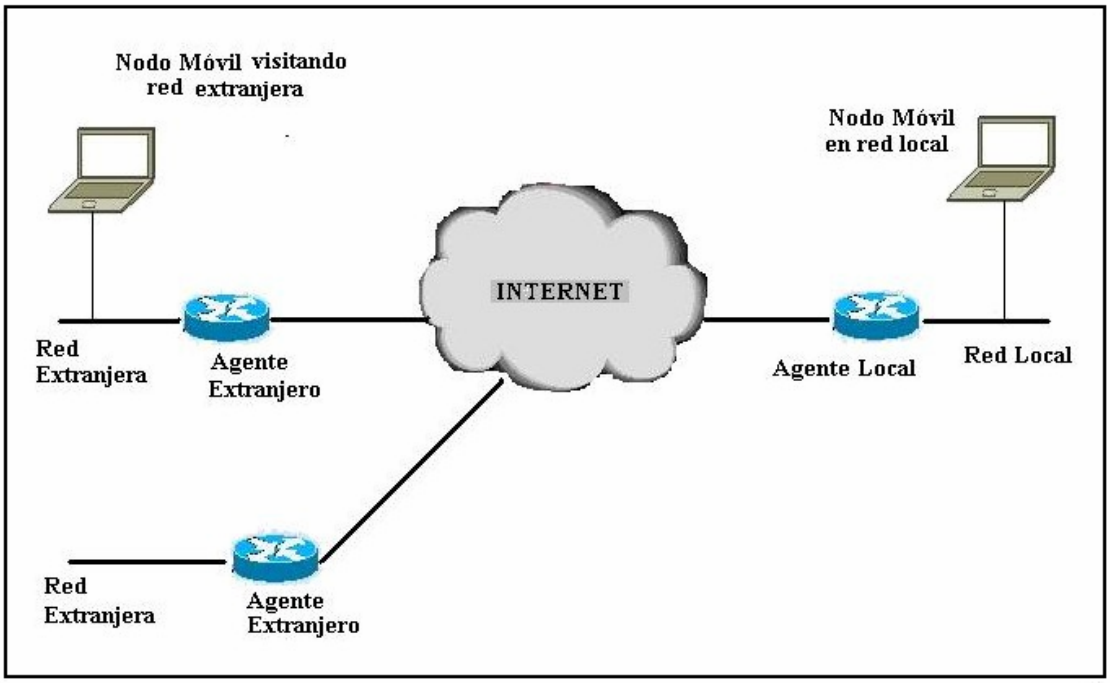

Figura 2. Componentes de la red Mobile IP

2.3.1 Nodo Móvil

El Nodo Móvil es un dispositivo como un teléfono celular, PDA, o computadora portátil cuyo software permite capacidades de roaming entre distintas redes.

2.3.2 Agente Local o Home Agent

El Agente Local es un router ubicado en la red local que sirve como el punto de referencia para la comunicación con el Nodo Móvil; este encapsula los paquetes de un dispositivo en la Internet el cual se comunica con el nodo móvil y que puede o no ser móvil, llamado Nodo Correspondiente o Correspondent Node, al Nodo Móvil que se encuentra en movimiento. Un túnel se establece entre el Agente local y un punto alcanzable para el Nodo Móvil en la red extranjera.

El agente local, es designado por la red local a la que pertenece el nodo móvil, mantiene una lista de relaciones de movilidad en una tabla de movilidad donde cada anotación es identificada por la dirección IP local permanente, la dirección de cuidado y el tiempo de vida. La Tabla 1 muestra una tabla de movilidad.

Dirección local	Dirección de cuidado	Tiempo de vida (s)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

Tabla 1. Tabla de Movilidad

El propósito de esta tabla es establecer la relación entre la dirección IP local del nodo móvil y su dirección de cuidado, y en consecuencia, distribuir los paquetes de acuerdo a la misma.

2.3.3 Agente Extranjero o Foreign Agent

El Agente Extranjero es un router que puede funcionar como el punto de atadura para el Nodo Móvil cuando vaga hacia una red extranjera, entregando los paquetes del Agente local al Nodo Móvil.

Los agentes extranjeros son routers en la red foránea donde el nodo móvil se pueda encontrar, de un momento a otro. El agente extranjero mantiene una lista de visitantes, la cual contiene información acerca de los nodos móviles que están de visita en su red. Cada anotación en la lista de visitantes es identificada por la dirección IP local permanente, dirección del agente local, dirección del medio del nodo móvil, y el tiempo de vida.

Dirección local	Dirección del Agente Local	Dirección MAC	Tiempo de vida (s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	200
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	150

Tabla 2. Lista de Visitantes

La Tabla 2 muestra un ejemplo de una lista de visitantes, en un agente extranjero.

2.3.4 Dirección de cuidado o Care-of Address

La “Dirección de cuidado” más conocida como Care-of Address es el punto de terminación del túnel hacia el Nodo Móvil cuando este está en una red externa.

El Agente Local, mantiene una relación entre la dirección IP de la red local del Nodo Móvil y su correspondiente Dirección de Cuidado, la cual es la ubicación actual del Nodo Móvil en la red externa que esta siendo visitada, cabe recalcar que la dirección de cuidado cambia en cada nuevo punto de enlace.

En un escenario típico, la dirección de cuidado de un nodo móvil es la misma que la dirección IP del agente extranjero. También existe otro tipo de dirección de cuidado, conocida como “Dirección de Cuidado Colocada”, la cual usualmente se obtiene por medio de un mecanismo externo, es decir es asignada a una de las interfaces del nodo móvil en lugar de haber sido ofrecida por un agente extranjero.

2.4 FUNCIONAMIENTO

El funcionamiento del protocolo IP Móvil consiste en la consecución de la siguiente serie de operaciones:

Los agentes local y extranjero (ver figura 3) anuncian su presencia al nodo móvil mediante *mensajes de anunciamiento de agente* que se generan periódicamente en la red. Opcionalmente, el nodo móvil puede solicitar tales mensajes a un agente cercano a través de un *mensaje de solicitud de agent*e.

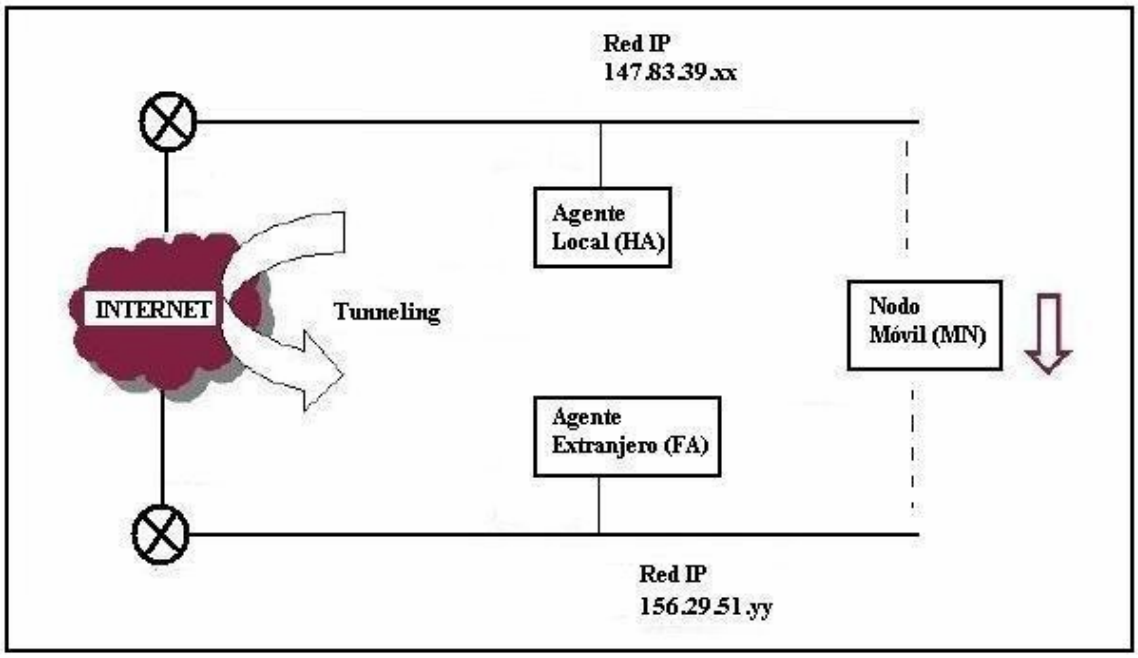

Figura 3: Arquitectura de Mobile IP según IETF

El nodo móvil recibe el mensaje de anunciamiento y determina si se encuentra en su red local o en una red externa.

Si el nodo móvil deduce que se encuentra en su red local, opera sin funciones de movilidad. Por otro lado, si ha regresado tras haber sido registrado en otra red, procede a *deregistrarse* a través de su agente local.

Si el nodo móvil detecta que se encuentra en una red externa, obtiene su dirección de cuidado en la nueva red. Esta dirección puede ser la del agente extranjero o una *Dirección de Cuidado Colocada* o Colocated Care-of Address.

Si el nodo móvil se encuentra fuera del alcance de ningún tipo de agente, el nodo móvil debe obtener su dirección de cuidado como una dirección IP local por algún método como, por ejemplo DHCP (Dynamic Host Configuration Protocol). En estos casos, se trata de una dirección de cuidado colocada. El nodo móvil registra su dirección de cuidado con su agente local. Este proceso se realiza enviando una *solicitud de registro* al agente local y recibiendo de éste un mensaje de contestación.

Todo paquete destinado al nodo móvil es interceptado por el agente local y enviado mediante *tunneling* por éste hacia la dirección de cuidado. Al otro lado del túnel, el agente extranjero recibe el paquete y lo envía al nodo móvil. Si el nodo móvil posee una dirección de cuidado colocada, el agente extranjero no interviene en la recepción del paquete.

Por su parte, los paquetes originados por el nodo móvil pueden ser transportados hasta la dirección IP de destino sin pasar necesariamente por el agente local.

2.5 PROCEDIMIENTOS

Móvil IP realiza tres procedimientos que son:

- Descubrimiento de agente.
- Registro.
- Enrutamiento y Tunneling.

2.5.1 DESCUBRIMIENTO DE AGENTE O AGENT DISCOVERY

El descubrimiento de agente es un procedimiento utilizado en el protocolo IP Móvil mediante el cual el nodo móvil determina si se encuentra conectado a su red local o a una red extranjera, si se ha desplazado de un enlace a otro, y también sirve para obtener una dirección de cuidado cuando se encuentra conectado a un red externa.

El procedimiento mediante el cual se realiza el descubrimiento de agente es relativamente sencillo y precisa únicamente de dos tipos de mensaje:

- Anunciamiento de Agente o *Agent Advertisement*
- Solicitud de Agente o *Agent Solicitation*

2.5.1.1 Anunciamiento de Agente

La primera acción a realizar para permitir la movilidad de un nodo es la de anunciar, por parte del agente local o extranjero, la disponibilidad para aceptar al nodo móvil en su red. El nodo móvil utiliza mensajes de anunciamiento para determinar su punto de conexión actual a Internet. El agente local deberá estar siempre listo para servir a sus nodos móviles. Para evitar una posible saturación debida al exceso de nodos móviles en una determinada red, es factible configurar múltiples agentes locales en una única red local, asignando a cada agente local una porción de la población de nodos móviles.

Por otro lado, es aceptable que un agente extranjero no tenga capacidad para servir a un nodo móvil no perteneciente a su red. Aún en ese caso, el agente extranjero debe continuar emitiendo mensajes de anunciamiento para que el nodo móvil sepa que se encuentra dentro de su área de cobertura o que no ha fallado.

El mensaje de anunciamiento consiste en un mensaje ICMP de Anunciamiento de Router o IRDP (ICMP Router Discovery Protocol) al cual se le ha añadido una extensión para permitir la gestión de los nodos móviles. Esta extensión tiene la forma que se presenta en la Figura 4.

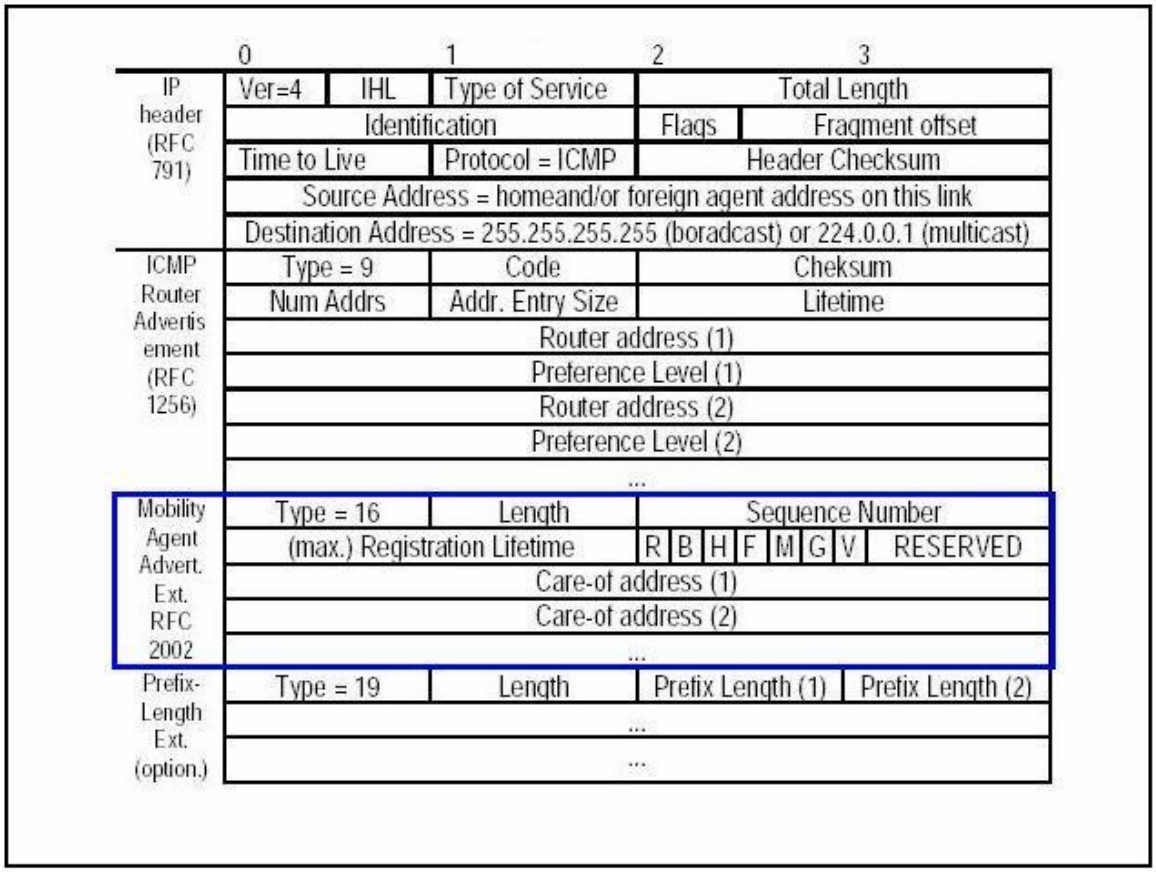

Figura 4. Mensaje de Anunciamiento de Agente

Los campos de la extensión de anunciamiento de agente son los siguientes:

Type: 16

Length: (6+4*N), donde N es el número de direcciones de cuidado anunciadas.

Sequence number: Número total de mensajes de anunciamiento enviados desde que el agente fue inicializado.

Registration lifetime: Tiempo de vida máximo (s) que este agente acepta en una solicitud de registro. (máximo 65535).

R: Registro solicitado. Es conveniente registrar con un agente extranjero en vez de usar una dirección de cuidado colocada.

B: El agente extranjero no puede aceptar nuevos registros, al estar ocupado (Busy)

H: Este agente ofrece servicios de agente local (Home Agent) en esta red.

F: Este agente ofrece servicios de agente extranjero (Foreign Agent) en esta red.

M: El agente soporta encapsulado mínimo.

G: El agente soporta encapsulado GRE.

V: El agente soporta la compresión de cabecera Van Jacobson.

Reserved: Reservado.

Care-of addresses: La dirección de cuidado anunciada por el agente externo.

Para que un nodo móvil pueda averiguar si se encuentra en su red local o, por el contrario, si se ha desplazado hacia una red extranjera, tan solo ha de verificar los bits F y H de alguno de los mensajes de anunciamiento que capture. De esta manera, sabrá si el agente está actuando como agente local o externo. La obtención de su dirección de cuidado se realiza a partir del campo de datos *care-of address* del mensaje de anunciamiento de agente.

2.5.1.2 Solicitud de agente

Los mensajes de solicitud de agente son enviados por los nodos móviles que no desean, o no pueden esperar hasta la siguiente transmisión periódica de mensajes de anunciamiento de agente. Por lo tanto, el único objetivo de un mensaje de solicitud de agente es forzar a cualquier agente ubicado en el mismo enlace a transmitir un mensaje de anunciamiento de agente de manera inmediata. Esto resulta especialmente útil en aquellos casos en los cuales la frecuencia de

los mensajes de anunciamiento es demasiado baja para un nodo móvil que cambia rápidamente de enlace.

El formato de los mensajes de solicitud de agente es exactamente idéntico al de los mensajes ICMP de solicitud de router (ver Figura: 4). La única diferencia reside en que los mensajes de solicitud de agente deben tener su campo de tiempo de vida o Time To Live (TTL) seteado en 1.

2.5.1.3 Descubrimiento automático del Agente local

En caso de que el nodo móvil no pueda avisar a su agente local predefinido, es posible que este nodo móvil se registre con otro agente local, esta vez desconocido para el, en su propia red local.

Este método, llamado Descubrimiento Automático del Agente Local, trabaja usando una transmisión de broadcast a la dirección IP, esto alcanza a los nodos IP en la red local, en lugar de la dirección IP del agente local. Los nodos IP en la red local que pueden operar como agentes locales, recibirán la transmisión de broadcast dirigida al paquete IP y enviará un rechazo al nodo móvil.

Este mensaje de rechazo contiene entre otras cosas la dirección IP de su nodo de origen. El nodo móvil podrá entonces utilizar esta dirección IP en un nuevo mensaje de la registro.

2.5.2 REGISTRO

El protocolo IP Móvil especifica varias circunstancias bajo las cuales todo nodo móvil debe registrarse. La primera de ellas es cuando detecta que su punto de conexión a Internet ha variado respecto a un instante anterior. También deberá registrarse si, aún sin haber cambiado su punto de conexión a Internet, el registro anterior está a punto de caducar. Finalmente, cuando el nodo móvil en una red extranjera detecta que su agente extranjero se ha reiniciado.

A continuación se muestra la estructura de datos del mensaje de registro.

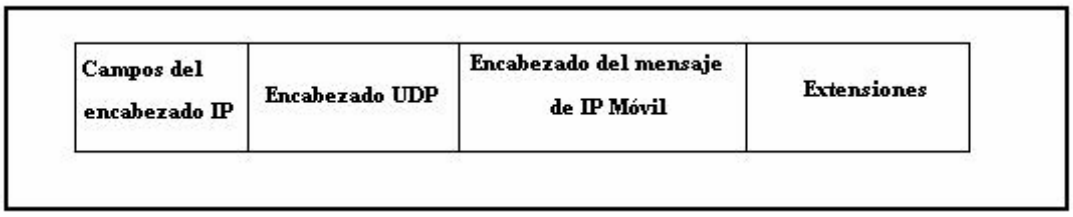

Figura 5: Estructura de datos del mensaje de registro

El procedimiento de registro sirve para solicitar los servicios de un agente extranjero. Acto seguido, el nodo móvil procede a informar a su agente local de su nueva dirección de cuidado en la red. Por el contrario, si el nodo móvil detecta que ha regresado a su red local tras haber permanecido fuera de ella, debe iniciar el procedimiento para desregistrarse con su nodo local para poder continuar funcionando como cualquier otro nodo fijo.

El procedimiento de registro comprende los siguientes pasos:

1. El nodo móvil envía un mensaje de *Petición de Registr*o. Según el caso, este mensaje se enviará directamente al agente local o vía el agente extranjero, previa aceptación del mismo.

2. El agente local recibe la petición de registro y envía a su vez al nodo móvil un mensaje de *Contestación de Registr*o. Éste último informa al nodo móvil si su petición de registro ha sido o no aceptada.

3. Si el nodo móvil no recibe la contestación de registro en un período razonable de tiempo, procede a retransmitir las peticiones de registro con intervalos cada vez más largos entre ellos, hasta recibir contestación.

Para poder llevar a cabo el procedimiento es necesaria la cooperación entre los agentes local y extranjero, intercambiando mensajes de petición de registro, de respuesta de registro además de datos opcionales.

2.5.2.1 Petición de registro

Un nodo móvil se registra con su agente local mediante un mensaje de petición de registro. De esta manera, el agente local puede crear o modificar la entrada del nodo móvil en su lista de nodos con movilidad. El mensaje de petición de registro presenta el formato mostrado en la Figura 6.

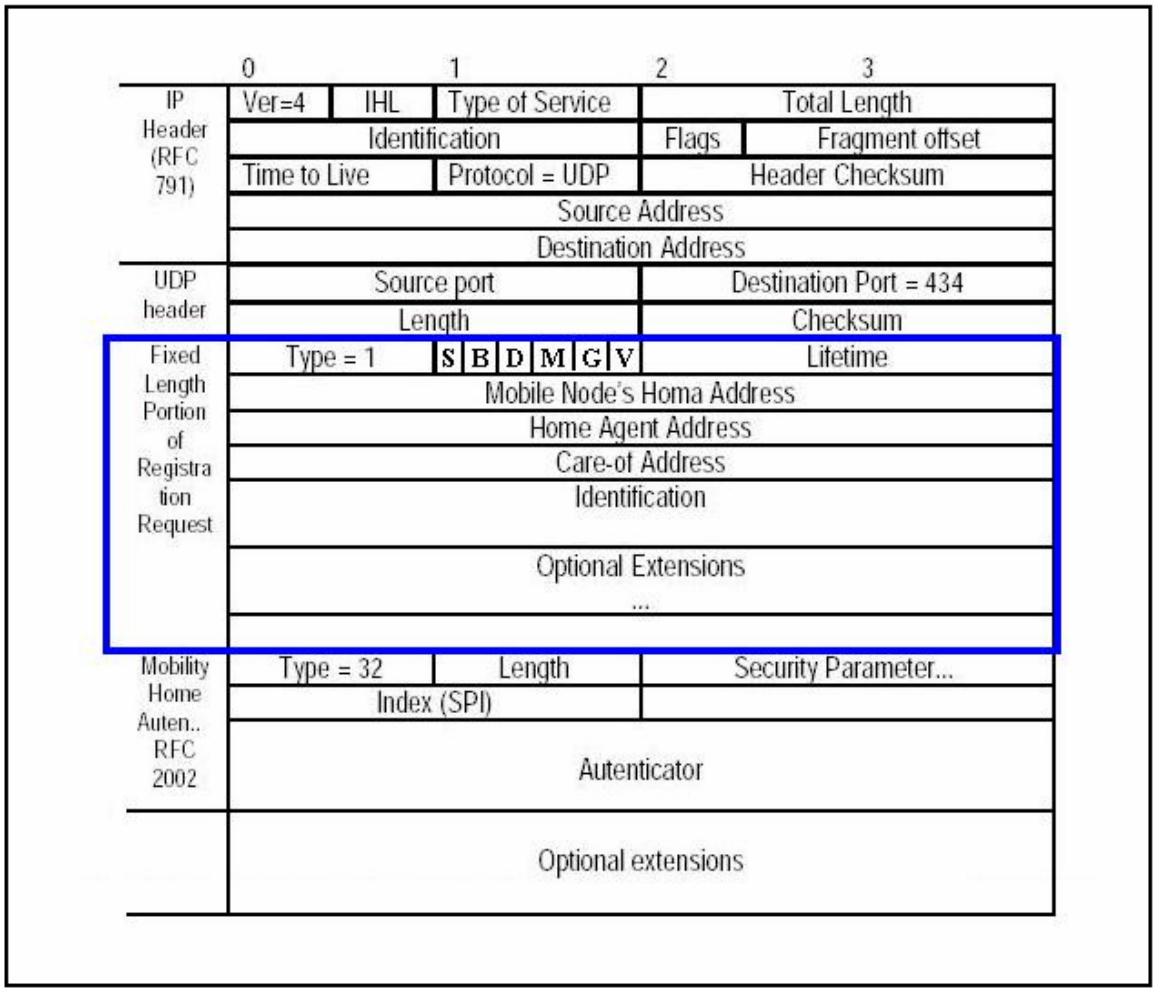

Figura 6: Mensaje de petición de registro

Los diferentes campos que conforman el mensaje de petición de registro son los siguientes:

Type: 1 (Petición de registro)

S: El nodo móvil solicita que el agente local mantenga sus anteriores entradas de movilidad.

B: El nodo móvil solicita al agente local que tunelee hacia él los paquetes de broadcast que se reciban en la red local.

D: El nodo móvil informa al agente local que desencapsulará los paquetes que le sean enviados a su dirección de cuidado. Esto implica que el nodo móvil esta utilizando una dirección de cuidado colocada.

M: El nodo móvil solicita que el agente local utilice encapsulado mínimo para los paquetes destinados a él.

G: El nodo móvil solicita que el agente local utilice encapsulado GRE para los paquetes destinados a él.

V: El nodo móvil solicita que el agente local que su agente de movilidad emplee la compresión de cabeceras de Van Jacobson.

Reserved: Reservado.

Lifetime: Número de segundos restantes antes de la caducidad del registro actual.

Home Address: Dirección IP del nodo móvil

Home Agent: Dirección IP del agente local del nodo móvil.

Care-of Address: Dirección de cuidado = dirección IP a la salida del túnel.

Identification: Número de 64 bits creado por el nodo móvil para asociar peticiones de registro con contestaciones de registro. También sirve para proteger contra contestaciones de registro fraudulentas.

Extensions: Extensiones

2.5.2.2 Respuesta de registro

Como ya se ha explicado anteriormente, tras la recepción de una petición de registro, el agente local devuelve al nodo móvil un mensaje de respuesta de registro.

Si el nodo móvil solicita el servicio a través de un agente extranjero, será éste quien reciba la contestación de registro y la envíe a continuación al nodo móvil. Por otro lado, si el nodo móvil está utilizando una dirección de cuidado colocada, será él mismo quien reciba la el mensaje de respuesta de registro.

Este mensaje informa al nodo móvil sobre el resultado de su petición de registro y del tiempo de vida del registro, que puede ser inferior o igual al solicitado por el nodo móvil. El agente externo no puede en ningún caso modificar el tiempo de vida asignado por el agente local.

El formato del mensaje de respuesta de registro es el mostrado en la Figura 7.

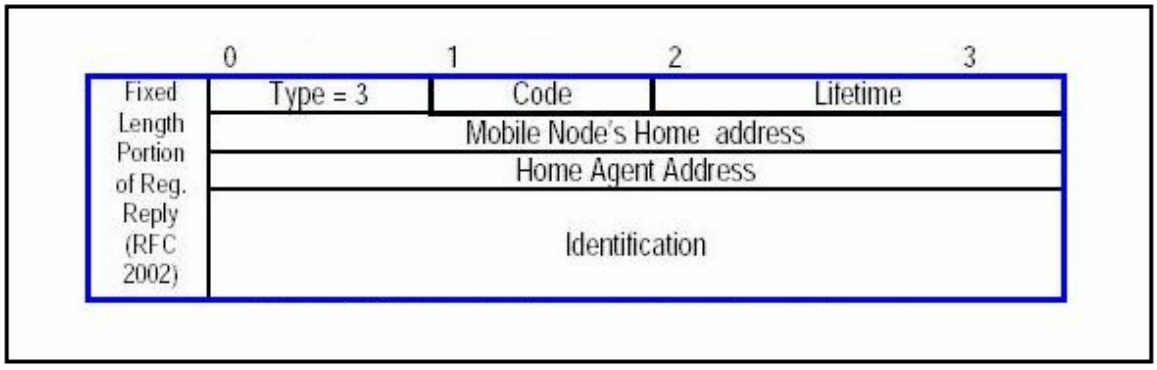

Figura 7: Mensaje de respuesta de registro

Los campos del mensaje son los siguientes:

Type: 3 (Contestación de registro)

Code: Código indicador del resultado de la petición de registro.

Lifetime: Tiempo de vida, en segundos, de la entrada del nodo móvil en la lista de movilidad del agente local.

Home Address: Dirección IP del nodo móvil.

Home Agent: Dirección IP del agente local del nodo móvil.

Identification: Número de 64 bits creado por el nodo móvil para asociar peticiones de registro con contestaciones de registro. También sirve para proteger contra contestaciones de registro fraudulentas.

Extensions: Extensiones.

A continuación se presenta un gráfico explicativo del proceso total de registro que se realiza en el protocolo Mobile IP.

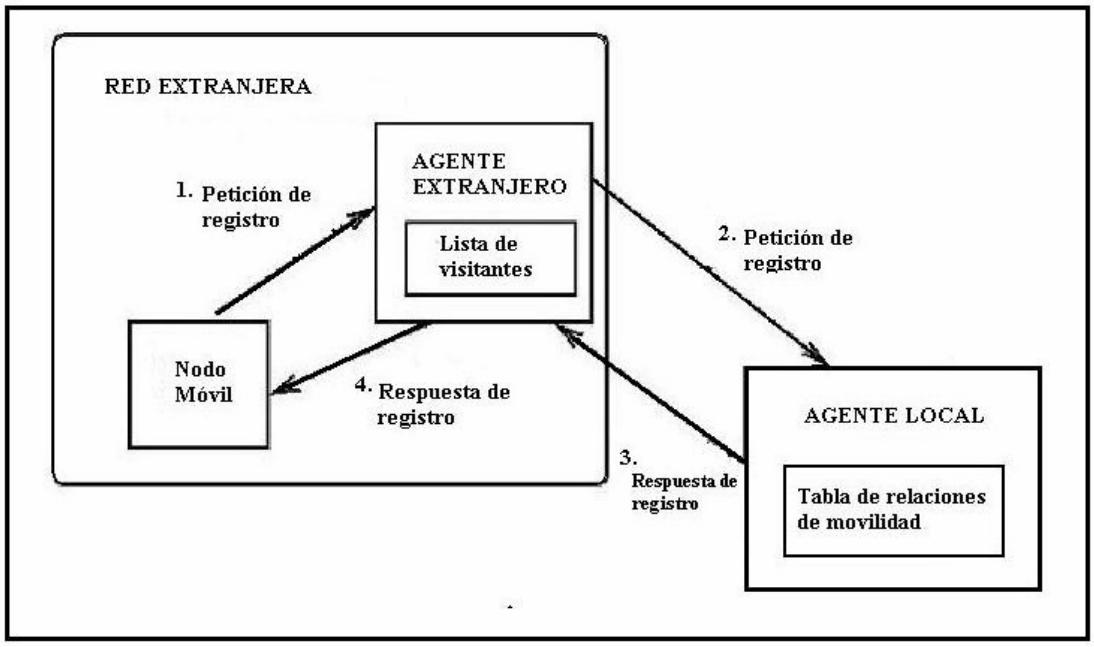

Figura 8. Proceso de registro

2.5.2.3 Posibilidades opcionales del procedimiento de registro

Además de las acciones anteriormente descritas, el procedimiento de registro permite también llevar a cabo otras interesantes funciones que se enumeran a continuación:

- Descubrir la dirección de un agente local si el nodo móvil no ha sido configurado con esta información.
- Seleccionar diferentes tipos de encapsulado de los paquetes.
- Utilizar la compresión de encabezados de Van Jacobson.
- Mantener varios registros simultáneos para que cada dirección de cuidado activa reciba una copia de los paquetes destinados al nodo móvil.
- Desregistrar ciertas direcciones de cuidado manteniendo otras activas.

2.5.3 ENRUTAMIENTO Y TUNNELING

Una vez analizados los procedimientos de descubrimiento de agente y de registro, se presentan los diferentes modos en que un paquete puede ser encaminado desde su dirección IP de origen hasta la dirección IP de destino en función de la situación del nodo móvil.

2.5.3.1 Enrutamiento de los paquetes

En primer lugar, cabe distinguir dos posibles escenarios: uno en el que el nodo móvil está conectado a su red local, o bien si éste se encuentra en una red extranjera.

2.5.3.1.1 Nodo móvil en red local.

Si el nodo móvil se encuentra en su red local, actúa como si se tratara de cualquier nodo fijo. Por lo tanto, las reglas para el enrutamiento de paquetes en este caso son las mismas que para el encaminamiento de paquetes IP hacia cualquier nodo o router convencional.

2.5.3.1.2 Nodo móvil en red extranjera.

Hacia el nodo móvil. El protocolo IP Móvil requiere que los paquetes enviados desde la red local hasta el nodo móvil sean encapsulados. El encapsulado altera el encaminamiento habitual de los paquetes ya que éstos atraviesan un nodo intermedio antes de llegar a su destino. Una vez que ha llegado al nodo intermedio, éste procede a desencapsularlo y enviar el paquete original al destinatario final. De manera general, las operaciones que comprende el envío de un paquete hacia un nodo móvil en una red extranjera son las siguientes:

1. Un router en la red local, generalmente el agente local, anuncia que existe conectividad hasta el prefijo de red equivalente al de la dirección local del nodo móvil. Por lo tanto, todo paquete destinado al nodo móvil es encaminado hacia su red local y, en concreto, es recibido por su agente local.

2. El agente local intercepta el paquete destinado al nodo móvil y consulta su entrada en su lista de movilidad para conocer las direcciones de cuidado registradas.

3. A continuación, el agente local envía una copia del paquete hacia cada dirección de cuidado a través de túneles *(tunnelin*g).

En cada dirección de cuidado (la del agente extranjero o una dirección de cuidado colocada), se extrae el paquete original y es entregado al nodo móvil.

Antes de enviar un paquete a través del túnel, el agente local realiza la operación de encapsulado dentro de un nuevo paquete cuya dirección de destino es la dirección de cuidado (ver Figura 9).

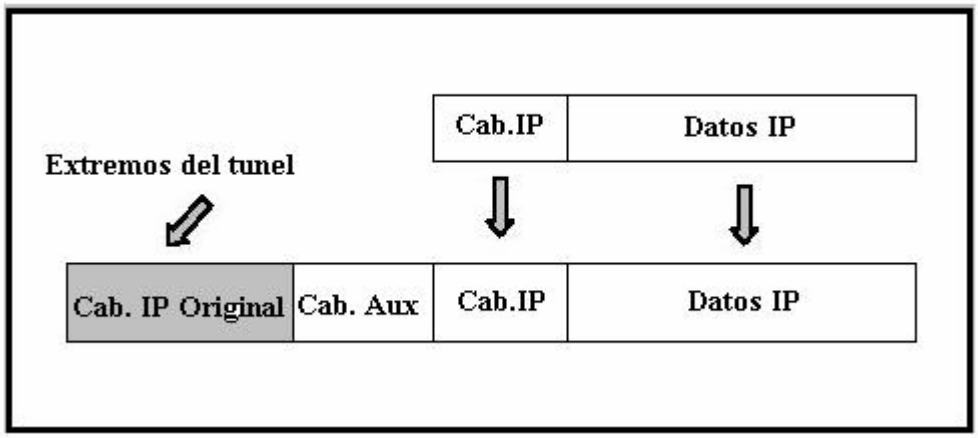

Figura 9: Operación de encapsulamiento

Si se trata de una dirección de cuidado de un agente extranjero, éste deshace el encapsulamiento exterior del paquete para recuperar el paquete original. A continuación consulta el campo de dirección IP de destino para comprobar si coincide con alguno de los nodos móviles a los que está prestando servicio. Si es este el caso, el agente extranjero envía el paquete al nodo móvil a través de la interfaz adecuada. Si la dirección de cuidado es colocada, el nodo móvil no recibe los servicios de ningún agente extranjero y, por lo tanto, efectúa él mismo las operaciones de desencapsulamiento.

Desde el nodo móvil. Para poder enviar paquetes a otros nodos, un nodo móvil debe encontrar la dirección de un router que pueda dar salida a estos paquetes. Si el nodo móvil depende de un agente extranjero, existen dos alternativas a la hora de determinar un router adecuado:

- El propio agente extranjero, según especifica el campo *IP Source Address* del mensaje de anunciamiento de agente.

- Cualquier router cuya dirección IP aparezca en los campos *Router Address* del mensaje de anunciamiento de router, porción del mensaje de anunciamiento de agente.

Sin embargo, esta última alternativa tan solo es válida si el nodo móvil es capaz de determinar la dirección de la capa de enlace del router deseado, sin enviar peticiones de ARP *(*Address Resolution Protocol) que contengan su dirección IP local.

Si el nodo móvil posee una dirección de cuidado colocada, es decir, no depende de ningún agente externo, también tiene dos alternativas a la hora de seleccionar un router:

- Escoger algún router que esté enviando mensajes de anunciamiento de router (no de agente) en la red en la que se encuentra.

- Mediante el mismo mecanismo por el que obtuvo su dirección de cuidado colocada puede obtener la dirección de un router adecuado. Por ejemplo, el protocolo DHCP ofrece todo tipo de información al nodo móvil, incluida la dirección de un router.

Contrariamente a los nodos móviles dependientes de un agente extranjero, los nodos móviles con una dirección de cuidado colocada pueden enviar peticiones ARP con su dirección local.

2.5.3.2 Tunneling

El término encapsulado es un equivalente al de tunelado o *tunnelin*g. Ello consiste en la inserción de un paquete IP dentro de otro paquete del mismo tipo o de otro. El paquete resultante es, a continuación, enviado a un nodo intermedio entre el nodo origen y el nodo destino final.

El escenario más habitual de utilización de túneles es el presentado en la Figura 10.

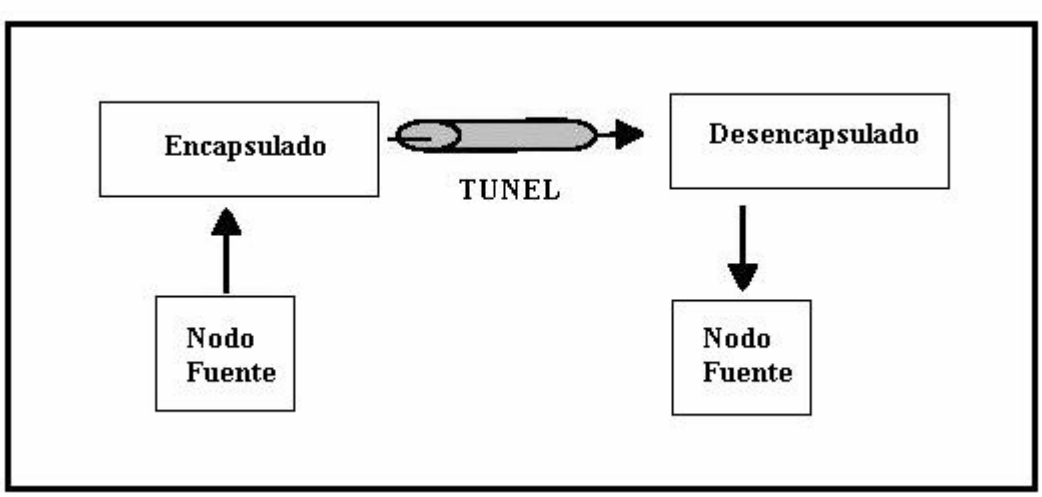

Figura 10. Escenario típico para la acción de Tunneling

El nodo encapsulador es generalmente considerado el punto de entrada al túnel y el nodo desencapsulador el punto de salida del túnel. Actualmente las técnicas de encapsulado IP son especialmente útiles para realizar transmisiones multicast, e incluso llevar a cabo acciones de seguridad y privacidad en Internet.

El protocolo IP Móvil requiere que los agentes locales, los agentes extranjeros y los nodos móviles con una dirección de cuidado colocada soporten el encapsulado IP-in-IP. A continuación se presentan éste y otros tipos de encapsulado que el agente local puede emplear para enviar los paquetes a través de túneles.

A continuación se muestra gráficamente el proceso de tunneling.

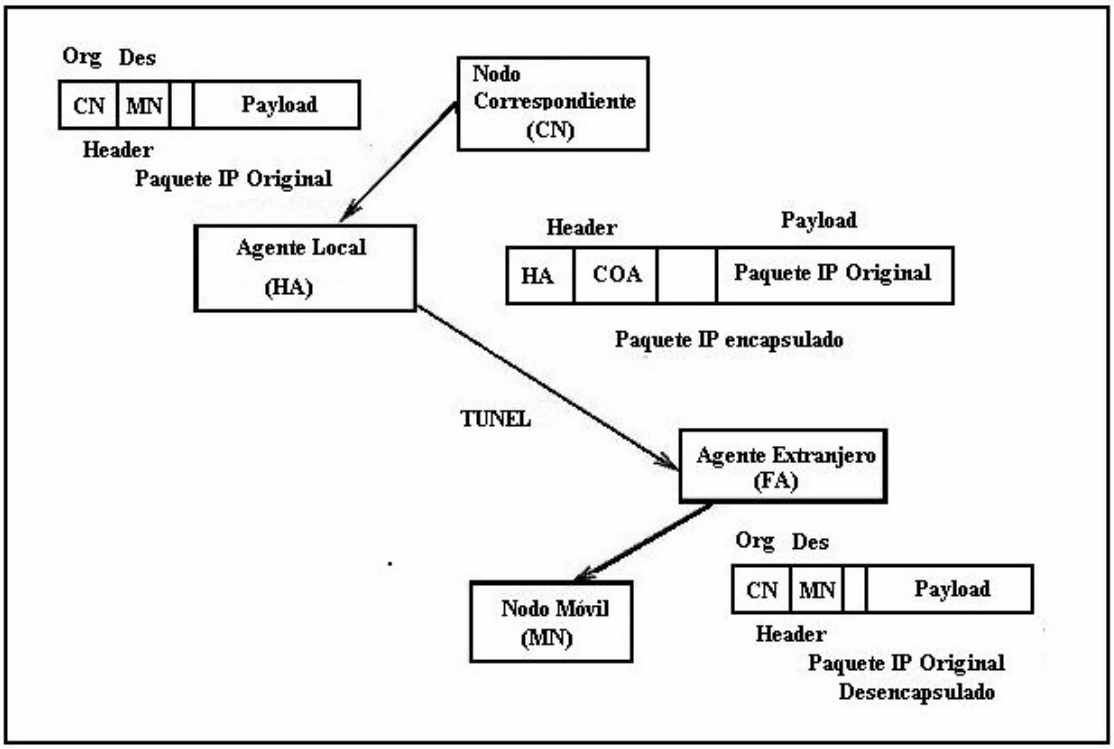

Figura 11. Procedimiento de Tunneling

2.5.3.2.1 Encapsulado IP- in - IP

El encapsulado IP-in-IP consiste en insertar una cabecera IP adicional antes de la cabecera propia del paquete inicial como se muestra en la Figura 12.

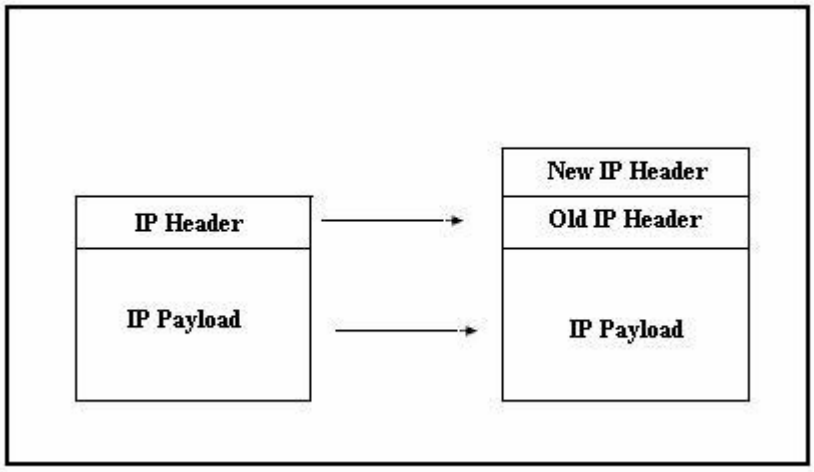

Figura 12. Encapsulado IP - in - IP

También es posible insertar otras cabeceras entre las dos cabeceras anteriores, como por ejemplo, requisitos de seguridad para proteger el paquete original durante el tunneling.

La cabecera exterior contiene información sobre los extremos del túnel. La cabecera interior contiene información sobre los nodos origen y destino del paquete inicial y no puede ser modificada en ningún caso, salvo para decrementar el tiempo de vida (TTL - Time To Live) del paquete, aunque tan solo una vez dentro del túnel, a pesar de que pueda atravesar varios routers.

A simple vista podría parecer que resulta imposible saber si se ha producido algún problema con el paquete mientras éste se encuentra dentro del túnel. No obstante, el punto de entrada al túnel mantiene una serie de informaciones, compuesto por un juego de variables que describen las características del túnel. Esta información consta de:

- Máxima MTU (Maximum Transfer Unit) del túnel.
- Longitud del túnel, contabilizada en hops (saltos).
- Si el extremo final del túnel es alcanzable

El punto de entrada al túnel actualiza estas variables mediante mensajes ICMP que recibe de los routers en el interior del túnel.

2.5.3.2.2 Encapsulado mínimo

El encapsulado suele conllevar el duplicado innecesario de numerosos campos de la cabecera IP interna. El encapsulado mínimo intenta minimizar al máximo la información de overhead de encapsulado para disminuir el tamaño del paquete resultante.

Como puede observarse en la Figura 9, la cabecera IP original es modificada y la cabecera de encapsulado mínimo es insertada entre la cabecera original modificada y la información.

Al desencapsular un paquete con encapsulado mínimo, se deberán restaurar los campos modificados en la cabecera original con los datos de la cabecera de encapsulado mínimo, actualizando los campos que así lo requieran como por ejemplo el campo de longitud del paquete, y el de checksum.

A pesar de todo, el encapsulado mínimo no está ampliamente difundido ya que presenta ciertas desventajas. Concretamente, no funciona con paquetes ya fragmentados. Además, este encapsulado fuerza a que el valor TTL sea decrementado en cada router dentro del túnel por lo que, puede suceder que los paquetes caduquen antes de llegar a su destino.

En la siguiente figura se presenta el esquema de encapsulado mínimo.

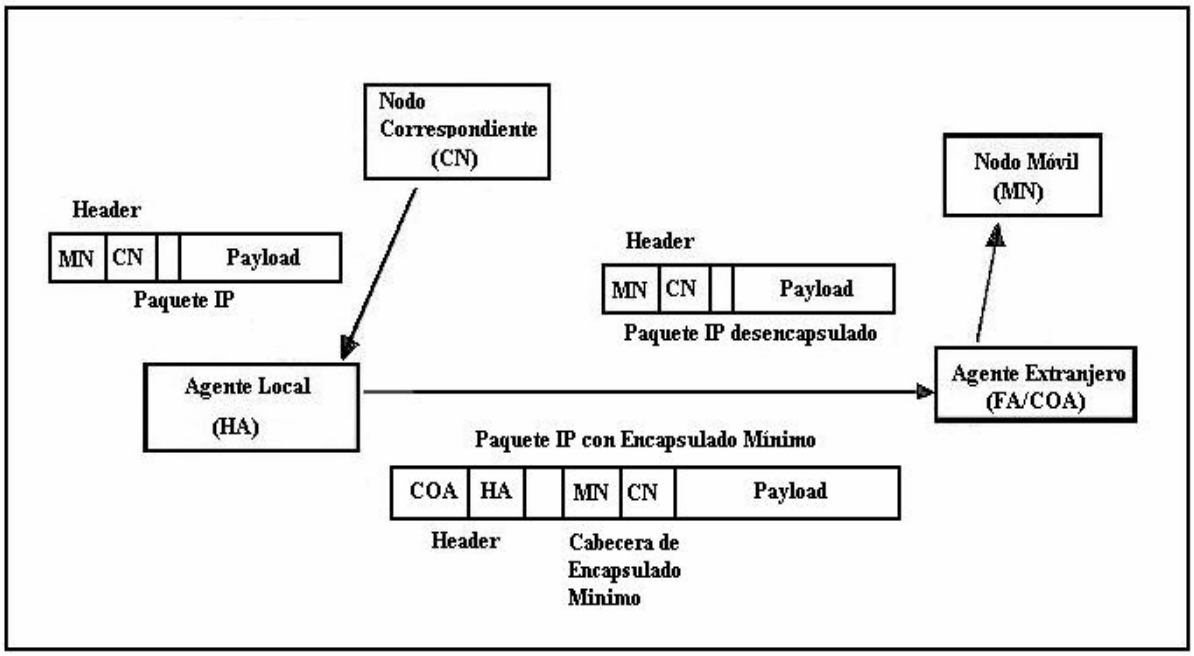

Figura 13. Esquema de encapsulado mínimo

2.5.3.2.3 Encapsulado GRE

El encapsulado GRE (Generic Record Encapsulation*)* es el más flexible los tres mencionados, ya que permite la encapsulación de cualquier tipo de paquete, incluidos los paquetes IP. El formato del paquete GRE es el que se presenta en la Figura 14.

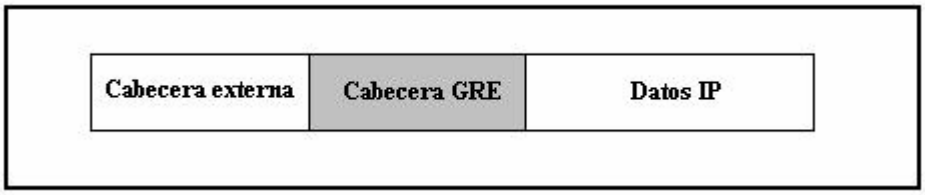

Figura 14. Formato de paquete GRE

Contrariamente a los encapsulados IP-in-IP y Mínimo, el encapsulado GRE ha sido específicamente diseñado para prevenir encapsulamientos recursivos.

Concretamente, el campo *recur* en la cabecera GRE es un contador que informa del número de encapsulados adicionales que son permitidos.

2.6 CONSIDERACIONES DE SEGURIDAD

La seguridad es importante en IP Móvil, ya que los nodos a menudo están conectados a Internet por medios o enlaces inalámbricos, los cuales son muy vulnerables a brechas de seguridad. Todos los mensajes de autorización entre el nodo móvil y el agente local requieren del llamado Mobile - Home Authentication Extensión (MHAE).

Por ejemplo, durante el proceso de registro, el agente local deberá estar convencido de que esta recibiendo una petición de parte de un nodo móvil autentico, y no de parte de uno falso. Mobile IP resuelve este problema especificando una asociación de seguridad entre el agente local y el nodo móvil. Esta asociación de seguridad actualmente es configurada a manualmente. Cada

mensaje de registro deberá tener la extensión de autenticidad del agente local del nodo móvil, la cual está contenida en el Security Parameters Index (SPI), seguido por un autenticador. El SPI es un índice en la asociación de seguridad de movilidad, el cual define el contexto de seguridad, esto es, un algoritmo usado para calcular y comprobar el autenticador. El algoritmo base, MD5 usa una llave de 128 bits. Cada registro contiene información única, para evitar la grabación de registro de parte de nodos malévolos.

Dos métodos son usados para generar estos datos únicos:

- **Timestamps**: El nodo que genera el mensaje, inserta la hora del día, y el nodo que recibe el mensaje comprueba si es suficientemente parecido a su propia hora.

- **Nonces**: El nodo A genera un nuevo numero arbitrario (randómico) en cada mensaje al nodo B, y comprueba si el nodo B devuelve el mismo numero en su respuesta hacia A. Ambos mensajes usan un código de autenticación para protegerse contra alteraciones de parte de algún forastero indeseado. El nodo B también puede crear números arbitrarios, e incluirlos en sus mensajes.

2.7 OPTIMIZACION DE RUTAS

En el protocolo básico de IP Móvil, es decir la versión 4, los paquetes de IP destinados a un nodo móvil que se encuentra fuera de su red, son encaminados a través del agente local. Sin embargo, paquetes del nodo móvil a nodos correspondientes (CN) son encaminados directamente. Esto es conocido como enrutamiento en triángulo o Triangle Routing. La siguiente figura ilustra el encaminado en triángulo.

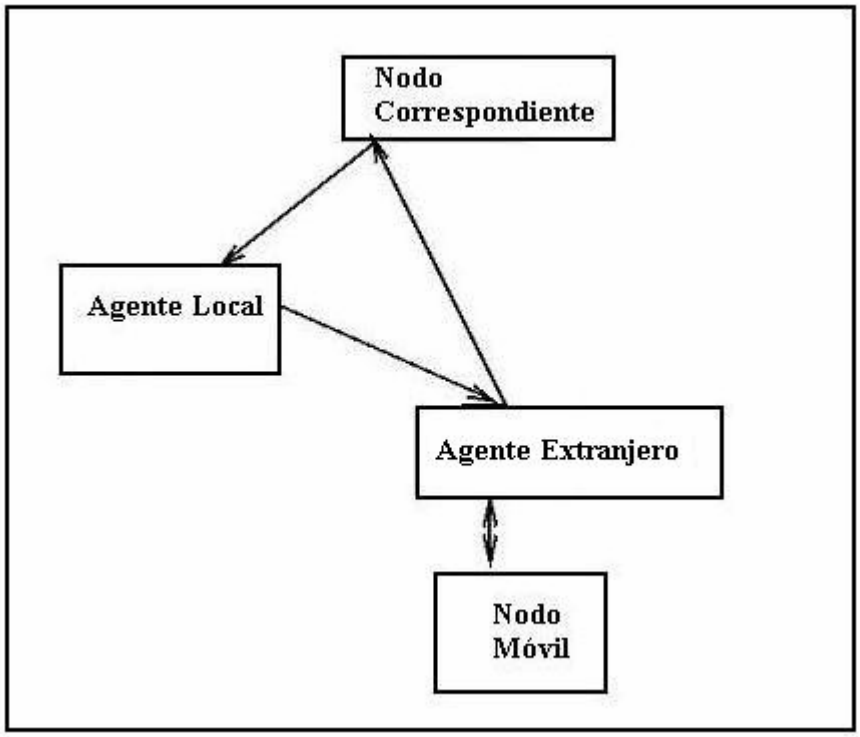

Figura 15. Enrutamiento en Triángulo

Este método puede ser ineficaz en muchos casos. Consideremos el caso cuando el nodo correspondiente y el nodo móvil se encuentran en la misma red, pero no en la red local del nodo móvil. En un caso tal, los mensajes se tardaran innecesariamente, porque tendrán que ser primero encaminados hacia el agente local, el cual reside en la red local. Una manera de mejorar esta situación es la Optimización de Rutas.

La Optimización de Rutas es una extensión propuesta al protocolo de IP Móvil y se halla en la nueva versión del mismo, Mobile IPv6.

En esta extensión, MIPv6, los mensajes del nodo correspondiente son encaminados directamente a la dirección de cuidado del nodo móvil, sin tener que visitar el agente local. La Optimización de Rutas proporciona cuatro operaciones principales. Estas son:

- Puesta al día de datos en memoria local (Binding Caches)
- Manejo de “Smooth Handoffs” entre los agentes extranjeros

- Adquirir llaves de registro para “Smooth Handoffs”
- Utilización de túneles especiales.

2.7.1 Puesta al día de datos en memoria local

Los datos en memoria local, son mantenidos por los nodos correspondientes por la asociación de la dirección local del nodo móvil con su dirección de cuidado. Una anotación en memoria local, también tiene un tiempo de vida, después del cual, será borrada. Si el nodo correspondiente no encuentra una anotación en su memoria local, referente al nodo móvil, procede a enviar un mensaje a su dirección local. Cuando el agente local intercepta este mensaje, lo encapsula y se lo manda de vuelta, al nodo móvil, a su dirección de cuidado. Después, el agente local envía información sobre la nueva relación de comunicación, al nodo correspondiente.

2.7.2 Manejo de “Smooth Handoffs” entre los agentes extranjeros

Cuando un nodo móvil se registra con un nuevo agente extranjero, IP Móvil no especifica un método para informarle previamente al agente extranjero. Por esto es que los datagramas ya encapsulados y enviados previamente a la dirección de cuidado, se pierden. Este problema es resuelto por medio de la Optimizacion de Rutas, porque introduce lo que se conoce como “Smooths Handoffs”. Los Smooth Handoffs proporcionan una manera de notificar previamente al agente extranjero acerca de la nueva relación de movilidad del nodo.

Si el agente extranjero tiene la característica de soportar Smoths Handoffs, este lo indica mediante su Mensaje de Anuncio De Agente. Cuando el nodo móvil se mueve a otra área, le pide al nuevo agente extranjero, durante el proceso de registro, que informe al previo agente extranjero acerca de su nueva relación. El nuevo agente extranjero entonces, prepara un mensaje, y se lo manda al agente extranjero previo. Gracias a este proceso, si el agente extranjero previo recibe paquetes para el nodo móvil, con relaciones expiradas, se lo puede enviar a la nueva dirección de cuidado. El agente extranjero previo también alerta al agente local del nodo móvil. El agente local, a su vez, informa al nodo correspondiente.

Este proceso también permite que datagramas mandados por nodos correspondientes con relaciones expiradas, sean enviados a la dirección de cuidado. Finalmente, este proceso permite que el agente extranjero previo libere espacio en su memoria, inmediatamente, en vez de esperar a que el tiempo de vida del nodo móvil expire.

2.7.3 Adquirir llaves de registro para "Smooth Handoffs"

Para manejar "Smooth Handoffs ", los nodos móviles necesitan comunicarse con agentes extranjeros previos. Esta comunicación deberá llevarse a cabo por medios seguros, porque el agente extranjero deberá tratar de asegurarse de que esta recibiendo información valida, y no que esta a punto de mandar paquetes a direcciones falsas. Por esta razón, una llave de registro es creada entre el agente extranjero y el nodo móvil, durante el proceso de registro. Los siguientes métodos, han sido propuestos para establecer llaves de registro:

- Si el agente local y el agente extranjero comparten una asociación de seguridad, el agente de casa puede escoger la llave de registro.

- Si el agente extranjero tiene una llave publica puede, otra vez, usar la llave del agente de casa.

- Si el nodo móvil incluye su llave pública, en su petición de registro, el agente extranjero puede escoger la nueva llave de registro.

- El nodo móvil y el agente extranjero pueden usar el protocolo de cambio de llaves Diffie-Hellman, como parte del registro.

Esta llave de registro es usada para formar una asociación de seguridad entre el nodo móvil y el agente extranjero.

2.7.4 Utilización de túneles especiales.

Cuando un agente extranjero recibe un datagrama encapsulado, para el cual no encuentra información en su lista de visitantes, concluye que el remitente posee información expirada referente al nodo móvil. Si el agente extranjero posee información en memoria, acerca del nodo móvil, deberá re-encapsular el paquete hacia la dirección de cuidado que posee. En contraparte, si no posee información en su lista de visitantes, ni en memoria, construirá un datagrama encapsulado especial. Este datagrama encapsulado especial tiene la dirección de destinatario externa, igual a la interna. Esto le permite al agente local ver la dirección del nodo que encapsuló el datagrama y prevenir el re-envió al mismo nodo. De esta forma se evita un posible lazo de encaminamiento, el cual podría ocurrir si el agente extranjero sufre una falla, y pierde información de estado.

CAPITULO III

RELACION DE MOBILE IP CON IPv4 E IPv6

3.1 INTRODUCCION

El aumento progresivo de aplicaciones que necesitan direcciones IP públicas globales, válidas para conexiones extremo a extremo, y por tanto, enrutables, unido al crecimiento de la nueva generación de telefonía móvil que actualmente supera al número de terminales fijos de Internet y que funcionará sobre IP, hace que la transición de IPv4 a IPv6 sea impostergable y urgente.

Por otra parte la red de Internet ha experimentado un enorme crecimiento en los últimos años y el número de direcciones disponibles se hace cada vez más pequeño frente a las necesidades existentes en un futuro cercano. Por ello, el IETF, organización encargada de la evolución de la arquitectura en la red de Internet, ha diseñado e introducido el Protocolo de Internet versión 6 más conocido como IPv6. Este nuevo modelo es el sucesor de la versión 4 puesto que resuelve sus deficiencias y aporta nuevas funciones acordes a la evolución actual de la red.

Estas carencias fundamentales que posee IPv4 y que podrán ser solucionadas con esta nueva versión son entre otras las siguientes:

Escalabilidad. Cada máquina presente en la red dispone de una dirección IP de 32 bits. Ello supone 4.300 millones de máquinas diferentes. Esta cifra, no obstante, es muy engañosa. El número asignado a un ordenador no es arbitrario,

sino que depende de una estructura jerárquica, lo cual ocasiona que se desperdicie una enorme cantidad de direcciones.

Enrutamiento. Otro de los grandes problemas del crecimiento de Internet es la capacidad de almacenamiento necesaria en los routers y el tráfico de gestión preciso para mantener sus tablas de enrutamiento. Existe un límite tecnológico al número de rutas que un nodo puede manejar, y como Internet crece de forma mucho más rápida que la tecnología que la mantiene, se intuye que pronto los routers alcanzarán su capacidad máxima y empezarán a desechar rutas, con lo que la red comenzará a fragmentarse en subredes sin acceso entre sí.

Seguridad. Con la aparición de servicios comerciales y la conexión de numerosas empresas, el enorme incremento en el número de usuarios por todo el planeta y la cantidad de sistemas que necesitan de Internet para su correcto funcionamiento, es urgente definir mecanismos de seguridad para la red. Son necesarios esquemas de autenticación y privacidad, tanto para proteger a los usuarios en sí, como la misma integridad de la red ante ataques malintencionados o errores.

Tiempo real. IPv4 define una red puramente orientada a datagramas y, como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tráfico en la red es muy variable y sujeto a congestión. Por ello, se necesita una extensión que posibilite el envío de tráfico en tiempo real, y así poder hacer frente a las nuevas demandas en este campo.

Tarifación. Con una red cada día más orientada hacia el mundo comercial, hace falta dotar al sistema de mecanismos que posibiliten el análisis detallado del tráfico, tanto por motivos de facturación, como para poder dimensionar los recursos de forma apropiada.

Comunicaciones Móviles. El campo de las comunicaciones móviles está en auge, y aún lo estará más en un futuro inmediato. Se necesita una nueva arquitectura con mayor flexibilidad topológica, capaz de afrontar el reto que supone la movilidad de sus usuarios. La seguridad de las comunicaciones en este tipo de sistemas se ve además, especialmente comprometida.

Por otro lado las principales características nuevas que aporta IPv6 frente a IPv4 son:

Aumento de las capacidades de direccionamiento. IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico. Estos 128 bits suponen 340 cuatrillones de direcciones con lo que incluso cada grano de arena del planeta podría tener su propia dirección IP.

Soporte mejorado para las Extensiones y Opciones. Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos y mayor flexibilidad para introducir nuevas opciones en el futuro.

Capacidad de Etiquetado de Flujo. Se agrega una nueva capacidad para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares, para lo cuál, el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

Capacidades de Autenticación y Privacidad. En IPv6 se especifican extensiones para utilizar autenticación, integridad de los datos, y confidencialidad de los datos.

Autoconfiguración. Esto permite lo que es conocido como *“Plug and Play”*, sin necesidad de servidores, y facilidades de reconfiguración. Los dispositivos pueden configurar sus propias direcciones IPv6 basándose en la información que reciban del router de la red.

Mecanismos de movilidad más eficientes y robustos. Mobile IP soporta dispositivos móviles que cambian dinámicamente sus puntos de acceso a la red, y concretamente Mobile IPv6 permite a un host IPv6 dejar su subred de origen mientras mantiene transparentemente todas sus conexiones presentes y sigue siendo alcanzable por el resto de Internet. Esto es precisamente lo que se verá en las siguientes secciones.

3.2 IP MOVIL VERSION 4 O MOBILE IPv4 (MIPv4)

La tecnología de Mobile IP descrita en detalle en el Capitulo 2 esta basada en su totalidad para IPv4 y como se vio consta de tres componentes fundamentales:

- El Agente Local
- El Nodo Móvil
- El Agente Extranjero

El agente local puede ser un servidor o un router que se despliega en la red base del usuario, por ejemplo, los servicios de red IP en la intranet de una empresa.

El nodo móvil reside en un dispositivo móvil y trabaja con el agente local para manejar transparentemente el manejo de la dirección IP y el reenrutamiento de la conexión.

El agente extranjero que reside en redes visitadas, es decir extranjeras, al nodo móvil, y conserva direcciones IP enrutables globalmente, mientras que reduce la necesidad de direcciones enrutables localmente dentro de la red extranjera, esta es una consideración importante para MIPv4.

El protocolo Mobile IPv4 tiene tres etapas, fáciles de distinguir que son:

1. **Descubrimiento de Agente:** El Descubrimiento de un Agente consiste de los siguientes pasos:
    1. Los Agentes de movilidad anuncian su presencia, difundiendo periódicamente, mensajes de anunciamiento de agente. Un mensaje de anuncio de agente, contiene una o mas direcciones de cuidado, y una bandera indicando si es un agente extranjero o un agente local.
    2. El nodo móvil que recibe el mensaje de anunciamiento de agente, reconoce si el mensaje viene de su agente local y si procede de su red local o de una red foránea.

3. Si un nodo móvil no desea esperar el mensaje periódico, puede mandar mensajes de solicitud de agente, que serán contestados por un agente de movilidad.

2. **Registro:** El Registro consiste de los siguientes pasos:
    1. Si un nodo móvil descubre que se encuentra en su red local, opera sin usar ninguno de los servicios de movilidad.
    2. Si el nodo móvil se encuentra en una red nueva (extranjera), se registra con el agente extranjero, enviándole una petición de registro, en la cual incluye la dirección IP permanente del host, y la dirección de su agente local.
    3. El agente extranjero entonces ejecuta el proceso de registro para el nodo móvil, mandando una petición de registro con la dirección IP permanente del nodo móvil y la dirección IP permanente del agente extranjero, hacia el agente local.
    4. Cuando el agente local recibe la petición de registro, cambia la relación de movilidad, por medio de la asociación de la dirección de cuidado del agente móvil con su dirección local.
    5. El agente local, entonces, envía un mensaje de recibo al agente extranjero.
    6. El agente extranjero en respuesta, cambia los datos en su lista de visitantes. Incluye una anotación referente al nodo móvil y le manda una respuesta.
    7. Deregistración: Si un nodo móvil desea dejar de usar su dirección de cuidado, entonces tiene que deregistrarse con su agente local. Esto se logra por medio del envío de una Petición de Registro con un valor de cero en el campo de tiempo de vida (life=0). No hay necesidad de desregistrarse con el agente extranjero porque la licencia expira automáticamente cuando el valor se convierte a cero. Sin embargo, si el nodo móvil visita una nueva red, la previa red foránea no sabe la dirección de cuidado de este nodo. Por esta razón, los datagramas ya expedidos por el agente local, al previo agente extranjero, se perderán.

3. **Encaminamiento y Tunneling:** Esta etapa se puede sub-dividir en los siguientes pasos:
    1. Cuando un nodo correspondiente desea comunicarse con el nodo móvil, le envía un paquete IP dirigido a la dirección IP permanente del nodo móvil.
    2. El agente local intercepta este paquete y consulta la tabla de movilidad para averiguar si el nodo móvil se encuentra visitando otra red.
    3. El agente local averigua la dirección de cuidado del nodo móvil, y genera un encabezado IP nuevo, que contenga dicha dirección como la dirección IP de destino del paquete. El paquete original de IP es añadido al payload de este nuevo paquete IP. El agente local, entonces, manda el paquete. Este proceso de encapsular un paquete IP dentro de la carga de otro, se conoce como Encapsulado IP-In-IP, o Tunneling.
    4. Cuando el paquete encapsulado llega a la red donde se encuentra el nodo móvil, el agente extranjero desencapsula el paquete y se entera de la dirección local del nodo móvil. Entonces consulta su lista de visitantes para ver si contiene información acerca de ese nodo móvil.
    5. Si la lista contiene información acerca del nodo visitante, el agente extranjero extrae la dirección del nodo correspondiente y se la entrega al nodo móvil.
    6. Cuando el nodo móvil desea mandar un mensaje a un nodo correspondiente, le envía el paquete al agente extranjero, el cual a su ves le envía el paquete al nodo correspondiente usando enrutamiento IP convencional.
    7. El agente extranjero le ofrece sus servicios al nodo móvil mientras este tiene licencia. Cuando esta licencia expira, si el nodo móvil desea continuar en servicio, tiene que reeditar la Petición de Registro.

3.3 DIFERENCIAS ENTRE IPv4 E IPv6

Son tres las mayores y más importantes diferencias entre IPv4 e IPv6, estas son:

- Encabezado principal IPv6
- Encabezado de extensión IPv6
- Tipos de direcciones IPv6

3.3.1 Encabezados IPv4 e IPv6

A continuación el encabezado de IPv4:

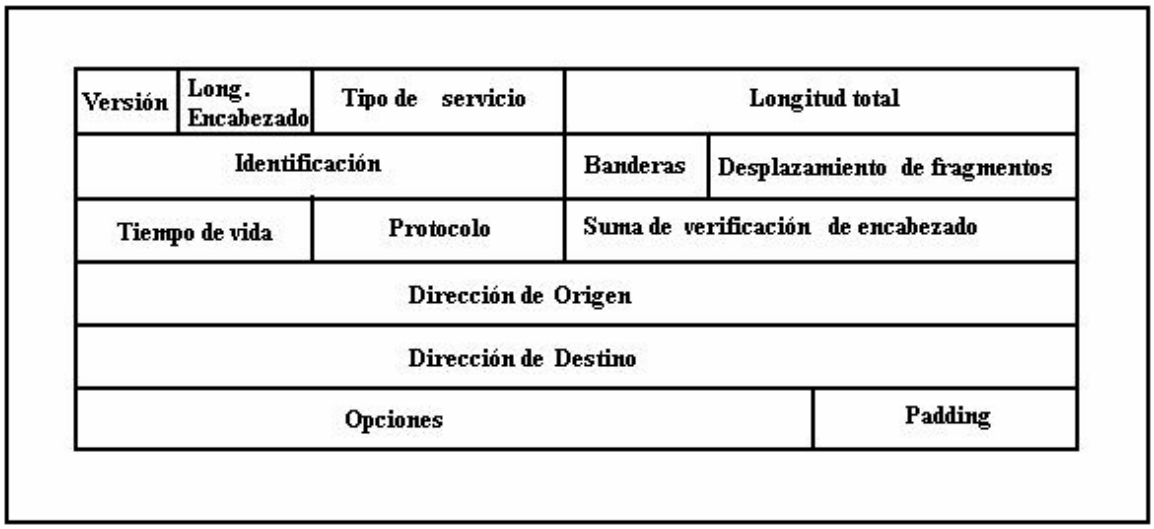

Figura 16. Encabezado de IPv4

Versión (4 Bits): Indica la versión del protocolo IP que está siendo utilizada. Si este campo es diferente en el dispositivo que esta recibiendo los paquetes, este desechará los mismos.

Longitud del encabezado (4 Bits): Este campo se lo conoce como HLEN, e indica la longitud del encabezado del datagrama en palabras de 32 bits, teniendo un máximo de 64 Bytes o 16 palabras. Esta es la longitud total de la información que se encuentra en el encabezado.

Tipo de servicio (8 Bits): Especifica el nivel de importancia que ha sido asignado a un protocolo de nivel superior.

Longitud total (16 Bits): Especifica la longitud del paquete entero expresado en Bytes, incluidos los datos y el encabezado. Para obtener la longitud de los datos (payload) se debe restar HLEN de la longitud total.

Identificación (16 Bits): Contiene un número entero que identifica el datagrama actual.

Banderas (3 Bits): Es un campo de tres bits en el cual los dos menos significativos controlan la fragmentación, el un bit especifica si un paquete puede ser fragmentado y el otro especifica si el paquete es el ultimo que ha sido fragmentado dentro de una serie de paquetes fragmentados.

Desplazamiento de fragmento (13 Bits): Es utilizado para juntar los fragmentos del datagrama.

Tiempo de vida (8 Bits): Conocido como TTL, este campo contiene el número en segundos que indican cuanto tiempo un paquete puede mantenerse en la red. Este número decrece de uno en uno cada vez que el paquete viaja a través de un router, cuando el contador está en cero el paquete es descartado.

Protocolo (8 Bits): Indica que protocolo de capa superior como TCPo UDP recibe los paquetes después de que el proceso de IP ha sido cumplido.

Suma de verificación de encabezado (16 Bits): Detecta errores, y ayuda a asegurar la integridad del encabezado IP.

Dirección de origen (32 Bits): Especifica la dirección IP del nodo de origen.

Dirección de destino (32 Bits): Especifica la dirección IP del nodo de destino.

Opciones: Permite a IP soportar varias opciones como son seguridad y longitud variable.

Padding: Ceros extras son añadidos a este campo para asegurar que el encabezado o header sea siempre múltiplo de 32 bits

Datos: Contiene información de capas superiores, su tamaño varía hasta 64Kb.

A continuación el encabezado de IPv6:

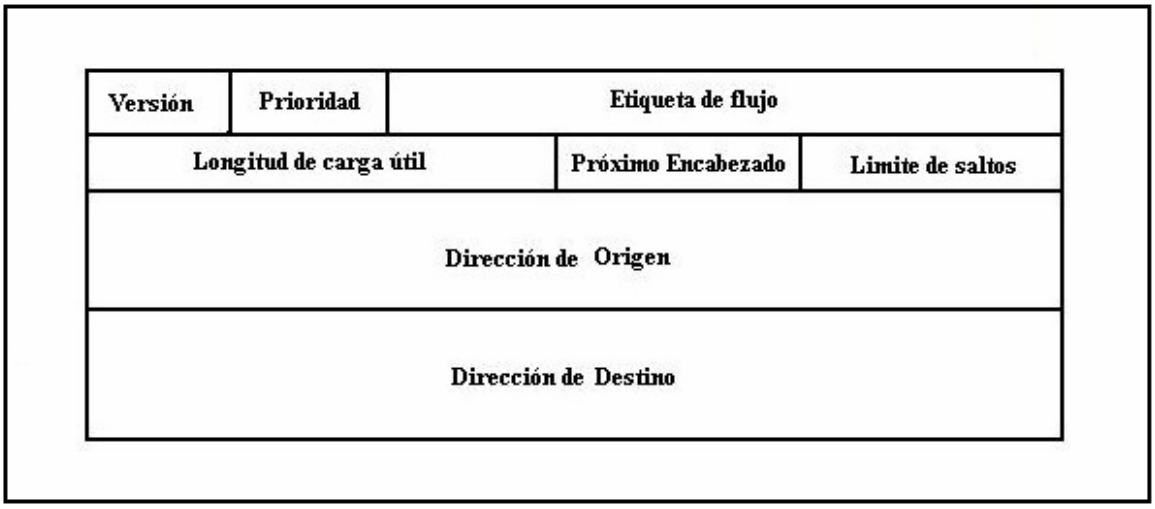

Figura 17. Encabezado principal de IPv6

Versión (4 Bits): Contiene la versión de protocolo IP en este caso es el 6, la versión 5 no puede ser utilizada ya que ha sido asignada a un protocolo experimental.

Clase de trafico o Prioridad (1 Byte): Este campo remplaza al campo de "Tipo de Servicio" en IPv4. Este campo facilita el manejo de datos de tiempo real y cualquier otro tipo de datos que requieran un tratamiento especial. Este campo también puede ser utilizado por nodos y routers para identificar entre diferentes clases o prioridades de los paquetes de IPv6.

Etiqueta de flujo (20 Bits): Este campo distingue paquetes que requieren el mismo tratamiento para facilitar el manejo de trafico en tiempo real.

Longitud de carga útil (2 Bytes): Este campo especifica la longitud del payload o carga útil, solamente contiene los datos que están después del

encabezado de IPv6, los encabezados de extensión son considerados parte del payload y están incluidos en el cálculo. El hecho de que este campo tenga 2 Bytes limita el tamaño de carga útil del paquete a un máximo de 64Kb.

Próximo encabezado (1 Byte): En IPv4 este campo indicaba el “Tipo de Protocolo”, en IPv6 ha sido renombrado con efecto de una nueva organización de paquetes IP. Si el próximo encabezado es TCP o UDP, este campo contendrá los mismos números de protocolo que IPv4, por ejemplo el número 6 para TCP y el número 17 para UDP. Pero si se utilizan encabezados de extensión este campo contiene el tipo del próximo encabezado de extensión. Este encabezado se encuentra entre el header de IP y el header de TCP o UDP. Los números del tipo de encabezado derivan del mismo rango de números como son los números del “Tipo de Protocolo”.

Limite de salto (1 Byte): Este campo es análogo al campo de “Tiempo de Vida o TTL” de IPv4. El valor en este campo expresa el número de saltos o hops y ya no el número de segundos. Cada nodo que reenvía un paquete decrementa este número de uno en uno.

Dirección de origen (16 Bytes): Este campo contiene la dirección IP del nodo origen del paquete.

Dirección de destino (16 Bytes): Este campo contiene la dirección IP del nodo que desea recibir el paquete. En IPv4 este campo siempre contenía la dirección del último destino del paquete, en IPv6 este campo puede no contener la dirección IP del destino final del paquete, si esta presente el “Encabezado de Enrutamiento”.

3.3.1.1 Encabezado de extensión IPv6

Algo fundamental con lo que cuenta IPv6 es un encabezado de extensión el cual se lo muestra en la siguiente figura.

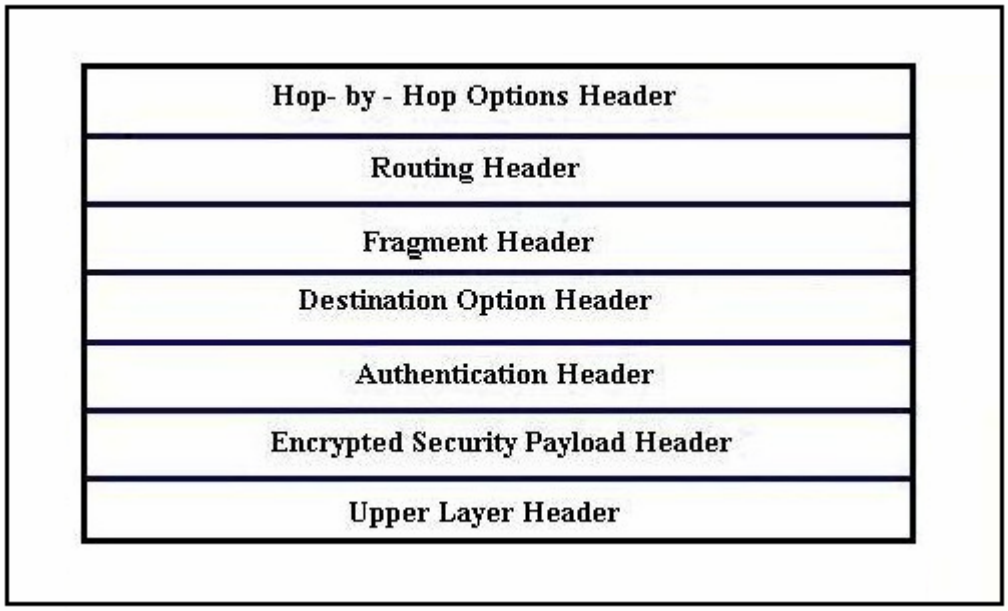

Figura 18. Encabezado de extensión de IPv6

Hop - by - Hop Options Header: Contiene opciones que son examinadas por cada uno de los routers a lo largo de la ruta o path.

Routing Header: Es utilizado en caso de “Enrutamiento de Origen”. Se lo explicara en detalle más adelante.

Fragment Header: Es utilizado por el nodo de origen cuando se envían paquetes más largos que la máxima unidad de transferencia.

Destination Option Header: Contiene opciones que son examinadas por el nodo de destino.

Authentication Header: Es utilizado para proveer autenticación.

Encrypted Security Payload Header: Es utilizado para proporcionar confidencialidad a la parte útil (payload) de IP.

Upper Layer Header: Es para instancias de los encabezados de los protocolos de capas superiores TCP o UDP.

3.3.1.2 Tipos de direcciones IPv6

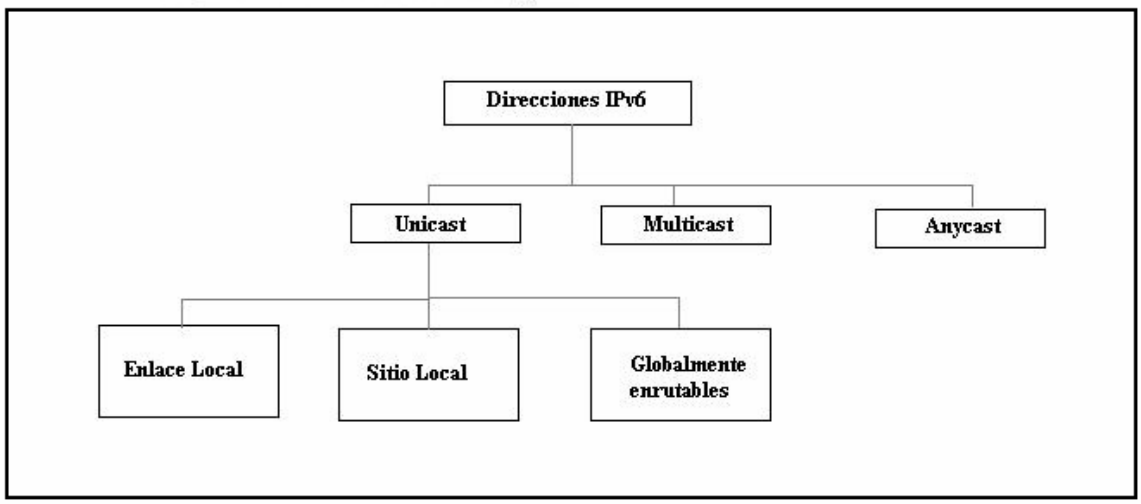

Figura 19. Tipos de direcciones IPv6

Algunas de las características de las direcciones IPv6 son:

- Son asignadas a interfaces lógicas
- Una misma interfaz puede tener varias direcciones

La Figura 19 muestra los tipos de direcciones de IPv6, las mismas que difieren de las direcciones IPv4.

El riesgo de broadcast es un caso especial de las **Direcciones Multicast**. Como resultado, no existe un tipo de dirección de broadcast ya que este no existe.

Por otra parte IPv6 define una **Dirección Anycast** que puede ser vista como una versión especial de las direcciones Multicast. Cuando una dirección Anycast es utilizada, un paquete es enviado a solo un miembro del grupo que tiene dirección anycast.

Existen también las **Direcciones Unicast** que puede ser divididas en tres tipos diferentes de direcciones según su ámbito de acción:

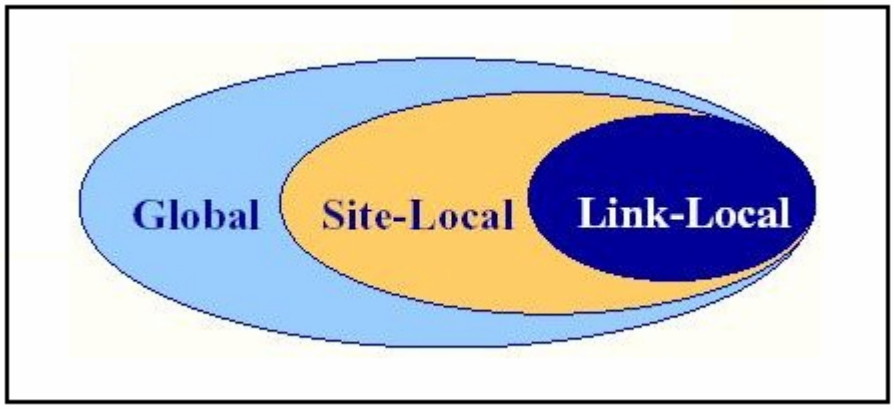

Figura 20. Ambitos de acción de las direcciones IPv6 Unicast

- Direcciones de enlace local o *Link Local Addresses*, las que solo tienen significado dentro del "enlace local". Esto significa que los paquetes que usan "dirección de enlace local" nunca son retransmitidos por routers. Las direcciones de enlace local son utilizadas en caso de Autoconfiguración y Descubrimiento de router "Router discovery"

- Direcciones de sitio local o *Site Local Addresses* que únicamente tienen significado en un sitio local, esto significa que los paquetes que utilizan esta dirección pueden ser reenviados por cualquier router dentro de un mismo lugar, excepto de los routers de salida conectados a la red global de Internet.

- Direcciones globalmente enrutables o *Globally Routable Addresses* que son únicas globalmente.

3.4 PRINCIPALES DIFERENCIAS ENTRE IPv4 E IPv6 EN RELACION AL DISEÑO DE MOBILE IPv6

Las diferencias más importantes entre IPv4 e IPv6 en relación al diseño de MIPv6 son:

- Direcciones más largas las mismas que permiten nuevas técnicas a ser usadas por el nodo móvil para la obtención de su dirección de cuidado, de hecho esto elimina la necesidad de un agente extranjero.

- El nuevo campo “Routing Header” o Encabezado de Enrutamiento, el mismo que permite el uso adecuado del Enrutamiento de Origen, este mecanismo hace posible que un nodo correspondiente pueda enviar paquetes directamente hacia un nodo móvil que se encuentre fuera de su red local, en lugar de utilizar el encapsulamiento IP, que es lo que utiliza MIPv4 para todos sus paquetes. Este encabezado es utilizado para proporcionar una lista de uno o varios nodos intermediarios que pueden ser visitados y que se encuentren en la ruta de destino de los paquetes.

- El nuevo campo “Authentication Header” o Encabezado de Autenticación, el mismo que permite la autenticación de los mensajes de asociación entre el nodo móvil y su dirección local, y el nodo móvil con su dirección de cuidado, estos mensajes son llamados “Binding Messages”.

- El nuevo campo “Destination Option Header” o Encabezado de Opción de Destino, el mismo que permite el uso de opciones sin una degradación significativa del desempeño. Esta degradación en el desempeño ocurre en IPv4 porque cada router a lo largo de la ruta tiene que examinar las opciones a pesar de que ellos solo son destinados a la recepción de los paquetes. Cabe recalcar que este encabezado lleva información opcional que es examinada exclusivamente por el nodo de destino y es utilizada por Mobile IPv6 para informar a varios nodos su dirección de cuidado.

3.5 IP MOVIL VERSION 6 O MOBILE IPv6 (MIPv6)

En las secciones anteriores se ha descrito como opera el protocolo Mobile IPv4 y cuales son sus componentes. El concepto básico de IP Móvil versión 6 es similar al de IP Móvil versión 4.

Hay que mencionar que en esta sección se utilizará cierta nomenclatura diferente que la que se ha venido utilizando, entre estos nuevos términos están:

Prefijo de red o de subred: Es una cadena de bits que consiste de algún número de bits iniciales de una dirección IP.

Enlace local o Home Link: Es el enlace en el cual el prefijo de red del nodo móvil es definido. Formas estándares de enrutamiento IP son empleadas para la entrega de paquetes destinados para la dirección local del nodo móvil y su enlace local.

Enlace extranjero o Foreign Link: Cualquier enlace que no sea el enlace local del nodo móvil.

Binding: Es la asociación de la dirección local de un nodo móvil con la dirección de cuidado para ese nodo móvil, a través del tiempo permitido para dicha asociación.

3.5.1 COMPONENTES DE UNA RED MOBILE IPv6

Un nodo móvil debe determinar su ubicación actual. Cuando un nodo móvil se encuentra en su enlace local este debe actuar simplemente como un host fijo o *Fixed Host*. Cuando un nodo móvil se encuentra en un enlace extranjero, este debe adquirir una dirección de cuidado colocada y notificar esta dirección a su agente local. El nodo móvil también reporta su dirección de cuidado a algunos de sus nodos correspondientes. El último componente de Mobile IPv6 son los paquetes enrutados desde y hasta los nodos móviles.

3.5.2 PROCEDIMIENTOS

Al igual que MIPv4 esta nueva versión funciona realizando algunos procedimientos los cuales se procede a explicar en detalle.

3.5.2.1 ICMPv6 DESCUBRIMIENTO DE ROUTER O R*OUTER DISCOVERY*

La nueva versión del protocolo ICMP, Internet Control Message Protocol, ICMPv6 tiene varias funciones que pueden ser utilizadas por Mobile IPv6.

Estas funciones incluyen:

- Anunciamiento de Router o *Router Advertisements*
- Solicitud de Router o *Router Solicitations*
- Auto configuración de direcciones
- Anunciamiento de Vecino o *Neighbor Advertisement*

3.5.2.1.1 Anunciamiento y solicitud de Router

Un nodo móvil puede determinar su ubicación actual estando atento al Anunciamiento de router y comparando el prefijo de red de su dirección de origen, dentro de este anunciamiento, con el prefijo de red de su enlace local o Home Link (HL). Si el prefijo de red de la dirección de origen dentro del Anunciamineto de Router es igual al prefijo de red de la dirección local del nodo móvil, entonces el nodo móvil se encuentra en su enlace local (HL). De otra manera el nodo móvil está en un enlace extranjero o Foreign Link (FL)

Similarmente el nodo móvil puede detectar su movimiento desde un enlace extranjero (FL) hacia otro cuando el prefijo de red de la dirección de origen, dentro del Anunciamiento de Router, cambia a otro prefijo de red que no es el prefijo de red de su enlace local.

Si el nodo móvil no desea esperar por un Anunciamiento de Router, este puede enviar una Solicitud de Router pidiendo a los routers que envíen un Anunciamiento de Router cuando este así lo desee.

3.5.2.1.2 Auto configuración de direcciones

En el momento en que un nodo móvil entra en una subred o en una red extranjera este puede obtener una dirección IPv6, que en este caso sería una dirección de cuidado colocada, utilizando la autoconfiguración que posee IPv6.

Para obtener una dirección de cuidado el nodo móvil puede utilizar auto configuración de direcciones de dos tipos:

- Stateful
- Stateless

En el primer caso, *Stateful Address Autoconfiguration,* el nodo móvil obtiene una dirección de cuidado de un servidor de direcciones como puede ser un servidor DHCP (Dynamic Host Configuration Protocol) este protocolo permite a un host obtener una dirección IP dinámicamente sin que el administrador de red tenga que setear un perfil individual para cada dispositivo.

En el caso de *Stateless Address Autoconfiguration* el nodo móvil extrae el prefijo de red del anunciamiento de router y lo concatena con la dirección MAC para formar así su dirección de cuidado.

Una ves que la dirección de cuidado es obtenida o formada, esta debe ser identificada como una dirección única o no.

3.5.2.1.3 Anunciamiento de vecino

Cuando el nodo móvil no se encuentra dentro de su enlace local, el agente local debe interceptar los paquetes destinados al nodo móvil. Para habilitar esta intercepción de los paquetes, el agente local debe realizar un multicast de un proceso conocido como Anunciamiento de Vecino “Gratuito” en el enlace local que contenga la dirección local del nodo móvil y su propia dirección MAC. De hecho, el agente local avisa a los nodos en el enlace local que la dirección IP del nodo móvil debe estar asociada con la dirección MAC del agente local, y los

paquetes de destino hacia el nodo móvil son enviados al agente local. El proceso de un que un nodo A permita a otros nodos que asocien la dirección IP de un nodo B con la dirección MAC del nodo A es llamado proceso de Descubrimiento de Vecino o *Neighbor Discovery,* y es utilizado en MIPv6 en reemplazo del ARP que era utilizado en MIPv4.

Cuando el nodo móvil regresa a su enlace local, este debe realizar un multicast de Anunciamiento de Vecino “Gratuito” que contenga su propia dirección MAC y su dirección local.

3.5.2.2 NOTIFICACION

Con el fin de hacer transparente el enrutamiento de paquetes a la dirección de cuidado del nodo móvil, y que son destinados a la dirección local del nodo móvil, tres nuevos procedimientos son introducidos en MIPv6 y son:

- *Binding Update*
- *Binding Acknowledgment*
- *Binding Request*

Estos tres procedimientos son utilizados para la notificación, la misma que se da cuando el nodo móvil informa o notifica a otros nodos (que pueden ser nodos correspondientes) su ubicación actual.

Esto es llevado a cabo cuando un nodo móvil se mueve hacia otro enlace, tal como se muestra en las Figuras 21A y 21B, donde el nodo móvil se mueve hacia un enlace extranjero y notifica su agente local (A) y a su nodo correspondiente (B) de su nueva ubicación. El agente local debe estar informado para ser capaz de enrutar, mediante tunneling, los paquetes destinados al nodo móvil y que llegan al agente local. En MIPv6 es posible que un nodo correspondiente pueda comunicarse directamente con un nodo móvil. Para esto el nodo móvil informa al nodo correspondiente de su ubicación actual mediante su dirección de cuidado. El nodo correspondiente utilizará esta dirección de cuidado como la dirección de destino y enviará sus paquetes directamente al nodo móvil.

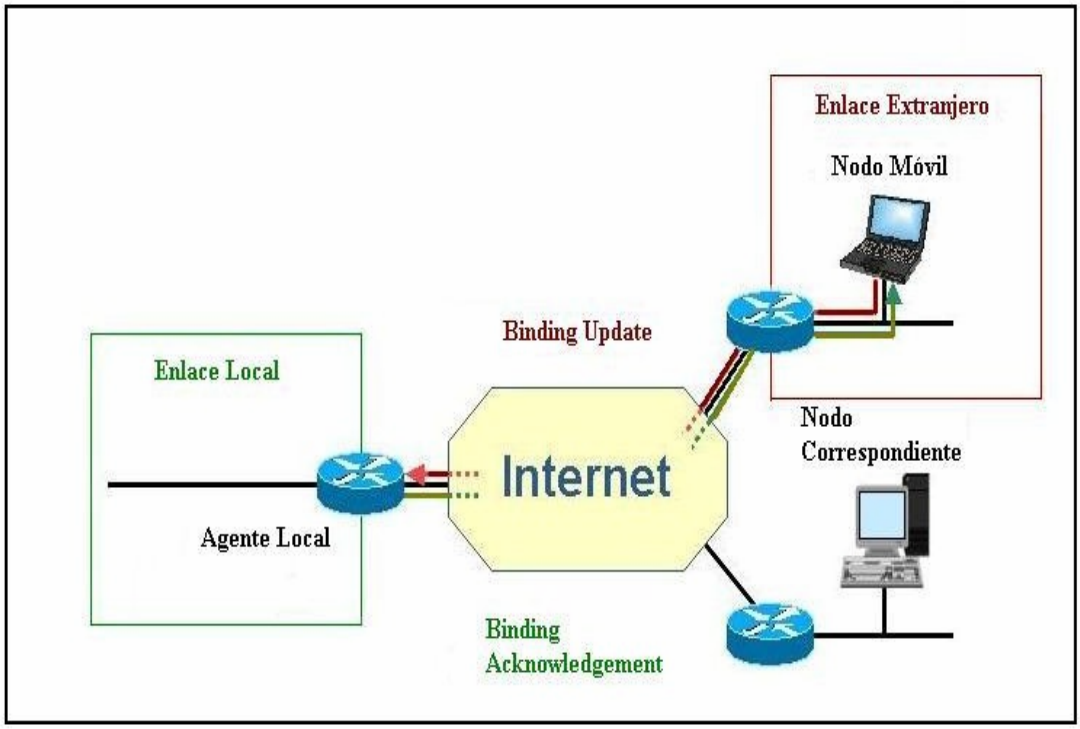

Figura 21 A. Nodo Móvil en un enlace extranjero notificando al agente local

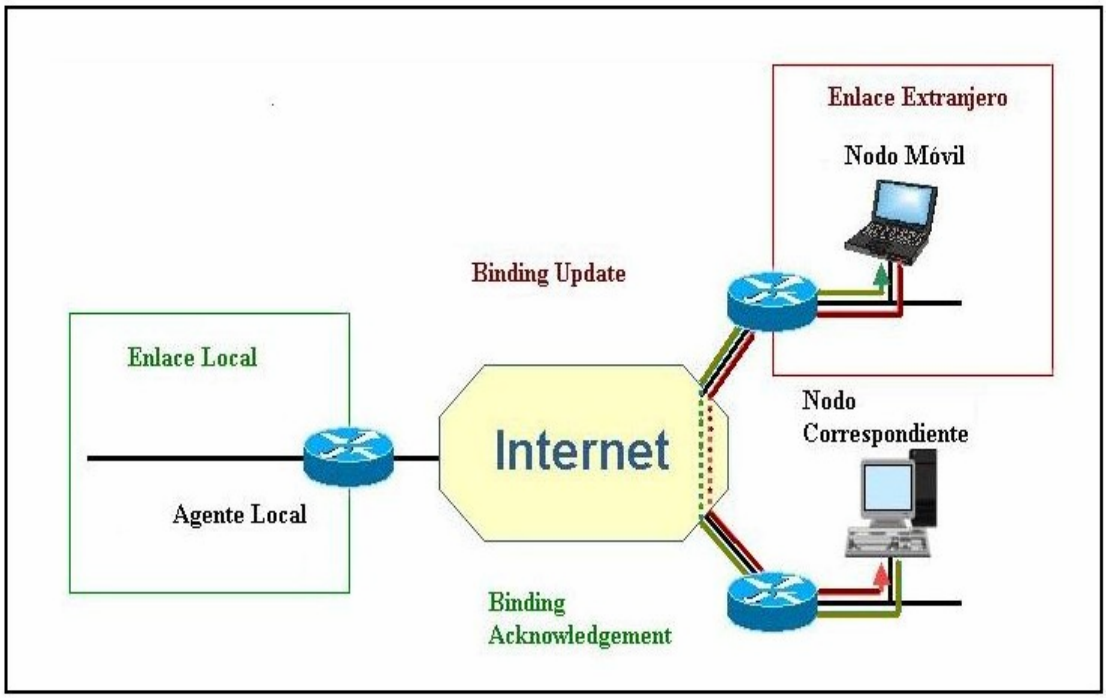

Figura 21 B. Nodo Móvil en un enlace extranjero notificando al nodo correspondiente

En la Figura 22 se muestra que el nodo móvil regresa a su enlace local y notifica a su agente local.

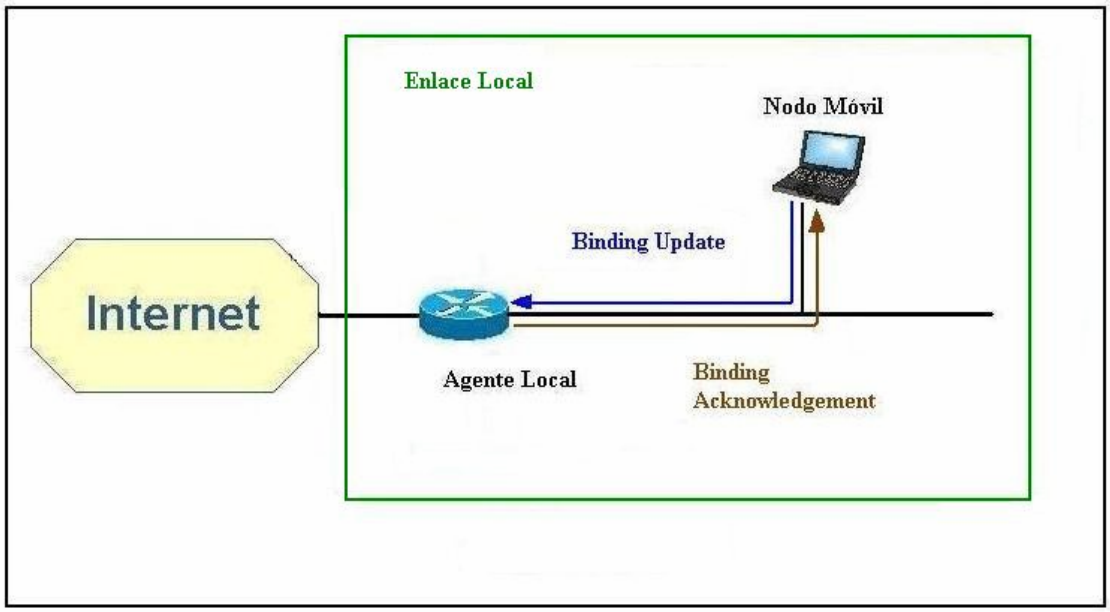

Figura 22. Nodo Móvil de regreso a su enlace local notificando al agente local

Los mensajes de asociación (Binding Messages) son transferidos en uno de los nuevos encabezados de extensión de IPv6, más específicamente en el Encabezado de opción de destino o *Destination Option Header.*

Como ya se ha visto este encabezado contiene información específica que es examinada y procesada únicamente por el destinatario final. Los mensajes de asociación o Binding Messages pueden ser también enviados como paquetes *Stand – Alone*, es decir sin datos de usuario, o pueden ser incluidos dentro de un paquete IPv6 llevando alguna carga útil en su payload, es decir con datos de usuario.

Cuando un nodo móvil se traslada a un nuevo enlace, este envía un mensaje llamado *Binding Update* hacia su agente local y hacia otros nodos correspondientes que se encuentren en su lista, para informarles y darles a conocer su dirección de cuidado. En MIPv6 el agente local puede utilizar encapsulamiento para Tunneling durante el inicio de la fase de Binding Update.

En la Figura 23, se muestra el encabezado, *Destination Option Header,* este contiene la opción de mensaje Binding Update para Mobile IPv6 y consiste en tres bits, A, H, y L y los campos:

- Lifetime
- Identification
- Direccion local del nodo móvil
- Dirección de cuidado

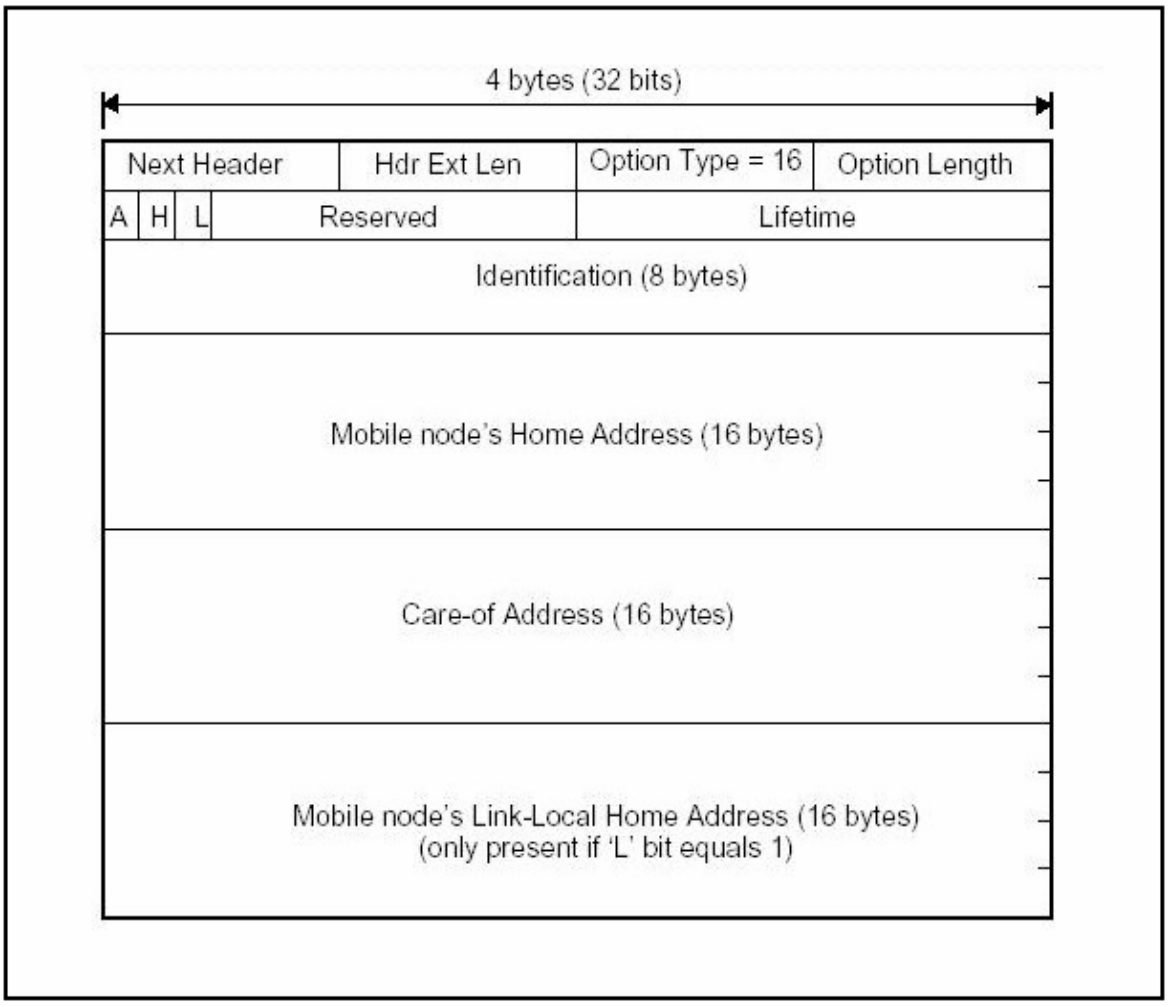

Figura 23. Destination Option Header con la opción Binding Update de MIPv6

El bit A indica si el destino puede reenviar utilizando un mensaje *Binding Acknowledgement* o no.

El bit H es utilizado si el nodo móvil desea que el nodo de destino sea su propio agente local.

El bit L es enviado si el nodo móvil también desea recibir paquetes destinados a su dirección local de enlace local.

Un mensaje llamado *Binding Acknowledgement* es enviado al nodo móvil por su agente local u otro nodo correspondiente para indicar que el *Binding Update* fue exitosamente recibido y si fue o no aceptado. El campo **Status** es utilizado para este propósito y es mostrado en la Figura 24.

Los campos Lifetime (Tiempo de vida), identification (identificación), y dirección local del nodo móvil. Son copiados directamente del mensaje Binding Update recibido. Un campo extra es el campo Refresh, el mismo que indica por cuanto tiempo el destinatario del mensaje Binding Acknowledgement puede guardar o almacenar la dirección de cuidado del nodo móvil. Un mensaje Binding Acknowledgement es requerido si el bit A en el mensaje Binding Update es seteado en 1.

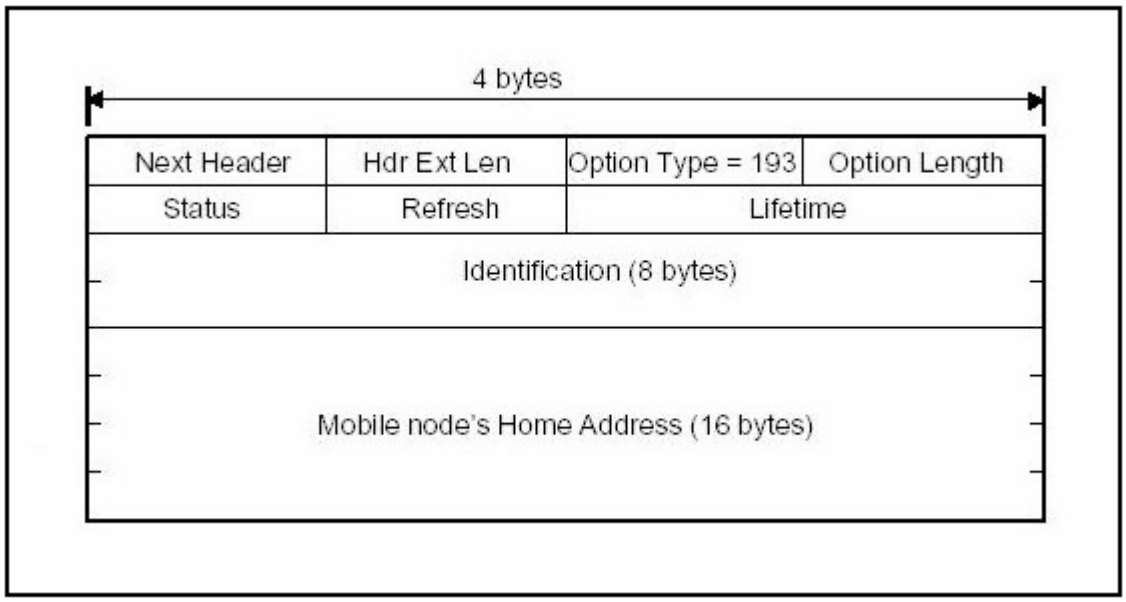

Figura 24. Destination Option Header con la opción Binding Acknowledgement de MIPv6

Si un nodo correspondiente desea saber la dirección de cuidado de un nodo móvil, este envía una petición llamada *Binding Request* a ese nodo móvil. La

única información en este mensaje de petición es la petición propiamente dicha, ya que este mensaje solo tiene los campos de *Tipo de opción* y *Longitud de opción,* como se muestra en la Figura 25. El nodo móvil no necesariamente tiene que responder a esta petición enviando un mensaje Binding Update. La petición es también utilizada para obtener nuevos valores en los campos Lifetime y Refresh, cuando estos expiran o necesitan ser actualizados.

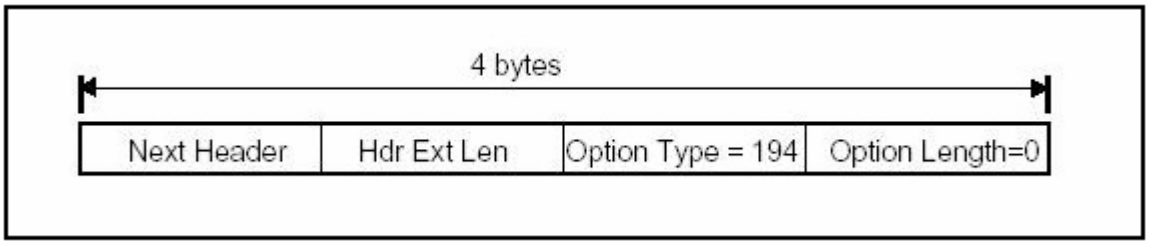

Figura 25. Destination Option Header con la opción Binding Request de MIPv6

3.5.2.3 ENRUTAMIENTO

Como ya se ha mencionado anteriormente una nueva opción que presenta IPv6 y por ende MIPv6 es el encabezado *Routing Header,* este campo contiene una lista de destinatarios intermedios a los cuales el paquete puede visitar a lo largo de su camino hacia la dirección final, la misma que es la dirección local del nodo móvil, y que se indica como Address [1] en el encabezado de enrutamiento mostrado en la Figura 26.

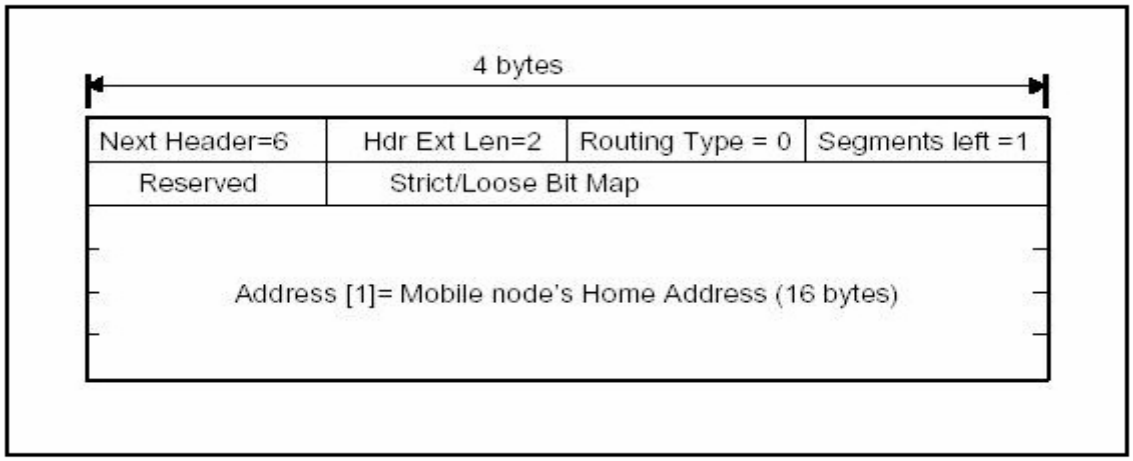

Figura 26. Encabezado de Enrutamiento o Routing Header

La actual dirección de cuidado del nodo móvil es utilizada como un destinatario intermedio, desde que la dirección de cuidado es colocada por el propio nodo móvil. Entonces, la dirección de cuidado del nodo móvil es utilizada como una dirección de destino. Ningún otro nodo reacciona ante el paquete a excepción del destinatario. Ya en su destino el nodo móvil ve su dirección local en el encabezado de enrutamiento o *Routing Header* y obtiene el paquete.

Si el nodo correspondiente conoce la dirección de cuidado del nodo móvil, este puede enviar paquetes directamente hacia el nodo móvil utilizando el encabezado de enrutamiento. Si el nodo correspondiente desconoce la dirección de cuidado del nodo móvil, este enviará los paquetes tal como se lo realiza en MIPv4 es decir utilizando la dirección local del nodo móvil como dirección de destino y los paquetes serán enviados al agente local, el mismo que los encapsulará y los enviara por medio de tunneling hacia la posición actual del nodo móvil, luego de recibir los paquetes. Luego de recibir los paquetes vía su agente local el nodo móvil sabrá que el nodo correspondiente no conoce su actual dirección de cuidado. En este caso en MIPv6 es posible, que el nodo móvil pueda considerar el envío de un mensaje Binding Update hacia el nodo correspondiente para informarle su actual dirección de cuidado, entonces de esta manera el nodo correspondiente podrá enviar paquetes directamente hacia el nodo móvil.

Un nodo móvil puede generar y enviar paquetes hacia cualquier router dentro de su enlace local si el mismo recibe un mensaje de aviso de router previamente. La tabla de enrutamiento en el nodo móvil es configurada de tal manera que el nodo móvil pueda enviar todos estos paquetes hacia ese router, el mismo que podrá reenviar los paquetes hacia el destino correcto.

3.5.2.4 DESCUBRIMIENTO DINÁMICO DE DIRECCIÓN DE AGENTE LOCAL O DYNAMIC HOME AGENT ADDRESS DISCOVERY.

Los nodos en una red IPv6 pueden ser reconfigurados y esto puede suceder si el nodo que está funcionando como agente local de un nodo móvil no está activo o es removido del enlace. En este caso es posible por parte del nodo móvil obtener dinámicamente la dirección de otro nodo que se encuentre en el enlace

local y que pueda funcionar como el nuevo agente local del nodo móvil. Esto es llevado a cabo con la opción existente en IPv6 llamada *Dynamic home agent address discovery* o Descubrimiento dinámico de dirección de agente local.

Para esto el nodo móvil construye un paquete destinado a todos los nodos dentro de su enlace local (direcciones multicast) en donde el bit H del mensaje Binding Update esté activado. Este paquete es encapsulado en otro paquete, que tiene como dirección de destino la dirección anycast de subred, la misma que va a ser entregada a cualquier router del enlace local. Una vez recibido este paquete, el router lo desencapsula y lo envía como multicast a todos los nodos de ese enlace. Todos los nodos que cuenten con la disponibilidad de ser agentes locales responderán al mensaje Binding Update enviando un mensaje Binding Acknowledgement en donde ellos rechazan la petición del nodo móvil, ya que ellos recibieron la petición dentro de un paquete de multicast. El paquete de Binding Acknowledgement de todas formas contendrá una dirección IPv6 unicast globalmente enrutable de cada nodo. El nodo móvil recolectará estas direcciones y seleccionará a uno de los agentes locales al cual enviar directamente un mensaje Binding Update subsecuente. Este momento el nodo aceptará la petición del nodo móvil de ser su nuevo agente local.

3.5.3 SEGURIDAD

A diferencia de MIPv4 el nuevo protocolo Mobile IPv6 utiliza protocolos de seguridad conocidos como IP-Sec y son implementados utilizando encabezados opcionales para proveer autenticación, y lo que es conocido como ESP, Encapsulating Security Payload. Con IP-sec es posible también brindar protección de integridad de datos, etc. Hay que recordar que en MIPv4 los requerimientos de seguridad se proveían mediante sus propios mecanismos de seguridad para cada función, basados en configuraciones estáticas.

3.5.4 DESPLIEGUE DE IPv6 EN REDES DE TERCERA GENERACION

Durante los últimos años, la telefonía móvil ha supuesto una verdadera revolución que ha hecho que los principales operadores y fabricantes inviertan

gran cantidad de recursos para desarrollar redes móviles de 3G. Al mismo tiempo, el desarrollo de Internet ha despertado grandes expectativas tanto para las empresas de servicios como para los usuarios que cada vez demandan servicios más avanzados tales como VoIP, videoconferencia, etc, que se ofrecen actualmente en redes fijas.

Los usuarios de telefonía móvil comienzan a demandar tecnologías que les permitan estar permanentemente conectados a dichas redes.

Para cubrir estas necesidades las arquitecturas de telefonía han ido migrando hacia sistemas basados en backbones IP a los que se conectan diferentes tecnologías radio como por ejemplo UMTS.

A este modelo se le conoce como el modelo "All-IP". Para ofrecer un mayor abanico de servicios se estudia la posibilidad de que incluso los nodos finales dispongan de direccionamiento IP que les permita estar siempre conectados a la red.

Con la gran cantidad de terminales móviles que podría haber, el uso de IPv6 como protocolo de red se convierte en una necesidad más que en una opción. A su vez, se hacen necesarios nuevos protocolos que faciliten la movilidad de terminales a nivel de red y nuevos mecanismos que permitan realizar handoffs eficientes.

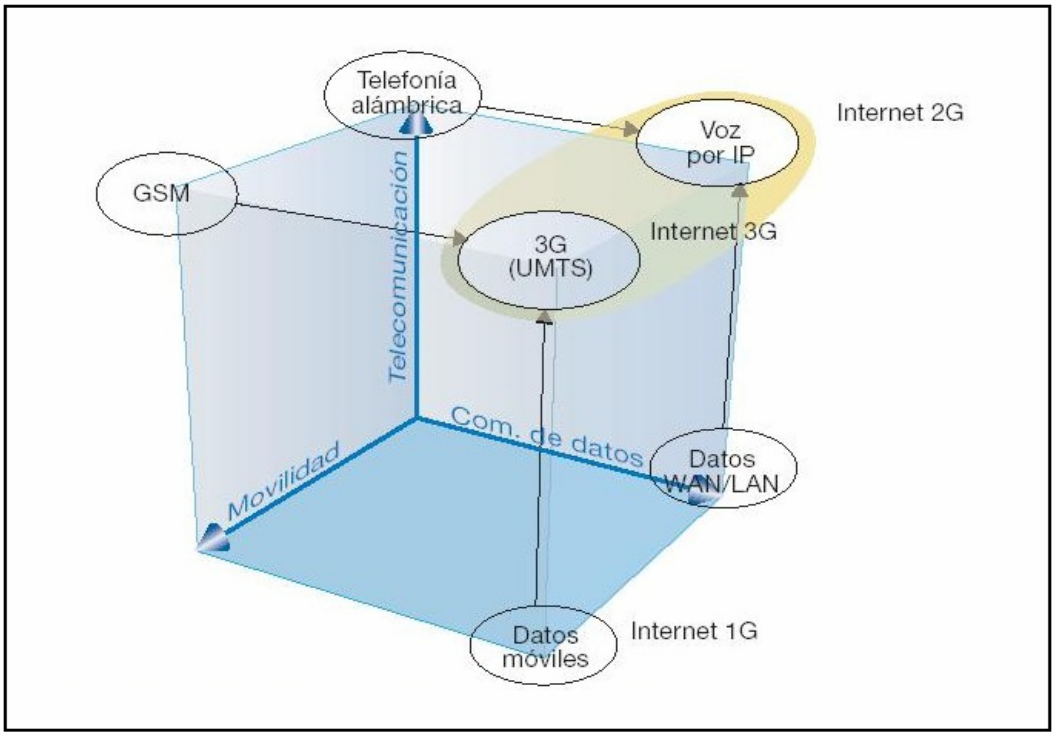

Figura 27. IPv6 en el nuevo mundo de las telecomunicaciones

La Figura 27 nos muestra como se desenvuelve IPv6 en diferentes tipos de redes de última generación, es por esta razón que la Tercera Generación móvil utiliza masivamente el protocolo IPv6 ya que presenta muchas ventajas sobre su predecesor como ya se ha mencionado en las secciones anteriores.

Para dar algunos ejemplos, actualmente la arquitectura 3GPP (3rd Generation Partnership Project), de la que se hablará en detalle en el siguiente capítulo, utiliza IPv6 para su *Subsistema multimedia IP*, IMS, por sus siglas en inglés. Todos los elementos de IMS se basan exclusivamente en IPv6, y ambos, el protocolo de señalización y el flujo de datos en el medio son conducidos solo por IPv6. Otros sistemas como 3GPP2 tienen arquitectura basadas en IPv4 pero se están haciendo grandes esfuerzos para que estas arquitecturas soporten IPv6. También redes WLAN aparecen como las plataformas más efectivas para el desarrollo de IPv6 y ya se encuentran instaladas.

CAPITULO IV

INTEGRACION DE MOBILE IP CON TECNOLOGIAS DE TERCERA GENERACION: UMTS Y CDMA2000

4.1 INTRODUCCION A TERCERA GENERACION

En los últimos años las comunicaciones inalámbricas y principalmente las tecnologías celulares y de Internet se han desarrollado ampliamente en todo el mundo, incluido nuestro país. Este desarrollo implica la fusión de estas dos tecnologías, la comunicación móvil y el Internet.

Mirando un poco hacia atrás, se aprecia que la industria de comunicaciones móviles ha evolucionado en tres etapas, con cada generación más fiable y flexible que la anterior.

La primera generación (1G) fue analógica y limitada en capacidad de roaming, permitía solamente llamadas de voz con baja calidad y los teléfonos se diseñaron para uso en vehículos. AMPS o Advanced Mobile Phone Service fue el principal standard de Primera Generación y se desarrolló entre 1982 y 1992. El sistema analógico empleado en Europa, fue TACS o Total Access Communications System, y estaba basado en AMPS.

La Segunda Generación móvil 2G, corresponde a los sistemas actualmente en uso como GSM o Globlal Sistem for Mobile Communications (apoyado por el ETSI), cdmaOne (apoyado por el ANSI) y TDMA, también llamado D-AMPS por

ser la versión digital de AMPS. Son sistemas digitales con técnicas avanzadas de uso del espectro radioeléctrico y con capacidades de roaming mejoradas. Se basan en un ancho de banda de 9,6 Kbps para datos y fax. Significa un incremento en la capacidad de la red, reducción de tarifas y los primeros servicios de valor añadido, como son los mensajes cortos SMS.

A la generación intermedia entre la 2G y la 3G se la denomina 2.5G, y corresponde a mejoras tecnológicas en las redes 2G las cuales tienden a entregar capacidades casi de tipo 3G, con una velocidad que puede llegar hasta los 384 Kbps, ya adecuada para muchas aplicaciones.

La actual generación de comunicaciones móviles, llamada 3G, está pensada para roaming global, transmisión de datos a alta velocidad a través de técnicas avanzadas de conmutación de circuitos y de paquetes, soporta tecnología IP (y ATM) lo que posibilita el acceso a Internet, y en general aplicaciones multimedia móviles, con servicios personalizados y basados en la localización de los usuarios.

Una vez realizado este resumen cronológico de las tecnologías celulares, podemos afirmar que la actual evolución de los sistemas celulares 2G hacia una red 2.5G o 3G esta directamente relacionada con Internet Móvil y por ende al protocolo IP Móvil. En tal grado que el protocolo IP adquiere un peso cada vez más relevante como protocolo para el transporte, no sólo de contenidos (voz, datos, etc.), sino también de información de control y señalización, hasta tal punto que puede decirse que 3G es una red que tiende a ser "Todo IP" o “All IP”.

Es así como en la actualidad se están diseñando redes para proveer servicios de Internet de alta velocidad y servicios multimedia de banda ancha en tiempo real a abonados móviles utilizando tecnologías inalámbricas de Tercera Generación (3G).

Es así que la ITU inicio el camino para la estandarización de los sistemas de comunicaciones de Tercera Generación, 3G, creando el estándar IMT-2000, o

Sistema Internacional de Telecomunicaciones Móviles, por sus siglas en inglés. El mismo que está definido por un grupo de recomendaciones de las series M, F, G y Q, y agrupa una familia de sistemas con capacidades y servicios 3G cuya puesta en servicio en Europa y Japón se ha venido dando desde el año 2002.

IMT-2000 entendida sobre la base de sistema de Tercera Generación y su futura evolución, viene a consolidar y unificar los diversos e incompatibles ambientes móviles de hoy a una infraestructura de red y radio capaz de ofrecer un amplio rango de servicios a escala global. Proporciona acceso a servicios de telecomunicaciones prestados por las redes fijas de telecomunicaciones como es la RDSI y a otros servicios específicos de los usuarios móviles. IMT-2000 abarca una gama de servicios y terminales móviles, enlazados a redes terrenas o satelitales, y los terminales pueden ser diseñados para uso móvil o fijo, para ambientes tanto profesional como doméstico, públicos o privados.

Para asegurar el éxito de los servicios 3G, se ha de proporcionar a los usuarios unas comunicaciones muy eficientes, con una alta velocidad y calidad y, además, fáciles de utilizar. Los sistemas de 3G deben ofrecer:

- Transmisión simétrica/asimétrica de alta fiabilidad.
- Uso de ancho de banda dinámico, en función de la aplicación.
- Velocidades binarias mucho más altas: 144 Kbps en alta movilidad, 384 Kbps en espacios abiertos y 2 Mbps en baja movilidad.
- Soporte tanto de conmutación de paquetes (IP) como de circuitos.
- Soporte IP para acceso a Internet (navegación WWW), videojuegos, comercio electrónico, vídeo y audio en tiempo real.
- Diferentes servicios simultáneos en una sola conexión.
- Calidad de voz como en la red fija.
- Soporte radioeléctrico flexible, con utilización más eficaz del espectro, con bandas de frecuencias comunes en todo el mundo.
- Personalización de los servicios, según perfil de usuario.
- Servicios independientes de la posición (localización) del usuario.
- Incorporación gradual en coexistencia con los sistemas actuales de 2G.

- Roaming, incluido el internacional, entre diferentes operadores y tipos de redes.
- Ambientes de funcionamiento marítimo, terrestre y aeronáutico.
- Capacidad de terminales, multibanda y multientorno.
- Economías de escala y un estándar global y abierto que cubra las necesidades de un mercado de masas.
- Provisión de un *Ambiente Local Virtual*, VHE: el usuario podrá recibir el mismo servicio independiente de su ubicación geográfica.

Existen razones evidentes que explican la necesidad de introducir la 3G: por una parte está la capacidad de las redes móviles actuales que permiten albergar un número limitado de usuarios, con un patrón de consumo similar al actual, y en cuanto se sobrepase la congestión de la red se manifiesta de manera insoportable para los usuarios; por otra parte, tenemos el incremento de tráfico motivado por la sustitución del tráfico fijo por el móvil, en cuanto el costo de las llamadas se reduzca y los hábitos de los usuarios se modifiquen, necesitándose entonces más espectro; y, por último, por la aparición de nuevos servicios, muchos de ellos personalizados, donde la convergencia con Internet y el aumento de aplicaciones multimedia significará un aumento significativo de tráfico.

Las tecnologías que se utilizan como interfaces aire entre las radiobases y los terminales móviles se las conoce como RTT (Radio Transmisión Technology) y fueron aprobadas por la ITU las siguientes:

- IMT-2000 CDMA Direct Spread (UTRA WCDMA)
- IMT-2000 CDMA Multi – Carrier (cdma2000)
- IMT-2000 CDMA TDD (UTRA TD-CDMA)
- IMT-2000 TDMA Single – Carrier (UWC-136)
- IMT-2000 FDMA/TDMA (DECT)

Las distintas interfaces aire propuestas por la ITU están basadas en CDMA con tres modalidades de operación, cada una de las cuales puede funcionar sobre la red base de GSM y sobre la red base de cdmaOne.

Actualmente existen dos grandes tendencias mundiales que dominan el mercado, estas son: TDMA/CDMA desarrollado por TIA (Telecommunications Industry Association) en Estados Unidos y GSM desarrollado por ETSI (European Telecommunicactions Standards Institute) en Europa.

Encaminados hacia el desarrollo de los sistemas 3G, recientemente la industria global de comunicaciones móviles ha creado dos nuevos consorcios empresariales que son:

1. **Proyecto conjunto de Tercera Generación o 3rd Generation Partnership Project (3GPP):** El mismo que desarrolla estándares 3G basados en sistemas GSM. Actualmente el principal estándar desarrollado por 3GPP es conocido como UMTS o WCDMA debido a que es este el interfaz de aire que utiliza.

Los socios organizativos actuales (que por definición se reconocen como SDOs) son:

- Association of Radio Industries and Businesses (ARIB), Japón
- Telecommunication Technology Committee (TTC), Japón
- Telecommunications Technology Association (TTA), Corea
- China Wireless Telecommunication Standard (CWTS), China
- Committee T1, Estados Unidos
- European Telecommunications Standards Institute (ETSI)

2. **Proyecto conjunto de Tercera Generación 2 o 3rd Generation Partnership Project 2 (3GPP2):** Quienes desarrollan estándares 3G basados en el estándar IS-95, es decir basados en sistemas CDMA. En la actualidad el principal estándar desarrollado por 3GPP2 es CDMA2000.

Los socios organizativos actuales son:

- Association of Radio Industries and Businesses (ARIB), Japón

- Telecommunication Technology Committee (TTC), Japón
- Telecommunications Technology Association (TTA), Corea
- China Wireless Telecommunication Standard (CWTS), China
- Telecommunications Industry Association (TIA), Estados Unidos

Quizás el aspecto más importante dentro de esta nueva red 3G es el de la movilidad en los terminales, y al ser esta una red con tendencia “All-IP” podemos afirmar que la base del soporte de movilidad en la red 3G es el protocolo Mobile IP.

4.2 NUEVAS CARACTERISTICAS DE IP PARA EL ENTORNO 3G

La evolución hacia las redes de Tercera Generación plantea un gran número de nuevos retos para la familia de protocolos IP, tales como:

- La necesidad de técnicas de conmutación más rápidas, capaces de soportar servicios multimedia cada vez más complejos y con mayores requisitos de ancho de banda.

- Implementación de mecanismos de calidad de servicio (QoS) que permitan transportar de forma diferenciada los distintos tipos de tráfico que va a soportar el protocolo IP: tráfico de gestión, tráfico de señalización y control, tráfico de usuarios con distintos requisitos de retardo, integridad de los datos, etc.

- Los problemas derivados de la movilidad de los usuarios, con las dificultades de encaminamiento que supone poder conectarse a la red en puntos de acceso muy distintos y la necesidad de ser localizado siempre con la misma dirección IP.

- La falta de espacio de direccionamiento IP que se deriva de la expansión exponencial de Internet y de los usuarios "A*lways On*".

- Necesidades de seguridad.

Estos nuevos retos han hecho necesaria una evolución de IP. Algunos de los problemas han encontrado solución en mecanismos adicionales que han venido a completar a IPv4, tales como *Diff Serv* para calidad de servicio, Mobile IP para la movilidad de los usuarios, IPSec para la seguridad o MPLS para aumentar el rendimiento de las redes de transporte.

4.3 INTEGRACION DE MOBILE IP CON UMTS

4.3.1 INTRODUCCIÓN

La evolución de las redes móviles hacia UMTS se producirá en varias fases hasta alcanzar el objetivo final que es una red integrada de servicios avanzados multimedia, independientes de la posición del usuario. En este proceso, las directrices básicas son dos:

1. La separación de los planos de transporte y servicio, que permitirá desarrollar nuevas aplicaciones, independizándolas de la red de transporte o de la tecnología de acceso. Esto es fundamental para el desarrollo de servicios integrados en tiempo de mercado. Asimismo, en el plano de transporte, se tenderá a la separación de las funcionalidades de conectividad o conmutación y de control.

2. Utilización de IP como protocolo de transporte a todos los niveles, tanto de datos como de señalización, hasta llegar a una red *"Todo I*P".

Otra constante a considerar en la evolución será la integración e interoperabilidad con otras redes, como la PSTN y las redes de Segunda Generación.

En la siguiente figura se puede ver mejor el panorama de la evolución hacia UMTS, dentro de este camino nos encontramos con la tecnología GPRS (General Packet Radio Service) de la cual cabe recalcar que en muchos países incluido el Ecuador está siendo utilizada y al ser algo tan popular alrededor del mundo es

importante incluirla dentro de esta sección a pesar de que esta tecnología no sea de Tercera Generación sino de la llamada 2.5G, pero si una parte importante en el camino hacia la misma.

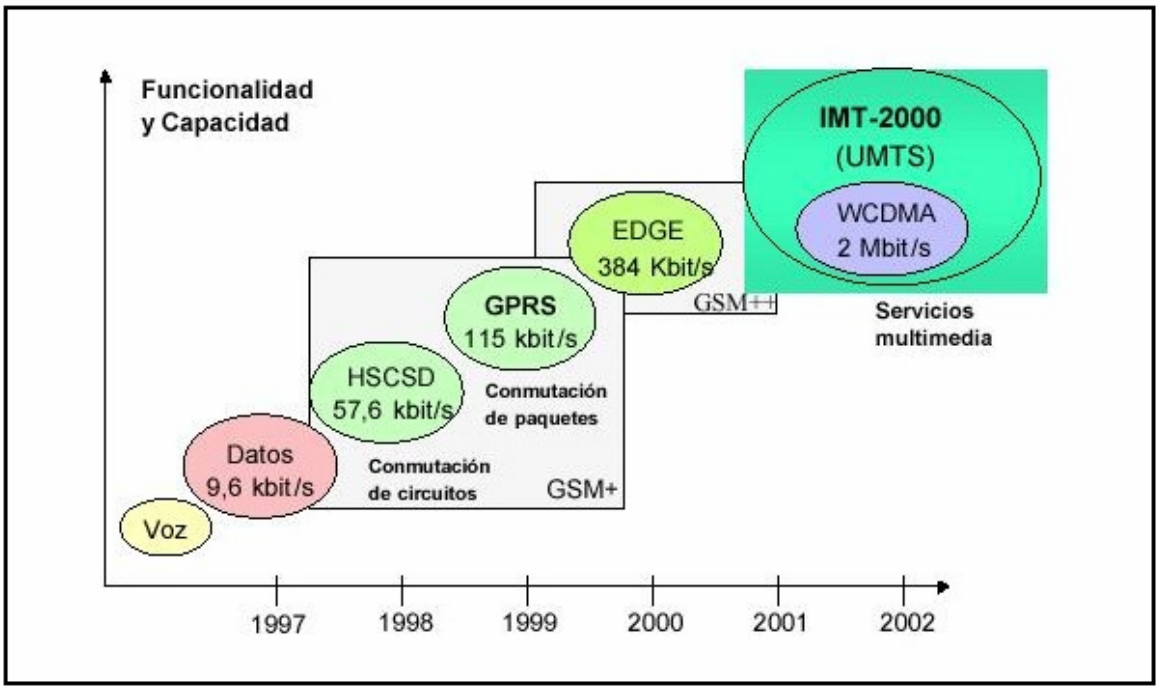

Figura 28. Evolución desde GSM hacia IMT-2000

A continuación se describe la fase previa a UMTS, haciendo énfasis en el sistema GPRS, y las tres fases previstas en la evolución de UMTS, con los avances más significativos de cada una de ellas.

4.3.2 HSCSD (High Speed Circuit-Switched Data)

HSCSD aumenta la capacidad de transmisión de GSM agrupando hasta 8 time-slots de un canal, con velocidades de Nx9,6 kbps con valores de N desde 1 hasta 8. Los canales de tráfico deben usar y emplear las mismas secuencias de Training y Frecuency Hopping. Así, HSCSD puede transmitir hasta 57,6 kbps en modo de conmutación de circuitos. Aquí el número de timeslots utilizados puede ser variable dependiendo de la saturación de la celda donde se encuentre el móvil pero el ancho de banda no se utiliza eficientemente, pues se trata de conmutación

de circuitos. Aunque requiere pocas inversiones en red, no parece ser muy adecuado y su adopción no se está llevando a cabo, salvo en contadas ocasiones.

4.3.3 GPRS (General Packet Radio Service)

GPRS básicamente añade conmutación de paquetes de datos a todos los niveles de la red GSM (radio, nodos de conmutación, red de transmisión, tarifación, etc) optimizando, de este modo, la utilización de los canales radio para el tráfico en ráfagas (por ejemplo, la navegación por Internet) y facilitando un uso más eficaz de los recursos de la red, de manera que:

- El canal radio sólo se mantiene mientras dure la transferencia de datos, liberándose a continuación.

- El canal físico puede ser compartido hasta por ocho usuarios y, para comunicaciones que requieran mayor ancho de banda, el número de canales puede ampliarse también hasta ocho.

El tipo de codificación empleada en el canal radio depende de la calidad de este canal. A peor calidad, se emplearán las codificaciones de menor velocidad de transmisión, pero que tienen mayor fiabilidad. Si las condiciones del canal son óptimas, se alcanzarán hasta 21,4 Kbps por timeslot, de modo que utilizando el número máximo de ocho timeslots o canales por usuario, se pueden lograr tasas máximas de 171 Kbps.

GPRS no utiliza las centrales de conmutación GSM para el transporte de datos, sino que las radio bases llamadas Estaciones Base Terminales o BTSs (Base Terminal Stations) están directamente conectadas a la red IP a través de dos nuevos tipos de servidores, también denominados *Nodos de soporte GPRS* o GSN *(GPRS Support Node*s):

- Nodo de Soporte de Servicio GPRS o SGSN *(Serving GPRS Support Node*)

- Nodo de Soporte de Gateway GPRS o GGSN *(Gateway GPRS Support Node*).

En el transporte de voz se siguen utilizando los mecanismos GSM convencionales.

Los nodos GSN son los responsables de la conmutación y el enrutamiento de los paquetes entre los nodos móviles y las redes de datos externas (PDN, *Packet Data Network*s). Estos nodos interoperan estrechamente con el Registro de Ubicación de Origen o HLR *(Home Location Register*), con el Centro de Conmutación Móvil o MSC *(Mobile Switching Center*), con el Registro de Ubicación de Visitantes o VLR *(Visitor Location Register*) y con el Subsistema de estaciones base o BSS *(Base Station Subsystem*), pertenecientes a la red GSM. En la Figura 29 puede verse la interrelación entre los componentes del sistema según la arquitectura de GPRS.

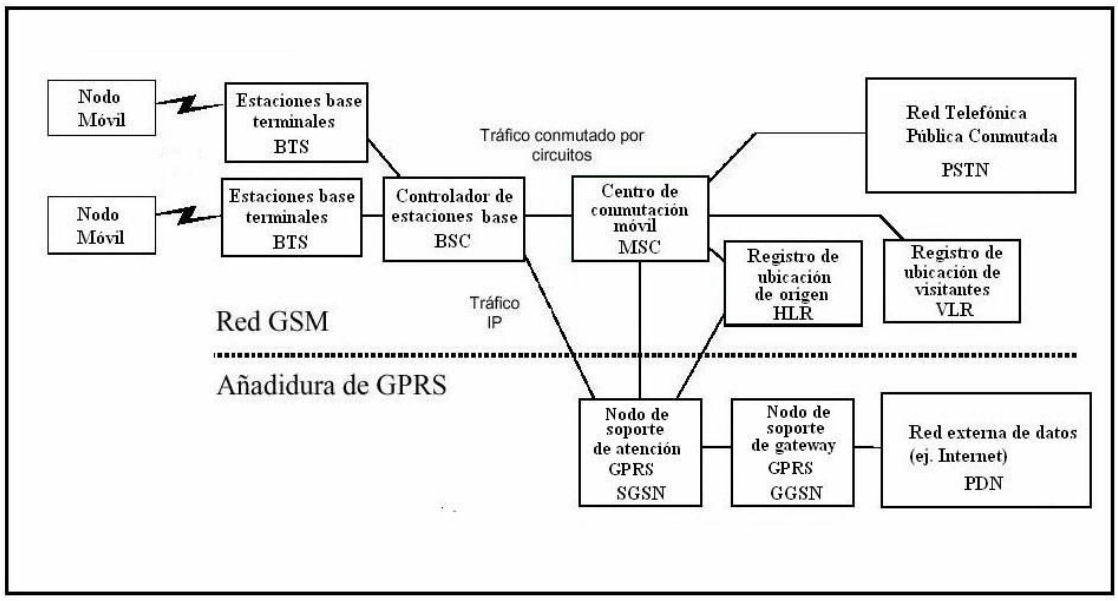

Figura 29. Arquitectura GSM / GPRS

Las funciones de los nodos GSN son:

4.3.3.1 SGSN

El *Serving GPRS Support Node* (SGSN) es el nodo de conmutación de paquetes y se sitúa en el mismo nivel jerárquico que las MSCs en GSM. Este nodo es el responsable de la gestión de la conexión del terminal móvil a la red GPRS *(GPRS Attac*h), lo que implica funciones de:

- Control de acceso a la red GPRS mediante el intercambio de información con el HLR, donde se encuentra el perfil de suscripción del usuario.

- Gestión de la localización y de la movilidad del usuario.

- Selección del nodo GGSN más apropiado para iniciar una sesión con la red de datos (Internet, red corporativa, etc.). El paso previo al establecimiento de la sesión es la activación del denominado contexto PDP (*Packet Data Protocol*). Durante esta fase, el SGSN y el GGSN negocian los parámetros necesarios para que la conexión entre el terminal móvil y la PDN pueda establecerse. La sesión permanecerá mientras el contexto PDP esté activo.

- Encaminamiento y transferencia de paquetes entre las MSs y el GGSN.

- Generación de registros de tarifación denominados CDRs *(Call Detail Record*s).

4.3.3.2 GGSN

El *Gateway GPRS Support Node* (GGSN) actúa como interfaz con la red externa de datos. Si se toma como referencia uno de los dos sentidos, el GGSN convierte los paquetes GPRS, provenientes del SGSN, en el formato correspondiente a la red externa de datos, efectuando después el envío de los mismos. En lo que respecta al sentido contrario, redirecciona los paquetes que llegan de las redes externas y los envía al SGSN que corresponda. Todo esto

implica funciones de direccionamiento y enrutamiento. El GGSN también se ocupa de tareas de autenticación para el acceso a las PDNs y de la generación de los CDRs.

El GGSN también se ocupa de tareas de autenticación para el acceso a las PDNs y de la generación de los CDRs.

4.3.4 EDGE (Enhanced Data-rates for GSM Evolution)

También llamado GSM384, utiliza un esquema de modulación y codificación alternativo que alcanza hasta 384 kbps, o sea 48 kbps por timeslot GSM. Tiene aplicación en ambiente urbano con movimientos lentos o casi estacionarios. Se acerca a las velocidades IMT-2000 (particularmente en exteriores), por lo que es una buena opción para aquellos operadores GSM que no han conseguido una licencia UMTS.

Luego de esta fase que es generalmente conocida únicamente como GPRS vienen tres fases fundamentales para llegar finalmente a UMTS estas son:

4.3.5 RELEASE 99 DE UMTS

Release 99 (R99) es un estándar firmemente establecido y será el que se utilice en el despliegue inicial de UMTS en todas las operadoras europeas. Conserva la estructura de la red GSM/GPRS, con la separación de los dominios de circuitos y paquetes, por lo que no introducirá cambios significativos en el *Core Network* o Núcleo de red, introducido en GPRS.

En la R99, y a diferencia de GPRS, aparece la nueva interfaz radio con la creación de la Red terrestre de acceso por radio UMTS o *UMTS Terrestrial Radio Access Network* (**UTRAN**).

Es así que en enero de 1998, el ETSI adoptó la tecnología W-CDMA (Wideband CDMA) en modo FDD (Frecuency Division Duplex) con provisión para

TDD (Time Division Duplex) como la tecnología apropiada para UTRAN, cada una diferente, pero basada en tecnologías similares. Es por esta razón que W-CDMA y UTRAN se usan como términos permutables y referidos a UMTS.

En la UTRAN las BTSs serán sustituidas por *Nodos B* y las BSCs por los *RNC (Radio Network Controlle*r). Aparece, por tanto, la interfaz *Iu* en lugar de la interfaz *A (Iu CS* para conmutación de circuitos e *Iu PS* para conmutación de paquetes).

Tanto en la red de acceso radio como en la interfaz de la misma con el *Core Network* se utilizará ATM como protocolo de transporte. La estructura de UMTS en la R99 se muestra en la Figura 30.

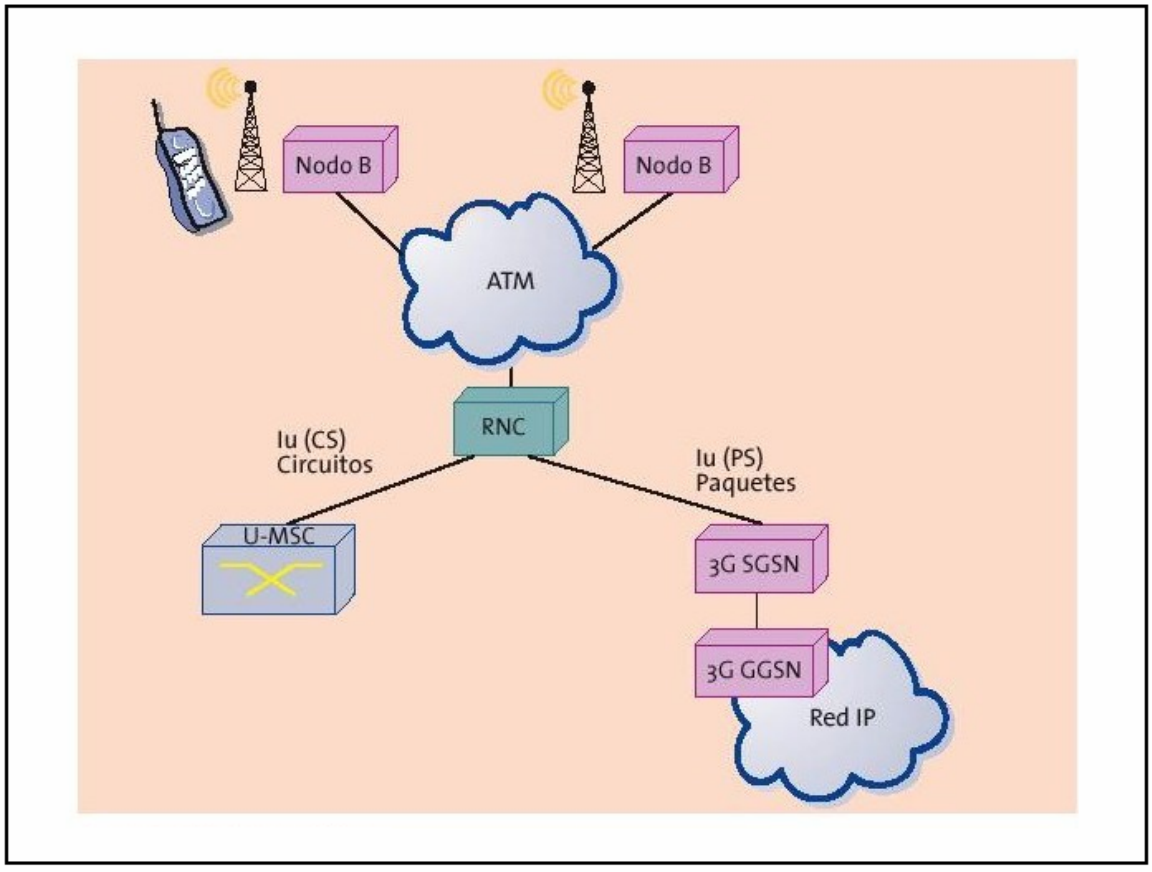

Figura 30. Arquitectura R99 de UMTS

4.3.6 RELEASE 4 DE UMTS

En *Release 4* (R4) de UMTS, la voz se transporta sobre IP y aparecen separadas las funciones de control y conectividad para voz: las MSCs se dividen en *Media Gateways* (MG) para conectividad y *Servidores de Control* para señalización.

El MG proporciona conexión con las redes de conmutación de circuitos, bajo las instrucciones de un *Media Gateway Controller* (MGC). Para la comunicación entre el MG y el MGC se utilizará el protocolo MEGACO.

La estructura de UMTS en la R4 se muestra en la Figura 31.

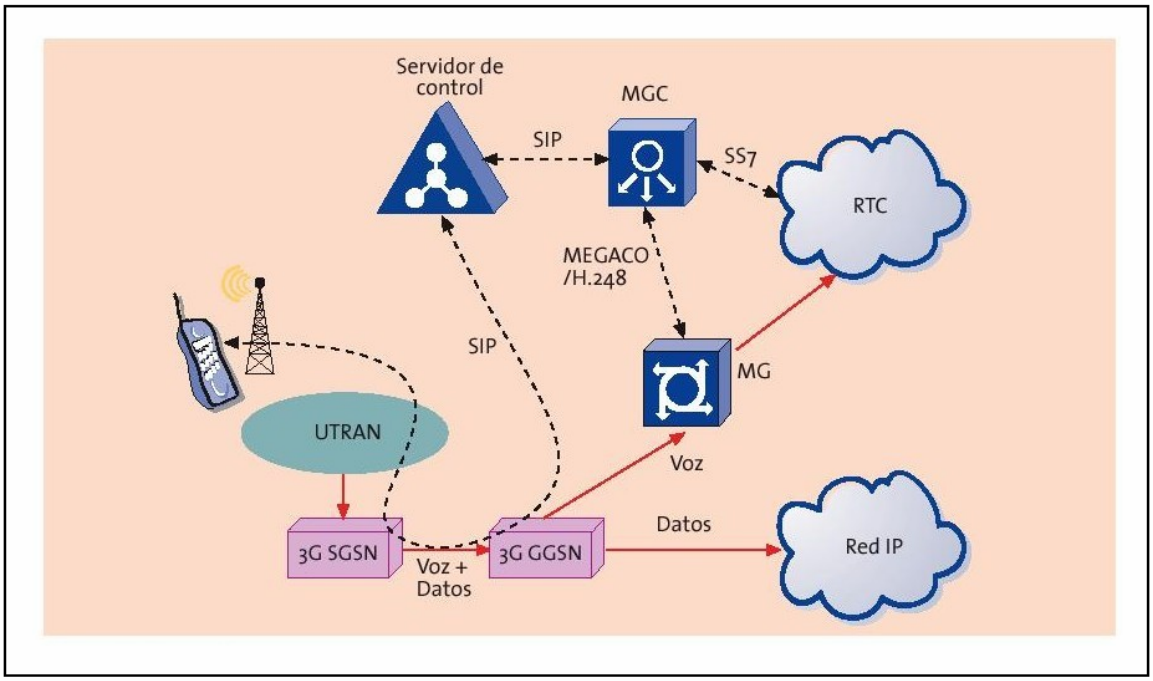

Figura 31. Arquitectura R4 de UMTS

4.3.7 RELEASE 5 DE UMTS

Esta versión es sin duda el desafió final, y por lo tanto la parte fundamental de la nueva red UMTS, por este motivo se realizara un análisis profundo de este estándar.

Release 5 (R5) será una versión Todo IP (All-IP). IP será la tecnología de transporte en la *Core Network* para todo tipo de datos e, incluso, posiblemente también en la UTRAN, en lugar de ATM. También surgirá el uso de tecnologías complementarias y estrechamente relacionadas con el protocolo IP como es el protocolo MPLS o Multiprotocol Label Switching.

Según 3GPP el estándar Release 5 es un modelo de referencia para el Núcleo o Core de la red UMTS, y cuenta con tres dominios que son:

- **Dominio de conmutación de circuitos (CS),** provee servicios similares a los que actualmente brindan las redes GSM como son Voz y Servicios suplementarios.

- **Dominio de conmutación de paquetes (PS),** se presenta en la red evolucionada GPRS.

- **Dominio de multimedia IP,** soporta aplicaciones multimedia IP.

En la R5 se culmina también la separación entre los planos de transporte y control, con la aparición del Subsistema IP multimedia o *IP Multimedia Subsystem* (IMS) para la gestión de servicios multimedia utilizando señalización SIP (Session Initiation Protocol) sobre portadora de paquetes.

4.3.7.1 Subsistema IP multimedia o *IP Multimedia Subsystem*

A continuación se muestra gráficamente y de manera simplificada este subsistema.

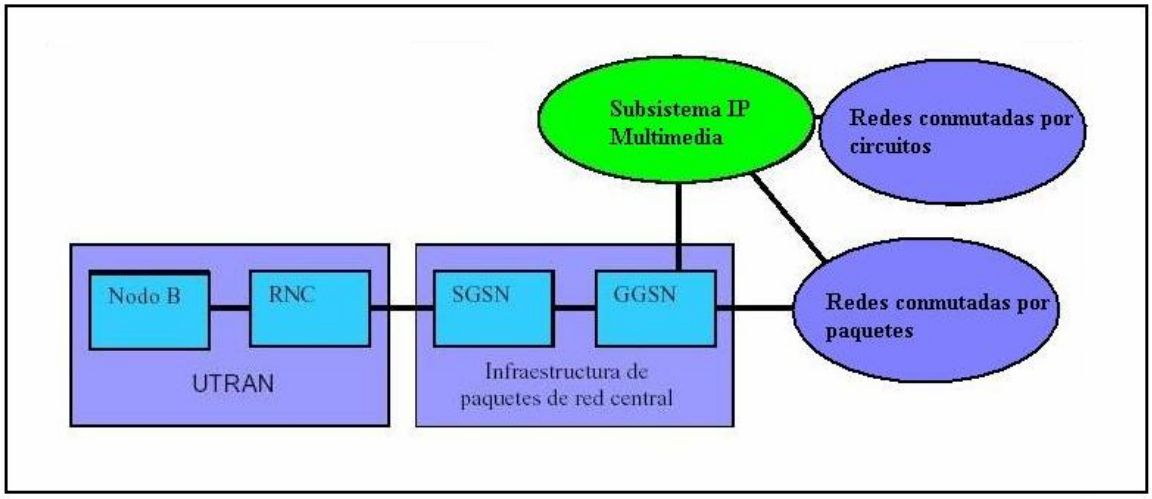

Figura 32. Subsistema IP multimedia

Las entidades funcionales del IMS son:

HSS (Home Subscriber Server). Es la base de datos maestra para un usuario con la información relativa a la suscripción, que necesitan los nodos de la red, para llevar a cabo el manejo de las llamadas y sesiones.

Realiza el AAA (Authentication, Authorization and Accounting) contiene la identificación del usuario (numeración y direccionamiento), la información de seguridad del usuario, la información de localización del usuario y el perfil del usuario (servicios subscritos, información relativa a esos servicios, etc.). El HSS es la evolución del HLR, que junto con las funciones primitivas del HLR incorpora funciones de traducción avanzadas para pasar de direcciones E.164, los actuales números de los móviles, por ejemplo 630123456, a direcciones SIP, por ejemplo fchang@espe.edu.ec.

CSCF (Call State Control Function). Es el nodo fundamental dentro del dominio IMS, pues soporta y controla las sesiones multimedia. En esencia es un servidor SIP que maneja las siguientes funciones: enrutamiento de llamadas entrantes (actúa como el primer punto de entrada de las llamadas y realiza su enrutamiento), control de llamada (realiza el establecimiento y terminación de la llamada, así como la gestión de los estados), servidor de los perfiles de la base de

datos (interactúa con el HSS para recibir y guardar en caché los datos de usuario), manejo de direcciones (análisis, traducción, modificación y mapeo de direcciones), señalización (SIP al terminal y al MGCF), soporta las APIs para las aplicaciones.

Se encarga del control de la sesión y está divido, a su vez, en varias entidades que se comunican entre sí y con el usuario utilizando el Protocolo de Inicialización de Sesión más conocido como SIP. Éstas son:

- *I-CSCF (Interrogating CSCF*). Es el punto de entrada y selecciona, con la ayuda del HSS, el S-CSCF apropiado.

- *S-CSCF (Serving CSCF*). Recibe las peticiones SIP del usuario y realiza el control de la sesión.

- *P-CSCF (Proxy CSCF*). En el caso de *roaming,* estaría localizado en la red visitada y seleccionaría el I-CSCF de la red de origen.

MGCF (Media Gateway Control Function). Controla el estado de la llamada para los canales de comunicación en el IM-MGW (negociación de codecs, control de eco…). Realiza la conversión del protocolo ISUP a SIP.

IM-MGW (IP Multimedia-Media Gateway). Convierte y adapta tráficos procedentes de una red de circuitos a una red de paquetes basada en IP.

T-SGW (Transport Signalling Gateway). Realiza la adaptación de los protocolos de transporte de señalización al mundo IP basándose en el estándar SIGTRAN del IETF. Con este enrutamiento las capas de transporte de SS7, se convierten a una capa de adaptación, SCTP (Stream Control Transmission Protocol), que corre directamente sobre IP.

MRF (Multimedia Resource Function). Gestiona las funciones de llamada o sesión con varios participantes y conexiones. Se ocupa de realizar las

conferencias multimedia, maneja los tonos y las locuciones. Tiene las mismas funciones que la MCU de H.323.

Las características generales del dominio IMS son:

El dominio IMS debe capacitar la convergencia de acceso a voz, vídeo, mensajes, datos y tecnologías basadas en web al usuario móvil. La idea inicial de partida es que los servicios no sean un mundo cerrado como ocurría hasta ahora, sino que sean desarrollados por operadores y terceras partes, incluyendo proveedores del mundo de Internet. Con la arquitectura desarrollada para capacitar aplicaciones multimedia, se ha tratado de dar la mayor flexibilidad tanto en el dispositivo de usuario final como en los servidores de red, asumiendo el concepto usado en Internet, donde se basan en una arquitectura lo más flexible posible. Con esta arquitectura junto con conceptos existentes en versiones anteriores, las aplicaciones serán transparentes a la red. Existen unas características generales que se deben cumplir para soportar aplicaciones IP multimedia:

- *Calidad de Servicio negociable* para sesiones IP multimedia, que se puede llevar a cabo durante el establecimiento de la sesión o durante la sesión ya establecida.

- *Calidad de servicio extremo a extremo* para la voz que por lo menos garantice una calidad tan buena como la de una llamada hecha a través del dominio de circuitos.

- *Soporte de roaming* que permita negociar de forma automática la calidad de servicio entre operadores así como las capacidades del servicio.

- *Control de políticas IP* para aplicaciones multimedia, que permitan al operador establecer una distinción entre abonados.

- *Una sesión IP multimedia soportará varias aplicaciones IP multimedia,* que pueden haber sido desarrolladas por terceras partes.

- *La privacidad, seguridad y autenticación* de las aplicaciones multimedia deben ser iguales o mayores que las que se poseen para los servicios basados en conmutación de circuitos o GPRS.

- *Debe permitir el interfuncionamiento* con Internet, PSTN, RDSI y otras redes heredadas.

- Las llamadas de voz entre usuarios IMS y del dominio de circuitos deben ser transparentes para el usuario, es decir, deben tener las mismas características que las de una llamada entre usuarios del dominio de circuitos.

En UMTS se mantendrá la interoperabilidad con otras redes de Segunda Generación y con las entidades que permiten dicha interconexión: *Media Gateways* (MG), *Media Gateways Controller* (MGC) y *Signalling Gateway* (SGW).

La arquitectura de UMTS R5 se muestra en la Figura 33.

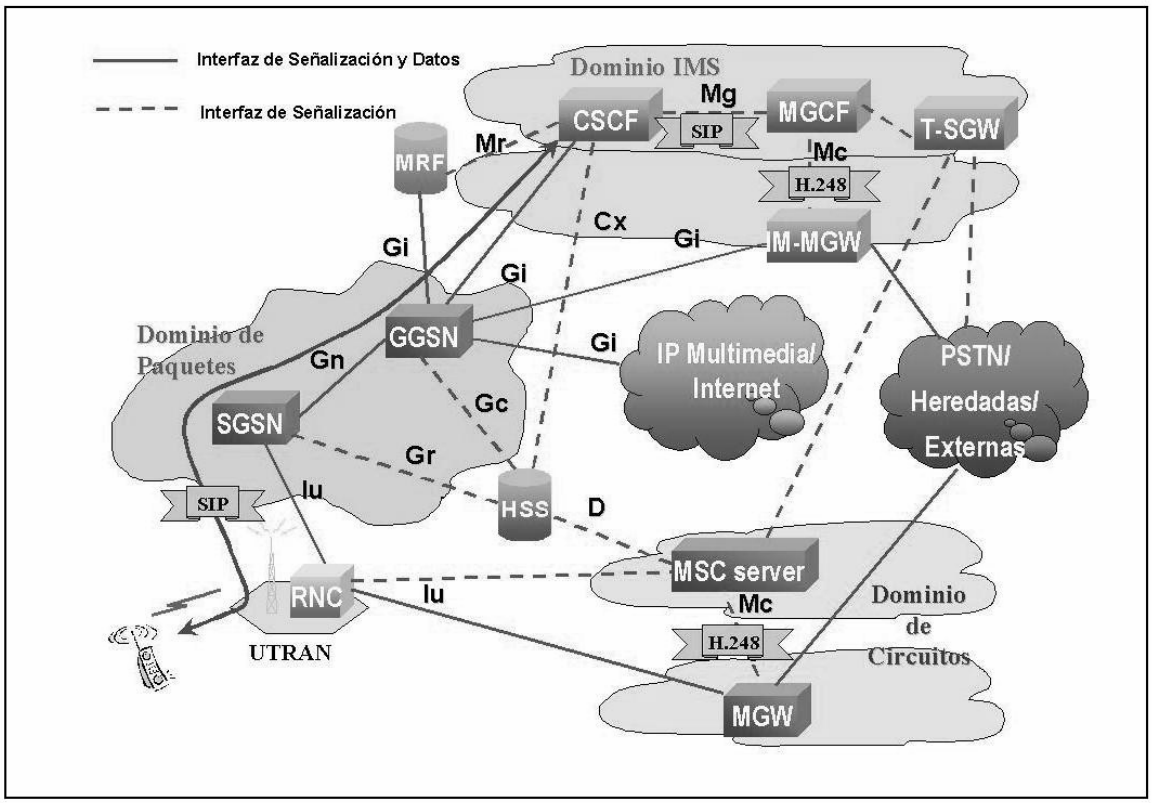

Figura 33. Arquitectura R5 de UMTS

Como se puede ver en la Figura 33, el terminal se conecta directamente al CSCF, usando la red de acceso UTRAN y el dominio de paquetes de forma transparente, usando una comunicación SIP extremo a extremo, donde el terminal debe ser un terminal SIP. Este último es un protocolo estandarizado en el IETF (RFC 2543), es decir, es un protocolo que se ha desarrollado para su uso en el mundo IP y que ahora es utilizado en las redes móviles, lo que demuestra el interés existente en tener una red móvil basada completamente en IP, donde los protocolos sean los ya estandarizados por el IETF sin tener que crearlos de nuevo y la confluencia de dos mundos hasta ahora separados, el mundo IP del mundo de las comunicaciones móviles.

SIP es un protocolo de control de la capa de aplicación, diseñado para proveer el control de la llamada y la señalización de la aplicación para llamadas de voz y multimedia, sesiones, en una red de paquetes. Por tanto, SIP permite la creación, modificación y terminación de sesiones con uno o más participantes. Como

ejemplos de sesiones SIP podemos destacar la telefonía IP, conferencias multimedia, etc.

4.3.8 NIVELES DE MOVILIDAD EN REDES "ALL- IP"

De acuerdo con la arquitectura de red "Todo-IP", existen tres niveles de movilidad que son:

Movilidad en capa de enlace o movilidad de acceso. Se refiere a métodos y protocolos, como el GTP (GPRS Tunnel Protocol), que aseguran una comunicación continua en el caso de cambios de posición entre Nodos B que se encuentren dentro del alcance de un solo RNC.

Movilidad de área extendida, movilidad global o macromovilidad. Se trata de un tipo de movilidad en la cual un terminal móvil cambia de posición entre diferentes nodos. Es generalmente soportada por el protocolo Mobile IP

Micromovilidad. Se aplica este termino a cualquier movimiento de un nodo móvil fuera del alcance de un RNC y que no necesite un cambio en su dirección de cuidado. Es soportada por protocolos como Hawaii, Cellular IP, etc

En las redes móviles de Tercera Generación, la movilidad es gestionada dentro del plano de usuario, es decir en la capa de enlace, nivel 2. La gestión de movilidad de capa 2 es también utilizada en otros sistemas como son WLANs, para handovers entre puntos de acceso.

La meta del dominio de conmutación de paquetes PS o Packed Switched Domain de UMTS R5 es proveer una conectividad global de capa 2 que pueda soportar cualquier protocolo de capa 3.

El protocolo GTP (GPRS Tunneling Protocol) es el encargado de mantener una movilidad global de capa de enlace. El terminal o nodo móvil es enlazado al mismo nodo GGSN todo el tiempo, y mantiene su dirección de capa 3, por ejemplo IPv6.

En este caso no existe una necesidad vital de Mobile IP. La figura 34 presenta la estructura simplificada de protocolos de transporte en el dominio PS de UMTS, donde el nivel de usuario IPv6 es tunelado a través de los elementos internos de GPRS. En la figura la Laptop es conectada a la red utilizando un terminal como nodo o modem WCDMA (esto se llama emulación dial-up).

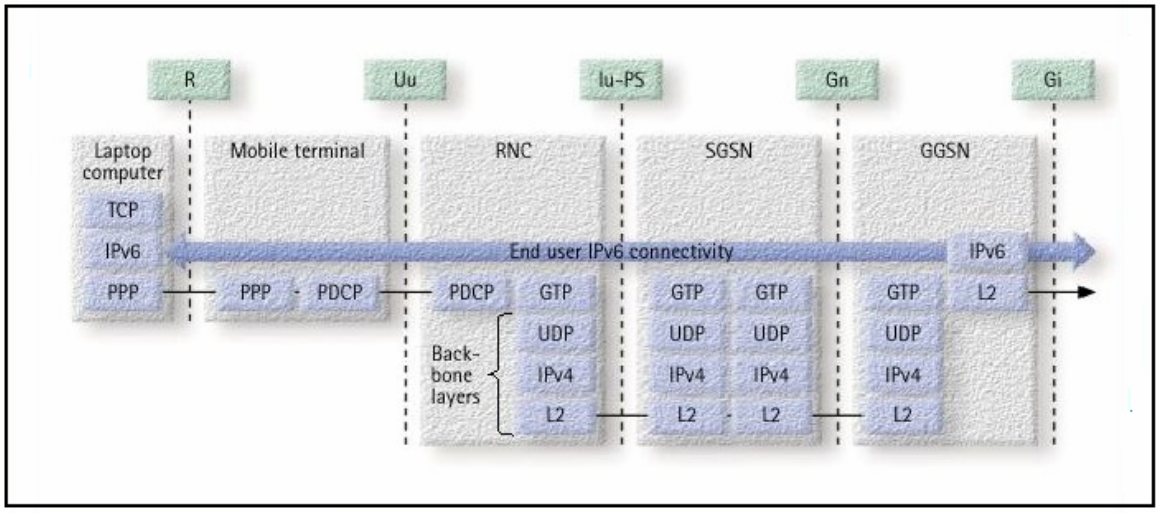

Figura 34. Arquitectura de protocolos simplificada para redes 3G

El nodo móvil enlazado a GPRS puede ser asignado con una dirección IP estática o dinámica. La dirección estática es asignada por el operador de la red local pública terrestre móvil o HPLMN (Home Public Land Mobile Network) en el momento de la suscripción al mismo.

La dirección IP dinámica puede ser designada por el nodo GGSN o también por la HPLMN o por la VPLMN (Red Visitada Pública Terrestre Móvil) en el contexto del tiempo de activación PDP (Packet Data Protocol). Adicionalmente la designación de la dirección, el nodo GGSN implementa la retransmisión de los paquetes IP desde el túnel GTP hacia la red PDN sobre la interfaz Gi y viceversa.

Existen dos clases de backbones de Redes Públicas Terrestres Móviles o PTMN:

- Los backbones Intra-PLMN

- Los backbones Inter-PLMN

Cada backbone de tipo Intra-PLMN es una red IP privada regida por el dominio de paquetes de datos y con señalización solamente dentro de una PLMN, un backbone Inter-PLMN es utilizado para el roaming entre una PLMN y otra, esto se da utilizando la interface Gp y gateways fronterizos. Los nodos SGSN y GGSN utilizan el backbone Intra-PLMN para intercambiar los datos y señalización en el dominio de conmutación de paquetes (PS). Cuando se da un roaming tanto el backbone Intra-PLMN de la red y la red visitada están en uso, adicionalmente al backbone Inter-PLMN.

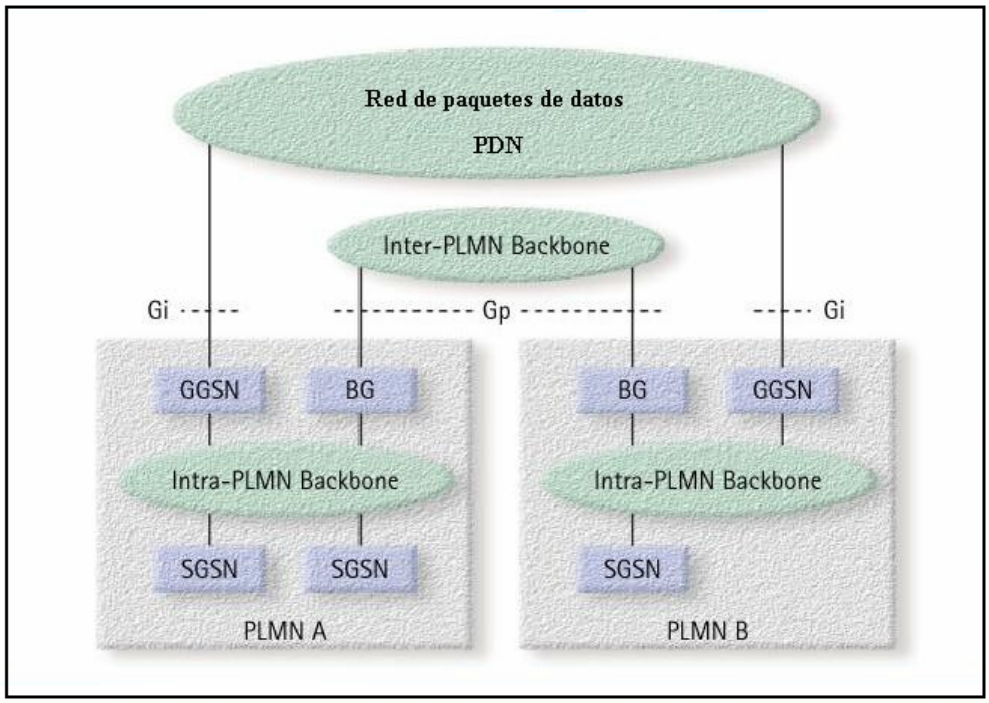

Figura 35. Backbones de red Intra PLMN e Inter PLMN

4.3.9 MOVILIDAD EN CAPA DE ENLACE EN REDES GPRS/UMTS

El backbone de la red Intra-PLMN interconecta los nodos SGSN y GGSN y el backbone de red Inter-PLMN en diferentes PLMNs.

Cuando un usuario hace roaming hacia otra PLMN, que es conocida como la PLMN Visitada o VPLMN, el usuario necesita primero engancharse a la red. En el enganche GPRS (GPRS Attach), el nodo móvil informa al SGSN de su intención de conectarse a la red mediante el envío de información a cerca de su identidad, capacidades y ubicación. El SGNS luego chequea la identidad del nodo móvil y realiza un proceso de autenticación para la seguridad de la ruta de transmisión. El enganche se completa luego que el SGSN ha recibido los datos del suscriptor de roaming desde el nodo HLR de la red local del suscriptor y se finaliza el proceso de la actualización de ubicación.

Después del enlace o enganche GPRS, el nodo móvil envía una solicitud de "Contexto Activo PDP" en el cual el nombre del punto de acceso o APN es una referencia a ser usada por el nodo GGSN AP incluso en una red PLMN local o visitada o en una red externa.

Cuando un usuario esta haciendo roaming en la red PLMN existen dos posibilidades para la selección del nodo GGSN.

1. Usar el nodo GGSN de la red local via backbone Inter-PLMN, BGs y mediante un túnel GTP sobre el interface Gp (Figura 35 y 36). El nodo GGSN local luego enruta los paquetes a su destino.

2. Utilizar el nodo GGSN de la red visitada, enruta los paquetes desde la VPLMN hacia su destino directamente a través de la red de paquetes de datos o PDN, de la manera en que el Internet público utiliza el interface Gi

El primer caso permite al nodo móvil tener una identidad a nivel de capa de red desde su red local. Pero esto puede no ser la manera más efectiva especialmente en el caso de que los servicios locales, topológicamente cerca de la red visitada, sean utilizados.

En el Segundo caso, al nodo móvil se le asigna una dirección IPv6 desde el nodo GGSN de la red visitada. En este caso es imposible para el nodo móvil ser

localizado mediante la dirección de su dominio local. Una solución para esto basada en MIPv6 es descrita a continuación.

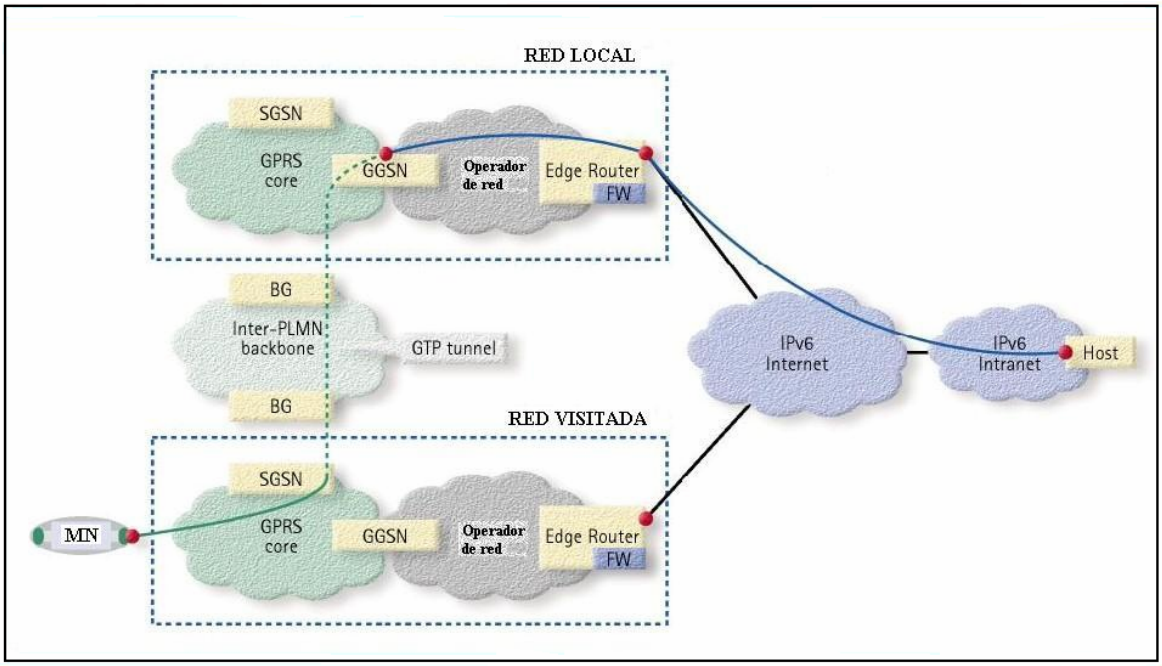

Figura 36. Movilidad en capa de enlace en redes 3G

4.3.10 MOVILIDAD EN CAPA DE RED EN REDES GPRS/UMTS

Considerando como ejemplo la situación de un usuario de GPRS suscrito a un operador en Finlandia que realiza roaming en los Estados Unidos, y accede a un servicio local ahí. Si la movilidad en la capa de enlace es utilizada, los paquetes IP del usuario deberían ser tunelados a Finlandia, y luego enrutados de regreso a los Estados Unidos. En este caso el tiempo que se demorarían los datos en viajar desde el nodo móvil y el servidor y viceversa puede ser inaceptable para muchos servicios.

Como una solución a este problema, el suscriptor GPRS que esta haciendo roaming, podría utilizar los servicios de un nodo local GGSN dentro de la red visitada, permitiendo a los paquetes IP ser enrutados lo mas rápido posible, sin tener que cruzar el largo camino hacia su red local. Como la dirección IP es ahora asignada por la red visitada, el nodo móvil no podrá ser accesible vía

identificación de capa de red de su red local. Para algunas aplicaciones esto no seria un problema, pero en general esto debería ser deseable si el nodo móvil podría ser alcanzado mediante una dirección IP asignada por su red local.

Una solución natural a este problema es utilizar Mobile IP, ya que este proporciona movilidad en capa de red (nivel 3), para registrar la dirección de la red visitada con la red local, permitiendo a los paquetes enviados a la dirección local ser entregados al nodo móvil.

4.3.10.1 Operación de Mobile IPv6 en redes GPRS/UMTS

Cuando un terminal móvil o nodo móvil se encuentra haciendo roaming en una red extranjera, es direccionable mediante su dirección de cuidado en lugar de su dirección local.

El prefijo de la dirección IPv6 en la dirección de cuidado del nodo móvil, es el prefijo del enlace extranjero.

La dirección de cuidado es adquirida mediante un mecanismo de direccionamiento proveído por la red visitada. Mientras el nodo móvil esta en roaming en una red extranjera este registra una de sus direcciones de cuidado con el agente local y envía un mensaje de “Binding Update” a su agente local.

El agente local responde con un mensaje “Binding Acknowledgement.” Todo paquete IPv6 contiene opciones de destino Binding Update o un Binding Acknowledgement que deben ser autenticados utilizando seguridad IP en el encabezado de autenticación. Después de los mensajes, esta dirección de cuidado se convierte en la *dirección de cuidado primaria* del nodo móvil.

El agente local intercepta todos los paquetes IPv6 desde un nodo correspondiente, por ejemplo un servidor WWW que se esta comunicando con el nodo móvil, el mismo que esta direccionado a la dirección local del nodo móvil. El agente local encapsula cada paquete interceptado utilizando el encapsulamiento

IPv6, con el encabezado de enrutamiento direccionado a la dirección de cuidado primaria del nodo móvil. Después de que el nodo móvil ha recibido el primer paquete encapsulado proveniente del agente local, este envía un mensaje Binding Update al nodo correspondiente informándole de su dirección de cuidado, luego el nodo correspondiente responde con un mensaje Binding Acknowledgement.

Después de esto, los paquetes enviados entre el nodo correspondiente y el nodo móvil, son reenviados y enrutados sin necesidad del agente local. Para los paquetes enviados por un nodo móvil que no se encuentre en su red local, la dirección de cuidado del nodo móvil es típicamente utilizada como la dirección fuente dentro de la cabecera de los paquetes IPv6. La opción de dirección local puede ser utilizada para informar el recibimiento de paquetes por la dirección local del nodo móvil.

El nodo correspondiente puede luego sustituir la dirección local del nodo móvil por su dirección de cuidado hacienda uso de una dirección de cuidado transparente al nodo correspondiente. Los protocolos de capas superiores como TCP solo pueden ver la dirección local. (Figura 37).

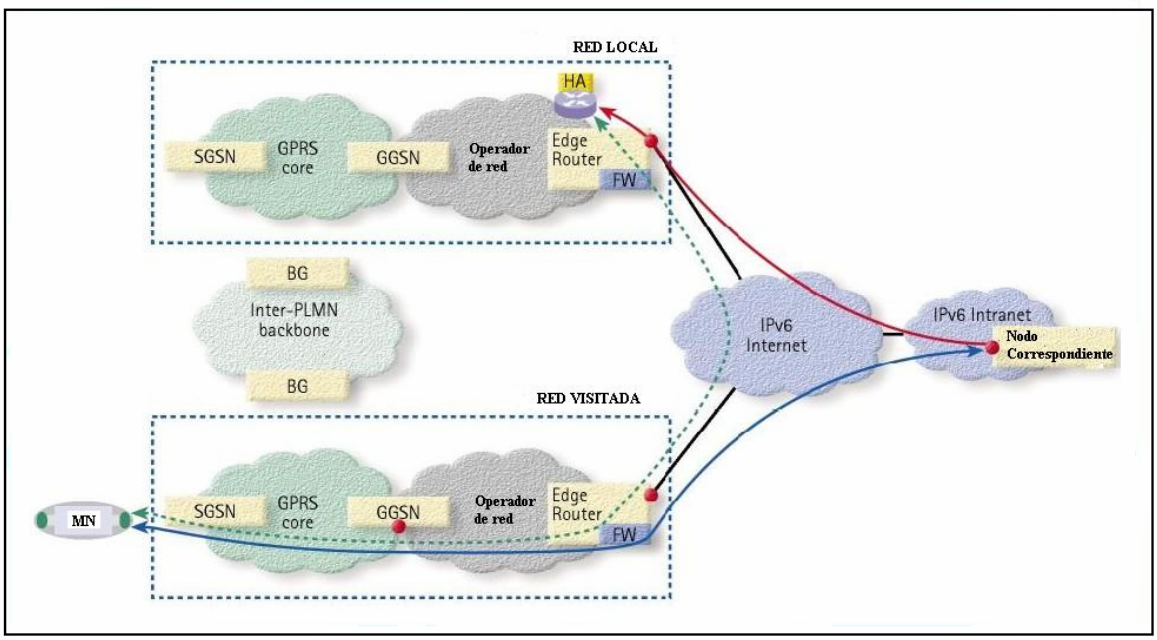

Figura 37. MIPv6 en redes móviles 3G

4.3.11 MODOS DE UTILIZACION DE MOBILE IP CON GPRS/UMTS

Mobile IP es soportado por GPRS/UMTS de las siguientes maneras:

La funcionalidad del agente extranjero debe ser sumada a solo un nodo GGSN dentro de la red PLMN. Esto implica que no existirán cambios en la arquitectura de red y tampoco se requerirán cambios en los nodos móviles. Este caso permite movilidad entre redes o backbones PLMN.

Mejorar los nodos GGSN con la funcionalidad del agente extranjero dentro del nodo GGSN/FA. Esto permitirá a los nodos GGSN ser cambiados si un nodo GGSN más conveniente esta disponible. En este caso se asegurara un uso mas eficiente de los recursos de los backbones PLMN creando una movilidad a nivel de nodos GGSN/SGSN.

Combinando los nodos SGSN y GGSN/FA en un Nodo de Soporte de Internet GPRS o IGSN (Internet GPRS Support Node). En este caso se puede proveer una gestión de macromovilidad con Mobile IP.

4.3.12 ROAMING ENTRE DIFERENTES TECNOLOGIAS DE ACCESO

La necesidad de una movilidad multiaccseso crece, cuando un terminal móvil multimodo se mueve entre diferentes redes de acceso. Por ejemplo, cuando un terminal multimodo se mueve de la cobertura de una red WCDMA hacia una red Bluetooth o WLAN este nodo obtiene nuevas direcciones IP. Cuando la dirección IP varia, las conexiones y las aplicaciones existentes se pierden, y necesitan ser reestablecidas.

Una solución a este problema es también la utilización de Mobile IPv6. Este protocolo permite a los paquetes enviados a la dirección local ser entregados a la actual dirección de cuidado del nodo móvil. Además, Mobile IP puede esconder cualquier cambio en las direcciones en las capas de transporte y aplicación,

permitiendo al nodo móvil realizar un roaming transparente entre diferentes redes de acceso.

4.3.13 MOBILE IPV6 COMO PROVEEDOR DE UN DIRECCIONAMIENTO ESTATICO IPv6 A LOS TERMINALES MOVILES

El método básico de direccionamiento en sistemas móviles GPRS y WCDMA es el direccionamiento dinámico dado por la autoconfiguarción de direcciones tipo Stateless de IPv6.

Esto significa que el nodo GGSN asigna direcciones IPv6 dinámicamente a los nodos móviles. Estas direcciones típicamente no tienen registrados nombres DNS, haciéndolas difíciles de utilizar, por ejemplo, servicios del tipo “Peer to Peer” sin un soporte especifico de un servidor de red que pueda mantener un registro de las direcciones dinámicas.

Existen servicios que se benefician de un direccionamiento estático de IPv6. Por ejemplo, servicios como WAP necesitan una identidad estática del usuario. Puede notarse que el uso estático de direcciones IPv6 y la utilización de Mobile IPv6 es una solución genérica para los requerimientos de una identidad estática.

La implementación de juegos para dos jugadores en los terminales móviles es un ejemplo de servicio “Peer to Peer”. Si no existiera direccionamiento estático (en la capa de usuario), los usuarios que deseen jugar dicho juego juntos deberían necesitar reunirse mediante un servidor de red residente. Esto puede significar que nuevos juegos puedan no ser introducidos en nuevos terminales móviles, antes de asegurarse que los servidores desplegados reúnan los requisitos específicos del juego en cuestión.

Mobile IPv6 puede ser utilizado como una solución a este problema. La dirección dinámica asignada por el nodo GGSN es utilizada como la dirección de cuidado colocada de Mobile IPv6.

Para el registro de esta dirección con el agente local, se crea un mapeo de la dirección dinámica con la dirección local más estática. Esto permite al nodo móvil ser localizado con su dirección local, y también a través de un nombre DNS, desde el momento en que la dirección local pueda registrarse con el DNS.

4.3.14 IMPLEMENTACION DE MOBILE IPv6 EN REDES GPRS/UMTS

La implementación de Mobile IPv6 en redes móviles de Tercera Generación principalmente requiere de: un plano de soporte de red IPv6 (capa de aplicación), la instalación del router del Agente Local en la red local, la utilización de terminales o nodos móviles capaces de soportar Mobile IPv6 y la implementación de una infraestructura de seguridad para IP ya que Mobile IPv6 utiliza IPsec para todos sus requerimientos de seguridad.

El agente local puede ser ubicado dentro de la red del operador de red o en otra red, por ejemplo el Intranet de una compañía o en la red local. En ambos casos, los elementos del nodo GGSN no necesariamente necesitan ser involucrados con el protocolo Mobile IPv6. Un lugar factible para la instalación del agente local podría ser un lugar cercano al router del borde de la red del operador.

Los principales beneficios de Mobile IPv6 en la capa de aplicación incluyen:

- Roaming eficiente desde la red visitada hacia los servicios de la red local

- Roaming transparente entre diferentes tecnologías de acceso, alcance mediante la misma dirección también desde otro tipo de redes de acceso como WLAN, Bluetooth, etc.

- Proveer un método de direccionamiento estático IPv6 factible a los terminales móviles

- Alcance mediante dirección local incluso cuando se utilizan servicios de un nodo GGSN visitado

- Servicios “Peer to Peer” para ser utilizados en el terminal móvil, permitiendo a los servicios ser corridos en los terminales sin un explicito soporte del operador de red.

4.4 INTEGRACION DE MOBILE IP CON CDMA2000

4.4.1 INTRODUCCION

La interfaz de red definida para CDMA2000 apoya la red de Segunda Generación de todos los operadores actuales, independientemente de la tecnología (cdmaOne, IS-136 TDMA o GSM). La TIA ha presentado esta norma ante la UIT como parte del proceso IMT- 2000. Operando en modo TDD y/o FDD, CDMA2000 ofrece velocidades desde 1,2 Kbps hasta 2 Mbps, y soporte para canales de 1.25, 3.75, 7.5, 11.25 y 15 MHz con una o múltiples portadoras.

Los 3.6864 Mcps (cps/Chip determina el grado de ensanchamiento del espectro) de CDMA2000 proporciona una capacidad superior al sistema en desarrollo de 10 y 20 MHz.

No así cuando se trata de desarrollos de 5 MHz donde los 4.096 Mcps de W-CDMA proporcionan un mejor rendimiento. CDMA2000 además agrega una banda de guardia de 640 KHz por lado para protección contra interferencia en canales adyacentes (interferencia cocanal).

CDMA2000 opera con sincronismo entre el móvil y la estación base.

Para llegar a este nuevo estándar a partir de redes CDMA de Segunda Generación o en el caso de las redes basadas en cdmaOne (IS-95A) de banda estrecha, existentes en los Estados Unidos y otros países de su área de

influencia, entre ellos el Ecuador, la transición hacia CDMA2000 consiste en dos pasos migratorios: IS-95B e IS-95C.

4.4.2 IS-95B.

La norma IS-95B mejora las velocidades de 64 a 115 Kbps agregando a los 8 canales de tráfico CDMA 14,4 Kbps y asignándolo a un móvil el tiempo que dure su operación (en ráfaga). Conveniente para acceso a Internet y aplicaciones que requieran velocidades medias, particularmente en áreas de bajo tráfico (suburbano/rural).

4.4.3 IS-95C.

IS-95C o CDMA2000 fase 1, también conocida como 1XRTT, emplea un canal de 1,25 MHz de ancho de banda y ofrece una velocidad nominal de 144 Kbps para aplicaciones móviles y estacionarias. Conveniente para requerimientos superiores en áreas de alto tráfico, pero no llega a soportar los servicios 3G.

4.4.4 ARQUITECTURA DE RED 3GPP2

3GPP2 combina el interfaz de radio WCDMA de alta capacidad con el protocolo IP Móvil, para alcanzar una arquitectura de red que provea capacidades IP. Este concepto se aprecia en la siguiente figura.

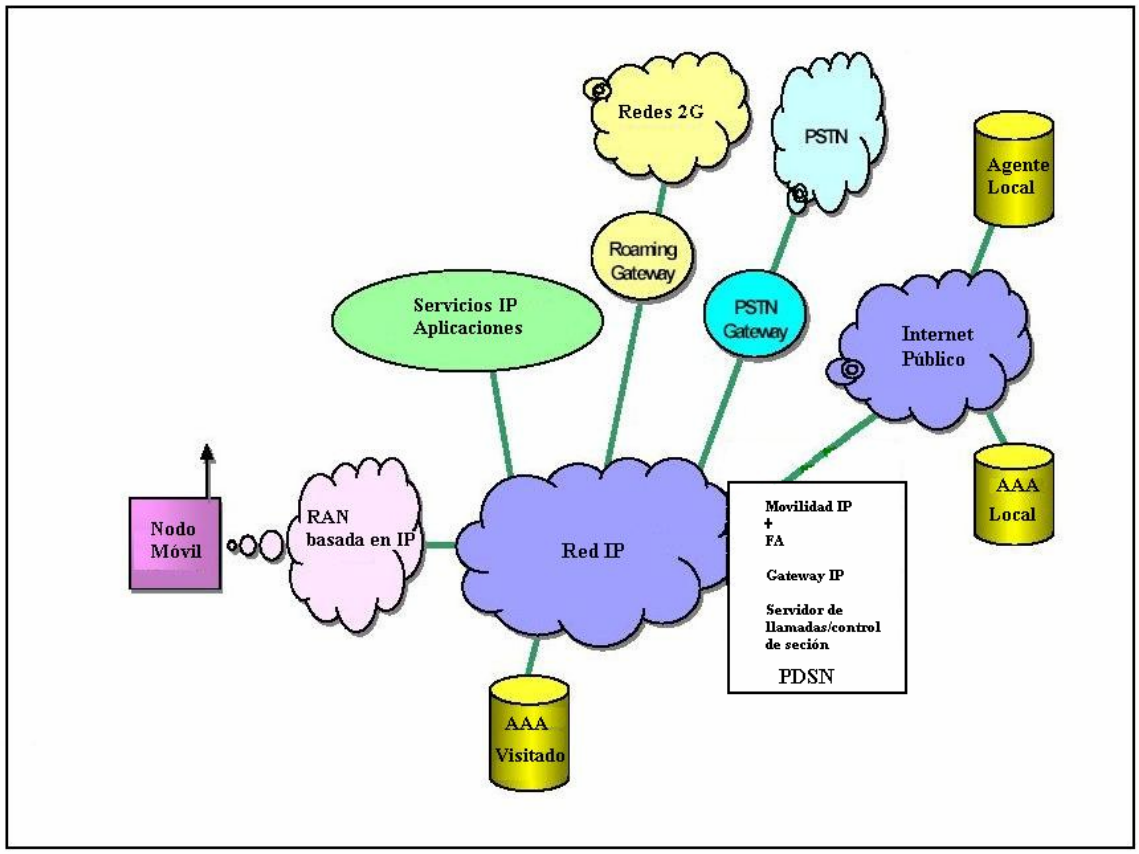

Figura 38. Arquitectura 3GPP2

Las funciones del Nodo de Servicio de Paquetes de Datos o *Packet Data Serving Node* (PDSN), en la arquitectura de redes 2G actuales esta distribuido como se muestra en la Figura 38. El nodo móvil utiliza protocolos basados en Mobile IP para identificarse. El PDSN contiene la funcionalidad del Agente Extranjero. Cuando el nodo móvil se enlaza al agente extranjero, este establece un túnel con el agente local y a través de este envía un mensaje de registro.

El agente local accede al servidor de Autorización Autenticación y Cuenta AAA (Authorization, Authentication and Accounting) para autenticar al nodo móvil. La dirección IP del nodo móvil es ahora anclada en el agente local para ser utilizada durante el tiempo que dure la sesión de datos. El dispositivo de datos conectado al nodo móvil puede realizar un handoff hacia otra red de acceso que soporte Mobile IP.

4.4.5 RELACIONES FUNCIONALES DE MOBILE IP EN CDMA

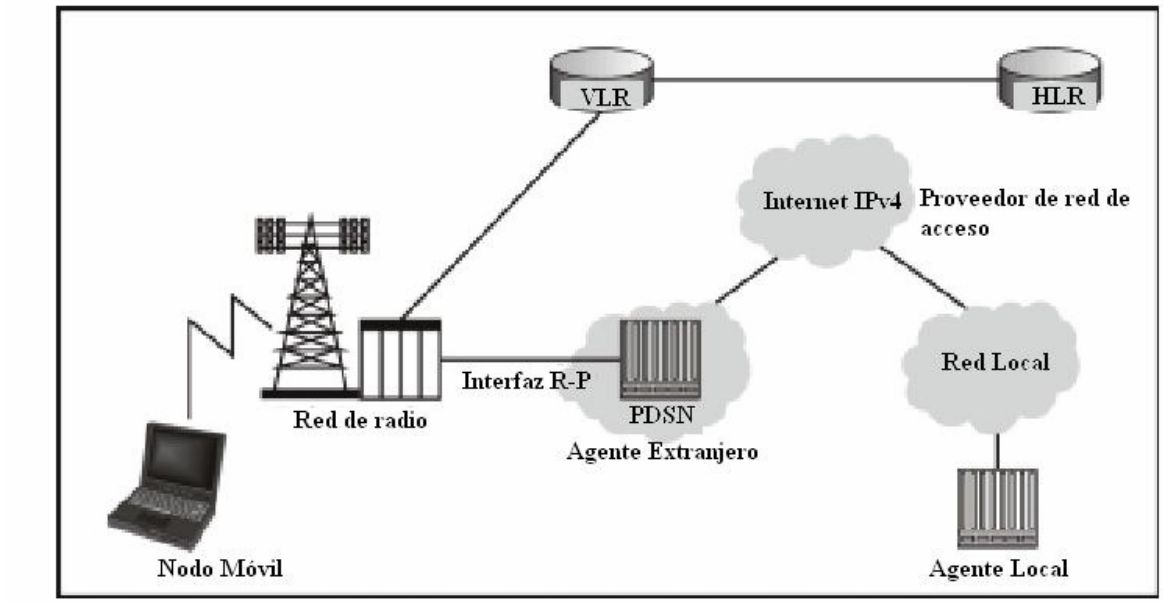

Figura 39. Red CDMA

4.4.5.1 Estación Móvil o Mobile Station (MS)

La Estación Móvil es el Nodo móvil de Mobile IP, este se conecta con la PDSN mediante el protocolo punto a punto o Point to Point Protocol (PPP). El nodo móvil puede realizar handoff entre distintas PDSN que no involucren la red local con Mobile IP y acepten un agente local dinámicamente asignado por AAA del proveedor de servicios de red o por la red local. La estación móvil puede utilizar una dirección local estática o una dirección local asignada dinámicamente.

Además a esto, la estación móvil puede almacenar paquetes para las aplicaciones móviles cuando los recursos de radio no están disponibles o cuando son insuficientes frente al flujo de la red.

4.4.5.2 Red de radio o Radio Network (RN)

Posee dos entidades que son:

- Recursos de Control de Radio o *Radio Resources Control (RRC)*
- Función de Control de Paquetes o *Packet Control Function (PCF)*

La RRC es la entidad en la cual el nodo móvil se conecta con la interfaz de aire. La RRC es responsable de establecer mantener y terminar los recursos de radio para el intercambio de paquetes entre las estaciones móviles y la función de control de paquetes o Packet Control Function (PCF).

La PCF reenvía paquetes hacia y desde el nodo PDSN. Este conecta al nodo PDSN en nivel de capa de enlace y se comunica con el RRC para administrar los recursos de radio para retransmitir paquetes hacia y desde la estación o nodo móvil. El PCF también recoge y envía información relacionada con el enlace de aire al nodo PDSN.

El PCF puede almacenar paquetes llegados desde el PDSN cuando los recursos de radio no están disponibles o cuando son insuficientes frente al flujo hacia el PDSN.

4.4.5.3 Nodo de Servicio de Paquetes de Datos o Packet Data Serving Node (PDSN)

PDSN es la entidad que soporta la funcionalidad del agente extranjero (FA). Esta establece, mantiene y termina la sesión PPP con el nodo móvil. El PDSN mapea las direcciones IP del nodo móvil y del agente local con un único identificador de capa de enlace utilizado para comunicarse con el PCF.

El PDSN envía Avisos de Agente si el PCF indica que el nodo móvil se esta acercando a un handoff. El PDSN puede también interactuar opcionalmente con un PDSN previo para soportar handoffs entre varios PDSN sin involucrar a la red local.

El PDSN puede enrutar paquetes hacia redes IP o directamente hacia agentes locales en el caso de tunneling reverso. También puede monitorear las

direcciones de origen de los paquetes recibidos desde las estaciones móviles. Cuando los paquetes son recibidos, y que no tengan asignadas o registradas direcciones de origen de las estaciones móviles, el PDSN descarta los paquetes y re inicia la sesión PPP con la estación móvil.

4.4.6 ARQUITECTURA DE DATOS CDMA BASADA EN MOBILE IP

Las redes CDMA basadas en el estándar IS-95 están en amplio uso actualmente especialmente en la provisión de servicios de voz para suscriptores móviles.

El servicio de voz se proporciona vía un circuito con una baja tasa (13 o 8 kbps) de conexión sobre el aire entre un nodo móvil y una Unidad de Selección y Distribución o *Selection and Distribution Unit (SDU),* vía una o más Estaciones Base de Transmisión/Recepción o *Base Tranceiver Station (BTS)*.

La SDU combina las señales de múltiples BTSs y convierte la baja tasa de datos comprimidos a tasas de tráfico de 64 kbps usados por la red conmutada de telefonía pública (PSTN). Es también responsable de seleccionar qué BTSs en el rango correspondiente al nodo móvil transmitirá actualmente tráfico, y de manejar la potencia de las transmisiones hacia y desde el MN.

Esto proporciona un cierto grado de movilidad: mientras que los nodos se mueven desde una BTS a otra BTS, éstos pueden generalmente seguir siendo asignados a la misma SDU. Esto es conocido como *soft-handoff*.

La funcionalidad de la SDU se puede centralizar como ejemplo ilustrativo en un switch de clase 5, pero puede ser también mejor distribuida. Lógicamente, la SDU es parte de una gran estación base (BS) que consiste en la SDU, una o más BTSs, y otros componentes.

La Figura 40 ilustra esta arquitectura básica, también muestra el MSC, que es responsable de interactuar con la PSTN y del manejar una o más BSs.

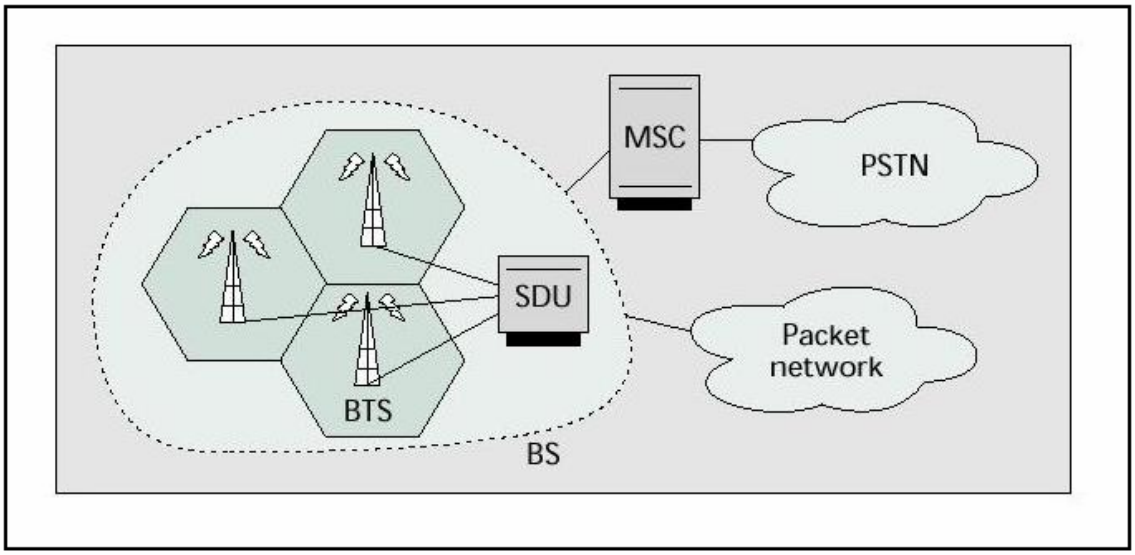

Figura 40. Arquitectura básica de la red celular CDMA

El desarrollo de los servicios de paquetes de datos en estas redes debe coexistir con el servicio de voz existente. En particular, la provisión de paquetes de datos no debe agregar un costo innecesario a los elementos de la red. En la práctica, esto implica que la arquitectura de red deba mantenerse sin cambios tanto como sea posible, y especialmente los cambios a los elementos del lado izquierdo de la Figura 40 (los que son más numerosos) deben ser mínimos. La interfaz de aire y los enlaces entre BTS y SDU deben ser capaces de soportar las tasas de datos más altas necesarias para los paquetes de datos.

La SDU es el primer elemento de la red que trata una sesión paquetes de datos de manera diferente a una llamada de voz. Esto se muestra en el hecho de que la SDU toma las cadenas o streams de datos desde la red de paquetes en lugar de la PSTN.

Debido a que el tráfico de datos es menos tolerante a las altas tasas de pérdidas típicas del ambiente inalámbrico, la SDU ejecuta un protocolo de retransmisión llamado *Radio Link Protocol (RLP)*. Este es un protocolo de reconocimiento negativo o *Negative Acknowledgment* donde el destinatario solicita la retransmisión de las tramas de los datos faltantes. Las tramas son

almacenadas en el punto de origen, y un número pequeño (generalmente uno o dos) de retransmisiones de cada trama es atendida antes de pasar a la siguiente.

Para realizar la interfaz con una red IP, se tienen que utilizar protocolos de capa de enlace por ahora el protocolo para esta función es el Protocolo Punto a Punto definido por el IETF. Esta elección fue motivada por la funcionalidad rica proporcionada por PPP así como su extensa implementación sobre muchas plataformas. Sin embargo, PPP es un protocolo absolutamente complejo, y algunas de sus características se traslapan con aquellas proporcionadas por Mobile IP. El agente extranjero de IP móvil se ubica en la capa IP, es decir se ubica sobre PPP.

Cabe recalcar que en esta sección se hará referencia solamente a IPv4 y por ende al funcionamiento de MIPv4, puesto que el tiempo para el despliegue de IPv6 es incierto y relativamente corto, y actualmente las redes CDMA todavía utilizan la versión 4 del protocolo de internet.

Se utilizará el término PDSN para referirse al agente extranjero y el término PCF para hacer referencia al elemento en la red de acceso de radio, como la SDU, que conecta el PDSN.

La PCF es responsable de retransmitir datos hacia y desde el PDSN y de aislar el PDSN de ciertos aspectos inalámbricos propios de la arquitectura tales como el estado actual de la interfaz de aire. El PDSN posee características de un Servidor de Acceso a la Red o *Network Access Server (NAS)* y del agente extranjero de IP móvil.

Para permitir a un portador inalámbrico proporcionar servicio de Internet en un ambiente *roaming*, el PDSN se debe conectar con una infraestructura de Autorización Autenticación y Cuenta (AAA). Esta infraestructura permitirá a la red ser visitada por un usuario roaming para luego preguntar a la red local las identificaciones de la autentificación y así asegurar el pago de los servicios prestados. Esto es adicional a la existencia de los nodos HLR y VLR, basados en

la autenticación para servicios de voz inalámbricos. Los servidores AAA se muestran en la Figura 41 junto con sus relaciones funcionales con los nodos PCF y PDSN.

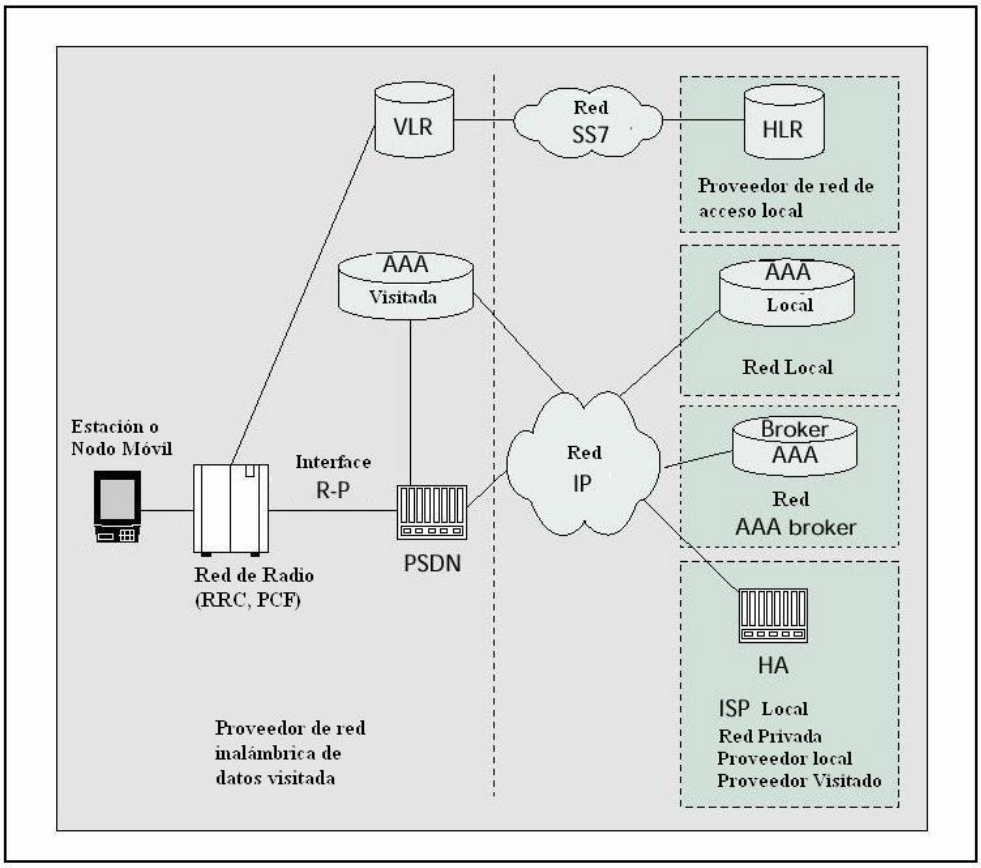

Figura 41. Mobile IP en CDMA2000

La arquitectura de la red celular CDMA2000 utiliza protocolos de estándares IETF para los servidores AAA, como por ejemplo RADIUS o DIAMETER. Esta red a su vez posee dos niveles de autenticación, el primero ocurre en la red inalámbrica mediante la utilización del protocolo ANSI-41 el mismo que es un protocolo de señalización para interfaces de aire que se ejecuta sobre el Sistema de Señalización Número 7 (SS7), y el segundo en la red de datos mediante la utilización de un identificador de acceso a la red o Network Access Identifier o NAI.

La red de datos CDMA soporta dos mecanismos AAA para la autenticación del usuario, los mismos que dependen de los requerimientos de servicio que necesite el usuario. Por ejemplo si se necesita un simple acceso a Internet que no requiera la utilización de Mobile IP, el protocolo de autenticación es el llamado *Challenge Hanshake Authentication Protocol* o CHAP que es parte del establecimiento de PPP.

Cabe mencionar que en algunas redes CDMA se hace también uso de las recientes actualizaciones del protocolo Mobile IP (MIPv6) las mismas que permiten codificar las identificaciones del usuario directamente mediante una petición del registro, y asignar dinámicamente una dirección local al nodo móvil. Esto esencialmente promueve la autentificación, el control de acceso de red, y la configuración de direcciones en la capa de red, quitándola del dominio del PPP donde se ha realizado tradicionalmente.

CAPITULO V

SERVICIOS Y APLICACIONES QUE BRINDA MOBILE IP

5.1 INTRODUCCION

En este capítulo se presentara la parte más importante de este trabajo, los servicios y las aplicaciones que brinda actualmente el protocolo Mobile IP. Los mismos que están orientados a grupos empresariales corporativos y también a servicios públicos de valor agregado que brindan empresas de telecomunicaciones y operadoras en todo el mundo.

5.2 OPORTUNIDADES DE MERCADO

Es muy importante recalcar que cualquier tipo de servicio se orienta hacia diferentes sectores de mercado, es así que siendo el protocolo Mobile IP un protocolo muy versátil con el cual se pueden brindar varios servicios se presentan a continuación los más importantes:

- Servicios de valor agregado en redes celulares 2.5G o 3G.

- Redes móviles, sub redes móviles entre automóviles, trenes, aviones o barcos.

- Campus y Empresas, movilidad en edificios y entre edificios, así como movilidad entre diferentes tipos de tecnologías y estándares.

- Proveedores de Internet Inalámbricos, como redes celulares 2G o 3G, movilidad entre “hot-spots” como WAN-Celular.

5.3 EJEMPLOS DE APLICACION

A continuación se presentan varios ejemplos de la utilización de Mobile IP.

Un avión, con un router IP Móvil con la funcionalidad de las redes móviles de Cisco, puede volar por todo el mundo con todos los pasajeros conectados continuamente a Internet. Los pasajeros conectan asistentes personales digitales o sus teléfonos celulares al router en el avión utilizando las tecnologías tradicionales LAN, como Ethernet o 802.11b. No se requieren dispositivos especiales de movilidad en la medida en que la red es la que permite la movilidad.

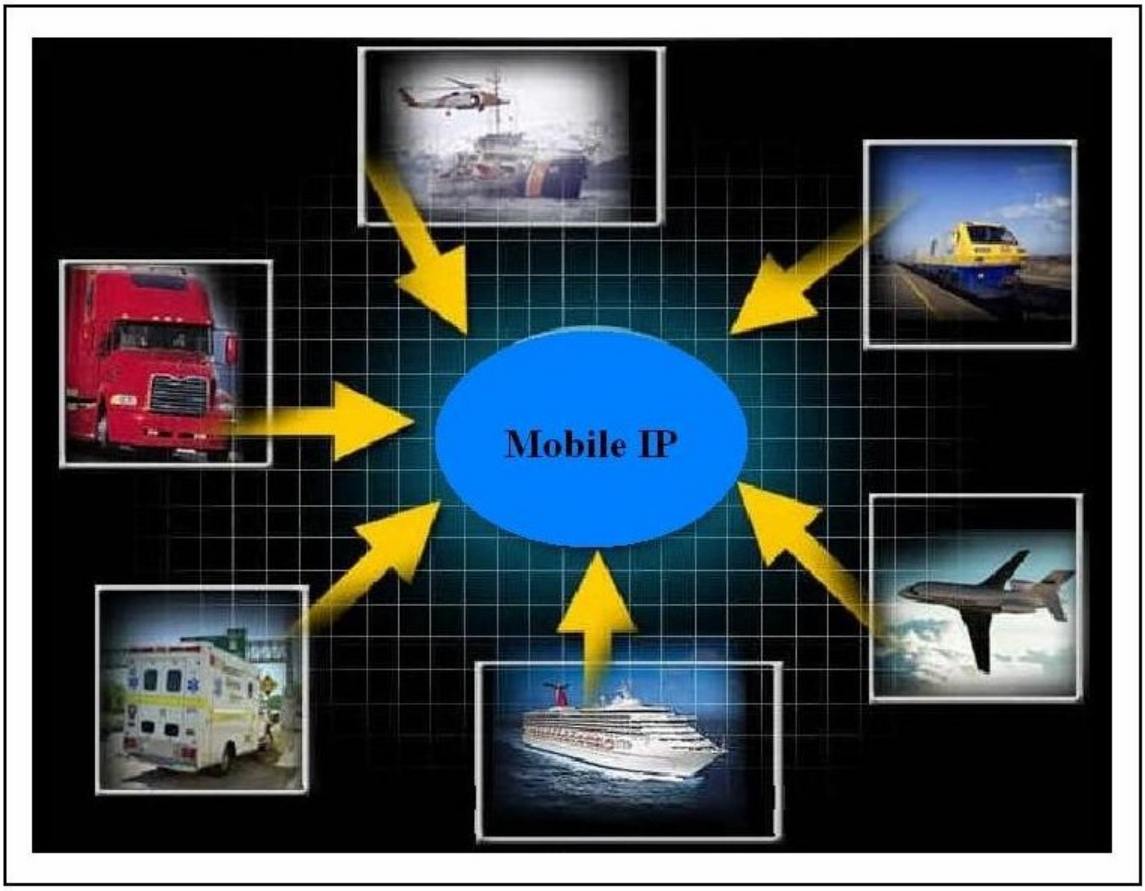

Figura 42. “Redes en movimiento” Mobile IP

Por ejemplo, ambulancias que necesitan viajar grandes distancias y que cuentan con una red móvil a bordo, podrán intercambiar información de diagnóstico y ofrecer tratamiento inmediato a pacientes.

Naves guardacostas podrán mantener la conectividad con sus estaciones de tierra mientras patrullan los mares.

5.4 CAMPO EXPERIMENTAL

No hay que olvidar que algunos de los principales desarrolladores de tecnología en el mundo son las Universidades. Es así como en algunas de estas prestigiosas instituciones desde su creación el protocolo Mobile IP ha sido probado experimentalmente en varias aplicaciones, en esta sección se presentaran tres de los mas importantes proyectos llevados a cabo en centros de estudios universitarios.

5.4.1 Proyecto MosquitoNet Mobile Computing Group de la Universidad de Stanford

La red MosquitoNet Mobile IP es una implementación del protocolo Mobile IP que tiene dos propósitos principales:

Utilizar este protocolo como la herramienta principal para el banco de pruebas de computación móvil de la Universidad, el cual soporta una movilidad transparente de computadores portátiles que se encuentran en movimiento entre diferentes redes cableadas o inalámbricas, por ejemplo Ethernet y el sistema de radio Metricom.

Explorar las diferentes aplicaciones en las cuales Mobile IP puede ser utilizado de la mejor manera. Para este estudio se han adherido algunas mejoras que se encontraron deseables para los hosts móviles a lo largo de la experimentación diaria. Algunas de las mejoras con las cuales se ha experimentado son:

- Se puede utilizar Tunneling Bi-direccional para cierto tráfico mientras se utiliza enrutamiento triangular para otro tipo de tráfico.

- Se puede apagar el soporte de movilidad para algunos flujos como trafico de Internet.

Esta implementación consiste en dos partes, la primera consiste en pequeños cambios dentro del kernel, la otra son programas tipo Daemons a nivel de capa de aplicación. Esta implementación esta llevada a cabo en sistema operativo Linux, utilizando la versión de kernel 2.2.16 (RedHat 7.0).

5.4.2 Proyecto Monarca de la Universidad de Rice

El Proyecto Monarca en el Departamento de Ciencias de la Computación de la Universidad de Rice se encarga del área de redes para usuarios inalámbricos y móviles. Usuarios móviles como una Laptop o una Palm están ahora disponibles y son alcanzables de mejor manera, así como nuevos productos y servicios disponibles incluyendo sistemas celulares, redes LAN infrarrojas o sistemas de radio de alta velocidad.

Dentro del Proyecto Monarca en la Universidad de Rice, se han desarrollado protocolos de red y protocolos de interface que permiten una interacción imperceptible y transparente entre host de diferentes redes inalámbricas y móviles. El alcance de su investigación incluye el diseño de nuevos protocolos, su implementación, evaluación de desempeño, y validación de los mismos desde la capa de enlace (2) hasta la capa de presentación (6). El objetivo de este trabajo es permitir la comunicación a los host móviles entre si y también entre usuarios estacionarios o cableados, de una manera transparente, haciendo un uso mas eficiente de la mejor conectividad de red disponible a los host móviles en cualquier momento.

5.4.3 Proyecto Mobile IP de la Universidad Nacional de Singapur

Este proyecto se fundamenta en la introducción de la computación móvil en el mundo del Internet. El objetivo se encuentra en el análisis del desempeño de

Mobile IP. La meta del estudio es caracterizar la eficiencia de Mobile IP y descubrir cualquier desempeño de cuello de botella de su arquitectura. Este estudio es llevado acabo simultáneamente por medio del análisis de modelos matemáticos, simulación por computadora y experimentación.

Se han hecho seis versiones de Mobile IP utilizando el Kernel de Linux.

La primera versión se realizó en diciembre de 1995, y básicamente comprendía la primera versión de Mobile IP.

La segunda versión, llamada versión 1.0, se la implemento en 1996 y con la misma se realizaron una serie de pruebas de interoperabilidad a través del Internet con otra implementación, la de los Laboratorios R&D en el Reino Unido. Estas pruebas incluían todas las combinaciones de Agentes Locales, Agentes Extranjeros y ubicación de los Nodos Móviles dentro de las dos subredes existentes en la Universidad Nacional de Singapur, los resultados demostraron una gran versatilidad de la nueva versión.

La tercera versión, la 1.1, fue hecha siguiendo los test de interoperabilidad. Con esta versión también se incluyo la implementación experimental del Protocolo de Optimización de Enrutamiento.

En Julio de 1996 se implemento la cuarta versión, llamada 1.2. los dos mayores cambios fueron: Tunneling bidireccional esta opción permite al sistema ser utilizado con routers para Internet que contengan firewalls y una solución al problema de la subred local.

En marzo de 1997 se realizó la versión 2.0 utilizando la versión del kernel de Linux 2.0.24.

Durante febrero de 1999 se implemento la versión 3.0 del software MIP, esta versión fue implementada utilizando la versión 2.0.34 del kernel de Linux. Las diferentes opciones de Mobile IP soportadas bajo esta versión son:

- Optimización De rutas
- Tunneling Bidireccional
- Handoff rápido
- Provee Calidad de Servicio entre diferentes redes.

5.5 REDES PRIVADAS VIRTUALES

Con el rápido crecimiento y la disponibilidad de las redes de datos móviles, herramientas de comunicaciones móviles y estándares Internet, los trabajadores móviles han encontrado nuevas formas de hacer negocios en el entorno competitivo actual. La necesidad para los trabajadores móviles de acceder a información crítica requiere el acceso a bases de datos corporativas y a aplicaciones Internet / Intranet. Además, la transferencia de mensajes fiables y adecuada, la integridad de mensajes, y la entrega de información personalizada permite al empleado móvil trabajar a altos niveles de productividad. El éxito en las comunicaciones entre trabajadores móviles y su entorno corporativo requiere una correcta combinación de las tecnologías. Desde el punto de vista de los negocios, estas tecnologías deben ser baratas y fáciles de usar. Para la viabilidad a largo plazo, deben basarse en arquitecturas de sistemas abiertos e interfaces industriales estándar. Las redes privadas virtuales han surgido para facilitar soluciones de interconexión a una creciente mano de obra móvil. Una red privada virtual permite a los negociantes facilitar a sus empleados móviles el acceso a la información y aplicaciones corporativas conectándoles a la empresa utilizando redes públicas, tales como Internet.

Utilizando las redes públicas como backbone de comunicaciones, una red privada virtual proporciona a la empresa una extensión barata, ofreciendo acceso seguro a un entorno abierto de red.

5.5.1 VPN o Redes privadas virtuales

Se crea una red privada virtual cuando un usuario móvil conecta un terminal de datos a una red ajena, bien por marcación privada o por redes públicas, y establece una presencia equivalente a una conexión directa con la red propia.

Se intenta una solución Mobile IP, para permitir la creación de redes privadas virtuales utilizando Internet como backbone de comunicaciones para conectar usuarios móviles. Las redes privadas virtuales se caracterizan por las propiedades siguientes:

*Presencia remot*a, la capacidad de establecer conexiones de red remotas y sin embargo aparecer como si se está conectado a la red propia.

*Independencia de re*d, la capacidad de migrar entre redes (por ej. BellSouth Wireless Data Network, CDPD, Wireless LAN-Ethernet). Tradicionalmente la independencia de la red IP (roaming) se hace sobre los mismos medios de acceso (por ej., SLIP, PPP, Ethernet). La implementación de Telcordia Technologies, Virtual Private Network ofrece la posibilidad de migrar no sólo a través de redes IP de medio único sino a través de múltiples medios fijos y móviles, sin la intervención del usuario.

Seguridad, la capacidad de ayudar a crear canales seguros para autenticación, integridad de datos y privacidad de datos. El **AirBoss™ Mobile System** desarrollado por Geoworks Corporation se utilizará para ilustrar las características y arquitectura de una solución basada en Mobile IP. Esta arquitectura particular proporciona una red IP móvil y fija y comunicaciones cambiando de medio para servicios Internet e Intranet. La capacidad de los usuarios móviles de migrar sin soluciones de continuidad y sin su intervención entre las redes radio y fijas para optimizar la eficiencia del sistema.

5.5.2 Seguridad de Mobile IP en VPN

La seguridad es una parte integrante de una solución de Red Privada Virtual. La AirBoss Mobile IP Network Configuration utiliza cifrado Mobile IP para formar un canal seguro entre el cliente AirBoss y el servidor, para soportar la autenticación del usuario, la integridad de datos y la privacidad de datos en entornos móviles.

La Figura 43 presenta como un cliente móvil puede conectarse con seguridad a un servidor de aplicaciones residente en la empresa del cliente móvil o red privada a través de redes ajenas fijas y móviles. Utilizando el cifrado AirBoss Mobile IP, se forma un canal seguro que permite a varias redes ajenas llegar a ser extensiones de la red privada.

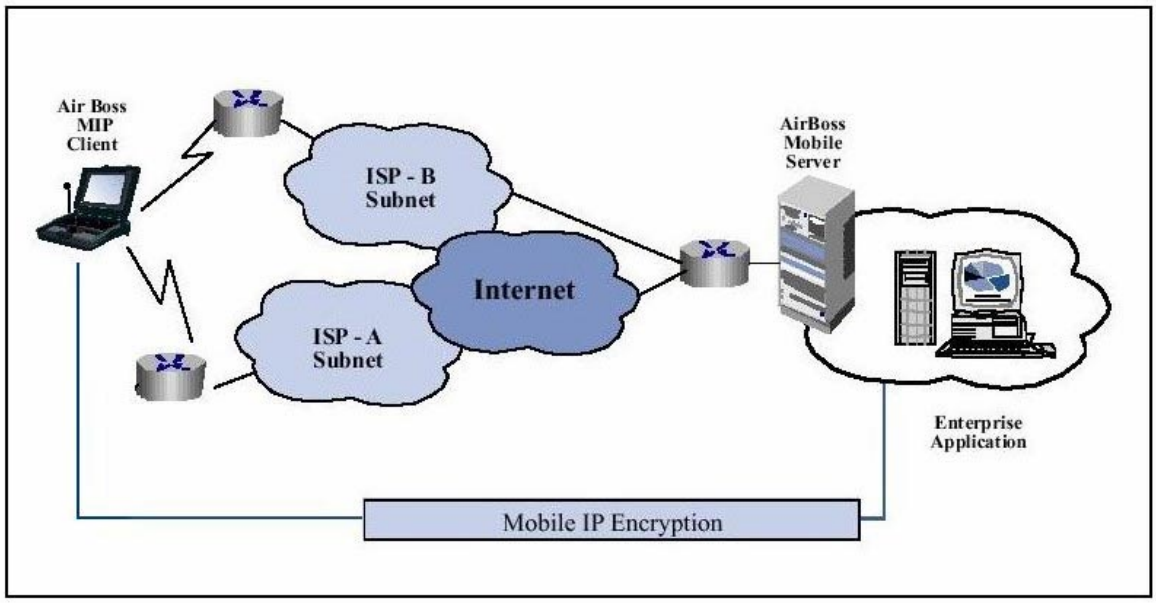

Figura 43. Seguridad AirBoss Mobile IP

5.5.3 Beneficios de una solución Mobile IP

Una solución Mobile IP ofrece los beneficios siguientes:

- Ayuda a proporcionar acceso seguro en un entorno de interconexión de redes abierto utilizando cifrado Mobile IP entre el cliente y el servidor.

- Permite a los trabajadores móviles establecer una presencia de red remota de una manera barata.

- Pretende proporcionar el encaminamiento más barato proporcionando la máxima eficiencia del sistema.

- Proporciona interconexión fija y móvil.

- Proporciona la posibilidad de migrar a través de redes sin intervención del usuario.

- Ofrece una solución barata para añadir movilidad a Intranets/Internet.

5.5.4 Soluciones para aplicaciones de movilidad corporativa

Las soluciones Mobile IP pueden ser utilizadas para permitir la posibilidad de migrar, sin rupturas, a través de redes móviles para extender las aplicaciones de empresa a trabajadores móviles. Las capacidades proporcionadas por la solución Mobile IP crea servicios mejorados para una variedad de aplicaciones verticales.

Los mercados verticales, tales como acarreo de mercancías y transporte, cuidado de la salud, seguridad pública y utilidades han hecho reales los beneficios que Mobile IP puede ofrecer para mejorar las comunicaciones empresariales.

Las soluciones Mobile IP pueden no sólo proporcionar transporte móvil fiable sobre redes geográficamente extensas, como son operadores celulares y PLMNs, sino permitir a un terminal de datos móvil migrar sin rupturas entre una PLMN y una LAN móvil.

Como una solución móvil Geoworks Corporation presenta una arquitectura Mobile IP llamada AirBoss Mobile System para permitir aplicaciones móviles de bases de datos móviles

Esta solución permite a un terminal de datos móvil migrar sin interrupción entre una LAN móvil y una PLMN. Las prestaciones de roaming permiten la conexión del servicio de datos ininterrumpida entre el servidor AirBoss y el terminal móvil de datos, que es también establecida para retransmitir datos sobre PLMNs.

Cuando está fuera de la red de área local móvil, el empleado móvil, usando un terminal móvil de datos, tiene acceso a las aplicaciones corporativas sobre una

red de área extensa. Sin embargo, cuando el terminal móvil de datos entra en el campo de acción de la LAN inalámbrica fija, el software Mobile IP migra automáticamente a la LAN inalámbrica fija, permitiendo el acceso más barato a la información corporativa. En resumen, la solución Mobile IP pretende proporcionar el enrutamiento más barato entre una LAN inalámbrica y una red móvil de área extensa.

En resumen, el éxito de una corporación en el entorno competitivo actual dependerá ampliamente de su capacidad para incrementar la productividad, proporcionando mientras tanto los niveles más altos del servicio a clientes. Las soluciones de interconexión fiables y eficientes en coste serán un componente crítico de la infraestructura de comunicaciones de la corporación. Las soluciones Mobile IP pueden permitir a las empresas crear sus propias Redes Privadas Virtuales, facilitando de esta forma:

- Bajos costes iniciales.
- Bajos costes de operación.
- Flexibilidad de soluciones.
- Ganancias de productividad significativas.

Mobile IP proporciona una solución de interconexión a ser tomada en cuenta por las empresas en el siglo XXI ya que proporciona roaming y altas capacidades de comunicación e interconexión.

5.6 REDES CELULARES

En la actualidad debido al despliegue de operadoras con licencias para servicios 3G, las mismas que están ganando terreno en la industria móvil, se han introducido nuevos conceptos o modelos de negocio estos son los Operadores Virtuales o Virtual Operators (VOs) y los Proveedores de Servicios y Aplicaciones Inalámbricas o Wireless Apllication Service Providers (WASPs).

Los VOs tienen acceso a redes de uno o más operadores móviles y ofrecen servicios a usuarios utilizando dichas redes. Algo que hay que recalcar es que los

VOs no tienen derechos para la utilización del espectro de radio para UMTS. Los operadores virtuales han invertido satisfactoriamente en su propia infraestructura, esto incluye inversiones en campos como SIM Cards, dispositivos móviles, centros de conmutación, servidores AAA, elementos de redes inteligentes, etc.

Dentro del concepto de mercado para redes 3G, se han identificado varios tipos de nuevos operadores virtuales, entre estos están:

- Proveedores de contenidos.
- Proveedores de servicios de Internet (ISP) y Proveedores de servicios de Internet inalámbrico (WISP).
- Operadores de red.

Dentro del concepto de WASP este mercado se ha dividido en dos partes, la primera los que están orientados a un mercado de usuarios corporativos y de negocios y la segunda los que se enfocan en los consumidores finales.

Como podemos darnos cuenta dentro de mercados tan competitivos cuyos servicios están orientados al uso de Internet, el protocolo Mobile IP juega un papel protagónico en un sin número de aplicaciones tales como:

- *Mensajería.* E-mails y mensajes multimedia (MMS) entregados al instante.

- *Juegos y entretenimiento.* Mejoramiento en los gráficos y respuesta inmediata a juegos interactivos en red, fácil y rápida descarga de contenidos multimedia.

- *Servicios de localización.* Por ejemplo servicios de localización basados en GPRS mucho más baratos.

- *Administración de datos personales.* Sincronización de calendario y libro de direcciones entre PDA, teléfonos móviles y PC.

- *Banca y finanzas.* Acceso a detalles de cuentas, facilidad de transacciones

Es así como en este mercado muchas empresas multinacionales entre ellas Nokia, Juniper y Ericsson han desarrollado soluciones Mobile IP para distintas plataformas, a continuación se muestran las soluciones que varias empresas han desarrollado.

5.6.1 Cisco

Es actualmente el mayor proveedor mundial de Mobile IP. A continuación presentamos la solución que esta empresa ha desarrollado para Mobile IP sobre CDMA2000.

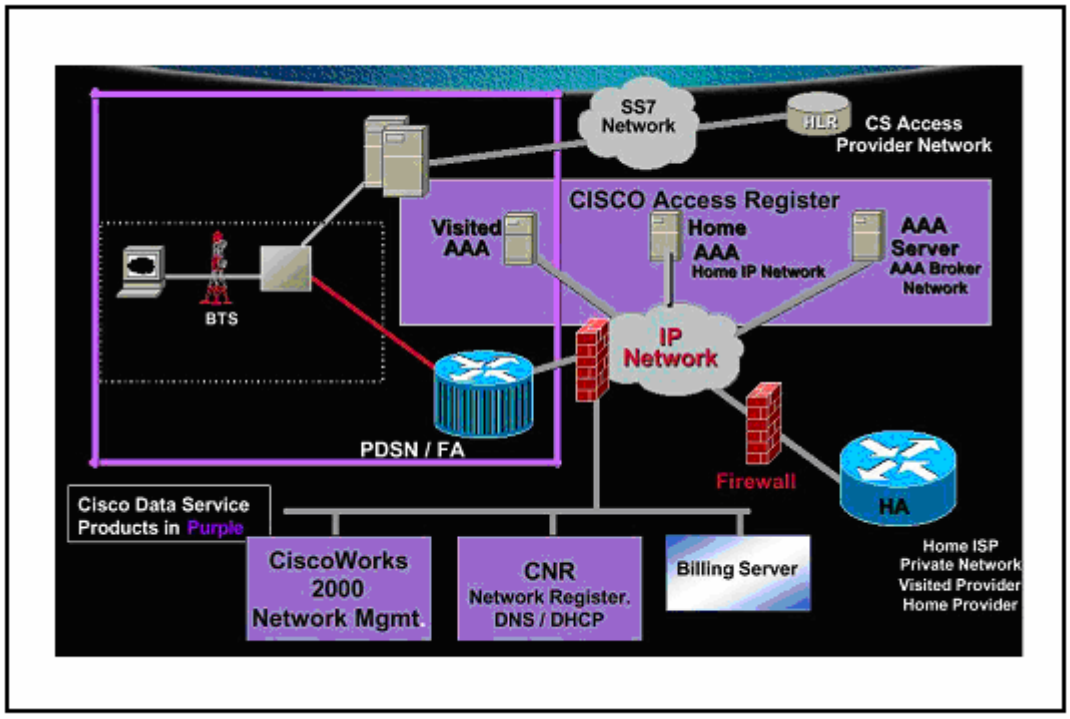

Figura 44. Solución Mobile IP de CISCO para redes CDMA

Esta solución cuenta con las siguientes características.

- Direcciones IP estáticas, públicas o privadas.
- Direcciones IP dinámicas, públicas o privadas.
- Autenticación del Nodo Móvil con el Agente Local.
- Autenticación del Nodo Móvil con el Agente Extranjero.

- Autenticación del Agente Local con el Agente Extranjero.
- Encapsulado IP-en IP (RFC 2003)
- Generic Route Encapsulation (GRE), RFC 1701
- Tunneling Reverso (RFC 2344)
- Mensaje Binding update para limpiar los registros luego de realizar hand-off con la red PDSN.

5.6.2 Birdstep Technology

Esta empresa brinda un servicio llamado **Birdstep Intelligent Mobile IP Client V 2.0 Universal Edition**, este es un servicio para empresas u operadoras celulares que brinda un servicio de roaming transparente.

Con esta solución de movilidad universal los operadores son capaces de introducir nuevos servicios a los ya existentes, los usuarios son capaces de moverse entre diferentes redes internas y entre diferentes redes de acceso externas como GSM, GPRS, CDMA200.

En el caso de utilizar esta herramienta en una empresa se logrará los siguientes tipos de movilidad.

- LAN-LAN: Entre oficinas en el mismo edificio o entre edificios.
- WLAN-LAN: Entre una oficina y salas de reuniones.
- WLAN-WLAN: Entre subredes desarrolladas a gran escala. Entre zonas WLAN en “Hot-Spots” públicos o privados.
- LAN/WLAN – Celular – WLAN: Entre una oficina y un socio o cliente.

Actualmente ya existen operadores celulares como Vodafone, NTT DoCoMo y Telefónica Móviles, ofreciendo servicios varios basados en Mobile IP en varios países del mundo y también en Latinoamérica.

Un caso concreto es la operadora NEXTEL, con su servicio NEXTEL ONLINE que brinda servicio de Internet inalámbrico sobre Mobile IP.

Algunos de los servicios que NEXTEL ONLINE brinda actualmente en países como México, Brasil, Argentina, Perú, Chile y Filipinas son:

- Servicio de Internet inalámbrico: e-mail, noticias, finanzas, alarmas de alerta.

- Es un servicio Mobile IP de extremo a extremo.

- Posee interoperabilidad entre Mobile IP de CISCO y MOTOROLA.

Dentro de las redes de tercera generación existen otras alternativas de acceso que las ya presentadas en el capitulo anterior, en las cuales también interviene el protocolo Mobile IP. A continuación se presenta una de ellas.

5.6.3 Provisionamiento satelital del servicio UMTS utilizando tecnología basada en IP.

Como ya se ha mencionado las tecnologías móviles y basadas en el protocolo IP constituyen los pilares de la estandarización de los sistemas de comunicaciones 3G.

Dentro de UMTS existe el provisionamiento satelital del servicio UMTS utilizando tecnología basada en IP.

UMTS Satelital (S-UMTS), jugara un papel muy importante en la implantación de los servicios de tercera generación. Por ejemplo los satélites pueden ofrecer varias ventajas en términos de cobertura de servicios globales.

La arquitectura presentada está en capacidad de soportar tecnologías como Mobile IP, Redes Inteligentes, y capacidad de terminales móviles para operar en ambientes satelitales y terrestres.

A continuación se presenta un grafico de la arquitectura de red S-UMTS, la misma que utiliza tecnologías basadas en el protocolo IP, como se puede observar el protocolo Mobile IP juega un papel fundamental.

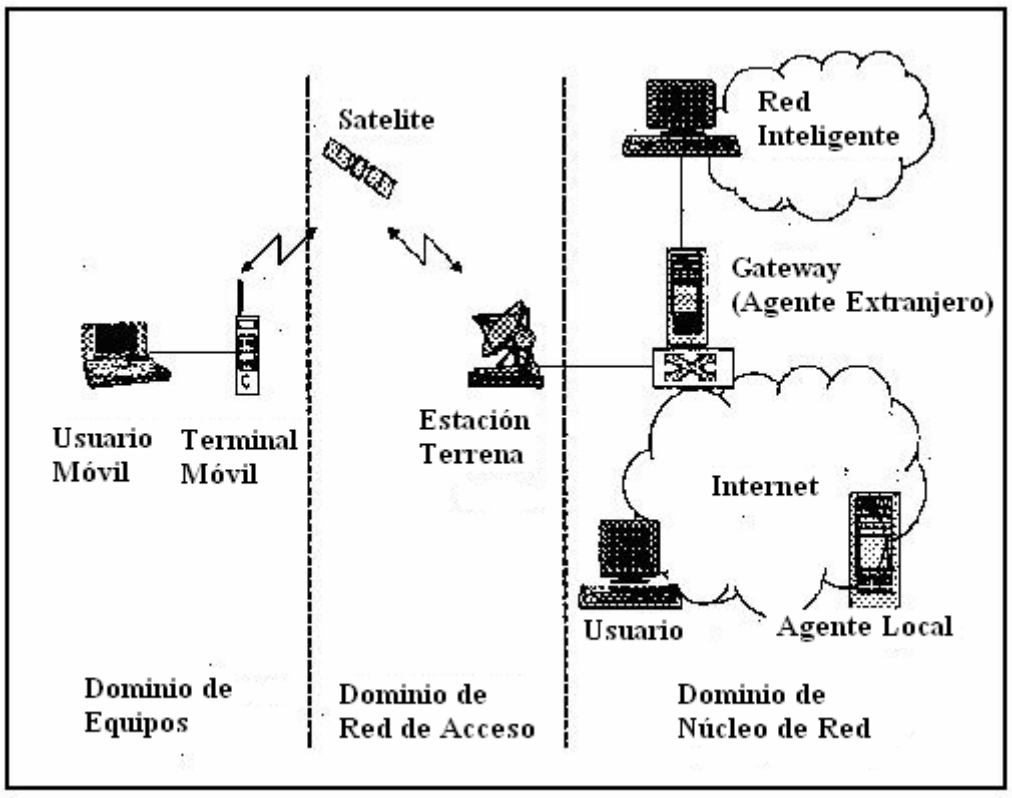

Figura 45. Arquitectura de integración de S-UMTS con Internet

Este modelo hace posible la integración transparente del servicio satelital UMTS con el núcleo de la red de Internet, proveyendo servicios complementarios a las redes de acceso basadas en Mobile IP.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

A lo largo de este trabajo se ha mostrado como el avance tecnológico crea y a la vez mejora servicios que en la actualidad ya son considerados como básicos, es el caso de Internet, y por ende ayudan significativamente al desarrollo y crecimiento de los pueblos.

“La tecnología es la capacidad humana de transformar los conocimientos en realidades”

6.1 CONCLUSIONES

En el presente proyecto se han entregado aspectos teóricos, funcionales, evolutivos, y sobre todo aplicativos del protocolo Mobile IP en redes celulares de Tercera Generación. Con este estudio se intenta proporcionar una idea clara del actual desarrollo tecnológico, y sus diversas aplicaciones en el campo de las comunicaciones móviles de última generación.

Como se ha visto a lo largo de este trabajo, el protocolo Mobile IP es un estándar moderno que involucra alta tecnología y que es muy versátil al momento de prestar diversos servicios, es en si mismo un servicio muy beneficioso principalmente en el campo empresarial, de campus y de servicios de valor agregado para operadoras móviles.

Cumple con el objetivo principal de la movilidad en Internet el mismo que es mantener una conectividad IP mientras se cruzan los límites de una red local. Esto se resume en que Mobile IP dota a un nodo móvil con la libertad para moverse libremente a través de varias redes y subredes permaneciendo siempre accesible mediante una única dirección IP, además el protocolo Mobile IP es el único capaz de proporcionar movilidad en cualquier tipo de medio y extensión geográfica.

El aumento progresivo de aplicaciones que necesitan direcciones IP públicas, unido al crecimiento de la nueva generación de telefonía móvil, hace que la transición de IPv4 a IPv6 sea impostergable y urgente. El protocolo IP Móvil contribuye claramente a la no proliferación de nuevas direcciones IP ya que asigna a cada nodo móvil una única dirección IP en todo momento.

Por otra parte la red de Internet ha experimentado un enorme crecimiento en los últimos años y el número de direcciones disponibles se hace cada vez más pequeño frente a las necesidades existentes. Por ello, se ha diseñado e introducido el Protocolo de Internet versión 6 más conocido como IPv6. Este nuevo modelo es el sucesor de la versión 4 puesto que resuelve sus deficiencias y aporta nuevas funciones acordes a la evolución actual de la red.

Con esto se ha demostrado la necesidad de adoptar al protocolo IPv6 como el nuevo estándar de comunicación debido a que presenta muchas ventajas sobre su predecesor IPv4.

Con esta nueva versión del Protocolo IP, también nace la nueva versión del protocolo Mobile IP, esta es Mobile IPv6, es así que este protocolo se vuelve aun mas versátil, disminuyendo y sobre todo optimizando varios procedimientos que se llevan a cabo en la versión anterior, concretamente aparece un nuevo procedimiento de Notificación para hacer transparente el enrutamiento de paquetes destinados al nodo móvil mediante el uso de mensajes o Bindings. Desaparece la necesidad del agente extranjero, ya que un nodo móvil puede ser alcanzado directamente por un nodo correspondiente debido a la facilidad de IPv6 de autoconfigurarse en cualquier red o sub red. MIPv6 incorpora protocolos de

seguridad IP-Sec lo que proporciona enlaces más seguros y difíciles de acceder por nodos falsos o intrusos maliciosos.

Luego de este estudio se ha demostrado que la actual evolución de los sistemas celulares 2G hacia redes 2.5G o 3G esta directamente relacionada con el Internet Móvil y por ende al protocolo IP Móvil. En tal grado que el protocolo IP se convierte en protagonista, hasta tal punto que puede decirse que 3G es una red que tiende a ser "Todo IP". Es así que Mobile IP es compatible, y puede ser utilizado, con cualquier estándar de comunicaciones considerado 3G, en consecuencia Mobile IP puede utilizarse en ambas arquitecturas ya sea 3GPP o 3GPP2, esto asegura que operadoras en todo el mundo que utilicen tecnologías diferentes (GSM, CDMA) y que se encuentren en camino de obtener una licencia 3G puedan utilizar este protocolo independientemente de la tecnología que posean.

Un aspecto muy importante es el hecho de que Mobile IP presta un nivel de movilidad en capa de red (capa 3) la misma que es la solución mas indicada para casi todas las aplicaciones referentes a roaming de datos entre redes geográficamente distantes. También soluciona la necesidad de una movilidad multiaccseso, es decir cuando un terminal móvil multimodo se mueve entre diferentes redes de acceso. Por ejemplo, cuando un terminal multimodo se mueve de la cobertura de una red WCDMA hacia una red Bluetooth o WLAN este nodo obtiene nuevas direcciones IP. Cuando la dirección IP varía, las conexiones y las aplicaciones existentes se pierden, y necesitan ser reestablecidas. Una solución a este problema es también la utilización de Mobile IPv6. Este protocolo permite a los paquetes enviados a la dirección local ser entregados a la actual dirección de cuidado del nodo móvil. Además, Mobile IP puede “esconder” cualquier cambio en las direcciones en las capas de transporte y aplicación, permitiendo al nodo móvil realizar un roaming transparente entre diferentes redes de acceso.

Dentro del ámbito de las redes celulares 3G y debido a la gran cantidad de terminales prevista para los próximos años, el uso de IPv6 como protocolo de red se convierte en una necesidad urgente. Es así como en septiembre del 2005, de acuerdo con datos proyectados por UMTS Forum, las operadoras DoCoMo y 3,

de Japón y de Europa, respectivamente, llegarán a 1.8 millones de usuarios del servicio 3G, conocido técnicamente por W-CDMA. La empresa japonesa DoCoMo es responsable por más del 50% de los 1.8 millones de usuarios. Con estos datos reales podemos darnos cuenta de que el desarrollo tecnológico que hace pocos años parecía una meta inalcanzable actualmente se esta convirtiendo en una realidad palpable que esperemos en poco tiempo se haga presente en nuestro país. .

En lo relacionado a sus servicios y aplicaciones, Mobile IP brinda nuevas oportunidades de mercado para varios tipos de proveedores de servicios y empresas de telecomunicaciones, entre ellos proveedores de Internet, y operadoras celulares, como son Nextel (Argentina, México), Vodafone (Reino Unido), DoCoMo (Japón).

También es muy útil en áreas como: grupos empresariales de distintos tipos, campus universitarios, etc. Brindando en estos casos principalmente un servicio de VPNs o Redes Privadas Virtuales, en los que convergen varias tecnologías inalámbricas.

Otra área de gran aplicabilidad es la de redes móviles en distintos medios de transporte, como son aviones, barcos, y automóviles dando soporte a varios importantes servicios como son la Policía, Cuerpos de Bomberos, Guardacostas, Ambulancias etc.

6.2 RECOMENDACIONES

En esta sección se presentarán varias recomendaciones relacionadas principalmente a incentivar la investigación y la utilización de nuevas tecnologías, ya que lamentablemente nos hemos convertido únicamente en consumidores de tecnología más no en desarrolladores de la misma.

El protocolo Mobile IP es una excelente opción para que empresas de telecomunicaciones como ISP y operadoras celulares proporcionen nuevos de servicios de valor agregado. A su vez su utilización crearía nuevas empresas que

actualmente son inexistentes en nuestro mercado como son los Proveedores de Internet inalámbrico o WISP por sus siglas en inglés. Sería importante que ingenieros jóvenes y emprendedores juntaran esfuerzos y capitales para proveer de nuevos e innovadores servicios como el antes mencionado.

Hay que recalcar que el correspondiente organismo de regulación, CONATEL (Consejo Nacional de Telecomunicaciones), por medio de la SENATEL (Secretaría Nacional de Telecomunicaciones) deberían realizar un documento regulatorio normando y regulando, en todos los aspectos, estos nuevos servicios. Los mismos que serian supervisados por la SUPTEL (Superintendencia de Telecomunicaciones). Así también las nuevas empresas y las operadoras que brinden este servicio deberán contar con planes de Calidad de Servicio que cumplan con normas internacionales de calidad como las exigidas por la UIT (Unión Internacional de Telecomunicaciones).

Es interesante conocer como varias universidades entre ellas la Universidad de Rice, la Universidad Nacional de Singapur, la Universidad de Stanford entre otras han desarrollado proyectos de investigación y experimentación con el protocolo Mobile IP, sería muy importante incentivar a las nuevas generaciones de alumnos de nuestra facultad a que participen activamente en proyectos relacionados con nueva tecnología.

REFERENCIAS BIBLIOGRAFICAS

- OLIVER, Miquel; LOURO, Oscar. **Mobile IP: Una solución para proporcionar la movilidad de los terminales en Internet,** Grup de Comunicacions Mòbils i de Banda Ampla, Departament de Matemàtica Aplicada i Telemàtica (DMAT), Universitat Politècnica de Catalunya.

- PERKINS, Charles, **Mobile IP,** IEEE Communications Magazine Volumen: 35 5, Mayo 1997, Paginas: 84 –99.

- LEE, David; LEE, William, **Mobile IP/sup 2,** Microwave and Millimeter Wave Technology, 2000, 2nd International Conference on ICMMT 2000, Paginas: 403 – 407.

- JAIN, Paresh; KELKAR, Rakesh, **Mobile IP,** TATA Consultancy Services.
- HAGEN Silvia**, IPv6 Essentials.**

- YEGIN, Alper; WILLIAMS, Carl, **IPv6: Necessary for Mobile and Wireless**
- **Internet,** Internet Society, Junio 2003.

- EL MALKI, Karim**, IPv6 and 3G Mobile Networks,** IP Infrastructure Core Unit Core Network Development Ericsson, Octibre 2003.

- PERKINS, C; JHONSON, D, ARKKO, J**, Mobility Support in IPv6,** IETF Mobile IP Working Group, Internet-Draft, 1999.

- AIT YAIZ Rachid; OZTURK Osman, **Mobility in IPV6**.

- GALINDO, Luis, **Multimedia Móvil: UMTS versión 5,** Mundo Internet 2002, VII Congreso Nacional de Usuarios de Internet, 2002.

- DE DIEGO, María; GALLEGO, Diego; LOPEZ, José; GOMEZ, Alberto, **UMTS: Hacia una red todp IP,** Comunicaciones de Telefónica Investigación y Desarrollo Número 24, Enero 2002.

- CUERVO, Miguel, **UMTS sobre IP,** Sistemas computacionales de alta velocidad, Universidad de Las Palmas de Gran Canaria.

- RYSAVY, Peter, **Capacidades de datos para la evolución GSM a UMTS,** Rysavy Research, Noviembre 2002, http://www.rysavy.com

- SCHMITZ Paul; WEAVER Geoff; **MIPv6: New Capabilities for Seamless Roaming Among Wired, Wireless, and Cellular Networks**, Intel Developer UPDATE Magazine, Septiembre 2002.
- GARG, Vijak; TEJWANI, Harish, **Mobile IP for 3G wireless networks,** Personal Wireless Communications, 2000 IEEE International Conference on, 2000, Paginas: 240 –244.

- BALI, Soshant; KORAH Jhon, **Quality of Service in 3G Wireless Networks**, Department of Electrical and Computer Engineering, Virginia Polytechnic Institute / State University.

- PHILIPPOPOULUS, Panos; KALOXYLOS, Alexandros; DAGIUKLAS, Tasos, **3G Network & Service Provisión Architecture Evolutions,** OTE-Consulting, Universidad de Atenas, Intracom S.A.

- PATEL, Girish; DENNETT, Steven, **The 3GPP and 3GPP2 Movements Toward an All-IP Mobile Networks,** IEEE Personal Communications, Agosto 2000.

- CUEVAS, Antonio; GARCIA, Carlos; MORENO, José; SOTO, Ignacio, **Los pilares de las redes 4G: QoS, AAA y Movilidad,** Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid.

- CHIUSSI, Fabio; KHOTIMSKY, Denis; KRISHNAN, Santosh, **Mobility Management in Thirtd Generation All-IP Networks,** IEEE Communications Magazine, Septiembre 2002.

- MOH, Melody; BERQUIN, Gregorie; YANJUN Chen, **Mobile IP telephony: Mobility Support of SIP,** Computer Communications and Networks, 1999. Proceedings. Eight International Conference on, 1999, Paginas: 554 –559.

- McCANN, Peter; HILLER, Tom, **An Internet infrastructure for cellular CDMA networks using mobile IP,** IEEE Personal Communications Volume: 7 4 , Agosto 2000, Paginas: 26 –32

- LA PORTA, Thomas; SALGARELLI, Luca; FOSTER, Gerard, **Mobile IP and Wide Area Wireless Data,** Wireless Communications and Networking Conference,1999. WCNC.1999 IEEE ,1999, Paginas: 1528 - 1532 volumen 3.

- LEMILAINEN, Jussi; HAVERINEN, Henry, **IP Telephony GSM Interworking,** Global Telecommunications Conference GLOBECOM '99 Volumen: 5, 1999 , Paginas: 2709 -2713 volumen 5.

- DAS, Subir; MISRA, Archan; AGRAWAL, Prathima, **TeleMIP: Telecommunications-Enhanced Mobile IP Architecture for Fast Intradomain Mobility,** IEEE Personal Communications Volume: 7 4 , Agosto 2000, Paginas: 50 –58.

- ROBERT, Lionel; PISSINOU, Niki; MAKKI, Sam, **Third Generation Wireless Network: The Integration of GSM and Mobile IP,** Wireless Communications and Networking Conference, 2000. WCNC. 2000 IEEE Volumen: 3, 2000, Paginas: 1291 –1296.
- FAN, L; SHERIFF, R; GARDINER, J, **Satellite-UMTS Service Provision Using IP-Based Technology,** Vehicular Technology Conference Proceedings, 2000. Tokyo. 2000 IEEE 51st Volumen: 3, 2000, Paginas: 1970 -1974 volumen 3.

- HAN-CHIEH Chao; YEN-MING Chu; MU-TAI Lin, **The Implication of the Next-Generation Wireless Network Design: Cellular Mobile IPv6,** Consumer Electronics, IEEE Transactions Volumen: 46 3 , Agosto 2000 , Paginas: 656 –663.

- www.nokia.com, Introducing Mobile IPv6 in 2G and 3G mobile networks.

- www.ericsson.com, KARAGIANNIS, Georgios, **Mobile IP,** Julio 1999.

- www.ipv6.unam.mx, Tutorial de IPv6. Diciembre 2000.

- www.cisco.com/go/mobile_ip, Cisco Mobile IP.

- www.umtsforum.net

- www.itba.edu.ar

- www.3gamericas.org, El Proyecto conjunto de Tercera Generación (3GPP) aprueba a 3G Americas como socio representante en el mercado.

- http://services.eng.uts.edu.au/kumbes/capstone/fdiop/mip-in-cdma2000.htm, MIP in CDMA 2000.

INDICE DE TABLAS

Capitulo II: Protocolo de Internet Móvil o Mobile IP

El agente local, mantiene una lista de relaciones de movilidad en una tabla de movilidad donde cada anotación es identificada por la dirección IP local permanente, la dirección de cuidado y el tiempo de vida.

El agente extranjero mantiene una lista de visitantes, la cual contiene información acerca de los nodos móviles que están de visita en su red. Cada anotación en la lista de visitantes es identificada por la dirección IP local permanente, dirección del agente local, dirección del medio del nodo móvil, y el tiempo de vida.

INDICE DE FIGURAS

Capitulo I: Introducción

Capitulo II: Protocolo de Internet Móvil o Mobile IP

Capitulo III: Relación de Mobile IP con IPv4 e IPv6

Capitulo IV: Integración de Mobile IP con tecnologías de Tercera Generación: UMTS y CDMA2000

Capitulo V: Servicios y Aplicaciones que brinda Mobile IP

Sangolquí,

ELABORADO POR:

_____

Sr. Francisco David Chang Baldeón

AUTORIDADES:

_____

Sr. Ing. Marcelo Gómez Cobos

TCRN. Estado Mayor

Decano de la Facultad de Ingeniería Electrónica

_____

Sr. Dr. Jorge Carvajal

Secretario Académico de la Facultad de Ingeniería Electrónica