IPV6 EN LAS REDES MOVILES

DAVID ENRIQUE CASTRO CAMPO
OSCAR DAVID MARTINEZ BARRIOS

DIRECTOR: GONZALO DE JESUS LOPEZ VERGARA

FACULTAD DE INGENIERÍAS
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
CARTAGENA DE INDIAS D.T.C. e H.
DICIEMBRE DE 2012

IPV6 EN LAS REDES MOVILES

DAVID ENRIQUE CASTRO CAMPO
OSCAR DAVID MARTINEZ BARRIOS

Monografía presentada como requisito para optar al título de Especialista en Telecomunicaciones.

Director:
Ing. Gonzalo López Vergara.

FACULTAD DE INGENIERÍAS
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
CARTAGENA DE INDIAS D.T.C. e H.
DICIEMBRE DE 2012

Cartagena, Diciembre de 2012.

Señores

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

Comité Evaluación de Proyectos

Ciudad.

Respetados señores.

Cordialmente nos permitimos hacer a ustedes entrega de la monografía titulada **"IPV6 EN LAS REDES MOVILES",** para su estudio y aprobación, como requisito para obtener el título de Especialista en Telecomunicaciones.

Espero cumplir con los estándares establecidos por la Institución.

Muy respetuosamente,

DAVID ENRIQUE CASTRO CAMPO OSCAR DAVID MARTINEZ BARRIOS

AUTORIZACIÓN

Cartagena de Indias, D. T. H. Y C. 13 de Diciembre de 2012

Yo **DAVID ENRIQUE CASTRO CAMPO** identificado con la cédula de ciudadanía número 73.007.115 de Cartagena.

Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

DAVID ENRIQUE CASTRO CAMPO

AUTORIZACIÓN

Cartagena de Indias, D. T. H. Y C. 13 de Diciembre de 2012

Yo **OSCAR DAVID MARTINEZ BARRIOS** identificado con la cédula de ciudadanía número 73.195.184 de Cartagena.

Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

OSCAR DAVID MARTINEZ BARRIOS

AGRADECIMIENTOS

Ante todo agradezco a Dios por brindarme salud y darme la luz para prepararme en estudios y la sabiduría para culminar con éxitos este proceso.

A mis padres Robinson Castro y Alma Campo, por darme la vida y encaminarme por el sendero del bien con sus sabios consejos; así como también la motivación necesaria para comenzar este arduo camino que si Dios lo permite en estos días se estará concretando con una graduación.

También se le agradece a mi única hermana, que con sus simples palabras y su ejemplo, me hace no pensar en abandonar los propósitos que he colocado en mi vida como proyecto de vida.

Obviamente a mi futura esposa Carla Díaz, quien con su interminable energía, es capaz de hacerme levantar en los momentos que pienso en abandonar el camino, y suplirlo por algún otro medio o mecanismo.

Mis sobrinos, también fueron de gran apoyo, aunque ellos ni se imaginen, me ponen a idealizar un mundo próximo, el cual me gustaría garantizarle las mejores cosas a ellos, y por lo cual estoy luchando y tratando de salir adelante, sobre todo para que puedan algún día verme como ejemplo y mencionarme en generaciones próximas, porque no me gustaría desfallecer y quedar en el olvido como un X.

GRACIAS

INGENIERO DAVID ENRIQUE CASTRO CAMPO

Este trabajo se lo dedico primeramente a Jehová DIOS, quién me ha dado todo, la vida, mis estudios, mi familia, amigos y la oportunidad de seguir triunfando en todos los aspectos de mi vida.

A mi madre querida; MARÍA BARRIOS LADEUS, gracias por tu apoyo incondicional y dedicación, porque gracias a ella y por ella soy lo que soy hoy en día. Así como a mi abuela Adelaida Ladeus por la crianza que me impartió, A mis primas Lilibeth y Marelis por su comprensión, apoyo y amistad.

Especialmente le dedico este logro a mi familia, a mi hija hermosa Sury Martínez Villarreal, el más grande logro de mi vida del cual me siento orgulloso, por ella lucho cada día por ser mejor y a mi esposa Marisol Villarreal por brindarme su paciencia, amor, apoyo, colaboración y comprensión.

Y en general a todas aquellas personas que hicieron posible alcanzar este logro tan importante en mi vida.

Gracias.

INGENIERO.OSCAR DAVID MARTINEZ BARRIOS

Nota de aceptación

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

TABLA DE CONTENIDO

Tabla de Figuras

LISTA DE TABLAS

INTRODUCCIÓN

Desde el punto de vista de la ingeniería, las redes de ordenadores no son un asunto trivial. Para empezar, los datos no se pueden enviar por un cable directamente, porque los ordenadores conectados a la red no tendrían modo de saber a cuál de ellos se dirigen o cuál es su contenido.

Por este motivo se inventaron los protocolos, un conjunto de mensajes que se envían por la red junto con los datos, y que traducidos al lenguaje humano representan el equivalente a los saludos y notificaciones que no aportan información: "Hola ordenador 2", "Te envío un archivo", "Ya lo he recibido", "Adiós". La información sería, claro está, el archivo.

Hasta el día de hoy la red Internet funciona gracias a un protocolo general para redes de ordenadores llamado TCP/IP (Transfer Control Protocol/Internet Protocol), en concreto la versión 4, o IPv4.

EL PROTOCOLO IP O INTERNET PROTOCOL

Los protocolos IP son de vital importancia en la interconexión de redes. Transmiten información entre redes autónomas e independientes (Como Ethernet, X.25 y RDSI). Los protocolos IP definen la forma en que las subredes se interconectan y la manera en que funcionan los dispositivos de interconexión.

IP define la manera que se enrutan los paquetes entre las redes. Cada nodo en cada una de las redes tiene una dirección IP diferente. Para garantizar un correcto enrutamiento, IP agrega su propio encabezado a los datagramas. Este proceso se apoya en tablas de enrutamiento que son actualizadas permanentemente. En caso

de que el paquete de datos sea demasiado grande, los protocolos IP lo fragmentan para poderlo transportar.

IP es un protocolo que no está orientado a la conexión y no es confiable, por lo que se usa con TCP, que ofrece la confiabilidad que hace falta. Para efectuar su labor, los protocolos IP se apoyan en diversos conceptos como son:

- DNS (Domain Name Servers)
- Direcciones Internet (Direcciones IP)
- Paquetes IP
- Enrutamiento IP/Protocolos de Enrutamiento
- ICMP (Internet Control Message Protocol)

Cada ordenador conectado a Internet debe tener su propia dirección IP, sea un servidor de páginas Web o un ordenador doméstico que se conecta temporalmente a la red mediante un módem. En este último caso se asigna una IP dinámica, que cuando ya no esté en uso puede asignarse a otro usuario. Por este motivo los proveedores de acceso a Internet o ISPs deben reservar un cierto número de direcciones IP para sus abonados.

En este módulo se analizan algunos problemas acerca de la implementación de IPv6 en la red móvil. El despliegue de IPv6 en la capa de usuario, la PLMN (Public Land Mobile Network), el (backbone), y la (inter-PLMN) capa (entre redes de los operadores), esto significa que las capas operan principalmente e independientemente una de otra. Esto es debido a la separación de la capa utilizada en GPRS (General Packet Radio Service) y UMTS (Universal Mobile Telecomunicaciones, System).

3GPP ha ordenado el uso de IPv6 en el subsistema multimedia IP. Desde el punto de vista de la red móvil, el creciente uso de IPv6 en la capa de usuario, incluyendo IPv6 terminales que permite una interoperabilidad sin fisuras a través de la

promoción de una versión del protocolo único para todos los dispositivos y servicios. IPv6 también es recomendado por el 3GPP para la RAN (Radio Access Network) y es opcional para todos los sistemas de datos móviles, incluyendo los basados en la versión 99 la tecnología GPRS.

Presentamos aquí algunos importantes componentes de IPv6 móvil, móvil cabecera IPv6 y la estructura de datos (Binding cache) que es una caché de enlace de autenticación, mantenida por cualquier nodo, el cual realiza la optimización de ruta, a la entrega directa de paquetes a MN.

Los principios de seguridad para redes fijas IPv6 no son las mismas para IPv6 móvil. El nodo móvil (MN) siempre es direccionable con su dirección asignado de home address. El cuidado de los cambios de dirección en cada momento es muy difícil de mantener pre configurado por la Asociación de Seguridad (SA). En caso de VPN, las reglas para el filtrado de datagrama cambia cada vez que se mueve cuando los nodos móviles de una red a otra.

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP.
El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de lo datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish.

Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente.

Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

1. OBJETIVOS

1.1. GENERAL

Traducir el módulo que habla de la implementación de ipv6 en las redes móviles

1.2 ESPECÍFICOS

- ✓ Describir que es, para qué sirve el protocolo ipv6.
- ✓ Detallar como se implementa el protocolo ipv6 en redes móviles
- ✓ Explicar las ventajas y desventajas de implementar este protocolo de nueva generación

2. JUSTIFICACION

- IPv6 retiene varias de las características que hicieron IPv4 exitoso. Por ejemplo IPv6 también es no orientado a la conexión (conectionless)
- Tamaño del direccionamiento: fue extendido a 128 bits.
- Formato del encabezado: más grande pero con menos campos.
- Encabezados de extensión: en lugar de opciones, el encabezado base puede preceder cero o más encabezados de extensión seguidos por los datos.
- Soporte de audio y video: IPv6 incluye mecanismos para ofrecer el tipo de servicio requerido por este tipo de tráfico.
- El protocolo es extensible: Es posible definir nuevos encabezados y con ello agregar o probar nuevas características.
- Como IPv4, IPv6 también usa un esquema de direcciones configurables.
- Se mantiene la jerarquía dirección de red como prefijo y la de la interfaz como sufijo.
- IPv6 no reserva direcciones broadcast (de difusión)
- Tipos de direcciones en IPv6:
- unicast: Corresponde a una interfaz única (un computador)
- multicast: Corresponde a un grupo de computadores. Cuando un datagrama es enviado a esta dirección, cada miembro del grupo multicast recibe una copia del mensaje.

- Cluster (también anycast): Corresponde a un grupo de computadores que comparten un prefijo común. El datagrama es enviado sólo a un computador de este grupo.

3. MARCO CONCEPTUAL

¿Qué es el IPv6?

IPv6 (Internet Protocol Version 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.

En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características.

¿Por qué surge IPV6?

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

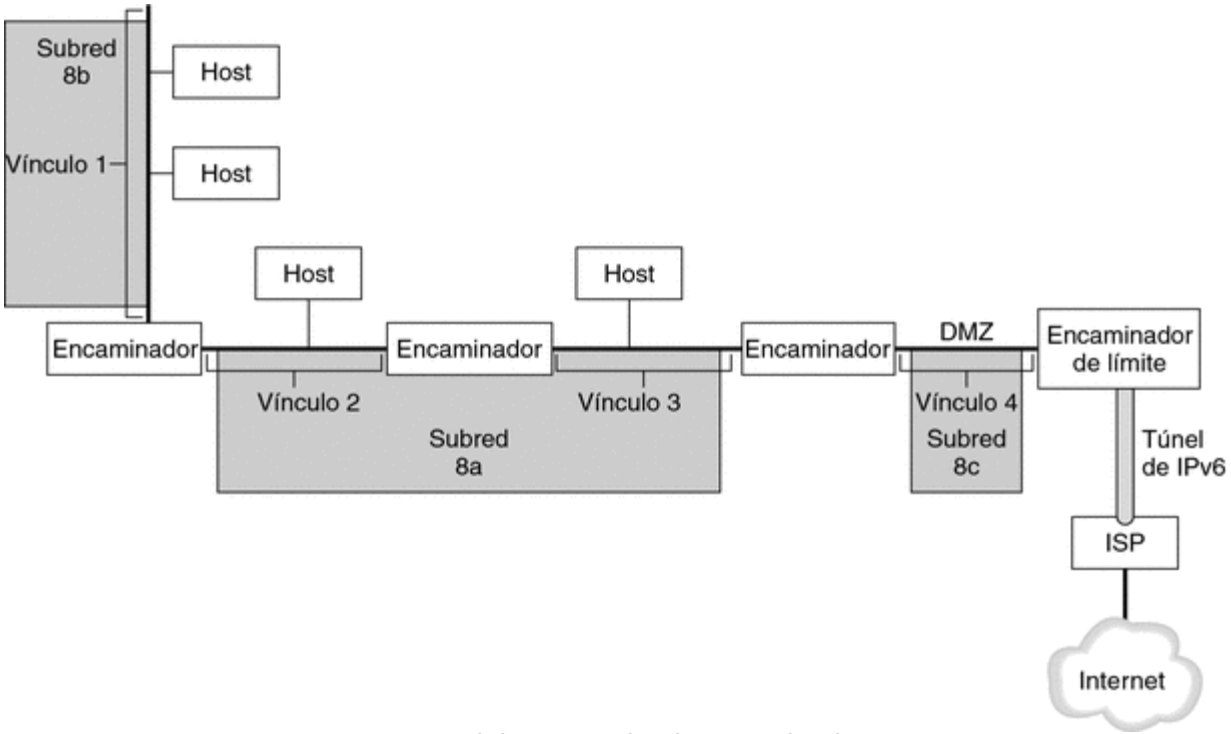
Otros de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el backbone de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad.

DESCRIPCIÓN GENERAL DE LAS REDES IPV6

En la figura siguiente se muestran los componentes básicos de una red IPv6.

Figura 1 Componentes básicos de una red IPv6



Fuente: ITU Module 5 IPV6 implementation in Mobile

La figura ilustra una red IPv6 y sus conexiones con un ISP. La red interna consta de los vínculos 1, 2, 3 y 4. Los hosts rellenan los vínculos y un enrutador los termina. El vínculo 4, considerado la DMZ de la red, queda terminado en un extremo por el enrutador de límite. El enrutador de límite ejecuta un túnel IPv6 a un ISP, que ofrece conexión a Internet para la red. Los vínculos 2 y 3 se administran como subred 8a. La subred 8b tan sólo consta de sistemas en el vínculo 1. La subred 8c es contigua a la DMZ del vínculo 4.

Como se muestra en la (Figura 1), una red IPv6 tiene prácticamente los mismos componentes que una red IPv4. No obstante, la terminología de IPv6 presenta ligeras diferencias respecto a la de IPv4. A continuación se presenta una serie de términos sobre componentes de red empleados en un contexto de IPv6.

Nodo

Sistema con una dirección IPv6 y una interfaz configurada para admitir IPv6. Término genérico que se aplica a hosts y enrutadores.

Enrutador de IPv6

Nodo que reenvía paquetes de IPv6. Para admitir IPv6, debe configurarse como mínimo una de las interfaces del enrutador. Un enrutador de IPv6 también puede anunciar el prefijo de sitio IPv6 registrado para la empresa en la red interna.

Host de IPv6

Nodo con una dirección IPv6. Un host IPv6 puede tener configurada más de una interfaz para que sea compatible con IPv6. Al igual que en IPv4, los hosts de IPv6 no reenvían paquetes.

Vínculo

Un solo soporte contiguo de red conectado por un enrutador en cualquiera de sus extremos.

Vecino

Nodo de IPv6 que se encuentra en el mismo vínculo que el nodo local.

Subred IPv6

Segmento administrativo de una red IPv6. Los componentes de una subred IPv6 se pueden corresponder directamente con todos los nodos de un vínculo, igual que en IPv4. Si es preciso, los nodos de un vínculo se pueden administrar en subredes independientes. Además, IPv6 no permite subredes multivínculo, en las cuales los nodos de vínculos distintos pueden ser componentes de una sola subred. Los vínculos 2 y 3 de la (Figura 3–1) son componentes de la subred 8a multivínculo.

Túnel de IPv6

Túnel que proporciona una ruta de extremo a extremo virtual entre un nodo de IPv6 y otro punto final de nodo de IPv6. IPv6 permite la configuración manual de túneles y automática de túneles de 6to4.

Enrutador de límite

Enrutador en el límite de una red que proporciona un extremo del túnel de IPv6 a un punto final fuera de la red local. Este enrutador debe tener como mínimo una interfaz de IPv6 a la red interna. En cuanto a la red externa, el enrutador puede tener una interfaz de IPv6 o IPv4.

CARACTERÍSTICAS PRINCIPALES DE IPVB6

- 1Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.

- Simplificación del formato de la cabecera. Algunos campos de la cabecera en IPv4 se quitan o se hacen opcionales

- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los enrutadores, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del enrutador.

- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.

- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.

- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.

- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.

- Renumeración y "multihoming": facilitando el cambio de proveedor de servicios.
- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Capacidades de autenticación y privacidad

¿Qué tan grande es el espacio de direcciones?

Habrían 2 ^ 128 direcciones IP diferentes, significa que si la población mundial fuera de 10 billones habría 3.4 * 10 ^ 27 direcciones por persona. O visto de otra forma habría un promedio de 2.2 * 10 ^ 20 direcciones por centímetro cuadrado. Siendo así muy pequeña la posibilidad de que se agoten las nuevas direcciones.

DIRECCIONAMIENTO

Las direcciones son de 128 bits e identifican interfaces individuales o conjuntos de interfaces. Al igual que en IPv4 en los nodos se asignan a interfaces.

Se clasifican en tres tipos:

- *Unicast* identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección.

- *Anycast* identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast.

- *Multicast* identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección.

En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

REPRESENTACIÓN DE LAS DIRECCIONES

Existen tres formas de representar las direcciones IPv6 como cadena de texto.

- x:x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo.

  Ejemplos:

  FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
  1080:0:0:0:8:800:200C:417A

- Como será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintácticamente **::**

para representarlos. El uso de :: indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección.

Por ejemplo:

1080:0:0:0:8:800:200C:417A	unicast address
FF01:0:0:0:0:0:0:101	multicast address
0:0:0:0:0:0:0:1	loopback address
0:0:0:0:0:0:0:0	unspecified addresses

podrán ser representadas como:

1080::8:800:200C:417A	unicast address
FF01::101	multicast address
::1	loopback address
::	unspecified addresses

- Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis:

  x:x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4. Ejemplos:

  0:0:0:0:0:0:13.1.68.3
  0:0:0:0:0: FFFF: 129.144.52.38

  o en la forma comprimida

:13.1.68.3

:FFFF:129.144.52.38

REPRESENTACIÓN DE LOS PREFIJOS DE LAS DIRECCIONES

Los prefijos de identificadores de subredes, routers y rangos de direcciones IPv6 son expresados de la misma forma que en la notación CIDR utilizada en IPv4.
Un prefijo de dirección IPv6 se representa con la siguiente notación:

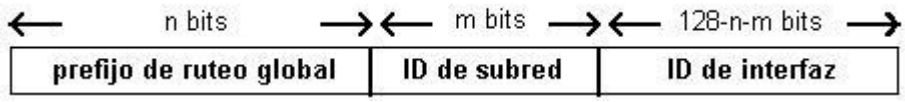
Direccion-ipv6/longitud-prefijo, donde

Direccion-ipv6: es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.

Longitud-prefijo: es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección.

Direcciones Global Unicast

Formato de las direcciones global unicast

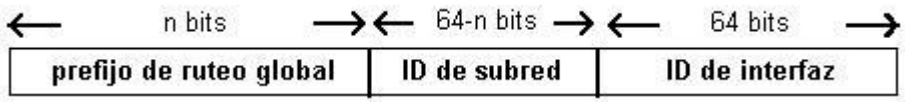


Prefijo de ruteo global: es un prefijo asignado a un sitio, generalmente está estructurado jerárquicamente por los RIRs e ISPs.

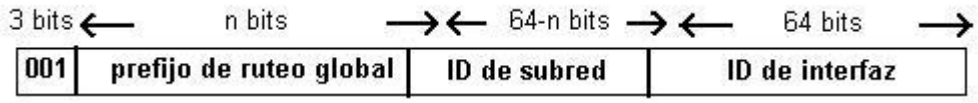
Identificador de Subred: es el identificador de una subred dentro de un sitio. Está diseñado para que los administradores de los sitios lo estructuren jerárquicamente

Identificador de Interfaz: es el identificador de una interfaz. En todas las direcciones unicast, excepto las que comienzan con el valor binario 000, el identificador de interfaz debe ser de 64 bits y estar construido en el formato Modified EUI-64.

El formato para este caso es el siguiente:



El siguiente es un ejemplo del formato de direcciones global unicast bajo el prefijo 2000/3 administrado por el IANA



La asignación del espacio de direcciones IPv6 global unicast está accesible en IPV6 GLOBAL UNICAST ADDRESS ASSIGNMENTS

DNS

El almacenamiento actual de direcciones de Internet en el Domain Name System (DNS) de IPv4 no se puede extender fácilmente para que soporte direcciones IPv6 de 128 bits, ya que las aplicaciones asumen que a las consultas de direcciones se retornan solamente direcciones IPv4 de 32 bits.

Para poder almacenar las direcciones IPv6 se definieron las siguientes extensiones un nuevo tipo de registro, el registro AAAA. Se usa para almacenar

direcciones IPv6, porque las extensiones están diseñadas para ser compatibles con implementaciones de DNS existentes;

- un nuevo dominio para soportar búsquedas basadas en direcciones IPv6. Este dominio es IP6.ARPA;
- Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también procesar direcciones IPv6.

Los cambios son diseñados para ser compatibles con el software existente. Se mantiene el soporte de direcciones IPv4.

MECANISMOS DE TRANSICIÓN BÁSICOS

Los mecanismos de transición son un conjunto de mecanismos y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de Internet al IPv6 con la menor interrupción posible.

Existen dos mecanismos básicos:

- *Dual Stack*: provee soporte completo para IPv4 e IPv6 en host y routers.
- *Tunneling*: encapsula paquetes IPv6 dentro de headers IPv4 siendo transportados a través de infraestructura de ruteo IPv4.

Dichos mecanismos están diseñados para ser usados por hosts y routers IPv6 que necesitan interoperar con hosts IPv4 y utilizar infraestructuras de ruteo IPv4. Se espera que muchos nodos necesitarán compatibilidad por mucho tiempo y quizás indefinidamente. No obstante, IPv6 también puede ser usado en ambientes donde no se requiere interoperabilidad con IPv4. Nodos diseñados para esos ambientes no necesitan usar ni implementar estos mecanismos.

DUAL STACK

La forma más directa para los nodos IPv6 de ser compatibles con nodos IPv4-only es proveyendo una implementación completa de IPv4. Los nodos IPv6 que proveen una implementación completa de IPv4 (además de su implementación de IPv6) son llamados nodos “IPv6/IPv4”. Estos nodos tienen la habilidad de enviar y recibir paquetes IPv6 e IPv4, pudiendo así interoperar directamente con nodos IPv4 usando paquetes IPv4, y también operar con nodos IPv6 usando paquetes IPv6.

TÚNELES (Tunneling).

En la mayoría de las empresas, la implantación de IPv6 en una red IPv4 ya configurada debe realizarse de manera gradual y por fases. El entorno de redes de pila doble de Oracle Solaris permite el funcionamiento compatible de IPv4 e IPv6. Debido a que casi todas las redes emplean el protocolo IPv4, en la actualidad las redes IPv6 necesitan una forma de comunicarse más allá de sus límites. Para ello, las redes IPv6 se sirven de los túneles.

En buena parte de las situaciones hipotéticas para túneles de IPv6, el paquete de IPv6 saliente se encapsula en un paquete de IPv4. El enrutador de límite de la red IPv6 configura un túnel de extremo a extremo a través de varias redes IPv4 hasta el enrutador de límite de la red IPv6 de destino. El paquete se desplaza por el túnel en dirección al enrutador de límite de la red de destino, que se encarga de desencapsular el paquete.

A continuación, el enrutador reenvía el paquete IPv6 desencapsulado al nodo de destino.

Los nodos o redes IPv6 que se encuentran separados por infraestructuras IPv4 pueden construir un enlace virtual, configurando un túnel. Paquetes IPv6 que van hacia un dominio IPv6 serán encapsulados dentro de paquetes IPv4. Los extremos del túnel son dos direcciones IPv4 y dos IPv6. Se pueden utilizar dos tipos de túneles: configurados y automáticos. Los túneles configurados son creados mediante configuración manual. Un ejemplo de redes conteniendo túneles configurados es el 6bone.

La red 6bone era una red IPv6 de carácter experimental creada para ayudar a los vendedores y usuarios a participar en la evolución y transición a IPv6. Su enfoque original fue la prueba de estándares e implementaciones. Su objetivo principal era la realización de pruebas de procedimientos interoperacionales y transicionales.

En marzo de 1996, la red 6bone empezó sus funciones como un proyecto de colaboración entre Norteamérica, Europa y Japón. Los primeros túneles se establecieron entre los laboratorios IPv6, G6 de Francia, UNI-C de Dinamarca y WIDE de Japón, bajo la coordinación de la IETF.

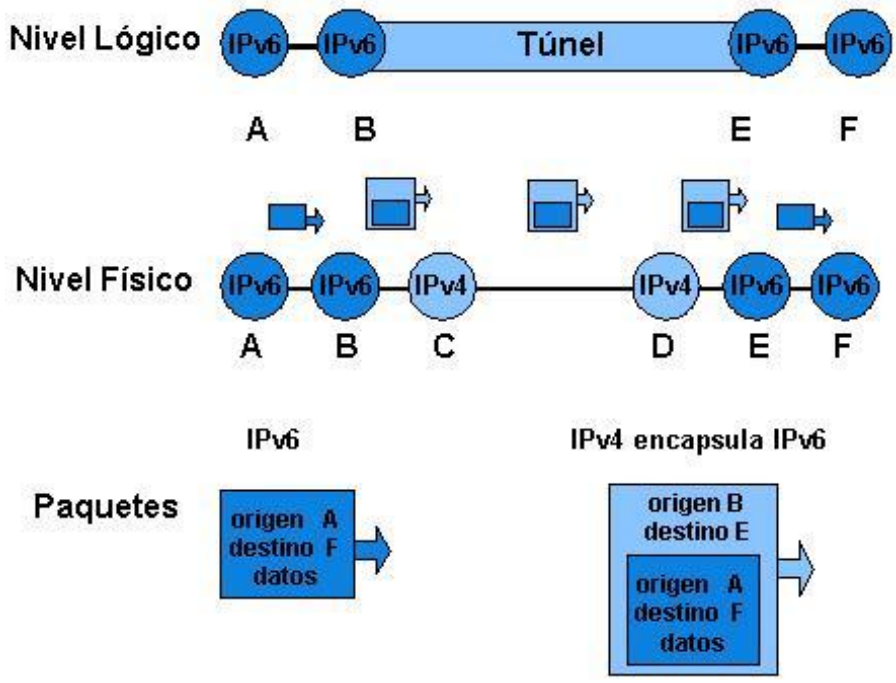
Breve reseña histórica

- 1999 Primera conexión al 6Bone por túnel con freenet6 en Canadá.
- 1999 Delegación bloque 3ffe:8070:100c::/48 por UNAM. (BGP).
- 2000 Conexión permanente a 6BONE por BGP vía UNAM en México.
- 2000 Servidor WWW sobre Windows NT 4.0.
- 2002 Obtención rangopNLA3ffe:400f::/32(6Bone).
- 2003 Obtención para REUNA del rango de Producción 2001:1310::/32.
- 2003 Conexión alM6Boneo red Multicast IPv6 vía UDG en México.
- 2003 Instalación de IPv6 enTroncalesde Investigación en REUNA.
- 2004 Aire-6 Proyecto de Redes inalámbricas con IPv6.

- 2005 UACh. Primera Red IPv6 de Producción Operativa en Chile.
- 2006 6 de junio, fue cerrado el proyecto.

Los túneles automáticos no necesitan configuración manual. Los extremos se determinan automáticamente determinados usando direcciones IPv6 IPv4-compatible

Figura 1.1. IPV6



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

4. IMPLEMENTACION DE IPV6 EN LAS REDES MOVILES

REDES MÓVILES E IPV6

El despliegue de IPv6 en la capa de usuario, la PLMN (Public Land Mobile Network) el backbone, y la inter-PLMN capa (entre redes de los operadores) significa que las capas operan principalmente independientemente uno de otro. Esto es debido a la separación de la capa utilizada en GPRS (General Packet Radio Service) y UMTS (Universal Mobile Telecommunications System) o a causa de los mecanismos de interoperabilidad IPv4/IPv6.

3GPP ha ordenado el uso de IPv6 en el subsistema multimedia IP. Desde el punto de vista de la red móvil, el creciente uso de IPv6 en la capa de usuario, incluyendo IPv6 terminales que permite una interoperabilidad sin fisuras a través de la promoción de una versión del protocolo único para todos los dispositivos y servicios. IPv6 también es recomendado por el 3GPP para la RAN (Radio Access Network) y es opcional para todos los sistemas de datos móviles, incluyendo los basados en la versión 99 la tecnología GPRS.

Una ventaja obvia del protocolo IPv6 es el espacio de direcciones de gran tamaño que proporciona. Por lo tanto, la necesidad de traductores de direcciones de red (NAT) que actualmente se requieren en las redes IPv4 base es eliminada. IPv6 proporciona espacio suficiente para acomodar la dirección de millones de usuarios en todo el mundo, e incluso un gran número de direcciones IPv6 personales pueden ser permitidas. Este es un escenario atractivo para los mercados emergentes, particularmente de redes totalmente nuevos operadores móviles, ya que las tareas son más fáciles a través de un número menor de elementos y protocolos que deben gestionarse. La razón de esto es que los traductores de

direcciones de red (NAT) y de mapeo entre espacios de direcciones privados y públicos no deben ser administrados.

NAT es ampliamente y con éxito el Internet de hoy en día, porque la mayoría de las aplicaciones están basadas en cliente/servidor. Este no es el caso en las redes móviles futuras, donde la comunicación entre los teléfonos móviles y cualquier otro dispositivo en red son en su mayoría peer to peer y requeriría direcciones globales.

La ausencia de NAT permite la accesibilidad global, con toda verdad a cualquier tipo de conectividad y de red iniciadas por los servicios IP. Esta es una ventaja importante para el interfuncionamiento de redes celulares y del Internet del futuro, y será crítico para el crecimiento continuo y el éxito de estas redes. La comunicación entre dispositivos de sólo IPv6 e IPv4 también es posible. Sin embargo, esto requiere un mecanismo de traducción, tales como la dirección de red Traductor / Protocolo Translator (NAT-PT), que puede convertirse en un cuello de botella del rendimiento y tal vez podría limitar la capacidad y escalabilidad de las plataformas de prestación de servicios.

4.1 ENLACE CAPA DE MOVILIDAD

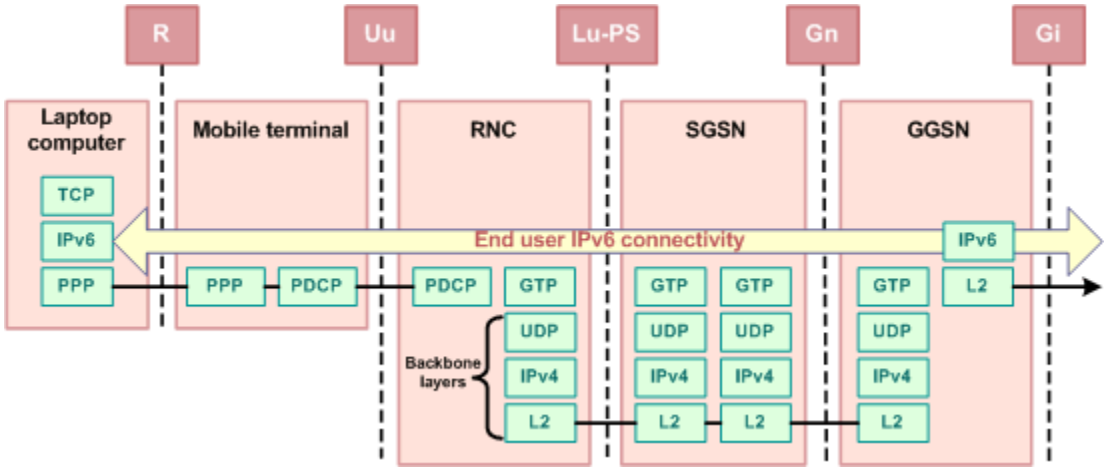
En 2G y 3G de redes móviles, se gestiona la movilidad es decir, por debajo del plano de usuario de capa de red en la capa 2 (la capa de enlace). La capa 2 de gestión de la movilidad también se utiliza en otros sistemas, tales como Wireless y LAN, por entregas entre puntos de acceso.

UMTS es un término más general para el sistema de telecomunicaciones 3G (tercera generación), basado en la interfaz de radio WCDMA de alta capacidad. El objetivo de UMTS es la conmutación de paquetes (Packet Switched (PS)) de dominio, es proporcionar conectividad de capa 2 global que pueda soportar

cualquier protocolo de capa 3. GPRS Tunneling Protocolo (GTP) se encarga de la global (macro) movilidad.

El MT (Mobile Terminal) está unido al mismo GGSN (Gateway nodo de soporte GPRS) AP todo el tiempo, y mantiene su dirección de capa 3 (por ejemplo direcciones IPv6). En este caso no hay necesidad vital para IP Móvil. La (figura 1.1) muestra una estructura simplificada del protocolo de transporte en el dominio UMTS PS, donde el nivel de usuario IPv6 es tunelizado a través de los elementos internos de GPRS. En la figura, un ordenador portátil está conectado a la red mediante un WCDMA (Wideband Acceso Múltiple por División de Código) de terminal como un módem. (El llamado telefónico de emulación).

Figura 1.2 WCDMA (Wideband Acceso Múltiple por División de Código)



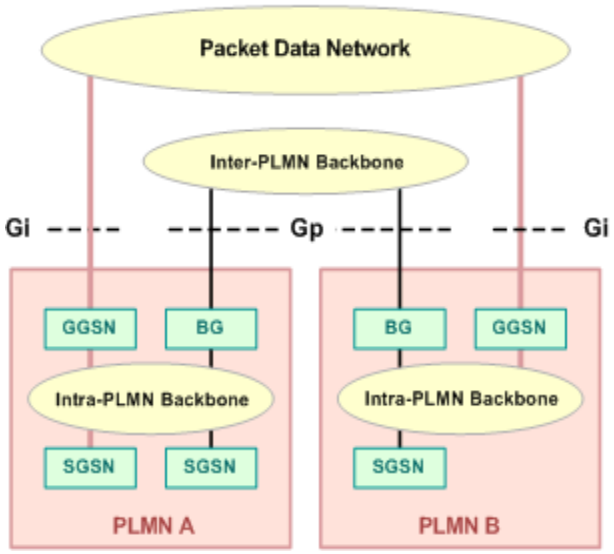
Fuente: ITU Module 5 IPV6 implementation in Mobile networks

El MT (móvil terminal) conectado al GPRS puede asignar una dirección IP estática o dinámica. La dirección estática asignada por el Home Public Land Mobile Network (HPLMN) es operada en el momento de la suscripción. La dirección IP dinámica puede ser asignada por el GGSN de cualquiera de HPLMN o la PLMN visitada (VPLMN) en el operador de PDP (Packet Data Protocol) en el tiempo de activación de contexto. Además de asignación de la dirección, un GGSN implementa el reenvío de paquetes IP desde el túnel de GTP a una de las

redes de datos por paquetes (PDN) más de la interfaz GI, y viceversa. Intra PLMN backbone e Inter PLMN backbone (Figura 1.3).

Cada red troncal dentro del PLMN es una red IP privada destinada a datos de dominio de paquetes y señalización dentro de una PLMN sola, y la troncal entre PLMN se utiliza para la itinerancia de una PLMN a otro (a través de la interfaz Gp y las Pasarelas de Frontera). SGSN (Nodo de Soporte GPRS de Servicio) y GGSN utiliza la intra PLMN backbone a cambio de datos de dominio PS y señalización. Durante la itinerancia, tanto la columna backbone de la PLMN de la casa y se utilizan las redes visitadas, además de la troncal entre PLMN

Figura 1.3 Inter PLMN Backbone



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

La red troncal inter PLMN interconecta los SGSN y GGSN y redes troncales intra PLMN en diferentes PLMS.

Cuando un abonado se encuentra en itinerancia a otra PLMN, conocida como la PLMN visitada (VPLMN), el usuario tiene que conectarse primero a la red. En GPRS Attach, el MT informa al SGSN de su intención de conectarse a la red para dar información sobre su identidad, capacidad y ubicación. El SGSN comprueba la

identidad del MT y realiza el procedimiento de autenticación con el fin de asegurar el recorrido de transmisión. La unión se completa después de que el SGSN ha recibido los datos del abonado de itinerancia de HLR de Inicio PLMN del abonado (HPLMN) y terminando el procedimiento de actualización de ubicación.

Después de GPRS Attach, el MT envía un "Activar contexto PDP" Solicitud, en la que el nombre de punto de acceso (APN) es una referencia a la AP GGSN a ser utilizado tanto en el hogar o Visitado por el PLMN backbone, o en una red externa. El SGSN selecciona el GGSN basado en el registro de suscripción del contexto PDP y envía los datos de contexto a un GGSN seleccionado.

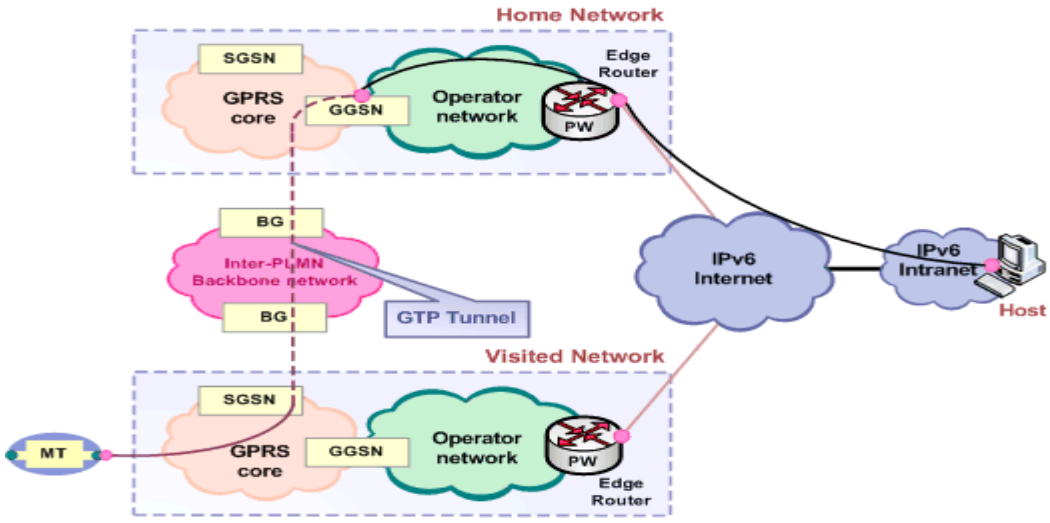
Los paquetes de rutas GGSN son apropiados para las redes de datos (PDN).

Cuando un abonado está en itinerancia en la VPLMN, hay dos posibilidades para la selección de GGSN:

- Utiliza el GGSN de red doméstica a través de la troncal entre PLMN, BGs (Border Gateway), y el túnel de GTP sobre la interfaz Gp (véase la figura 2). La home GGSN en ruta los paquetes a su destino.

- Utiliza un GGSN dominio visitado, el enrutamiento de los paquetes de la VPLMN a su destino directamente a través de una red de paquetes de datos, tales como la Internet pública mediante la interfaz Gi.

Figura 2. Túnel GTP



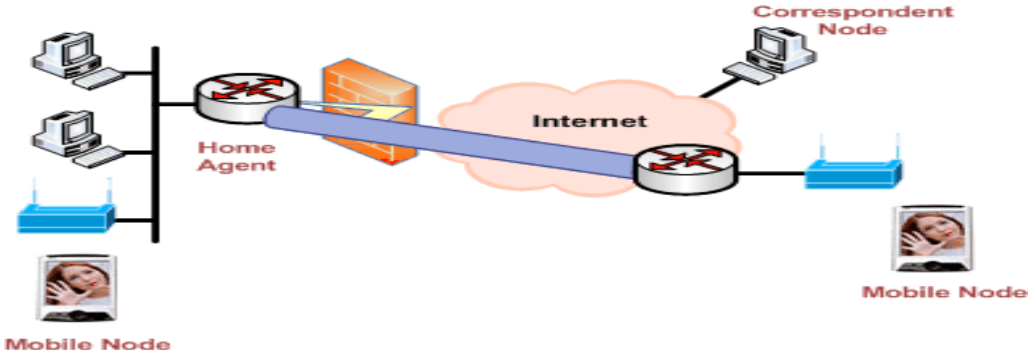
Fuente: ITU Module 5 IPV6 implementation in Mobile networks

En el primer caso, se permite que el terminal móvil tenga una identidad de capa de red de la red doméstica. Pero podría no ser la manera más eficaz, se utilizan especialmente en el caso de los servicios locales (topológicamente cerca de la red visitada).

En el segundo caso, el terminal móvil se le asigna una dirección IPv6 de la piscina de dirección del GGSN visitado. En ese caso, es imposible para el terminal móvil para ser alcanzable a través de una dirección desde el dominio de origen.

4.2 COMPONENTES DE IPV6 MOVILIDAD

Figura 3. Componentes de IPV6



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

4.2.1 Mobile Nodo (MN)

Un nodo móvil es un nodo que cambia su ubicación dentro de la topología Internet. La movilidad de un nodo podría ser el resultado del movimiento físico o de cambios dentro de la topología. Es decir, el movimiento puede ser debido a un dispositivo que se mueve de un enlace a otro debido a su movimiento físico (por ejemplo, un dispositivo en un coche o un tren) o debido a cambios en la topología que hacen que el dispositivo sea conectado a un router diferente (por ejemplo, insuficiencia de router) mientras se está en el mismo lugar físico.

Mobile IPv6 se dedica a organizar la movilidad, por lo tanto, el término "host móvil" habría sido más apropiado en este contexto. Sin embargo, las conversaciones Mobile IPv6 se especifican sobre los "nodos móviles" (aparentemente refiriéndose sólo a hosts), por lo que se utiliza el mismo término en este libro para evitar una mayor confusión.

4.2.2 Nodo correspondiente (CN)

Es cualquier nodo que se comunica con el nodo móvil. Tenga en cuenta que los términos "móviles" y los nodos "corresponsal" se refieren a ciertas funciones dentro de un nodo IPv6. Por lo tanto, un nodo móvil puede también ser un nodo correspondiente, y viceversa, dependiendo del contexto. Por ejemplo, un anfitrión puede ser visto como un nodo correspondiente por el móvil (en movimiento) que se comunica con el nodo. Al mismo tiempo, el nodo corresponsal también puede moverse, lo que hace que sea un nodo móvil (porque se está moviendo) mientras está siendo visto como un nodo corresponsal por su interlocutor móvil.

4.2.3 Dirección del hogar

Es una dirección estable que pertenece al nodo móvil y se utiliza por los nodos correspondientes para llegar a los nodos móviles. Como todas las direcciones

IPv6, la dirección local se basa en el prefijo de 64-bit asignada al enlace hogar combinado con identificador de interfaz del nodo móvil.

Un nodo móvil puede tener más de una dirección de casa. Paquetes IP dirigidos a la dirección de su casa se dirigen a la casa de enlace utilizando protocolos estándar de enrutamiento.

Home enlace

Enlace a la cual se le asigna el prefijo de la dirección de origen.

Home Agent (HA)

Es un router ubicado en el enlace de casa, que actúa en nombre del nodo móvil cuando no esté en el enlace de la casa. El agente interno redirige los paquetes dirigidos al domicilio de un nodo móvil a su ubicación actual (asistencia de dirección) usando IP sobre IP túneles.

Enlace Exterior

Cualquier enlace (que no sea el home link) a la visita de un nodo móvil.

Dirección de custodia (CoA)

Es la dirección que se asigna al nodo móvil cuando se encuentra en un enlace exterior. Esta dirección se basa en el prefijo del enlace exterior combinado con el identificador de interfaz del nodo móvil. No existe un formato especial para una dirección de auxilio, sino que es una normal de direcciones IPv6 unicast.

Esta dirección identifica la ubicación actual del nodo móvil.

Binding (Encuadernación)

La asociación de la dirección inicial de nodo móvil con una dirección de custodia por un período de tiempo determinado. Es decir, entre la dirección de su casa estable y la ubicación actual del nodo móvil. Esto permite que el agente local (post office) para reenviar paquetes a la ubicación actual del nodo móvil. La unión se actualiza (si el temporizador expira) o actualizado cuando el nodo móvil obtiene una nueva dirección de custodia (porque se trasladó a un nuevo enlace).

Binding cache (vinculación de Caché)

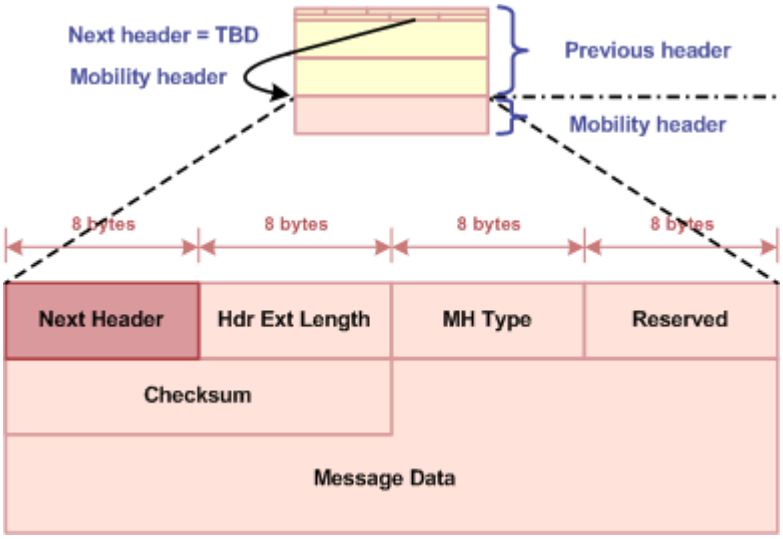
La memoria caché almacena en la memoria volátil que contiene una serie de enlaces para uno o más nodos móviles. Una memoria caché de unión se mantiene, por tanto en el nodo corresponsal y el agente de origen. Cada entrada de la caché de vinculación contiene la dirección del nodo móvil, dirección de custodia, y el tiempo de vida que indica la validez de la entrada. Cuando la caché de vinculación se mantiene mediante nodos correspondientes, también contiene algunos parámetros de seguridad.

Lista Binding Update (BUL)

Es una lista mantenida por el nodo móvil en la memoria volátil. Esta lista contiene todos los enlaces que se enviaron al agente local del nodo móvil y los nodos correspondientes. Esta lista se mantiene para que el nodo móvil sepa cuando un enlace se debe actualizar y se utiliza también para la selección de la atención de la dirección a la derecha cuando se comunica directamente con un nodo corresponsal.

4.3 MOVILIDAD DE CABECERA IPV6

Figura 4. Cabecera IPV6



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

Es una nueva cabecera de extensión para ser utilizada por el nodo móvil, agente principal, y el Nodo Corresponsal en toda la mensajería relacionada con la creación y la gestión de la unión. La opción de Cabecera IPv6 puede permitir llevar a cuestas de estos mensajes

.

La cabecera de movilidad es identificada por el valor de la cabecera siguiente, 135 en la cabecera anterior. El formato de la cabecera se muestra en la Figura 5. Cada campo se describe de la siguiente manera:

La parte fragmentable del paquete original se divide en fragmentos de tamaño múltiplo de 8 bytes, excepto el último. Cada fragmento se envía en paquetes separados.

- La cabecera de 8 bits siguiente. EL valor de la siguiente cabecera es igual al campo siguiente cabecera IPv6.
- Los 8 bits de encabezado de extensión campo Longitud indica la longitud de la cabecera de la Movilidad en 8-byte unidades excepto el campo siguiente cabecera.
- El 8 bits Tipo de MH es el identificador de tipo de variable entre la cabecera de Movilidad. Los valores actuales de tipo MH se especifican en la Tabla 1.

- El próximo campo de 8 bits se reserva para el uso futuro y debe ser inicializado a cero por el remitente. Si este campo contiene cualquier otro valor, que debe ser ignorado por el receptor.

- El campo Suma de verificación de 16 bits contiene el checksum de la cabecera de la Movilidad.

Tabla 1. Cabecera IPV6

MH	TIPO DESCRIPCIÓN
0	Indica mensaje Binding Request Refresh
1	Indica Principal Prueba Init (hoti) Mensaje
2	Indica Cuidado de prueba Init (COTI) Mensaje
3	Indica Principal Prueba (HoT) Mensaje
4	Indica Care-of Test (COT) mensaje
5	Indica Binding Update (BU) mensaje
6	Indica Reconocimiento Binding (BA) mensaje
7	Indica un error de enlace (BE) mensaje

Fuente: ITU Module 5 IPV6 implementation in Mobile networks

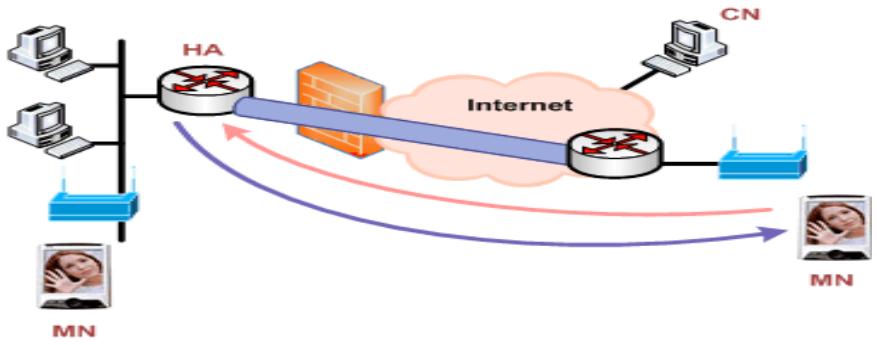
Los datos específicos de acuerdo con el indicado Tipo MH se encuentran en el campo de datos del mensaje. Las opciones de mensajes que contienen el campo de movilidad son:

- Consejos Binding Refresh
- Care-of Alternate Dirección
- Índices nonce
- Enlace de datos de autorización

El encaminamiento triangular no requiere que todos estos mensajes, sólo BU, BA y BE.

4.4 DYNAMIC HOME AGENT ADDRESS DISCOVERY (DHAAD)

Figura 4.1 DHAAD



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

El Home Agent Dirección solicitud de descubrimiento (DHAAD) es enviado a la dirección anycast Inicia agentes de su propio prefijo de subred de origen. (DHAAD) de MIPv6 también proporciona soporte para múltiples Agentes de Inicio y un soporte limitado para la reconfiguración de la red doméstica.

En estos casos, el nodo móvil no conoce la dirección IP de su agente local propio, e incluso los prefijos de subred de origen pueden cambiar con el tiempo. Un

mecanismo DHAAD permite a un nodo móvil para descubrir dinámicamente la dirección IP de un agente local en su enlace casa, incluso cuando el nodo móvil está fuera de casa. El nodo móvil también puede aprender nueva información sobre los prefijos de subred de origen a través del mecanismo ¨ Mobile prefix discovery

4.5. MOVILIDAD IPV6 ESTRUCTURA DE DATOS

Las siguientes estructuras de datos son necesarias para facilitar los procesos de movilidad IPv6:

- Binding cache
- Binding update list
- Home agents list

Binding Cache

La Binding cache es una tabla mantenida por cada nodo corresponsal y agente de origen y contiene los enlaces actuales de los nodos móviles. Cada entrada de caché de enlace contiene la siguiente información:

- La dirección local para el nodo móvil.
- La dirección de custodia para el nodo móvil.
- La vida útil de la entrada de caché vinculante
- La vida útil se obtiene de la Vida campo de la última actualización de unión que se ha recibido para esta entrada de antememoria.
- Una bandera que indica si el enlace es un registro de la casa.
- Esta bandera se establece sólo para las entradas de caché de unión sobre los agentes domésticos.

- Una bandera que indica si el nodo móvil de esta entrada de caché vinculante debería ser lo anuncian como un router.

Si se establece este indicador, el agente va a anunciar el nodo móvil como router (estableciendo el indicador del router) al proxy mensajes de anuncio de vecino en nombre del nodo móvil. Esta bandera sólo es válida para las entradas de registro de origen y establecerse solamente para las entradas de la caché de unión sobre los agentes domésticos

- El valor del campo de longitud del prefijo de la última actualización vinculante que fue recibido por esta entrada de caché.
- El valor máximo del campo de número de secuencias de las actualizaciones de unión que se han recibido para esta entrada de antememoria.
- El tiempo que la solicitud de enlace se envió de última.

La información de la Binding cache tiene prioridad sobre la información de la caché de vecinos.

Para los destinos móviles que están fuera de casa, los paquetes deben ser enviados a la dirección local por medio de la dirección de custodia. Si los paquetes se envían directamente a la dirección de la casa mientras que el nodo móvil está fuera de casa, el agente local debe interceptar los paquetes y el túnel al nodo móvil, disminuyendo la eficacia y el rendimiento de la comunicación entre el nodo corresponsal y el nodo móvil.

LISTA DE ACTUALIZACIONES BINDING

La lista de actualización de Biding es mantenida por un nodo móvil para registrar

las actualizaciones de unión más reciente enviado por el agente doméstico y los nodos correspondientes. Una entrada de actualización de la lista de enlace contiene:

- La dirección del nodo al que se envió la actualización de vinculación.
- La dirección local para la actualización de vinculación.
- La dirección de custodia enviado en la última actualización de vinculación.
- El valor del campo de por vida en la actualización de vinculación.
- El tiempo de vida restante de la unión.

El valor inicial es el valor del campo de por vida en la actualización de vinculación. Cuando el tiempo de vida expira, la entrada se elimina de la lista de actualizaciones vinculantes.

- El valor máximo del campo de número de secuencia enviado en las anteriores actualizaciones de unión.
- El tiempo que la actualización de vinculación se envió el último.
- Una indicación de si una retransmisión es necesaria para las actualizaciones de unión enviados con el reconocimiento (A) establecido el indicador y cuando la retransmisión se va a enviar.
- Una bandera que indica que no hay actualizaciones obligatorias futuras deben ser enviados.

El flag está puesto cuando el nodo móvil recibe un parámetro ICMPv6 de problemas no reconocidos IPv6 Opción detectando un mensaje en respuesta a una actualización obligatoria.

Home Agents List.

Los Home Agent List (lista de los agentes hogar) son mantenidos por agentes internos y los nodos móviles, y registra información sobre cada router desde el que se recibió un anuncio de enrutador en el enlace de casa con el Home Agent (H) Grupo de bandera. La home list mantiene la lista de Home Agent List para que puedan enviar la lista de agentes de origen a un nodo móvil solicitante fuera de casa durante el descubrimiento dirección principal del agente. Los nodos móviles mantener la lista de agentes a casa para que puedan seleccionar un agente local.

Un Home Agent List contiene lo siguiente:

- El vínculo de la dirección local del router en el enlace, que se obtiene a partir de la dirección de origen del mensaje de anuncio de enrutador recibido.
- La dirección global de direcciones o del agente local, que se obtiene desde el campo Prefijo en las opciones Prefijo de información en el mensaje de anuncio de enrutador con la dirección del router (R) set bandera.

- El tiempo de vida restante de esta entrada.

La duración inicial se obtiene, ya sea del campo Inicio Vida agente en la opción Inicio Información del agente o el campo Router Lifetime en el mensaje de anuncio de enrutador. Cuando el tiempo de vida expira, la entrada se elimina de la Home Agent List

- La preferencia por el agente de origen, que se obtiene desde el campo Preferencia Home Agent en la opción Inicio Información del agente.

Si el anuncio del enrutador no contiene un Home Agent opción de información, la preferencia se establece en 0. Sobre la base de la definición del campo de Inicio Preferencia agente, 0 es un nivel de prioridad media. Un nodo móvil utiliza el valor de preferencia para seleccionar el agente de origen.

Un agente de origen utiliza el valor de preferencia para ordenar por valor de preferencia de Home Agent List es devuelto a un nodo móvil durante el descubrimiento dirección principal del agente. Cuando el nodo móvil que recibe la lista de agentes de origen, se elige el agente de origen primero en la lista.

4.6. MOBILE IPV6 RESUMEN DE OPERACIONES

La IPv6 Home Address (HA)) se asigna al nodo móvil. El nodo móvil obtiene una nueva dirección IPv6 (Cuidado de Dirección) en redes que se conecta.

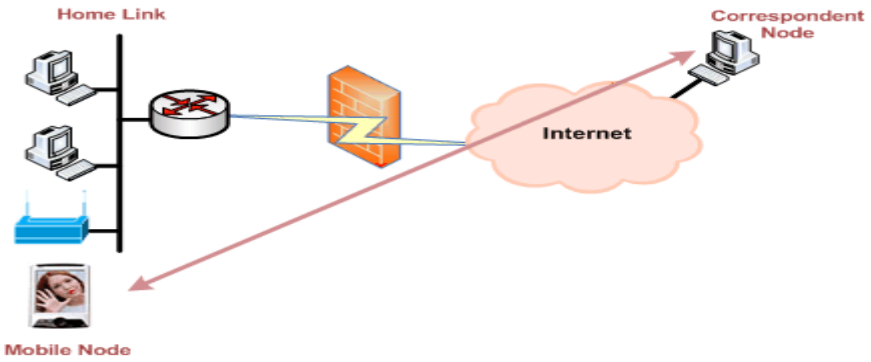
El nodo móvil informa a un agente local en su red principal la originalidad de su nueva dirección.

El Home Agent se hace pasar por el nodo móvil:

- La captura de tráfico al nodo móvil.
- Transferencia de tráfico desde el nodo móvil.
- Nodo móvil también puede informar a los otros nodos:
- Nodo Corresponsal (se comunica con ella sobre CoA)
- Nodo Corresponsal directamente puede enviar tráfico al nodo móvil.

4.6.1. NODO MÓVIL EN LA RED DOMÉSTICA

Figura 5. Nodo móvil



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

Mientras que el nodo móvil está en casa, los paquetes dirigidos a su dirección de casa se enrutan a casa enlace del nodo móvil, utilizando mecanismos convencionales de enrutamiento de Internet. El nodo móvil está siempre espera que sea direccionable a su casa, ya sea en la actualidad está unido a su home link o está fuera de casa. La "home address" es una dirección IP asignada al nodo móvil dentro de su prefijo de subred casa en su home link.

4.6.2. EL NODO MÓVIL SE ESTÁ MOVIENDO A UN NUEVO ENLACE

Figura 6. Nodo móvil

Fuente: ITU Module 5 IPV6 implementation in Mobile networks

Binding Update

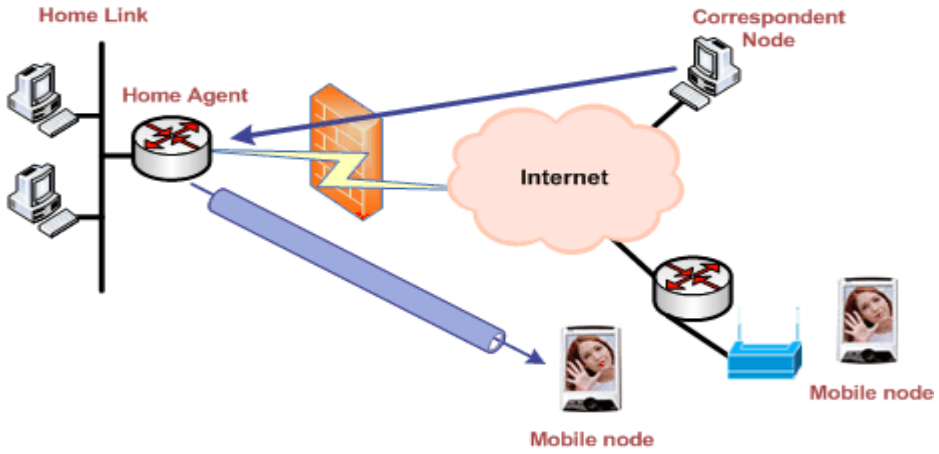
Si bien fuera de casa, el nodo móvil registra su atención de la dirección primaria con un router en su home link, solicitando este router para que funcione como "Home agent" para el nodo móvil.

Cuidado de Dirección

El Nodo móvil obtiene una dirección IPv6 en la red visitada a través de, con o sin estado de configuración automática.

4.6.3. REENVÍO DE PAQUETES BI-DIRECCIONAL MODO DE TÚNEL

Figura 7. reenvío de Paquetes Bi-direccional



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

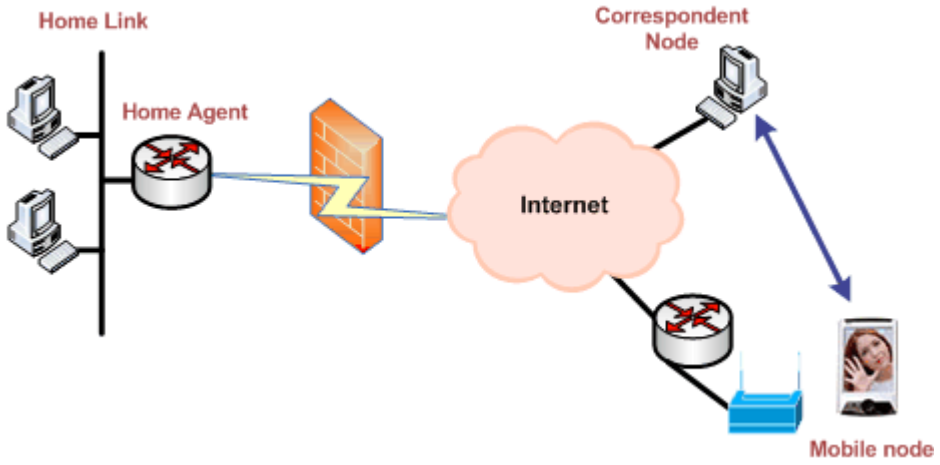
Los paquetes desde el nodo corresponsal se encaminan al agente local y, a continuación del túnel al nodo móvil. No se requiere para soportar IPv6 Móvil en el Nodo Corresponsal. No es un registro obligatorio entre el nodo móvil y el nodo corresponsal.

Home Agent utiliza el proxy Neighbor Discovery para interceptar los paquetes IPv6 dirigidos a la dirección del nodo móvil en el enlace de la casa. Cada paquete interceptado se canaliza a la CoA del nodo móvil. Los paquetes al nodo correspondiente se tunelizan desde el nodo móvil al agente inicial ("revertir túnel")

y luego es dirigido normalmente a partir de la red doméstica para el nodo corresponsal.

4.6.4. REENVÍO DE PAQUETES DE OPTIMIZACIÓN DE MODO RUTA

Figura 8. Optimización de modo Ruta



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

El tráfico se va a través del Agente de inicio hasta que el procedimiento se lleva a cabo Ruteabilidad Retorno. La señalización a través de Home Agent y Registros Home Home Agent todavía mantiene informado. Nodo Corresponsal debe apoyar MIPv6. Requiere nodo móvil para registrar su asociación vinculante al Nodo Corresponsal. Nodo móvil puede también ser un nodo correspondiente al nodo móvil comunicarse con otro.

Los paquetes de Nodo Corresponsal se dirigen directamente al Comité de Agricultura de la Mobile Node. Cuando se envía un paquete a cualquier destino IPv6, el Nodo Corresponsal comprueba sus enlaces en caché para una entrada de dirección de destino del paquete. Si un enlace en la caché para esta dirección de destino se encuentra, el Nodo Corresponsal utiliza IPv6 tipo RH 2 para encaminar el paquete al nodo móvil.

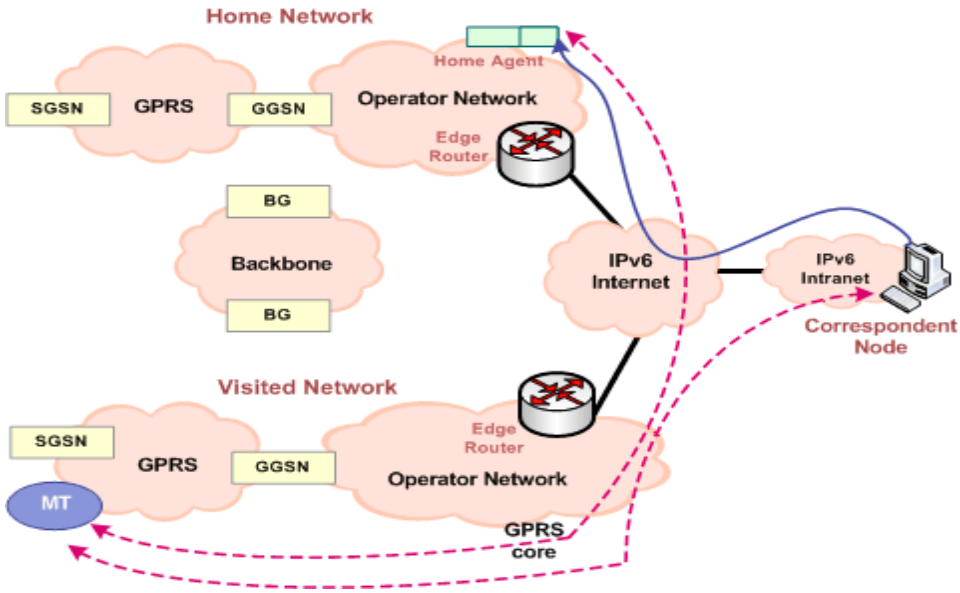
Al pasar los paquetes directamente al nodo corresponsal Nodo Móvil establece la dirección de origen en el encabezado IPv6 del paquete a su actual CoA. Nodo Mobile IPv6 añade "Domicilio" opción de destino para llevar a su domicilio. La inclusión de las direcciones de inicio en estos paquetes hace que el uso de la dirección de custodia transparente por encima de la capa de red.

4.7 IMPLEMENTACIÓN DE IPV6 MÓVIL EN 2G Y 3G DE REDES MÓVILES

La movilidad inalámbrica (GPRS y UMTS) se logra a través de la conectividad de capa de enlace, que proporciona acceso a la red IP a través de un enrutador de IP específico GGSN (nodo de soporte GPRS) (ver Figura 9).

Cuando el terminal móvil está en itinerancia en una red visitada situado lejos de la red doméstica, que está todavía unido a la GGSN casa. Cuando se utilizan los servicios locales, el encaminamiento es ineficiente. Uso de la movilidad capa IP resuelve estos problemas.

Figura 9. IPV6 MÓVIL EN 2G Y 3G



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

La implementación de IPv6 en las redes móviles 2G y 3G requiere soporte de capa de aplicación IPv6 de la red, la instalación de un enrutador de HA en la red doméstica, y los nodos móviles que soportan IPv6 móvil y la infraestructura IPsec. Cuando el terminal móvil está en itinerancia en una red extranjera, es direccionable por dos direcciones: la dirección de auxilio y la dirección de su casa. Cuando el terminal móvil entra en una red extranjera, registra su dirección de custodia con la HA mediante el envío de una actualización de vinculación.

Él HA a continuación, envía un acuse de recibo de unión. La actualización de enlace y reconocimiento deben ser autenticados por IPsec AH (Authentication Header). Todos los paquetes dirigidos a la red móvil son interceptados por la HA, que a continuación encapsula los paquetes IPv6 utilizando la encapsulación, con el encabezado exterior dirigida al móvil dirección de custodia. Cuando el terminal móvil recibe el primer paquete de la HA, envía una actualización de ligadura al nodo corresponsal, informando acerca de su dirección de atención primaria.

El nodo corresponsal a continuación, envía un acuse de recibo de vuelta de unión al terminal móvil. Los paquetes son entonces transferidos entre el terminal móvil y el nodo corresponsal sin el requisito de la HA. El uso de Mobile IPv6 proporcionará eficiente de enrutamiento y QoS en redes 2G y 3G móviles.

Las actualizaciones son necesarias en la red para utilizar las funciones de IPv6. Aunque IPv6 resuelve las limitaciones de IPv4, sigue siendo un gran reto en la migración a IPv6.

Todas las ventajas de IPv6 son para nada si no se puede implementar, y muchos problemas se asocian con la migración.

El costo es uno de los problemas que dificultan el despliegue de IPv6. Como mínimo, una actualización de software se debe realizar en cada host y el router de la red. El lado positivo es que el costo sigue siendo aceptable, en comparación con el costo de la aplicación de parches y la fijación de IPv4.

¿Cuándo es el momento adecuado para cambiar a IPv6? La posibilidad de convertir IPv4 "off" y conmutación IPv6 "on" es casi impracticable debido a la infraestructura, la logística y el costo asociado con la transición. El intento de hacer que todos los eventos del interruptor ocurrir al mismo tiempo, no es factible.

Además, todos los routers también se deben actualizar a nivel mundial para lograr una transición rápida. El ISP con las redes actuales basadas en IPv4 no estará dispuesto a gastar pródigamente en este tipo de transición. Por lo tanto, es probable que los dos tengan que convivir durante algún tiempo hasta que una transición completa se lleva a cabo. Este tipo de enfoque presenta problemas. Debido a que los dos protocolos son totalmente diferentes, que no son compatibles. Esto significa que las aplicaciones IPv6 no va a funcionar con aplicaciones IPv4 y IPv6 nodos no van a "hablar" con nodos IPv4. Para superar estos problemas, el IETF y IPng han propuesto las siguientes soluciones:

Dual IP Stack

Esta solución proporcionará soporte completo para las aplicaciones IPv6 e IPv4 y los nodos IPv4 de modo que se pueden utilizar cuando IPv6 no esté disponible tanto para los usuarios.

Tunneling

Esta solución va a encapsular paquetes IPv6 en IPv4 con cabeceras de modo que puedan ser enviados a través de la infraestructura de enrutamiento actual de IPv4.

Traducción

Aunque los nodos IPv6 y nodos IPv4 no interactúan, existe un ámbito para los mecanismos de traducción, que son muy complejos.

Incluso simples pilas duales IP y un sencillo túnel no resuelve totalmente el problema. Una pila IP no resuelve el problema de la demanda de direcciones enrutables globalmente y, de hecho, aumenta la complejidad de la red por tener que proporcionar IPv4 e IPv6 infraestructuras de enrutamiento. Simple efecto túnel es muy difícil de escalar debido a que requiere la configuración manual considerable.

Para superar los inconvenientes de la simple pila doble enfoque, las herramientas avanzadas han sido puestas disponibles para los usuarios.

DSTM (dual-stack mecanismo de transición):

Esta herramienta consiste en asignar dinámicamente las direcciones IPv4 y el uso de IPv4 a través de un tunel IPv6 para transportar paquetes IPv4 en la red.

Dual-Stack ALG (gateway a nivel de aplicación)

Esta herramienta de doble pila limita su uso a través de la red mediante la migración a una red IPv6 sólo que se comunica con el mundo a través del proxy de IPv4 en la aplicación de doble pila.

NAT-PT (Network Address Translator-Protocol Translator)

Esta herramienta consiste en utilizar una red IPv6 completa y comunicarse con el mundo usando IPv4 NAT-PT las unidades que se traducen entre IPv6 a IPv4.

Para superar el problema de escalabilidad de sencilla construcción de túneles, los siguientes conceptos se han considerado:

6 to 4

Este concepto ofrece una manera de conectar redes IPv6 automáticamente por túnel a través de la red IPv4 utilizando un prefijo de enrutamiento único para cada sitio de usuario final que lleva a una dirección de punto final del túnel IPv4.

6 sobre 4

Este concepto permite a los hosts IPv6 aislados, sin conexión directa a un router IPv6 para convertirse en anfitriones IPv6 completamente funcionales.

Los anfitriones a realizar el túnel, al proporcionar un router que comprende más de 6 4, a la 6 anfitriones sobre 4 puede conectarse a un host IPv6. Los paquetes IPv6 se encapsulan en paquetes IPv4 y enviado sobre la red IPv4.

Tunnel Broker

Tunnel Broker son servidores operados por los proveedores de Internet IPv6 se despliegan para ayudar a los clientes IPv4 interconectados en el túnel y la configuración del DNS (Domain Name System).

4.8. MOBILE IPV6 FOR INTER-PLMN MOBILITY

Consideremos la situación en que un abonado de GPRS de un operador en Finlandia está en itinerancia en los EE.UU. y acceder a un servicio local de allí. Si la capa de enlace de movilidad se utiliza paquetes IP del usuario, primero se tunelizado a Finlandia, y luego envía de vuelta a los EE.UU.

En este caso un tiempo de ida y vuelta desde la terminal móvil a un servidor y de vuelta podría ser inaceptable para muchos servicios.

Como una solución a este problema, el abonado en itinerancia GPRS debería usar los servicios de un GGSN local en la red visitada, permitiendo que los paquetes IP sean transferidos tan pronto como sea posible, sin sobrepasar la red doméstica.

Como la dirección IP está asignada desde la red visitada, el nodo móvil no sería accesible a través de una identidad de capa de red, de la red doméstica.

Para algunas aplicaciones esto puede no ser un problema, en general, sería deseable si el nodo móvil se podría alcanzar con una dirección IP se asigna a partir de la red doméstica también.

Una solución natural a este problema es el uso de IP móvil para registrar la dirección de la red visitada con la red de origen, permitiendo que los paquetes enviados a la dirección de su casa para ser entregados al nodo móvil

4.9 LA OPERACIÓN BÁSICA DE IPV6 MÓVIL EN GPRS / WCDMA RED

Cuando el terminal móvil está en itinerancia en una red extranjera, es direccionable por una dirección de atención, además de su domicilio. El prefijo de la dirección IPv6 en el cuidado de la terminal móvil es el prefijo de dirección del enlace exterior.

El cuidado de la dirección es adquirido por el mecanismo de direccionamiento proporcionado por la red visitada. En itinerancia la red extranjera, el terminal móvil se registra en el cuidado de direcciones con el Home Agent y envía una "Binding Update" al agente local. El agente responde con " Binding Acknowledgement".

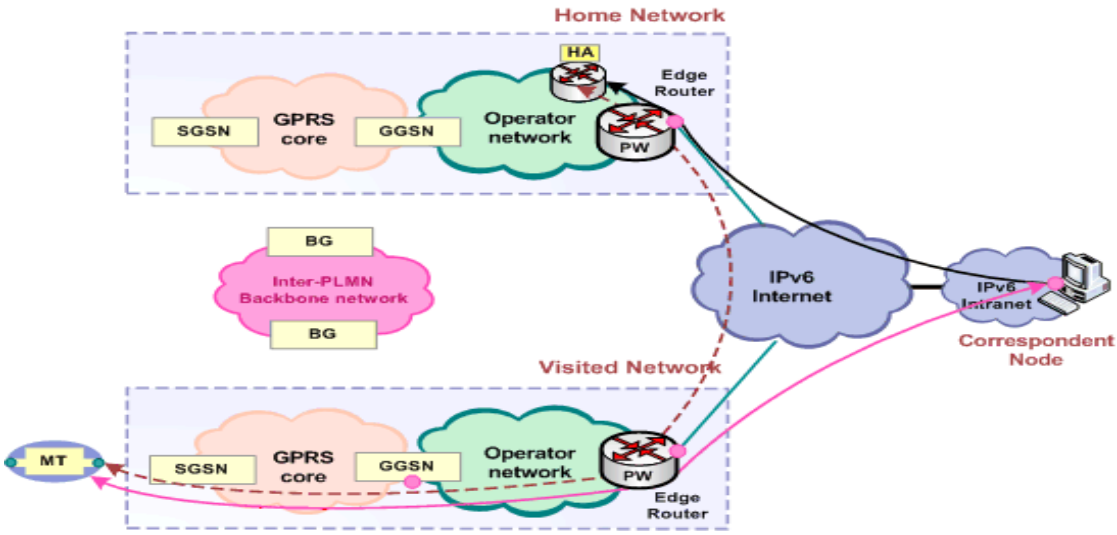
Los paquetes de IPv6 contienen Binding Update o Binding Acknowledgement y las opciones de destino deben ser autenticadas mediante la seguridad IP AH (Authentication Header). Después de la unión, esta dirección de auxilio se convierte en atención primaria de la dirección del terminal móvil.

El home agent intercepta los paquetes IPV6 correspondiente (por ejemplo un servidor WWW que se comunica con el terminal móvil) dirigidos a la dirección del terminal móvil.

El home agent encapsula cada paquete interceptado mediante la encapsulación IPv6, con el encabezado exterior dirigido a la atención primaria de la dirección del terminal móvil. Después de que el terminal móvil ha recibido el primer paquete encapsulado desde el agente local, envía una actualización de ligadura al nodo corresponsal informándole de su atención a la dirección, el nodo corresponsal a continuación, responde con un Binding Acknowledgement. Después de esto, el envío de paquetes IP entre el nodo corresponsal y el terminal móvil es sencillo y el encaminamiento a través de un agente de origen no es necesario.

Para los paquetes enviados por un terminal móvil, mientras esta fuera de casa, el cuidado de la terminal móvil de dirección se utiliza típicamente como la dirección de origen en el encabezado del paquete IPv6. La opción de Dirección de la casa se puede utilizar para informar al destinatario de paquetes de dirección del nodo móvil. El nodo corresponsal puede entonces sustituir la dirección de nodo móvil para esta dirección de auxilio de hacer el uso de la dirección de custodia transparente al nodo corresponsal. Las capas superiores de protocolo (por ejemplo, TCP), lo que sólo ven es la dirección de su casa. (Figura 10.)

Figura 10. Capas superiores



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

4.10. 3GPP, 3GPP2 IMPLEMENTACION

3GPP ha ordenado el uso de IPv6 en el subsistema multimedia IP. Desde el punto de vista de la red móvil, el aumento del uso de IPv6 en la capa de usuario, incluyendo IPv6 terminales que permite la interoperabilidad sin fisuras a través de la promoción de una versión del protocolo único para todos los dispositivos y servicios. IPv6 también es recomendado por el 3GPP para la RAN (Radio Access Network) y es opcional para todos los sistemas de datos móviles, incluyendo las tegnologias basadas en la versión 99 GPRS (General Packet Radio Service).

Una ventaja obvia del protocolo IPv6 es el espacio de direcciones de gran tamaño que proporciona. Por lo tanto, la necesidad de traductores de direcciones de red (NAT) que actualmente se requieren en las redes IPv4 base es eliminada.

IPv6 proporciona espacio suficiente para acomodar direcciones de millones de usuarios en todo el mundo, e incluso un gran número de direcciones IPv6 personales puede ser permitido.

Este es un escenario atractivo para los mercados emergentes, particularmente de redes para operadores móviles totalmente nuevos, ya que las tareas son más fáciles a través de un número menor de elementos y protocolos que deben gestionarse.

La razón de esto es que los traductores de direcciones de red (NAT) y de mapeo entre espacios de direcciones privados y públicos no deben ser administrados.

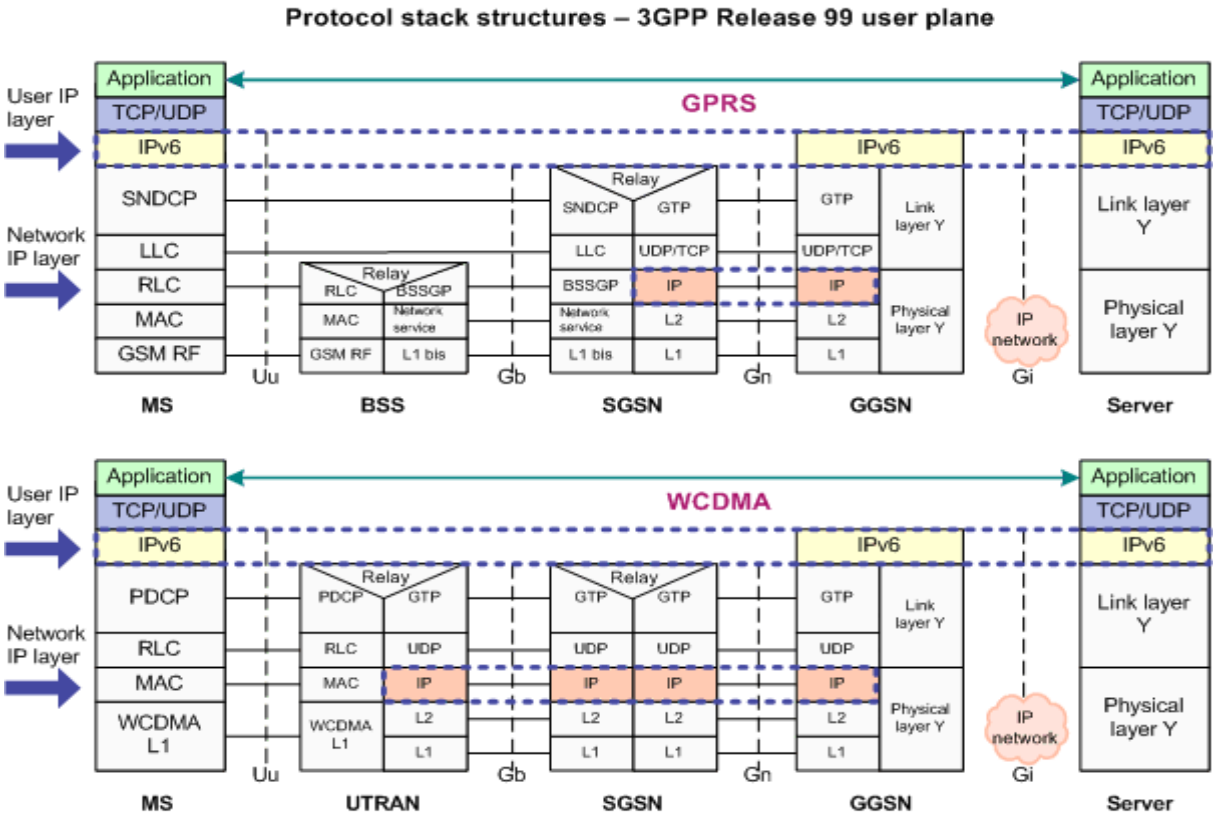
NAT es ampliamente y con éxito en Internet de hoy en día, porque la mayoría de las aplicaciones son basadas en cliente/servidor. Este no es el caso en las redes móviles futuras, donde la comunicación entre los teléfonos móviles y cualquier otro

dispositivo en red son en su mayoría peer to peer y requeriría direcciones globales.

La ausencia de NAT permite la accesibilidad global, con cierta conectividad (any-to-any) extremo a extremo y de red iniciadas por los servicios IP. Esta es una ventaja importante para el interfuncionamiento de redes celulares y del Internet del futuro, y será crítico para el crecimiento continuo y el éxito de estas redes.

La comunicación entre dispositivos sólo IPv6 e IPv4 también es posible. Sin embargo, esto requiere un mecanismo de traducción, tales como la dirección de red Traductor / Protocolo Translator (NAT-PT), que puede convertirse en un cuello de botella en el rendimiento y tal vez podría limitar la capacidad y escalabilidad de las plataformas de prestación de servicios.

Figura 11.Protocol stack structures



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

4.10.1. TRANSICIÓN A IPV6 EN LAS REDES 3GPP

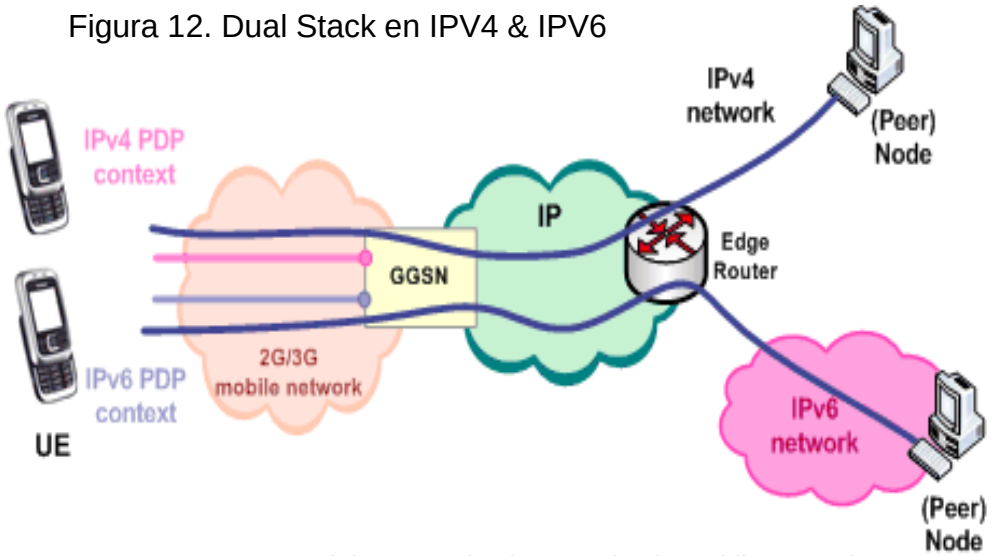
Redes 3GPP tienen diferentes necesidades y situaciones de transición que los nodos de Internet en general tendría. 3GPP celular redes IPv6 transición / interoperabilidad ha sido analizado en el Grupo de Trabajo del IETF v6ops.

GPRS ESCENARIOS DE TRANSICIÓN:

Dual Stack UE se conecta a nodos IPv4 e IPv6.

Este es el escenario más amplio. Las pilas de ambas pueden estar activas simultáneamente. Gestionar el conjunto de direcciones IPv4 es un reto y el uso de direcciones IPv4 privadas significa el uso de NAT. Tunneling se pueden hacer en el UE si es necesario (en el caso de que el GGSN no es compatible con IPv6 Puntos de Acceso).

Figura 12. Dual Stack en IPV4 & IPV6

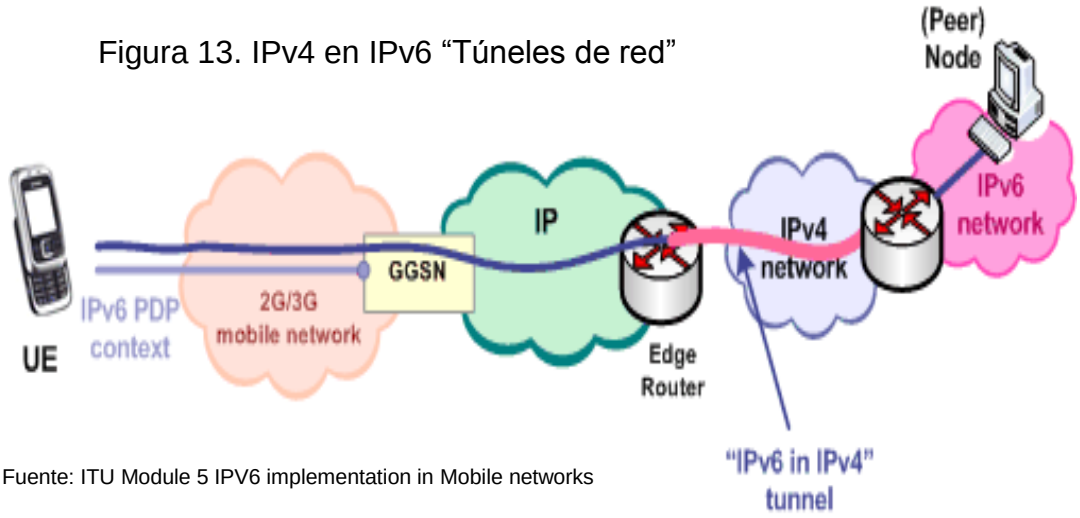


Fuente: ITU Module 5 IPV6 implementation in Mobile networks

1) **IPv6 UE se conecta a un nodo IPv6 a través de una red IPv4.**

Aquí se toma el "IPv6 en IPv4" y el túnel la red puede ser estático o dinámico.

Figura 13. IPv4 en IPv6 “Túneles de red”

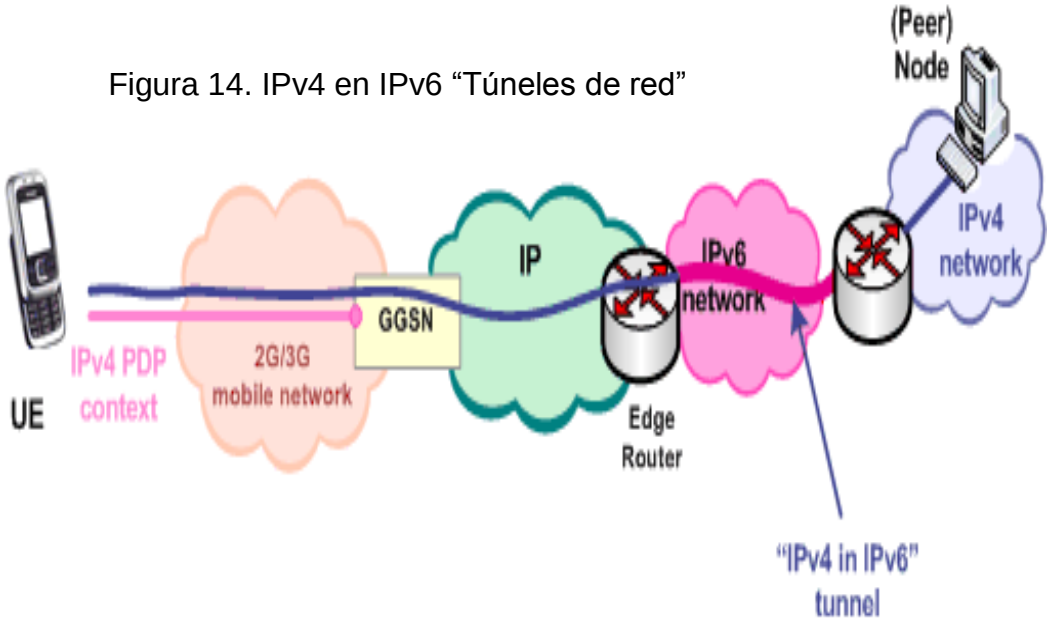


Fuente: ITU Module 5 IPV6 implementation in Mobile networks

2) **IPv4 UE se conecta a un nodo IPv4 a través de una red IPv6**

En este escenario está haciendo "IPv4 en IPv6" (estático o dinámico) túneles de la red. Este escenario no se considera muy probable en las redes 3GPP.

Figura 14. IPv4 en IPv6 “Túneles de red”

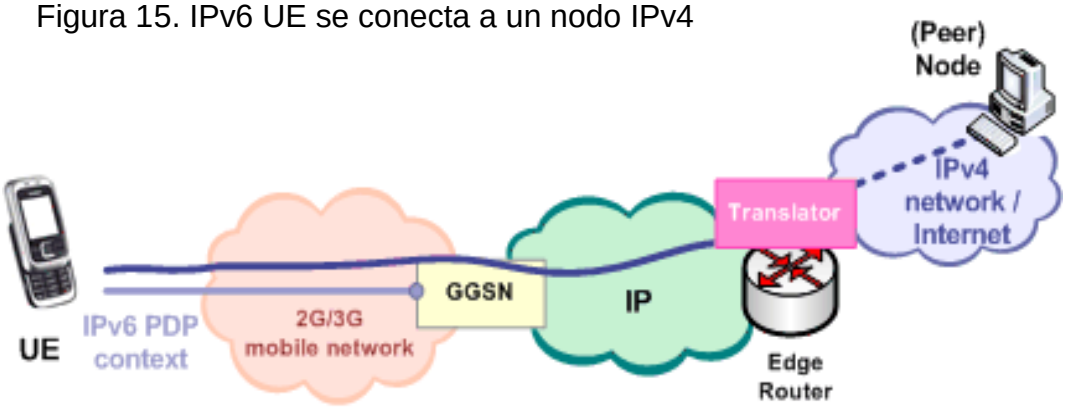


Fuente: ITU Module 5 IPV6 implementation in Mobile networks

3) IPv6 UE se conecta a un nodo IPv4

En este escenario la traducción es necesaria, ya que la UE y el nodo del mismo nivel no comparten la misma versión IP.

Figura 15. IPv6 UE se conecta a un nodo IPv4

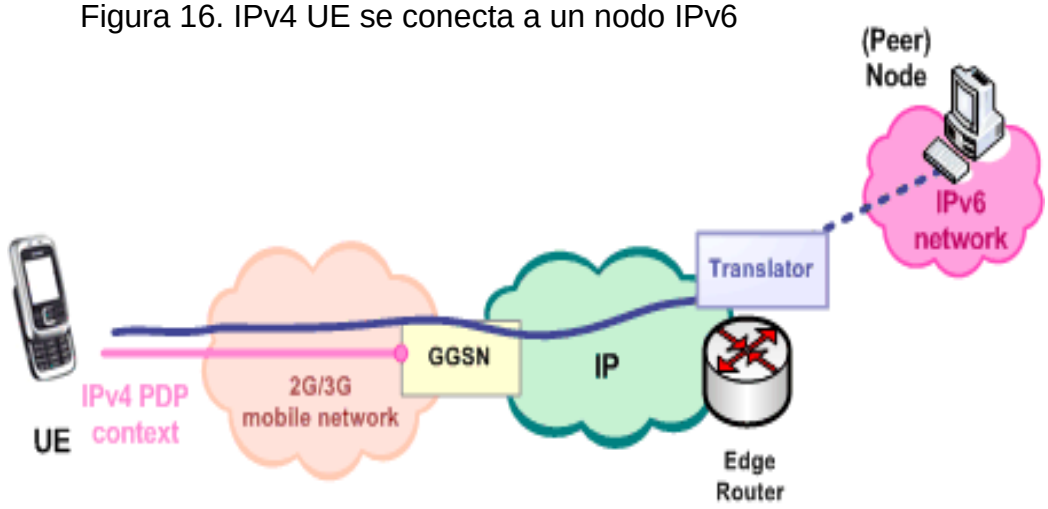


Fuente: ITU Module 5 IPV6 implementation in Mobile networks

4) IPv4 UE se conecta a un nodo IPv6

La traducción es necesaria, ya que la UE y el nodo del mismo nivel no comparten la misma IP versión.

Figura 16. IPv4 UE se conecta a un nodo IPv6



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

IMS ESCENARIOS DE TRANSICIÓN:

1) UE se conecta a un nodo en una red IPv4 a través de IMS.

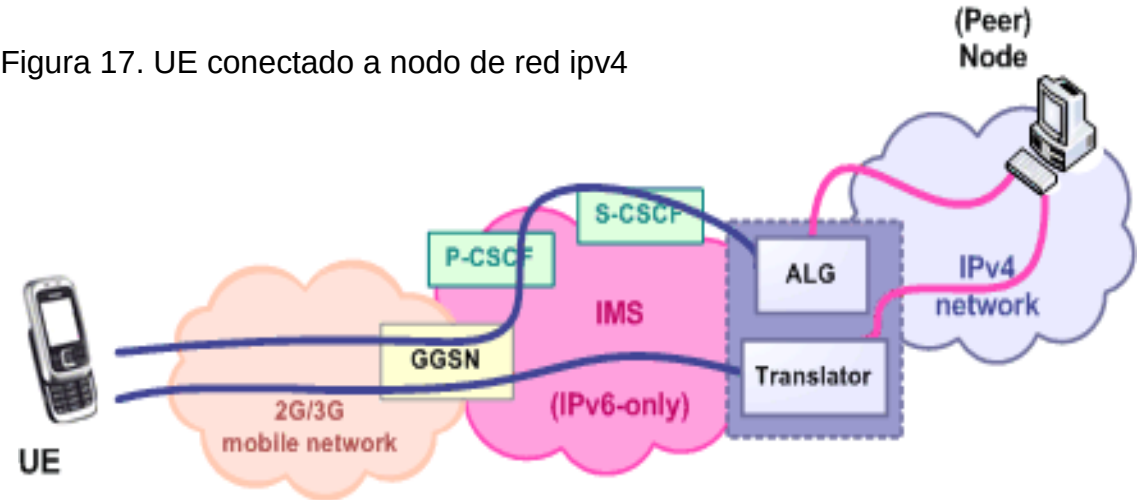
Aquí el UE tiene conexión IPv6 al IMS y de IMS a un nodo IPv4.

La traducción es necesaria en dos niveles:

Nivel 1: SIP y SDP en un ALG

Nivel 2: El usuario tráfico de datos a nivel IP

Figura 17. UE conectado a nodo de red ipv4

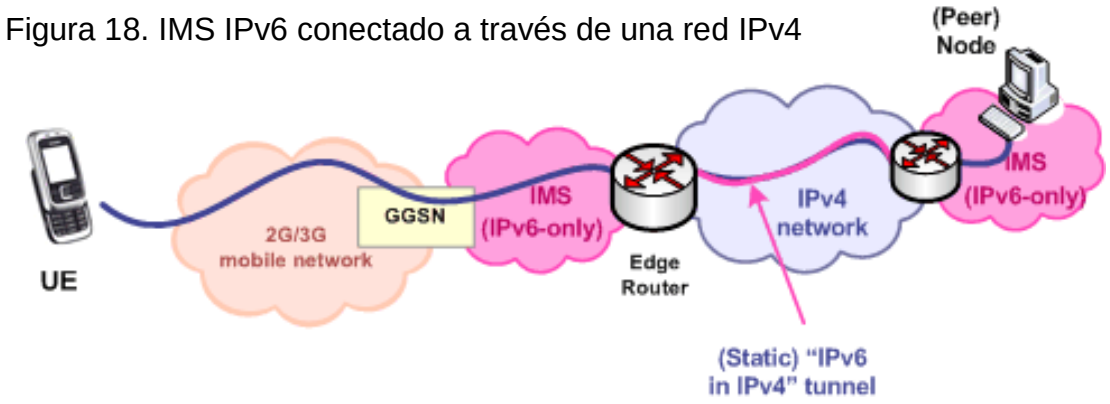


Fuente: ITU Module 5 IPV6 implementation in Mobile networks

2) Dos IMS IPv6 conectado a través de una red IPv4.

Está estrechamente relacionado con este escenario GPRS 2. Conexión de dos islas IPv6-only IMS sólo tiene que ser hecho a través de la red IPv4.

Figura 18. IMS IPv6 conectado a través de una red IPv4



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

4.10.3. ESCENARIOS DE TRANSICIÓN 3GPP2 OPERADORES

Hay muchos escenarios posibles para la transición de la red:

Sencillo IPv4 IPv6 -> Simples
Mobile IPv4 - IPv6> simple
Mobile IPv4 -> Mobile IPv6

Y varias opciones para la actualización de la red:

Actualiza terminales móviles y PDSN y algunos servicios de doble pila. Deja operador de red de núcleo como IPv4.

Actualiza sólo los terminales móviles y algunos servicios a doble pila. Emplear mecanismo de transición en el móvil.

Dual-Stack

Perspectiva móvil:

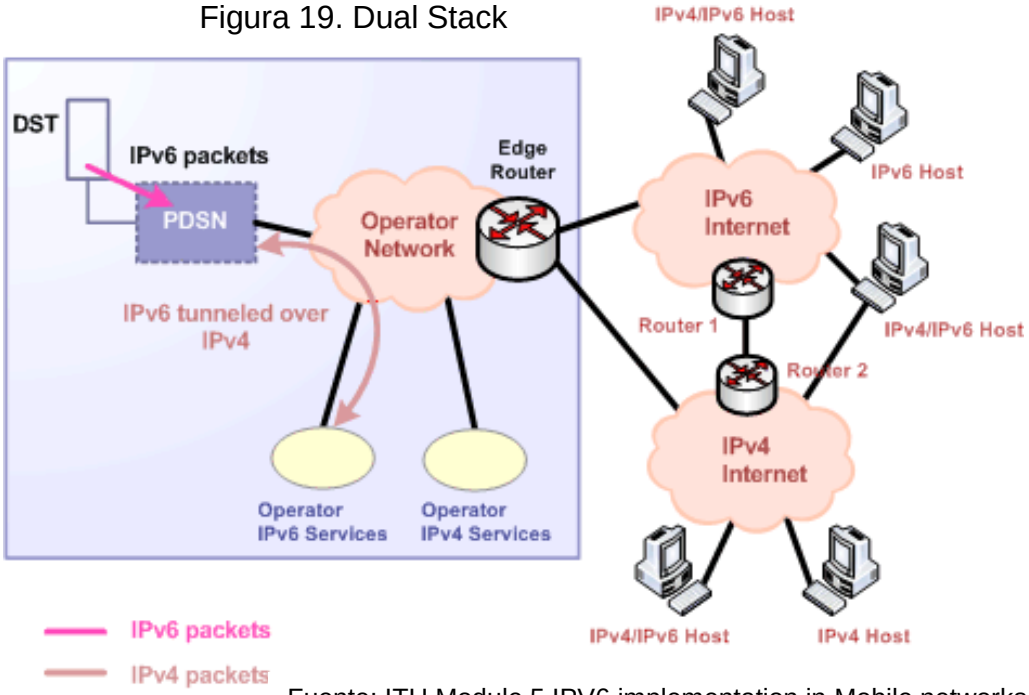
- Un Mobile puede abrir un solo IPv4, IPv6 o ambos de conexión sólo IPv4 e IPv6 con el PDSN.
- Un Mobile puede agregar o quitar NCPsat IP o IPv6 cualquier momento
- Un Mobile usará DNS para determinar la dirección de la familia del extremo receptor.
- Un Mobile decide utilizar IPv4 o IPv6 basado en la familia de direcciones del fin de acogida.

Red Perspectiva:

- PDSN y el enrutador perimetral debe ser actualizado a doble pila.

- PDSN pueden crear un túnel paquetes IPv6 sobre IPv4 si la red principal operador es sólo IPv4.
- PDSN IPv4 -> doble pila actualizaciones suelen ser actualizaciones de software.

Figura 19. Dual Stack



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

La Dual stack no requiere el túnel en el enlace inalámbrico. Con Dual stack los servicios se pueden actualizar a IPv6. Usando los registros DNS (AAAA o registros A) es el punto central de control para la transición de servicios.

4.11. ROAMING ENTRE DIFERENTES TECNOLOGÍAS DE ACCESO

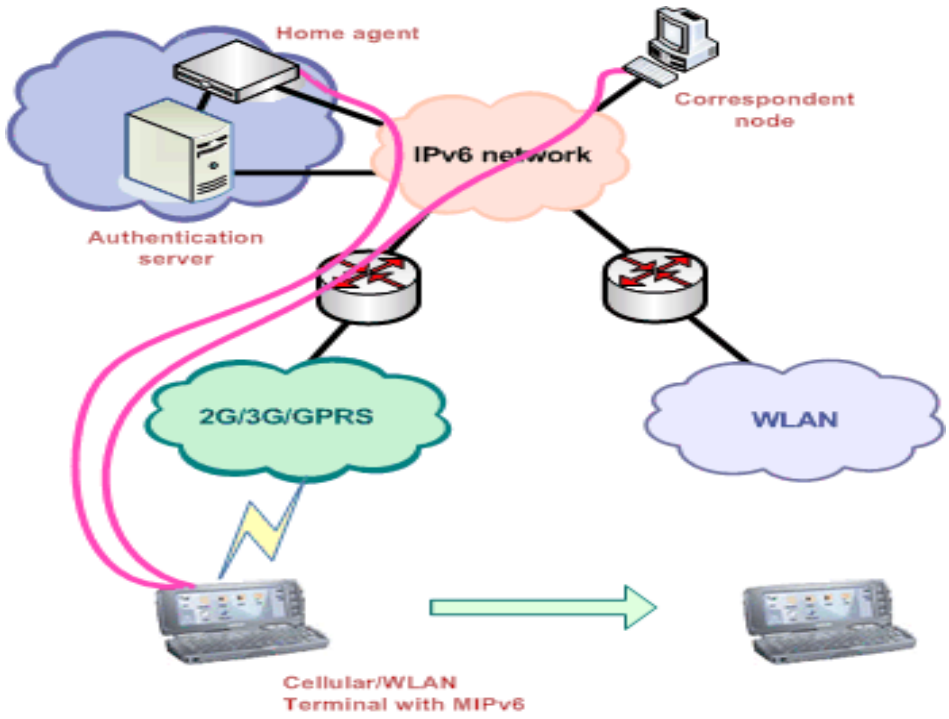
La necesidad en el planeta de movilidad y acceso múltiple, cuando un terminal móvil multi-modo de roaming entre diferentes redes de acceso. Por ejemplo, cuando se mueve un terminal multi-modo de la cobertura de WCDMA a la zona de cobertura Bluetooth o WLAN (Wireless Local Area Network), se le asigna una

nueva dirección IP. Cuando se cambia la dirección IP, las conexiones existentes de la aplicación se pierden, y necesitan ser renovadas.

Una solución a este problema es utilizar también la movilidad de la capa de IP (IPv6 móvil). Esto permite que los paquetes enviados a la dirección de su casa para ser entregado a la corriente del nodo móvil dirección de custodia. Además, IP móvil puede ocultar cualquier cambio de dirección del transporte y capas de aplicación, permitiendo que el terminal móvil para vagar sin problemas entre diferentes redes de acceso.

4.11.1. ROAMING ENTRE REDES CELULARES Y WLAN

Figura 20. Roaming

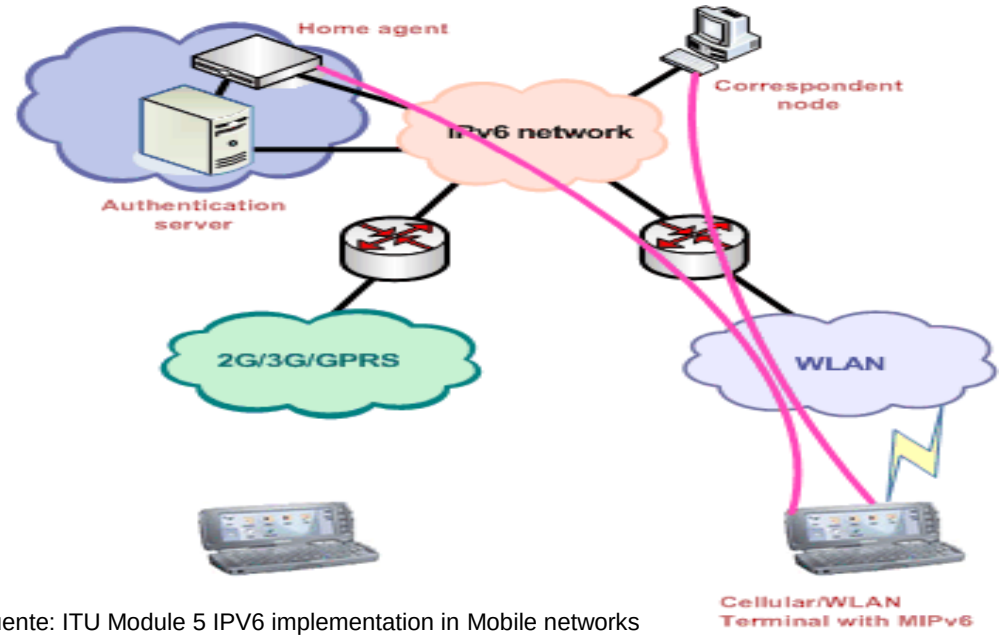


Fuente: ITU Module 5 IPV6 implementation in Mobile networks

En el terminal se abre una sesión Web con el CN, utilizando su propio CoA como la dirección IPv6 de origen y la Dirección de la casa en la opción Dirección de inicio. El terminal también envía una BU al CN.

Durante la sesión de WWW, el terminal se mueve a WLAN y tiene acceso y una nueva CoA a partir de ella. El terminal crea un contexto PDP y envía MIPv6 BU a HA, indicando su nueva CoA asignado por el GGSN.

Figura 21. Indicación de Nueva CoA



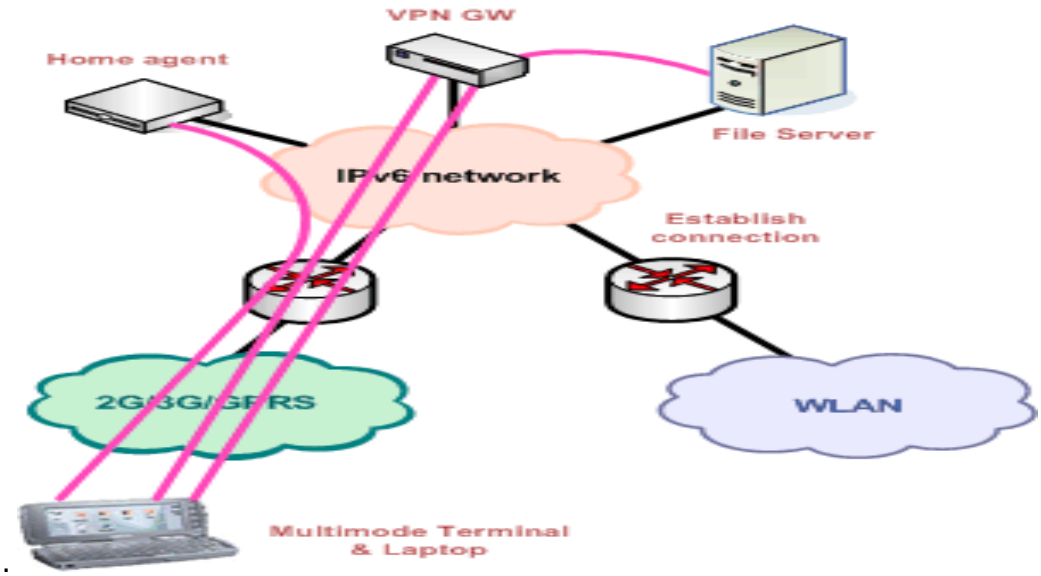
Fuente: ITU Module 5 IPV6 implementation in Mobile networks

Terminal envía un nuevo BU a HA y CN indicando su nueva CoA.

4.11.2. EJEMPLO VPN

El usuario abre una conexión VPN para la GW VPN y también envía una BU a la GW VPN. Así, el GW VPN sabe CoA del usuario actual. Crear acceso (contexto PDP) y enviar un BU para HA.

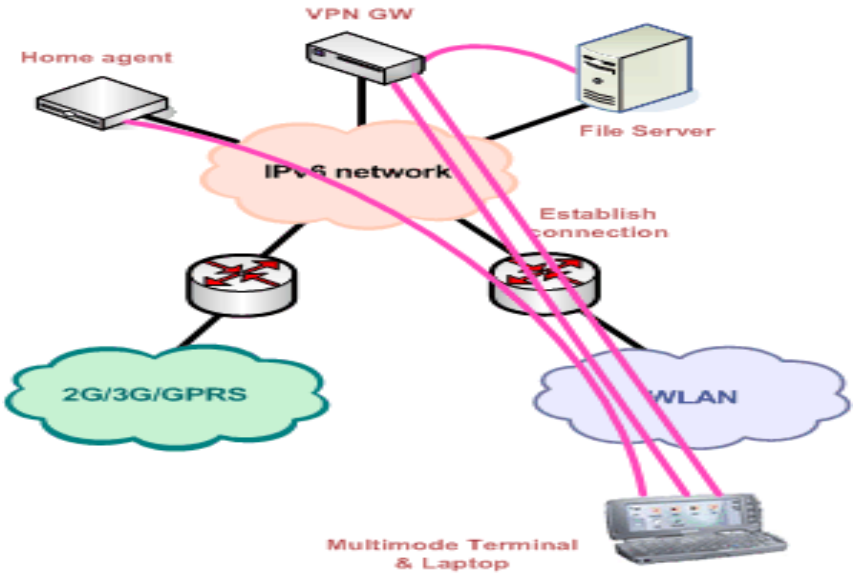
Figura 22. VPN para GW



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

El TCP abierto, se mueve de un terminal a WLAN. Obtiene acceso y envía una BU a HA. Terminal BU envía al GW VPN, lo que indica su nueva CoA. GW VPN envía los paquetes a la nueva CoA correspondientes a la Dirección de la casa.

Figura 23. Nueva CoA



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

4.12. PRINCIPALES BENEFICIOS DE IPV6 EN LA CAPA DE APLICACIÓN MOBILE

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

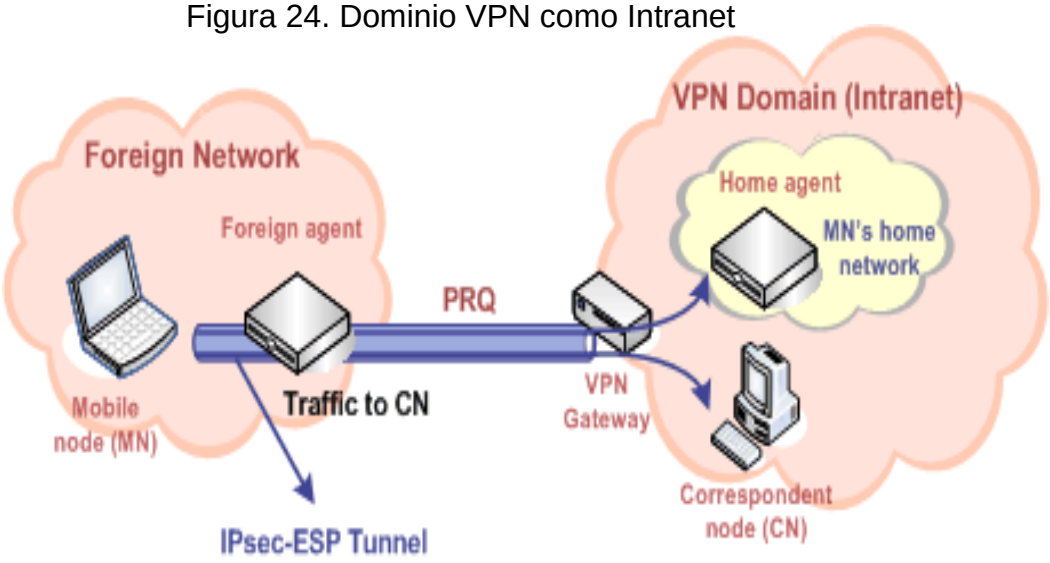
- El roaming es eficiente desde la red visitada hasta los servicios de red local
- la itinerancia sin fisuras entre tecnologías de acceso diferentes, es decir, posibilidad de conexión a través de la misma dirección también de otros tipos de redes de acceso (WLAN, Bluetooth, etc.);
- IPv6 proporciona un método viable de la dirección estática para terminales móviles.
- Accesibilidad a través de la dirección de la casa también cuando utilice los servicios de un GGSN visitado;
- peer-to-peer para ser utilizado por el nodo móvil, que permite servicios que se ejecutan en los terminales con ningún apoyo explícito por la red del operador.

4.12.1. CONCEPTO DE IPV4 MOBILE SECURITY.

El Nodo móvil siempre es direccionable con su domicilio, asignado de red doméstica. La atención fuera de los cambios de dirección en cada momento y que es tan difícil mantener el pre-configurado Asociación de Seguridad (SA). En caso de VPN, las reglas para el filtrado de datagrama cambia cada vez que se mueve cuando los nodos móviles de una red a otra.

El número de cambios de socket extranjero y aquí necesitamos un mecanismo para configurar cortafuegos (VPN) las normas. Para garantizar la seguridad, las comunicaciones móviles nodo de uso de software y MIPv4 IPsec. En el ámbito interno, el cifrado no se aplica. El dominio VPN actúan como Intranet y su dominio pertenecen a la red de confianza.

Figura 24. Dominio VPN como Intranet



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

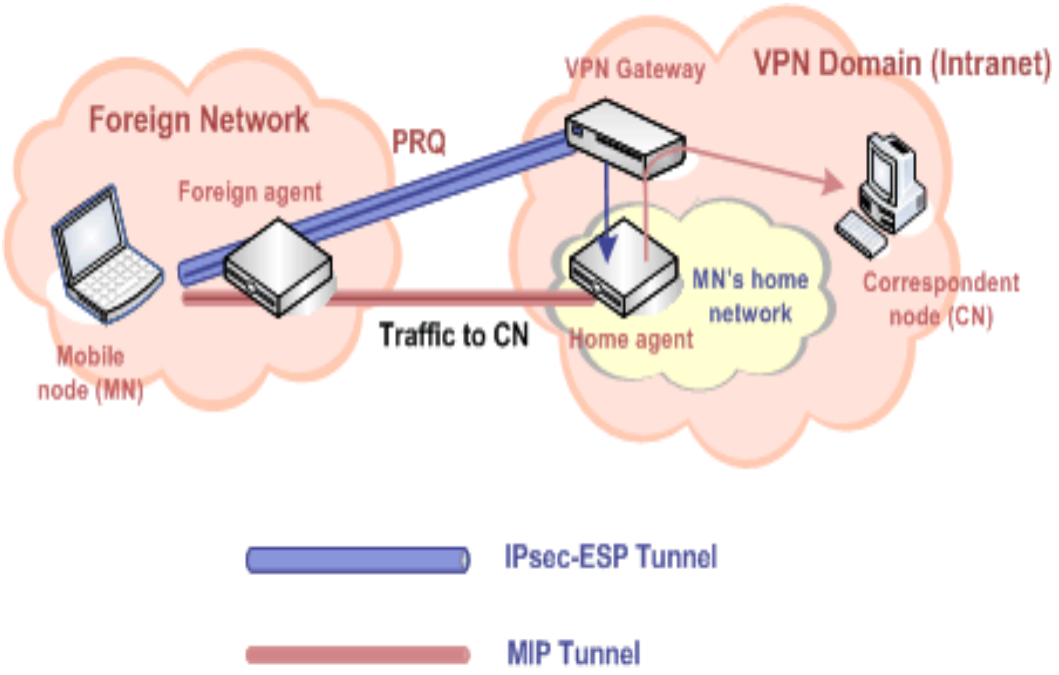
MIPv4 agentes están desplegados dentro de la red Intranet. Los nodos móviles fuera de la red no tienen un permiso para conectarse directamente a los nodos de Intranet. Uso de una conexión VPN entre nodos dentro y fuera de Intranet es una forma de intercambio de datos y de prestación de servicio. Decisión actual presenta los siguientes problemas:

1) Cuando la red exterior usa el tipo especial de agente encryption/decryption el procedimiento no es posible para ambos lados.

2) El Túnel VPN tiene que ser renegociado cada vez que los nodos móviles cambiar su puerto.

La figura 25 muestra una variante para conectar agente extranjero al nodo móvil en la red Intranet utilizando VPN y el agente de Inicio en paralelo.

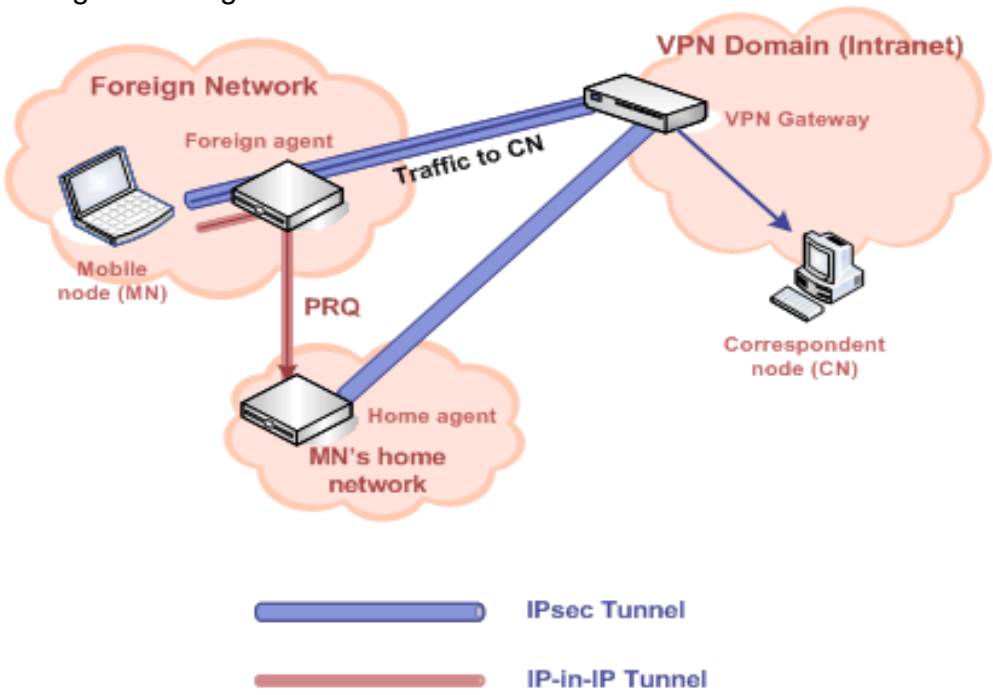
Figura 25. Conexión de agente extranjero al nodo móvil



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

En otro caso, el Agente de inicio puede ser un trabajo fuera del dominio VPN.

Figura 26. Agente fuera de dominio VPN



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

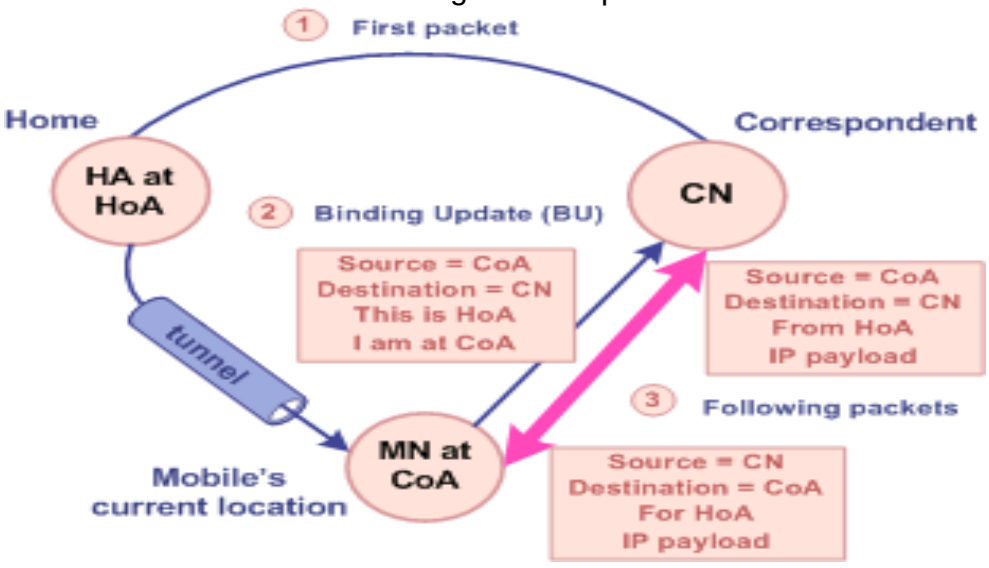
MOBILE IPV6 TIENE DOS OBJETIVOS BÁSICOS.

- Toda la capa de transporte y conexiones de capa superior y asociaciones de seguridad.
- Entre el móvil y sus corresponsales debe sobrevivir el cambio de dirección, y el host móvil debe ser accesible, siempre que esté conectado a la Internet en alguna parte en el mundo.
-

4.12.2. OPTIMIZACIÓN DE ENRUTAMIENTO

El protocolo de túnel es suficiente para permitir la movilidad, pero el resultado es de enrutamiento sub-óptimo. Paquetes entre el móvil y sus corresponsales tienen que viajar a través de la red de origen, que puede estar muy lejos. Para corregir este problema, Mobile IPv6 define un mecanismo llamado optimización de rutas. La optimización requiere cambios en el interlocutor pero se considera tan importante que cada host IPv6 tiene que soportar el protocolo. Optimización de la ruta típicamente funciona tal como se muestra en la Figura 27:

Figura 27. Optimización de la ruta



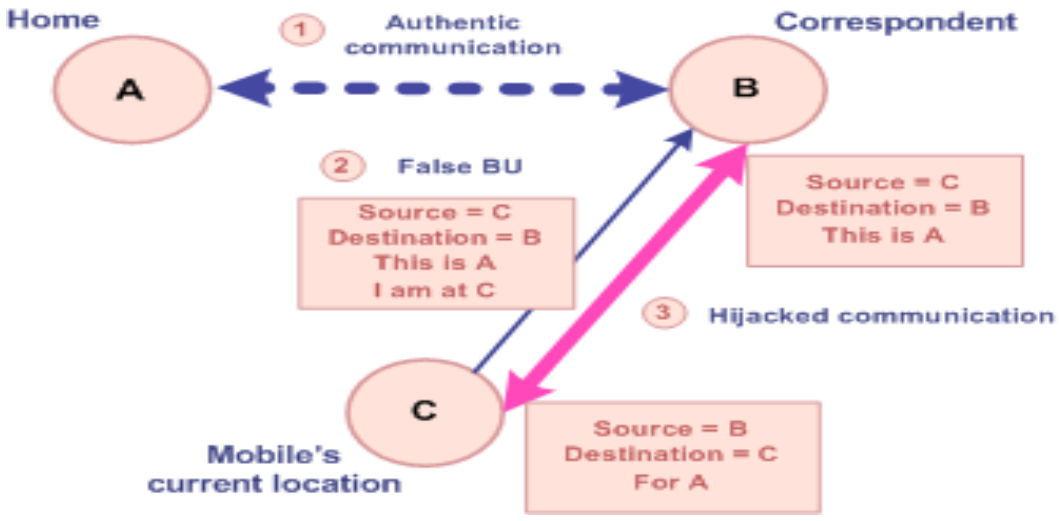
Fuente: ITU Module 5 IPV6 implementation in Mobile networks

Cuando el móvil recibe un paquete tunelado, se inicia el protocolo de optimización de ruta. El móvil envía al corresponsal un mensaje denominado actualización de enlace (BU). La actualización de vinculación contiene la dirección del móvil de origen y actúa como dirección de custodia. El corresponsal almacena esta información en su caché vinculante, lo que es en realidad una tabla de enrutamiento: se dice que los paquetes destinados a HA en lugar deberá enviarse a CoA. Por último, el corresponsal reconoce la actualización de vinculación. (Por simplicidad, los acuses de recibo no se muestran en las figuras e ignoramos la autenticación de los mensajes de la correspondiente a la móvil.)

Es bastante obvio que el protocolo de actualización de enlace, si se implementa como se ha descrito anteriormente, pudiera crear graves nuevas vulnerabilidades de seguridad. Lo primero que se nota es que las actualizaciones de unión no están autenticadas. Esta sección describe los ataques básicos que utilizan unidades de negocio inauténtica y un mecanismo de autenticación BU.

4.12.3. ALGUNOS POSIBLES ATAQUES

Figura 28. Posible Ataque



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

Un intruso en la dirección C envía una actualización falsa se une a un nodo B de Internet, que afirma ser un móvil con dirección a casa A. Si B, que actúa en el papel de un corresponsal, cree que esta actualización es obligatoria, volverá a dirigir a todos los paquetes que C están destinados a (A).

Por lo tanto, el atacante puede interceptar los paquetes enviados de B Asia A.

El atacante también puede falsificar paquetes de datos de A mediante la inserción de una falsa dirección de casa opción en ellas. Esto permite al atacante secuestrar las conexiones existentes entre A y B, y abrir otras nuevas que pretenden ser A. El atacante también puede redirigir los paquetes a otro lugar que no sea C, que impide que A y B se comuniquen entre sí. De extremo a extremo (End-to-end) la protección de datos, por ejemplo, IPSec o SSL, impide la negación mayoría de los ataques, pero no de servicio (DoS).

Estos ataques son graves porque A, B y C puede ser cualquier dirección IPv6 en cualquier parte en Internet. Todo el atacante tiene que saber es las direcciones IPv6 de A y B. Puesto que no hay diferencia visible entre una dirección de casa móvil y una dirección IPv6 estacionaria, los ataques funcionan bien en contra de los nodos de Internet estacionarios como en contra de los móviles.

La posibilidad de que estos ataques hayan causado IETF para detener el proceso de normalización Mobile IPv6 hasta que una solución para la autenticación de actualizaciones obligatorias fue encontrada. Se cree que el despliegue del protocolo sin seguridad podría resultar en una avería de en toda la Internet. Obviamente, la solución es para autenticar las actualizaciones de unión. Un mecanismo de autenticación típico implicaría un servidor de confianza en línea o una infraestructura de clave pública (PKI).

El problema es que la autenticación debe trabajar entre cualquier nodo de Internet móvil y cualquier corresponsal. Hay actualmente no existe ninguna infraestructura

de autenticación que se podría utilizar para la autenticación tales global entre cualesquiera dos nodos IPv6.

Tampoco es realista sugerir la creación de dicha infraestructura para las necesidades de Mobile IPv6. Por lo tanto, utilizando el mecanismo de autenticación convencional limitaría la optimización de ruta para uso dentro de la organización donde los servicios de seguridad requeridos están en su lugar

.

LA CAPA IP PROPORCIONA DOS TIPOS DE INFRAESTRUCTURA:

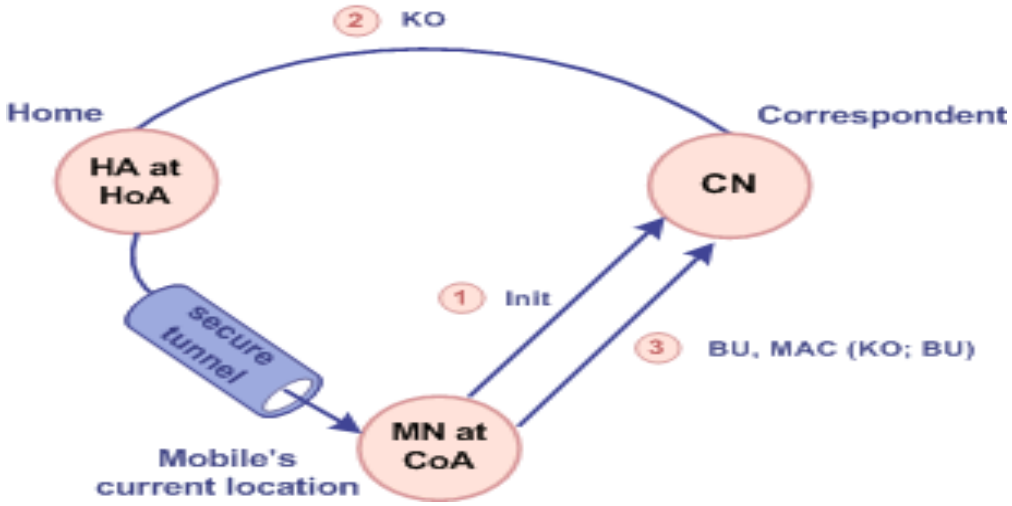
- En primer lugar, la arquitectura de direccionamiento proporciona nodos de Internet direcciones únicas, IPv6 globalmente enrutables
- En segundo lugar, la infraestructura de enrutamiento entrega los paquetes a través de Internet a su dirección de destino.

Resulta que tanto el direccionamiento y el encaminamiento puede ser utilizado para inicializar alguna forma de autenticación, no necesariamente tan fuerte como una PKI permitiría en redes cerradas pero sin embargo mejor que ninguna autenticación. Dado que estas técnicas no requieren ninguna infraestructura especial de seguridad, que son, algo engañosamente llamado autenticación de protocolos.

4.12.4. ENRUTAMIENTO DE LA AUTENTICACIÓN

El segundo método de enrutamiento de autenticación se basa en el hecho de que el encaminamiento en la Internet es semifiable. Es difícil para un atacante remoto cambiar la ruta de los paquetes que no viajan a través de la red del atacante. Por lo tanto, para poder rastrear o interceptar un paquete, el atacante tiene que estar en su ruta. La primera versión del protocolo de autenticación BU se muestra en la Figura 29.

Figura 29 Primera versión de autenticación BU



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

La idea es que después de que el móvil inicia el protocolo de BU (mensaje 1), el corresponsal envía una clave secreta como texto sin formato a la dirección del móvil (mensaje 2).
El Home Agent intersecciona el mensaje y lo reenvía al móvil a través de un túnel seguro. El móvil utiliza la clave para calcular un código de autenticación de mensaje para la actualización del enlace (mensaje 3).

Este mecanismo se denomina retorno routability prueba para la dirección de su casa debido a que el móvil tiene que volver a la corresponsal (en función de) un valor enviado por el corresponsal de la dirección de su casa.

En efecto, el corresponsal verifica que el móvil sea capaz de recibir mensajes en la dirección de su casa. Con el fin de romper el protocolo, es decir, para simular una actualización de vinculación, el atacante tiene que estar en la ruta entre el corresponsal y el móvil. Por lo tanto, el protocolo no es seguro contra el atacante modelo estándar en el que el atacante puede oler e interceptar todos los mensajes en la red.

Es natural que la mayoría de los lectores ya estén familiarizados con el protocolo en este punto del objeto a la idea de enviar una clave en texto plano. Hay, sin embargo, existen sólidos argumentos a favor del diseño.

En primer lugar, el número de posibles atacantes y metas se reduce drásticamente. Sin autenticación, cualquier nodo de Internet C podría suplantar actualizaciones de unión de cualquier nodo de Internet de A a B. cualquier nodo de Internet En nuestro protocolo, el atacante debe ser C en la ruta desde B a A, lo que significa que hay decenas típicamente solos o cientos de nodos que pueden ejecutar ese ataque, es decir, los encaminadores entre A y B y los hosts en las redes locales de A y B. Por otra parte, un nodo malicioso es capaz de dirigirse sólo las conexiones que pasan a pesar de que su red local. Para un ataque típico, tal como un huésped comprometido, el número de conexiones de este tipo es pequeño. Esta reducción en la magnitud del daño potencial solo significa que el despliegue de IPv6 Móvil ya no sería un peligro para la estabilidad de Internet.

En segundo lugar, el protocolo cumple el objetivo de diseño explícito de ser tan segura como la Internet actual sin movilidad. Suponga que el nodo móvil nunca sale de su red doméstica y siempre se comunica directamente en la dirección de su casa. En ese caso, un atacante en la ruta entre A y B puede falsificar, interceptar y rastrear paquetes entre ellos, y puede ejecutar todos los mismos ataques que fueron posibles gracias a la explotación de las debilidades de nuestro protocolo de autenticación BU.

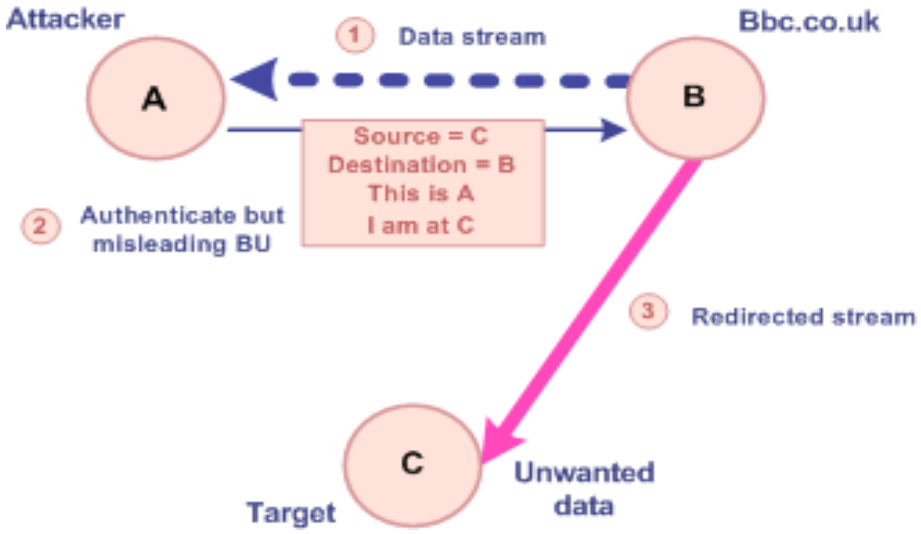
4.12.5. ATAQUES CON BOMBAS

La observación de clave es que una actualización de enlace contiene dos piezas de información, HA y la CoA, y el protocolo descrito anteriormente sólo verifica la

exactitud de la HA. Incluso si la actualización de unión es auténtica en el sentido de que fue enviado por un nodo móvil cuya dirección es la casa que aparece en el paquete, el móvil podría proporcionar un valor falso para la dirección de auxilio. En otras palabras, el móvil puede estar tumbado sobre su propia ubicación.

La Figura 30 muestra un escenario en el que el atacante un trucos un sitio web B público en el envío de un flujo de paquetes no deseados a tercera parte C. El atacante Una primera inicia la descarga de una corriente de datos, tales como una larga secuencia de TCP, desde un público se servidor B. A continuación, envía una actualización de unión autenticado al servidor que dice ser, en la dirección de auxilio de C. El servidor de aceptar la actualización de vinculación porque A utiliza una dirección auténtica. (A no tiene que ser móvil. Se puede usar su propia dirección estacionaria A como la dirección de su casa y actuar como el agente de origen y el nodo móvil en el protocolo de actualización de enlace.) Como resultado de ello, el servidor redirige el flujo de datos al falso atención de la dirección C.

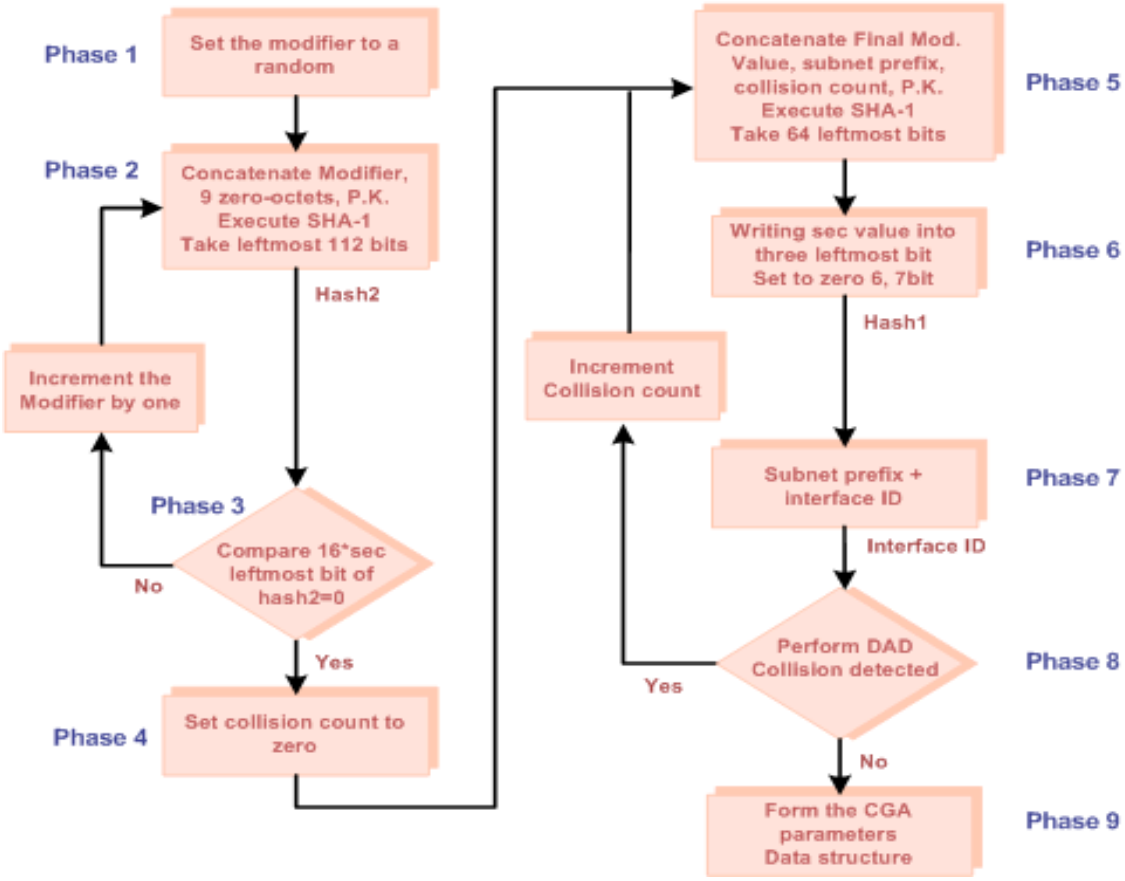
Figura 30 Ataque a sitio web



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

Para optimizar la seguridad en IPv6 uno de solución posible es utilizar criptográficamente técnicas para la generación de direcciones IPv6. Este método proporciona un conjunto de bits, generados por hashing la clave pública del propietario de la dirección IPv6. Una variante para la generación de esta dirección se muestra en la Figura 31.

Figura 31 Forma de optimizar la seguridad en ipv6



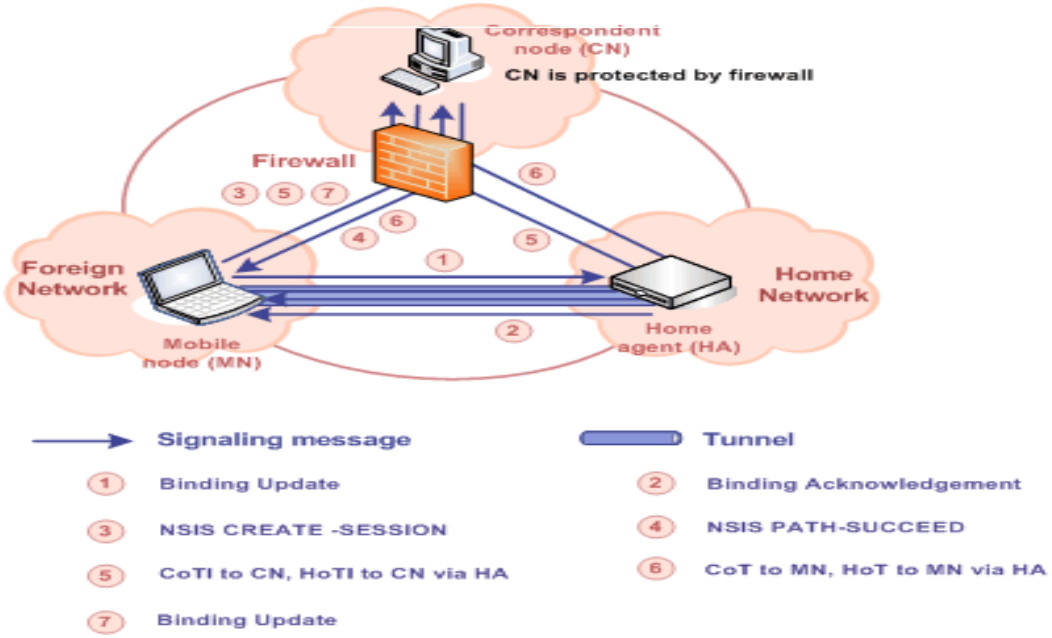
Fuente: ITU Module 5 IPV6 implementation in Mobile networks

4.12.6. FIREWALL

Una gran cantidad de servidores de seguridad utilizan el filtrado de paquetes stateful. Por lo tanto, un protocolo de señalización que puede hacer MIPv6 mensaje de atravesar varios cortafuegos de acuerdo con ciertas reglas que se

necesita. Por esta razón, un nuevo protocolo está diseñado para MIPv6 - NAT / Firewall NSIS Protocolo de señalización (NSLP).

Figura 32. Nodo correspondiente protegido por Firewall



Fuente: ITU Module 5 IPV6 implementation in Mobile networks

En la Figura 32 el nodo correspondiente está protegido por firewall. Cuando el nodo móvil se mueve fuera de la red doméstica que tiene que realizar el procedimiento de ruteabilidad de retorno antes de enviar actualización binging para el nodo de envío. El nodo móvil inicia la sesión NSIS mediante el envío de un mensaje CREATE en el modo correspondiente. El cortafuegos no puede reconocer con el nodo móvil y el servidor de seguridad no puede ser capaz de autenticar el nodo móvil. El nodo corresponsal aprueba la solicitud y el servidor de seguridad se instalará la política pertinente.

CONCLUSIONES

Los cambios de IPv4 a IPv6 radican principalmente en las siguientes categorías:

- Mejora en las capacidades de routing y direccionamiento: IPv6 aumenta el tamaño de la dirección IP de 32 a 128 bits para dar soporte a más niveles de jerarquía y a un nombre mucho más extenso de nodos direccionables, simplificando al mismo tiempo la autoconfiguración de direcciones.

- Cambios en el tipo de direcciones: En IPv6 hay tres tipos de direcciones: unicast, anycast y multicast. Las direcciones unicast identifican un solo destino. Un paquete que se envía a una dirección unicast llega sólo al ordenador al que corresponda. En el caso de las direcciones anycast se trata de un conjunto de ordenadores o dispositivos, que pueden pertenecer a nodos diferentes. Si se envía un paquete a una de estas direcciones lo recibirá el ordenador más cercano de entre las rutas posibles. Las direcciones multicast definen un conjunto de direcciones pertenecientes también a nodos diferentes, pero ahora los paquetes llegan a todas las máquinas identificadas por esa dirección.

- Simplificación del formato de la cabecera: Algunos campos de la cabecera de IPv4 han sido eliminados o convertidos en opcionales para reducir el coste de proceso de las cabeceras y para mantener el tamaño de éstas tan pequeño como sea posible a pesar del aumento en el tamaño de las direcciones de IPv6.

- Mejora en el soporte para opciones: Los cambios en la manera en que las opciones de la cabecera son codificadas permiten una menor severidad en la longitud de las opciones y una mayor flexibilidad para introducir nuevos opciones en el futuro.

- Mejora en la Quality-of-Service (QoS): Una nueva funcionalidad permite el etiquetaje de los paquetes que pertenecen a un determinado flujo, para el cual se necesitan tratamientos especiales como por ejemplo: non-default quality of service o "real- time" service.

- Capacidad de Autentificación y Privacidad: IPv6 incluye la definición de extensiones que proporcionan soporte para la autentificación, integridad de los datos y confidencialidad. Estas extensiones son uno de los elementos básicos de IPv6 y serán incluidas en todas las implementaciones del protocolo

BIBLIOGRAFIA

Cicileo, G., Gagliano, R., O'Flaherty, C., Rocha, M., Olvera, C., Palet, J., & Vives, A. (2009). IPv6 for all. 1ª edición. Buenos Aires: ISOC.Ar.

Eiji Oki, Roberto Rojas-Cessa, et al (2012). Advanced Internet Protocols, Services, and Applications.

Goralski, Walter(2009). The Illustrated Network. Massachusetts: Morgan Kauffman Publishers.

Hagen, Sylvia (2006). IPV6 Essentials. 2ª Edición. California: O'Railly Media.

Quing, L. Jinmei, T. & Shima, K.(2007). IPv6 Core Protocols Implementation. California : Morgan Kauffman Publishers.

WEBGRAFÍA

Colombia, Ministerio de TIC. Todo lo que debe saber sobre IPv6 en Colombia. (2011). Recuperado en: http://www.mintic.gov.co/index.php/mn-news/197-20110624.

García, Emilio. Transición a IPv6: ¿ha llegado el momento?(2010). Recuperado en: http://www.astic.es/sites/default/files/articulosboletic/tecnologdega_2_transicicn_a_ipv6.pdf

Matas, Diego. IPv6: la promesa de Internet sin límites (2011). Recuperado en: http://www.itespresso.es/ipv6-la-promesa-de-internet-sin-limites-49394.html

Palet, Jordi. Manual para la transición de IPv4 a IPv6. (2011). Recuperado en: http://www.baquia.com/posts/2011-03-21-manual-para-la-transicion-de-ipv4-a-ipv6

Palet, Jordi. Portal de Transición a IPv6 de América Latina y el Caribe. (2012). Recuperado en: http://portalipv6.lacnic.net/

Wonnink, Jasper. IPv6 Hosting. (2010). Recuperado en: http://www.fix6.net/ipv6-webhosting/

Este trabajo integrador está basado en el documento de la ITU

IPv. Serivices,Addressing and Routing.

Quality and Network Management. Security Problems.Network Convergence. Marketing Trends.

Module No. 5 IPv6 Implementation in Mobile Networks