
# UNIVERSIDAD NACIONAL AUTONÓMA DE MÉXICO

## FACULTAD DE INGENIERÍA

# Movilidad IPv6: Estudio, pruebas y propuesta de uso

TESIS

Para obtener el título de
**INGENIERO EN COMPUTACIÓN**

Presenta:
**DOMÍNGUEZ LÓPEZ GEOVANI**

Director de Tesis:
ING. AZAEL FERNÁNDEZ ALCÁNTARA


CIUDAD UNIVERSITARIA, MÉXICO D.F 2012

# Agradecimientos

A Dios porque:

Me ha dado el regalo más grande que una persona puede recibir en su vida, la salvación.

Tengo unos padres idóneos que me han apoyado, que de distintas maneras han estado para mí, que de diferentes formas me han guiado y que de múltiples modos he aprendido. Y que decir de la peques que con su fortaleza y fragilidad he cultivado más la persona que algún día seré.

Gozo de una familia llena de defectos y virtudes, y sin ellos, sin su comprensión, sin su ayuda, sin su sola presencia simplemente nada sería igual, no habría podido conocer lo que hoy sé ni sería lo que hoy soy.

A lo largo de mi recorrido me he topado con muchas clases de personas a través de los años, las cuales han tocado de una u otra forma mi vida.

He tenido incontables oportunidades, y a pesar de que aún no cumplo con mi promesa, él ha tenido una enorme paciencia conmigo, gracias.

# Tabla de contenido

## *Capítulo 4 Movilidad IP (MIP)*



## *Capítulo 5 Seguridad en MIPv6*



## *Capítulo 6 Mejoras en Movilidad IP*

## *Capítulo 7 Estado actual y futuro de la Movilidad IP*



## *Capítulo 8 Propuesta de MIPv6 en RedUNAM*

# Índice de Figuras

## *Capítulo 1*



## *Capítulo 2*

## *Capítulo 3*



## *Capítulo 4*

## *Capítulo 5*

## *Capítulo 6*

## *Capítulo 7*

## *Capítulo 8*

# Índice de Tablas

## *Capítulo 1*



## *Capítulo 3*



## *Capítulo 4*

## *Capítulo 5*



## *Capítulo 6*



## *Capítulo 7*

## *Capítulo 8*

# Introducción

ANTECEDENTES

Cada vez es más común hablar de una próxima convergencia en los medios y en las redes, y ante esta situación el protocolo de Internet (IP) comienza a tomar más fuerza e interés, tal y como sucedió cuando apareció en el siglo pasado. Ante este escenario, será la movilidad una de las principales funcionalidades más exigidas por los usuarios, cuestión que últimamente se ve reflejada en los requerimientos actuales de las comunicaciones inalámbricas. Por si esto no fuera suficiente, al día de hoy (específicamente a partir del 1 de febrero de 2011) se han asignado simbólicamente los últimos bloques de direcciones IPv4 disponibles a los Registros Regionales de Internet (RIRs), hecho que ratifica el inminente agotamiento de este tipo de direcciones.

Afortunadamente gracias a las capacidades y características que maneja del protocolo de Internet versión 6 (IPv6), varios de los problemas y retos que enfrentan las comunicaciones a nivel mundial se verán solucionados tales como: el espacio de direcciones IP disponibles para todo tipo de dispositivos, la auto-configuración de los dispositivos, mejoras y eficiencias en la distribución de las direcciones, etc.

DEFINICIÓN DEL PROBLEMA

Conociendo que las exigencias actuales en las comunicaciones inalámbricas son muy altas, es indispensable considerar que la implementación de la movilidad IP requiere modificaciones para mejorar la experiencia final de los usuarios, por ello se decidió abordar el uso de IPv6 como el referente para manejar la movilidad en capa de red, ya que es dicha versión de IP la que ofrece mejores capacidades en el funcionamiento de la movilidad IP.

OBJETIVO

El objetivo de esta tesis radica en documentar y exhibir el grado de desarrollo de la movilidad IPv6 (MIPv6), brindando una visión más clara del papel que asumirá en las comunicaciones inalámbricas, y planteando una propuesta de su uso en RedUNAM.

MÉTODOLOGÍA

Para conocer el estado actual de la movilidad IPv6 y ser conscientes de su funcionamiento, capacidades y limitantes se recurrió a la realización de una serie de pruebas a través de las siguientes opciones:

a) Uso de equipo físico: a través de la búsqueda de diferentes productos comerciales bajo los cuales fuera factible realizar diversos escenarios de prueba o en su defecto mediante el empleo de software libre.

b) Uso de simuladores: contempló la búsqueda y empleo de algún producto de software mediante el cual fuera posible llevar cabo distintas pruebas de la movilidad con IPv6.

ESTRUCTURA DE LA TESIS

El trabajo consta de 8 capítulos, mismos que se conforman de la siguiente manera:

En el capítulo 1 se habla de los modelos de comunicación, principalmente enfocándose al modelo de referencia OSI y la pila TCP/IP.

En el capítulo 2 se toma el tema de la movilidad, incluyendo sus clases y alcances, así como las consideraciones efectivas realizadas en distintas capas para disfrutar de ella.

En el capítulo 3 se hace referencia a IP, mostrando la situación de su versión 4, así como los elementos y características principales que giran en torno a la versión 6.

En el capítulo 4 se explora la movilidad IP, tanto en IPv4 (MIPv4) como en IPv6 (MIPv6), lo que permite distinguir las facilidades que ofrece IPv6 respecto a su predecesor.

En el capítulo 5 se examina la seguridad en MIPv6, introduciendo algunas de las amenazas que existen en las comunicaciones móviles y varias contramedidas de seguridad.

En el capítulo 6 se indagan las mejoras realizadas a MIPv6, de tal forma que se presentan sus capacidades, características y limitantes.

En el capítulo 7 se explora el estado de la movilidad IP, incluyendo su uso en las redes 3G y 4G, las redes de Próxima Generación, así como los retos que debe confrontar para lograr un despliegue a mayor escala.

En el capítulo 8 se presentan una serie de pruebas de MIPv6 realizadas para distintos tipos de tráfico (ICMPv6, TCP y UDP), mismas que se llevaron a cabo por medio de un simulador y de una maqueta; además se ofrece una propuesta del uso de MIPv6 en RedUNAM.

Posteriormente se presentan las conclusiones obtenidas y al final en la última sección, los anexos muestran algunas gráficas obtenidas de las pruebas realizadas en la maqueta.

CONTRIBUCIONES

La realización del presente trabajo pone de manifiesto las facilidades que ofrece IPv6 a la movilidad y al mismo tiempo deja en evidencia la conveniencia del uso de la movilidad IPv6, además con los resultados de las pruebas realizadas se exponen las deficiencias que posee y los retos que tendrá que enfrentar para lograr un despliegue a mayor escala.

# Capítulo 1

## Modelos de Comunicación

*The secret of getting ahead is getting started. The secret of getting started is breaking your complex overwhelming tasks into small manageable tasks, and then starting on the first one. -Mark Twain*

## 1.1 INTRODUCCIÓN

A lo largo de la historia el proceso de comunicación siempre ha permanecido como uno de los pilares esenciales y fundamentales en toda sociedad, y aunque básicamente se conserva un objetivo simple y sencillo: transmitir y expresar ideas, se han presentado con el paso de los años diversas formas de establecer una comunicación.

Actualmente una de las herramientas más recurridas para comunicarse es la Internet pues a través de esta red de redes se han plasmado un sinfín de ideas, conocimientos y pensamientos de prácticamente todos los rincones del mundo. Actualmente no es de extrañarse que para que la Internet funcione requiera de un trasfondo inimaginablemente complejo, llegando a hacer uso de una arquitectura fundamentada en protocolos y normas, a través de los cuales es posible establecer una conexión armónica de funciones físicas y lógicas de todos los dispositivos implicados en una red, ejemplo claro de ello es el modelo de referencia OSI por sus siglas en inglés (Open System Interconnection) y la pila de protocolos TCP/IP; para comprender mejor todo esto en las siguientes secciones se describen más a detalle dichos elementos.

## 1.2 MODELO DE REFERENCIA OSI

Las comunicaciones en las redes comenzaron con diversas deficiencias debido a que no se contaba con un conjunto de reglas y acuerdos que permitieran a todos los participantes mantener un orden y administración en el proceso de comunicación, inclusive se llegaron a presentar problemas de compatibilidad entre diferentes equipos, sistemas operativos y arquitecturas.

Frente a tales carencias una organización dedicada a definir normas: la Organización Internacional de Normalización, ISO por sus siglas en inglés (International Organization for Standardization) desarrolló en 1977 el primer borrador del modelo de Interconexión de Sistemas Abiertos (OSI) pero, no fue hasta 1983 que se terminó de desarrollar completamente [1]; su creación tenía el propósito de proveer un marco de referencia para mantener una consistencia en todas las comunicaciones, independientemente del protocolo de red que se estuviera usando o el servicio que se fuera a ofrecer. Fue así que a través del modelo OSI, se logró mantener de manera clara y legible el conjunto de funciones y procesos involucrados en el funcionamiento de las redes y en el correcto desarrollo de sus comunicaciones.

El modelo OSI en realidad no es un estándar en sí, más bien representa una guía para conocer en detalle todo el proceso de comunicación que existe en una red no obstante, hoy en día son las normas las que permiten manejar la complejidad que implica la

comunicación a través de una red de computadoras, cuestión que no fue nada sencilla porque en un principio la existencia de tantos elementos a considerar propició que el modelo OSI tuviera que adoptar un enfoque divide y vencerás; precisamente por esto se tomó la decisión de conformarlo de 7 capas, cada una de las cuales desarrollando un conjunto de funciones específicas (tabla 1.1).

Tabla 1.1 Modelo de referencia OSI

| Capa | Descripción |
|---|---|
| 1. Física | Define características física (eléctricas, mecánicas, etc.) de los medios físicos. |
| 2. Enlace de datos | Especifica la forma en que los nodos acceden y comparten el medio físico. |
| 3. Red | Se encarga de la entrega de un paquete desde su origen hasta su destino. |
| 4. Transporte | Permite la comunicación simultánea punto a punto de varias conexiones en un mismo nodo. |
| 5. Sesión | Gestiona la comunicación: establecimiento, administración y terminación. |
| 6. Presentación | Representación correcta de los datos. |
| 7. Aplicación | Interfaz entre usuario-aplicación que provee acceso a servicios de red |

Particularmente la idea de un modelo compuesto de varias capas obedece a varios motivos, razones que principalmente traen consigo varias ventajas, entre las cuales se encuentran:

- Cada capa es independiente en su propósito y en sus responsabilidades, situación que favorece y facilita el desarrollo de mejoras significativas sin tener que preocuparse que su alteración modifique el funcionamiento del resto de las capas; por lo tanto es posible obtener una constante y continua evolución.

- Todas las capas guardan una estrecha relación entre sí pero cada una de estas no conoce los procesos realizados en otras capas, sino que cada capa únicamente ofrece servicios a la capa superior contigua y al mismo tiempo hace uso de los servicios de la capa inferior adyacente.

- La creación de un sistema modular provoca que el diseño y la implementación sean más flexibles para los desarrolladores, ambiente que convierte la resolución de problemas en una tarea distribuida y menos compleja.

- Permitir una cooperación entre competidores provoca que los productos de diferentes fabricantes sean interoperables.

Para entender mejor la importancia del modelo OSI y el papel que desempeña es conveniente comenzar por conocer las 2 relaciones de comunicación que existen (figura 1.1):

I. Vertical: se desarrolla en un mismo dispositivo al transferir la información entre las capas adyacentes.

II. Horizontal: se presenta entre varios dispositivos al existir una comunicación entre la misma capa de los respectivos dispositivos.

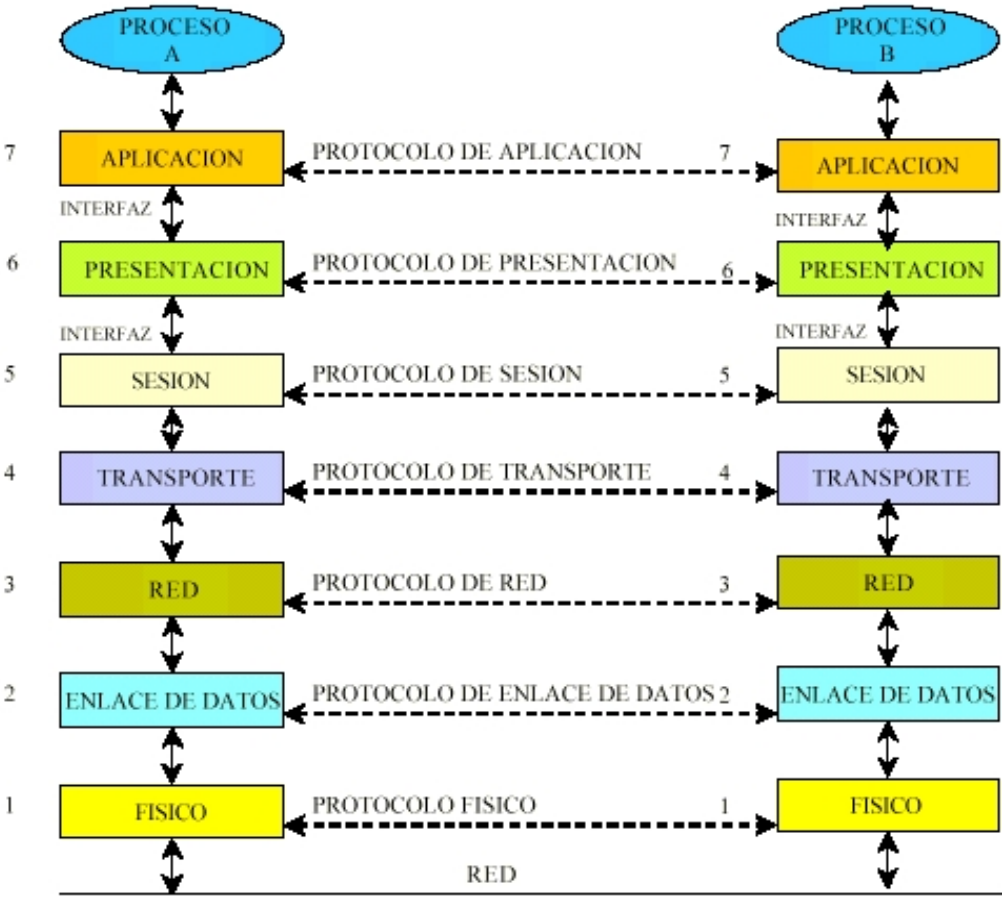



Figura 1.1 Comunicación punto a punto

Finalmente teniendo los elementos del modelo OSI en mente es posible conocer algunas características y funciones asociadas a cada capa, ya que esto permite comprender y delimitar mejor las responsabilidades que se le asignan a cada una:

1. Capa Física
   - Topología física de la red.
   - Métodos de codificación.
   - Duración y transmisión de bits.

- Características de materiales: conectores y cables en medios de transmisión; niveles de voltaje, frecuencia o pulsos de luz; distancia y velocidad máxima de transmisión, etc.

2. Capa de Enlace de Datos: se subdivide en 2 subcapas:
   a) Control de Acceso al Medio, MAC por sus siglas en inglés (Medium Access Control).
      - Direccionamiento físico (MAC).
      - Administración de acceso al medio.
      - Se comunica directamente con la capa física.
   b) Control de Enlace Lógico, LLC por sus siglas en inglés (Logical Link Control).
      - Verificación y corrección de errores.
      - Identificación del tipo de protocolo de red utilizado.
      - Determinación del inicio y fin de las tramas.

3. Capa de Red
   - Direccionamiento lógico (IP).
   - Proporciona un enrutamiento para los paquetes.
   - Manejo de cada paquete de manera independiente.

4. Capa de Transporte:
   - Segmentación y re-ensamblado.
   - Asociación de cada conexión a un socket.
   - Multiplexaje de las comunicaciones de varias aplicaciones sobre un mismo medio.
   - Dependiendo del tipo de protocolo a utilizar también puede encargarse de:
     - Control de flujo y de conexión de extremo a extremo.
     - Verificar el correcto envío y recepción de los datos.

5. Capa de Sesión
   - Establecer, mantener el intercambio de mensajes y finalizar las sesiones.
   - Servicios de sincronización en ambos puntos de la sesión y recuperación de problemas en la comunicación.
   - Control de diálogo en las comunicaciones en curso: identificar quién transmite, cuándo y por cuánto tiempo.

6. Capa de Presentación.
   - Funciones de cifrado.
   - Compresión de la información.
   - Formato y representación de los datos.

- Permite que el nodo receptor reciba una información legible.
- Esta capa no está asociada a ningún protocolo sino a códigos.
- Usa esquemas de conversión para sistemas que manejan diferentes representaciones de datos.

7. Capa de Aplicación
   - Determinación de los recursos disponibles en la red.
   - Sincronización de la comunicación entre aplicaciones.
   - Interfaz entre usuario-aplicación para proveer acceso a servicios de red.

Con el conocimiento de las características y funciones principales antes descritas ahora es más clara la manera en que se llevan a cabo las comunicaciones en una red de computadoras, a pesar de ello es necesario complementar y asociar estos elementos a alguna pila de protocolos, cuestión que se abordarán a continuación.

## 1.3 PILA DE PROTOCOLOS

Aunque a través del modelo OSI se conoce de forma abstracta y sencilla el funcionamiento del proceso de comunicación en las redes, lamentablemente dicho modelo de referencia no se encuentra implementado por algún propietario sino que cada particular u organización es libre de crear su propia implementación con el diseño y estructura que requiera.

A través de los años fueron surgiendo un sinfín de pilas de protocolos (también llamados suite de protocolos) que representan una colección de servicios y elementos, éstas tenían como objetivo brindar una solución para interconectar múltiples redes; algunos ejemplos de dichas suites son: TCP/IP, AppleTalk, IPX/SPX, etc. Pese al surgimiento de todas esas opciones en la actualidad es sin duda TCP/IP la pila de protocolos más utilizada (en comparación con el resto) debido principalmente a su diseño y al esquema bajo el cual fue establecido.

### 1.3.1 TCP/IP

Todo comenzó por los grandes cambios en las exigencias de los mercados presentados en la segunda parte del siglo pasado y por el desconcierto que existía de si funcionarían las comunicaciones a través de las redes de computadoras pero, fue el desarrollo de la Internet a principios de los 70s por parte del Departamento de Defensa de los Estados Unidos, DoD por sus siglas en inglés (Department of Defense), el acontecimiento que marcó el inicio de una importante revolución en las comunicaciones. Por esas fechas la suite TCP/IP fue creada (entre 1972 y 1974) para tiempo después

comenzar a ganar gran popularidad y aceptación pública, esto al ser elegida y adoptada en las máquinas basadas en UNIX, evento que indudablemente desencadenó su impulso; finalmente la flexibilidad que mostraba y su constante desarrollo dieron frutos, y a inicios de los 80s el DoD la implementó en su red ARPANET con resultados satisfactorios.

TCP/IP es una norma abierta que se basa en una pila de protocolos y en su creación aconteció una situación particular: el modelo OSI se desarrolló antes de que se construyeran los protocolos correspondientes a cada capa, mientras que para el caso de TCP/IP los protocolos se desarrollaron primero y posteriormente se diseñó la pila de protocolos respectiva.

Las capas que por las que está conformando TCP/IP son cuatro, a continuación se describe brevemente cada capa:

1) *Acceso a la red*: no existe una correlación directa con las capas correspondientes del modelo OSI pero, sus 2 funciones básicas son: trasmitir los datos en el medio físico y administrar el enlace de datos, es decir, especifica que cada nodo se debe conectar a la red mediante el mismo protocolo para que sea posible el envío de paquetes.

2) *Internet:* se fundamenta en el protocolo de Internet, IP por sus siglas en inglés (Internet Protocol) y presenta una comunicación basada en una conmutación de paquetes. Se constituye como la pieza principal de TCP/IP y básicamente se encarga de tomar los segmentos de la capa de Transporte, encapsularlos en paquetes (figura 1.2) y asignarles una dirección IP de origen y destino, para posteriormente seleccionar la mejor ruta de entrega. Para obtener información más detallada remítase al documento 791 de Solicitud para Comentarios, RFC por sus siglas en inglés (Request for Comments).

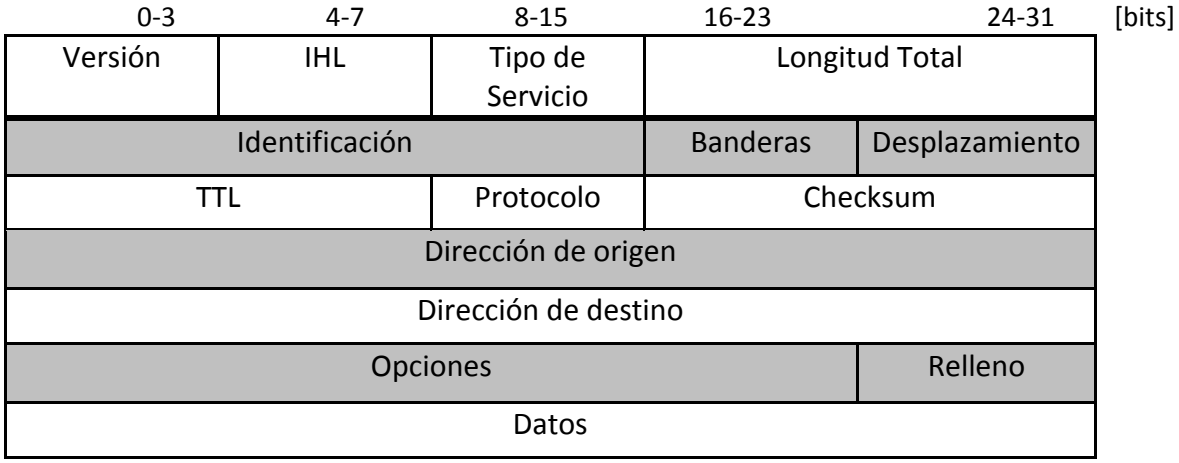



Figura 1.2 Encabezado IP

3) *Transporte:* administra el control de flujo de la información entre los hosts, pudiéndose llegar a presentar una comunicación orientada o no a conexión, estado que depende del tipo de protocolo que se utilice: Protocolo de Control de Transmisión, TCP por sus siglas en inglés (Transmission Control Protocol) o Protocolo de Datagrama de Usuario, UDP por sus siglas en inglés (User Datagram Protocol). Para ambos protocolos existen ciertas características distintivas, mismas que se observan en la tabla 1.2.

Tabla 1.2 Diferencias entre TCP y UDP

| TCP | UDP |
|---|---|
| Orientado a conexión | No orientado a conexión |
| Confiable | No confiable |
| Retransmisión de segmentos y control de flujo | Sin retransmisión ni control de flujo |
| Confirmación de recepción | Sin confirmación de recepción. |
| Manejo de números de secuencia | No existen números de secuencia. |
| Usualmente presenta mayores tiempo de retraso | Generalmente es más rápido para transmitir. |

Para entender mejor el porqué de las diferencias entre TCP y UDP se presentan sus encabezados correspondientes. En la figura 1.3 se presenta el encabezado de TCP.

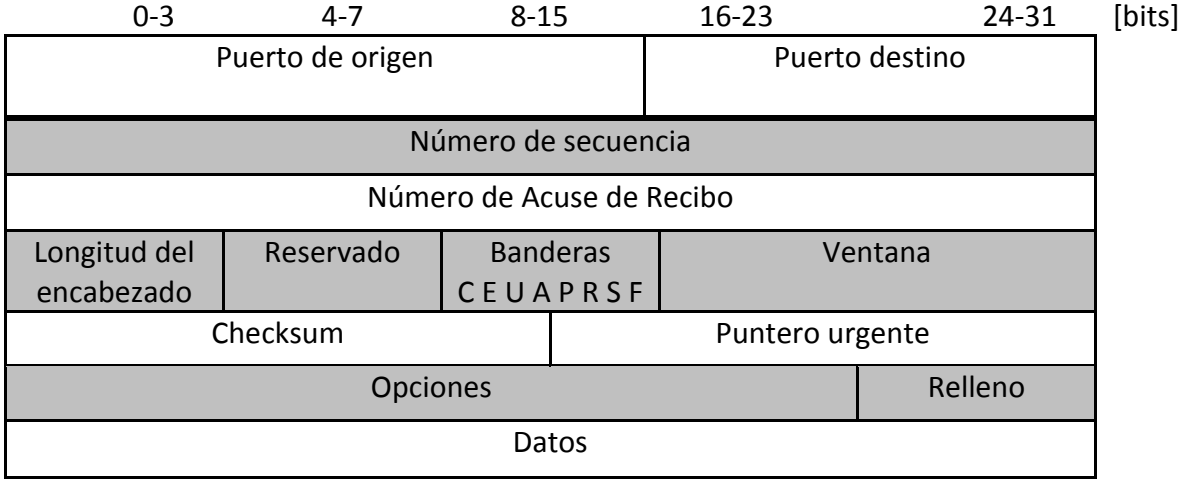



Figura 1.3 Encabezado TCP

Mientras tanto el formato del encabezo UDP está en la figura 1.4.

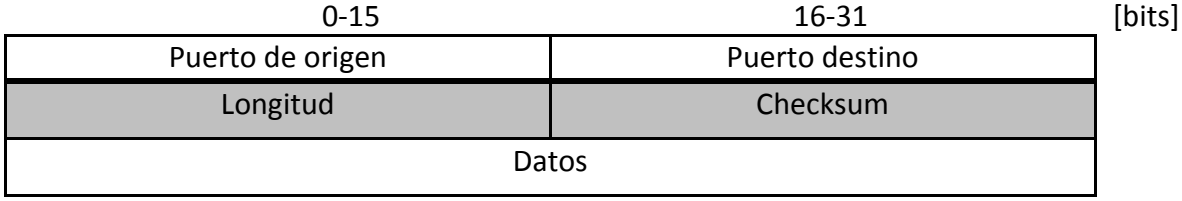



Figura 1.4 Encabezado UDP

4) *Aplicación:* define todas las funciones necesarias para actuar como la interfaz entre las aplicaciones y los usuarios finales del host, convirtiéndose en la capa que posee más protocolos asociados a ella, por ejemplo: FTP, HTTP, SNMP, SMTP, etc.

Las funciones y actividades asociadas a cada capa de TCP/IP guardan cierta similitud con el modelo OSI aunque, como tal y como se aprecia en la figura 1.5 ciertamente tienen un alcance distinto.

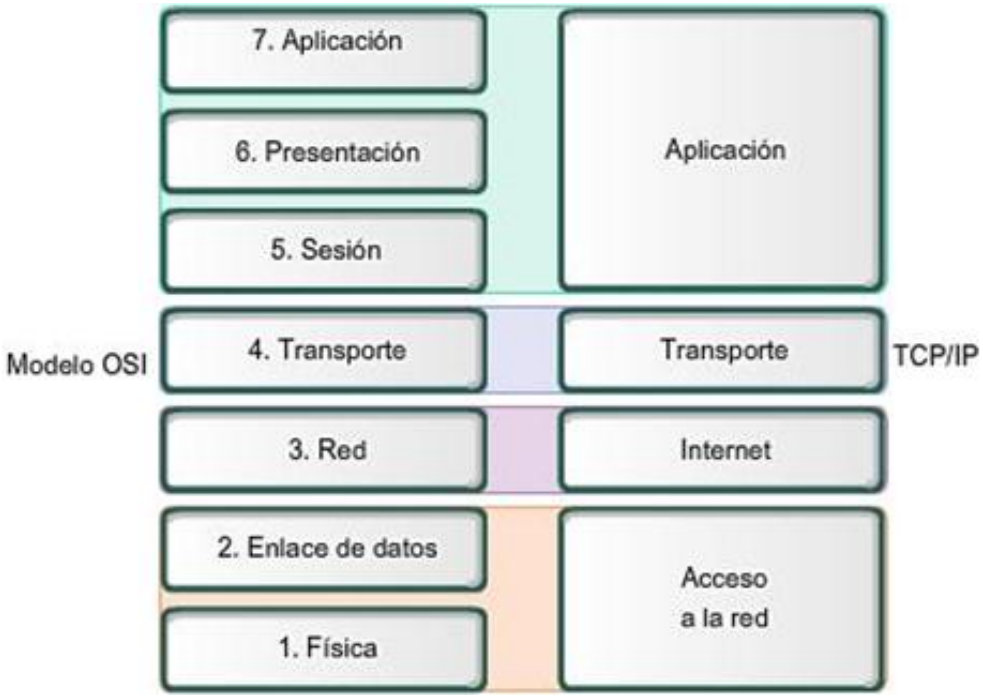



Figura 1.5 Comparación del modelo OSI y TCP/IP [2]

En la actualidad TCP/IP es ampliamente utilizada a nivel mundial porque es soportada por múltiples vendedores, es decir, una gran variedad de compañías relacionadas con el ámbito de las redes como Apple, DEC, IBM, Novell, Microsoft y Sun hacen uso de TCP/IP. Este hecho principalmente se debe a algunas de las características que posee esta pila de protocolos, tales como:

- ✓ Interoperabilidad: TCP/IP puede ser utilizada desde redes de área local hasta redes de área metropolitana, e incluso en la Internet misma.
- ✓ Flexibilidad: la existencia de múltiples protocolos permite que cada implementación se desarrolle para cubrir necesidades específicas.
- ✓ Sencillez: su diseño es simple pero efectivo, es decir, a pesar de que cada una de sus capas es independiente, sus funciones se complementan.

### 1.3.2 ENCAPSULACIÓN

Una vez descritas las acciones y funciones que se llevan a cabo en cada capa del modelo OSI y de la pila de protocolos TCP/IP, únicamente resta averiguar la forma en que la información pasa entre cada una de las capas de TCP/IP. Para lograr esto habrá que considerar que tanto en el nodo transmisor como en el receptor se establece la misma pila de protocolos, y aunque se conservan las mismas capas, el proceso que se lleva a cabo es inverso, es decir, mientras que en el emisor la comunicación comienza por la capa de Aplicación hasta llegar a la capa de Acceso a la Red, en el receptor se recibe la información por la capa de Acceso a la Red y se culmina con la capa de Aplicación.

Para comprender la interacción que se forma es importante mencionar un proceso denominado encapsulación, donde a medida que la información se encuentra en una determinada capa se le adicionan o eliminan ciertos encabezados, conformando de esta forma una unidad de datos apropiada en cada capa denominada Unidad de Datos de Protocolo, PDU por sus siglas en inglés (Protocol Data Unit) [1]. Precisamente en cada capa el nombre asociado a la PDU es diferente, ya que esto permite diferenciar la capa a la que se hace referencia (figura 1.6):

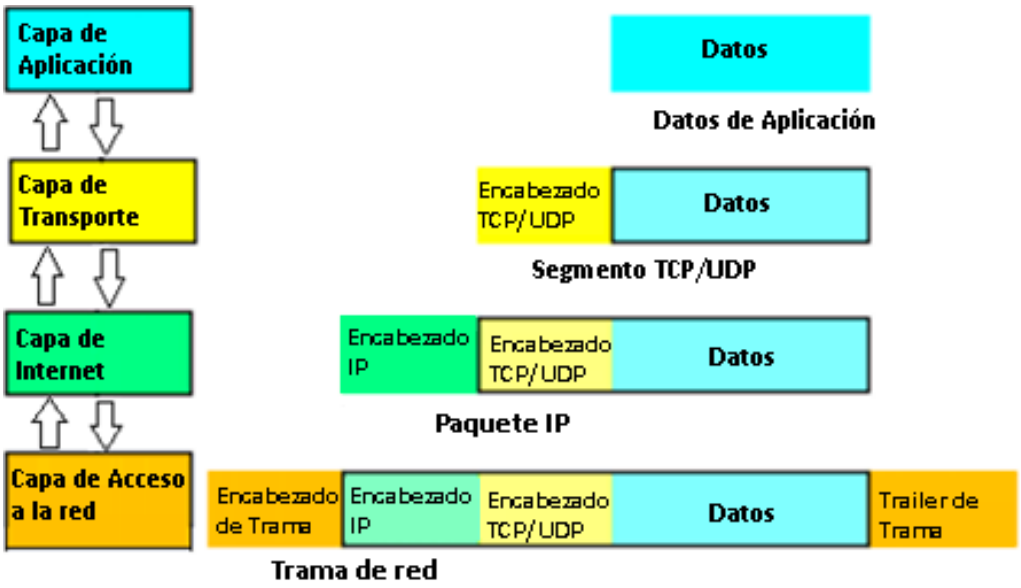



Figura 1.6 Encapsulación y PDU

- En el emisor este proceso sencillamente consiste en recibir la información de la capa superior y agregar un encabezado (representa cierta información relacionada con la capa correspondiente), de este modo al manejar un formato distinto cada capa puede reconocer y entender lo que debe procesar.

- De manera similar en el receptor se produce un proceso denominado desencapsulación, en donde a medida que el mensaje va pasando de las capas inferiores a las superiores se va retirando el encabezado correspondiente de cada capa, hasta que simplemente se entrega el mensaje original que fue enviado.

Ya sea que se hable del modelo de referencia OSI o de la pila de protocolos TCP/IP, una de las características más representativas que ambas poseen es la modularidad, es decir, se encuentran divididas en una serie de capas mediante las cuales dividen un proceso en varias etapas. Precisamente es gracias a esa característica que TCP/IP no sólo se mantiene hasta el momento como la pila de protocolos dominante, sino que además ha dado pie a que su protocolo principal (IP) se perfile como un referente a nivel mundial, lo cual a su vez hará posible que próximamente IP sea el protocolo absoluto implicado en todas las comunicaciones desarrolladas a través de redes de computadoras.

# Capítulo 2

## Movilidad

*No computer has ever been designed that is ever aware of what it's doing; but most of the time, we aren't either. - Marvin Minsky*

## 2.1 INTRODUCCIÓN

La movilidad está en la naturaleza humana, y en el mundo de las comunicaciones digitales es cada vez más indispensable que mientras una persona se desplace físicamente sea capaz de comunicarse, teniendo de manera simultánea la capacidad de acceder, generar, compartir o procesar grandes cantidades de información. Todo esto se ha desarrollado a tal grado que hoy en día las exigencias que genera la sociedad han impulsado a que esta idea pase de la imaginación a la realidad.

La tendencia actual de tener una conectividad continua ha dado origen a la expresión: Siempre Mejor Conectado, ABC por sus siglas en inglés (Always Best Connected) que hace referencia a una serie de demandas altamente exigentes, manteniendo una independencia del dispositivo utilizado, ubicación geográfica, momento del día, aplicación empleada o tecnología de acceso a la red disponible.

Claramente son muchos los factores que detonaron el rápido desarrollo de las comunicaciones móviles pero, el mercado social sin duda juega el papel más importante porque las demandas de los usuarios han provocado que nuevas tecnologías vayan tomando fuerza, y en un mundo inmensamente interconectado es cada vez más común que los usuarios, dadas sus nuevas formas y estilos de vida, vayan necesitando de más y más servicios nuevos, siendo precisamente uno de éstos el disfrutar la experiencia de movilidad. Se numeran a continuación algunas de las causas que provocan que este fenómeno se vea fortalecido:

- Constantes cambios en la ubicación física de las personas.
- Las capacidades de las redes van en aumento.
- Exigencias de mayor libertad y menos restricciones.

Frente a ello las grandes motivaciones que impulsan al desarrollo de la movilidad son:

- El enorme crecimiento en la Internet y en las comunicaciones móviles.
- Mantener una conectividad de banda ancha con retrasos mínimos a un bajo costo.
- Futuros retos, por ejemplo soportar una movilidad entre diferentes tipos de redes (todas conectadas por un núcleo basado en IP), inclusive llegando a satisfacer los requerimientos de aplicaciones basadas en tiempo real.

Con toda esta serie de acontecimientos es innegable que ya no se vislumbra la movilidad como algo tan lejano sino todo lo contrario, y todo gracias al gran desarrollo e innovación en diferentes áreas técnicas, tales como:

- Progreso en las tecnologías del desarrollo de las baterías, obteniendo una mayor duración en los dispositivos móviles a menores costos.
- Creación de dispositivos más ligeros y pequeños con mayores capacidades de procesamiento, por ejemplo: laptops, teléfonos celulares, PDAs, tabletas, teléfonos inteligentes, etc.
- Avances en las redes inalámbricas a través del uso de diversas técnicas para acceder al medio (TDMA, CDMA, FDMA), resultando en transmisiones con mayores velocidades de transferencia y mejoras en Calidad de Servicio, QoS por sus siglas en inglés (Quality of Service).
- Las mejoras en el desarrollo de software permiten disfrutar de un soporte de movilidad más estable.

No cabe duda que las nuevas generaciones de sistemas móviles tendrán que usar los avances recientes de muchos campos de estudio, basando su diseño en las nuevas teorías, algoritmos, arquitecturas, normas y protocolos, para que en un futuro cercano más y más servicios de Internet puedan ser accedidos fácilmente con diferentes tipos de dispositivos móviles en prácticamente cualquier lugar.

Innegablemente todo esto conllevará de manera gradual a la formación de un sistema integral con miras a lograr una conectividad global, por ejemplo actualmente las redes 3G han comenzado el desarrollo de aplicaciones multimedia, mientras que las redes 4G han sido orientadas con miras a mayores demandas sin embargo, aún no existe nada escrito y en un mundo tan cambiante habrá que esperar lo inesperado.

## 2.2 CONCEPTO DE MOVILIDAD

Una vez descrita la perspectiva general de lo que acontece hoy en día es necesario introducir un concepto importante, movilidad, es la característica que poseen los cuerpos para poder desplazarse físicamente (figura 2.1) [3]:

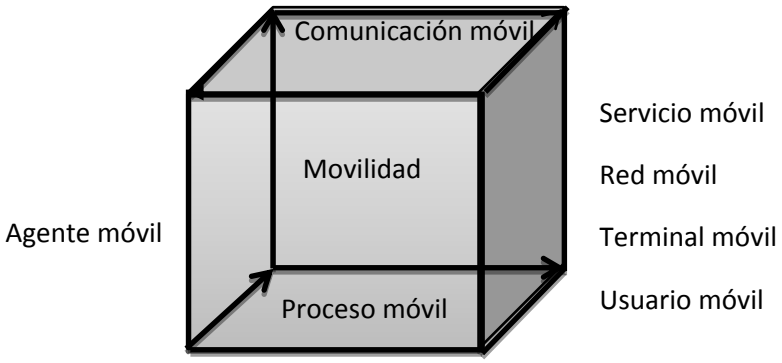



Figura 2.1 Movilidad

i) Proceso móvil: es la abstracción de una aplicación en ejecución que puede ser transferida entre diferentes sistemas.

ii) Agente móvil: su objetivo es mejorar el rendimiento y la confiabilidad a través de atributos como movilidad, autonomía, reactividad y colaboración.

iii) En una comunicación móvil los objetos móviles se integran de diversos componentes, lo que da origen a escenarios como:

   a) Servicio móvil: permite a un usuario con un dispositivo móvil continuar accediendo al mismo servicio a través de otro dispositivo.

   b) Red móvil: redes que pueden cambiar su posición física y seguir brindado un servicio continuo a sus usuarios.

   c) Terminal móvil: permite a un usuario con un dispositivo móvil desplazarse dentro de una red o entre un conjunto de éstas y mantener una comunicación accesible y estable.

   d) Usuario móvil: usuarios finales que a través del uso de un identificador pueden acceder a diferentes servicios, incluso al desplazarse entre distintas redes.

No hay duda que la movilidad trae consigo un sinfín de ventajas y nuevas oportunidades pero, al mismo tiempo, también una serie de requerimientos que deben ser tomados en cuenta para ofrecer una experiencia de movilidad completa e integral a los usuarios, por ejemplo una de las visiones y retos más complicados a enfrentar es ABC, asunto que se discute a continuación.

## 2.3 CONCEPTO "ALWAYS BEST CONNECTED" (ABC)

Este concepto fue creado por Gustaffson y Johnsson de la empresa Ericsson y como su nombre lo indica hace referencia no solamente a estar siempre conectado sino también disfrutando del mejor servicio posible en todo momento. Las implicaciones que comprende son muy variadas, van desde el tamaño y capacidad del dispositivo, requerimientos de la aplicación, hasta cuestiones como seguridad, políticas del operador, e inclusive se llegan a contemplar recursos de red disponibles, área de cobertura, etc.

Cada uno de los elementos anteriores deben estar disponibles para quien así lo requiera o solicite, y para llegar a esta meta, los servicios de ABC requieren plantear una solución completa para el administrador de la movilidad, sobre todo porque se persiguen retos como: permitir a un nodo moverse a través de diferentes tecnologías de acceso a la red mientras mantiene sus conexiones ininterrumpidas e incluso manteniendo conexiones de

manera simultánea, y administrar independientemente los flujos de cada aplicación (tomando decisiones diferentes con base en sus requisitos). Evidentemente para que esto sea una realidad habrá que contemplar los distintos escenarios que se puedan presentar, de manera que el administrador de movilidad tendrá que cumplir requerimientos significativos como:

- Lidiar con diferentes aplicaciones y decidir la mejor opción para cada una de éstas de acuerdo a distintos criterios como: costo, delay/jitter, seguridad, QoS, pérdidas de paquetes, velocidad de transmisión, etc.

- Compatible con NAT, en caso de que uno o más accesos a la red utilicen un direccionamiento privado.

- Soportar aplicaciones de todo tipo incluyendo las basadas en TCP, UDP, etc., independientemente de si son nuevas o antiguas no habrá que re-escribirlas o recompilarlas para que funcionen en un ambiente de movilidad. Al mismo tiempo debe ser sencillo desarrollar nuevas aplicaciones o mejorar las existentes para explotar completamente las capacidades ofrecidas por el administrador de movilidad.

- No se tienen que realizar modificaciones a los nodos que no posean un administrador de movilidad, todos los nodos (independientemente de si lo poseen o no) deben ser capaces de comunicarse entre sí, y particularmente aquellos que sí lo posean podrán hacer uso de los servicios de una manera más eficiente.

- La solución es escalable y permite la optimización del envío de información.

- Ocultar la ubicación actual y la información de los movimientos de los usuarios para preservar su privacidad.

- Frente a un cambio de punto de acceso se realiza una nueva asociación lo más rápido posible para que el usuario no perciba ninguna interrupción (o al menos la mínima posible) de los servicios que esté usando.

- Proporcionar servicios de seguridad: autenticación, privacidad, confidencialidad, etc. sin depender exclusivamente de un protocolo de seguridad en particular.

- Al cambiar de un punto de acceso a otro, la señalización del administrador de movilidad es enviada a la nueva red sin que deje de estar disponible la red anterior, por lo tanto se evita que se deba realizar nuevamente el proceso completo de asociación en la nueva red y se ofrece a los usuarios la capacidad de

explotar de forma concurrente ambas hasta que alguna de ellas deje de estar disponible.

Sin duda alguna aún falta un gran camino por recorrer sobre todo si se recuerda que las necesidades y requerimientos se intensifican día a día pero, de una u otra forma habrá que resolver este dilema para hacer frente a la incertidumbre del futuro.

## 2.4 CLASES Y ALCANCES

Ahora ya se conoce lo que existe detrás de ABC y es claro que pasarán algunos años para llegar ahí, mientras tanto habrá que retomar el tema central de este capítulo: movilidad.

Antes que nada para entender la administración de movilidad que se necesita llevar a cabo debemos precisar un concepto denominado *Handover*: es un proceso que se presenta cuando un nodo móvil cambia su punto de acceso a la red, es decir, pasa de una red a otra pero, mantiene sus sesiones activas. Realizada esta aclaración es de utilidad mencionar que para las redes se distinguen 3 clases principales de movilidad de acuerdo a las relaciones espacio-tiempo que existen (figura 2.2).

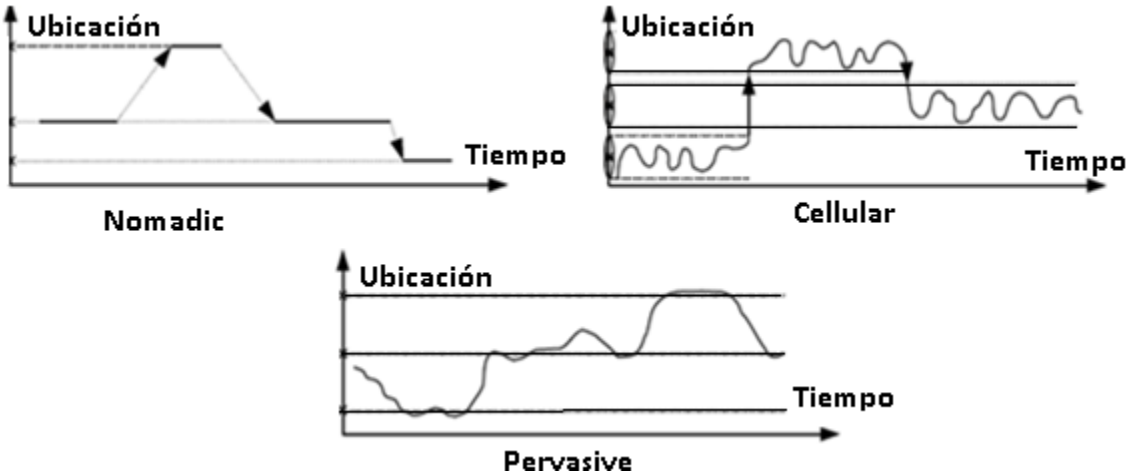



Figura 2.2 Clases de movilidad [4]

1. *Nomadic (comunicación portable):* no se requiere una conexión permanente de red mientras se está en movimiento ya que una nueva conexión es establecida después de que el nodo móvil llega a su nueva ubicación, por lo tanto los otros nodos pueden o no estar conscientes que un nodo móvil experimentó un cambio en su ubicación. Gracias a esto, únicamente la administración de localización es significante y no es necesaria la administración del handover; esto implica que las comunicaciones portables no necesariamente empleen redes inalámbricas.

2. *Celular (comunicación móvil):* la red inalámbrica está organizada en una estructura de célula, cada una de las cuales comprende cierta distancia y área de cobertura, permitiendo el reúso de frecuencias. La conectividad continua se logra cuando un dispositivo móvil se mueve de una célula a otra, y para ello se debe hacer uso de la administración de localización y handover pero, esta última solamente se usa cuando el nodo móvil se desplaza entre los límites de cobertura de las áreas.

3. *Pervasive (comunicación ad-hoc):* la comunicación entre los nodos móviles es común e incluso transparente, para lo cual se emplea una administración de localización y de handover. Este escenario generalmente no utiliza una infraestructura de red pre-existente, motivo por el que se llega a considerar este caso como un sistema autónomo, un ambiente donde los nodos móviles están conectados por enlaces inalámbricos y son libres de moverse a cualquier lugar, actuando al mismo tiempo como nodos finales y como ruteadores.

En el siguiente capítulo se retomarán las implicaciones que tiene el handover en la movilidad, mientras tanto se presentan los diversos alcances de movilidad que existen.

Actualmente un nodo móvil puede desplazarse dentro de un sistema completo de comunicaciones o entre varios sistemas (pasando a través de un conjunto de redes interconectadas), para ello usualmente una red se divide en dominios, donde cada dominio cuenta con una cierta cantidad de áreas, dentro de cada área existe un conjunto de regiones y para cada región hay determinados puntos de acceso, cada uno de los cuales posee diferentes canales lógicos. Para visualizar mejor este tipo de situaciones se enuncian algunos de los alcances de movilidad que suelen presentarse (figura 2.3):

- *Mega-movilidad:* la movilidad se desarrolla entre redes de distintas tecnologías o pertenecientes a diferentes proveedores, por ejemplo: UMTS, CDMA-2000, etc.

- *Macro-movilidad:* es la movilidad que existe entre diferentes dominios de red que aún pertenecen a una misma red. A pesar de que usualmente se desarrolla en extensas áreas geográficas suele producirse un cambio de dirección IP (existen pocos handovers). La movilidad normalmente depende de la capa de aplicación por ejemplo SIP, o de la capa de red por ejemplo IP móvil.

- *Micro-movilidad:* la movilidad se lleva a cabo entre diferentes áreas pero, todas vinculadas al mismo dominio de red. Se utilizan técnicas de capa de enlace de datos (GPRS, Wi-Fi, etc.) aunque, el proceso de enrutamiento aún sigue jugando un rol importante. Se desarrolla normalmente en pequeñas áreas geográficas por lo que se llegan a presentar frecuentes y rápidos handovers.

- *Mini-movilidad:* es la movilidad entre las diferentes regiones de una misma área.
- *Pico-movilidad:* la movilidad se desarrolla entre los diferentes puntos de acceso de una región en particular.
- *Nano-movilidad:* el nodo móvil se desplaza dentro del área de cobertura de un único punto de acceso.

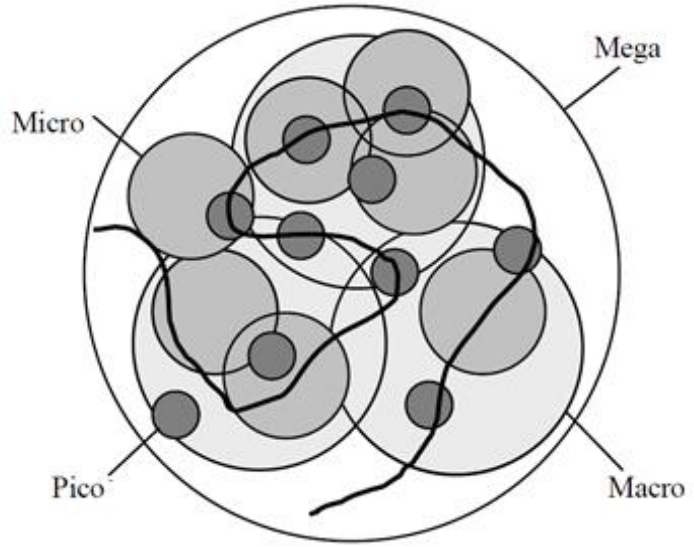



Figura 2.3 Alcances de movilidad [4]

Cada uno de estos alcances no conlleva una relación directa con el tamaño del área de cobertura o la velocidad con la que se desplaza el nodo móvil, más bien depende de una infinidad de factores.

## 2.5 CONSIDERACIONES PARA UNA EFECTIVA MOVILIDAD

Si bien es cierto que ya que se han visto las distintas clases y alcances asociados a la movilidad al final del día lo que a los usuarios les interesa, es tener soporte de movilidad, no les inmuta la forma en que se logra, lo que se hace para obtenerla o la manera en que funciona. Precisamente por ello es sumamente importante que aquellos que estén detrás de su implementación comprendan perfectamente lo que se pretende lograr, en este caso todo se reduce a mantener una sesión persistente y de calidad, es decir, conservar una sesión de forma ininterrumpida mientras uno o más nodos involucrados en la comunicación están desplazándose físicamente. Visto de esa forma pareciera que es una cosa sencilla e inclusive trivial pero, pronto se descubrirá que de cierto hay en esto.

Los efectos que provoca la movilidad en las comunicaciones y en la arquitectura de los protocolos de la red son inimaginables, y diversos mecanismos han intentando proporcionar una solución que permita manejar la movilidad. Es necesario retomar

algunos de los conceptos que se trataron en el capitulo 1 donde se hizo alusión a los modelos de comunicación: modelo de referencia OSI y pila de protocolos TCP/IP.

Antes que nada hay que recordar que el establecimiento de una sesión depende de que en cada extremo de la comunicación se cree un socket: una dirección IP y un número de puerto. El problema reside precisamente en que un nodo se identifica por su dirección IP, la cual al mismo tiempo hace referencia a su ubicación física en la red, de manera que cuando el nodo cambia su ubicación física al mismo tiempo debe cambiar su dirección IP y por ende el identificador de la sesión cambia e inevitablemente la propia sesión finaliza.

Este problema existe porque en un inicio cuando se creó TCP/IP se consideraba a los nodos finales de la comunicación como puntos estáticos que permanecían fijos en un lugar, es decir, no se planteó una solución para la movilidad y ni siquiera se dedicó una parte de su diseño para lidiar posteriormente con esa funcionalidad porque se imaginaba que no sería algo que se necesitaría en el futuro cercano sin embargo, el futuro ha llegado y es momento de plantear opciones y alternativas de solución.

Es preciso tener en cuenta lo que pasa con la movilidad en cada una de las capas, conocer las alternativas que éstas ofrecen y la facilidad de usarla en nuestras redes actuales, por ejemplo: ya que la capa de Acceso a la red de TCP/IP administra el establecimiento de un enlace entre el punto de acceso y el dispositivo móvil, no se requiere procedimientos extra cuando el dispositivo móvil se mueve dentro de una misma subred; por otra parte, si el punto de acceso pertenece a una nueva subred el soporte de movilidad podrá estar basado en la capa de red, transporte, sesión o aplicación. En la figura 2.4 se muestra que la movilidad puede ser desarrollada en diferentes capas, en cada una de las cuales se realizan diversas estrategias.

La gran pregunta que surge al respecto es ¿En qué capa se puede manejar la movilidad?, y posteriores preguntas van formulándose, tales como ¿Qué beneficios y complicaciones surgen?, ¿Bastará únicamente con realizar modificaciones o se tiene que llevar a cabo un cambio radical?

En caso de que se decidiera dar soporte de movilidad en la capa de Acceso a la red (de TCP/IP) habría que construir enlaces de radio, es decir, se necesitarían realizar modificaciones de hardware en los dispositivos actuales de red. Hecha esta observación se procederá a abordar las distintas opciones de las que se disponen.

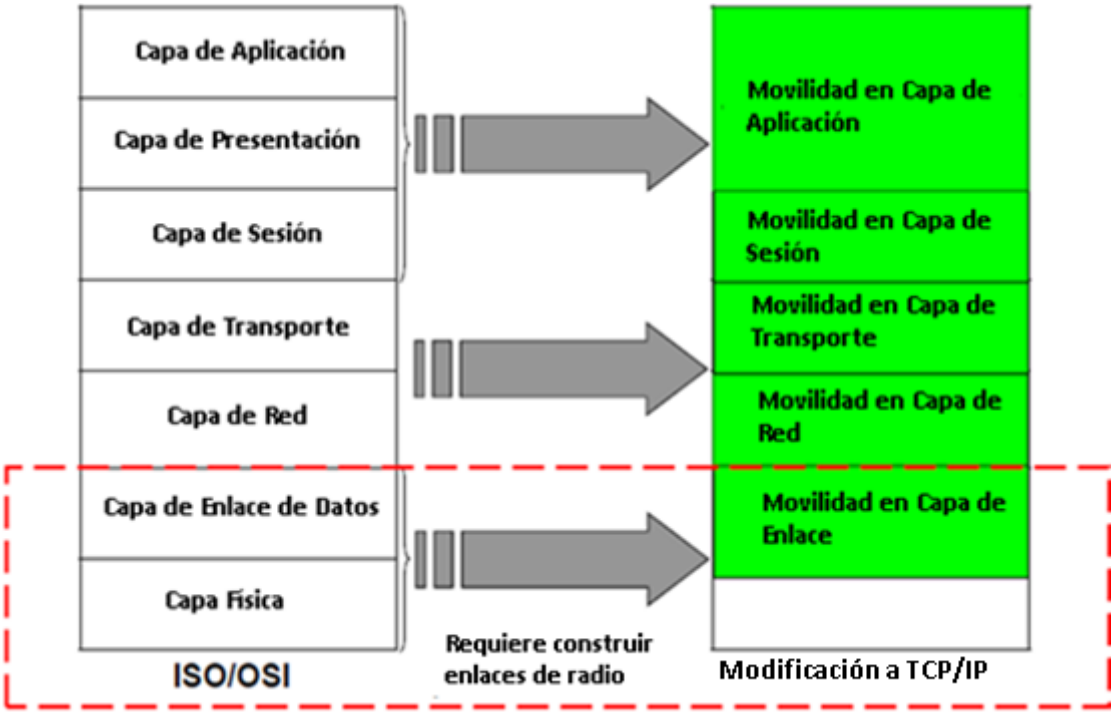



Figura 2.4 Movilidad, modelo OSI y modificación a TCP/IP

### 2.5.1 MOVILIDAD EN CAPA DE ENLACE

La capa de enlace permite a un usuario unirse a un punto de acceso a la red a través del establecimiento de una asociación, ofreciendo así un acceso ininterrumpido a los servicios de red mientras el movimiento se ubica dentro de un mismo segmento de red no obstante, para ampliar el alcance de la administración de la movilidad en esta capa es necesario que para cada una de las distintas tecnologías de acceso a la red se cuenten con características similares en ancho de banda, confiabilidad, seguridad, técnicas de corrección de errores, administración de recursos, detección de congestionamiento, etc., ya que de lo contrario la experiencia no sería la misma al pasar entre diferentes puntos de acceso que pertenezcan a redes heterogéneas.

Implementar la movilidad en la capa de enlace permite ocultar la movilidad a la capa de red y al resto de las capas superiores no obstante, la implementación llega a variar dependiendo de la tecnología de acceso a la red utilizada. Algunas de las implementaciones más representativas incluyen los siguientes tipos de redes:

- *WLAN:* usualmente con el manejo de controladoras se administran de manera centralizada los atributos y características de múltiples APs, siendo esta característica por lo general aprovechada por algunos fabricantes para implementar el soporte de movilidad y permitir que los usuarios se desplacen entre varios APs que pertenecen a diferentes controladoras pero, que integran un

mismo Conjunto de Servicios Extendido, ESS por sus siglas en inglés (Extended Service Set). En la figura 2.5 se aprecia un ejemplo de su uso.

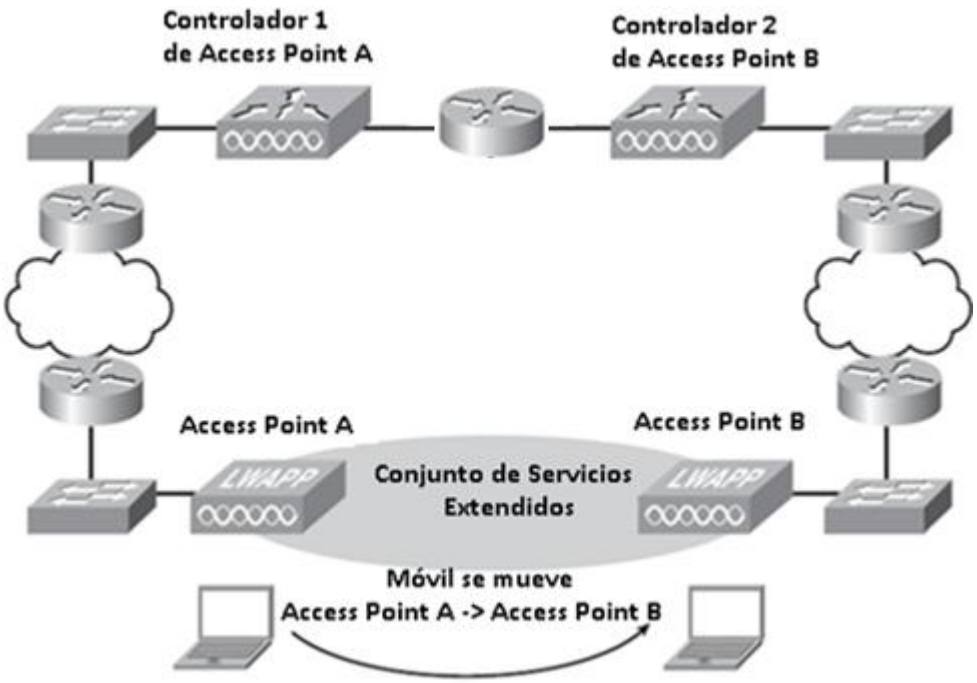



Figura 2.5 Movilidad en redes WLAN

- *WiMAX:* hoy en día este tipo de red está enfocada a proveer micro y macro movilidad, generalmente empleando un protocolo denominado PMIP (se explica en el capítulo 6) y auxiliándose de todos los elementos de la infraestructura de WiMAX para proporcionar la autenticación y configuración de los parámetros de movilidad a cada usuario móvil.

- *3GPP:* normalmente hace uso de GTP para permitir que los usuarios finales perciban toda la red celular como una conexión punto a punto, independientemente del cambio que experimente entre varios puntos de acceso a la red. Se detallará este punto posteriormente en el capítulo 7.

El mayor desafío hoy en día al manejar la movilidad en la capa de enlace es que a pesar de presentar gran funcionalidad en ambientes homogéneos (un mismo tipo de red) aún no existe un sólido desarrollo cuando la movilidad ocurre entre ambientes heterogéneos (distintos tipos de redes), tales como ir de una red de 3GPP a una que no lo es.

### 2.5.2 MOVILIDAD EN CAPA DE RED

Dado que en la capa de red se manejan direcciones IP la idea de proveer movilidad en esta capa se concentra en crear nuevos algoritmos de enrutamiento que permitan pasar del ruteo clásico (nodos fijos) a lidiar con paquetes destinados a nodos móviles que

se mueven constantemente y que cambian continuamente el punto de acceso a la red al que están asociados.

Se debe tomar en cuenta que para obtener una efectiva movilidad en esta capa habrá que lograr que mientras el dispositivo móvil se desplace se mantengan activas sus conexiones, siendo necesario conocer en todo momento su ubicación a fin de entregarle correctamente los paquetes que reciba. Uno de los principales desarrollos de movilidad de red es conocido como Movilidad IP, este protocolo se asegura de que los paquetes sean entregados a su destino final independientemente de su punto físico de acceso a la red, favoreciendo que exista una transparencia de la movilidad en los protocolos de capas superiores, situación que conlleva a que las aplicaciones de los nodos móviles continúen comunicándose sin tener que someterse a alguna modificación. Por el momento es todo lo que se mencionará de la Movilidad IP y se retomará en el capítulo 4.

### 2.5.3 MOVILIDAD EN CAPA DE TRANSPORTE

Debido a que la capa de transporte tiene una estrecha relación con la capa de red, a lo largo de los años han surgido diversos desarrollos para tratar de dar soporte de movilidad, principalmente debido a que en dicha capa existen importantes beneficios que no pueden ser cubiertos en algunas de las capas inferiores, por ejemplo:

1. No se requieren cambios en la capa de red ni en la arquitectura de ruteo actual: se mantiene intacta la naturaleza de conmutación de paquetes de la Internet, además se tiene una independencia de la capa de enlace lo que permite que se puedan soportar diferentes tecnologías de acceso a la red; esto sin duda facilita que los dispositivos móviles se muevan con facilidad entre redes heterogéneas como WLAN, 3G, etc.

2. Inherente optimización de ruta: no existe necesidad de crear túneles que oculten el cambio del punto de acceso de los dispositivos móviles. Adicionalmente se tiene la habilidad de aplicar mecanismos de optimización para las diferentes conexiones existentes, es decir, se le permite a cada usuario de un dispositivo móvil aplicar políticas únicas de optimización dependiendo del tipo de aplicación que emplee o del servicio que esté usando.

3. Capacidad de pausar las transmisiones durante una desconexión temporal: cuando hay un cambio en el punto de acceso el nodo móvil será inaccesible hasta que pueda reconectarse nuevamente, mientras tanto la capa de transporte al estar consciente de dicha desconexión pausa la transmisión hasta que pueda ser restablecida.

A pesar de estos beneficios existen al mismo tiempo una serie de complejidades implicadas, entre las que se incluyen:

a) El desarrollo de una conexión punto a punto provoca que el control de congestión sea una tarea compleja, situación que guarda una relación con las diferentes características de los tipos de enlaces implicados en la comunicación.

b) Tanto TCP y UDP asumen que una comunicación punto a punto debe permanecer estable, cuestión que dificulta ofrecer el soporte de movilidad. Particularmente debido a la naturaleza de TCP se pueden presentar problemas asociados a controles de calidad debido al cambio en la ruta que experimentan los paquetes, por ejemplo puede producirse un impacto en el control de congestión por cambios bruscos en el ancho de banda disponible, porcentajes en la pérdida de paquetes, tiempos de latencia implicados, etc.

La movilidad en la capa de transporte ocasiona que no se necesiten realizar modificaciones a la capa de red pero, lo que aún sigue siendo necesario es actualizar las conexiones existentes de los dispositivos móviles y asociarlas a la nueva dirección IP que obtengan. Para lidiar con esto se deben crear nuevos protocolos de la capa de transporte o actualizar los ya existentes, algunos ejemplos de dichos protocolos son:

A. *Protocolo de Control de Transmisión de Flujo*, SCTP por sus siglas en inglés (Stream Control Transmission Protocol): este protocolo está definido en el RFC 4960 [5] e intenta remplazar a TCP ya que permite que cada nodo maneje asociaciones: conformadas por un puerto y adicionalmente soportando de manera nativa múltiples direcciones IP, gracias a esto SCTP ofrece la facilidad de agregar o eliminar las direcciones empleadas en cada asociación.

   Adicionalmente este protocolo sigue proporcionado servicios de transporte similares a los de TCP, por ejemplo: establecimiento de conexiones punto a punto, manejo de un servicio orientado a conexión, realización de una entrega confiable de la información, considera el control de congestión, permite la recuperación de paquetes perdidos y soporta adaptación en la frecuencia de trasmisión.

   Por otro lado las 2 características clave que lo diferencian de TCP son:

   i) <u>Multi-streaming:</u> para cada asociación formada entre 2 nodos se trata a cada "stream" de manera independiente, además gracias a esta característica existe un reordenamiento de cada stream de todas las asociaciones existentes, generando así un mecanismo de control de congestión más robusto y

permitiendo por lo tanto a SCTP priorizar determinados streams, y eliminar posibles problemas de latencia. Se ilustra en la figura 2.6 esta característica.

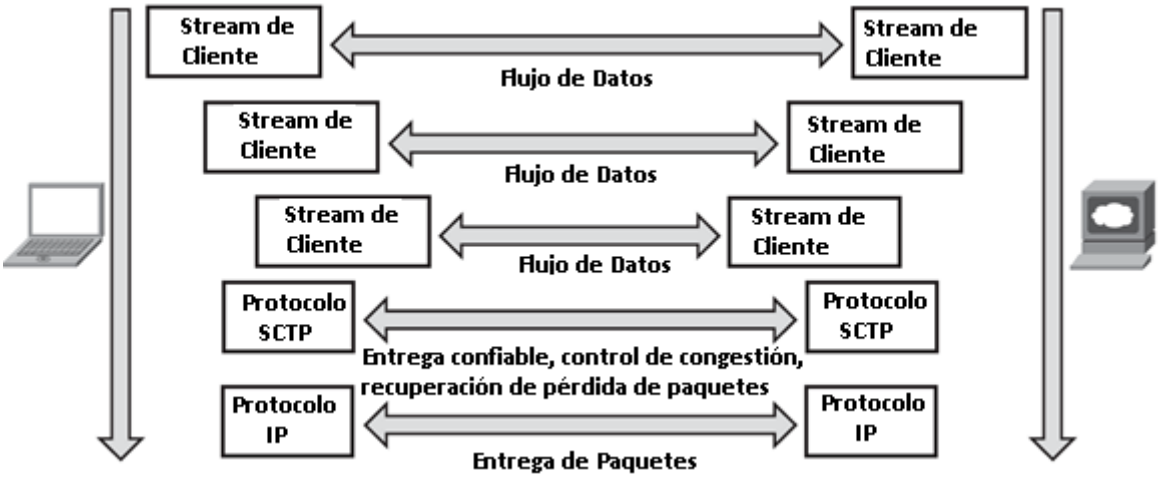



Figura 2.6 Multi-streaming en SCTP

ii) Multi-homing: al tratar la capa de red de forma independiente se tolera el uso de múltiples direcciones IPv4, IPv6 o ambas, dando así la facilidad a SCTP de manejar asociaciones persistentes. Esta situación representa una gran ventaja para las comunicaciones móviles gracias a que el multi-homing promueve la continuidad de las asociaciones de los nodos mientras cambian su punto de acceso a la red.

A pesar de los beneficios del multi-homing ofrecidos por SCTP es importante conocer que las direcciones IP que integran la asociación deben ser mutuamente excluyentes, por lo tanto no pueden utilizarse todas las direcciones al mismo tiempo en una misma asociación, es decir, se debe seleccionar una dirección IP como la ruta primaria para el proceso de comunicación mientras que las direcciones restantes, únicamente son de respaldo y se utilizan solamente cuando existe una falla o se experimenta una cierta pérdida de paquetes en la ruta primaria. En caso de que nuevamente se detecte la accesibilidad de la ruta principal se restablece el envío de paquetes a la ruta primaria y la ruta temporal vuelve a convertirse en una ruta de respaldo; de ahí la importancia de conocer el estado actual de las rutas, situación que regularmente se maneja a través del intercambio periódico de mensajes de actualización. La figura 2.7 muestra esta característica.

Adicionalmente a las 2 características anteriores, pensando en optimizar la experiencia final de los usuarios, SCTP ofrece una mejora significativa en el rendimiento de las comunicaciones, ya que permite a un nodo consumir las

porciones de información disponibles (aquellas que ya ha recibido) mientras espera a que el resto de la información le sea entregada.

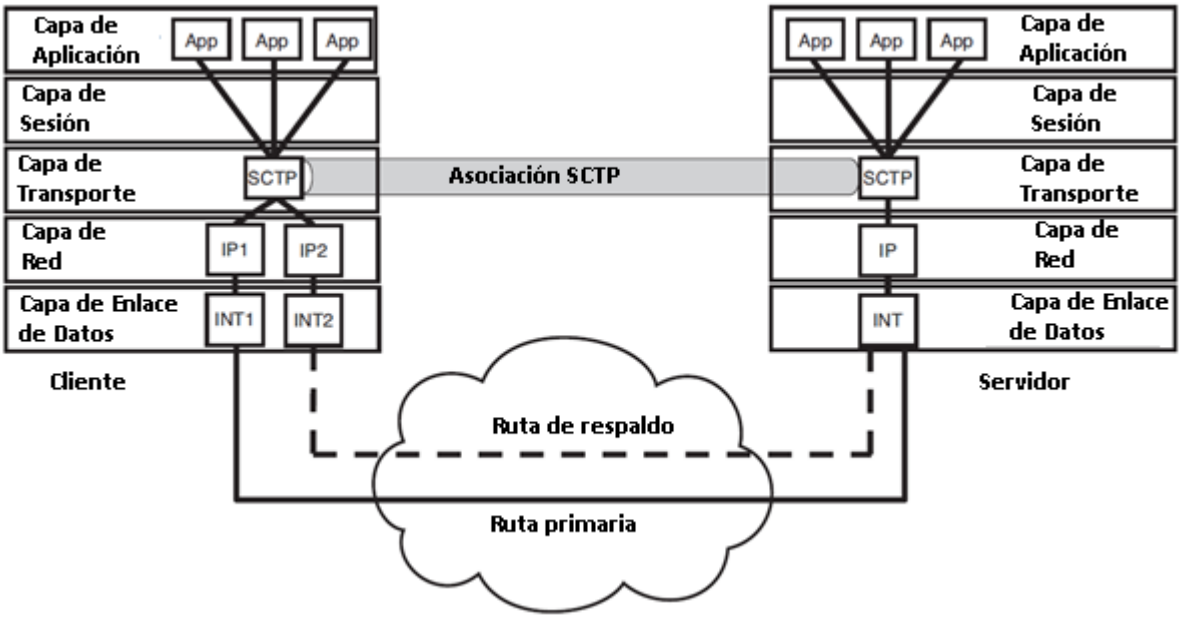



Figura 2.7 Multi-homing en SCTP

B. *Múltiples rutas TCP*, MPTCP por sus siglas en inglés (Multipath TCP): brinda extensiones a TCP para que sea capaz de soportar varias de las funciones presentes en SCTP y no exista necesidad de ser remplazado, esta situación sin duda provoca que sea más viable su desarrollo. MPTCP se define en el RFC 6182 [6] y algunos de los beneficios que proporciona son:

- Compatibilidad con la infraestructura actual de Internet.
- Transparencia en los nodos que se encuentran en la ruta de las comunicaciones.
- Estabilidad sobre las diversas rutas existentes en Internet.

MPTCP se basa en el principio de pooling, es decir, TCP puede operar de manera simultánea con múltiples interfaces y varias rutas de red, y todo es visto como un único recurso lógico. Esta particularidad sin duda incrementa la flexibilidad de la capa de transporte porque provee una protección de interfaz y de ruta, y además aumenta el uso de recursos a través de la distribución de sesiones TCP (situación que convierte a MPTCP en un candidato a considerar en la movilidad).

Existe una pila de protocolos denominada MPTCP que define una separación entre MPTCP y TCP, con lo cual se puede controlar de manera independiente la inserción y eliminación de múltiples sesiones TCP; por lo tanto al recurrir a MPTCP se puede administrar para cada sub-flujo (sesión TCP) lo siguiente: las rutas por donde se

envía la información, selección de la interfaz a usar, etc.; y todo esto culmina con la particularidad que ofrece MPTCP de tomar información de la capa de aplicación y distribuirla a través de las diferentes sesiones disponibles de TCP, tal como se muestra en la figura 2.8.

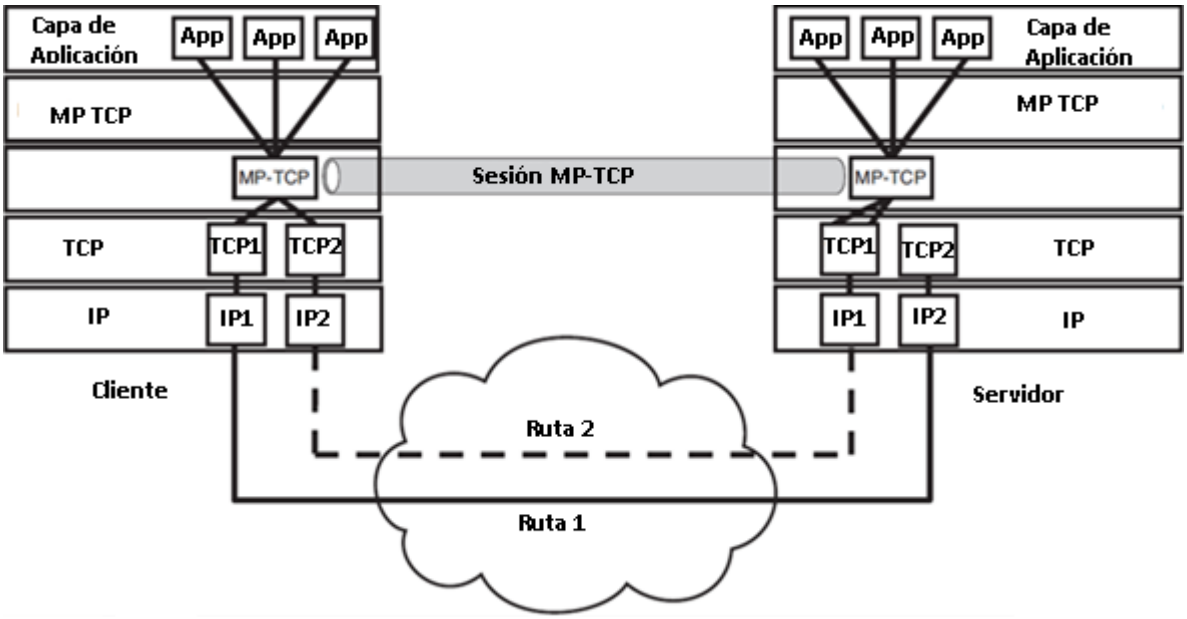



Figura 2.8 Funcionamiento de MPTCP

Finalmente antes de terminar de hablar de esta opción habrá que tomar en cuenta que al emplear MPTCP no hay forma de garantizar que exista una redundancia completa, es decir, este protocolo no tiene manera de distinguir o identificar rutas únicas ya que simplemente verifica que la existencia de redundancia en las interfaces mejore el nivel de confiabilidad.

C. *MSOCKS:* surgió como un proyecto de investigación entre IBM y la Universidad de Carnegie Mello y culminó con la creación de una arquitectura conocida como Movilidad en Capa de Transporte, TLM por sus siglas en inglés (Transport Layer Mobility) [7]. El propósito que perseguía era permitir a un cliente cambiar su punto de acceso a la red usando dos interfaces al mismo tiempo y determinar que tráfico de entrada y salida sería enviado sobre cada una.

   En la arquitectura que TLM usa existe un nodo intermediario (ubicado entre el cliente y el servidor) conocido como proxy, éste nodo se encuentra en la ruta del flujo de tráfico no sólo para mediar la comunicación sino también para proveer servicios en representación de los nodos finales, cuestión que se logra al habilitar múltiples interfaces en el proxy y asignándoles las rutas respetivas al servidor.

Habrá que contemplar que TLM no solamente requiere un proxy sino también la modificación de la pila TCP/IP en el cliente, con tales elementos esta arquitectura es capaz de soportar la movilidad al proveer un mecanismo para migrar la conexión entre el cliente y el proxy a una nueva interfaz, y al mismo tiempo manteniendo sin cambios la conexión entre el proxy y el servidor implicado en la comunicación. Se presenta un ejemplo en la figura 2.9.

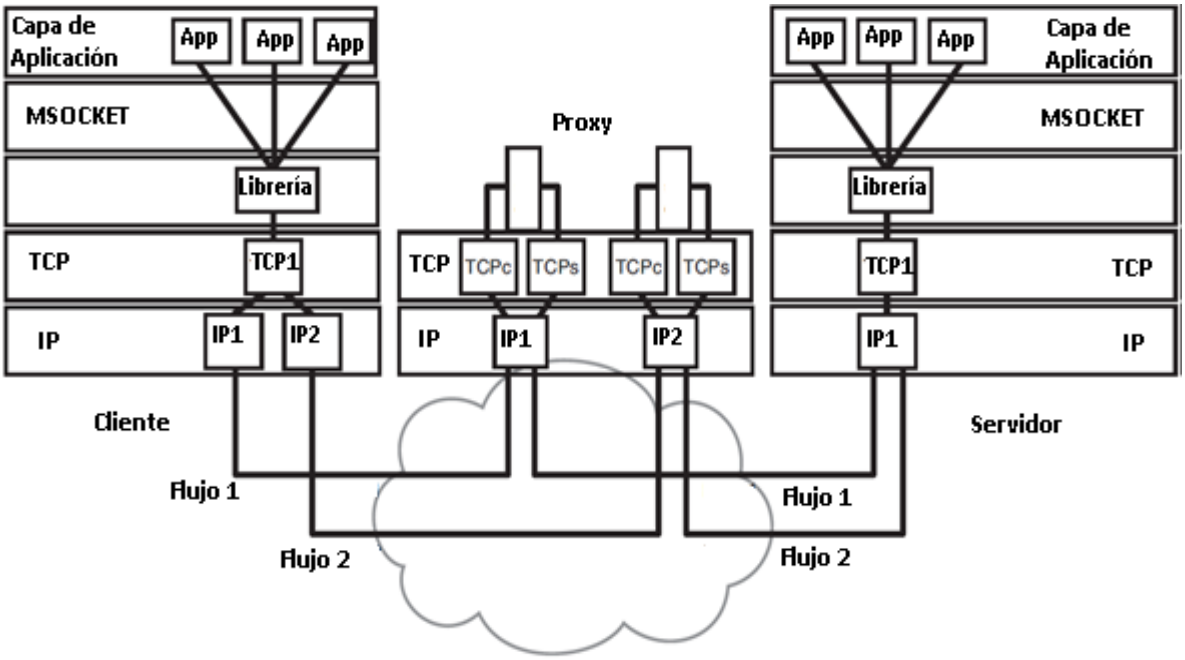



Figura 2.9 Funciones de control de interfaz TLM

A pesar de los beneficios que ofrece TLM actualmente no es muy utilizado porque al mantener fijo el proxy se provoca una ineficiencia al trabajar entre diversos dominios o múltiples operadores, cuestión que resulta ser una limitante muy importante sobre todo en ambientes donde la movilidad es continua y extensa.

### 2.5.4 MOVILIDAD EN CAPA DE SESIÓN

A lo largo de la historia la capa de sesión ha sido omitida en la mayoría de las pilas de protocolos existentes, por el contrario en vez de utilizar la capa de sesión son las propias aplicaciones las que crean y usan las conexiones de la capa de transporte, situación que provoca que la administración de la movilidad tenga que ser manejada en cada conexión de la capa de transporte. Fue entonces que surgió la idea de aprovechar la capa de sesión y emplearla para administrar la movilidad, delegándole las funciones de monitorear el movimiento de los nodos y activar las asociaciones correspondientes según se vayan necesitando.

Aunque propiamente no existe la capa de sesión en TCP/IP sin duda resulta una opción atractiva utilizar la Movilidad en la Capa de Sesión, SLM por sus siglas en inglés (Session Layer Mobility) porque ya no habría necesidad de modificar o reemplazar la capa de transporte sino simplemente adicionar esta nueva capa a las implementaciones ya existentes. SLM administra la movilidad punto a punto sin hacer uso de túneles IP, en vez de ello se basa en una pequeña capa denominada Administración de Sesión, SM por sus siglas en inglés (Session Management) que actúa como intermediaria entre las capas de aplicación y transporte, y adicionalmente provee un control en todas las conexiones que se establecen, soportando de esta manera algunas de las características de multi-homing de SCTP, tal como se aprecia en la figura 2.10.

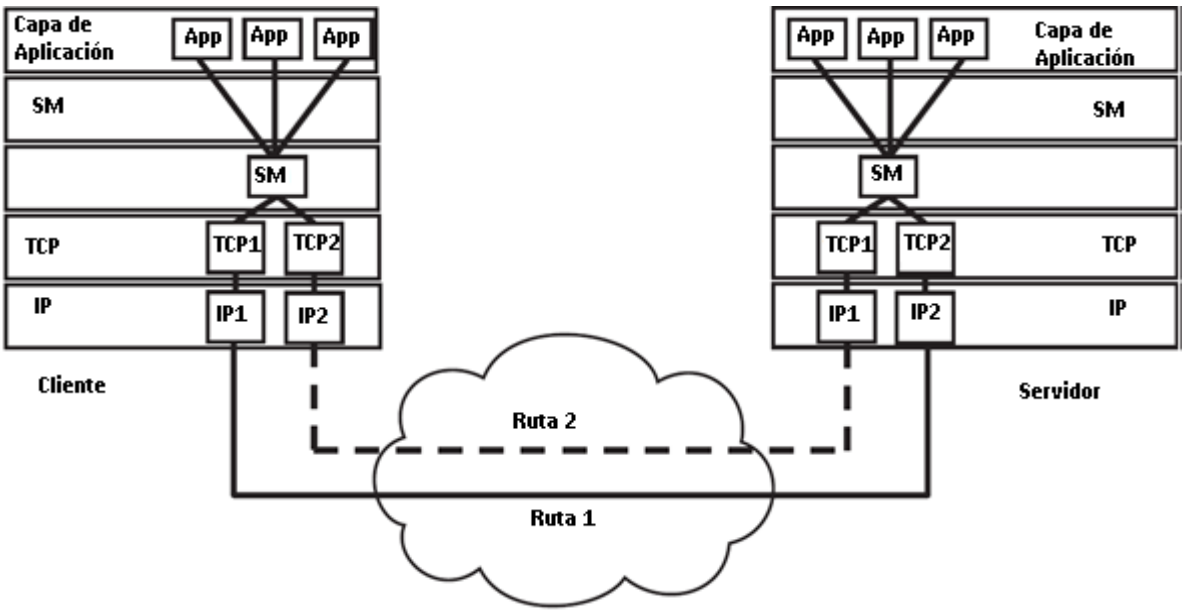



Figura 2.10 SM en SLM

En SLM se identifica a un nodo denominado Servidor de Localización de Usuario, ULS por sus siglas en inglés (User Location Server) el cual se encarga de ubicar a la parte interesada y realizar las traducciones necesarias de direcciones, por ejemplo cuando un nodo móvil cambia su punto de acceso a la red, envía un mensaje de actualización al ULS (informándole de su nueva ubicación) y este último comunica la ubicación actual del nodo móvil cuando algún otro nodo le solicita dicha información; se observa este caso en la figura 2.11.

El mayor problema de esta solución son los tiempos de retraso implicados en las comunicaciones móviles debido al envío de mensajes de actualización, además su desarrollo implica realizar algunos cambios en la arquitectura de la Internet actual, teniendo que modificar las funciones de la capa de aplicación para delegar las funciones respectivas a la capa de sesión, lo que sin duda puede resultar ser un factor determinante.

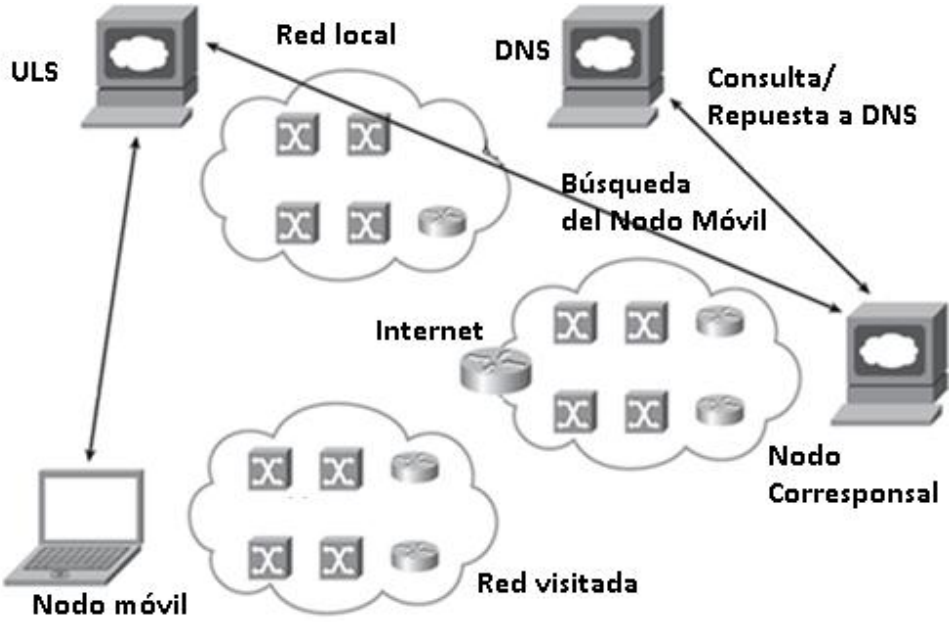



Figura 2.11 ULS en SLM

### 2.5.5 MOVILIDAD EN CAPA DE APLICACIÓN

Esta propuesta se basa en el uso de nuevos protocolos en la capa de aplicación que provean el soporte de movilidad, por lo tanto no se necesita realizar ningún cambio a las redes actuales no obstante, existen ciertos efectos contraproducentes, por ejemplo los nodos que se están comunicando estarán totalmente conscientes de cualquier cambio en la dirección IP del otro nodo, es decir, se puede rastrear la nueva ubicación de los usuarios. Precisamente para solucionar esta situación es necesario implementar mecanismos adicionales que permitan ocultar esta información y continuar ofreciendo privacidad.

Una particularidad importante es que la movilidad en la capa de aplicación no utiliza las direcciones IP como identificadores personales, lo cual facilita el manejo de diversos tipos de relaciones, por ejemplo: una relación uno a uno entre un identificador personal y un usuario; una relación de varios a uno, donde un usuario tiene múltiples identificadores personales; o una relación uno a varios, donde un identificador personal se comparte entre diversos usuarios. En la figura 2.12 se observan varios ejemplos de estas relaciones.

El desarrollo más prometedor es el Protocolo de Iniciación de Sesión, SIP por sus siglas en inglés (Session Initiation Protocol). Este protocolo se define en el RFC 3261 [8] y es independiente de protocolos de capas inferiores (IP, TCP, UDP, SCTP, etc.), generalmente es empleado para crear, modificar y finalizar las sesiones entre uno o varios nodos a través de un cambio en la relación nombre de usuario/dirección IP, por ejemplo es regularmente empleado en conferencias multimedia, VoIP, etc.

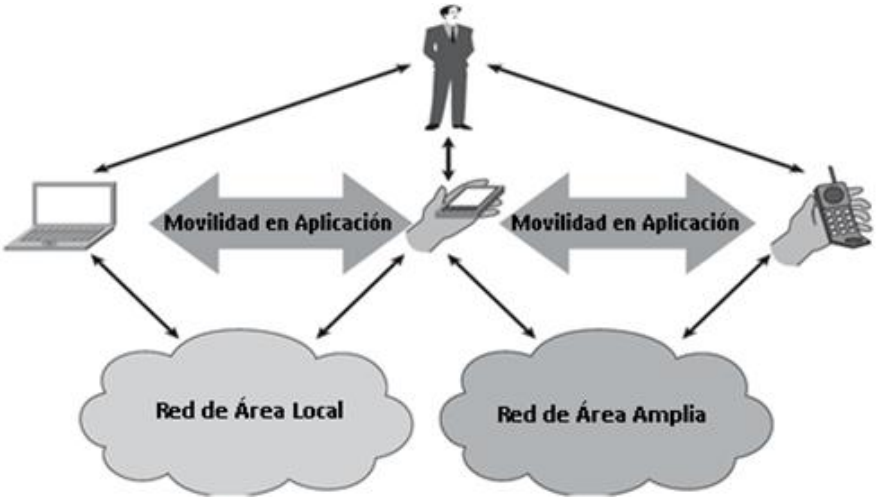



Figura 2.12 Relaciones de dispositivos móviles

No se debe perder de vista que la movilidad a nivel de aplicación maneja una característica muy representativa: movilidad inter-dispositivo, es decir, se puede mantener una continuidad en los servicios usados incluso cuando el usuario cambia el dispositivo mediante el cual accede a dichos servicios. Específicamente SIP hace esto posible al realizar una transferencia de sesiones entre los dispositivos implicados en la comunicación, tal como se observa en la figura 2.13.


Figura 2.13 Transferencia de sesión en SIP

Todas las opciones a considerar que existen, dependiendo del tipo de red en que se usan y para que se emplean, tienen sus bondades y limitantes, por lo cual sería admisible contemplar una solución que incluya varias capas para dar soporte de movilidad, después de todo hay que ofrecer una experiencia lo más robusta posible, manteniendo características como seguridad, escalabilidad, facilidad de integración y sencillez.

## 2.6 MERCADO ACTUAL

Debido a que hoy en día las exigencias de la sociedad son muy altas, el brindar movilidad lleva tras de sí una enorme cantidad de esfuerzos, y pensar que todo comenzó por el gran auge en la adopción del servicio celular en los 90s y principios de la década pasada. En cuestión de años se fue de un servicio de voz basado en conmutación de circuitos que era empleado en redes GSM (Global System for Mobile Communications) o CDMA (Code Division Multiple Access) a un servicio de conmutación de paquetes utilizado en redes GPRS (General Packet Radio Service) o

cdma2000, para finalmente llegar a disfrutar de los servicios móviles de banda ancha a través de WiMAX o LTE (explicados en el capítulo 7).

Tan sólo hay que mirar a nuestro alrededor para darse cuenta que las personas se desplazan continuamente, moviéndose de un lugar a otro con suma rapidez y facilidad y lo único que les importa es mantenerse comunicados en cualquier lugar y en todo momento. Si además se toma en cuenta que los dispositivos móviles son cada vez más pequeños y ligeros, económicos y fáciles de usar; no es de extrañarse que estos elementos se combinen y den paso a una tendencia donde la cantidad de dispositivos móviles llegue a ser de varios billones a nivel mundial. Estos sucesos son confirmados por el estudio "Visual Networking Index" [9] realizado por Cisco Systems, tal como lo muestra la figura 2.14.

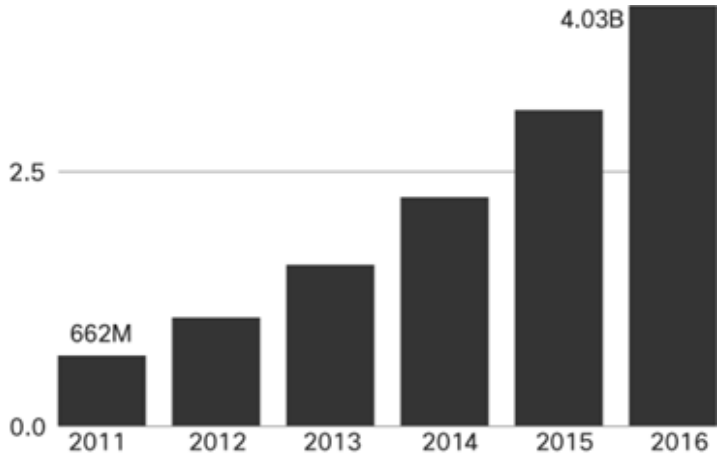



Figura 2.14 Crecimiento de dispositivos móviles

Por otra parte, gracias al gran impulso en las comunicaciones móviles es cada vez más común que las personas utilicen sus dispositivos móviles en el hogar, en la calle, e inclusive en el trabajo. Especialmente ha surgido una tendencia donde los trabajadores utilizan sus propios dispositivos móviles para acceder a los recursos privados del lugar donde laboran, comúnmente conocido como Trae tu propio dispositivo, BYOD por sus siglas en inglés (Bring Your Own Device). Este escenario implica la modificación o readaptación de las políticas de seguridad para asegurar que se mantenga un control en el acceso y se garantice la seguridad de información confidencial, para hacer esto posible es vital realizar el cifrado de las transmisiones y emplea una autenticación mutua, ya que de lo contrario BYOD muy probablemente se convertiría en Bring Your Own Disaster.

Como era de esperarse el hecho va más allá de que los usuarios utilicen más dispositivos móviles, los usuarios desean disfrutar de nuevos servicios y ya no se conforman con mandar mensajes, tomar fotos, realizar llamadas telefónicas, navegar por Internet o consultar su correo electrónico; ahora es más recurrente el uso de redes sociales, jugar en línea, comprar apps, realizar video-llamadas, descargar o compartir videos, y un sinfín de

servicios que se avecinan en la presente década. Esto nuevamente se ve ratificado por el grupo IBSG de Cisco [10], en la figura 2.15 se aprecian las nuevas direcciones en el uso de los dispositivos móviles.

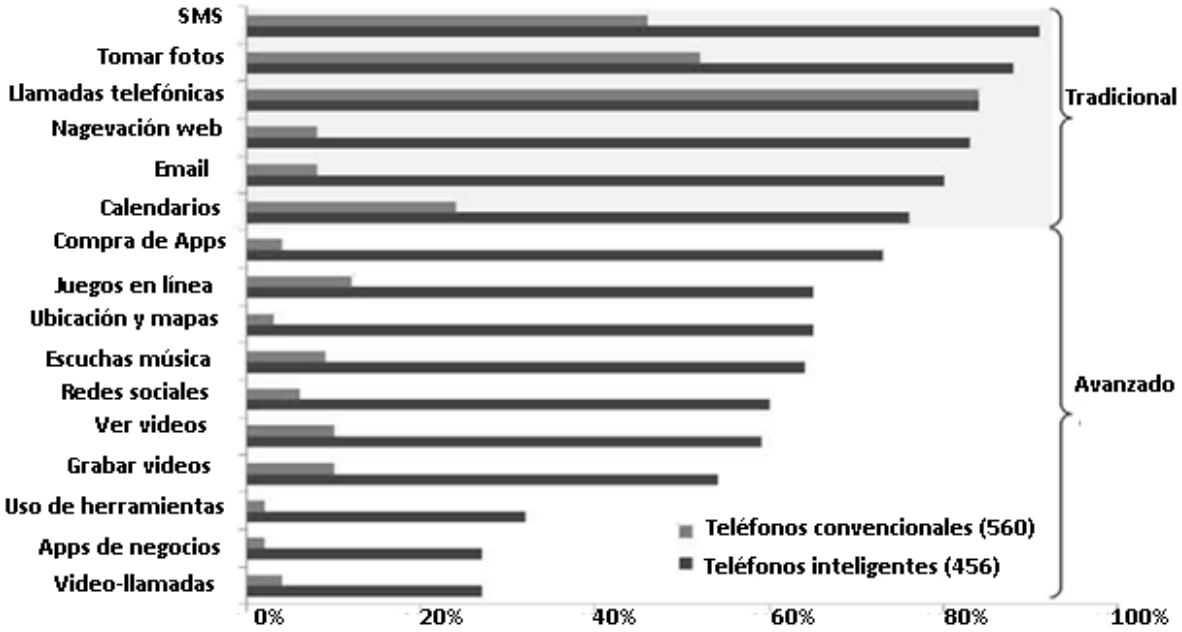



Figura 2.15 Uso de servicios en dispositivos móviles

Los casos mostrados anteriormente resultan ser factores decisivos para ofrecer el soporte de movilidad a los usuarios no obstante, para tener la capacidad de soportar servicios más demandantes se requiere de una mayor capacidad en los anchos de banda de las comunicaciones inalámbricas. Esta cuestión sin duda explica porque existe en los dispositivos inteligentes un reciente crecimiento en la adopción de la norma IEEE 802.11 [11], llegando a convertir está década en la era de dispositivos con múltiples radios. Según las estadísticas de la "Wi-Fi Alliance" las proyecciones calculadas en el crecimiento de la certificación Wi-Fi van en aumento (figura 2.16).

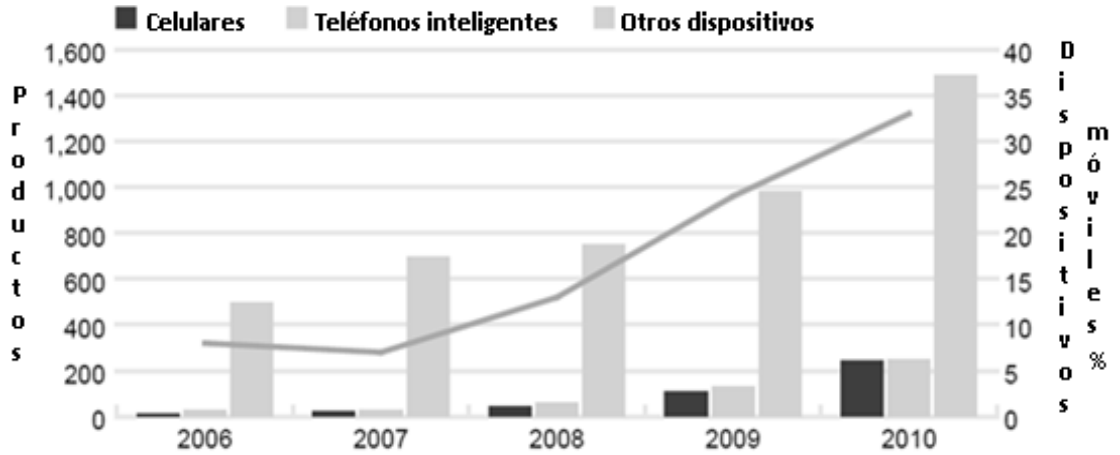



Figura 2.16 Certificación Wi-Fi en dispositivos móviles

La información tratada hasta el momento es bastante ilustrativa pues hace tan sólo unos años únicamente unos cuantos pudieron imaginar que esto pasaría y la interrogante que surge ahora es "¿Hasta dónde llegarán esta serie de eventos?". Para tener una idea de lo que se aproxima basta con observar la figura 2.17 (basada en el estudio Internet Trends de Morgan Stanley) que claramente muestra que los suscriptores móviles de banda ancha continúan creciendo, y es tal el ritmo que se estima que para el año 2014 llegarán incluso a superar al número de usuarios fijos que acceden a Internet pero, esto llega más allá porque el tráfico IP global que se genere llegará a ser de varios Exabytes por mes.

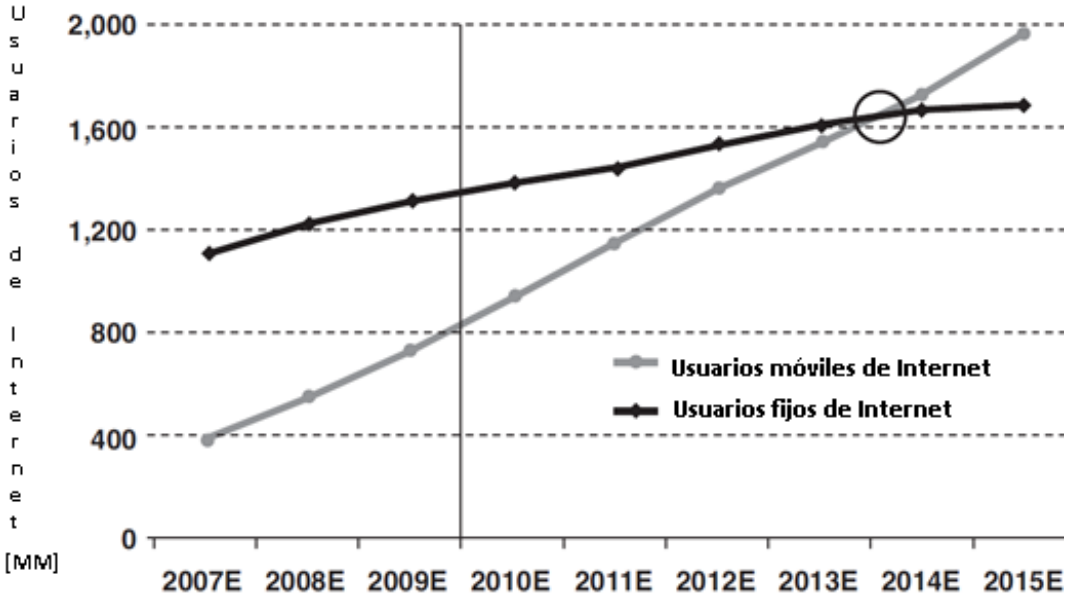



Figura 2.17 Futuro de los usuarios en Internet

Todos los elementos que hasta ahora se han descrito relatan la situación actual del mercado de la movilidad: próximamente los entornos móviles serán muy comunes en nuestras actividades diarias y poco a poco comenzarán a adquirir un valor muy significativo en una infinidad de ambientes, desde los empresariales y educativos, pasando por los profesionales, culturales y de entretenimiento. Precisamente esto lleva a pensar y valorar la importancia que tendrá brindar un soporte estable y robusto de movilidad.

# Capítulo 3

## Protocolo de Internet (IP)

*I think there is a world market for maybe five computers –Thomas Waton CEO of IBM*

## 3.1 INTRODUCCIÓN

En el mundo digital hoy en día de todas las pilas de protocolos existentes es TCP/IP la más ampliamente difundida y utilizada, sin embargo como era de esperarse con el paso de los años las tendencias en los mercados han ido cambiando, las necesidades de hoy son diferentes a las del siglo pasado y día a día surgen nuevas problemáticas y soluciones para los recientes servicios que se pretenden ofrecer. Antes que nada hay que realizar una pequeña remembranza para recordar lo que ha acontecido, iniciando con la versión 4 del protocolo de Internet (IP).

## 3.2 PROTOCOLO DE INTERNET VERSIÓN 4: IPv4

El Protocolo de Internet se localiza en la capa de red y fue desarrollado desde sus inicios para trabajar sobre redes de conmutación de paquetes. IP en su versión 4 utiliza una dirección IPv4 como un identificador único para cada nodo, es decir, un número de 32 bits es utilizado para que en cada comunicación se pueda diferenciar de forma inequívoca los nodos de origen y destino.

Frente al desarrollo y crecimiento de la Internet fue la Autoridad de Asignación de Números en Internet, IANA por sus siglas en inglés (Internet Assigned Numbers Authority) la responsable de administrar las direcciones IP; con el paso de los años debido al incremento acelerado del uso de tales direcciones se crearon Registros Regionales de Internet, RIRs por siglas en inglés (Regional Internet Registries) encargados de administrar ciertos bloques de direcciones y facilitando de esa forma, una correcta asignación y distribución de estos y otros recursos de Internet. Se muestra en la figura 3.1 el área de cobertura actual de los RIRs.


Figura 3.1 Registros Regionales de Internet [12]

Dada la trascendencia de una dirección IPv4 es importante conocer su notación y estructura: está compuesta de 32 bits que a su vez se dividen en 4 octetos separados por

un punto, cada octeto puede tomar un valor de entre 0 y 255, de manera que su valor se representa en una notación decimal o binaria, por ejemplo: 192.168.20.1 y 11000000.10101000.00010100.00000001 son equivalentes.

Para cada dirección IPv4 se identifica una parte asignada a la red, a través de la cual se conoce el segmento de red con que se está trabajando, y una parte que identifica de manera única a cada host dentro de esa red. Precisamente el uso de ambos elementos es lo que permite mantener una estructura jerárquica, fortaleciendo el orden y claridad en las comunicaciones. Se muestra en la figura 3.2 los elementos de una dirección IPv4.

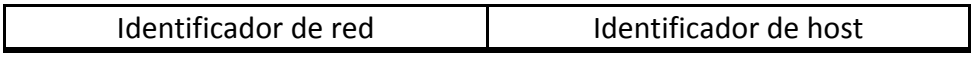



Figura 3.2.Partes de una dirección IPv4

Ahora que ya se tiene claro el concepto de una dirección IPv4 sólo resta mencionar algunas de las características representativas de IPv4:

- No confiable: no garantiza la entrega de los paquetes.
- No orientado a conexión: se transmite sin haber establecido una conexión previa.
- Independencia del medio: no importa el medio físico en que viajen los paquetes.

### 3.2.1 SITUACIÓN ACTUAL

"There is no reason for any individual to have a computer in his home", fueron las palabras de Ken Olsen fundador de la empresa Digital Equipment Corporation (DEC) en 1977. Frases como esa manifiestan lo complicado y complejo que es predecir el crecimiento y la diversidad de las aplicaciones en las redes de computadoras. Precisamente hoy en día existen varias situaciones que se presentan en torno a IPv4, algunas de las más representativas se describen en la tabla 3.1.

Tabla 3.1 Situación actual de IPv4

| Situación | Descripción |
|---|---|
| Escasez de direcciones IPv4 | El 1 de febrero de 2011 la IANA informó que asignó las últimas direcciones IPv4 disponibles a los RIRs, los cuales ahora sólo podrán administrar los bloques disponibles a su región. |
| | El crecimiento de la población usando Internet no sólo aumenta numéricamente sino también en tiempos de conexión. |
| | Los usuarios móviles utilizan cada vez más dispositivos habilitados con IP. |
| Mejorar escalabilidad y longevidad | Permitir un acceso continuo y prolongado de los actuales y futuros usuarios. |
| | Establecer un mejor direccionamiento jerárquico y una mejor |

| | |
|---|---|
| | distribución de las direcciones. |
| QoS para las nuevas aplicaciones | Se ha extendido el uso de las aplicaciones basadas en IP. |
| Se dificulta el uso de algunas aplicaciones por la existencia de NAT | Algunas aplicaciones resultan costosas, complejas y difíciles de operar con NAT (VoIP, fax IP, servidores para el hogar, etc.) |

Afortunadamente tratando de aprender de experiencias pasadas a principios de los 90s se vislumbró que habría que hacer frente a las grandes problemáticas y retos del futuro y se planteó una nueva versión de IP, misma que se trata a continuación.

## 3.3 PROTOCOLO DE INTERNET VERSIÓN 6: IPV6

A principios de 1994 frente a la gran demanda de direcciones IPv4 y vislumbrando su inminente agotamiento el Grupo de Trabajo de Ingeniería de Internet, IETF por sus siglas en inglés (Internet Engineering Task Force) [13] creó el grupo de trabajo Protocolo de Internet de Siguiente Generación, IPng por sus siglas en inglés (Internet Protocol Next Generation) para desarrollar una nueva versión del Protocolo de Internet: IPv6, por sus siglas en inglés (Internet Protocol version 6) fue el nombre que finalmente se decidió.

### 3.3.1 CARACTERÍSTICAS

En definitiva IPv6 fue pensado para anticipar varios de los próximos movimientos de la era digital, lo cual claramente se ve reflejado en algunas de sus características, entre las cuales se encuentran [14]:

I. *Direccionamiento mejorado:* permite una mejor jerarquización de los prefijos IPv6 en las tablas de ruteo, además por la gran cantidad de direcciones disponibles se puede llegar a prescindir de NAT, lo que facilita nuevamente la comunicación extremo a extremo.

i. *Encabezado simplificado:* su encabezado es más sencillo que el de IPv4 y por medio de los encabezados de extensión ofrece cierta modularidad, además ya no se realiza una desencapsulación del paquete para identificar el tipo de tráfico que contiene (existe un campo que lo define explícitamente); unir estos elementos contribuye a ahorrar tiempos de procesamiento en los dispositivos de interconexión y se mejora el rendimiento general en las comunicaciones.

ii. *Movilidad:* a través del uso de encabezados adicionales para este fin, IPv6 permite a los dispositivos habilitados con dicho protocolo disfrutar del soporte de movilidad de una manera más óptima que con IPv4.

iii. *Seguridad:* las funciones de seguridad incorporadas permiten implementar prácticas de seguridad más eficientes que muchas redes actuales necesitan. Esto se puede lograr mediante IPSec y aunque también es posible implementar este protocolo de seguridad en IPv4, la diferencia radica en que para IPv4 es opcional y un agregado.

iv. *Mecanismos de transición:* dada la complejidad que resulta llevar a cabo la migración de IPv4 a IPv6 existen una serie de mecanismos de transición que permitirán que gradualmente exista una convivencia de ambas hasta llegar a una adopción dominante de IPv6. Estos mecanismos incluyen: Pila doble, Encapsulación (6to4, Teredo, 6in4) y traductores.

### 3.3.2 ENCABEZADO PRINCIPAL

Muchas de las características propias de IPv6 antes mencionadas se comprenden mejor cuando se observa su encabezado respectivo (figura 3.3).

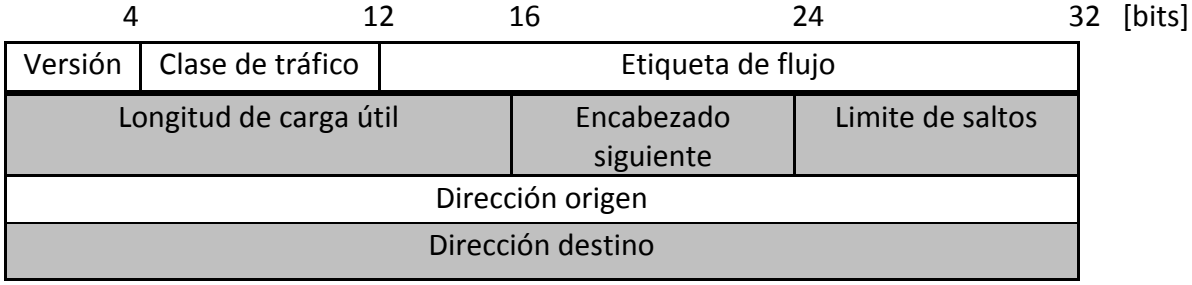



Figura 3.3 Encabezado principal de IPv6

El encabezado de IPv6 tiene un tamaño fijo de 40 bytes y se encuentra compuesto de un total de 8 campos, mismos que se describen en la tabla 3.2.

Tabla 3.2 Campos del encabezado principal de IPv6

| Nombre del campo | Longitud [bits] | Descripción |
|---|---|---|
| Versión | 4 | Específica la versión del protocolo, en este caso es 6. |
| Clase de Tráfico | 8 | Remplaza al tipo de servicio del encabezado IPv4. Usa el método de Servicios Diferenciados para distinguir e identificar las diferentes clases o prioridades de los paquetes. |
| Etiqueta de Flujo | 20 | Permite realizar un procesamiento más eficiente al identificar los paquetes que pertenecen a determinado flujo de datos para proporcionarles el mismo trato. |
| Longitud de Carga Útil | 16 | Especifica la longitud de la carga del paquete (todo aquello que se encuentra después del encabezado principal de IPv6). |
| Encabezado | 8 | Identifica el encabezado que sigue inmediatamente al |

| | | |
|---|---|---|
| Siguiente | | encabezado IPv6. |
| Limite de Saltos | 8 | Determina el número máximo de saltos que un paquete puede realizar en la red para llegar a su destino final antes de ser descartado. |
| Dirección Origen | 128 | Identifica el dispositivo o la interfaz del nodo que generó el paquete. |
| Dirección Destino | 128 | Identifica el dispositivo o la interfaz del nodo al que está dirigido el paquete. |

### 3.3.3 ENCABEZADOS DE EXTENSIÓN

Se mencionó con anterioridad que para reducir el tiempo de procesamiento de un paquete IPv6 se decidió mantener el encabezo principal de IPv6 lo más simple posible y para conseguir esto se optó por crear extensiones que se agregaran sólo cuando se necesitara hacer uso de tales.

Propiamente cada uno de estos encabezados de extensión es colocado entre el encabezado principal de IPv6 y el encabezado de la capa superior, para ello es necesario asignarle a cada encabezado de extensión un identificador único a fin de que puedan ser diferenciados correctamente. Es importante además que estos encabezados se agreguen bajo un orden específico, tal como se aprecia en la tabla 3.3.

Tabla 3.3 Encabezados de Extensión de IPv6 [15]

| Orden | Tipo de encabezado | Código asociado |
|---|---|---|
| 1 | Encabezado Principal de IPv6 | - |
| 2 | Salto a Salto | 0 |
| 3 | Opciones de destino (con opciones de enrutamiento) | 60 |
| 4 | Enrutamiento | 43 |
| 5 | Fragmentación | 44 |
| 6 | Autenticación | 51 |
| 7 | Encapsulamiento de Seguridad de la Carga | 50 |
| 8 | Opciones de Destino | 60 |
| 9 | Protocolo de capa superior (TCP, UDP, ICMPv6) | (6,17,58) |
| - | Movilidad | 135 |
| - | Sin Siguiente Encabezado | 59 |

Cada uno de los encabezados anteriores provee información específica que generalmente es usada por dispositivos de interconexión y por los nodos finales para decidir como procesar cada paquete IPv6, por ejemplo todos los encabezados anteriores (con excepción del de Salto a Salto) no son examinados por los nodos que existen en la ruta que siguen los paquetes, sino que únicamente son procesados por el destinatario final.

### 3.3.4 DIRECCIONES IPV6

Ya se han descrito los aspectos representativos de IPv6 por lo que ahora es posible detallar las características más importantes de sus respectivas direcciones: están compuestas de 8 grupos separados por dos puntos, cada grupo formado por 4 números hexadecimales (cada número es representado a través de 16 bits), lo que da un total de 128 bits para cada dirección, es decir, el número total de direcciones IPv6 es $2^{128}$ lo cual es equivalente a 340,282,366,920,938,463,463,374,607,431,768,211,456 direcciones; definitivamente es una cifra asombrosa y por el momento son más que suficientes.

#### 3.3.4.1 FORMATO

Similar a lo que ocurre en IPv4 para una dirección IPv6 se encuentran 2 partes: un identificador de red y un identificador de interfaz, cada uno de los cuales está constituido por 64 bits, permitiendo de esta forma que las tablas de ruteo sean más pequeñas y se obtenga un mejor rendimiento en las tareas de enrutamiento, por ejemplo para la siguiente dirección IPv6 su identificador de red y de interfaz correspondientes son:

Dirección IPv6 = 2001:0db8:3c4d:0015:0000:0000:abcd:ef14
Identificador de red = 2001:0db8:3c4d:0015
Identificador de interfaz: 0000:0000:abcd:ef14

Para manejar direcciones tan bastas es posible hacer uso de prefijos equivalentes a la mascara de red de IPv4, a través de los cuales se puede expresar el bloque de red, por ejemplo (con base en la dirección IPv6 anterior) 2001:0db8:3c4d::/48 hace referencia al prefijo de red manejado. Existen adicionalmente ciertas facilidades ofrecidas al momento de expresar estas direcciones (véase el RFC 5952), de tal forma que en ocasiones es posible encontrarlas bajo una notación más corta. A continuación se presentan algunos de los casos en que esto es posible:

a) Los ceros iniciales de cada bloque son opcionales.

| | | |
|---|---|---|
| Dirección IPv6 original | --> | 2001:0db8:3c4d:0015:0000:0000:abcd:ef14 |
| Dirección IPv6 simplificada | --> | 2001:db8:3c4d:15:0:0:abcd:ef14 |

b) Una serie consecutiva de bloques de ceros puede ser expresada con doble dos puntos "::" pero, esta abreviación sólo puede utilizarse una vez por dirección.

| | | |
|---|---|---|
| Dirección IPv6 original | --> | 2001:0db8:3c4d:0015:0000:0000:abcd:ef14 |
| Dirección IPv6 simplificada | --> | 2001:0db8:3c4d:0015::abcd:ef14 |

Al mismo tiempo se puede llevar a cabo una combinación de las opciones anteriores:

Dirección IPv6 original --> 2001:0db8:3c4d:0015:0000:0000:abcd:ef14
Dirección IPv6 simplificada --> 2001:db8:3c4d:15::abcd:ef14

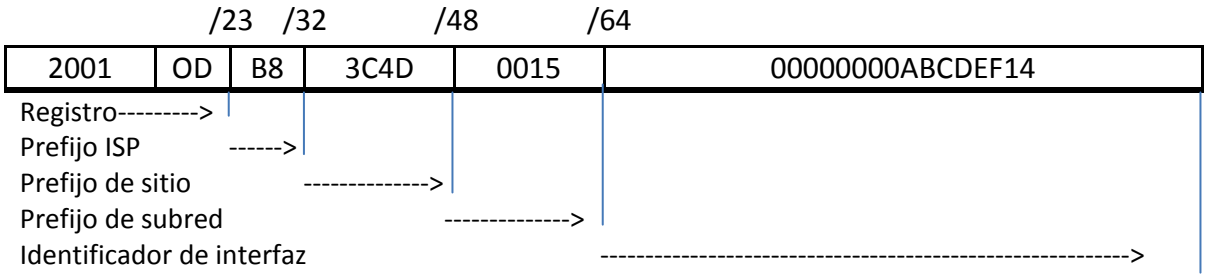
c) Una dirección no especificada se escribe "::"

Dirección IPv6 original --> 0000:0000:0000:0000:0000:0000:0000:0000
Dirección IPv6 simplificada --> ::

Todos los dispositivos que soportan IPv6 reconocen los casos anteriores y son capaces de pasar de una dirección simplificada a su forma original, lo único que hacen es identificar la cantidad de ceros faltantes separando las 2 partes de la dirección y añadiendo ceros hasta completar los 128 bits.

### 3.3.4.2 ÁMBITOS DE ACCIÓN

Anteriormente se mencionó que una dirección IPv6 está compuesta de un identificador de red y un identificador de interfaz sin embargo, existen otros identificadores más específicos mediante los cuales se obtiene información más detallada, a continuación se muestran estos elementos en la figura 3.4.




Considerando lo anterior habrá que indicar que una dirección IPv6 es definida para tener un alcance particular, existiendo una serie de ámbitos que a continuación se describen:

1) *Enlace local:* hace referencia a un enlace físico en particular e identifica una interfaz en un segmento de red, por lo que se usan sólo para comunicaciones desarrolladas en un enlace (configuración automática de direcciones, detección de vecinos y ruteadores, etc.), es decir, cuando se envía algún paquete a otro enlace no se puede usar una dirección de enlace local como origen.

   El rango designado por la IANA define en el RFC 4291 que las direcciones comienzan con: FE8, FE9, FEA, FEB, pudiendo abreviarse como FE80::/64. Se observa su representación en la figura 3.5.

| 1111111010 | 0 | ID interfaz (64 bits) |
|---|---|---|

Figura 3.5 Formato de una dirección de enlace local

2) *Unicast global:* paquetes con una dirección (de origen o destino) dentro de este rango pueden ser enviados a través de Internet. Normalmente se componen de un prefijo de enrutamiento de 48 bits y un ID de subred de 16 bits.

   La asignación de la IANA define en el RFC 3587 que el rango a utilizar se ubica dentro del prefijo 2000::/3, lo que a su vez representa una octava parte del total de direcciones IPv6. En la figura 3.6 se aprecia este caso.

| 001 | Prefijo Global de enrutamiento | ID subred | ID interfaz |
|---|---|---|---|
| 3 bits | (45 bits) | (16 bits) | (64 bits) |

Figura 3.6 Formato de una dirección unicast global

3) *Única local:* la IANA designó a este ámbito el rango comprendido en FC00::/7 y aunque prácticamente son únicas, no son enrutables en Internet, paquetes con una dirección (de origen o destino) dentro de este rango son similares a las direcciones privadas de IPv4.

   Estas direcciones más bien son utilizadas en comunicaciones locales ya sea dentro de un mismo sitio o incluso entre un conjunto de éstos, de esa manera cuando 2 segmentos de red con esas direcciones se unen no existen conflictos en las direcciones en ninguno de los nodos; precisamente por esta razón es posible que dentro de un sitio se lleguen a encontrar varios prefijos de este tipo de direcciones. Se presenta en la figura 3.7 la representación de este ámbito (para más detalles remítase al RFC 4193).

| Prefijo | L | ID global | ID subred | ID interfaz |
|---|---|---|---|---|
| 7 bits | 1 | 40 bits | 16 bits | 64 bits |

Figura 3.7 Formato de una dirección única local

Donde:
Prefijo: el prefijo FC00::/7 identifica a una dirección IPv6 unicast local.
L: activado indica que puede ser definido en el fututo, desactivado denuncia que el prefijo es asignado localmente.
ID global: es creado de manera pseudo-aleatoria, siendo utilizado en la formación de un prefijo único global.
ID subred: identificador asignado a la subred de un determinado sitio.
ID interfaz: identificador de una interfaz en un enlace.

Sitio local: se definió originalmente dentro del prefijo de red FECO::/10 no obstante, desde 2004 ya no deben usarse porque dentro de una organización pueden existir prefijos de direcciones duplicados, situación que agrega complejidad y ambigüedad a las comunicaciones.

### 3.3.4.3 TIPOS

Para IPv4 los diferentes tipos de direcciones que se manejan suelen ser unicast, broadcast y multicast sin embargo, para IPv6 existen ciertas particularidades que es necesario mencionar, por ejemplo ya no existen direcciones broadcast. Se definen a continuación los diferentes tipos de direcciones IPv6 que existen [14]:

a. *Unicast:* dirección que identifica de manera única a un dispositivo o diferencia a sus interfaces, es decir, estas direcciones normalmente son las más utilizadas y es posible encontrar tanto direcciones locales como globales.

b. *Anycast:* representa a un identificador de un conjunto de interfaces, mismas que generalmente pertenecen a diferentes nodos por lo tanto, al momento de enviar un paquete destinado a este tipo de dirección el paquete es entregado únicamente a la interfaz más cercana (usualmente basada en métricas de protocolos de enrutamiento) configurada con esa dirección. Habrá que aclarar que no se puede usar una dirección anycast como dirección de origen de ningún paquete y tampoco se debe asignarla a ningún cliente, sino que solamente se utiliza en los ruteadores.

   Estas direcciones pueden tener un ámbito de sitio y de enlace local o global, además ya que no poseen un rango propio de direcciones, comparten el mismo espacio asignado a las direcciones unicast; por esta razón no es posible hacer una distinción entre ambas. Existe por tanto, para cada subred una dirección anycast: "dirección anycast del ruteador de la subred" caracterizada porque los bits menos significativos (64 o más) son cero, tal y como se aprecia en la figura 3.8.


Figura 3.8 Formato de una dirección anycast del ruteador de la subred

c. *Multicast:* este tipo de dirección se define en el RFC 2375 y es similar a las direcciones anycast puesto que identifica a un conjunto de interfaces (usualmente asociados a diferentes nodos) no obstante, un paquete enviado a este tipo de dirección es entregado a todas las interfaces asociadas a un grupo multicast. En la figura 3.9 se ilustra su representación.

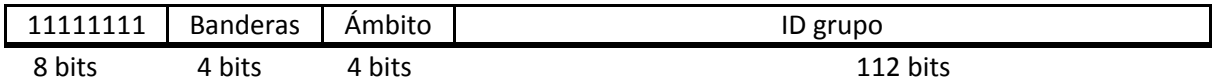



Figura 3.9 Formato de una dirección multicast en IPv6

Donde las
Banderas:0PRT

P: activado indica que la dirección multicast se construyó con base a un prefijo de red, desactivado indica que no ha sido asignada con base a un prefijo de red.
R: activado indica que la dirección multicast incorpora la dirección del Rendezvous Point (RP) del grupo, desactivado no incorpora tal dirección.
T: activado indica que es una dirección temporal, desactivado indica que la dirección ha sido asignada por la IANA.
Ámbito: limita el alcance del grupo multicast:

0. Reservado 1. Interfaz local 2. Enlace local 5. Administración local
6. Sitio local 8. Organización local E. Global

El resto está reservado o no asignado

Finalmente la tabla 3.4 muestra algunas direcciones multicast reservadas.

Tabla 3.4 Direcciones multicast reservadas en IPv6 [15]

| Dirección IPv6 | Ámbito | Grupo multicast |
|---|---|---|
| FF01::1 | Nodo local | Todos los nodos |
| FF01::2 | | Todos los ruteadores |
| FF02::1 | Enlace local | Todos los nodos |
| FF02::2 | | Todos los ruteadores |
| FF02::5 | | OSPF-Todos los ruteadores (excepto DR) |
| FF02::6 | | OSPF-Ruteador Designado (DR) |
| FF02::9 | | RIP-Ruteadores |
| FF02::A | | EIGRP-Ruteadores |
| FF02::B | | Agentes de movilidad |
| FF02::D | | PIM-Ruteadores |

d. *Loopback:* de manera similar que en IPv4, se utiliza esta dirección para hacer pruebas, es decir, los paquetes que son enviados a la dirección ::1 son dirigidos al dispositivo emisor. La diferencia radica en que no existe todo un bloque designado para esta función sino que solamente se definió una única dirección Loopback.

#### 3.3.4.4 FORMAS DE CONFIGURACIÓN

Una importante característica introducida en IPv6 es la capacidad que tienen los nodos de auto-configurarse, condición que permite que no se tenga una dependencia de otros dispositivos para obtener una configuración válida. Existen principalmente 2 formas de realizar esta tarea e inclusive se pueden usar ambas simultáneamente:

i) *Autoconfiguración sin estado (stateless):* no se requiere ninguna configuración manual en los hosts pero, si en el ruteador (sin que exista una intervención de un servidor dedicado), es decir, el host genera una dirección en base a su información local y a los datos que obtiene de un ruteador. Este mecanismo se define en el RFC 4862 [16] y de manera general el proceso involucrado es el siguiente:

a) El host crea el identificador de su interfaz mediante diversas formas, tales como: EUI-64, generación pseudo-aleatoria, etc.

   Paralelamente el host puede enviar un mensaje de Solicitud de Ruteador dentro de su enlace local a la dirección del grupo multicast FF02::2

b) El host crea una dirección de enlace local.

c) El host lleva a cabo el proceso DAD para la dirección de enlace local.

d) El ruteador recibe el mensaje Solicitud de Ruteador (enviado anteriormente) y manda como respuesta un mensaje unicast de Anuncio de Ruteador con información del prefijo del segmento de red.

e) El host agrega el prefijo a su dirección de enlace local (construida en el paso b) y forma una dirección unicast global.

f) Opcionalmente el nodo puede llevar a cabo el proceso DAD para su nueva dirección global (depende de la implementación).

Debido a su gran uso a continuación se presenta un ejemplo de EUI-64: se basa en la dirección MAC del host, en la figura 3.10 se muestra un ejemplo.

| 34 | 90 | 27 | 17 | FC | 0F |
|---|---|---|---|---|---|

Figura 3.10 Ejemplo de dirección MAC

Este método utiliza la dirección MAC (48 bits) para formar el identificador de interfaz no obstante, para completar los 64 bits hace uso de 16 bits extras (FFFE) que son insertados en medio de la dirección MAC. La dirección EUI-64 se muestra en la figura 3.11.

| 34 | 90 | 27 | **FF** | **FE** | 17 | FC | 0F |
|---|---|---|---|---|---|---|---|

Figura 3.11 Dirección EUI-64

Posteriormente para asegurarse de que la dirección creada es única en los 8 bits más significativos de la dirección MAC se cambia el bit universal/local, siendo colocado de 0 (ámbito local) a 1 (ámbito global), quedando como se aprecia en la figura 3.12.

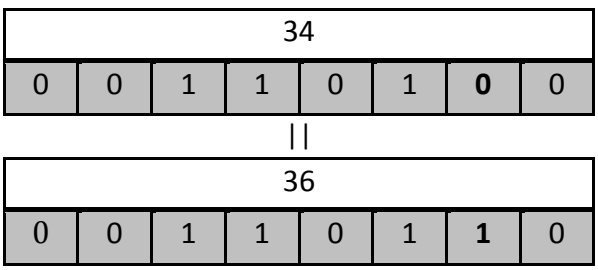



Figura 3.12 Cambio de bit universal/local de la dirección MAC

Por último se muestra en la figura 3.13 el identificador de interfaz definitivo:

| 36 | 90 | 27 | FF | FE | 17 | FC | 0F |
|---|---|---|---|---|---|---|---|

Figura 3.13 Identificador de interfaz resultante en EUI-64

ii) *Autoconfiguración con estado (stateful):* la configuración de cada nodo depende de la existencia de un servidor (por ejemplo un servidor DCHPv6) para obtener la dirección para su interfaz y otros parámetros adicionales que se hayan configurado en dicho servidor; este método resulta una buena opción cuando se desea mantener un mejor control y una administración centralizada.

### 3.3.5 PROTOCOLO DE DESCUBRIMIENTO DE VECINOS (ND)

Otros de los ejes centrales en IPv6 es el Descubrimiento de Vecinos, ND por sus siglas en inglés (Neighbor Discovery), este protocolo se encuentra definido en el RFC 4861 [17] y su funcionamiento depende del intercambio de mensajes ICMPv6. Haciendo una analogía con IPv4 se puede decir que comprende las funcionalidades de ICMPv4 y ARP.

En ND existen varios mensajes que permiten obtener ciertos parámetros de configuración y conocer los estados y las relaciones existentes entre vecinos, definiendo un vecino como un ruteador o cualquier otro host pero, todos conectados en el mismo segmento de red. Principalmente se reconocen 2 tipos de mensajes, aquellos que se desarrollan entre un host y un ruteador, y aquellos que únicamente implican hosts. Ambas comunicaciones se muestran en la figura 3.14.

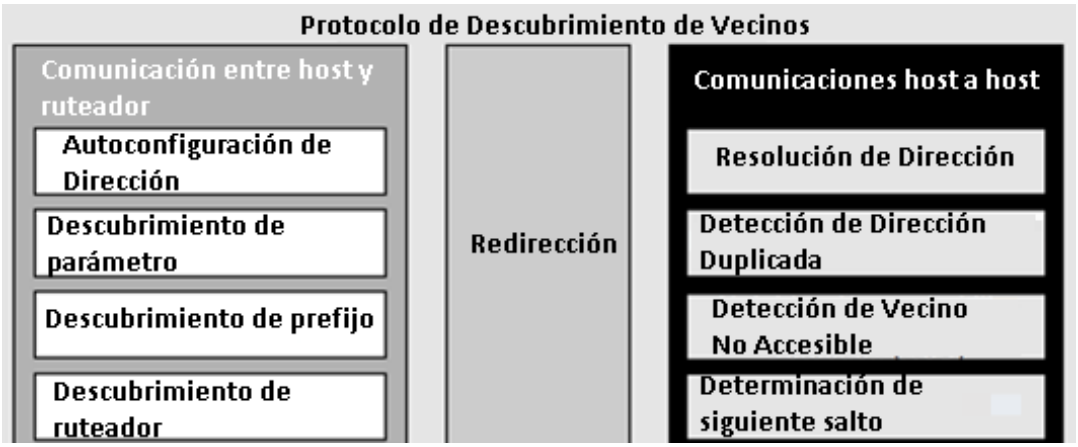



Figura 3.14 Mensajes de Descubrimiento de Vecinos

Para comprender mejor la utilidad de ND habrá que describir las funcionalidades implicadas en las comunicaciones entre un host y un ruteador:

- *Descubrimiento de Ruteador*, RD por sus siglas en inglés (Router Discovery): permite a un host conocer de su enlace local los ruteadores disponibles existentes.

Para lograr sus fines RD utiliza los siguientes mensajes:

- Solicitud de Ruteador, RS por sus siglas en inglés (Router Solicitation): usado para solicitar anuncios de los ruteadores disponibles del segmento de red o en casos donde el mensaje de Anuncio de Ruteador que el host haya recibido no contenga toda la información que requiera conocer. El mensaje ICMPv6 correspondiente (figura 3.15) se envía a la dirección multicast FF02::2

| Tipo | Código | Suma de comprobación |
|---|---|---|
| Reservado | | |
| Opciones … | | |

Figura 3.15 Encabezado de Solicitud de Ruteador

Donde:
Tipo: 133
Código: 0
Suma de comprobación: verifica que no existan errores en el mensaje ICMPv6.
Reservado (32 bits): reservado para uso futuro.
Opciones: dirección MAC origen.

- Anuncio de Ruteador, RA por sus siglas en inglés (Router Advertisement): mensaje de respuesta que cada ruteador envía a la dirección IPv6 del host que lo haya solicitado (en caso de que posea una dirección válida) o en su defecto el ruteador envía este mensaje pseudo-periódicamente (evitando una inundación de estos mensajes) a la dirección multicast FF02::1 para brindar la información que los hosts usualmente necesitan para unirse al segmento de red correspondiente. En aquellos casos donde el mensaje RA sobrepase el MTU del enlace, el ruteador podrá enviar varios mensajes de RA, cada uno conteniendo un subconjunto de la información a anunciar.

  Es importante cuidar que exista un equilibrio entre los tiempos de envío de estos mensajes de tal forma que se generen lo suficientemente frecuente para que los hosts noten su presencia pero, sin que sean tan reiterativos como para que los hosts asuman la ausencia de estos mensajes como un indicador de que ha ocurrido una falla en el ruteador. Se muestra en la figura 3.16 el encabezado del mensaje ICMPv6 utilizado.

| Tipo | Código | | | Suma de comprobación |
|---|---|---|---|---|
| Limite de saltos | M | O | Reservado | Tiempo de vida del Ruteador |
| Tiempo de validez | | | | |
| Temporizador de retransmisión | | | | |
| Opciones… | | | | |

Figura 3.16 Encabezado de Anuncio de Ruteador

Donde:
Tipo: 134
Código: 0
Suma de comprobación: verifica que no existan errores en el mensaje ICMPv6.
Limite de saltos (8 bits): valor que indica el número de saltos permitidos para los mensajes.
M (1 bit): bandera que informa que puede usarse un servidor DHCP para proveer direcciones en el segmento de red.
O (1 bit): bandera que informa que servidor DCHP provee información de configuración adicional.
Reservado (32 bits): reservado para uso futuro.
Tiempo de vida del Ruteador (16 bits): indica el tiempo de vida (en segundos) de la información.
Tiempo de validez (32 bits): tiempo en milisegundos en que los nodos asumen que cierto vecino se encuentra alcanzable.
Opciones: información adicional (MTU, prefijos, dirección de MAC origen).
Temporizador de retransmisión (32 bits): tiempo en milisegundos entre la retransmisión de los mensajes de Solicitud de Vecino.

Los mensajes RA proveen valiosa información a los hosts permitiéndoles conocer los parámetros para conectarse correctamente al segmento de red, específicamente los datos que el ruteador anuncia permiten llevar a cabo lo siguiente:

- *Autoconfiguración de Dirección:* utilizada en la configuración sin estado, permite a un host obtener su propia dirección IPv6 sin usar algún dispositivo dedicado.

- *Descubrimiento de Parámetro*, PD por sus siglas en inglés (Parameter Discovery): los hosts pueden descubrir algunos parámetros adicionales del enlace local, por ejemplo la MTU, el límite de saltos predeterminados para los paquetes, etc.

- *Descubrimiento de Prefijo*, por sus siglas en inglés (Prefix Discovery): permite a un host descubrir los prefijos de red que existen en el segmento de red donde se encuentra, esta información le sirve para auto-configurarse y conocer los rangos de las direcciones IPv6 que pueden ser asignados a sus vecinos. El encabezado del mensaje ICMPv6 se presenta en la figura 3.17.

| Tipo | Longitud | Longitud del prefijo | L | A | Reservado 1 |
|---|---|---|---|---|---|
| Tiempo de vida válido | | | | | |
| Tiempo de vida preferido | | | | | |
| Reservado 2 | | | | | |
| Prefijo | | | | | |

Figura 3.17 Encabezado de Información de Prefijo

Donde:
Tipo (8 bits): corresponde al número 3
Longitud (8 bits): 4
Longitud de prefijo (8 bits): longitud en bits para un prefijo válido.
L (1 bit): se puede usar el prefijo para determinar el enlace.
A (1 bit): el prefijo puede ser usado para una configuración de dirección autónoma.

Reservado 1 (6 bits): reservado para uso futuro.
Tiempo de vida válido (32 bits): indica el tiempo de validez del prefijo.
Tiempo de vida preferido (32 bits): indica el tiempo de preferencia de las direcciones obtenidas a través de stateless.
Reservado 2 (32 bits): reservado para uso futuro.
Prefijo: prefijo del segmento de red.

También es posible ubicar en ND una función denominada redirección.

- *Redirección:* es el proceso a través del cual un ruteador analiza la ruta asignada a un paquete e informa al host origen que existe una mejor ruta disponible a ese destino en particular, para llevar esto acabo el ruteador crea un mensaje ICMPv6 informando de esta situación a fin de que los futuros paquetes que pertenezcan a esa misma conexión cambien la ruta por la que viajarán. A continuación se observa en la figura 3.18 el encabezado del mensaje ICMPv6.

| Tipo | Código | Suma de comprobación |
|---|---|---|
| Reservado | | |
| Dirección objetivo | | |
| Dirección destino | | |
| Opciones … | | |

Figura 3.18 Encabezado de Redirección

Donde:
Tipo: 137
Código: 0
Suma de comprobación: verifica que no existan errores en el mensaje ICMPv6.
Reservado (29 bits): reservado para uso futuro.
Dirección objetivo (128 bits): dirección IPv6 asociada a una mejor ruta.
Dirección destino (128 bits): dirección IPv6 redirigida al nodo asociado a la dirección IPv6 objetivo.
Opciones: incluye la dirección MAC del dispositivo con una mejor ruta, etc.

Finalmente se describen las comunicaciones desarrolladas entre hosts que pertenecen a un mismo segmento de red, los mensajes que se utilizan son:

- *Solicitud de Vecino*, NS por sus siglas en inglés (Neighbor Solicitation): mensaje utilizado por un host para solicitar la dirección MAC de un vecino, o para verificar si cierto vecino aún es alcanzable (figura 3.19).

| Tipo | Código | Suma de comprobación |
|---|---|---|
| Reservado | | |
| Dirección objetivo | | |
| Opciones … | | |

Figura 3.19 Encabezado de Solicitud de Vecino

Donde:
Tipo: 135

Código: 0
Suma de comprobación: verifica que no existan errores en el mensaje ICMPv6.
Reservado (32 bits): reservado para uso futuro.
Dirección objetivo (128 bits): dirección IPv6 objetivo de la solicitud (no debe ser una dirección multicast).
Opciones: información extra (dirección MAC origen).

- *Anuncio de Vecino*, NA por sus siglas en inglés (Neighbor Advertisement): mensaje no confiable enviado en respuesta a un mensaje NS recibido aunque, también se transmite sin haber sido solicitado cuando algún host desea propagar rápidamente nueva información acerca de sí mismo, por ejemplo para anunciar algún cambio en su dirección MAC. En la figura 3.20 se observa claramente el encabezado.

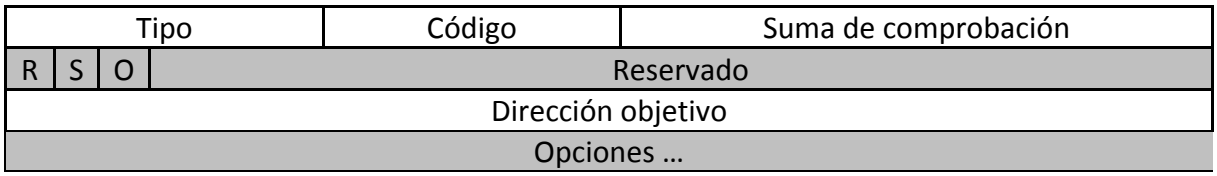



Figura 3.20 Encabezado de Anuncio de Vecino

Donde:
Tipo: 136
Código: 0
Suma de comprobación (32 bits): verifica que no existan errores en el mensaje ICMPv6.
R (1 bit): indica que el emisor es un ruteador y se utiliza en NUD (se explica más adelante) para detectar cuando algún nodo actúa como ruteador.
S (1 bit): señala que el mensaje se envía como respuesta a un mensaje NS.
O (1 bit): denota que el contenido del mensaje debe sobrescribir a la entrada existente en la cache del host a quien vaya dirigido este mensaje.
Reservado (32 bits): reservado para uso futuro.
Dirección objetivo (128 bits): dirección IPv6 objetivo (no debe ser una dirección multicast).
Opciones: información extra (dirección MAC de origen, etc.)

Principalmente los mensajes anteriores suelen utilizarse para llevar a cabo las siguientes actividades:

- *Resolución de Dirección*: proceso a través del cual un nodo determina la dirección MAC de un vecino del cual únicamente conoce su dirección IPv6 (debe realizarse entre hosts que pertenecen al mismo segmento de red).

  El host interesado en resolver la dirección generalmente tiene paquetes destinados a ese vecino ante lo cual envía un mensaje multicast NS, mientras espera a que el vecino correspondiente responda debe almacenar los paquetes que reciba o que vaya a enviar hasta que haya completado la resolución de la dirección buscada o al menos tanto como sea posible (dependiendo de su capacidad de

almacenamiento). De esta forma cuando el vecino le haya proporcionado su dirección MAC podrá enviarle todos los paquetes que tenga almacenados.

- *Detección de Dirección Duplicada*, DAD por sus siglas en inglés (Duplicate Address Detection): antes de que cualquier host asigne una dirección (local o global) a su interfaz debe hacer uso de este mecanismo para verificar que esa dirección tentativa no está siendo utilizada por otro host, en cuyo caso dicha dirección se convierte en válida aunque, en caso contrario se necesitará de una intervención manual. Existen 3 escenarios posibles en el uso de DAD que definirán si la dirección puede o no emplearse por un host:

  1) Otro host está realizando de manera simultánea este mismo proceso para la misma dirección IPv6.

  2) Otro host responde con un mensaje NA lo que significa que ya no es posible utilizar dicha dirección.

  3) Después de determinado tiempo de no recibir ninguna respuesta (NA) la dirección tentativa es considerada única en el segmento de red y se convierte en una dirección válida.

- *Detección de No Accesibilidad de Vecino*, NUD por sus siglas en inglés (Neighbor Unreachability Detection): existen 2 maneras de detectar si hay una falla en un vecino o en la ruta que se sigue para llegar a éste, ya sea que se empleen mensajes unicast NS o mediante el uso de protocolos de capa superior.

  Particularmente cuando el vecino es un ruteador se dice que es alcanzable si puede procesar correctamente en la capa de red los paquetes que recibe y es capaz de renviarlos por la interfaz respectiva, mientras que si el vecino es un host el que sea alcanzable únicamente se limita a que pueda procesar correctamente los paquetes que reciba.

  Cada vecino almacena información acerca de sus demás vecinos para optimizar las comunicaciones, por ejemplo: direcciones IPv6 y MAC, estado de accesibilidad, y especialmente en éste último se encuentran los siguientes estados [17]:

  - Incompleto: aún no concluido la resolución de dirección, es decir, se ha enviado un mensaje NS pero, todavía no se obtiene la dirección MAC correspondiente por lo que se está en espera del mensaje NA.

  - Accesible: se sabe que el vecino ha estado accesible recientemente (hace tan sólo unos segundos).

- Retraso: se asume que el vecino no es alcanzable porque no se ha recibido una confirmación que así lo corrobore pero, un paquete ha sido enviado recientemente; a pesar del posible retraso de accesibilidad se da cierto tiempo adicional para que los protocolos de capa superior confirmen la accesibilidad de dicho vecino.

- No efectivo (Stale): no se ha recibido recientemente una confirmación de accesibilidad de cierto vecino pero, no se tiene planes de verificar su estado actual hasta que se tenga tráfico destinado a éste.

- Examinar: se sabe que el vecino no es alcanzable por lo que se envía una serie de mensajes unicast NS para determinar si ha cambiado su situación.

*Determinación del Siguiente Salto:* cuando un host necesita enviar información a una determinada dirección destino esta función permite al host origen conocer la dirección del vecino (siguiente salto) al que enviará el primer paquete. Para el correcto funcionamiento de ND además del intercambio de mensajes que se presentan también es necesario hacer uso de varias estructuras de datos, pues en éstas se almacena temporalmente la información de los distintos mensajes ND recibidos, tal como se observa en la tabla 3.5

Tabla 3.5 Estructuras de datos en ND [17]

| Estructura de Datos | Descripción |
|---|---|
| Cache de Vecinos | Contiene una lista de vecinos con los que se ha tenido comunicación reciente. La información incluye las direcciones MAC e IPv6, una indicación de si es un ruteador o un host, estado de accesibilidad, etc. |
| Cache de Destinos | Contiene entradas asociadas a los destinos con los que se ha intercambiado tráfico recientemente. |
| Lista de Prefijos | Enlista el conjunto de prefijos que se anuncian en el segmento de red local y sus respectivos tiempos de validez. Esta información se extrae de los mensajes RA recibidos. |
| Lista de Ruteadores por defecto | Define una lista de ruteadores a los cuales pueden ser enviados los paquetes cuando el destinatario no se encuentra en el segmento de red local. |

El host origen verifica la lista de prefijos para determinar si la dirección se encuentra en el mismo segmento de red, en cuyo caso podrá enviar el paquete directamente al destino, de lo contrario deberá enviarlo al ruteador default (en ambos casos debe conocerse la dirección MAC asociada del siguiente salto). Para todos los paquetes posteriores enviados al mismo destino en particular el host simplemente tendrá que consultar su cache de destinos, ahorrando tiempo al no tener que enviar mensajes innecesarios.

Una vez descritas las funcionalidades anteriores se procede a ilustrar de una manera más clara (figura 3.21) las interacciones que existen entre un ruteador y un host haciendo uso de los mensajes implicados en ND, se tomará como ejemplo la autoconfiguración de un host que pretende enviar paquetes a uno de sus vecinos.

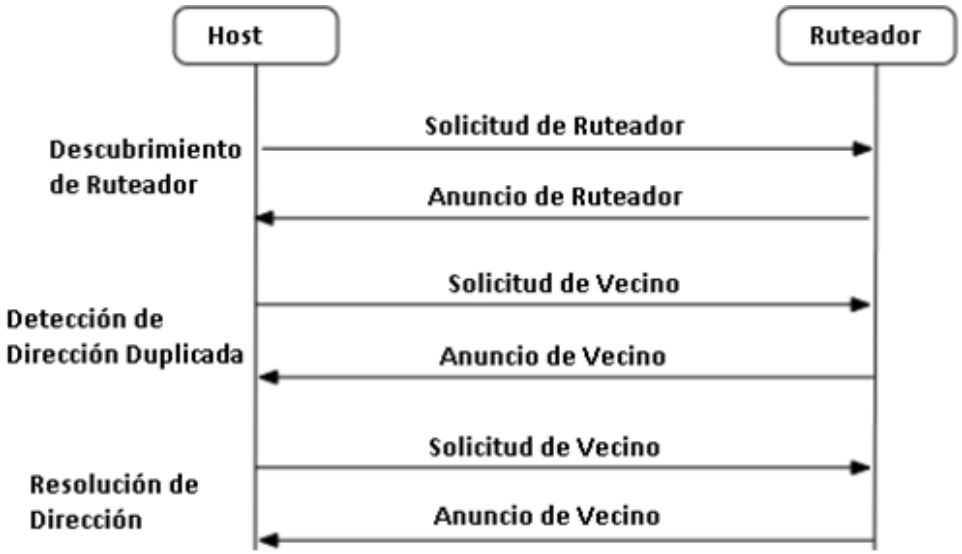



Figura 3.21 Interacción host/ruteador en ND

## 3.4 PROTOCOLO DE INTERNET DE MENSAJES DE CONTROL VERSIÓN 6 (ICMPV6)

IPv6 además de trabajar con ND también está estrechamente relacionado con el Protocolo de Internet de Mensajes de Control versión 6, ICMPv6 por sus siglas en inglés (Internet Control Message Protocol version 6), protocolo que se encuentra definido en el RFC 4443 [18]. ICMPv6 es una parte fundamental de IPv6 ya que además de ser el encargado de proporcionar mensajes cuando los paquetes no pueden ser procesados correctamente también informa sobre el estado actual de las comunicaciones en la red.

Tabla 3.6 Diferencias entre ICMPv4 e ICMPv6

| Tipo de Mensaje ICMP | ICMPv4 | ICMPv6 |
|---|---|---|
| Verificación de conectividad | ✓ | ✓ |
| Mensajes de información/error | ✓ | ✓ |
| Notificación de fragmentación | ✓ | ✓ |
| Asignación y resolución de dirección | | ✓ |
| Descubrimiento de ruteador/vecino | | ✓ |
| Administración de grupos multicast | | ✓ |
| Soporte de movilidad IPv6 | | ✓ |

ICMPv6 agrega algunas funcionalidades que no están presenten en ICMPv4, sobre todo relacionadas con el soporte que proporciona a ND. Para entender mejor estas diferencias

entre ambas versiones de ICMP se presentan en la tabla 3.6 algunas de las características más representativas.

El encabezado de ICMPv6 se distingue por poseer un valor de 58 en el campo Siguiente Encabezado, se observa en la figura 3.22 su encabezado respectivo.

| Tipo | Código | Suma de comprobación |
|---|---|---|
| Contenido del mensaje | | |

Figura 3.22 Encabezado ICMPv6

Donde:
Tipo (8 bits): identifica el tipo de mensaje (informativo, error).
Código (8 bits): dependiendo del tipo de mensaje proporciona información adicional.
Suma de comprobación (8 bits): verifica que no existan errores en el mensaje ICMPv6.
Contenido del mensaje (variable): contiene información de acuerdo al tipo de mensaje al que se haga referencia.

Ahora que se ya se ha descrito el encabezado de ICMPv6 será útil conocer la forma en que pueden clasificarse los mensajes de este protocolo; principalmente existen 2 tipos:

1) *Mensajes de error:* cada mensaje presenta ligeras diferencias en el encabezado dependiendo del tipo de error que notifique, por ejemplo en el campo tipo el rango va de 0 a 127. Algunos de los mensajes más representativos se encuentran en la tabla 3.7.

Tabla 3.7 Mensajes de error de ICMPv6

| Mensajes de error | Descripción |
|---|---|
| Destino inalcanzable<br>Tipo: 1 | El paquete enviado no pudo ser entregado.<br>Los posibles códigos son:<br>0: No existe una ruta al destino.<br>1: Comunicación administrativamente prohibida.<br>3: Dirección inalcanzable.<br>4: Puerto inalcanzable. |
| Paquete muy grande<br>Tipo: 2 | No se puede entregar el paquete a su destinatario porque se supera la longitud de la MTU de algún enlace de la ruta.<br>El código no es usado y sólo se pone en 0. |
| Tiempo excedido<br>Tipo: 3 | El ruteador descartó un paquete por haber superado el límite de saltos que le fue asignado.<br>Los posibles códigos son:<br>0: Límite de saltos excedido.<br>1: Tiempo de fragmentación/re-ensamblaje excedido. |
| Problema de parámetro<br>Tipo: 4 | El paquete no puede ser procesado porque se identificó un problema en algún campo del encabezado y el paquete fue descartado.<br>Los posibles códigos son: |

| | |
|---|---|
| | 0: Error encontrado en alguno de los campos.<br>1: No se reconoce el tipo indicado en el Encabezado Siguiente.<br>2: No se reconoce una opción IPv6. |

2) *Mensajes informativos:* además de los campos que tiene en común con ICMPv4, ICMPv6 también incluye mensajes de ND y lleva a cabo las funciones del Protocolo de Internet de Administración de Grupos, IGMP por sus siglas en inglés (Internet Group Management Protocol). Existen diferentes cambios en el encabezado ICMPv6 dependiendo del tipo de información, por ejemplo el campo tipo se encuentra en el rango 128-255. La tabla 3.8 ilustra algunos de los mensajes informativos más comunes.

Tabla 3.8 Mensajes informativos de ICMPv6

| Mensajes informativos | Descripción |
|---|---|
| Solicitud echo<br>Tipo: 128 | Enviado para realizar una prueba de conectividad hacia algún nodo de la red y conocer su estado. El código no es usado y sólo se pone en 0. |
| Respuesta echo<br>Tipo: 129 | Se genera como respuesta a una solicitud echo, llegando a ser muy utilizado como indicador de posibles problemas en la red. El código no es usado y sólo se pone en 0. |
| Petición de escucha multicast<br>Tipo: 130 | General: permite determinar las direcciones de todos los grupos multicast que existen en un enlace.<br>Específica: empleado para determinar si existen miembros de un determinado grupo multicast en un enlace. |
| Reporte de escucha multicast<br>Tipo: 131 | Generado (por cualquier nodo que pertenezca a un grupo multicast) como respuesta a un mensaje de petición recibido. |
| Escucha multicast realizada<br>Tipo: 132 | Es enviado a un nodo que decide dejar de ser miembro de un cierto grupo multicast al que pertenecía. |
| Solicitud de ruteador<br>Tipo: 133 | Uso en ND y autoconfiguración |
| Anuncio de ruteador<br>Tipo: 134 | |
| Solicitud de vecino<br>Tipo: 135 | |
| Anuncio de vecino<br>Tipo: 136 | |
| Mensaje de redirección<br>Tipo: 137 | |

Con todos los mensajes y encabezados vistos a lo largo de este capítulo sobre IPv6, ND e ICMPv6, es claro que guardan entre sí una estrecha relación para trabajar en conjunto a fin de brindar un soporte robusto en las comunicaciones desarrolladas en una red IPv6.

Por otra parte, es necesario tener en mente cada uno de los elementos descritos porque varios de ellos se retomarán en el próximo capítulo para explicar la manera en que ayudan a dar soporte de movilidad en la capa de red. Particularmente es con la ayuda y participación de los principales mecanismos y mensajes relacionados con IPv6 que la Movilidad IPv6 logra funcionar de manera clara y precisa, es decir gracias al diseño modular de IPv6 únicamente se toman como base los principales mensajes y se les añaden determinados campos o banderas, logrando de esta manera hacer uso de lo ya presente para dar marcha e impulso a los nuevos desarrollos.

# Capítulo 4

## Movilidad IP

*We can't solve problems by using the same kind of thinking we used when we created them. - Albert Einstein*

## 4.1 INTRODUCCIÓN

Anteriormente se han descrito algunas propuestas que han surgido en las diferentes capas del modelo TCP/IP para tratar de proveer un soporte para desarrollar la movilidad no obstante, una de los soluciones más prometedores se ubica en la capa de red, comúnmente denominada Movilidad IP, MIP por sus siglas en inglés (Mobile IP).

MIP proporciona un soporte para el desarrollo de la movilidad en Internet y su objetivo es mantener activas las comunicaciones de los usuarios sin que exista una interrupción significativa de los servicios que estén usando, especialmente cuando el usuario cambia entre varios puntos de acceso a la red.

Dado que actualmente IP posee 2 versiones se presentará en las siguientes secciones una descripción de la movilidad en cada una de ellas, conociendo sus diferencias, así como sus pros y contras, después de lo cual se podrá entender porque IPv6 resulta ser una mejor opción.

## 4.2 HANDOVER

En el capítulo 2 se mencionó la existencia del handover en la movilidad y como era de esperarse sin duda representa uno de los principales elementos que deben tomarse en cuenta, sobre todo para lograr que los dispositivos móviles no interrumpan sus comunicaciones cuando se desplazan a través de diferentes puntos de acceso de la red. Este evento (también conocido como Handoff) se clasifica en diferentes tipos de acuerdo a los ambientes que se involucran, siendo los casos más representativos los siguientes [19]:

a) *Momento de ejecución:* hace referencia al momento en que se lleva a cabo el handover, principalmente existen 2 tipos:

   1. No anticipados (romper antes de hacer): un dispositivo móvil únicamente puede asociarse con un único punto de acceso al mismo tiempo, por esta razón debe eliminar su asociación con su punto de acceso actual y posteriormente establecer una nueva asociación con un punto de acceso distinto, es decir, el móvil únicamente puede configurar su nueva conexión una vez que haya finalizado su conexión anterior.

      Debido a su naturaleza, mantener una continuidad en las sesiones es más difícil de lograr ya que el tiempo involucrado en el desarrollo del handover es mayor y consecuentemente existe una alta pérdida de paquetes a pesar de ello, se emplean menos recursos y la complejidad implicada es menor.

Generalmente aunque el móvil se percata de la existencia de otras redes decide seguir bajo la cobertura de su red actual, posponiendo la ejecución del handover para más adelante (figura 4.1).


Figura 4.1 Handover no anticipado

2. Anticipados (hacer antes de romper): generalmente esta situación requiere que el dispositivo móvil posea varias interfaces de red ya que el móvil puede asociarse simultáneamente con varios puntos de acceso, es decir, tiene la capacidad de establecer una nueva conexión con cierto punto de acceso antes de liberar la conexión con su punto de acceso actual (figura 4.2).

   Este caso usualmente se basa en el móvil ya que éste se percata de que existe una nueva red y que hay una degradación de la calidad de la señal de su red actual, gracias a ello este tipo de handover facilita la continuidad de las sesiones porque el tiempo en que se presenta el handover es mínimo y existe una menor perdida de paquetes; por el contrario aumenta la complejidad asociada y el móvil debe hacer uso de más recursos.

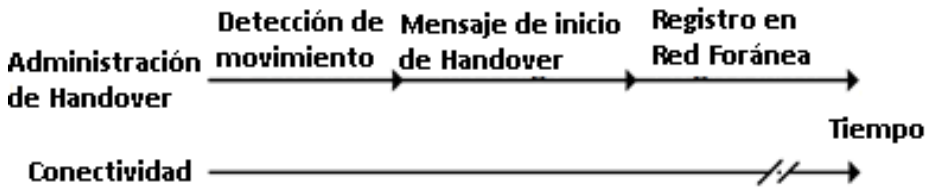



Figura 4.2 Handover anticipado

b) *Tipo de tecnología de acceso a la red:* implica el conjunto de parámetros que maneja la red, por ejemplo: cobertura, velocidad de transferencia, frecuencias de operación, ancho de banda, etc. Existen 2 escenarios principales:

   1) Horizontal (Intra-Tecnología): el móvil cambia entre puntos de acceso que pertenecen a la misma tecnología de acceso, por ejemplo al estar únicamente en una red WLAN, 3G, WiMAX, etc.

      En la mayoría de los casos este tipo de handover se realiza en la capa de enlace por lo que no existe necesidad de cambiar la dirección IP del dispositivo móvil, precisamente por esto el alcance de la movilidad únicamente se desarrolla a nivel local. Se presenta un ejemplo en la figura 4.3.

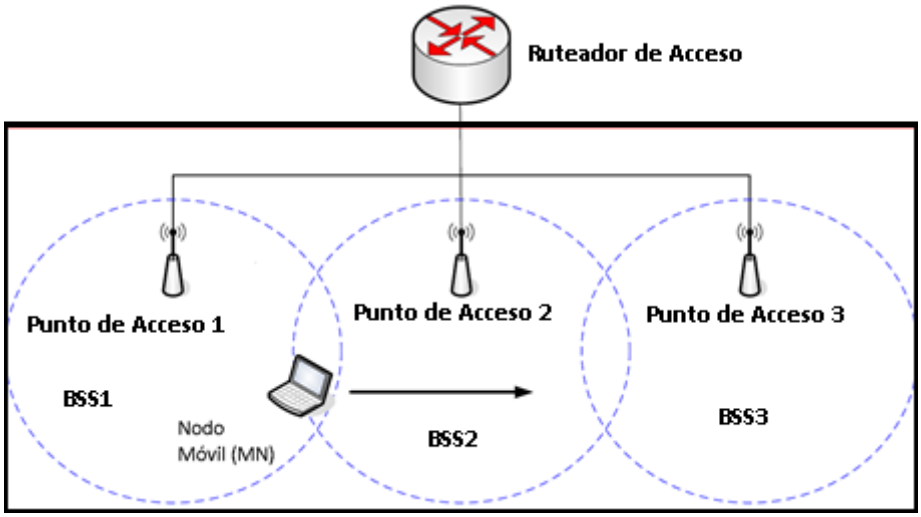



Figura 4.3 Handover Horizontal

2) Vertical (Inter-Tecnología): el dispositivo móvil se desplaza entre puntos de acceso que pertenecen a diferentes tecnologías de acceso, en cada una de las cuales adquiere una dirección IP distinta. Esta situación se presenta porque el handover se desarrolla en la capa de red y el dispositivo móvil cambia entre varios dominios de red, gracias a lo cual se puede ofrecer una movilidad a nivel global, por ejemplo al pasar de una red UMTS a una red WLAN, de una red WLAN a una red GPRS, etc. Se presenta un ejemplo en la figura 4.4.

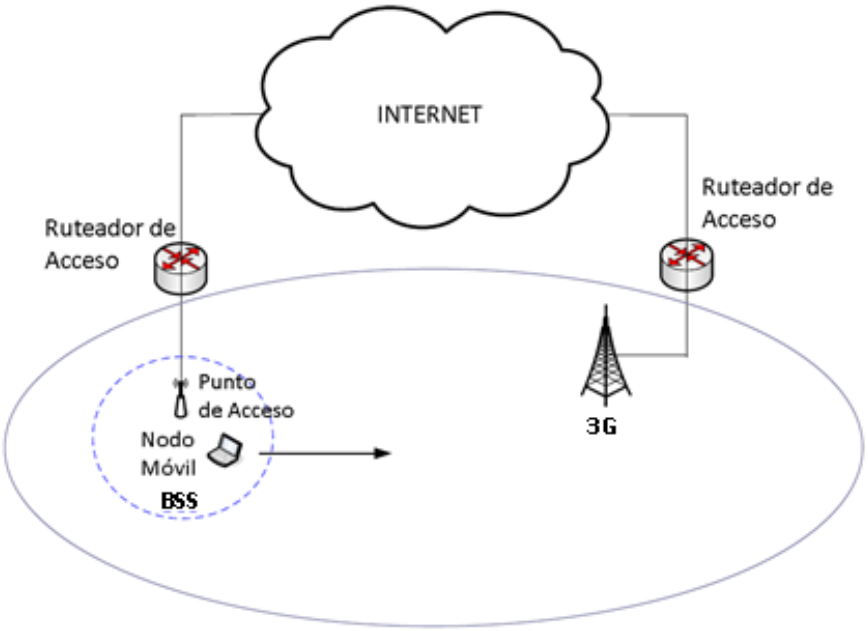



Figura 4.4 Handover Vertical

De aquí en adelante simplemente se manejará el término handover como concepto general no refiriéndose a un tipo particular pero, será importante tener en mente las capacidades asignadas a cada uno de los ejemplos antes descritos.

### 4.2.1 IMPLICACIONES EN LAS COMUNICACIONES

Gracias a la clasificación anterior es posible apreciar que la existencia del handover trae consigo varias implicaciones en las comunicaciones, mismas que deben ser consideradas no sólo para mantener activas las conexiones de los dispositivos móviles sino también para que exista una mínima pérdida de paquetes.

En la actualidad es usual utilizar diferentes tecnologías de acceso a la red para comunicarse mientras se está en movimiento sin embargo, esto implica que el dispositivo usado debe ser capaz de soportar el acceso a cada una de ellas, y todo para que al final los usuarios puedan pasar entre todos estos tipos de redes en tan sólo una fracción de segundo y sin perder alguna de sus conexiones actuales; precisamente por esto surge la necesidad de usar un mecanismo que gestione el handover de una manera eficiente y escalable. Esta visión aunque prometedora también es ambiciosa porque actualmente existen varios problemas y limitantes, sobre todo porque los usuarios finales buscan pasar entre redes de forma transparente y sin configuraciones complejas. Desafortunadamente hoy en día los parámetros de autenticación, seguridad, etc., se traducen en un importante consumo de tiempo y en una degradación en la experiencia de los usuarios mientras tanto, se describen varios de los retos que existen para proporcionar un soporte genuino de movilidad:

- *Multimodo:* deben existir dispositivos que puedan trabajar con varias tecnologías de acceso a la red, lo cual implica usar distintas frecuencias de operación, manejar diferentes velocidades de transferencia, etc.

- *Detección de cobertura de red:* los dispositivos deben detectar de manera fácil y eficiente la presencia del área de cobertura de una red, usualmente mediante el procesamiento de las señales de las redes que existen en su entorno.

  Hay que tomar en cuenta que una interfaz activa consume energía de la batería del dispositivo, incluso cuando no se envía o recibe ningún paquete, habrá que buscar un equilibrio, un escenario donde las interfaces permanezcan activas tanto como sea posible para que el móvil detecte las redes rápidamente pero, no activas tanto tiempo como para drenar una gran cantidad de energía de la batería.

- *Selección de la red más apropiada:* esto depende en la mayoría de los casos de los usuarios, por ejemplo: costo implicado, plan que se tiene contratado, preferencias, etc. por su parte, también puede estar definido por aspectos técnicos, tales como: calidad de la señal, velocidad de transferencia, área de cobertura, ubicación del usuario, comportamiento del movimiento, etc.

- *Calidad de Servicio:* debido a que se vislumbra a IP (no confiable) como el protocolo común a todas las tecnologías de acceso a la red es necesario considerar el QoS para proporcionar un trato particular a cada tipo de tráfico (sobre todo a aquellas aplicaciones de tiempo real) por ende, habrá que llegar a una similitud de elementos como: ancho de banda, confiabilidad, porcentajes de error, latencia de la red, congestionamiento, etc.

- *Seguridad:* se debe proporcionar a los usuarios el mismo nivel de seguridad independientemente del tipo de red en que se encuentren, lo que se traduce en el manejo del mismo nivel de confiabilidad, confidencialidad, integridad, etc.

- *Transferencia de contexto:* este elemento es útil porque permite a las diferentes tecnologías de acceso no solamente compartir la información del usuario sino también determinar los parámetros configurados, es decir, al no limitarse a la entrega de paquetes se logra minimizar el impacto del handover. Con este elemento mientras el dispositivo móvil se mueve de una red a otra puede seguir disfrutando de manera transparente de los mismos servicios que tenía en su red anterior (o al menos muy similares).

Todos los aspectos mencionados hasta el momento manifiestan que existen muchos retos que enfrentar para ofrecer un soporte de movilidad de una manera eficiente y escalable en ambientes reales. Teniendo esto en cuenta fue que se pensó desarrollar MIP, un protocolo de capa de red que es capaz de dar soporte de movilidad, es en las secciones siguientes que se detallarán sus aspectos más sobresalientes.

## 4.3 MOVILIDAD IPV4 (MIPV4)

En TCP/IP se considera a una dirección IP como un identificador único asignado a un dispositivo o a alguna de las interfaces de éste, de esta forma cuando un nodo cambia su punto de acceso tiene que adquirir una nueva dirección en la red donde se encuentre, y como se comentó en el capitulo anterior esto ocasiona que exista una finalización prematura en las conexiones ya establecidas. Tratando de resolver este problema surgió la Movilidad IPv4, MIPv4 por sus siglas en inglés (Mobile IP version 4), este desarrollo está definido en el RFC 5944 [20] y pretende ofrecer una solución lo más simple y sencilla posible, sin realizar grandes modificaciones en la arquitectura de las redes actuales, agregando pocos dispositivos adicionales a la red y facilitando su integración a la infraestructura de las redes existentes, por ejemplo: un nodo móvil debe ser capaz de comunicarse con otros nodos que no soporten MIPv4. Antes de comenzar a explicar su funcionamiento y los procesos involucrados, en la tabla 4.1 se describen sus elementos.

Tabla 4.1 Elementos de MIPv4

| Entidad | Descripción |
|---|---|
| Nodo Móvil | MN por sus siglas en inglés (Mobile Node): es cualquier nodo que cambia su punto de acceso a la red al desplazarse físicamente a otra ubicación (el cambio de punto de acceso no necesariamente implica un cambio de dirección IPv4). |
| Agente Local | HA por sus siglas en inglés (Home Agent): ruteador en la red local del MN que recibe y renvía los datagramas al MN cuando dicho móvil se encuentra en otra red. |
| Agente Foráneo | FA por sus siglas en inglés (Foreign Agent): ruteador ubicado en una red foránea al MN (no es su red local) que proporciona los servicios de movilidad a los MNs visitantes. |
| Nodo Corresponsal | CN por sus siglas en inglés (Correspondent Node): cualquier nodo (estacionario o móvil) que actualmente se encuentra en comunicación con algún MN. |
| Home of Address (HoA) | Para el MN es la dirección IPv4 de la red local que le es asignada permanente (por un periodo extendido de tiempo). El MN usa dicha dirección IP como origen de los paquetes que envía o como destino para los paquetes que recibe. |
| Care of Address (CoA) | Dirección IPv4 que la red foránea le asigna temporalmente a un MN (al encontrarse fuera de su red local) y que refleja la ubicación actual del punto de acceso en que dicho móvil se encuentra. |

### 4.3.1 FUNCIONAMIENTO GENERAL

Debido a que ya que se conocen los elementos en MIPv4 ahora se presenta una descripción de la forma en que interactúan y de su funcionamiento en general. Dado que la movilidad es más común bajo un ambiente inalámbrico se considerará el siguiente escenario:

- Estando el MN en su red local usa su dirección HoA (ya se ha registrado con anterioridad) para establecer una comunicación con algún CN. El MN no necesita utilizar el servicio de movilidad aún.
- Posteriormente el MN comienza a desplazarse físicamente hasta estar fuera del área de cobertura de su red local y al mismo tiempo se encuentra dentro del área de cobertura de una red foránea, razón por lo que el MN comienza su registro en dicha red para obtener una dirección válida (CoA).
- El MN aún debe poder seguir comunicándose con el CN, este último no está consciente del cambio de punto de acceso a la red del MN y continúa enviando los paquetes dirigidos al MN de manera normal, es decir, a la dirección HoA.

- Una vez que el HA registra al MN procede a establecer un túnel hacia la dirección CoA del MN, de esta forma ahora puede interceptar todos los paquetes dirigidos a la respectiva dirección HoA y enviárselos al MN a través de dicho túnel.

- Por su parte el CN no tiene manera de conocer todo el proceso involucrado en MIPv4 pero, el MN puede seguir comunicándose directamente con éste (excepto cuando existe un filtrado en la red foránea). Un ejemplo de las rutas de la comunicación antes descrita se presenta en la figura 4.5.

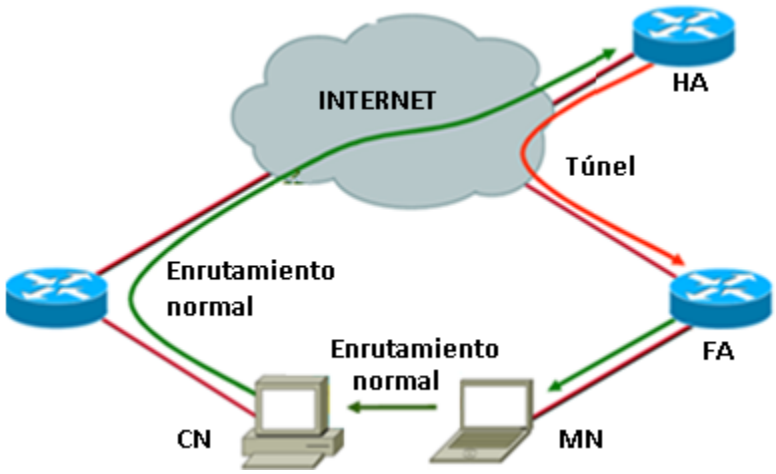



Figura 4.5 Funcionamiento de MIPv4

### 4.3.2 MECANISMOS ARP (PROXY ARP, GRATUITOUS ARP)

Para desarrollar comunicaciones de manera exitosa MIPv4 necesita ciertos elementos, por ejemplo a través de los mensajes ARP es posible dar claridad a las comunicaciones, siendo particularmente 2 las funcionalidades indispensables:

1. *Proxy ARP:* es un mensaje de respuesta ARP que un nodo envía en representación de otro, cuando este último no se encuentra actualmente en el segmento de red y no puede responder a la solicitud realizada, por ejemplo cuando un nodo local B desea conocer la dirección MAC de un nodo local A, un nodo local C regresa su dirección MAC en vez de la del nodo A solicitado, por lo que el nodo B asocia en su cache ARP la dirección MAC de C con la dirección IP del nodo A.

   Cuando un MN se encuentra registrado en una red foránea el HA utiliza la función proxy ARP por ende, cuando el HA recibe una solicitud ARP examina la dirección IP y si ésta corresponde a la dirección HoA de cualquier MN (ubicado en una red foránea y registrado actualmente), el HA en representación de dicho host inserta su propia dirección MAC en el mensaje ARP de respuesta que transmite. Es así que a través del HA actuado como proxy el resto de los nodos en la red local pueden

enviar paquetes dirigidos al MN cuando éste se encuentra en una red foránea. Se ilustra en la figura 4.6 este proceso.

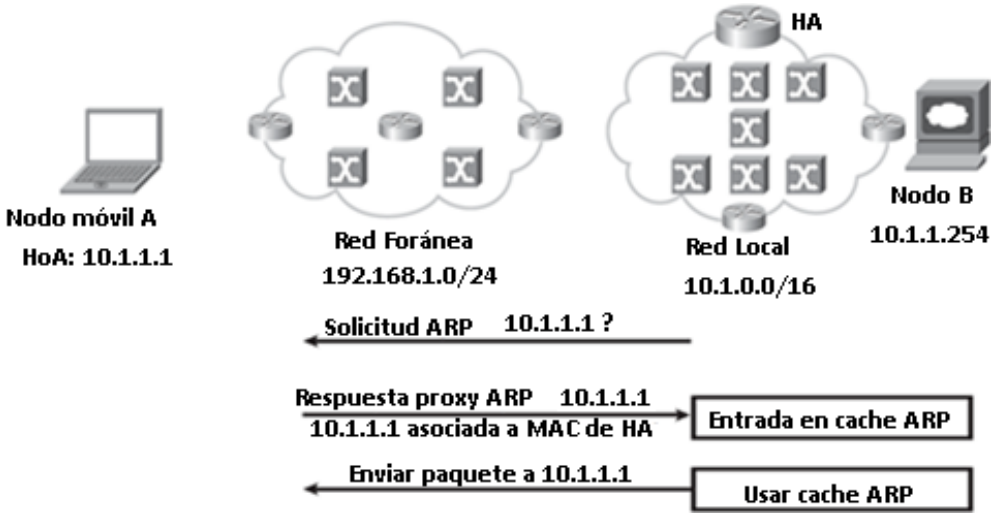



Figura 4.6 Uso de Proxy ARP en MIPv4

2. *Gratuitous ARP:* es un paquete ARP transmitido por algún nodo que pretende ocasionar que todos los nodos en el segmento de red actualicen una cierta entrada en sus caches ARP. Con esta funcionalidad se puede usar una solicitud o una respuesta ARP en cuyo contenido se almacene la dirección IP a ser actualizada, generalmente con nueva información de la dirección MAC.

   Cuando el MN deja su red local y existe en el HA una asociación de su registro en una red foránea, el HA envía un paquete gratuitous ARP en forma de broadcast para dicho segmento de red (incluso puede mandar varias retransmisiones) actuando en representación del MN. El HA informa al resto de los nodos que actualicen sus respectivas caches ARP para que puedan asociar la dirección HoA del MN con la dirección MAC del HA. Se observa un ejemplo en la figura 4.7.

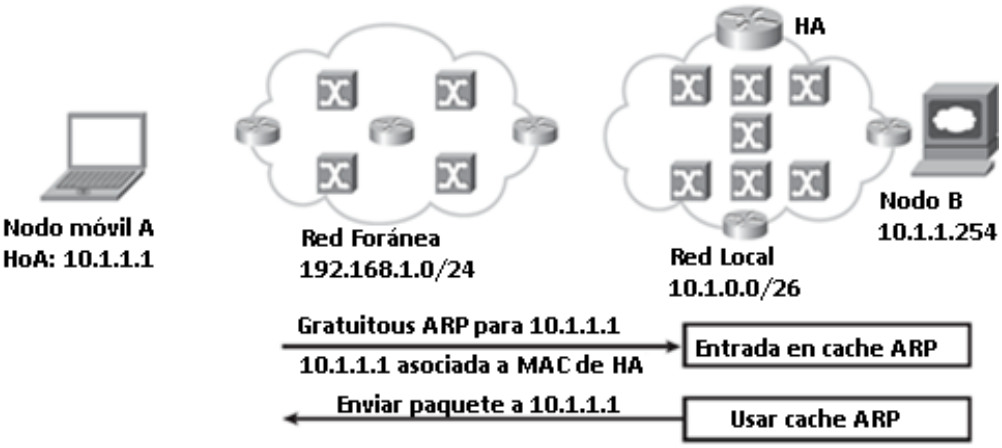



Figura 4.7 Uso de Gratuitous ARP en MIPv4

### 4.3.3 FORMAS DE ADQUISICIÓN DE DIRECCIÓN

El túnel entre el HA y la dirección CoA es crucial en MIPv4 y determinar la ruta que seguirán los paquetes se vuelve sumamente importante, precisamente para lograr esto es primordial diferenciar los 2 modos en que el MN adquiere esa dirección:

a) *Care of Address:* es una dirección IPv4 asignada del FA, es decir, en la red foránea el FA presta su dirección a todos los MNs visitantes para evitar que exista una gran demanda en el espacio de direcciones solicitadas por lo tanto, un túnel es creado entre el HA y el FA, siendo este último quien recibe los paquetes dirigidos a cada MN y los envía al destino final correspondiente.

b) *Co-located Care of Address:* es una dirección IPv4 temporal que cada MN adquiere a través de un mecanismo presente en la red foránea, por ejemplo un servidor DHCP, por lo tanto este modo está limitado por el número de direcciones disponibles que la red foránea asigna para ser utilizadas por los MNs visitantes. A pesar de ello el túnel se construye entre el HA y la interfaz del MN, situación que permite que los paquetes se entreguen directamente.

Es importante no confundir las funciones de una dirección CoA y el FA: la dirección sólo representa el punto final del túnel mientras que el FA es el agente de movilidad que provee el soporte de movilidad a los MNs visitantes, es decir, el MN debe registrarse con el FA respectivo aunque haga uso de una dirección Co-located CoA.

### 4.3.4 ESTRUCTURAS DE DATOS

Para mantener la información de los registros de movilidad es necesario que tanto el MN como su HA posean ciertas estructuras de datos, ya que en estos lugares se almacenarán las entradas de movilidad recientes. Las estructuras que existen son [20]:

1) *Lista de Visitantes:* es usada por el FA para almacenar entradas asociadas a MNs que están presentes en algún segmento de red al que está conectado. Únicamente se colocan entradas validas, es decir, cada MN debe estar registrado con su HA.

2) *Tabla de Asociación de Movilidad:* es mantenida por el HA y posee la información de los registros que ha llevado a cabo (figura 4.8).

| Dirección HoA del MN | Dirección CoA del MN | Identificación | Tiempo de vida restante |
|---|---|---|---|
| 11.1.1.1 | 169.2.2.2 | 150 | 20[s] |

Figura 4.8 Ejemplo de tabla de Asociación de Movilidad

Donde:

Dirección HoA del MN: dirección IPv4 del MN adquirida en su red local.
Dirección CoA del MN: dirección IPv4 del MN adquirida en una red foránea.
Identificación: permite identificar el valor contenido en el mensaje de Respuesta de Registro.
Tiempo de vida restante: valor que representa el tiempo de validez de la entrada, dicho valor va disminuyendo y al llegar a 0 la entrada correspondiente se elimina.

### 4.3.5 REGISTRO DEL NODO MÓVIL

El MN necesita llevar a cabo un proceso de registro con su HA para comunicarle: que ha regresado a su red local, solicitar una renovación de registro o informar su dirección CoA actual, uno de los casos antes mencionados, por ejemplo cuando el MN se encuentra en una red foránea tiene la necesidad de adquirir una nueva dirección en el segmento de red donde se encuentra, después de lo cual da a conocer a su HA dicha información en su registro; este proceso comprende un intercambio de varios mensajes que permiten ofrecer el soporte de movilidad, los pasos implicados son los siguientes:

El MN al detectar que se ha movido a una nueva red foránea (explicado más adelante) obtiene una dirección CoA mediante la cual pueda tener acceso a dicha red, tal y como se describió en la sección anterior existen 2 escenarios posibles:

- *El MN se registró usando la dirección CoA del FA (figura 4.9):* el MN se auxilia del FA y le envía un mensaje de Solicitud de Registro, a su vez el FA procesa dicho mensaje para enviarlo al HA correspondiente. El HA manda al FA un mensaje de Respuesta de Registro informándole al MN si aceptó o denegó la solicitud que recibió. Posteriormente el FA procesa la respuesta y la transmite de vuelta al MN.


Figura 4.9 Uso de dirección CoA

- *El MN utilizó una dirección Co-located CoA (figura 4.10):* el MN adquiere una dirección IPv4 perteneciente a dicho segmento de red, por lo cual al adquirir su

nueva dirección CoA el MN transmite directamente a su HA (a través de un Ruteador de Acceso) un mensaje de Solicitud de Registro informándole de su dirección recién adquirida. Por su parte el HA envía directamente al MN la respuesta informando si aceptó o denegó tal solicitud.

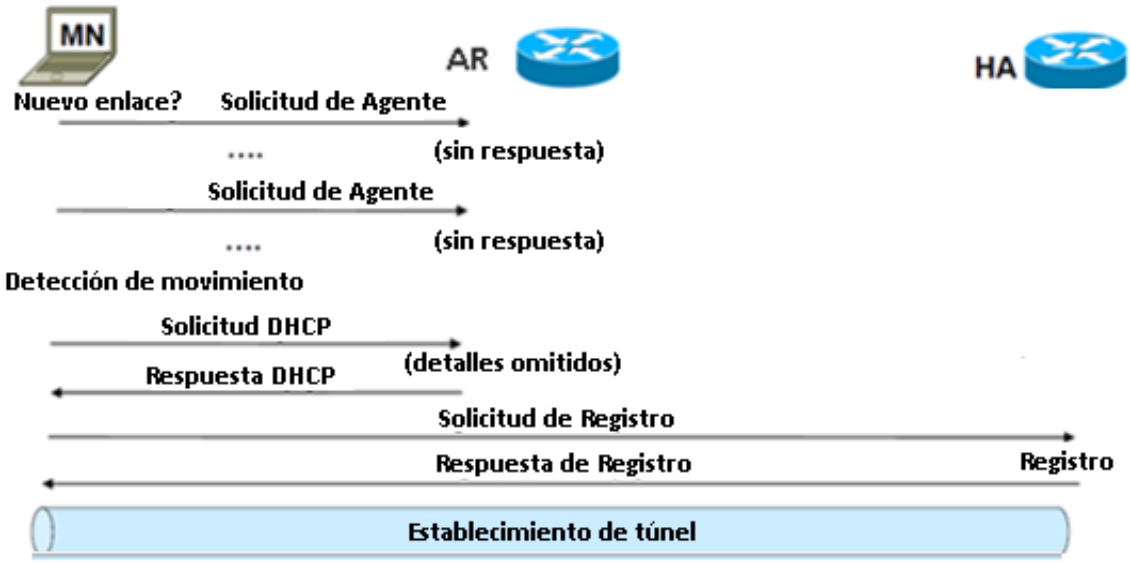



Figura 4.10 Uso de dirección Co-located CoA

Para ambos casos el HA crea una entrada en una cache asociando la dirección HoA del MN con la dirección CoA recién adquirida. Por su parte mientras el MN permanezca en esa red foránea deberá llevar a cabo una renovación de registro antes de que expire en el HA la entrada existente.

### 4.3.6 ENCAPSULACIÓN

Después de que el registro del MN se lleva a cabo de manera exitosa, es necesario que tanto el FA como el HA hagan uso de un túnel y lo mismo se aplica para el MN (en caso de que posea una dirección Co-located CoA). Esta encapsulación normalmente es realizada a través de una encapsulación mínima (IP/IP) aunque, también se puede llevar a cabo mediante una Encapsulación Genérica de Enrutamiento, GRE por sus siglas en inglés (Generic Routing Encapsulation).

En la figura 4.11 se presenta un ejemplo de la encapsulación utilizando una dirección CoA, en ella se observa que el MN posee la dirección HoA 10.1.1.1 mientras se encuentra en su red local y adquiere la dirección CoA 192.168.1.25 al ubicarse en una red foránea. Para que el MN mantenga ininterrumpidamente su comunicación con el CN (cuya dirección es 172.16.1.1) su HA debe realizar una encapsulación de los paquetes que envíe, para ello es necesario que sea insertado un paquete IP dentro de otro paquete IP, situación que involucra una sobrecarga en cada paquete enviado y un retraso en las comunicaciones.

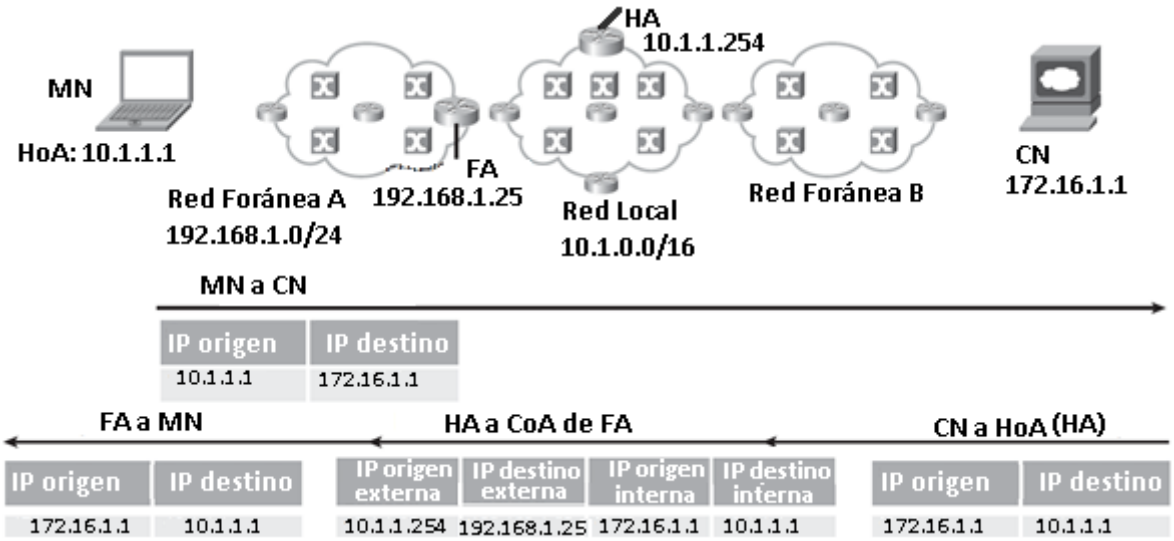



Figura 4.11 CoA y encapsulación

En caso de que el MN use una dirección CoA, el CN le envía los paquetes a su dirección HoA y es el HA el encargado de colocar en el paquete IP su dirección como origen y la dirección CoA del MN como destino, este paquete encapsula a su vez a otro paquete IP donde la dirección del CN es el origen y la dirección HoA del MN el destino. El HA procede a mandar el paquete a la dirección CoA del MN y es el FA el encargado de: remover el encabezado exterior del paquete, examinar la dirección HoA del MN al que va dirigido y finalmente transmitir el paquete con base en la dirección MAC asociada a dicho nodo.

Ocurre algo similar cuando se usa una dirección Co-located CoA, con la única diferencia de que en tal escenario el MN, de una lista que recibe (contenida en el mensaje de Anuncio de Ruteador), selecciona un ruteador por defecto de la red foránea, además el FA no es el punto final del túnel sino que éste se forma entre la dirección Co-located CoA del MN y la dirección de su HA (figura 4.12).

Anteriormente se describieron algunos de los usos recurrentes de ARP no obstante, es necesario mencionar una serie de reglas que el MN y los agentes móviles deben adoptar para el correcto funcionamiento de MIPv4 estas reglas son:

- Mientras el MN se encuentre en una red foránea no debe enviar mensajes de solicitud ARP para pedir la dirección MAC de algún otro nodo ni responder a una solicitud ARP dirigida a su dirección HoA, a menos de que sea el FA el nodo que envíe el mensaje (unicast) de solicitud.
- El FA no debe mandar un mensaje broadcast de ARP para determinar la dirección MAC del MN, sino que obtendrá dicha dirección de algún mensaje de Solicitud de Agente enviado por parte de dicho móvil.

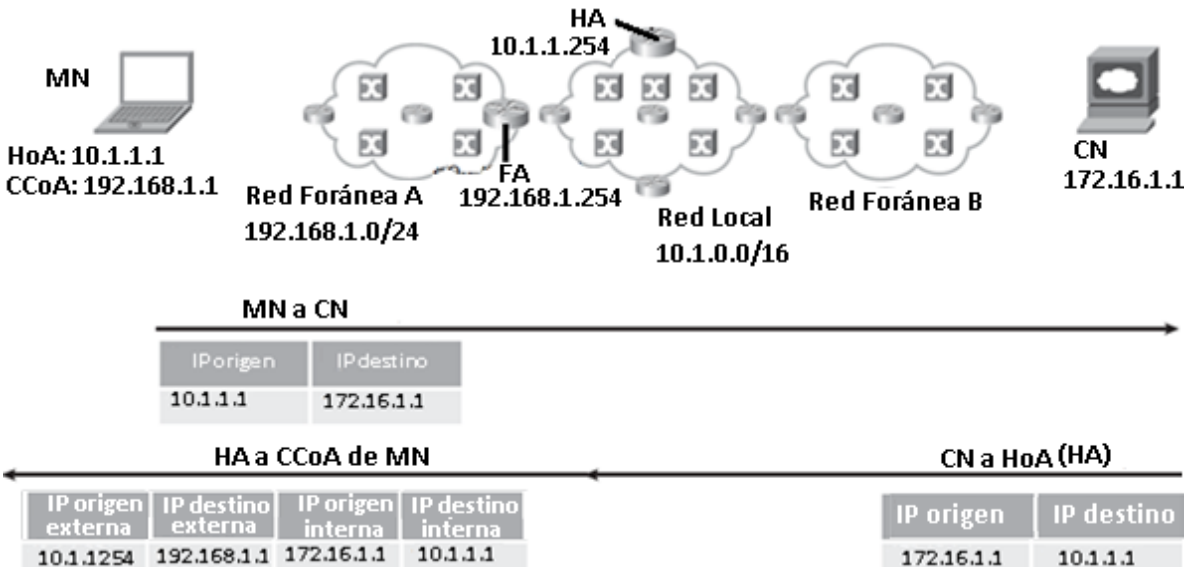



Figura 4.12 Co-located CoA y encapsulación

Estas reglas necesitan cumplirse estrictamente porque existe un problema cuando el CN está en la misma red foránea donde actualmente está ubicado el MN. Supongamos que el CN realiza una solicitud ARP para determinar la dirección MAC del MN, si este último responde, el HA no estará consciente del envío de tales paquetes. Concretamente la magnitud del problema reside en que el CN no necesita entender o estar consciente del soporte de movilidad del MN, ya que cuando dicho nodo cambia nuevamente su punto de acceso a la red, el CN no se percatará de ello y continuará usando el contenido de su tabla ARP para determinar como transmitir los paquetes dirigidos al MN, rompiendo por consiguiente la conexión que existía hasta ese momento.

### 4.3.7 COMUNICACIÓN TRIANGULAR

Hasta ahora se sabe que el CN manda los paquetes al MN a través de la intervención del HA, el cual a su vez hace uso de un túnel para entregar los paquetes a la respectiva dirección CoA pero, adicionalmente es importante estar conscientes de que el MN puede enviar los paquetes directamente al CN. Particularmente este fenómeno es conocido como Enrutamiento Triangular (se visualiza en la figura 4.13) por la ruta que siguen los paquetes y porque no existe un uso bidireccional del túnel.

Está comunicación resulta no sólo ineficiente (debido a que el HA recibe el tráfico de cada MN que se encuentra en una red foránea) sino que además causa problemas a varios de los elementos de la red involucrados en la ruta de comunicación, por ejemplo: firewalls y otros ruteadores de borde en la red pueden descartar el tráfico destinado al HA porque la conexión iniciada por el MN ocurre por un ruteador de borde diferente. Por su parte si el MN decidiera seguir utilizando su dirección HoA en una red foránea, los paquetes serían

descartados debido a la presencia de algún dispositivo de filtrado que perciba que la dirección HoA no pertenece al rango de direcciones correspondientes a la red foránea.

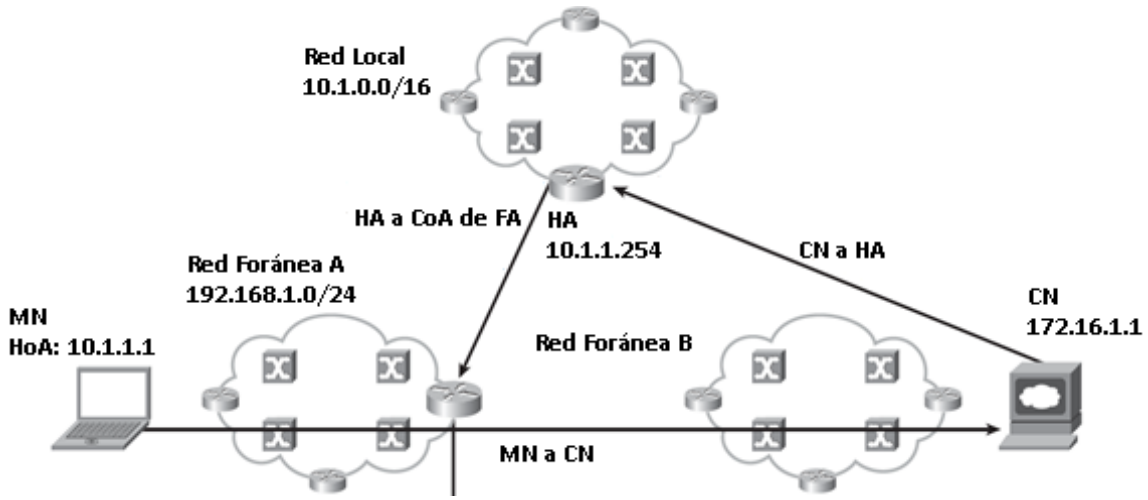



Figura 4.13 Enrutamiento Triangular en MIPv4

Precisamente para resolver algunos de estos inconvenientes surge la técnica conocida como *Encapsulación Inversa*, la cual obliga a que todas las comunicaciones entre el MN y el CN hagan uso del túnel, es decir, se lleva a cabo una comunicación bidireccional donde el HA actúa siempre como intermediario. Se aprecia la ruta que siguen los paquetes en la figura 4.14.

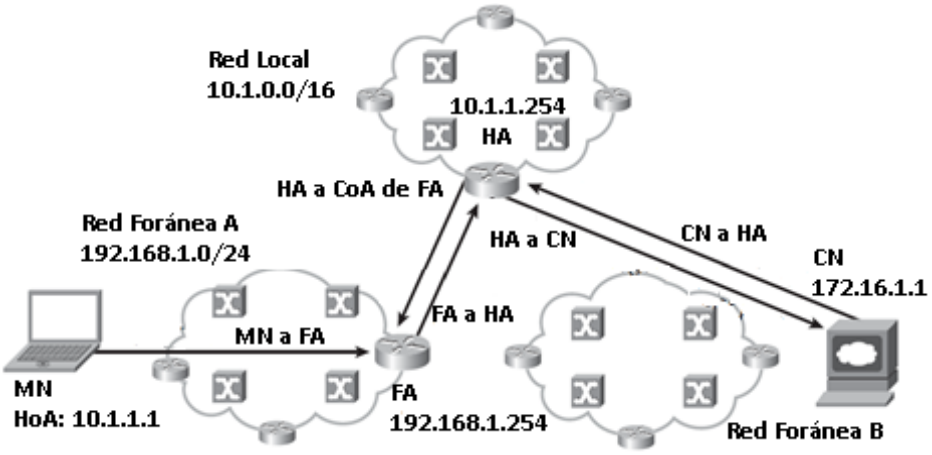



Figura 4.14 Encapsulación Inversa en MIPv4

### 4.3.8 DETECCIÓN DE MOVIMIENTO

Hasta ahora se conocen las operaciones y procesos que se llevan a cabo en MIPv4 pero, aún no se menciona la manera en que ocurre la detección de movimiento. Claramente el MN necesita percatarse cuando ya no se encuentre en su red local, situación que descubre a través de la información que obtiene de los mensajes ICMPv4 de Descubrimiento de Ruteador (método principal que usa MIPv4 para llevar a cabo el

Descubrimiento de Agentes de movilidad). Los agentes móviles anuncian constantemente su presencia en un determinado segmento de red mediante el envío de mensajes de Anuncio de Agente, mismos que resultan de anexar la siguiente información a un mensaje ICMPv4 de Anuncio de Ruteador: extensión de Anuncio de Agente Móvil y opcionalmente la extensión de longitud de prefijo y extensión de relleno.

Una vez que el MN recibe estos mensajes para conocer si se encuentra en su red local o en una red foránea analiza la siguiente información:

a. *Campo de Tiempo de vida*: el MN almacena la información contenida en dicho campo hasta que el valor expira, si el MN no recibe otro anuncio del mismo Agente dentro de este tiempo debe asumir que ha perdido contacto con dicho nodo. Dado que la frecuencia de envío de los mensajes de Anuncio de Agente es 3 veces más pequeño que el valor del campo de Tiempo de vida es posible que el MN pierda 3 mensajes consecutivos antes de eliminar la información del agente.

b. *Prefijo de red:* el MN examina este campo para saber si en la misma red donde recientemente ha adquirido una dirección CoA ha recibido un mensaje diferente de Anuncio de Agente, por lo tanto el MN asume que se encuentra en una nueva red si los prefijos de red son diferentes a pesar de ello, el MN sólo podrá hacer uso de este método si su Agente actual y su Agente nuevo poseen dicho campo en sus mensajes de Anuncio de Agente.

### 4.3.9 REGRESO A RED LOCAL

Se han descrito varios escenarios y el caso restante es aquel donde el MN estando en una red foránea vuelve a su red local, este acontecimiento involucra (figura 4.15):

a) El MN detecta que ha regresado a su red local cuando recibe un mensaje de Anuncio de Agente de su propio HA.

b) A continuación el MN configura su tabla de ruteo, para ello habilita nuevamente la característica que le permite procesar cualquier mensaje de Solicitud ARP.

c) Posteriormente el MN elimina el registro de su HA, ya que no solamente ha cambiado de red sino que particularmente ya no necesita disfrutar del soporte de movilidad. Este paso implica:

   i. El MN transmite inicialmente un mensaje broadcast gratuitous ARP para provocar que todos los nodos de su red local actualicen sus caches ARP de manera que, vuelvan a asociar la dirección HoA del MN con la dirección MAC del propio MN, en vez de la del HA.

ii. Se transmite un mensaje de Solicitud de Eliminación del MN a su HA.

iii. El HA recibe y acepta la solicitud para luego mandar un mensaje Respuesta de Eliminación al MN respectivo. Al mismo tiempo el HA transmite un mensaje gratuitous ARP en la red local del MN tratando de ayudarlo a que todos los nodos asocien la dirección HoA del MN con la MAC del MN. Posteriores mensajes gratuitous ARP son transmitidos por el MN (simultáneamente al enviar un mensaje Solicitud de Eliminación) y su HA (al mismo tiempo en que manda un mensaje Respuesta de Eliminación) para incrementar la confiabilidad de una entrega exitosa.

iv. Mientras que todos los nodos de la red local cambian la entrada de sus respectivas caches ARP, el HA deja de actuar como proxy para el MN y desiste de enviar respuestas a las solicitudes ARP dirigidas a la MAC del HA (relacionada hasta ese momento con la dirección HoA del MN). Si el HA rechaza el mensaje de Solicitud de Eliminación del MN, éste debe seguir actuando como proxy para ese MN y además prosigue con el envío de paquetes ARP (gratuitous y proxy).

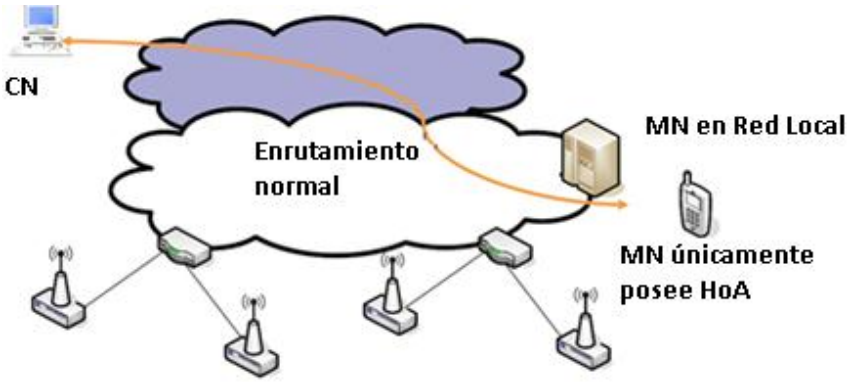



Figura 4.15 MN regresa a su red local en MIPv4

## 4.4 MOVILIDAD IPV6 (MIPV6)

Las primeras pruebas de MIP fueron desarrolladas sobre IPv4 y con base en los resultados obtenidos se llegaron a determinadas resoluciones, se desarrollaron mejoras en los problemas encontrados y al mismo tiempo se adicionaron nuevos procedimientos y procesos involucrados para dar un mejor soporte. Fue así que para la creación de IPv6 se contempló un diseño y una arquitectura que permitiera beneficiar el soporte de movilidad en la capa de red a pesar de ello, muchas de las características de la movilidad no fueron definidas desde un inicio sino que se realizaron consideraciones que permitieran agregarlas e implementarlas sin demasiada complejidad con el transcurso del tiempo.

El protocolo de Movilidad IPv6, MIPv6 por sus siglas en inglés (Mobile IP version 6) está definido en el RFC 6275 [21] y lo que busca es permitir a un nodo móvil conservar una comunicación continua con algún otro nodo mientras se desplaza a través de una red IPv6, es decir, el móvil puede moverse físicamente a una nueva ubicación y cambiar su punto de acceso a la red mientras disfruta del soporte de movilidad. A pesar de las funcionalidades que provee dicho protocolo, MIPv6 en definitiva no resuelve todos los problemas involucrados en la movilidad, se muestran en la tabla 4.2 los casos que no son considerados.

Tabla 4.2 Casos no considerados en MIPv6

| | |
|---|---|
| MIPv6 no intenta solucionar: | Control de acceso en el enlace de una red visitada por el MN. |
| | Administración de movilidad jerárquica. |
| | Asistencia para adaptar aplicaciones. |
| | Ruteadores móviles. |
| | Descubrimiento del soporte de movilidad. |
| | Distinción de pérdida de paquetes por error o por congestión de la red. |

Hechas estas aclaraciones es preciso definir (tabla 4.3) algunos de los elementos que cambian en MIPv6 (respecto a MIPv4) y que se mencionarán de aquí en adelante.

Tabla 4.3 Elementos de MIPv6

| Elemento | Descripción |
|---|---|
| Red Local | Red que posee un prefijo de donde le es asignada una dirección permanente a un MN. |
| Red Foránea | Cualquier otra red que no sea la red local de un MN. |
| Home of Address (HoA) | Dirección IPv6 unicast perteneciente a la red local del MN y que le es asignada permanentemente. El MN incluso puede poseer varias direcciones HoA con diferentes prefijos de red. |
| Care of Address (CoA) | Dirección IPv6 unicast asociada temporalmente a un MN mientras se encuentra de visita en una red foránea. |
| Agente Local (HA) | Ruteador ubicado en la red local del MN con el cual este último registra su dirección CoA. |
| Binding | Asociación de la dirección HoA de un MN con su nueva dirección CoA. |

Una vez que ya se conocen los elementos anteriores es necesario familiarizarse con las nuevas características de MIPv6 y las principales diferencias que presenta con respecto a MIPv4 (tabla 4.4).

Tabla 4.4 Diferencias entre MIPv6 y MIPv4 [21]

| Diferencias |
|---|
| No existe necesidad de un FA (utilizado sólo en MIPv4) por lo tanto, ya no se requiere un soporte especial de dicha funcionalidad en los ruteadores locales. |

| |
|---|
| La optimización de ruta no necesita extensiones adicionales ni Asociaciones de Seguridad previas, pudiendo coexistir con ruteadores que implementan un filtrado de ingreso. |
| NUD asegura la accesibilidad mutua entre el MN y su ruteador por defecto. |
| Se utiliza el encabezado de Enrutamiento Tipo 2 en vez de emplear alguna clase de encapsulación IP. |
| Al remplazar ARP con ND no se depende de ningún protocolo de capa de enlace. |
| Al usar el Descubrimiento Automático de Home Agent sólo hay una respuesta al MN. |

### 4.4.1 FUNCIONAMIENTO GENERAL

MIPv6 permite que un MN pueda desplazarse físicamente y cambiar su punto de acceso a la red pero, conservando una sesión continúa de todas sus comunicaciones en curso, para lograr esto MIPv6 admite que cada MN posea una dirección permanente (HoA) y a través de su uso no importa que el MN cambie su ubicación física porque todos los paquetes dirigidos a él son enviados a su dirección HoA. Se describe a continuación el proceso involucrado en MIPv6 (figura 4.16).

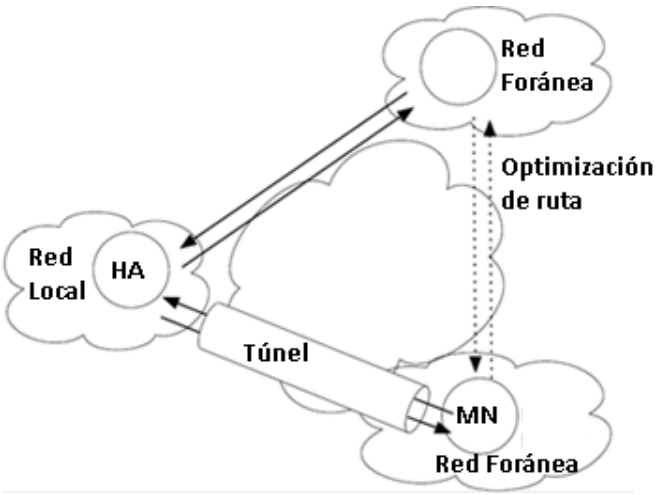



Figura 4.16 Funcionamiento de MIPv6

- El MN estando en su red local mantiene una o varias comunicaciones en curso con uno o varios CNs, al desplazarse físicamente debe cambiar su punto de acceso a la red y consecuentemente adquiere una nueva dirección (CoA) en la red foránea donde se encuentre actualmente (mediante mecanismos convencionales de IPv6).

- El CN mantiene hasta el momento una comunicación continua con el MN aunque con cierto porcentaje de pérdida de paquetes. Particularmente el CN puede o no estar consciente del desplazamiento físico del MN y la implicación del cambio de punto de acceso. Si el CN soporta el protocolo MIPv6 entonces se podrá comunicar directamente con el MN sin tener que utilizar al HA como intermediario; en caso contrario el HA debe interceptar todos los paquetes dirigidos al MN y verificar su

información interna para saber si el móvil se ha registrado correctamente en la red foránea, de ser así podrá usar el túnel establecido entre él y la nueva dirección CoA del MN para enviarle todos los paquetes, de lo contrario descarta los paquetes.

### 4.4.2 MENSAJES: ICMPv6 Y DE DESCUBRIMIENTO DE VECINOS

En secciones posteriores se describirán los procesos de MIPv6, entidades que participan, forma en que interactúan, rutas que siguen los paquetes, etc. y en cada uno de estos aspectos se hablará de los mensajes que interactúan para formar las estructuras de datos correspondientes por ello, a fin de entender mejor los campos que contienen y la información que transportan es necesario que primero se conozcan los formatos de los principales mensajes que intervienen en MIPv6. Se presentan los encabezados de extensión de IPv6 que ayudan a desarrollar las funciones de MIPv6 son [20]:

A. *Encabezado de Movilidad:* utilizado por el HA, MN y CN para la creación y administración de los registros que se llevan a cabo (figura 4.17).

| Protocolo de carga útil | Longitud de Encabezado | Tipo de Encabezado de Movilidad | Reservado |
|---|---|---|---|
| Suma de Comprobación | | Información de mensaje | |
| | | | |

Figura 4.17 Encabezado de Movilidad

En la tabla 4.5 existe una breve descripción de cada uno de los campos anteriores.

Tabla 4.5 Campos del encabezado de Movilidad

| Nombre del campo | Longitud [bits] | Descripción |
|---|---|---|
| Protocolo de carga útil | 8 | Identifica el tipo de encabezado que sigue después del Encabezado de Movilidad. |
| Longitud de Encabezado | 8 | Expresa la longitud del Encabezado de Movilidad. |
| Tipo de Encabezado de Movilidad | 8 | Identifica cada mensaje de movilidad de manera particular. Las posibles opciones son:<br>0 Binding Refresh Request<br>1 Home Test Init<br>2 Care-of Test Init<br>3 Home Test<br>4 Care-of Test<br>5 Binding Update<br>6 Binding Acknowledgement<br>7 Binding Error |

| | | |
|---|---|---|
| Reservado | 8 | Reservado para uso futuro. |
| Suma de Comprobación | 16 | Verifica posibles errores en el Encabezado de Movilidad. |
| Información del mensaje | Variable | Contiene la información asociada al tipo de Encabezado de Movilidad. |

B. *Encabezado de Enrutamiento Tipo 2:* es una variante del Encabezado de Enrutamiento y su uso permite que los paquetes sean enviados directamente del CN a la dirección CoA del MN porque los firewalls aplican diferentes reglas a los paquetes que contienen este encabezado (figura 4.18).

| | | | |
|---|---|---|---|
| Siguiente Encabezado | Longitud de Encabezado Extendido=2 | Tipo de Enrutamiento=2 | Segmentos faltantes=1 |
| Reservado | | | |
| Home Address | | | |

Figura 4.18 Encabezado de Enrutamiento Tipo 2

En la tabla 4.6 se aprecia la explicación de los campos anteriores.

Tabla 4.6 Campos del encabezado de Enrutamiento Tipo 2

| Nombre del campo | Longitud [bits] | Descripción |
|---|---|---|
| Siguiente Encabezado | 8 | Identifica el tipo de encabezado que sigue después del Encabezado de Enrutamiento. |
| Longitud de Encabezado Extendido=2 | 8 | Longitud del Encabezado de Enrutamiento. |
| Tipo de Enrutamiento=2 | 8 | Permite diferenciar entre los tipos de Encabezado de Enrutamiento que existen. |
| Segmentos faltantes=1 | 8 | Describe el número de segmentos faltantes. |
| Reservado | 32 | Reservado para uso futuro. |
| Home Address | 128 | Dirección IPv6 permanente del MN (HoA). |

C. *Encabezado de Opciones de Destino:* es usado por el MN para enviar paquetes mientras está fuera de su red local para informar a algún CN de su dirección HoA. El encabezado posee un valor de 60 en el Encabezado Siguiente (figura 4.19).

| | | |
|---|---|---|
| | Tipo de Opción | Longitud de Opción |
| Home Address | | |

Figura 4.19 Encabezado de Opción Home Address

La descripción de los campos anteriores se encuentra en la tabla 4.7.

Tabla 4.7 Campos del encabezado Opciones de Destino

| Nombre del campo | Longitud [bits] | Descripción |
|---|---|---|
| Tipo de Opción | 8 | Contiene el valor asignado de 201. |
| Longitud de Opción | 8 | Expresa la longitud del mensaje, excluyendo los campos Tipo de opción y Longitud de Opción. |
| Home Address | 128 | Dirección IPv6 permanente del MN (HoA). |

Se desglosan a continuación los tipos de mensajes de movilidad que existen:

a) *Solicitud de Renovación de Asociación*, BBR por sus siglas en inglés (Binding Refresh Request): es un mensaje enviado por el CN solicitándole al MN que actualice alguna de sus asociaciones de movilidad (figura 4.20).

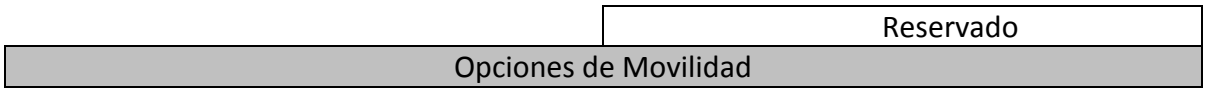



Figura 4.20 Formato del mensaje de Solicitud de Renovación de Asociación

Donde:
Reservado (16 bits): reservado para uso futuro.
Opciones de Movilidad (variable): posee campos opcionales y su formato es: tipo, longitud y valor.

b) *Home Test Init* (HoTI): mensaje con que el MN inicia el proceso Return Routability, solicitando al CN el "token Home keygen" (figura 4.21).

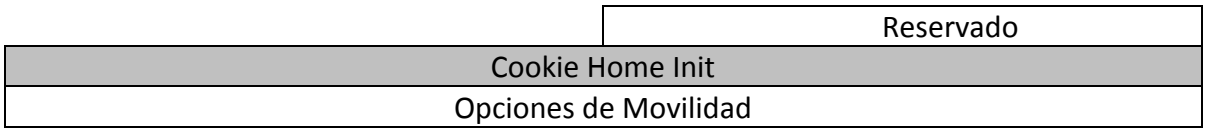



Figura 4.21 Formato del mensaje Home Test Init

Donde:
Reservado (16 bits): reservado para uso futuro.
Cookie Home Init (64 bits): contiene un valor aleatorio.
Opciones de Movilidad (variable): posee campos opcionales y su formato es: tipo, longitud y valor.

c) *Care-of Test Init* (CoTI): mensaje enviado por el MN directamente al CN en el proceso Return Routability para solicitar el "token Care-of keygen" (figura 4.22).

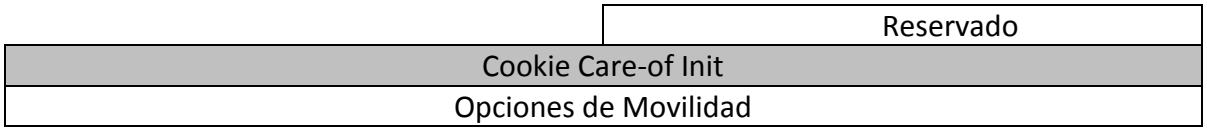



Figura 4.22 Formato del mensaje Care-of Test Init

Donde:
Reservado (16 bits): reservado para uso futuro.
Cookie Care-of Init (64 bits): contiene un valor aleatorio.
Opciones de Movilidad (variable): posee campos opcionales y su formato es: tipo, longitud y valor.

d) *Home Test* (HoT): mensaje transmitido por el CN al MN en respuesta de un mensaje HoTI recibido. Se aprecia el formato del mensaje en la figura 4.23.

| | Home Nonce Index |
|---|---|
| Cookie Home Init | |
| Token Home keygen | |
| Opciones de Movilidad | |

Figura 4.23 Formato del mensaje Home Test

Donde:
Home Nonce Index (16 bits): su valor debe ser devuelto por el MN en su siguiente mensaje BU.
Cookie Home Init (64 bits): valor obtenido del mensaje HoTI que recibió el CN.
Token Home keygen (64 bits): token utilizado en el proceso Return Routability.
Opciones de Movilidad (variable): posee campos opcionales, su formato es: tipo, longitud y valor.

e) *Care-of Test* (CoT): mensaje enviado por el CN directamente al MN en respuesta de un mensaje CoTI, su formato se muestra en la figura 4.24.

| | Care-of Nonce Index |
|---|---|
| Cookie Care-of Init | |
| Token Care-of keygen | |
| Opciones de Movilidad | |

Figura 4.24 Formato del mensaje Care-of Test

Donde:
Care-of Nonce Index (16 bits): su valor debe ser devuelto por el MN en su siguiente mensaje BU.
Cookie Care-of Init (64 bits): valor obtenido del mensaje CoTI que recibió el CN.
Token Care-of keygen (64 bits): token utilizado en el proceso Return Routability.
Opciones de Movilidad (variable): posee campos opcionales, su formato es: tipo, longitud y valor.

f) *Binding Update* (BU): mensaje usando por el MN para notificar a otros nodos (CN, HA, MN) su dirección CoA recién adquirida (figura 4.25).

| | | | | | Número de Secuencia |
|---|---|---|---|---|---|
| A | H | L | K | Reservado | Tiempo de vida |
| Opciones de Movilidad | | | | | |

Figura 4.25 Formato del mensaje Binding Update (BU)

En la tabla 4.8 se presenta la descripción de los campos anteriores.

Tabla 4.8 Campos del mensaje Binding Update (BU)

| Nombre del campo | Longitud [bits] | Descripción |
|---|---|---|
| Acuse de Recibo (A) | 1 | Activado cuando el MN desea solicitar un mensaje BA |
| Registro Local (H) | 1 | Activado si el MN solicita al destinatario que actué como su HA. |
| Compatibilidad | | Activado cuando la dirección HoA del MN tiene el mismo |

| | | |
|---|---|---|
| de Dirección de Enlace Local (L) | 1 | identificador de interfaz que la dirección de enlace local del MN. |
| Clave de Administración de Capacidad de Movilidad (K) | 1 | Al desactivarlo el protocolo usado para establecer la Asociación de Seguridad de IPSec entre el HA y el MN no permanecerá activa ante los movimientos del MN. Debe activarse sólo en mensajes enviados al HA. |
| Reservado | 16 | Reservado para uso futuro. |
| Número de secuencia | 16 | Usado por el destinatario para numerar los mensajes BUs recibidos. |
| Tiempo de vida | 16 | Segundos restantes antes de que la asociación sea inválida y la entrada correspondiente se elimine. |
| Opciones de Movilidad | Variable | Contiene campos opcionales, su formato es: tipo, longitud y valor. |

g) *Binding Acknowledgement* (BA): mensaje utilizado para confirmar la recepción de un mensaje BU; su formato se ilustra en la figura 4.26.

| | | | |
|---|---|---|---|
| | Estado | K | Reservado |
| Número de Secuencia | Tiempo de vida | | |
| Opciones de Movilidad | | | |

Figura 4.26 Formato del mensaje Binding Acknowledgment (BA)

La descripción de los respectivos campos se encuentra en la tabla 4.9.

Tabla 4.9 Campos del mensaje Binding Acknowledgment (BA)

| Nombre del campo | Longitud [bits] | Descripción |
|---|---|---|
| Estado | 8 | Indica el estado del registro del MN, por ejemplo valores menores a 128 indican que el mensaje BU fue aceptado y valores mayores o iguales indican que fue rechazado.<br>Los valores más representativos son:<br>0 Aceptado.<br>1 Aceptado pero se necesita Descubrimiento de Prefijo.<br>128 Razón no especificada.<br>129 Administrativamente prohibido.<br>130 Recursos insuficientes.<br>131 Registro no soportado.<br>132 No subred local<br>133 No existe Home Agent para este nodo móvil.<br>134 Falla al ejecutar DAD.<br>135 Número de secuencia fuera de ventana.<br>136 Expiración de Home Nonce Index.<br>137 Expiración. |
| Clave de | | Al desactivarlo el protocolo usado para establecer la |

| | | |
|---|---|---|
| Administración de Capacidad de Movilidad (K) | 1 | Asociación de Seguridad de IPSec entre el HA y el MN no sobrevivirá ante los movimientos del MN. Se activa sólo en mensajes enviados desde el HA. |
| Reservado | 16 | Reservado para uso futuro. |
| Número de secuencia | 16 | Valor utilizado para relacionar este mensaje con el correspondiente BU recibido. |
| Tiempo de vida | 16 | Tiempo (en unidades de 4 segundos) en que el HA mantendrá la entrada respectiva en su Binding Cache. |
| Opciones de Movilidad | Variable | Contiene campos opcionales, su formato es: tipo, longitud y valor. |

h) *Binding Error* (BE): mensaje utilizado por el CN y el HA para notificar al MN que existió un error de movilidad. Se presenta en la figura 4.27 el formato respectivo.

| | | |
|---|---|---|
| | Estado | Reservado |
| Home Address | | |
| Opciones de Movilidad | | |

Figura 4.27 Formato del mensaje Binding Error (BE)

Se describen los campos anteriores en la tabla 4.10.

Tabla 4.10 Campos del mensaje Binding Error (BE)

| Nombre del campo | Longitud [bits] | Descripción |
|---|---|---|
| Estado | 8 | Indica la razón por la que se originó este mensaje:<br>1 No se reconoce la Opción de Destino Home Address.<br>2 Tipo de Encabezado de Movilidad no reconocido. |
| Reservado | 16 | Reservado para uso futuro. |
| Home Address | 16 | Dirección contenida en la Opción de Destino Home Address que el MN usa para determinar si la asociación fue o no exitosa (en caso de que posea varias direcciones HoA). |
| Opciones de Movilidad | Variable | Contiene campos opcionales, su formato es tipo, longitud y valor. |

Finalmente se describen los últimos mensajes ICMPv6 implicados entre el MN y su HA:

1. *Solicitud de Descubrimiento de Dirección Home Agent:* mensaje usado por el MN para solicitar la dirección de su HA en su red local (figura 4.28).

| | | |
|---|---|---|
| Tipo | Código | Suma de Comprobación |
| Identificador | | Reservado |

Figura 4.28 Formato del mensaje Solicitud de Descubrimiento de Home Agent

Donde:

Tipo (8 bits): contiene un valor asignado de 144.

Código (8 bits): contiene un valor asignado de 0.
Suma de Comprobación (16 bits): verifica que no existan errores en el mensaje ICMPv6.
Identificador (16 bits): establece una relación con la respuesta futura que se espera recibir.
Reservado (16 bits): reservado para uso futuro.

2. *Respuesta de Descubrimiento de Dirección Home Agent:* mensaje de respuesta enviado al MN por parte del HA más cercano (figura 4.29).

| Tipo | Código | Suma de Comprobación |
|---|---|---|
| Identificador | | Reservado |
| Dirección Home Agent | | |

Figura 4.29 Formato del mensaje Respuesta Descubrimiento de Home Agent

Donde:
Tipo (8 bits): contiene un valor asignado de 145.
Código (8 bits): contiene un valor asignado de 0.
Suma de Comprobación (16 bits): verifica que no existan errores en el mensaje ICMPv6.
Identificador (16 bits): valor obtenido del mensaje de solicitud recibido.
Reservado (16 bits): reservado para uso futuro.
Dirección Home Agent (variable): lista de los HAs presentes en la red local del MN.

3. *Solicitud de Prefijo de Movilidad:* mensaje que envía el MN a su HA solicitando un Anuncio de Prefijo de Movilidad para configurar o actualizar su dirección HoA (figura 4.30).

| Tipo | Código | Suma de Comprobación |
|---|---|---|
| Identificador | | Reservado |

Figura 4.30 Formato del mensaje Solicitud de Prefijo de Movilidad

Donde:
Tipo (8 bits): contiene un valor asignado de 145.
Código (8 bits): contiene un valor asignado de 0.
Suma de Comprobación (16 bits): verifica que no existan errores en el mensaje ICMPv6.
Identificador (16 bits): establece una relación con la futura respuesta esperada.
Reservado (16 bits): reservado para uso futuro.

4. *Anuncio de Prefijo de Movilidad:* mensaje que manda el HA para proporcionarle información al MN acerca del prefijo de su red local (figura 4.31).

| Tipo | Código | Suma de Comprobación | | |
|---|---|---|---|---|
| Identificador | | M | O | Reservado |
| Opciones | | | | |

Figura 4.31 Formato del mensaje Anuncio de Prefijo de Movilidad

Donde:
Tipo (8 bits): contiene un valor asignado de 147.
Código (8 bits): contiene un valor asignado de 0.
Suma de Comprobación (16 bits): verifica que no existan errores en el mensaje ICMPv6.
Identificador (16 bits): valor obtenido del mensaje de Solicitud Prefijo de Movilidad.

Configuración de Administración de Dirección (M): activado indica que los nodos además de usar una configuración stateless también pueden hacer uso de una configuración stateful.
Otra Configuración Stateful (O): activado indica que los nodos usan un mecanismo stateful para obtener información adicional.
Reservado (16 bits): reservado para uso futuro.
Opciones (variable): opciones adicionales.

### 4.4.3 ESTRUCTURAS DE DATOS

Una vez que ya se han detallado los formatos de los mensajes implicados en MIPv6 es importante conocer que cada una de las diferentes entidades participantes almacena cierta información de las comunicaciones móviles, esto es posible a través de diversas estructuras de datos que mantienen un conjunto de entradas y que son consultadas para saber que asociaciones tiene con otras entidades. Las estructuras son las siguientes:

- *Binding Cache* (BC): la poseen HA y CN, y contiene las asociaciones respectivas que tienen con otros nodos. Se presenta un ejemplo en la figura 4.32.

| HoA de MN | CoA de MN | Tiempo de vida | Bandera | Número de secuencia | Información de uso |
|---|---|---|---|---|---|
| 2001:db8:1:1::10 | 2001:db8:3:1::10 | 150s | Deshabilitada | 3 | Uso reciente |
| 2001:db8:1:4::10 | 2001:db8:1:5::1 | 200s | Deshabilitada | 14 | Uso reciente |

Figura 4.32 Formato de Binding Cache

Donde:
HoA de MN: usada en la búsqueda de la dirección destino de un paquete a enviar.
CoA de MN: dirección temporal asociada al MN. Es utilizada en la optimización de ruta con algún CN, y para el HA representa un registro de algún MN.
Tiempo de vida: indica el tiempo de validez restante de una entrada antes de ser eliminada.
Bandera: señala si la entrada corresponde a un registro (aplica sólo a nodos con soporte de HA).
Número de secuencia: valor máximo recibido en previos mensajes BU.
Información de uso: datos usados para implementar políticas de asociación o de registro.

- *Binding Update List* (BUL): es mantenida por el MN y cada entrada representa una asociación que el MN tiene o que trata de establecer con algún otro nodo. En la figura 4.33 se tiene un ejemplo.

| Dirección IPv6 de nodo | HoA de MN | CoA de MN | Tiempo de vida inicial | Tiempo de vida restante |
|---|---|---|---|---|
| 2001:db8:1:4::10 | 2001:db8:4:1::100 | 2001:db8:3:1::100 | 600s | 200s |

| Número de secuencia | Tiempo de envío del mensaje BU | Estado de retransmisión | Bandera |
|---|---|---|---|
| 35 | 12:05 | 20s | Habilitada |

Figura 4.33 Formato de Binding Update List

Donde:
Dirección IPv6: representa la dirección del nodo al que el mensaje BU fue mandado.
HoA de MN: dirección principal del MN.

CoA de MN: dirección temporal del MN.
Tiempo de vida inicial: valor inicial del campo Tiempo de vida del mensaje BU enviado.
Tiempo de vida restante: valor restante del tiempo de vida inicial del mensaje BU enviado.
Número de secuencia: valor que diferencia cada mensaje BU transmitido.
Tiempo de envío del mensaje BU: restringe la frecuencia máxima de envío.
Estado de retrasmisión: incluye el tiempo para la próxima retransmisión del mensaje BU.
Bandera: especifica si se deben o no enviar futuros mensajes BU a cierto destino. Se activa al recibir un mensaje ICMPv6 con problemas en algún parámetro, mensajes de error en el proceso Return Routability o en el envío de un mensaje BU.

La información contenida en la lista anterior es usada por el MN para determinar si un paquete es mandado directamente al CN o a través del túnel que tiene con su HA. Para el proceso Return Routability la información auxiliar se ilustra en la figura 4.34.

| Tiempo de envío | Estado de retransmisión | Cookies | Tokens | Nonce index | Tiempo de recepción |
|---|---|---|---|---|---|

Figura 4.34 Información adicional en Binding Update List

Donde:
Tiempo de envío: lapso en que los mensajes HoTI y CoTI fueron enviados a su destino.
Estado de retransmisión: indica si hay que hacer una retransmisión en el proceso Return Routability (incluye el tiempo restante para la siguiente retransmisión).
Cookies: valores usados en los mensajes HoTI y CoTI.
Tokens: corresponden al Home keygen y Care-of keygen recibidos por algún CN.
Índices: Home nonce y Care-of nonce recibidos por un CN.
Tiempo de recepción: tiempo en que fueron recibidos los tokens e índices enviados por cierto CN.

- *Home Agents List* (HAL): únicamente la posee el HA y permite conocer la existencia de otros HAs en el mismo segmento de red. Se pueden tener listas independientes para cada interfaz donde un ruteador actúa como HA. La información es utilizada para brindar información al MN cuando algún HA recibe una Solicitud de Descubrimiento Automático de Dirección de Home Agent. Se ilustra un ejemplo en la figura 4.35.

| Dirección IPv6 de HA | Dirección IPv6 global de HA | Tiempo de vida [s] | Preferencia |
|---|---|---|---|
| 2001:db8:1:1::1/64 | 2001:1218::2/48 | 300 | 0 |
| 2001:db8:1:1::7/64 | 2001:1218::10/48 | 100 | |
| 2001:db8:1:1::5/64 | 2001:1218::7G/48 | 600 | 10 |

Figura 4.35 Formato de Home Agents List

Donde:
Dirección IPv6 local de HA: obtenida del mensaje RA recibido.
Dirección IPv6 global de HA: aprendida de un mensaje RA.
Tiempo de vida: lapso en que la entrada será valida.
Preferencia: valores más altos indican mayor preferencia. Se usa para ordenar la lista de HAs.

### 4.4.4 REGISTRO DEL NODO MÓVIL

Para que el MN mantenga una comunicación continua con cualquier otro CN no sólo basta con que tenga el par de direcciones HoA y CoA, sino que además necesita registrarse con su HA para brindarle esa información; el proceso consiste en (figura 4.36):

- Tanto el MN como el HA deben usar una Asociación de Seguridad (a través de IPSec) para proteger la integridad, confidencialidad y autenticidad de los mensajes intercambiados. El MN para informar de su nueva dirección necesita enviar un mensaje BU a su HA, e incluso podrá mandárselo a algún CN con el que se esté comunicando; para el segundo caso el procedimiento se denomina Return Routability y podrá efectuarse únicamente después de que el MN se haya registrado con su HA.

- El HA primero confirma que el MN pertenece a su red local y que en realidad tiene asignada cierta dirección HoA, también verifica que esa dirección ha sido utilizada con la Asociación de Seguridad correcta por lo tanto, comprueba que exista la entrada correspondiente; de cumplirse estos requisitos el HA crea una asociación entre la dirección HoA de un cierto MN y su nueva dirección CoA. Si el MN no tenía una asociación previa, el HA lleva a cabo el proceso DAD en su red local y de ser satisfactorio, le responde con el envío de un mensaje BA a su nueva dirección CoA, informándole que ha creado la asociación exitosamente.

  En caso de que haya existido algún error en los parámetros recibidos o el MN no perteneciere a la red local del HA, en vez de un mensaje BA el HA le manda al MN un mensaje BE. Frente a una asociación exitosa se crea un túnel seguro entre el HA y la dirección CoA del MN. El MN tendrá que repetir este proceso antes de que el tiempo de vida de la asociación expire y la entrada correspondiente en su HA sea eliminada.

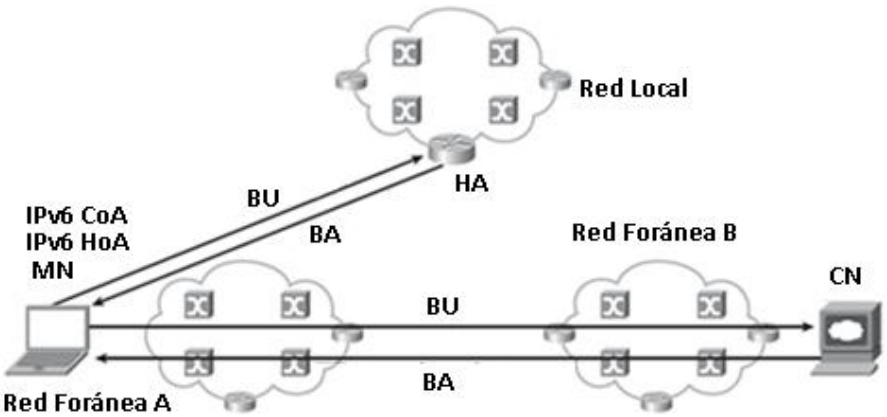



Figura 4.36 Registro de nodo móvil en MIPv6

### 4.4.5 ENCAPSULACIÓN

En secciones pasadas ya se describió de manera general el proceso de comunicación no obstante, aún falta conocer los modos por los que el MN puede comunicarse con el CN: el primero denominado *Encapsulamiento Bidireccional* se usa principalmente cuando el CN no soporta MIPv6 (la ruta que siguen los paquetes entre el CN y el MN es análoga a como ocurría en el Encapsulamiento Inverso de MIPv4). Se presenta enseguida un ejemplo de comunicación entre un MN y un CN (figura 4.37):

- El MN no envía los paquetes dirigidos al CN de manera directa sino que hace uso del túnel creado anteriormente con su HA.
- El HA procede a recibir los paquetes transmitidos por parte del MN y los renvía a la dirección del CN.
- Dado que el CN no está consciente del cambio de punto de acceso del MN sigue enviándole todos los paquetes a su dirección HoA.
- El HA usa el protocolo ND para emplear la funcionalidad de proxy, con lo cual es capaz de interceptar todos los paquetes dirigidos a la dirección HoA del MN y enviarlos a través del túnel existente con la respectiva dirección CoA.
- Finalmente el MN recibe los paquetes originados por el CN a través de su HA y los procesa de manera natural.

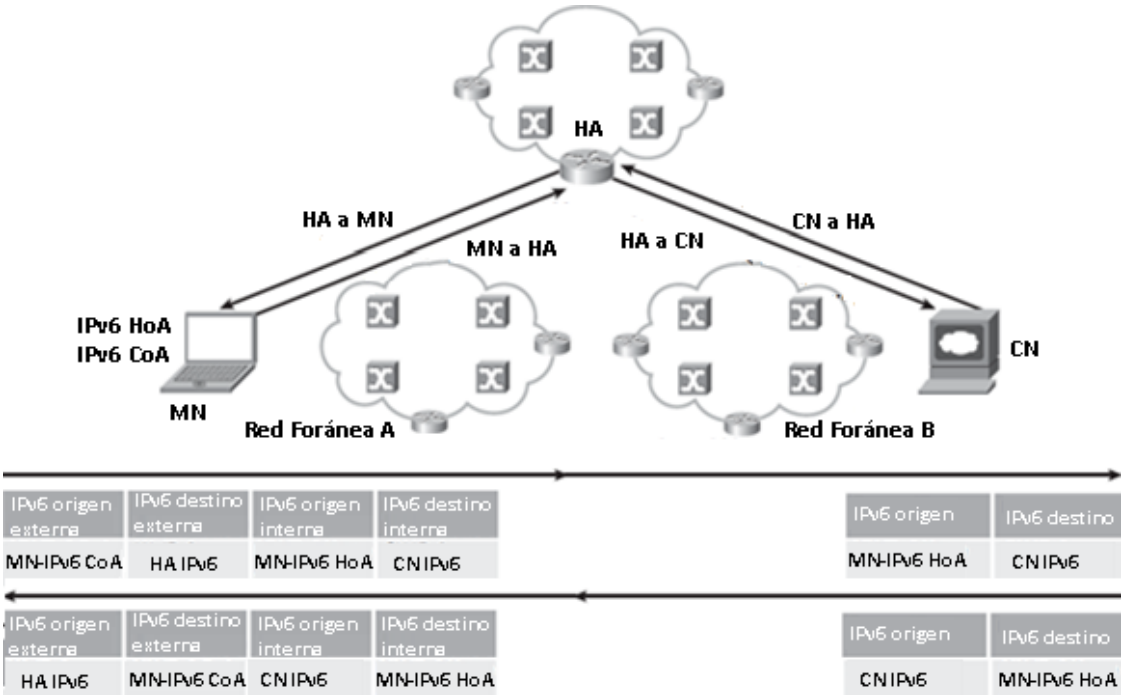



Figura 4.37 Encapsulamiento Bidireccional en MIPv6

En la figura 4.37 se ilustra que al utilizar el túnel existen 2 encabezados IPv6: las direcciones externas se utilizan para enviar los paquetes por el túnel que existe entre el HA y la dirección CoA del MN, mientras que las internas son las que mantienen intactas las direcciones finales de origen y destino de la comunicación (CN, HoA).

Esta forma de comunicación es más segura (todos los paquetes son enviados por el túnel protegido) no obstante, existen una serie de desventajas importantes tales como: retraso en las comunicaciones e ineficiencia en el propio envío de los paquetes, un ejemplo claro se presenta en la figura 4.38 donde a pesar de que tanto el MN como el CN están en la misma red foránea no pueden comunicarse directamente entre sí.

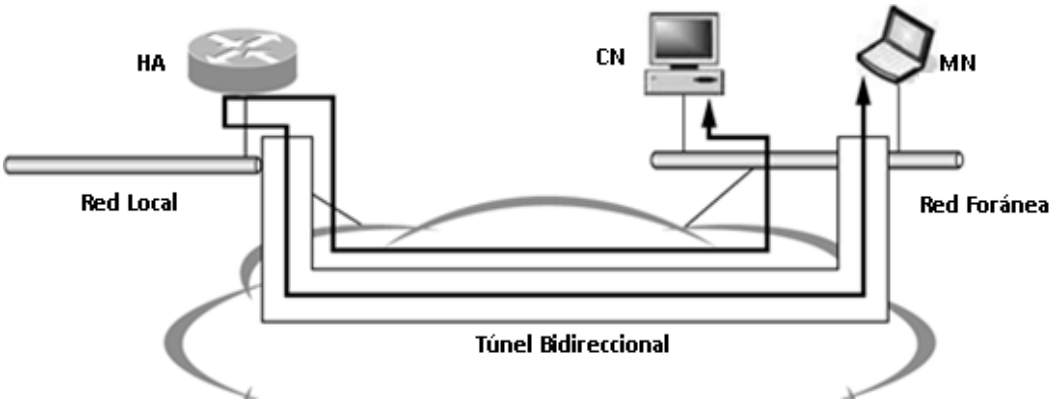



Figura 4.38 Ineficiencia del Encapsulamiento Bidireccional en MIPv6

### 4.4.6 MEJORAS RESPECTO A IPV4

En el inicio de esta sección se comentaron los casos que no se consideran en MIPv6 y las diferencias principales que existen en torno a MIPv4, lo que sin duda ha ayudado a entender las razones principales por las cuales es preferible usar IPv6 para proveer soporte de Movilidad IP. Por lo tanto únicamente falta por describir aquellas mejoras que existen en MIPv6 que lo hacen un mejor candidato.

Gracias a la forma en que IPv6 fue diseñado existen encabezados y campos que le ayudan a brindar características adicionales a la movilidad IP (que no son ofrecidas en MIPv4) y que mejoran significativamente el rendimiento de las comunicaciones. Enseguida se mencionan tales características a fin de reforzar la razón de emplear MIPv6.

#### 4.4.6.1 PROCEDIMIENTO "RETURN ROUTABILITY"

Recientemente se mencionó uno de los modos de comunicación entre el MN y el CN, y antes de hablar de la segunda forma que existe es necesario llevar acabo un intercambio de mensajes entre el MN y el CN (ambos con soporte de MIPv6). Particularmente se debe seguir el procedimiento conocido como *"Return Routability"*,

pues es a través de éste que se logra proteger el intercambio de futuros mensajes de registro.

Una de las bondades de Return Routability es que no requiere que existan configuraciones previas de Asociaciones de Seguridad ni que exista una infraestructura de autenticación entre el MN y el CN; su objetivo es crear una importante mejora en MIPv6 sin introducir nuevos problemas de seguridad, y su principal ventaja es limitar que posibles atacantes con acceso a la red fraudulentamente traten de enviar mensajes BU. Para hacer esto posible se verifica que el MN que está mandando un mensaje BU es quién dice ser, de modo que el CN tenga una mayor certeza de que el MN posee ambas direcciones (CoA y HoA); a pesar de ello habrá que tomar en cuenta que este método no puede proteger de atacantes que se ubiquen entre la ruta de la red local y del CN.

Es importante considerar que la ejecución de este procedimiento introduce un retraso adicional en las comunicaciones entre un MN y un CN porque implica el intercambio de varios mensajes no obstante, los beneficios que proporciona claramente son mayores. El proceso consta de los siguientes pasos (figura 4.39):

1) El MN genera dos mensajes (HoTI y CoTI) que envía de manera simultánea. El primero se envía a través del HA quien a su vez lo envía al CN, mientras que el segundo se envía directamente al CN. Ambos mensajes contienen cookies (Home init y Care-of init respectivamente) que el MN espera recibir en las respuestas del CN por lo tanto, el MN debe almacenar información de los mensajes transmitidos, por ejemplo: dirección IPv6 del nodo al que fue enviado, tiempo en que se realizó la transmisión, dirección HoA del MN, cookies utilizadas, etc.

2) Debido a que el CN puede o no tener soporte de MIPv6 (condición desconocida por el MN) hay que considerar los siguientes casos:

   - Si el CN no tiene el soporte, cuando reciba los mensajes de movilidad retornará un mensaje ICMPv6 informando de un problema de parámetro, y una vez que el MN reciba dicha notificación entenderá que no puede llevar a cabo el proceso de Return Routability y que debe regresar a la forma de comunicación original (encapsulación bidireccional).

   - En caso contrario el CN al recibir los mensajes de movilidad verifica que en ninguno de ellos exista la Opción de Destino Home Address, una vez que ya los haya procesado crea 2 mensajes de respuesta: HoT, responde al mensaje HoTI recibido (se manda a la dirección HoA del MN); CoT, es la respuesta del mensaje CoTI recibido (se envía directamente a la dirección CoA del MN).

El CN con base en los mensajes HoTI y CoTI que recibe genera 2 tokens: Home keygen y Care-of keygen respectivamente, es el uso de ambos tokens lo que prueba que el MN puede recibir mensajes a través de sus direcciones HoA y CoA.

Los parámetros que se envían en el mensaje HoT son: la misma cookie contenida en el mensaje HoTI (Home init), el token recién generado (Home keygen) y un valor auxiliar que será utilizado por el MN (Home nonce index) mientras tanto, el mensaje CoT contiene los siguientes parámetros: la cookie Care-of init, el token Care-of keygen y el valor Care-of nonce index. Todos estos elementos ayudarán a proteger futuros registros de posibles atacantes y falsos mensajes de asociación.

3) El proceso Return Routability se completa cuando el MN reciba los mensajes HoT y CoT y compare la siguiente información con la que anteriormente había generado y almacenado: las cookies y la dirección del CN. De cumplirse lo anterior el MN comienza a procesar el resto de los datos de los mensajes HoT y CoT.

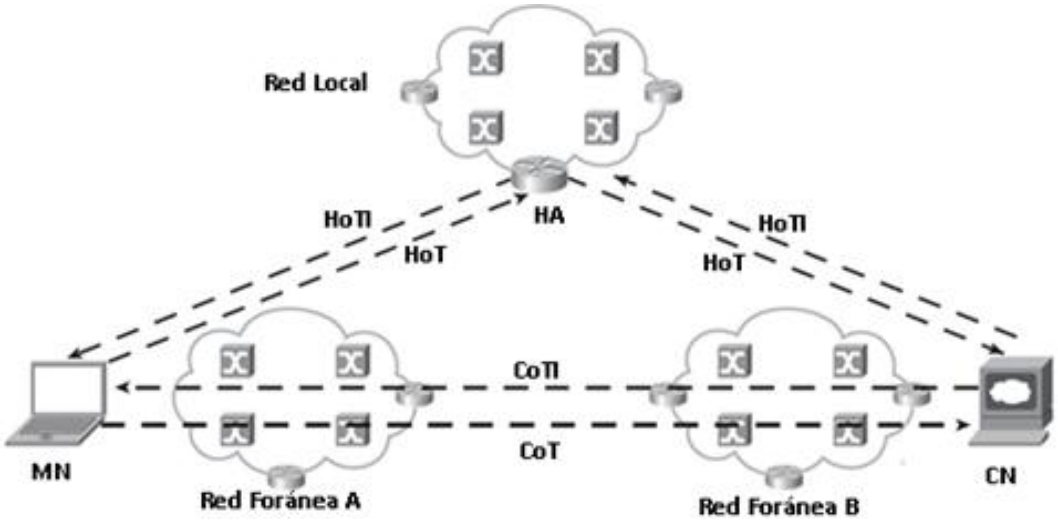



Figura 4.39 Procedimiento "Return Routability"

### 4.4.6.2 OPTIMIZACIÓN DE RUTA

Ahora que ya se ha comentado el mecanismo Return Routability se procederá a detallar la segunda manera por la que el CN se comunica con el MN, la cual consiste en: el CN envía los paquetes a la dirección CoA actual del MN, es decir, este modo de comunicación resuelve el problema de Enrutamiento Triangular (presentado en MIPv4).

La *optimización de ruta* ofrece mejoras significativas en la comunicación ya que no es necesario involucrar al HA en el envío de los paquetes. Las principales ventajas de ello son:

- ✓ Se eliminan posibles congestiones en los enlaces del HA de la red local del MN.
- ✓ Reducción de la carga de red producida por el uso de una comunicación triangular.

- ✓ Protección contra fallas temporales presentes en la red local o en el HA del MN.
- ✓ Disminución de los recursos que el HA utiliza para la intercepción, procesamiento y envío de los paquetes transmitidos entre un CN y algún MN.
- ✓ Reducción de la latencia en la entrega de paquetes entre un CN y un MN.

Las ventajas que existen en la optimización de ruta son muy importantes pero, para poder mandar los mensajes de forma directa el MN primero debe establecer una asociación con el CN, algo muy similar al registro que realiza con su HA. Los pasos involucrados son (figura 4.40):

a. Después de realizar el proceso Return Routability el MN tiene la información necesaria para enviar un mensaje BU al CN sin embargo, adicionalmente requiere una forma de autorizar dicho mensaje, para ello combina los tokens recibidos y genera una Llave de Administración de Asociación, Kbm por sus siglas en inglés (Binding Management Key).

   Así el MN crea un mensaje BU que contendrá los siguientes parámetros: HoA (contenida en la Opción de Destino Dirección Local), número de secuencia, índices (Home nonce y Care-of nonce) y un valor obtenido a través de una función hash (utilizando la llave Kbm).

b. A continuación el MN envía un mensaje BU al CN, la dirección de origen es su CoA y como destino la dirección del CN. En comparación con el mensaje BU que manda a su HA la diferencia de este mensaje radica en la desactivación de algunas banderas ya que propiamente el MN no se está registrando con el CN, únicamente le está ofreciendo información acerca de su dirección actual.

   Adicionalmente el mensaje BU contiene la opción Información de Autorización de Asociación, esto con el propósito de asegurar que los índices contenidos en el mensaje sean válidos. Específicamente hacer uso de esta opción permite autenticar el mensaje BU utilizando una función hash (SHA-1).

c. El CN recibe el mensaje BU y corrobora la siguiente información: la dirección HoA es unicast, la bandera de registro está desactivada, los índices están presentes. De cumplirse lo anterior el CN genera nuevamente los tokens (Home keygen y Care-of keygen) con la información contenida en el mensaje recibido y posteriormente procede a construir la llave Kbm.

   Enseguida el CN utiliza dicha llave para generar un valor con el que verifique la autenticidad del mensaje BU. Finalmente el CN compara el valor que recién ha generado con el valor contenido en la opción Información de Autorización de

Asociación (contenido en el mensaje BU): si ambos valores coindicen se acepta la validez de dicho mensaje, de lo contrario lo rechaza y manda un mensaje BA informando de ello.

d. Inmediatamente el CN almacena una entrada en su BC que relaciona las direcciones HoA y CoA del MN, posteriormente crea un mensaje BA informando sobre el éxito de la asociación: se especifica la dirección HoA en el Encabezado de Enrutamiento y se agrega la opción Información de Autorización de Asociación.

   El mensaje BA debe contener los siguientes parámetros: número de secuencia (obtenido del mensaje BU recibido), estado de la asociación y un valor obtenido a través de una función hash (utilizando la llave Kbm generada por el CN) para autenticar la veracidad del mensaje BA.

e. El CN transmite finalmente el mensaje BA (recién creado) a la dirección CoA del MN para informarle que ha procesado correctamente su mensaje y que se encuentra listo para comunicarse de manera directa con el MN.

f. El MN recibe el mensaje BA y analiza lo siguiente: existe la opción Información de Autorización de Asociación y el número de secuencia es igual al valor que el MN creó en el mensaje BU que envió anteriormente.

   En caso de que lo anterior no se cumpla el mensaje se ignora y es descartado. Por el contrario al corroborarse que el mensaje es válido (el estado indica que la asociación se realizó correctamente) el MN almacena dicha información y actualiza la entrada correspondiente en su BUL.

   Finalmente el MN deberá transmitir un mensaje BU antes de que el tiempo de vida de la asociación expire y la entrada correspondiente sea eliminada.

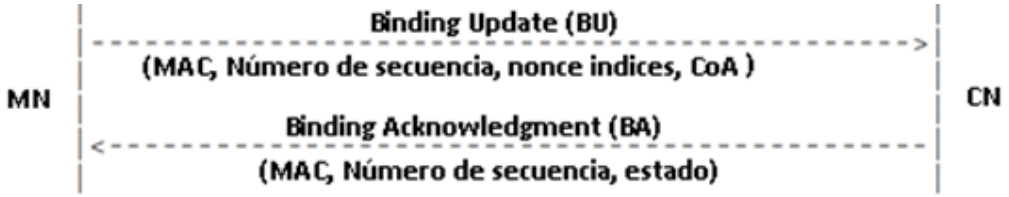



Figura 4.40 Mensajes de movilidad entre CN y MN

Ahora los siguientes paquetes enviados entre el CN y el MN se mandan directamente pero, para mantener la comunicación ininterrumpida para cada paquete, se lleva a cabo un procesamiento adicional que se describe enseguida (figura 4.41):

- Para los paquetes transmitidos del MN al CN: la dirección destino es la del CN y la dirección origen es la dirección CoA del MN, adicionalmente la dirección HoA del

MN es colocada en la opción Home Address (ubicada en el campo del Encabezado de Opciones de Destino).

Cuando el CN recibe los paquetes del MN verifica si posee una entrada en su BC que haga referencia a la dirección HoA contenida en el paquete, si no existe la entrada respectiva el CN manda un mensaje BE con un estatus de 0 para notificarle al MN que necesita enviarle un mensaje BU. Esto se lleva a cabo para prevenir que algún nodo malicioso use una cierta dirección CoA que no le pertenece e intente realizar una suplantación de identidad de un MN legítimo.

Si el CN posee la entrada correspondiente en su BC acepta el paquete e intercambia la dirección origen con la dirección HoA, de esta manera se logra mantener las comunicaciones en curso sin interrupciones porque los protocolos de capas superiores observan la misma dirección de origen (HoA) para todos los paquetes.

- Para los paquetes enviados del CN al MN: la dirección del CN es la dirección origen mientras que la dirección CoA del MN es la dirección destino, y adicionalmente el CN coloca la dirección HoA del MN en el Encabezado de Enrutamiento tipo 2.

  El MN al recibir los paquetes extrae la dirección HoA y verifica que dicha dirección le pertenezca, de ser así la coloca como la dirección destino del paquete, en caso contrario descarta el paquete. Con esto se logra que la comunicación del CN al MN no sufra alteraciones, debido a que los protocolos de capas superiores no están conscientes del proceso de intercambio que se ha suscitado en la capa de red.

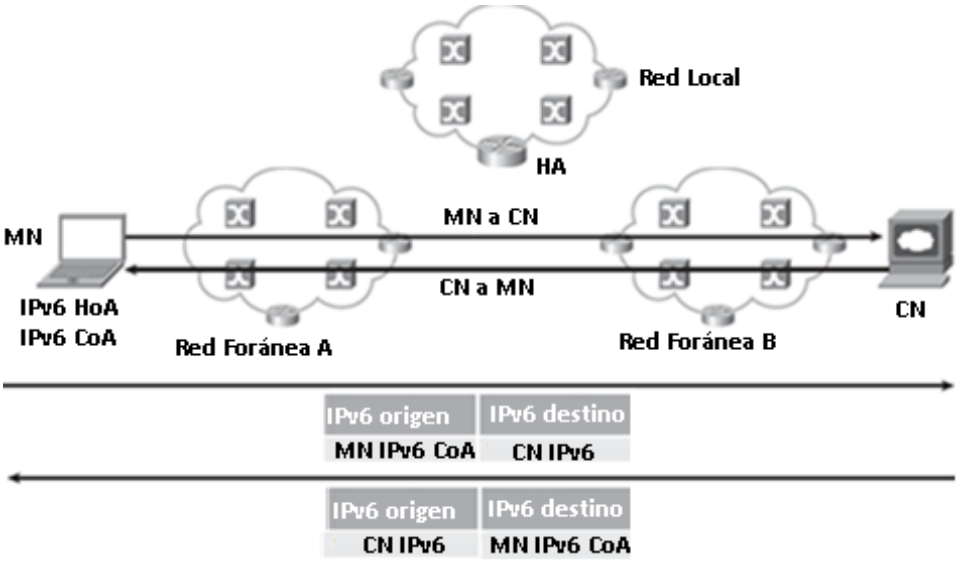



Figura 4.41 Optimización de ruta entre CN y MN

### 4.4.6.3 DESCUBRIMIENTO DINÁMICO DE "HOME AGENT"

Hasta ahora se ha considerado que el MN tiene su información de configuración completa pero ¿Qué pasa si sólo posee su dirección HoA y su prefijo de red? Es vital que descubra la dirección de su HA en su red local. Como se recodará, cada HA mantiene una estructura HAL donde almacena información de todos los nodos que poseen la función de HA y que se encuentran en el mismo segmento de red; cada entrada es extraída de los mensajes de Anuncios de Ruteador que éstos envían de manera no solicitada, así cuando un HA recibe un Anuncio de Ruteador verifica si tal ruteador se declara como HA, de ser así crea o actualiza la entrada correspondiente de su HAL con la siguiente información: dirección IPv6 origen, preferencia y tiempo de vida; por lo tanto cuando un MN necesita mandar un mensaje BU pero desconoce la dirección IPv6 de su HA puede utilizar el mecanismo de Descubrimiento Dinámico de Dirección de Home Agent, DHAAD por sus siglas en inglés (Dynamic Home Agent Address Discovery); para entender este proceso habrá que tomar en cuenta lo siguiente (figura 4.42):

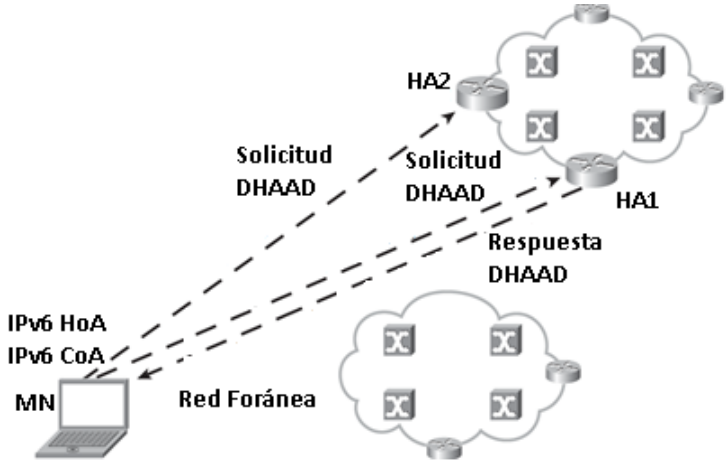



Figura 4.42 Descubrimiento Automático de Dirección de Home Agent

Para cada subred existe una dirección IPv6 anycast reservada para los Home Agents de dicha subred. La figura 4.43 presenta el formato de dicha dirección.

| Prefijo | ID interfaz | |
|---|---|---|
| | 1111111…111111 | Anycast ID=7E |

Figura 4.43 Formato de dirección IPv6 anycast de Home Agent

- El MN transmite un mensaje ICMPv6 de Solicitud de Descubrimiento de Dirección de Home Agent hacia la dirección anycast del segmento de red correspondiente a su red local.
- Únicamente el HA más cercano (determinado a través de métricas de ruteo), de dicho segmento de red, recibe el mensaje de solicitud y manda al MN un mensaje

ICMPv6 de Respuesta de Descubrimiento de Dirección de Home Agent. También es posible que el HA mande dicho mensaje de manera no solicitada cuando hayan cambiado los tiempos de vida de los HAs o sus respectivas direcciones.

El mensaje de respuesta contiene los siguientes datos: una lista decreciente ordenada con base en la preferencia de cada HA, junto a su correspondiente dirección IPv6 (el HA obtiene estos datos de su HAL).

- El MN recibe el mensaje de respuesta y con ello ahora conoce la información de cada HA de su red local, por lo tanto solicita su registro, que consiste en: al estar en su red local solicita una dirección HoA, mientras que en una red foránea comienza su registro con el HA con la mayor preferencia. En caso de que el MN no se registre correctamente, debe intentar registrarse con el siguiente HA con la segunda mayor preferencia y así sucesivamente hasta lograr un registro exitoso. Pensado en términos de eficiencia es aconsejable que el MN almacene la lista que obtiene en una memoria no volátil para su uso futuro, evitando de esta forma que nuevamente necesite realizar dicho intercambio de mensajes cuando se apague.

En lo que respecta a la seguridad en DHAAD actualmente no se definen mecanismos de autenticación por lo que, el HA no puede verificar la dirección HoA del MN que lleve a cabo la solicitud DHAAD, afortunadamente los atacantes no puede obtener más información que la dirección de los HA en la red local porque para el resto de las comunicaciones existen mecanismos de seguridad (excepto al usar optimización de ruta).

Adicionalmente existen mensajes ICMPv6 referentes al proceso denominado Descubrimiento de Prefijo de Movilidad, mismos que deben ser protegidos mediante IPSec en modo transporte (utilizando ESP) porque contienen información de la topología de red del HA y los tiempos de vida de los prefijos correspondientes. Es posible que el MN (al estar en una red foránea) envíe a su HA un mensaje Solicitud de Prefijo de Movilidad, MPS por sus siglas en inglés (Mobile Prefix Solicitation) cuando desee conocer información del prefijo de movilidad asociada a su dirección HoA o cuando dicha dirección se haya convertido en inválida. Por su parte el HA procede a transmitir al MN un mensaje Respuesta de Solicitud de Prefijo de Movilidad, MPA por sus siglas en inglés (Mobile Prefix Advertisement) dándole a conocer información sobre dicho prefijo.

Cabe mencionar que el Descubrimiento de Prefijo de Movilidad también puede ser iniciado por el HA (asumiendo que tenga un registro actual de un MN) cuando existan cambios en los tiempos de validez y preferencia del prefijo de la red local del MN o en alguna de sus banderas. Opcionalmente otros eventos pueden detonar el envío de mensajes MPA, por ejemplo: adicionar un nuevo prefijo en la red local del MN, cambiar

banderas o tiempos de vida en un prefijo diferente al que el MN pertenece, etc. (estos últimos casos dependen de las políticas bajo las cuales se configure al HA).

### 4.4.7 DETECCIÓN DE MOVIMIENTO

En las secciones anteriores se explicaron muchos de los procesos involucrados en las asociaciones entre el MN, su HA y algún CN aunque, hasta el momento no se ha detallado la manera en que el MN determina cuando se ha desplazado a otra red, y será dicho tema el que se explique en esta sección.

La detección de movimiento tiene como objetivo principal detectar handovers L3 (implica un cambio en la dirección IP) porque la efectividad del algoritmo usado define en gran medida el rendimiento de este proceso y por consecuencia el tiempo implicado en el handover, es decir, existe una pérdida de paquetes (figura 4.44) todo el tiempo involucrado en las siguientes tareas: una vez que se presenta un movimiento es hasta cierto tiempo después que se logra detectar dicho suceso, ante ello el MN adquiere una nueva dirección CoA (y lo que ello implica) o en su defecto dejar de disfrutar del soporte de movilidad (al regresar a su red local o simplemente al apagar el móvil) y finalmente se registra con su HA (manda un mensaje BU y espera la recepción del mensaje BA).

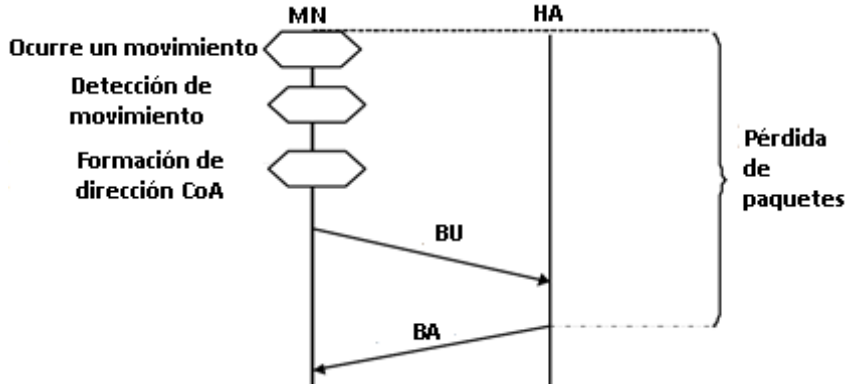



Figura 4.44 Pérdida de paquetes

El método por defecto usado para detectar el movimiento hace uso de ND, específicamente de RD y NUD. Para conocer el intercambio de mensajes implicados en este proceso es necesario mencionar los eventos indicadores que suelen presentarse:

a. *Anuncio de Ruteador:* cuando el MN recibe un mensaje RA de un nuevo ruteador (que contiene un conjunto diferente de prefijos de red) necesita detectar si aún es accesible su ruteador anterior, para ello sigue los siguientes pasos:

   i. El MN envía un mensaje unicast RS a la dirección de su ruteador anterior, si recibe una respuesta debe seguir usando la información de tal ruteador, de lo contrario debe utilizar NUD (paso ii).

ii. *Detección de No Accesibilidad de Vecino*: Esta opción generalmente es utilizada cuando el MN tiene paquetes que mandar y existe una baja frecuencia en el envío de mensajes RA o incluso ausencia de tales mensajes.

A través de NUD el MN verifica si su ruteador por defecto aún accesible, de no serlo el MN manda un mensaje multicast NS para buscar los posibles ruteadores del segmento de red actual donde se encuentra.

El que un MN reciba mensajes de un nuevo ruteador en su mismo segmento de red no necesariamente indica que ha ocurrido un handover L3 (puede haber varios HAs en el mismo segmento de red), se debe considerar que las direcciones de enlace local de los ruteadores no son globalmente únicas ya que generalmente los ruteadores usan la misma dirección de enlace local en los anuncios que envían a sus diferentes interfaces, precisamente para resolver esta situación habrá que configurar a cada HA para que anuncie su dirección global.

b. Los mensajes RA contienen una opción que indica el intervalo de envío de estos mensajes, situación que permite al MN definir su propia política que determine el número de mensajes de su ruteador por defecto perdidos que indiquen que ha ocurrido un posible handover L3 o que conlleven al MN a pasar al paso anterior.

Una vez que el MN detecta que ocurrió un handover L3 necesita adquirir una nueva dirección CoA, enseguida ejecuta el proceso DAD y posteriormente lleva a cabo el proceso RD de su red foránea actual para elegir un nuevo ruteador por defecto. Después de esto el MN está listo para iniciar el proceso de su registro.

Llegado a este punto sólo resta describir los posibles movimientos del MN que se presentan, en la figura 4.45 se observa el procedimiento que acontece cuando el MN pasa por primera vez de su red local a una red foránea y que comprende los siguientes pasos:

1. El MN al verificar que su ruteador por defecto ya no está presente transmite un mensaje multicast RS para conocer los posible ruteadores del nuevo segmento de red donde se encuentra.

2. Cada uno de los ruteadores por defecto de la red foránea envían al MN un mensaje unicast RA. Con base en dichas respuestas el MN elige uno de ellos.

3. Si el MN lo necesita puede mandar un mensaje de Solicitud de Descubrimiento de Dirección de Home Agent.

4. El MN espera recibir el mensaje Respuesta de Descubrimiento de Dirección de Home Agent (en caso de que aplique).

5. IPSec: negociación de Asociaciones de Seguridad (veáse el capitulo 5).
6. El MN envía un mensaje BU desde su dirección CoA a la dirección de su HA.
7. El HA registra al MN y manda un mensaje multicast NA en su respectiva red local.
8. El HA transmite un mensaje BA a la dirección CoA del MN.

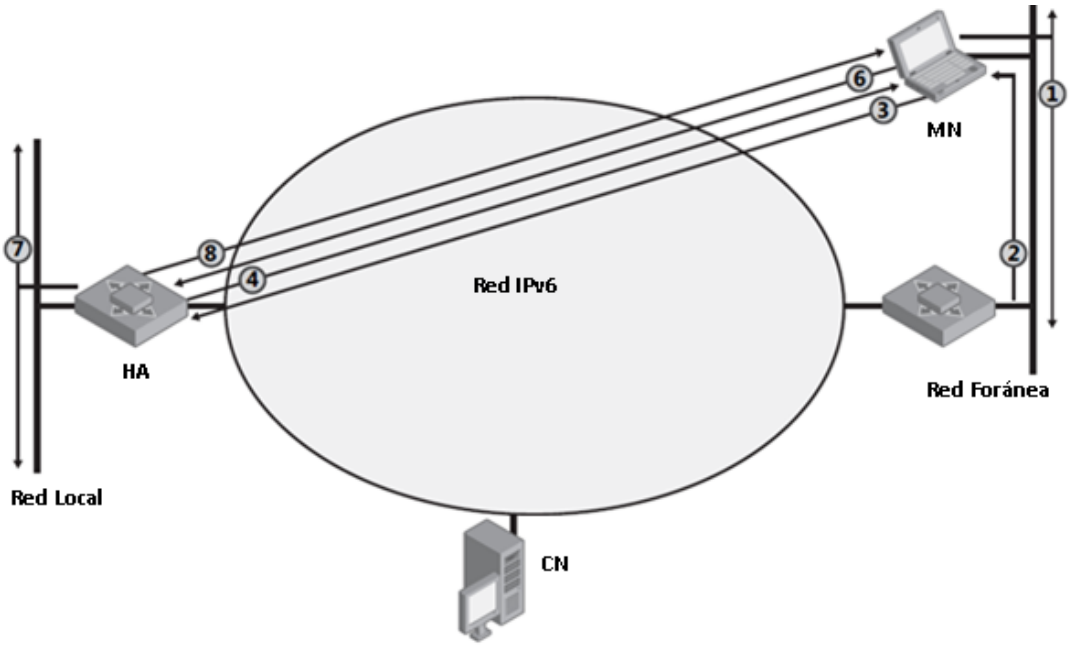



Figura 4.45 MN por primera vez en una red foránea

Por su parte cuando el MN se mueve de una red foránea a otra red foránea se siguen los pasos mostrados en la figura 4.46 que comprenden:

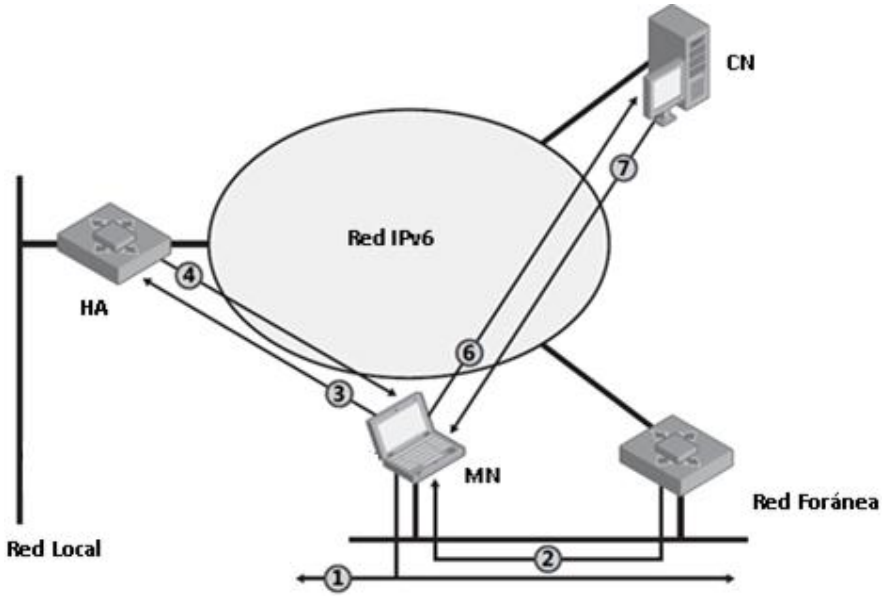



Figura 4.46 MN de una red foránea a otra

1) El MN al verificar que su ruteador por defecto ya no está presente envía un mensaje multicast RS para conocer los ruteadores de su nuevo segmento de red.

2) Cada uno de los ruteadores default de la red foránea mandan al MN un mensaje unicast RA, con base en dichas respuestas el MN elige uno de ellos.

3) El MN transmite un mensaje BU de su dirección CoA a la dirección de su HA.

4) El HA crea el registro respectivo y manda un mensaje BA a la dirección CoA del MN.

5) Se lleva a cabo el método Return Routability (explicado con anterioridad).

6) El MN envía un mensaje BU de su dirección CoA a la dirección del CN.

7) El CN transmite un mensaje BA a la dirección CoA del MN.

### 4.4.8 REGRESO A RED LOCAL

Un último caso falta considerar y se presenta cuando el MN regresa a su red local. En primer lugar el MN debe detectar este evento y particularmente sabe que ha regresado a su red local utilizando las mismas opciones descritas en la sección anterior, específicamente ocurre cuando el MN descubre que la red donde se encuentra tiene el mismo prefijo que el de su red local. Teniendo dicha información el MN realiza algunos pasos adicionales para actualizar la información de sus asociaciones existentes, tal como se describe a continuación (figura 4.47):

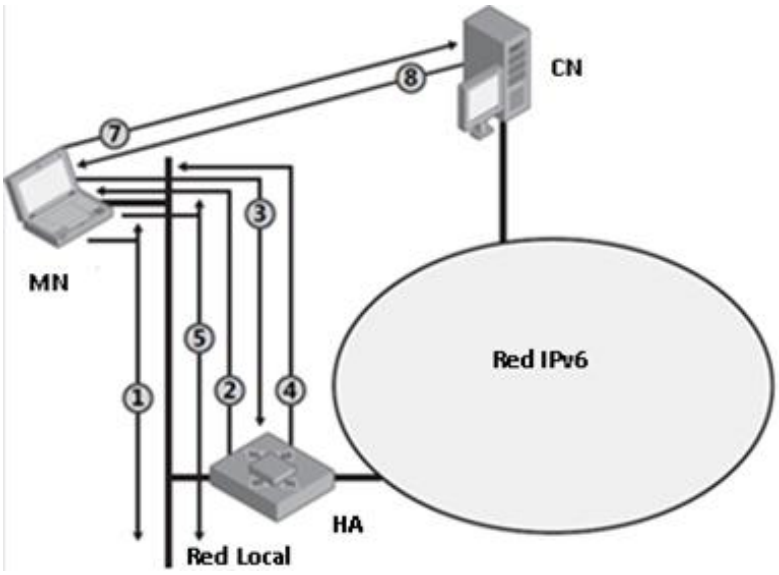



Figura 4.47 MN regresa a su red local

1. Normalmente el MN obtiene la dirección MAC de su HA a través de los mensajes NA que recibe pero, frente a la ausencia de dichos mensajes o al existir múltiples

HAs en su red local, el MN manda un mensaje multicast NS con las siguientes características: dirección origen no especificada (::), su dirección HoA como dirección objetivo; esto es necesario porque hasta ese momento el HA a través de ND se encuentra configurado para interceptar todos los paquetes dirigidos a la dirección HoA del MN.

2. El HA al recibir la solicitud del MN transmite un mensaje multicast NA hacia el segmento de red de donde recibió dicha solicitud.

3. A continuación el MN manda a su HA un mensaje BU con las siguientes características: valor de 0 en el campo tiempo de vida, su dirección HoA en los campos CoA y dirección origen. Estos campos le indican al HA no seguir interceptando los paquetes dirigidos a la dirección HoA del MN.

   Después de transmitir el mensaje BU el MN se configura para responder mensajes NS dirigidos a su dirección HoA.

4. El HA recibe el mensaje BU y al procesar los valores que contiene, sabe que debe dejar de responder a los mensajes NS dirigidos a la dirección HoA del MN.

   Posteriormente el HA envía un mensaje BA destinado a la dirección HoA del MN y al mismo tiempo elimina la entrada que asocia las direcciones HoA y CoA del MN, finalmente destruye el túnel creado con la respectiva dirección CoA.

   Una vez que el MN recibe el mensaje BA puede hacer uso nuevamente de su dirección HoA en su red local. Si el MN regresa a su red local antes de que haya expirado la validez de su dirección CoA, no debe utilizar el mecanismo DAD para evitar que se presente algún conflicto o confusión; de lo contrario el MN puede emplear este mecanismo sin ningún problema.

5. Adicionalmente el MN transmite un mensaje multicast NA para informar a todos los nodos de su red local que su dirección MAC ha cambiado y que ahora está asociada a su respectiva dirección HoA. El mensaje tiene las siguientes características: dirección HoA en el campo dirección objetivo, su dirección MAC en el campo dirección MAC destino.

6. El MN puede retransmitir el mensaje multicast NA en varias ocasiones para incrementar la confiabilidad de entrega de la información enviada a pesar de ello, es posible que durante un cierto lapso de tiempo (antes de que el HA acepte el mensaje BU) tanto el HA como el MN respondan a mensajes NS dirigidos a la dirección HoA del MN.

7. Algo similar sucede cuando el MN está utilizando la optimización de ruta, para ello necesita transmitir un mensaje BU desde su dirección HoA a la dirección del CN solicitándole que elimine la entrada correspondiente en su BC. Las características particulares para lograr esto son: su dirección HoA en el campo CoA y tiempo de vida en 0.

8. El CN al recibir el mensaje BU elimina la entrada respectiva de su BC, para finalmente mandar un mensaje BA a la dirección HoA del MN.

Es así como quedan concluidos los posibles movimientos que el MN llega a desarrollar en MIPv6 y a pesar de que se consideran varios casos, aún existen ciertos avances y cambios que se han hecho para mejorar la experiencia de movilidad (para más información remítase al capítulo 6).

Con todos los temas que se han tratado a lo largo de este capítulo ahora ya es más claro la ventaja que representa el uso de MIPv6 respecto a MIPv4 a pesar de ello, en la actualidad es más común encontrar la versión de IPv4 debido a que el uso masivo de IPv6 todavía tardará algunos años en llegar. Debido a que MIPv4 tiene más años de estudio e investigación las implementaciones que existen suelen tener más opciones, mismas que se conjugan en escenarios más completos y con mayor integración. Afortunadamente en los últimos meses las investigaciones y propuestas que se han hecho en torno a MIPv6 han sido muy intensas y eventos como el día mundial y el lanzamiento de IPv6 (llevados a cabo el 8 y el 6 de Junio del 2011 y 2012, respectivamente) auguran un mayor desarrollo de IPv6 y disminuyen la brecha para el día en que sea cada vez más común el encontrar implementaciones de MIPv6 (o alguna de sus mejoras).

# Capítulo 5

## Seguridad en MIPv6

*There are 10 types of people: those who understand binary and those who do not understand it. –Anonymous*

## 5.1 INTRODUCCIÓN

Al borde de una sociedad más demandante existen millones y millones de usuarios conectados a la Internet diariamente, algunos son personas que simplemente navegan en la red para subir sus fotos de Navidad a Facebook y otros son individuos con capacidades extraordinarias que pueden entrar de manera no autorizada a prácticamente cualquier red desde donde sea. Es así como la seguridad de la información se perfila como uno de los principales ejes que hay que considerar cada vez más en esta era digital, principalmente a través de la definición de políticas que restrinjan de manera cautelosa y minuciosa no solamente el acceso y uso de ciertos servicios, sino también el nivel de autorización al que los diferentes usuarios tienen derecho.

Si bien es cierto que IPv6 trata de ser más sencillo y seguro, es indudable que aún existen un sinfín de vulnerabilidades que son introducidas cada vez que se desarrolla un nuevo servicio, por ejemplo en el ambiente empresarial es más usual que empleados accedan a información privada de la empresa desde cualquier parte (a través de dispositivos inalámbricos) y para garantizar la seguridad, se necesitan desarrollar nuevas formas de protección. Definitivamente la seguridad resulta ser un elemento importante en la movilidad pues su objetivo es brindar privacidad, confidencialidad y autenticidad; en las siguientes secciones se explicarán algunas de las amenazas que enfrenta MIPv6.

## 5.2 AMENAZAS EN LAS COMUNICACIONES MÓVILES

Al estar los dispositivos móviles fuera de su red local es posible que sean más propensos a ataques porque ahí no cuentan con la protección de los dispositivos de su red y es necesario que implementen sus propias medidas de seguridad, por ejemplo: usando antivirus, algún tipo de firewall o filtrado, e incluso hasta un Sistema de Prevención de Intrusión de Host, HIPS por sus siglas en inglés (Host Intrusion Prevencion System) sin embargo, esto depende del tipo de dispositivo y de las capacidades que posea.

Las posibilidades ciertamente son infinitas cuando se habla de las consideraciones que se deben tomar en cuenta para proteger algún activo, no obstante existen ciertos enfoques fundamentales que deben ser supervisados y fortalecidos. A continuación se presentan algunas de las principales amenazas y consideraciones relacionadas con MIPv6:

- *Home Agent Falso:* la existencia de un HA falso configurado para realizar un ataque puede llegar a eliminar los mensajes del proceso Return Routability y forzar a que las comunicaciones del MN siempre se intercepten por este otro HA; debido a esta amenaza es urgente bloquear dicho nodo y analizar toda la infraestructura para conocer el impacto ocasionado y los dominios que fueron comprometidos.

- *Seguridad en el medio de comunicación:* el uso de MIPv6 generalmente implica el empleo de un medio de transmisión inalámbrico, lugar donde regularmente se tienen mayores debilidades (a menos de que exista una autenticación y se cifre el tráfico) por lo tanto, es importante considerar que cuando un MN se encuentra en una red foránea como un hotel o un hotspot, las posibilidades de que un atacante intercepte el tráfico son mayores, situación que deja vulnerable la señalización de MIPv6 a ser capturada por algún atacante.

- *Hombre en el Medio*, MITM por sus siglas en inglés (Man In The Middle): se desarrolla cuando existe un atacante lo suficientemente cerca del MN o del CN para capturar los mensajes intercambiados durante el proceso Return Routability: HoTI, HoT, CoTI y CoT. Con estos elementos el atacante fácilmente puede hacerse pasar por el CN o el MN, y enviar paquetes que parezcan venir de alguna de dichas entidades. Particularmente cuando el atacante no está tan cerca del MN o del CN simplemente puede obtener la mitad de la información requerida, por ejemplo al estar cerca del HA únicamente conseguiría los mensajes HoTI y HoT lo que claramente es insuficiente.

  Para que pueda realizarse un ataque de este tipo es necesario que el atacante tenga conocimiento de la dirección IPv6 de alguno de los siguientes elementos: CN, HA o MN, lo cual suele ser complicado a menos de que el atacante se ubique en la ruta por donde viajan los paquetes o esté muy cerca de alguno de dichos nodos. Un elemento más que agrega dificultad al desarrollo de este tipo de ataque es cuando el MN y el CN están en movimiento, situación que obstaculiza que el atacante pueda observar los paquetes intercambiados, a menos claro que dicho nodo también sea móvil.

- *Intercepción de conexión entre MN y CN:* este ataque se logra si el nodo malicioso está en la misma red que el MN y logra capturar su información de configuración, con esto el atacante puede mandar un mensaje BU simulando ser el MN (para informar que cambia su posición o en su defecto al desconectarse el MN de la red) e inclusive, es capaz de mandar nuevamente los mensajes HoTI y CoTI para forzar al CN a revelar sus tokens en la respuesta que envíe, y de esa manera confundirlo con nueva información. Para que este ataque funcione el mensaje BU del atacante debe llegar al CN antes de que se agote el tiempo de validez de la asociación respectiva; precisamente para limitar ataques de este tipo se define un tiempo de vida no muy largo para las entradas de la BC.

  Un atacante inclusive podría aprovechar la información que ya posee para infiltrarse en la red local del HA e intentar ganar acceso a los recursos de dicha

red. Considerando ese escenario es vital establecer dispositivos de seguridad como firewalls que permitan proteger a las redes de este tipo de ataques.

- *Intercepción de conexión entre MN y HA:* básicamente ocurre cuando un nodo malicioso crea asociaciones falsas con un HA con el objetivo de hacerle creer que es un MN válido pero, en realidad es un atacante. Las repercusiones que produce son peligrosas por ejemplo: una vez que se crea una asociación falsa el atacante puede redirigir hacia si mismo el tráfico destinado a un cierto MN y posteriormente renviárselo a dicho móvil sin que éste último tenga conocimiento de lo acontecido. El atacante logra esto fingiendo ser el MN y enviando un mensaje BU al HA respectivo informándole de su nueva dirección CoA (dirección del atacante), si el HA no autentica al MN simplemente aceptará dicha información y regresará un mensaje BA, con lo cual en un par de segundos el atacante logra su objetivo.

- *Ataques de Denegación de Servicio*, DoS por sus siglas en inglés (Denial of Service): un atacante puede impedir que todos los MNs que necesiten utilizar el soporte de MIPv6 no puedan establecer una comunicación con el HA. Para lograrlo el atacante realiza un envío excesivo de mensajes BU dirigidos al HA, con ello este último necesita utilizar cierto porcentaje de sus recursos para procesar los mensajes de movilidad que recibe, y al experimentar una gran demanda el HA paulatinamente llega a su punto límite y comienza a desechar todos los mensajes que recibe o incluso deja de funcionar completamente.

  El atacante puede realizar algo similar en contra del MN al enviar mensajes ICMPv6 con anuncios de prefijo falsos, de esta forma el MN confunde la información real con la falsa y se suscitan fallas en sus comunicaciones. Otro caso ocurre cuando el atacante se hace pasar por cierto MN con el que algún CN desee comunicarse, de manera que el atacante aprovecha esa situación y manda demasiadas peticiones o paquetes al CN, llegando hasta el punto donde este último agota toda su capacidad de procesamiento y es incapaz de mantener el resto de sus comunicaciones.

## 5.3 CONTRAMEDIDAS DE SEGURIDAD

Ante la presencia de todas las amenazas existentes (o al menos las más conocidas) no se debe tomar a la ligera la seguridad en las comunicaciones móviles, por lo tanto habrá que tomar e implementar ciertas medidas para proteger cada una de las conexiones que establezcan los usuarios móviles. Algunos de los elementos que permiten desarrollar dicha tarea se tratan a continuación.

### 5.3.1 FILTRADO DE MENSAJES

Una manera de prevenir posibles ataques en MIPv6 es el uso de Listas de Control de Acceso, ACL por sus siglas en inglés (Access Control Lists) [22], las cuales se pueden implementar para filtrar paquetes indeseables o peligrosos a fin de permitir que sólo cierto tráfico sea intercambiado entre el HA, MN y CN.

El filtrado de mensajes de MIPv6 tiene el propósito de crear un conjunto de reglas que permitan a dicho protocolo operar de la manera más segura posible y al mismo tiempo mantener satisfactoriamente las comunicaciones. Estas reglas están enfocadas principalmente al tráfico de señalización y a la información transmitida en las comunicaciones de los dispositivos participantes.

El mayor desafío que presenta esta opción es crear un modelo de seguridad que pueda lidiar con dispositivos móviles que cambian su ubicación física con suma facilidad. Claramente la existencia de un dispositivo de administración central resulta bastante complejo puesto que esto implica agregar más dispositivos que entiendan los mensajes de MIPv6a, además de ello se requiere contemplar que cada organización implementa sus propias políticas de seguridad, lo que conlleva a tener diferentes esquemas de permiso y denegación del tráfico, por ejemplo para aquellos lugares donde no se permita el uso de MIPv6 o no se tenga contemplada su implementación, se debe filtrar todo ese tipo de tráfico y rechazar cualquier mensaje que contenga los encabezados de extensión correspondientes (véase la tabla 5.1).

Tabla 5.1 Consideraciones de filtrado en MIPv6

| Mensaje | Descripción |
|---|---|
| Encabezado de Enrutamiento Tipo 2<br>Siguiente Encabezado: 43 | Para mayor seguridad se recomienda filtrar el encabezado tipo 0, previniendo problemas de ataques source-routing. Para evitar crear riesgos de seguridad en la red local el encabezado tipo 2 sólo debe ser permitido en los HAs asignados y de CNs autorizados. |
| Encabezado de Opciones de Destino: Home Address<br>Siguiente Encabezado: 201 | Para el funcionamiento de la comunicación directa entre el MN y el CN debe permitirse este tipo de tráfico en el firewall de la red foránea. |
| Encabezado de Movilidad<br>Siguiente Encabezado: 135 | Es vital en el funcionamiento de MIPv6 ya que transporta la mayoría de los mensajes de señalización. |
| Descubrimiento Automático de Home Agent. Encabezados ICMPv6: 144, 145 | Al no estar utilizando MIPv6 es recomendable filtrar este tipo de mensajes ICMPv6 (tal como se describe en el RFC 4890) sin embargo, al estar usando MIPv6 se deben permitir para que el MN conozca cierta información de su red local, tal como la dirección de su HA y el prefijo de movilidad respectivo. |
| Descubrimiento de Prefijo de Movilidad. Encabezados ICMPv6: 146, 147 | |

Además del reto de mantener una administración de las ACLs también es importante considerar que la propia naturaleza de éstas sólo permite encontrar en cada mensaje una coincidencia regla-tipo, es decir, no se puede configurar una regla que busque simultáneamente tanto en el encabezado IPv6 como en un encabezado de extensión, por lo cual no es posible que para un mismo paquete se encuentre una coincidencia de varios encabezados. Esto sin duda dificulta el diseño y la creación de las reglas, debiendo escribir primero los casos más específicos y posteriormente los más generales.

Otra opción contempla distribuir la tarea de filtrado entre varios elementos, cada uno empleando las reglas necesarias para distinguir los mensajes de MIPv6, situación que se traduce en un mejor control y una mayor flexibilidad en el nivel de seguridad que requiere cada organización. Los elementos donde es posible realizar la tarea de filtrado son:

a. CN: debido a que este nodo puede o no tener soporte de MIPv6 las implicaciones de filtrado varían, se depende sobre todo de las políticas de seguridad implementadas en la red donde se encuentra porque es posible que el tráfico de MIPv6 no sea permitido. Debido a tales implicaciones en la mayoría de los casos no se necesita de un filtrado propiamente en el CN, más bien son los mecanismos de su red los que habrá que configurar apropiadamente.

b. MN: así como la red foránea no está consciente de la presencia de MNs, un MN también desconoce si la red foránea donde se encuentra permite el funcionamiento de MIPv6, por ejemplo: si no se permite la negociación IKE entre el HA y el MN no es posible formar de manera segura la entrada en la BC, o simplemente el usar NAT imposibilitaría las comunicaciones. Específicamente para el MN una opción es usar un Agente de Seguridad, de manera que por sí mismo el MN es capaz de filtrar conexiones indeseables y por lo tanto puede protegerse de atacantes hostiles.

c. HA: resulta un dispositivo de gran interés pues a través del él se pueden evitar ciertos ataques hacia los MNs y además se llegan a prevenir con relativa facilidad posibles riesgos de seguridad, por ejemplo: evitar asociaciones de MNs falsos o identificar la existencia de algún HA falso en la red. Para lograr esto se deben desarrollar actividades como: monitorear el estado del HA, conocer la actividad de sus asociaciones, determinar el tráfico dirigido desde/hacia los MNs, etc.

   Dada la importancia del HA en el funcionamiento de MIPv6 habrá que administrar y usar sus recursos de la mejor manera, tratando de garantizar que pueda cumplir correctamente con sus funciones y evitando que se llegue a sobrecargar por lo tanto, se necesita reducir el número máximo de entradas permitidas en la BC,

limitar la cantidad de memoria utilizada en MIPv6, definir un tiempo de vida en la validez de los registros, etc. La tabla 5.2 muestra los mensajes que se necesitan permitir, por ejemplo una configuración de ACLs para desarrollar un correcto funcionamiento de MIPv6 en el HA.

Tabla 5.2 Ejemplo de configuración de ACLs para el filtrado de mensajes MIPv6 [22]

| Tráfico de entrada | Tráfico de salida |
|---|---|
| remark Permitir SSH<br>permit tcp any any eq 22 | |
| remark Permitir ping6<br>permit icmp any any echo-request<br>permit icmp any any echo-reply | |
| remark Permitir otros mensajes ICMPv6<br>permit icmp any any 1<br>permit icmp any any 2<br>permit icmp any any 3<br>permit icmp any any 4<br>permit icmp any any nd-na<br>permit icmp any any nd-ns | |
| remark Permitir Anuncios/Solicitudes de Ruteador<br>permit icmp any any router-advertisement<br>permit icmp any any router-solicitation | |
| remark Permitir IKE y ESP en modo transporte | |
| permit udp host <CoA> host <HA> eq isakmp<br>permit esp host <CoA> host <HA> | permit udp host <HA> host <CoA> eq isakmp<br>permit esp host <HA> host <CoA> |
| remark Permitir BU de MN a HA<br>permit ipv6 host <CoA> host <HA> mobility-type bind-update<br>permit ipv6 host <CoA> host <HA> dest-option-type home-address | remark Permitir BA de HA a MN<br>permit ipv6 host <HA> host <CoA> mobility-type bind-acknowledgement<br>permit ipv6 host <HA> host <CoA> routing-type 2 |
| remark Permitir Descubrimiento de HA | |
| permit icmp host <HA> host <CoA> dhaad-request | permit icmp host <HA> host <CoA> dhaad-reply |
| remark Permitir Descubrimiento de prefijo de HA | |
| permit icmp host <CoA> host <HA> mpd-solicitation<br>permit ipv6 host <CoA> host <HA> dest-option-type home-address | permit icmp host <HA> host <CoA> mpd-advertisement<br>permit ipv6 host <HA> host <CoA> routing-type 2 |
| remark Permitir BU de MN a CN<br>permit ipv6 host <CoA> host <CN> mobility-type bind-update<br>permit ipv6 host <CoA> host <CN> dest-option-type home-address | remark Permitir BA de CN a MN<br>permit ipv6 host <CN> host <CoA> mobility-type bind-acknowledgement<br>permit ipv6 host <CN> host <CoA> routing-type 2 |
| remark Permitir paquetes de MN a través de HA | |

| | |
|---|---|
| permit ipv6 host <HoA> host <CN> | permit ipv6 host <CN> host <HoA> |
| remark Permitir procedimiento RR | |
| permit ipv6 host <HoA> host <CN> mobility-type hoti<br>permit ipv6 host <CoA> host <CN> mobility-type coti | permit ipv6 host <CN> host <CoA> mobility-type bind-acknowledgement<br>permit ipv6 host <CN> host <CoA> routing-type 2 |
| remark Permitir optimización de ruta | |
| permit ipv6 host <CoA> host <CN> dest-option-type home-address | permit ipv6 host <CN> host <CoA> routing-type 2 |
| remark Bloquear el resto de los paquetes IPv6<br>deny ipv6 any any log | |

### 5.3.2 PROTOCOLO DE AUTENTICACIÓN PARA MIPV6

En ocasiones en algunas redes no es deseable hacer uso de IPSec (solución que se explicará más adelante) o simplemente no se puede emplear, por lo que una alternativa a considerar es utilizar la opción de Autenticación para MIPv6 (véase el RFC 4285 [23]). Básicamente lo que se hace es proteger el envío y recepción de los mensajes BU y BA entre un MN y su HA, además esta opción está contenida en dichos mensajes por lo que no se requieren definir nuevos encabezados. Principalmente se suele emplear la Autenticación para MIPv6 en ambientes con las siguientes características:

- Redes donde el MN forzosamente debe interactuar con algún servidor AAA para tener acceso al servicio de red.
- Redes donde se pretende minimizar el envío de mensajes de señalización.
- El MN de manera dinámica adquiere su HA y su respectiva dirección HoA.
- El MN o el HA soportan el uso de servidores AAA.

El MN necesita poseer los siguientes elementos: una llave compartida (adquirida estáticamente o creada dinámicamente), un SPI, un algoritmo de autenticación (SHA1) y un mecanismo de protección anti-respuesta (mediante la opción Timestamp o por el campo Número de Secuencia); al reunir todos estos elementos el MN puede autenticarse con su HA o con algún servidor local de Autenticación (AAA) no obstante, existe una limitante en su empleo ya que no provee confidencialidad para los mensajes intercambiados en el proceso Return Routabilty ni autenticación o integridad al usar el Descubrimiento de Prefijo de Movilidad.

En la figura 5.1 se aprecian los mensajes involucrados en el registro del MN y la forma en que éste interactúa para registrarse con su HA o con algún servidor local AAA. Para entender este proceso se comenzará por explicar la opción de Identificación:

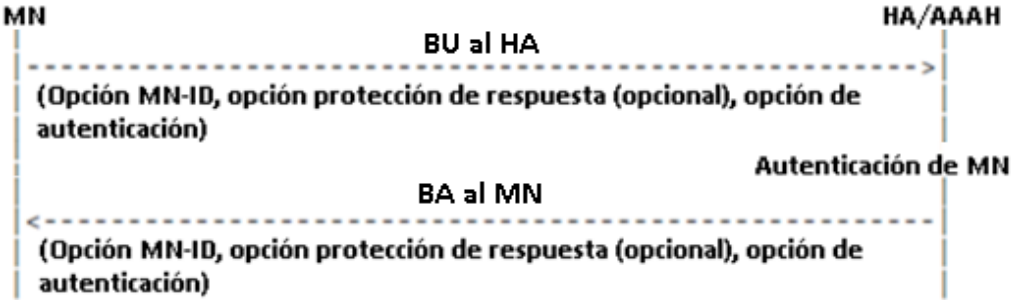



Figura 5.1 "Home Registration" con el protocolo de Autenticación para MIPv6

El MN en el encabezado de Movilidad incluye una opción denominada Identificador de Nodo Móvil, MNI por sus siglas en inglés (Mobile Node Identifier), dicho elemento está definido en el RFC 4283 [24] y es usado por el MN para identificarse consigo mismo y autenticarse con su HA para lograr registrarse exitosamente. Esta opción proporciona una mayor flexibilidad porque el MN puede o no tener configurado desde un inicio una dirección IPv6 (HoA) en su red local, pudiéndola llegar a adquirir más tarde de manera dinámica. Se muestra el encabezado del MNI en la figura 5.2.

| | Tipo de opción | Longitud de opción |
|---|---|---|
| Subtipo | Identificador | |

Figura 5.2 Formato de opción de Identificador de Nodo Móvil

Donde:
Tipo de opción (8 bits): 8 es el valor asignado por la IANA.
Longitud de opción (8 bits): longitud de los campos Identificador y Subtipo
Subtipo (8 bits): tipo específico de identificador a usar
Identificador (variable): contiene la opción especificada en el campo Subtipo.

Un ejemplo de este tipo de identificador es el Identificador de Acceso a la Red, NAI por sus siglas en inglés (Network Access Identifier) definido en el RFC 4282 [25]. Para el caso de MIPv6 la opción MN-NAI es usada por el MN para identificarse así mismo y con los demás, por ejemplo un MN podría identificarse como: netlab@dgtic.unam.mx.

Por otro lado es importante considerar que el uso permanante de un identificador puede comprometer la privacidad de los usuarios, mantener un mismo identificador durante cierto tiempo facilita que los atacantes logren rastrear la ubicación actual de un móvil; aun así esta vulnerabilidad sólo existe cuando el MN va a registrarse por primera vez con su HA (en los registros posteriores el MN puede usar su dirección HoA asignada), además es posible contrarrestar esta vulnerabilidad al hacer uso de mecanismos como los siguientes:

- ⇒ Cifrado del tráfico en la capa de enlace: permite proteger la privacidad de los mensajes del MN de aquellos nodos que estén en ese mismo segmento de red.
- ⇒ Cifrado del paquete completo: uso de IPSec.
- ⇒ Uso de un pseudónimo temporal como identificador.

En lo que respecta a la opción de autenticación (figura 5.3), cuando se desea hacer uso de ésta es posible que en un mensaje puedan existir diferentes alternativas de autenticación, cada una con distintos valores del campo subtipo a pesar de ello, siempre se debe respetar el siguiente orden de opciones de autenticación: primero aparece MN-HA y después MN-AAAH, por sus siglas en inglés (AAA server in Home Network).

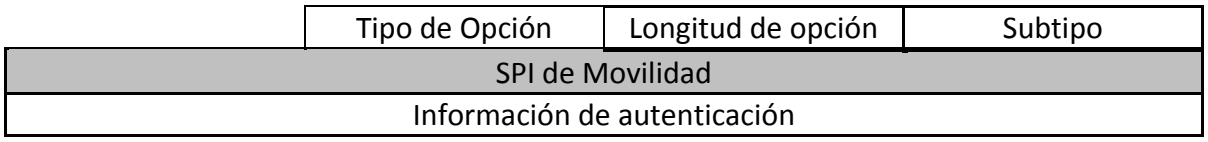



Figura 5.3 Formato de opción de Autenticación

Donde:
Tipo de opción (8 bits): 9 es el valor asignado por la IANA.
Longitud de opción (8 bits): longitud de los campos subtipo, SPI e información de autenticación.
Subtipo (8 bits): identifica el mecanismo que se usará para autenticar el mensaje.
SPI de Movilidad (32 bits): Índice del Parámetro de Seguridad de Movilidad.
Información de autenticación (variable): contiene los datos para autenticar el mensaje.

En cuanto a los subtipos de autenticación actualmente existen los siguientes:

- *Autenticación con el HA:* posee un valor de 1 en el campo subtipo y ayuda al HA en la autenticación AAAH. Este subtipo lo usa el HA cuando manda algún mensaje BA aunque, también puede ser empleado por el MN cuando envía un mensaje BU.

- *Autenticación con el servidor AAA de la red local (AAAH):* posee un valor de 2 en el campo subtipo y el MN puede usarlo en los mensajes BU que transmita.

No solamente se usa el campo Número de Secuencia del mensaje BU, también se puede emplear la opción Protección Anti-respuesta cuando el HA no mantiene información del MN una vez que ha eliminado la entrada correspondiente; situación que suele ser muy frecuente cuando el MN se registra con varios HAs (es poco eficiente que cada HA guarde toda esa información que ya no le es útil). Específicamente el campo de la opción Protección Anti-Respuesta le permite al HA verificar que el mensaje BU ha sido generado recientemente por el MN y que no se trata de algún atacante que intenta usar mensajes previos enviados por parte de dicho móvil. Cuando el HA recibe el mensaje BU verifica primero este campo y posteriormente lo autentica, si el proceso es exitoso el HA manda un mensaje BA que contenga dicho campo para facilitarle al MN relacionar la respuesta recibida con el mensaje BU que envió con anterioridad. En la figura 5.4 se encuentra el encabezado de la opción Protección Anti-respuesta.

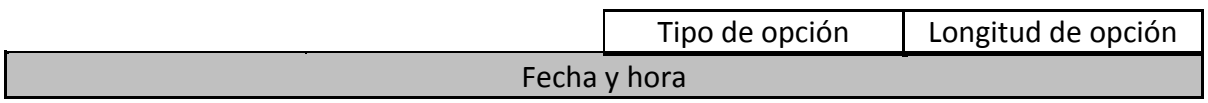



Figura 5.4 Formato de opción de Protección Anti-respuesta

Donde:
Tipo de opción (8 bits): 10 es el valor asignado por la IANA
Longitud de opción (8 bits): longitud del campo Fecha y hora.
Fecha y hora (64 bits): contiene la fecha y hora en que se envía el mensaje.

Fecha y hora es el campo más representativo y está formado de 2 partes, los últimos 32 bits representan los segundos y los primeros 32 bits se generan aleatoriamente. Este campo contiene la hora actual del MN en la que se genera el mensaje BU, de esta manera cuando el HA lo recibe verifica que dicho valor sea muy cercano a su hora actual: la diferencia existente por defecto no debe ser mayor a 7[s]; de cumplirse esta condición el HA copia dicho campo en el mensaje BA, de lo contrario el HA copia los últimos 32 bits del campo Fecha y hora del mensaje BU mientras que los primeros 32 bits corresponden a su hora actual. Finalmente el HA manda el mensaje BA al MN y este último al recibirlo conoce si el registro fue o no exitoso.

### 5.3.3 IPSEC

La seguridad no ha sido siempre una de las principales preocupaciones y por ello no fue considerada durante el desarrollo del IPv4, afortunadamente fue tomada en cuenta para IPv6 como un elemento importante, con la finalidad de hacer más seguras las comunicaciones de extremo a extremo y tras muchos esfuerzos conjuntos se planteó un protocolo que trabajara en la capa de red: Protocolo de Seguridad de Internet, IPSec por sus siglas en inglés (Internet Protocol Security). IPSec está definido en el RFC 4301 [26] y puede ser implementarlo en un host, gateway o cualquier otro dispositivo, de manera que al utilizarlo entre el HA y el MN la mayoría de los mensajes intercambiados entre estas entidades quedan reducidos a entradas de IKE y ESP porque el resto de los mensajes están contenidos dentro de un túnel seguro. Particularmente IPSec juega un papel importante en MIPv6 pues además de crear un entorno seguro de comunicación también optimiza el uso de recursos y las tareas administrativas (se reducen considerablemente las reglas definidas); a pesar de ello también trae consigo desventajas, por lo cual habrá que estar seguros de que sea la opción correcta de acuerdo a las necesidades de cada persona o empresa. A continuación se plantea la información más sobresaliente de IPSec para entender mejor su papel en las comunicaciones de MIPv6.

#### 5.3.3.1 ENCABEZADOS Y MODOS DE OPERACIÓN

Antes que nada es necesario comprender que IPSec no resuelve la cuestión de la seguridad y no es a prueba de todo, incluso utilizarlo en determinadas circunstancias puede llegar a dificultar tareas como el monitoreo de la red, análisis forense y la resolución de diversos problemas; todo esto depende del tipo de tráfico donde se use, de ahí la importancia de plantear correctamente que las políticas de seguridad vayan acorde

a mejorar la seguridad y no a entorpecer el resto de las operaciones de la red. IPSec para proveer servicios de seguridad (tanto en IPv4 como en IPv6) utiliza 2 encabezados: Encabezado de Autenticación, AH por sus siglas en inglés (Authentication Header) y Carga de Seguridad de Encapsulamiento, ESP por sus siglas en inglés (Encapsulating Security Payload, inclusive se pueden usar ambos para proveer un nivel más robusto de seguridad, quedando a consideración de los requerimientos que se necesiten. Se definen en la tabla 5.3 los servicios de cada uno de estos encabezados.

Tabla 5.3 Comparación de AH y ESP

| Servicio de seguridad | ESP | AH |
|---|---|---|
| *Control de acceso*: previene el uso no autorizado de recursos, garantizando que sólo accedan los usuarios con los permisos suficientes. | x | x |
| *Integridad*: verifica que los datos no se hayan modificado o corrompido, recibiéndose tal y como fueron enviados originalmente. | x | x |
| *Autenticación*: comprueba la procedencia de la información para garantizar la identidad del remitente.<br>ESP: indirectamente realiza esta función al verificar la integridad de la identidad del otro nodo.<br>AH: puede autenticar la mayor parte del encabezado IP. | x | x |
| *Protección Anti-Repuesta*: asegura que una transacción sólo se realiza una vez, a menos que se autorice una repetición de ésta.<br>ESP: integridad parcial de Número de Secuencia Extendido. No se negocia.<br>AH: uso del campo Número de Secuencia. | x | x |
| *Confidencialidad*: la información sólo es entendible por entidades autorizadas, asegurando la privacidad de la comunicación. Se hace uso de algoritmos de cifrado para proporcionar la protección requerida. | x | |

Se presenta la descripción de los correspondientes encabezados usados en IPSec:

a) ESP está definido en el RFC 4303 [27] y se reconoce porque el campo "Siguiente Encabezado" tiene un valor asociado de 50. Su encabezado está en la figura 5.5.

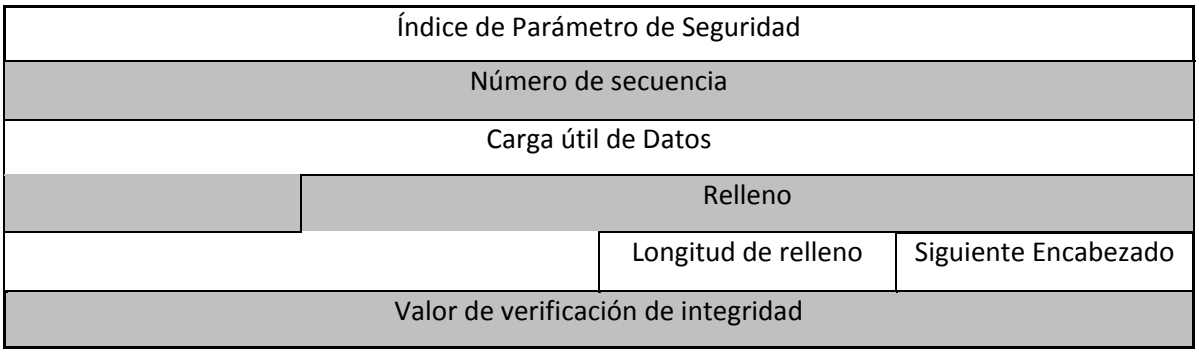



Figura 5.5 Encabezado de ESP

Donde:

Índice de Parámetro de Seguridad (32 bits): ayuda al receptor a identificar la Asociación de Seguridad relacionada con los paquetes de entrada.
Número de Secuencia (32 bits): contador que se incrementa en uno al enviar un paquete.
Carga útil (variable): contiene información a utilizar por ESP.
Relleno (0-255 bits): su longitud varía para asegurar que se cumpla con el numero de bits necesarios para formar el bloque de cifrado correspondiente.
Longitud de relleno (8 bits): indica el número de bits usados como relleno.
Siguiente Encabezado (8 bits): señala el tipo de información de la carga útil.
Valor de verificación de integridad, ICV por sus siglas en inglés (Integrity Check Value): valor opcional de longitud variable usado para proveer una forma adicional de integridad.

b) AH se define en el RFC 4302 [28] y al emplearlo el campo "Encabezado Siguiente" posee un valor asociado de 51. Su encabezado se observa en la figura 5.6.

| Siguiente Encabezado | Longitud de Carga Útil | Reservado |
|---|---|---|
| Índice de Parámetro de Seguridad | | |
| Número de secuencia | | |
| Valor de verificación de integridad | | |

Figura 5.6 Encabezado de AH

Donde:
Siguiente Encabezado (8 bits): define el tipo de carga útil que se encuentra después del encabezado de Autenticación.
Longitud de Carga Útil (8 bits): indica la longitud del Encabezado de Autenticación.
Reservad (16 bits): reservado para uso futuro.
Índice de Parámetro de Seguridad (32 bits): usado por el receptor para identificar la Asociación de Seguridad relacionada con los paquetes de entrada.
Número de secuencia (32 bits): contador que se incrementa en uno al enviar un paquete.
Valor de verificación de integridad (variable): provee una forma adicional de integridad.

Para AH y ESP existen 2 modos de uso: transporte, usado frecuentemente para brindar protección a protocolos de capa superior; y túnel, emplearlo provoca que los paquetes utilicen túneles IP (a través de un encabezado IP externo e interno). Se presenta a continuación una explicación de cada modo para mejorar la comprensión de su uso y características:

1. *Modo Transporte:* se caracteriza por no realizar modificaciones al encabezado IP y generalmente es empleado en una comunicación extremo a extremo, es decir, se implementa entre 2 nodos finales de comunicación. Particularmente el encabezado ESP se coloca después del encabezado principal de IPv6 y el cifrado comprende a todos los encabezados del paquete que aparecen a continuación, y opcionalmente (al brindar autenticación al mismo tiempo) el campo trailer ESP. Por su parte el uso del Encabezado AH implica la autenticación completa del paquete (incluyendo el encabezado principal de IPv6). La figura 5.7 ilustra los alcances antes mencionados.

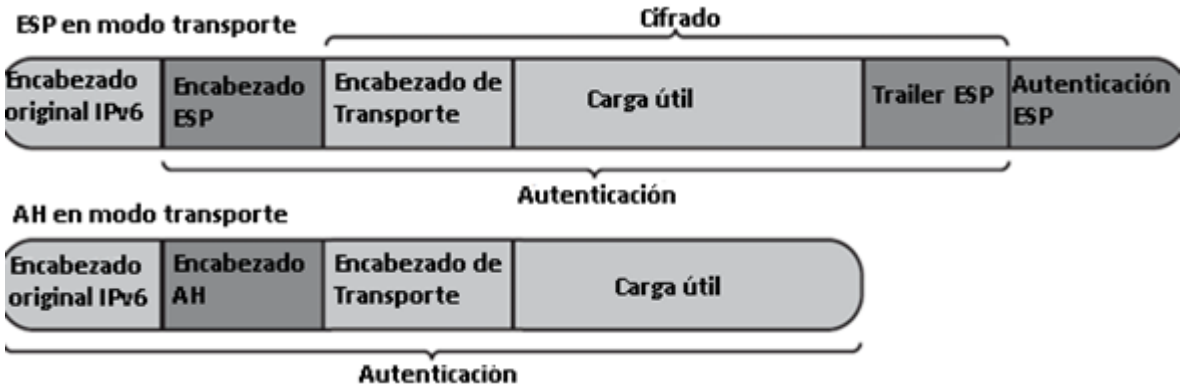



Figura 5.7 Modo Transporte de IPSec

2. *Modo Túnel:* en una comunicación entre nodos finales en algún punto de la ruta que siguen los paquetes se crea un túnel entre 2 nodos intermediarios (comúnmente denominados Gateways de Seguridad), los cuales representan los extremos finales en el uso de IPSec pero, sin ser los puntos finales de la comunicación, para esto se encapsula el encabezado IP del paquete original en un encabezado IP externo. Para IPv6 se coloca en un inicio un nuevo encabezado IPv6, posteriormente se encuentra el encabezado ESP y le sigue el encabezado original de IPv6, a partir de este último se comienza el cifrado hasta el campo trailer ESP (ubicado después del contenido del protocolo de capa superior). Al usar también el servicio de autenticación al final se incluye el campo de Autenticación ESP. Por su parte el Encabezado AH se coloca entre los encabezados IPv6 (nuevo y original) y es capaz de autenticar todo el contenido del paquete (figura 5.8).

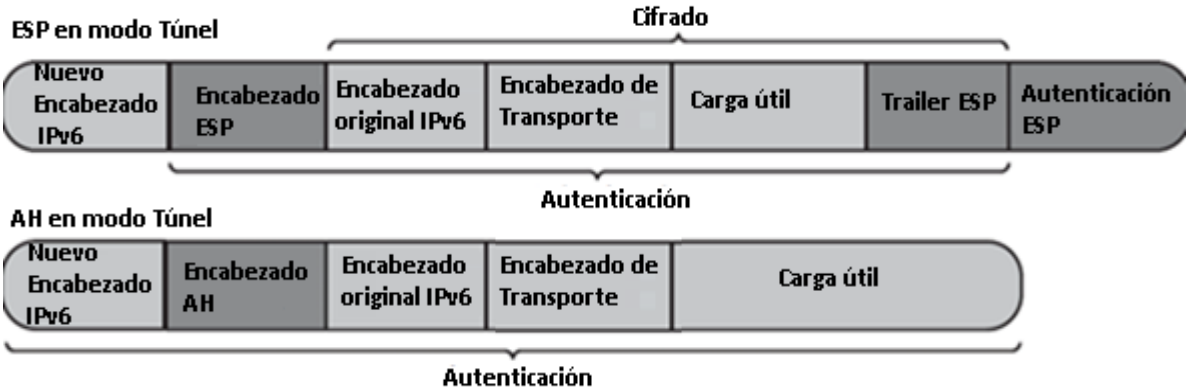



Figura 5.8 Modo Túnel de IPSec

### 5.3.3.2 ASOCIACIONES DE SEGURIDAD

Una parte fundamental para el funcionamiento de IPSec corresponde a las Asociaciones de Seguridad, SAs por sus siglas en inglés (Security Associations), a través de éstas se establecen una serie de servicios de seguridad (según se esté utilizando ESP o AH) en la transmisión de información, por ejemplo: a pesar de que tanto ESP como AH ofrecen

integridad y autenticación, el servicio es aplicado a distintas partes del paquete dependiendo del modo que se esté usando. Por medio de una SA definimos los encabezados de IPSec a usar, las transformaciones a realizar, las llaves empleadas y la validez de las mismas. En lo que concierne a su administración se presentan tareas de creación, modificación y eliminación, asunto que es importante tomar en cuenta porque una SA es unidireccional, por ejemplo cada entidad implicada en IPSec para un tráfico C debe tener dos SAs: una para entrada y otra para salida.

#### 5.3.3.3 BASES DE DATOS

Además de las SAs también es necesario que las entidades que participan en IPSec posean ciertas estructuras de datos para almacenar información crucial de cada uno de los eventos que acontecen. Actualmente las bases de datos que existen son:

- *Base de Datos de Asociación de Seguridad*, SAD por sus siglas en inglés (Security Association Database): es la encargada de mantener información sobre las SAs existentes. Se muestra en la tabla 5.4 los elementos que la componen.

Tabla 5.4 Elementos de SAD

| Parámetro | Descripción |
|---|---|
| Contador de Número de Secuencia | Valor de 64 bits usado para generar un número de secuencia para los paquetes que tienen encabezados ESP y AH. |
| Contador de sobre-flujo del Número de Secuencia | En caso de un sobre-flujo se genera un evento donde se registra que se deben prevenir transmisiones de paquetes adicionales para una cierta SA. |
| Ventana de Anti-Réplica | Determina si ciertos paquetes con encabezados AH o ESP están siendo retransmitidos por algún host sospechoso. |
| Tiempo de vida | Tiempo de validez de cada SA y su respectivo SPI. También indica la acción a realizar. |
| Modo de transporte | Específica si se emplea el modo Transporte, Túnel o si es indistinto el uso de alguno en particular. |
| Destino del túnel | Usado en modo túnel para indicar la dirección IP destino del nuevo encabezado. |
| Parámetros PMTU | Indica el Path MTU y sus variables asociadas. |
| Índice de Parámetro de Seguridad | Relaciona el tráfico de entrada a una SA.<br>En tráfico de salida ayuda a construir el encabezado ESP o AH. |
| Parámetros de AH | Implica información del algoritmo de autenticación, llaves, etc. |
| Parámetros de ESP | Informa sobre el algoritmo de cifrado y autenticación así como sus llaves respectivas y el modo que se emplea. |
| Verificación de fragmentación | Bandera que indica si se verifica o no la fragmentación para una cierta SA. |

- *Base de Datos de Políticas de Seguridad*, SPD por sus siglas en inglés (Security Policy Database): para cada comunicación existe una política de seguridad que indica la acción a realizar, es decir, todos los paquetes (enviados/recibidos) se comparan con esta base de datos para saber que hacer con ellos: los paquetes viajan protegidos (usan servicios de seguridad), se descartan (no están permitidos) o se les permite el paso (no emplean IPSec). La SPD define una pareja de entradas para un cierto tráfico (ingreso y egreso), la tabla 5.5 muestra los elementos que la conforman.

Tabla 5.5 Elementos de SPD

| Campo | Descripción |
|---|---|
| Nombre | Identificador simbólico para una dirección remota o local. |
| PFP | Banderas que indican la dirección y puerto locales o remotos, así como el protocolo de la capa superior. |
| Selector(es) | Define la condición para aplicar una acción en particular. |
| Información de procesamiento | Contempla las siguientes tareas: permitir, descartar, proteger (se indica modo y protocolo de IPSec, algoritmos, etc.) |

- *Base de Datos de Autorización de Par*, PAD por sus siglas en inglés (Peer Authorization Database): algunas de sus funciones incluyen identificar a los grupos de pares autorizados para comunicarse con la entidad presente, así como definir el protocolo y método de autenticación a usar con cada par. Para realizar sus funciones la PAD contiene entradas que permiten enlazar la SPD con el protocolo de administración de las SAS que se vaya a emplear, es decir, sólo se puede usar la PAD cuando se trabaja con un protocolo de Administración Dinámica de Llaves; sus elementos se presentan en la tabla 5.6.

Tabla 5.6 Elementos de PAD

| Campo | Descripción |
|---|---|
| Identificador | Utilizado para diferenciar a cada par o grupo de pares relacionados. |
| Protocolo de Autenticación | Específica el protocolo de autenticación a usar, por ejemplo: IKE1, IKEv2, etc. |
| Método de Autenticación | Define los elementos a utilizar en la tarea de autenticación, por ejemplo: secretos compartidos, certificados, etc. |
| Información de Autenticación | Contiene los datos que se emplean para validar al par con que se van a establecer una comunicación. |

### 5.3.3.4 GESTIÓN DE LLAVES

Ya que a través de las llaves de IPSec se establece un medio seguro de comunicación, resulta importante administrarlas correctamente, precisamente esta tarea fundamental se puede desarrollar de 2 formas:

- *Manual:* para cada entidad implicada en IPSec se realiza una configuración manual de las llaves y de la información concerniente a las SAs, por esta razón sólo es recomendable su uso en ambientes estáticos y pequeños donde no se tengan planes inmediatos de expansión y únicamente se cuente con un dominio de administración. Adicionalmente es aconsejable usar IPSec únicamente para ciertos tipos de tráfico en particular a fin de no sobrecargar el uso de la red.

- *Automática:* es pensado en ambientes amplios porque puede generar múltiples llaves para una sola SA, cuestión que facilita el uso de distintos servicios de seguridad. Especialmente para este tipo de gestión se recomienda emplear IKEv2.

  El Intercambio de Llaves de Internet, IKE por sus siglas en inglés (Internet Key Exchange) se define en el RFC 5996 [29] y básicamente es un protocolo que ofrece servicios de seguridad y que autentica dos entidades. Específicamente IKE permite llevar a cabo de manera dinámica la negociación, establecimiento y mantenimiento de las SAs (protocolos, algoritmos, generación de claves de cifrado y autenticación). IKEv2 ha comenzado a remplazar a IKEv1 (son incompatibles) ya que posee varias mejoras:

  - Soporta al Protocolo de Autenticación Extensible, EAP por sus siglas en inglés (Extension Authentication Protocol) y Extensiones de Movilidad y Multihoming, MOBIKE por sus siglas en inglés (IKEv2 Mobility and Multihoming Protocol).
  - Reduce la complejidad y latencia de los mensajes de señalización.
  - Al simplificar el intercambio de mensajes ayuda a mejorar la flexibilidad y permite tener un mejor control y protección contra ataques DoS.

IKE es un mecanismo de acuerdo punto a punto, es útil para establecer una SA y autenticar tanto a la entidad que inicia la conversación como a la entidad que responde. Fundamentalmente se produce el intercambio de los siguientes pares de mensajes:

1) En el primer intercambio de mensajes (IKE_SA_INIT) se negocian los parámetros de seguridad que se usarán para proteger el resto de los mensajes (figura 5.9).

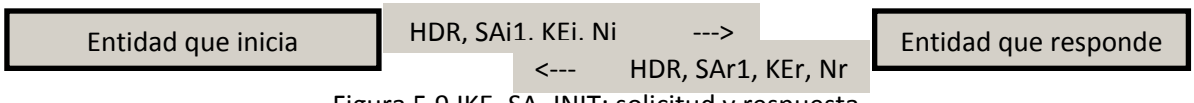



Figura 5.9 IKE_SA_INIT: solicitud y respuesta

Donde:
HDR: contiene SPI y número de versión.
SAi1: informa los algoritmos de cifrado que soporta.
KEi: valor Diffie-Hellman a usar.
Ni: contiene un valor aleatorio

HDR: contiene SPI y número de versión.
SAr1: informa los algoritmos de cifrado elegidos.
KEr: completa el intercambio Diffie-Hellman.
Nr: contiene un valor aleatorio.

2) En el segundo intercambio (IKE_AUTH) se realiza el intercambio de identidades y certificados para autenticar los mensajes anteriores, además se configura la primer SA para ESP o AH (Child SA). Estos mensajes están cifrados porque se usan las llaves intercambiadas en el primer par de mensajes (figura 5.10).

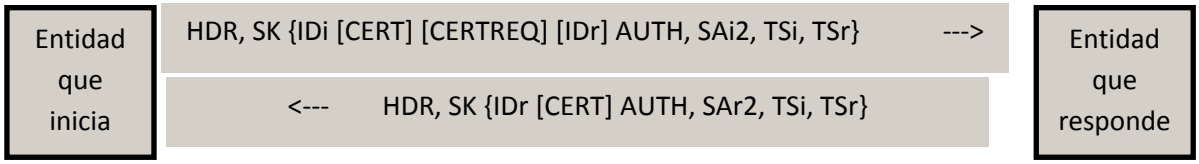



Figura 5.10 IKE_AUTH: solicitud y respuesta

Donde:
IDi: da a conocer su identidad.
AUTH: permite proteger el contenido del mensaje.
CERT: envío de sus certificados.
CERTREQ: lista las entidades de su confianza.
IDr: específica la identidad con a la que desea comunicarse.
SAi2: comienza negociación de Child SA.
TSi: contiene primer selector de tráfico (dirección IP origen y rangos de puertos).
TSr: contiene segundo selector de tráfico.

IDr: identidad con que se identifica.
ERT: contiene sus certificados.
AUTH: autentica su identidad.
SAr2: completa la negociación de Child SA.

3) Los siguientes intercambios (CREATE_CHILD) crean una Child SA (figura 5.11).

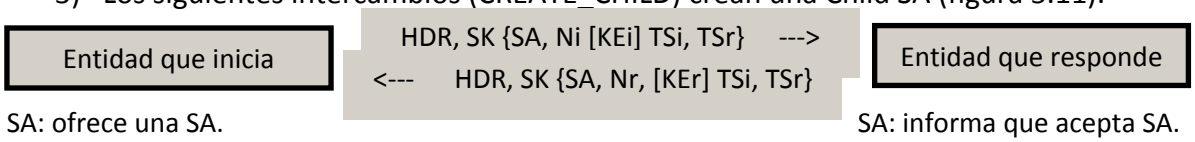



Figura 5.11 Child SA: solicitud y respuesta

Ocasionalmente se suelen presentar intercambios Informativos para anunciar sobre ciertos eventos como: eliminar alguna SA, reportar condiciones de error, etc., por ejemplo al existir una pareja de SA (una SA en cada dirección) ya sea para ESP o AH se deben eliminar ambas SAs a través de un intercambio Informativo.

El envío de todos los mensajes anteriores es a través de UDP por el puerto 500 o 4500, aspecto que habrá que considerar para que no exista una pérdida de paquetes. Afortunadamente IKE define un temporizador de espera con el propósito de asegurar la correcta entrega de los paquetes, es decir, en dicho periodo se espera antes de retransmitir aquellos mensajes de los que no se ha recibido respuesta alguna.

### 5.3.3.5 PROCESAMIENTO DE TRÁFICO

Finalmente se presenta el procesamiento de los paquetes, de manera que dependiendo de si son de entrada o salida se tendrá un procedimiento distinto:

- Paquetes salientes: se ilustra en la figura 5.12 [29]

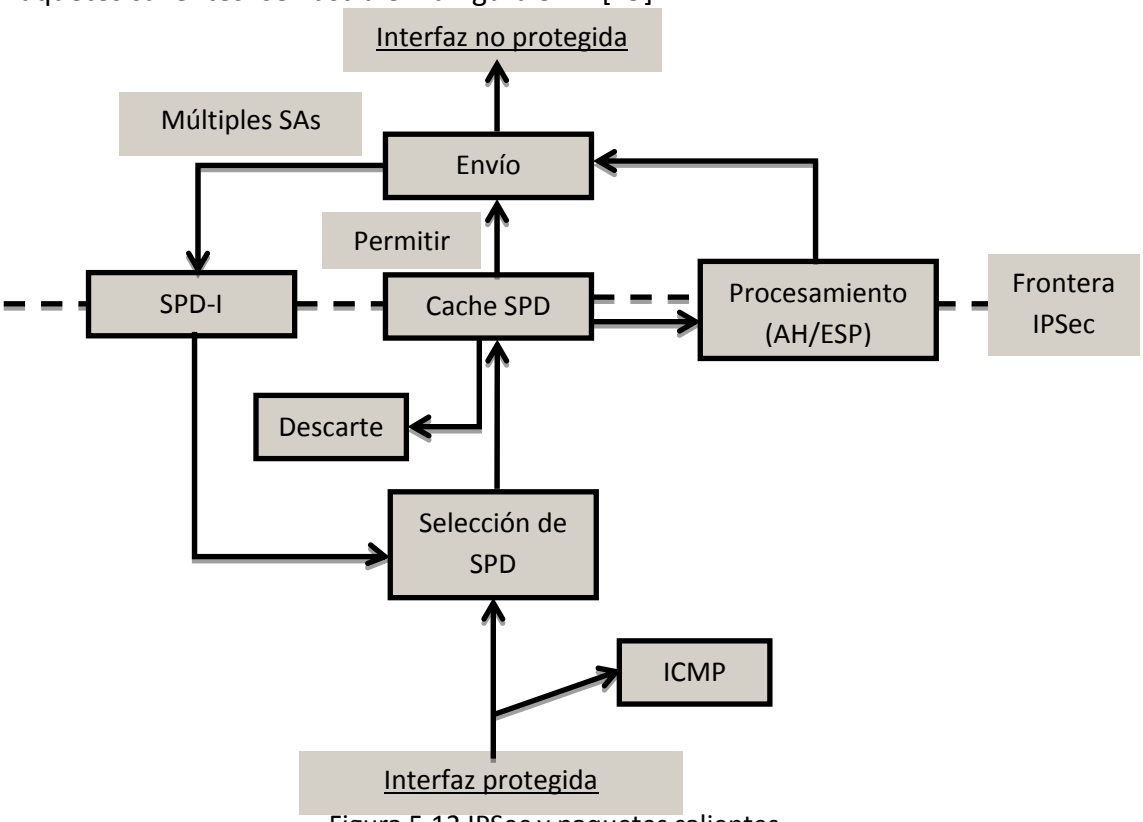



Figura 5.12 IPSec y paquetes salientes

1. Al recibir un paquete se usa la función de selección para obtener el identificador de la SPD (SPD-I) que se vaya a utilizar (en caso de contar con varias SPD).

2. Se procede a encontrar una coincidencia del encabezado del paquete en la cache de la SPD seleccionada. Pueden existir 2 opciones posibles:

   a) Si existe una coincidencia se procesa el paquete de acuerdo a la acción indicada (proteger, descartar, permitir). En caso de que se deba proteger se debe especificar el modo de transporte, algoritmos de cifrado, llaves a usar, SPI, etc.

   b) Al no encontrar una coincidencia en la cache seleccionada se busca directamente en la SPD: cuando se deba descartar el paquete se crean las entradas en la cache y se indica que se recibirán dichos paquetes por la interfaz protegida; si se permite el paso del paquete se crean las entradas en la cache para indicar que se recibirán tales paquetes de la interfaz no protegida, finalmente en caso de que haya que proteger el paquete se crea la SA correspondiente y se agregan las entradas (de ingreso y egreso) en la cache; al no encontrar una coincidencia el paquete es eliminado y se informa de dicha situación transmitiendo un mensaje ICMP (al mismo tiempo se guarda un registro de tal evento).

3. El paquete se pasa a la función de envío de salida para que pueda ser transmitido por la interfaz de salida correspondiente.

❖ Paquetes entrantes: el trato de los paquetes es diferente al caso anterior porque se usan los SPIs para mapear el tráfico de IPSec a las SAs, además es importante mencionar que todos los paquetes que hayan sido fragmentados deben ser re-ensamblados antes de poder procesarlos. La figura 5.13 se muestran los detalles [29].

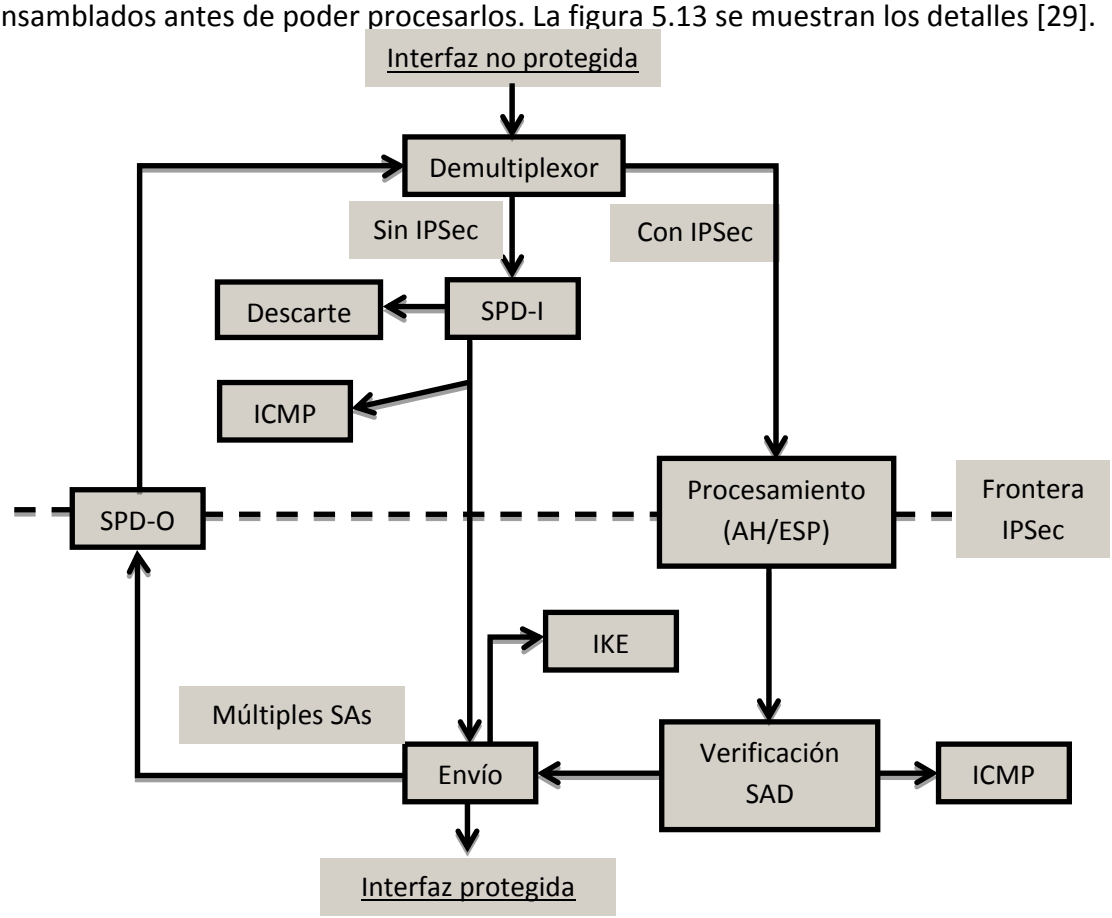



Figura 5.13 IPSec y paquetes entrantes

1) Cada paquete que llega debe ser etiquetado con el identificador de la interfaz (física o virtual) por la que ingresa para poder asociarlo a una cache SPD.

2) Se examina el paquete para clasificarlo en una de las siguientes categorías:

   a. El paquete está protegido por IPSec y está dirigido al dispositivo actual: a través del procesamiento de los encabezados ESP o AH el paquete se asocia a una SA activa para conocer su SPI (usando la SAD). De no encontrar una coincidencia el paquete se descarta y se registra un evento, si hay una coincidencia ir al paso 3.

   b. El tráfico no es dirigido a este dispositivo o sí lo está pero, no se usa IPSec: el paquete se envía a la cache SPD respectiva (dependiendo del ID de la interfaz por

la que llegó el paquete) para buscar una coincidencia, de encontrarla se realiza la acción indicada (permitirle el paso o descartar), de lo contrario se busca dicha información en la SPD y se crea la entrada correspondiente en una cache SPD; si no existe tal información se descarta el paquete y se registra el evento.

3) Procesamiento de mensajes protegidos, no protegidos y mensajes ICMP, para estos últimos se busca en las políticas locales para determinar si se acepta o rechaza el mensaje, así como las acciones a ejecutar en cada caso.

4) Se busca una coincidencia con los selectores de entrada para verificar que el paquete está asociado a la SA correcta, si hay una inconsistencia el paquete es descartado y se registra el evento, e incluso puede enviarse una notificación IKE a la fuente que envió dicho paquete para informarle lo acontecido; de ser correcta la información pasar a 5.

5) De existir procesamientos adicionales que tengan que realizársele al paquete éste deberá ser comparado con las entradas de salida respectivas de la SPD y llevar a cabo los procesamientos requeridos. De lo contrario el paquete se manda a su destino final o se procesa en el dispositivo actual (según sea el caso).

#### 5.3.3.6 USO EN MIPV6

Muchos de los posibles ataques dirigidos hacia los mensajes MIPv6 pueden solucionarse con el uso de IPSec, razón por la cual el RFC 6275 especifica que este protocolo de seguridad debe ser un requerimiento en las comunicaciones de MIPv6. Respecto a la administración de las llaves existe la libertad de crearlas de manera dinámica o estática: en el primer caso las llaves se eliminan al expirar cierto tiempo, mientras que en el segundo caso éstas se conservan y son empleadas cuando el MN se mueve a otra red. En ambas opciones las SAs creadas se basan en la dirección HoA del MN y únicamente la SPD se actualiza ante cambios en la dirección CoA.

Es recomendable utilizar IKEv2 para negociar las SAs a fin de proteger los mensajes que contengan algún encabezado de Movilidad, incluyendo actividades de registro, proceso Return Routability, etc. Al usar IPSec en MIPv6 no necesariamente se requiere el uso del encabezado AH en la opción Home Address (excepto que todo el encabezado IPv6 esté haciendo uso de tal encabezado) a pesar de ello, es recomendable el uso del encabezado ESP en modo de transporte para proteger los mensajes transmitidos entre el MN y su HA:

- HoTI y HoT: mejora la seguridad del proceso Return Routability al disminuir la generación de ataques exitosos. Es común que se emplee ESP en modo túnel.

- BU y BA: garantizan que el MN se registre confidencialmente con su HA, dando la certeza al HA de que el mensaje que recibió fue enviado por un MN auténtico.

  Opcionalmente se pueden proteger los mensajes de Descubrimiento de Prefijo de Movilidad para ocultar información de la topología de la red local del HA, e incluso también se puede proteger el resto de los paquetes (situación no recomendable).

Para entender mejor la relación que existe entre IPSec y MIPv6 se muestra a continuación el procesamiento de los principales mensajes y la forma en que se protegen:

- El MN envía un mensaje BU a su HA.
  1. El MN crea los encabezados ilustrados en la figura 5.14.

| **Encabezado IPv6**<br>Origen=HoA, Destino=HA | **Encabezado de Movilidad**<br>BU |
|---|---|

Figura 5.14 Encabezado de Movilidad en BU

  2. El paquete se compara en la SPD del MN, determinando que se debe usar IPSec.
  3. Se adiciona al paquete el encabezado Opciones de Destino (figura 5.15).

| **Encabezado IPv6**<br>Origen: HoA<br>Destino: HA | **Encabezado de Opciones de Destino**<br>Home Address Option (CoA) | **Encabezado de Movilidad**<br>BU |
|---|---|---|

Figura 5.15 Adición de HoA a BU

  4. Se agregan los encabezados IPSec correspondientes: ya que la dirección primaria CoA del MN no está protegida el MN puede usar el campo CoA alterna (protegido por IPSec) para evitar que un atacante engañe al HA de su verdadera posición. Este campo se emplea sólo cuando el MN está en una red foránea, es decir, el MN no debe emplearlo en el mensaje BU cuando regrese a su red local (figura 5.16).

| **Encabezado IPv6**<br>Origen: HoA<br>Destino: HA | **Encabezado de Opciones de Destino**<br>Home Address Option<br>CoA | **Encabezado ESP**<br>SPI=spi_u | **Encabezado de Movilidad**<br>BU | **CoA alterna** |
|---|---|---|---|---|

Figura 5.16 Adición de encabezado ESP a BU

  5. Se intercambia el valor del campo Dirección Origen con el valor contenido en opción Home Address (figura 5.17).

| **Encabezado IPv6**<br>Origen: CoA<br>Destino: HA | **Encabezado de Opciones de Destino**<br>Home Address Option<br>HoA | **Encabezado ESP**<br>SPI=spi_u | **Encabezado de Movilidad**<br>BU | **CoA alterna** |
|---|---|---|---|---|

Figura 5.17: Formación de mensaje BU

- El HA recibe el mensaje BU del MN.
  1. El HA recibe el paquete que se observa en la figura 5.17.
  2. Se procesa el encabezado de Opciones de Destino, es decir, se realiza el intercambio de direcciones (figura 5.16).
  3. Ahora se procesa el encabezado ESP.
  4. Con los datos obtenidos del encabezado ESP se busca una política de seguridad que coincida con la SA respectiva.
  5. El encabezado de Movilidad se envía al modulo de MIPv6 para su procesamiento.
  6. La SAD es actualizada con la nueva dirección CoA (SA asociada con el MN).

- El procesamiento llevado a cabo para enviar la respuesta desde el HA al MN implica:

  I. El HA crea los encabezados observados en la figura 5.18.

| **Encabezado IPv6**<br>Origen: HA, Destino: HoA | **Encabezado de Movilidad**<br>BA |
|---|---|

Figura 5.18 Encabezado de Movilidad en BA

  II. A fin de conocer el trato que se le dará al paquete se compara con las políticas respectivas de IPSec.

  III. Se agregan el encabezado de Enrutamiento al paquete (figura 5.19).

| **Encabezado IPv6**<br>Origen: HA<br>Destino: HoA | **Encabezado de Enrutamiento (Tipo 2)**<br>CoA | **Encabezado de Movilidad**<br>BA |
|---|---|---|

Figura 5.19 Adición de CoA a BA

  IV. Se aplican las políticas de seguridad de IPSec y se agrega el encabezado ESP (figura 5.20).

| **Encabezado IPv6**<br>Origen=HA<br>Destino=HoA | **Encabezado de Enrutamiento (Tipo 2)**<br>CoA | **Encabezado ESP**<br>SPI=spi_b | **Encabezado de Movilidad**<br>BA |
|---|---|---|---|

Figura 5.20 Adición de encabezado ESP a BA

  V. Finalmente se intercambian las direcciones entre los encabezados IPv6 y Enrutamiento (figura 5.21).

| **Encabezado IPv6**<br>Origen=HA<br>Destino=CoA | **Encabezado de Enrutamiento (Tipo 2)**<br>HoA | **Encabezado ESP**<br>SPI=spi_b | **Encabezado de Movilidad**<br>BA |
|---|---|---|---|

Figura 5.21 Formación de mensaje BA

- El MN recibe el mensaje Binding Acknowledgment de su HA

  I. El MN recibe el paquete mostrado en la figura 5.21.

II. Se procesa el encabezado de Enrutamiento, es decir, se realiza el intercambio de direcciones (figura 5.20).
III. A continuación se procesa el encabezado ESP.
IV. El paquete se compara con la SA correspondiente para saber el trato que debe recibir.
V. Se entrega el encabezado de Movilidad al módulo de MIPv6 para su procesamiento.

En lo que respecta al proceso Return Routability:

- El MN envía un mensaje Home Test Init a su HA.

1. El MN crea los encabezados que se ilustran en la figura 5.22.

| **Encabezado IPv6** Origen: HoA, Destino: CN | **Encabezado de Movilidad** HoTI |
|---|---|

Figura 5.22 HoTI en encabezado de Movilidad

2. A continuación al examinar dicho paquete se determina que debe ser enviado al HA mediante el túnel seguro creado anteriormente.
3. Posteriormente se compara dicho paquete con las políticas de seguridad de IPSec para determinar la protección que requiere.
4. Se agregan los encabezados para usar el modo túnel (figura 5.23).

| **Encabezado IPv6** Origen: CoA Destino: HA | **Encabezado ESP** SPI=spi_hi | **Encabezado IPv6** Origen: HoA Destino: CN | **Encabezado de Movilidad** HoTI |
|---|---|---|---|

Figura 5.23 Uso de modo túnel para HoTI

5. El MN envía el mensaje Home of Test Init a su HA.

- Por su parte el HA recibe el mensaje Home of Test Init.

I. El HA almacena el paquete que se muestra en la figura 5.23.
II. Una vez que se deja de usar el encabezado exterior de IPv6 se elimina.
III. Para conocer el trato que se le dará al paquete se procesa el encabezado ESP buscando la SA respectiva en la SPD (figura 5.22).
IV. El HA envía el paquete al CN.

⇒ Una vez que el CN recibe el mensaje HoTI comienza a construir el mensaje de repuesta y lo envía a la dirección HoA del MN. De esta forma para el HA se tiene:

1. El HA recibe el mensaje Home Test (figura 5.24):

| **Encabezado IPv6**<br>Origen: CN, Destino: HoA | **Encabezado de Movilidad**<br>HoT |
|---|---|

Figura 5.24 HoT en encabezado de Movilidad

2. A continuación cuando el HA determina que ese paquete está dirigido a la dirección HoA de alguno de sus MNs identifica la interfaz por la que debe enviarlo.
3. Se compara el paquete con la SPD (para la interfaz seleccionada), percatándose de la necesidad hacer uso de IPSec.
4. Se agrega el encabezado ESP al paquete (el HA ya debió haber actualizado la dirección IPv6 correspondiente a la SA asociada). Se ilustra en la figura 5.25.

| **Encabezado IPv6**<br>Origen: HA<br>Destino: CoA | **Encabezado ESP**<br>SPI=spi_h | **Encabezado IPv6**<br>Origen: CN<br>Destino: HoA | **Encabezado de Movilidad**<br>HoT |
|---|---|---|---|

Figura 5.25 Uso de modo túnel para HoT

5. El paquete se envía del HA a la dirección CoA del MN.

⇒ Finalmente se describe lo que acontece en el MN.

I. El MN recibe el mensaje HoT, se observa en la figura 5.25.
II. Se elimina el encabezado IPv6 exterior y se procesa el encabezado ESP (figura 5.24).
III. Se compara el paquete con las entradas de la SPD para conocer la acción asociada a la SA.
IV. El paquete se entrega al módulo de Movilidad para su procesamiento.

Un proceso similar ocurre con la transmisión de los siguientes mensajes: Mensaje de Solicitud/Respuesta de Prefijo de Movilidad, Descubrimiento Automático de Home Agent, así como para el resto de los paquetes.

En lo que respecta a la protección de las comunicaciones entre el MN y algún CN no se ha definido hasta el momento un método o proceso para proteger la información que intercambian entre sí a pesar de ello, cuando el CN tiene soporte de MIPv6 el MN debe colocar la opción Información de Autorización de Asociación en el mensaje BU que envía y así mismo el CN deberá colocar la misma opción en su mensaje de respuesta BA.

A pesar de que usar IPSec en la Movilidad IPv6 trae grandes ventajas habrá que tomar en consideración las implicaciones que esto conlleva. De acuerdo a la IETF se calcula que los desarrolladores gastan tan sólo 20% de su tiempo en crear una implementación de MIPv6, y el 80% de tiempo restante es empleado para poder unirlo con IPSec; además es muy frecuentemente que aún así existan problemas de interoperabilidad entre los desarrollos

de MIPv6. Frente a estas situaciones es evidente que hasta el momento IPSec no provee seguridad a las comunicaciones de manera transparente, ya que numerosas interacciones deben ocurrir entre IPSec y los subsistemas de MIPv6, condición que en cierta medida ha frenado el uso de este protocolo.

Mientras tanto, hoy en día la principal desventaja de usar IPSec es la capacidad de procesamiento que exige a los dispositivos, ya que para emplearlo se necesitan llevar a cabo complejas operaciones computacionales para desarrollar los cálculos criptográficos necesarios, razón por la cual no es usual que se implemente en teléfonos celulares, tablets, etc. Otros de los problemas a considerar son:

- Existen sistemas operativos propietarios que no tienen implementado algún modulo destinado a la seguridad a través de IPSec, IKEv2, etc.
- IPSec e IKEv2 no están implementados por defecto ni en los nodos con capacidad IPv6 ni en aquellos con soporte dual (IPv4 e IPv6).
- Las restricciones en las políticas de IPSec de las redes foráneas pueden provocar que el MN no pueda implementar una conexión segura con su HA.
- Problemas de escalabilidad se presentan al tener que lidiar con una configuración manual de llaves o en su defecto con la creación de certificados digitales.
- En ciertas redes el uso masivo de IPSec e IKEv2 produce una sobrecarga en la red, lo que lleva a preferir prescindir de su presencia.
- La administración de llaves usualmente se provee por software de un tercero, lo que dificulta a MIPv6 saber cual es específicamente el que se encuentra instalado en el dispositivo del usuario.

Con todos los elementos que se describieron es claro ver que a pesar de que IPSec ofrece grandes capacidades de protección pero actualmente no existen escenarios de amplio uso y desarrollo, por esta razón podría ser más viable implementar otro tipo de mecanismos de seguridad, por ejemplo: hoy en día algunos teléfonos inteligentes cuentan con un software cliente para el manejo de VPNs y capacidades de cifrado a través de SSL. Mientras tanto, en un escenario optimista habrá que esperar un tiempo a que cobre fuerza la implementación de IPSec en hardware ya que esto permitirá fácilmente su integración en dispositivos con soporte de IPv6 y en futuros dispositivos inteligentes

# Capítulo 6

## Mejoras en Movilidad IP

*The best way to predict the future is to invent it. -Alan Kay*

## 6.1 INTRODUCCIÓN

Es evidente que MIPv6 trae consigo muchos beneficios aunque también presenta ciertas limitantes, precisamente por esto se decidieron diseñar diferentes mejoras que lo ayuden en aspectos como: reducir las interrupciones en las comunicaciones, mantener un porcentaje menor en la pérdida de paquetes, delegar el soporte de movilidad a la red (no al host), promover un desarrollo basado en jerarquías, disminuir la señalización requerida de movilidad, etc.

En las siguientes secciones se hablará de la manera en que funciona cada una de estas mejoras que han sido propuestas en la IETF, pues sin duda la combinación de algunas de ellas favorecerá el desarrollo y adopción de MIPv6 en ambientes reales.

## 6.2 FAST MIPV6

Una de las principales dificultades que enfrenta MIPv6 es el porcentaje de paquetes perdidos cuando el MN experimenta un handover, cuestión que dificulta mantener una transmisión sin interrupciones en las comunicaciones, siendo consientes de esta situación miembros de la IETF decidieron trabajar en una mejora que permitiera confrontar este tipo de adversidades: FMIPv6 por sus siglas en inglés (Fast MIPv6).

Este protocolo se encuentra definido en el RFC 5568 [30] y permite al MN transmitir sus paquetes apenas detecte que se encuentra en un nuevo punto de acceso, es decir, está enfocado en cuidar los tiempos de latencia de los paquetes en los handovers. En la figura 6.1 se aprecian los elementos que se consideran en dicho protocolo.

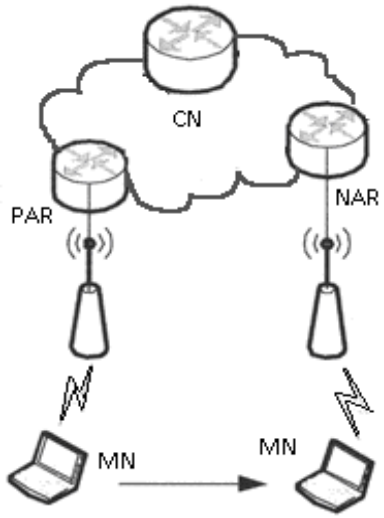



Figura 6.1 Elementos de Fast MIPv6

En la tabla 6.1 se explican las nuevas entidades participantes en FMIPv6.

Tabla 6.1 Elementos de FMIPv6

| Elemento | Descripción |
|---|---|
| Ruteador de Previo Acceso | PAR por sus siglas en inglés (Previous Access Router): es el ruteador por defecto antes de que el MN experimente un handover. |
| Ruteador de Nuevo Acceso | NAR por sus siglas en inglés (New Access Router): será el ruteador por defecto del MN una vez que este último experimente un handover. |
| CoA Previa | PCoA por sus siglas en inglés (Previous CoA): dirección IPv6 asignada al MN en la red de su PAR. |
| CoA Nueva | NCoA por sus siglas en inglés (New CoA): dirección IPv6 que el MN adquirirá en la red de su NAR. |
| Solicitud de Ruteador por Anuncio Proxy | RtSolPr por sus siglas en inglés (Router Solicitation for Proxy Advertisement): mensaje que el MN manda a su PAR para solicitarle información sobre la presencia de un posible handover. |
| Anuncio Proxy de Ruteador | PrRtAdv por sus siglas en inglés (Proxy Router Advertisement): a fin de facilitar la detección de movimiento el PAR envía este mensaje a un MN para proporcionarle información de sus enlaces vecinos. |
| Inicio de Handover | HI por sus siglas en inglés (Handover Initiate): mensaje enviado por el PAR al NAR para informarle del handover experimentado por el MN. |
| Acuse de Recibo de Handover | HAck por sus siglas en inglés (Handover Ack): mensaje transmitido del NAR al PAR en respuesta a un mensaje HI. |
| Anuncio no solicitado de Vecino | UNA por sus siglas en inglés (Unsolicited Neighbor Advertisement): mensaje NS que expresa que la información que contiene no debe sobrescribir la información de la cache Vecinos. |
| Actualización Rápida de Asociación | FBU por sus siglas en inglés (Fast BU): mensaje que manda el MN a su PAR para que este último redirija el tráfico hacia el NAR donde actualmente se ubica. |
| Acuse Rápido de Recibo de Asociación | FBAck por sus siglas en inglés (Fast BA): mensaje que el PAR envía en respuesta a un mensaje FBU recibido. |
| Información del Ruteador de Acceso | AR-Info: duplas formadas por la dirección MAC e IPv6 del AR y el prefijo asociado a la interfaz donde se localiza el MN. |

En FMIPv6 cada cierto tiempo el MN transmite mensajes RtSolPr a su AR para conocer la identidad de los puntos de acceso que detecta, de esta forma tras evaluar las duplas el MN fácilmente puede detectar si su desplazamiento ha provocado que se tenga que asociar a otro punto de acceso, y de ser así el MN tiene lista la información de su NAR. El AR envía un mensaje de respuesta (PrRtAdv) proporcionando la información que le fue solicitada, y con los datos obtenidos el MN manda un mensaje FBU a su AR para informarle la dirección NCoA que desea usar, de esta forma ese ruteador puede asociar las direcciones del MN (PCoA y NCoA). Si el MN está en la red de su PAR debe enviar el mensaje FBU con su dirección PCoA pero, si manda dicho mensaje estando en la red de su

NAR tiene que usar su dirección NCoA, es decir, dependiendo del lugar en que el MN transmita el mensaje FBU se presentan 2 escenarios [30]:

a) *Handover Rápido Predictivo:* el MN puede enviar un mensaje FBU a su PAR incluso antes de unirse a un NAR, si dicho móvil no recibe el mensaje de respuesta (FBAck) el handover se convierte en reactivo (se explica más adelante), de lo contrario los pasos que se presentan se explican enseguida (figura 6.2):

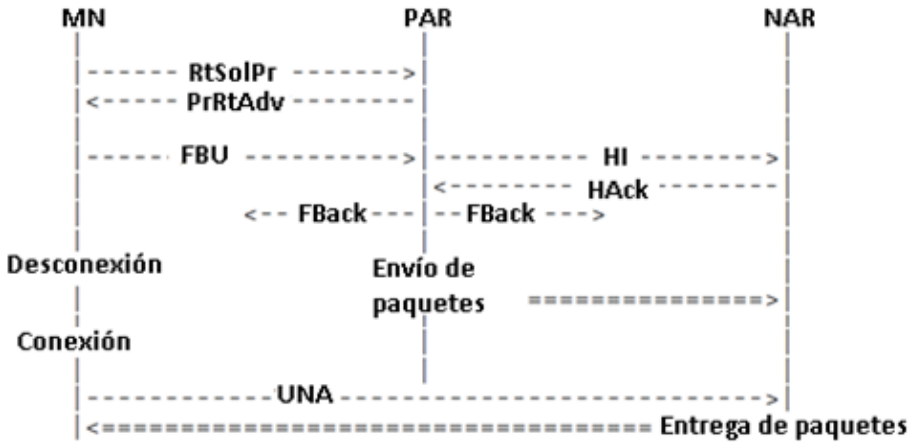



Figura 6.2 Handover Rápido Predictivo

- Antes de que el PAR envíe el mensaje FBAck primero necesitará mandar un mensaje HI al NAR para informarle datos importantes acerca del MN como: la dirección NCoA que desea usar, su dirección IPv6 (PCoA) y su MAC. Esta información le permitirá al NAR almacenar temporalmente los paquetes que reciba que estén destinados a la dirección NCoA del MN.

- El NAR al recibir el mensaje HI lleva a cabo el proceso DAD para verificar que la dirección NCoA solicitada no está siendo usada actualmente, posteriormente decide si se la asigna al MN o le otorga una dirección distinta. Debido al tiempo implicado en DAD puede omitirse este paso en ambientes donde la probabilidad de que existan direcciones duplicadas sea muy baja aunque, la decisión depende de las políticas aplicadas en la red donde se encuentre el NAR. Finalmente la decisión que determine el NAR la da a conocer en el mensaje HAck que transmite al PAR. Ahora este último conoce la dirección NCoA asociada al MN y por ende envía un mensaje FBAck para informárselo. Con esto el PAR está listo para reenviar los paquetes que reciba (destinados al MN) hacia el NAR apropiado.

- Finalmente el MN al recibir el mensaje FBAck conocerá la dirección NCoA que debe emplear e inmediatamente procede a transmitir un mensaje UNA a su NAR para que dicho ruteador le envíe los paquetes que reciba destinados a su

dirección NCoA; el MN al no recibir el mensaje FBAck asume que la red donde se encuentra no soporta FMIPv6 y deja de usarlo.

b) *Handover Rápido Reactivo:* el MN manda un mensaje FBU cuando ya está unido a la red de su NAR. Los eventos implicados son mostrados en la figura 6.3 y explicados a continuación:

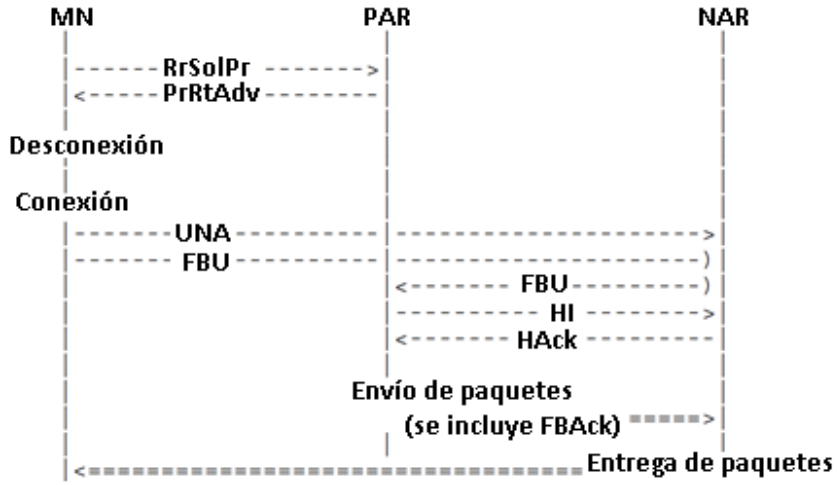



Figura 6.3 Handover Rápido Reactivo

⇒ Ya que el MN no recibió el mensaje FBAck cuando estaba en la red de su PAR (cuando se encontraba en dicha red no envió el mensaje FBU o tras enviarlo inmediatamente abandonó tal red) debe mandar a su NAR un mensaje UNA.

⇒ Cuando el NAR recibe dicho mensaje analiza la información y en caso de que decida asignarle al MN una dirección NCoA distinta debe informárselo a través del envío de un mensaje RA con la opción NACCK.

⇒ Por su parte el MN ejecuta el proceso DAD para asegurarse de que su dirección NCoA se esté usando actualmente. Al terminar tal verificación el MN transmite un mensaje FBU a su PAR.

⇒ Finalmente una vez que el MN ya tiene una dirección NCoA definitiva, le manda un mensaje NA al resto de los nodos de su nueva red para indicarles que actualicen en su cache de Vecinos dicha dirección.

Es evidente que debe existir una asociación entre el PAR y el NAR, es decir, estas entidades establecen un túnel entre la direcciones PCoA y NCoA que permanece activo hasta que el MN completa su nuevo registro con algún CN con el que se esté comunicando por lo tanto, el MN no puede comunicarse directamente con el CN (asumiendo que en su BC posea una entrada con la dirección PCoA del MN) y por ende usa dicho túnel para realizar la entrega final de los paquetes porque de lo contrario, serían eliminados por

algún filtro de ingreso (la dirección PCoA no pertenece a los prefijos asignados al NAR donde actualmente se ubica el MN).

Además del uso del túnel es aconsejable que el NAR tenga un buffer destinado al manejo de tráfico dirigido a los MNs que estén experimentando un handover, y de la misma forma el PAR debe poseer un buffer similar como almacenamiento temporal, al menos hasta que pueda mandar los paquetes correctamente a la dirección NCoA del MN. Particularmente el uso de ambos buffers permite que el MN pierda una menor cantidad de paquetes durante un handover no obstante, se deben tener las siguientes consideraciones al emplearlos:

- En el búfer durante un periodo de tiempo ciertas aplicaciones pueden transmitir más información que otras pero, existen diferentes requerimientos porque la prioridad de cada una de éstas llega a variar, por ejemplo el almacenar demasiados paquetes podría contribuir a aumentar los tiempos de retraso, situación que repercute significativamente en aplicaciones basadas en tiempo real.
- Cuando el NAR o el PAR tengan paquetes almacenados para un MN, no deben enviárselos demasiado rápido o podrían sobrecargar el uso de sus recursos o congestionar los enlaces, es preferible que cuando el NAR reciba un mensaje UNA de algún MN le envíe gradualmente todos los paquetes que tiene almacenados.
- La entrega de los paquetes puede verse afectada por la capacidad del enlace donde ahora se encuentra el MN, situación muy común cuando hay un cambio de un tipo de red a otra, por ejemplo de una red WLAN a una red GPRS.

Es claro que FMIPv6 trae consigo varias mejoras a MIPv6 pero, hay que considerar que el uso de ND generalmente acarrea tiempos considerables de retraso (las retransmisiones por defecto se realizan cada segundo), además la velocidad a la que el MN puede desplazarse aún sigue siendo otra limitante a considerar. Algunos de los principales problemas que llegan a presentarse son:

- *Movimiento ping-pong:* el que un MN regularmente se desplace a gran velocidad entre 2 redes (pertenecientes a distintos AR) causa que el tiempo requerido para intercambiar los mensajes de señalización y almacenar los paquetes sea insuficiente, llegando al punto de sobrecargar la red y causar problemas en mantener comunicaciones estables e ininterrumpidas.
- *Movimiento erróneo:* el MN no permanece el tiempo suficiente en una red como para que le sean entregados los paquetes que tiene almacenado su PAR o NAR.

Este ambiente ocasiona un aumento considerable en los tiempos de retraso en las comunicaciones y la eliminación eventual de tales paquetes.

Para lidiar con los casos anteriores si el MN regresa su PAR antes de actualizar sus asociaciones respectivas, debe enviar nuevamente un mensaje FBU a su PAR con las siguientes características: la dirección PCoA contenida en la opción Home Address y tiempo de vida en 0; de esta forma al recibir el mensaje el PAR elimina el túnel correspondiente y nuevamente le manda directamente al MN los paquetes que le lleguen. Además de esto es aconsejable que el tiempo de vida de los túneles sea corto, tan sólo los segundos necesarios para que el MN actualice correctamente sus asociaciones.

En lo concerniente a la seguridad, FMIPv6 utiliza el campo Información de Autorización de Asociación para FMIPv6, BADF por sus siglas en inglés (Binding Authorization Data for FMIPv6) en los mensajes FBU y FBAck para asegurar que el MN es legítimo y verificar que dicho host realmente posee la dirección PCoA. Adicionalmente el PAR necesita verificar que la dirección NCoA que el MN desea usar pertenece a la red del NAR, de manera que al no cumplirse esta condición no se crea ninguna asociación. En lo que respecta al intercambio de mensajes HI y HAck, se puede hacer uso de IPSec para proporcionar integridad a las comunicaciones y autenticidad de las entidades (verificando la identidad del NAR y el PAR) para impedir que existan nodos falsos implicados en las comunicaciones desarrolladas por el MN.

## 6.3 MIPv6 JERÁRQUICO

Otro de los principales problemas de MIPv6 es la escalabilidad, inconveniente que de cierta forma ha frenado su despliegue a una mayor escala. Precisamente con dicha idea en mente se desarrolló HMIPv6, por sus siglas en inglés (Hierarchical MIPv6). Este protocolo se define en el RFC 5380 [31] y básicamente minimiza el impacto de usar MIPv6 al reducir el intercambio de señalización que el MN manda a su HA y a los CNs con los que se esté comunicando actualmente.

Para lograr su propósito HMIPv6 maneja dominios dentro de los cuales el MN pueda desplazarse con facilidad, inclusive disfrutando un mejor rendimiento en sus comunicaciones cuando suele experimentar algún handover. El tamaño de tales dominios debe definirse de acuerdo a la infraestructura de cada red y al alcance que ésta llegue a tener, por ejemplo es recomendable que existan diferentes dominios en aquellas redes lo suficientemente extensas o cuyos requerimientos así lo exijan.

Para entender mejor el funcionamiento de HMIPv6 se presentan en la tabla 6.2 los nuevos elementos implicados en este protocolo.

Tabla 6.2 Elementos de HMIPv6

| Elemento | Descripción |
|---|---|
| Punto de Anclaje de Movilidad | MAP por sus siglas en inglés (Mobility Anchor Point): ruteador presente en una red foránea que es utilizado por el MN como si se tratara de un HA local. |
| CoA Regional | RCoA por sus siglas en inglés (Regional CoA): dirección IPv6 asignada por el MAP a un MN. Está formada del prefijo de red anunciado por el MAP y el identificador de la interfaz del MN. |
| CoA de Enlace | LCoA por sus siglas en inglés (Link CoA): dirección IPv6 de la interfaz del MN que está basada en el prefijo que anuncia su ruteador por defecto. |
| BU Local | Mensaje que el MN transmite a su MAP para crear la asociación entre sus direcciones LCoA y RCoA. |
| MN con soporte HMIPv6 | MN que puede enviar, recibir y procesar correctamente las opciones que emplea el MAP en sus mensajes. |

En la figura 6.4 se observa el movimiento de un MN que se desplaza dentro de un dominio o incluso pasando de un dominio a otro.

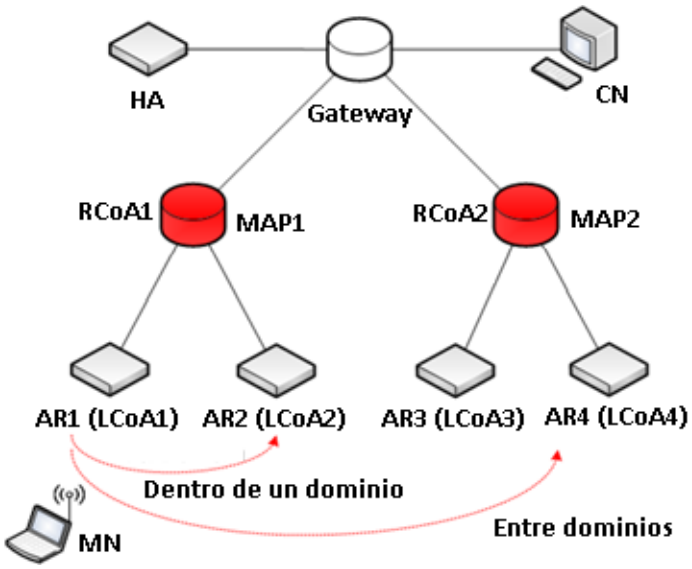



Figura 6.4 Movimiento de un MN con HMIPv6

Con MIPv6 el MN depende exclusivamente de su HA, es decir, hay un sólo punto de fallo y existe cierto tiempo de retraso generado por el registro que se lleva a cabo por lo tanto, la distancia a la que se encuentra el MN de su red local se convierte en un factor clave, por ejemplo si el MN y su HA están en partes opuestas del mundo el retraso generado sería mucho mayor que si estuvieran en la misma ciudad. Por esta razón se espera que los dispositivos con soporte de HMIPv6 puedan elegir entre utilizar dicho protocolo o MIPv6, la decisión dependerá de las circunstancias en que el MN se encuentre, la forma en que haya sido configurado y las capacidades de la red en que se encuentre.

Particularmente lo que HMIPv6 pretende es incluir diferentes MAPs hasta formar una red jerárquica, condición que limita la señalización de movilidad y mejora el impacto y velocidad del MN al experimentar un handover; esto es posible gracias a lo siguiente:

- ✓ El MN al desplazarse dentro de un dominio sólo debe enviar mensajes BU a su MAP, ya no es necesario enviar tales mensajes a algún CN o a su HA. El uso de HMIPv6 permite mantener una mejor administración de micro-movilidad porque disminuye considerablemente los tiempos de retraso de los registros y ayuda a reducir el número de paquetes perdidos ante la presencia de un handover.

- ✓ El MN al unirse a un nuevo dominio y mientras permanezca en éste únicamente manda un mensaje BU para que su HA y CN conozcan su nueva ubicación. Esto es posible porque el MN se registra ante ellos con una dirección RCoA, esto a su vez constituye una mejora en la privacidad del MN (haciendo más difícil que pueda ser rastreado) debido a que dentro de un dominio se identifica con una dirección LCoA, mientras que los nodos fuera del dominio lo identifican bajo una dirección RCoA.

El intercambio de mensajes implicados en el funcionamiento de HMIPv6 depende del desplazamiento del MN, es decir, dicho host debe percatarse cuando se mueve de una red a otra para saber si se encuentra en el mismo dominio o en otro diferente, para ello el MN emplea ND y además recibe información valiosa en los mensajes RA (analizando la opción Dirección Global de MAP). Los casos que llegan a presentarse son [31]:

a) *Desplazamiento dentro de un mismo dominio:* mientras el MN se mueva entre ARs que pertenezcan al mismo dominio únicamente tiene que registrarse de forma local con su MAP y formar sus direcciones LCoA y RCoA. Cuando el MN ya tiene dichas direcciones simplemente las transmite en un mensaje BU local a su AR para que este último sea el encargado de retransmitirlas hacia el MAP correspondiente.

   Una vez que el MAP recibe la información anterior verifica que la dirección RCoA sea única (a través de DAD). Si el MAP tiene una lista con los prefijos de red usados para formar las direcciones LCoA, tendrá que verificar que los mensajes BU que reciba contengan una dirección que pertenezca a uno de los prefijos de dicha lista, de lo contrario el MAP transmite un código de error informando que no se le puede seguir brindando el servicio de movilidad a tal MN.

   De cumplirse con los requisitos antes mencionados el MAP transmite un mensaje BA (Encabezado de Enrutamiento tipo 2: RCoA) para informarle al MN que la asociación fue exitosa o que se presentó algún problema. En caso de que no haya existido ninguna falla el MAP asocia al MN las direcciones LCoA y RCoA, y crea un

túnel bidireccional (hacia la dirección LCoA) por donde mandará todos paquetes que reciba y que estén dirigidos al MN.

Con la información que posee el MAP manda un mensaje BU a los nodos relacionados con el MN (HA, CN) para informarles de la nueva dirección RCoA que ahora posee. Una vez que tales nodos crean la entrada respectiva en sus estructuras de datos mandan un mensaje BA al MAP, el cual a su vez almacena una nueva entrada con la información del MN (figura 6.5).

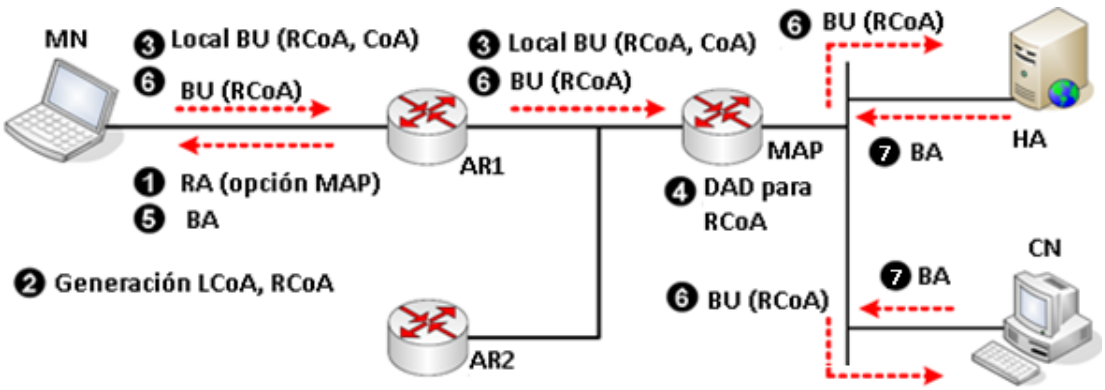



Figura 6.5 Registro del MN en un solo dominio HMIPv6

b) *Desplazamiento entre dominios:* es necesario que el MN se registre nuevamente con su HA o con cierto CN para informarles de su nueva ubicación porque al estar en un nuevo dominio adquiere otra dirección RCoA.

En primer lugar el MN manda un mensaje BU local a su nuevo MAP para informarle de su dirección LCoA (opción Home Address: RCoA, y sin la opción CoA Alterna). Al procesar la información el MAP guarda esos datos y manda un mensaje BA al MN. Ahora el MN podrá transmitir mensajes BU (Opción Home Addres: HoA, CoA: RCoA) a su HA o a algún CN, los cuales responderán con un mensaje BA informando el estado del registro correspondiente.

Llegado a este punto el MN ahora podrá hacer uso del túnel bidireccional que establece con su MAP a fin de seguir recibiendo y enviando paquetes de manera ininterrumpida. El MAP se convierte en un intermediario que intercepta los paquetes dirigidos al MN a través del envío de mensajes NA. En el túnel el encabezado externo utiliza la dirección del MAP y la dirección LCoA del MN como origen o destino (según la dirección de la comunicación) y el encabezado interno emplea la dirección RCoA del MN y aquella dirección asignada al nodo final de la comunicación (figura 6.6).

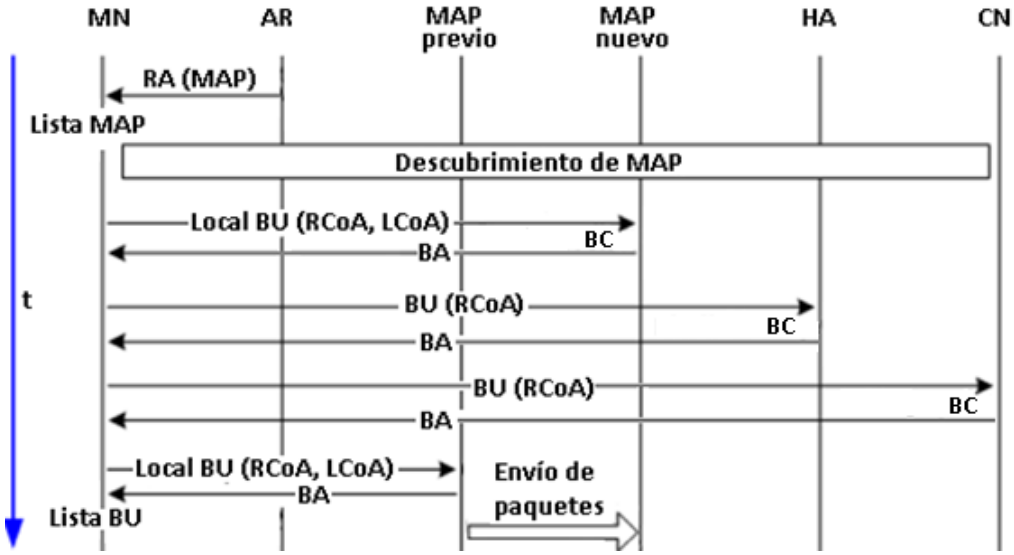



Figura 6.6 Registro del MN entre dominios HMIPv6

Para disminuir la pérdida de paquetes cuando el MN se mueve entre diferentes dominios adyacentes, de manera opcional, cuando el MN se mueve a un nuevo dominio puede enviar un mensaje BU local a su antiguo MAP solicitando que le envíe todos los paquetes que reciba (destinados a su antigua dirección RCoA del MN) a su dirección LCoA actual. Habrá que considerar que esta situación depende de las políticas que se tengan configuradas en los dominios porque los administradores pueden o no permitir el intercambio de estos mensajes.

En HMIPv6 pueden llegar a presentarse diversos escenarios adicionales que ayudan a mejorar la eficiencia en las comunicaciones, incluyendo aquellos casos donde el MN tiene la capacidad de registrarse simultáneamente con varios MAPs (perteneciente al mismo dominio), esto abre la posibilidad de que el MN utilice una determinada dirección RCoA para comunicarse con cierto grupo de CNs o incluso pueda manejar una especie de redundancia, evitando que un MAP se convierta en un único punto de fallo. Para estos escenarios recién descritos es necesario que los MAPs sean capaces de transferir información de sus BCs entre sí y que permitan al MN mantener su misma dirección RCoA, es decir, todos los MAPs tienen que anunciar el mismo prefijo en la opción MAP.

Habrá que tomar en cuenta que permitir registros simultáneos al MN implica que éste no debe usar una dirección RCoA (asignada por cierto MAP) como su dirección LCoA (asignada por otro MAP), de lo contrario los paquetes serían encapsulados varias veces y por consecuencia se provocaría una ineficiencia en el protocolo y una degradación del rendimiento de las comunicaciones. Se tendrá entonces que respetar la manera en que se forman dichas direcciones, es decir, así como la dirección RCoA de un MN está en función de un MAP, su dirección LCoA lo estará con respecto al AR más próximo al MN.

Específicamente el MN se percata de que existen diferentes MAPs en un dominio cuando en los mensajes RA que recibe encuentra varias direcciones en la opción Dirección Global de MAP, tras verificar este escenario el MN almacena esa información para utilizarla como punto de comparación ante los siguientes mensajes que reciba, de esa forma es capaz de detectar cuando se haya desplazado a una ubicación diferente. Actualmente es posible encontrar 2 mecanismos de detección de movimiento:

- *"Impaciente":* El MN se registra con mayor frecuencia con su HA o con algún CN porque cuando detecta un nuevo MAP lleva a cabo una nueva asociación con dicho nodo (a pesar de que tenga asociaciones vigentes).
- *"Perezoso":* el MN mantiene las asociaciones que tiene hasta que reciba un mensaje que le informe que su MAP ha fallado, es decir, no crea nuevas asociaciones hasta que expire el tiempo de vida de aquellas que ya posee.

En algunas redes puede ser necesario que se implementen múltiples MAPs en diferentes niveles, por ejemplo se puede tener un MAP en el ruteador por defecto de la red entera y al mismo tiempo varios MAPs ubicados en los ARs de cada segmento de red. En estos casos el MN selecciona algún MAP considerando su situación: si se mueve constantemente es mejor que elija al ruteador por defecto de la red como su MAP porque no tendrá que cambiar frecuentemente su dirección RCoA y disminuirá por ende el número de registros que deberá llevar a cabo con los nodos fuera del dominio; por el contrario si la frecuencia con que cambia de ubicación no es muy grande podrá elegir a su AR más cercano como MAP, condición que le permitirá reducir el tiempo implicado en sus registros con los nodos fuera del dominio y mejorar sus comunicaciones dentro de éste.

Usualmente el MN elige el MAP con el valor más alto en su campo Preferencia, por su parte el algoritmo por defecto se basa en seleccionar el MAP que se encuentra más alejado del MN (en orden de jerarquía) para evitar que se tenga que registrar constantemente. Los pasos que el MN sigue dentro de un dominio para seleccionar el MAP son los mencionados a continuación y mostrados en la figura 6.7:

1) Recibir y procesar las entradas que encuentre en la opción MAP.
2) Ordenar los MAPs en orden descendente, es decir, primero se colocan aquellos que posean el valor más alto en el campo Distancia.
3) Seleccionar el primer MAP de la lista, si el campo Tiempo de vida del MAP seleccionado es 0 se debe seleccionar el siguiente MAP de la lista.

4) Repetir el paso anterior mientras haya MAPs disponibles hasta que se seleccione un MAP con un valor mayor a 0 en sus campos Preferencia y Tiempo de vida.

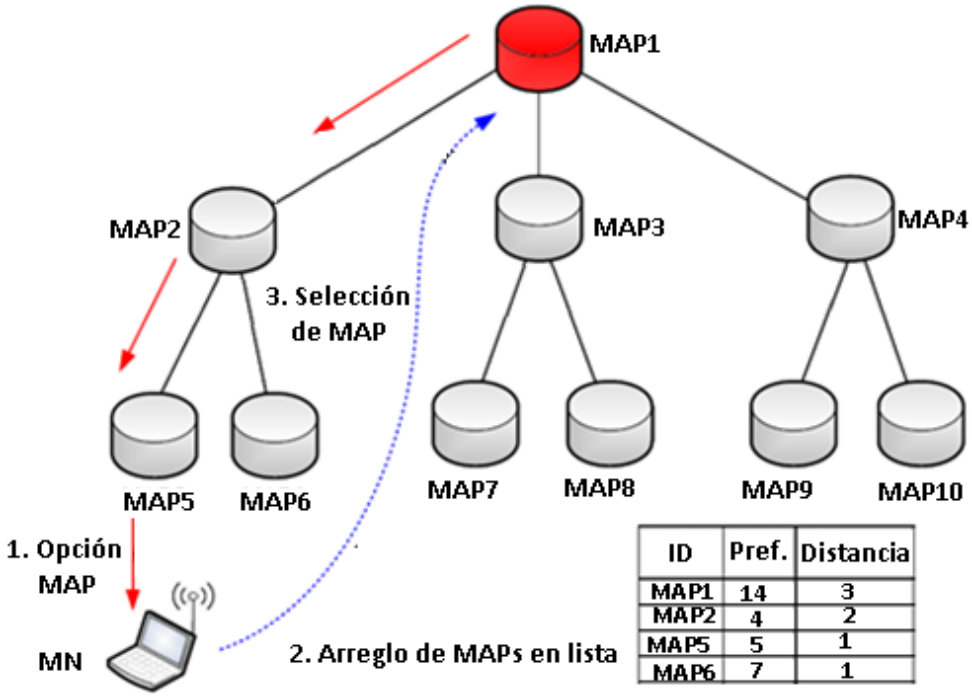



Figura 6.7 Selección del MAP

Estrictamente el MN no debe mandar nuevos mensaje BU a los MAPs que tengan 0 en su campo Tiempo de vida porque dicho valor es un indicador de que existe una falla en tales ruteadores por lo tanto, si el MN tiene un registro activo con dichos MAPs debe dar por perdida su asociación y registrarse con un MAP distinto. Bajo estas circunstancias los ARs juegan un papel muy importante en la detección de fallas de algún MAP porque son los encargados de comunicar dicha información a los MNs; afortunadamente hay 2 formas de conocer esta información: estáticamente (interviene el administrador) o dinámicamente (probando la conectividad del MAP cada cierto tiempo).

Hasta ahora se ha hablado de las comunicaciones desarrolladas en HMIPv6 y los distintos escenarios que se pueden encontrar pero, no se debe dejar de lado el aspecto de la seguridad. La seguridad en HMIPv6 comprende la autenticación mutua, integridad en las comunicaciones, protección anti-respuesta y confidencialidad de los paquetes intercambiados. Para lograr esto el MN únicamente debe intercambiar los mensajes necesarios para unirse a un MAP, de lo contrario un nodo malicioso podría realizar ataques de suplantación de identidad (al quererse hacer pasar por otro MN o inclusive tratando de fingir ser un MAP auténtico). Las principales relaciones de seguridad a considerar son:

a) MN-MAP: ya que el MAP no tiene conocimiento de la identidad de ningún MN o de algún HA es necesario que antes de registrar a un MN primero lo autentique, es decir, una vez que el MN se ha autenticado el MAP puede permitirle usar cierta dirección RCoA mientras dicho móvil esté dentro de ese dominio.

   Puede recurrirse a la negociación de una SA para corroborar la identidad del MN o del MAP (inclusive de ambos), o auxiliarse de una entidad en la que ambos nodos confíen, regularmente una Autoridad Certificadora, CA por sus siglas en inglés (Certifique Authority). Para cumplir con lo anterior tanto el MN como el MAP necesitan soportar IKEv2 porque esto les facilitaría usar un mecanismo que tenga alguna extensión disponible, por ejemplo EAP permitiría realizar el "bootstrapping" de las SAs involucradas entre los nodos y evitar que se dependa de certificados.

   Otra opción a considerar es el uso de IPSec (en modo de transporte) para proteger los mensajes de registro entre el MN y su MAP.

b) MN-CN: a pesar de que el mecanismo "Return Routablity" no se ve afectado habrá que tener cuidado de las direcciones que se usan en los mensajes HoTI (la dirección de origen tiene que ser la dirección HoA del MN). Estos mensajes deben encapsularse: en el encabezado interior la dirección RCoA es el origen y la dirección de su HA es el destino, mientras que el encabezado exterior usa la dirección LCoA del MN como origen y la dirección de su MAP como destino.

c) MN-HA: ya que HMIPv6 no modifica esta relación los aspectos de seguridad aplicados en MIPv6 se mantienen.

Adicionalmente también se deben definir mecanismos para proteger las comunicaciones desarrolladas entre los MAPs y sus ARs, de lo contrario podrían presentarse problemas de seguridad en el MAP (elemento principal en HMIPv6). Precisamente por esto se necesitan definir sistemas de autenticación que permitan verificar las identidades de los nodos, por ejemplo a través de servidores AAA.

## 6.4 PROXY MIPv6

Hasta el momento las mejoras de MIPv6 de las que se han hablado se concentran en mejorar el rendimiento de las comunicaciones no obstante, todos los casos se basan en dar soporte de movilidad a nivel de host, es decir, cada MN debe tener soporte de MIPv6, particularidad que en cierta medida dificulta su uso en la actualidad. Tomando esto en cuenta se pensó en desarrollar un soporte de movilidad basado en red, PMIPv6 por sus siglas en inglés (Proxy MIPv6), esta mejora se encuentra definida en el RFC 5213 [32] y permite que cada MN disfrute de movilidad sin tener que participar en los mensajes de

señalización por lo tanto, los elementos de la red llevan a cabo el intercambio de la señalización requerida y dan oportunidad a los MNs para que se desplazasen libremente mientras mantienen sus comunicaciones continuas, pero sin tener implementado MIPv6. Antes de detallar el funcionamiento de PMIPv6 se requieren conocer los elementos más representativos de este protocolo, mismos que se describen en la tabla 6.3.

Tabla 6.3 Elementos de PMIPv6

| Elemento | Descripción |
|---|---|
| Dominio PMIPv6 | Conjunto de redes que proporcionan soporte de movilidad a través de PMIPv6. |
| Ancla de Movilidad Local | LMA por sus siglas en inglés (Local Mobility Anchor): representa un HA con capacidades mejoradas dentro de un dominio PMIPv6. |
| Nodo Móvil | MN por sus siglas en inglés (Mobile Node): nodo con soporte IPv4 y/o IPv6 que no participa en los mensajes de movilidad de PMIPv6. |
| Gateway de Acceso Móvil | MAG por sus siglas en inglés (Mobile Access Gateway): ruteador de acceso que participa en los mensajes de PMIPv6 en representación de los MNs ubicados en alguna de sus redes locales. |
| Dirección LMA | LMAA por sus siglas en inglés (LMA Address): dirección del LMA que representa un punto del túnel bidireccional creado con un MAG. |
| Proxy-CoA | Dirección de la interfaz de egreso de un MAG que representa un punto del túnel que establece con un LMA.<br>Para el LMA representa la dirección CoA de cada MN que tiene registrado. |
| Prefijo de Red Local del Nodo Móvil | MN-HNP por sus siglas en inglés (Mobile Node´s Home Network Prefix): conjunto de prefijos que se administran como una sesión de movilidad y que son asignados al enlace que existe entre el MN y su MAG. |
| HoA de Nodo Móvil | Dirección obtenida del MN-HNP (MN-HoA) que es usada por el MN mientras éste se encuentre en un dominio PMIPv6. |
| Enlace Local del Nodo Móvil | Enlace asignado al MN cuando entra a un dominio PMIPv6 y que percibe mientras se encuentra dentro de tal entorno. |
| Proxy BU | PBU por sus siglas en inglés (Proxy Binding Update): mensaje que manda un MAG a su LMA para solicitar una asociación entre su dirección Proxy-CoA y el prefijo asociado a cierta interfaz del MN. |
| Proxy BA | PBA por sus siglas en inglés (Proxy Binding Acknowledgment): mensaje que un LMA envía a un MAG como respuesta a un mensaje PBU recibido. |

Los elementos anteriores ayudan a PMIPv6 no sólo a proporcionar el soporte de movilidad a los MNs sino también a rastrear cada uno de sus movimientos, a fin de conocer su ubicación actual y determinar si deben o no seguir disfrutando de movilidad. El LMA y el MAG son las entidades principales, el primero mantiene el estado del MN y registra completamente las sesiones de todo un dominio PMIPv6, el segundo administra la

movilidad en representación de cada MN que se encuentre en alguna de sus redes de acceso y detecta sus movimientos para precisar si debe o no registrarlos con el LMA. Gracias a estas 2 entidades el MN percibe a un dominio PMIPv6 como un único enlace, de tal forma que mientras se desplaza dentro de dicho entorno no experimenta ningún cambio en la dirección IP que adquirió la primera vez que se unió a tal dominio.

En un dominio PMIPv6 existe un LMA y varios MAGs, esto depende del tipo de red en que se implemente, la demanda del soporte de movilidad y la extensión de la red. Además el hecho de que el MN puede ser incluso un nodo con soporte dual provoca que PMIPv6 pueda trabajar sobre una red IPv4 o IPv6 aunque, es claro que resulta preferible utilizar las características mejoradas que ofrece IPv6.

Para entender mejor la ubicación de estos elementos se observa en la figura 6.8 algunas de las relaciones que guardan entre sí.

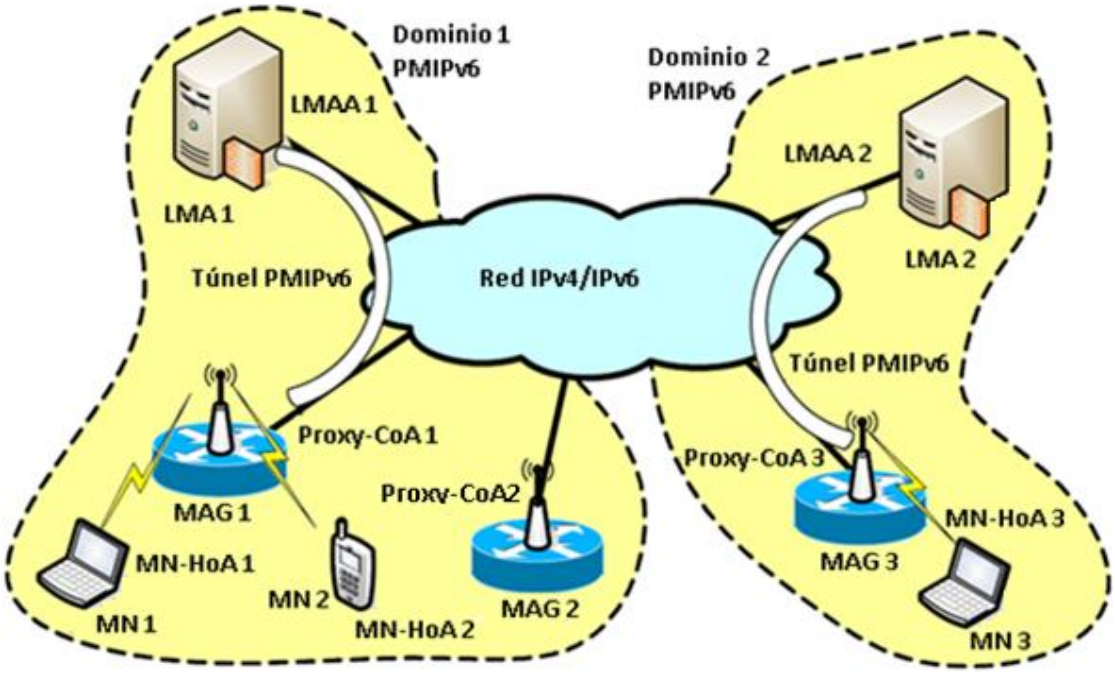



Figura 6.8 Elementos de PMIPv6

Antes de continuar con la descripción del funcionamiento de PMIPv6 habrá que contemplar que existen ciertos campos en los mensajes de movilidad que ya no son utilizados (en comparación con MIPv6) por ejemplo: Opción de Destino Home Address y Encabezado de Enrutamiento Tipo 2, estos elementos ya no se usan y en caso de estar presentes simplemente son ignorados y por lo tanto se carecen de ciertas características en el dominio PMIPv6, tales como: Descubrimiento de Prefijo de Movilidad, Optimización de Ruta y DHAAD.

Realizadas tales aclaraciones ahora se describen los 2 eventos significativos que suelen presentarse en PMIPv6 [38]:

a) *El MN entra a un nuevo dominio PMIPv6* (figura 6.9): la primera vez que un MN entra a un dominio diferente necesita adquirir una nueva dirección a través del envío de un mensaje RS a su MAG actual (usualmente es su ruteador de acceso).

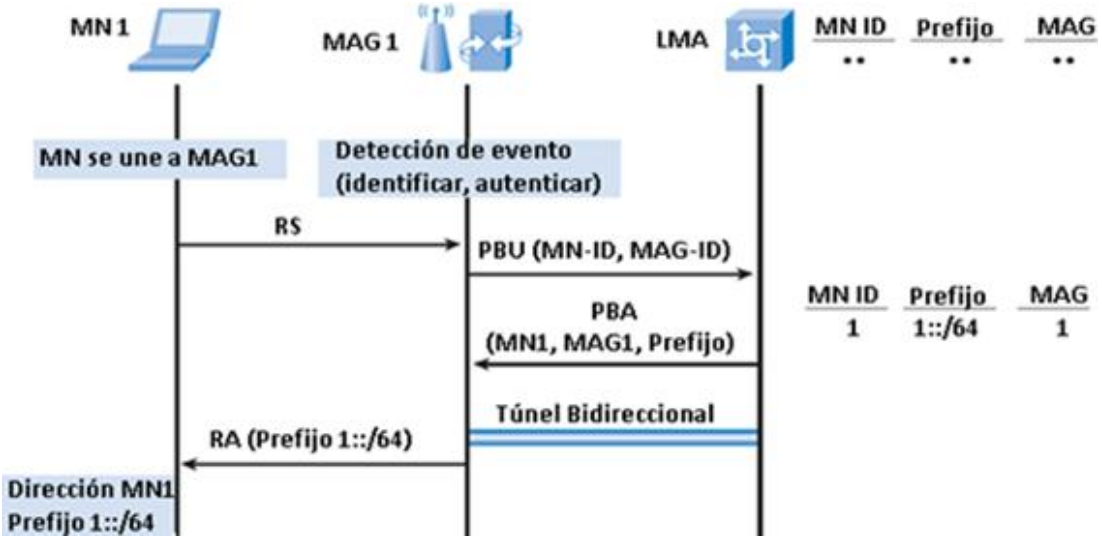



Figura 6.9 Entrada de MN a un nuevo dominio PMIPv6

En un inicio el MAG identifica al MN para determinar si está autorizado para brindarle el soporte de movilidad y a continuación manda un mensaje PBU al LMA para informarle sobre la identidad y ubicación actual de un nuevo MN. Para que el mensaje PBU sea aceptado debe contener los datos mostrados en la figura 6.10.

| **Encabezado IPv6**<br>Origen: Proxy-CoA<br>Destino: LMAA | **Encabezado de Movilidad**<br>BU (P, A) | **Opciones de Movilidad**<br>MNI, HNP, Indicador de handover, Tipo de tecnología de acceso. [Fecha y hora, Identificador de capa de enlace del MN, Dirección de enlace local] |
|---|---|---|

Figura 6.10 Mensaje PBU

Donde:
MNI: identificación por la que el LMA sabe si proporciona o no el soporte de movilidad a un MN.
HNP: en el primer registro contiene solamente 0´s, para renovación o eliminación de un registro contiene aquel prefijo que le fue asignado anteriormente a un MN.
Tipo de tecnología de acceso: es el tipo de red en que se ubica el MN, por ejemplo virtual, PPP, Ethernet, WLAN, WiMAX, etc.
Fecha y hora: se usa al no utilizar el campo Número de Secuencia del Encabezado de Movilidad.
Identificador de capa de enlace del MN: identificador estable de la interfaz donde se ubica el MN.
Dirección de enlace local: representa la dirección que el MAG comparte con un MN, en el primer registro contiene solamente 0's, en casos posteriores lleva la dirección otorgada por el MAG.

A continuación el LMA procesa el campo Opción de Identificación de Nodo Móvil (del mensaje PBU recibido) para verificar la identidad del MN y decidir si le brinda o no el soporte de movilidad. Si el LMA acepta el mensaje crea una entrada en su BC (para registrar una nueva sesión de movilidad) y de acuerdo a las políticas de la red, envía un mensaje PBA al MAG informándole sobre los prefijos asignados al MN. En caso contrario el MAG informa la causa por la que no pudo crear la sesión de movilidad.

Posteriormente el LMA determina si debe o no configurar uno de los puntos del túnel bidireccional que creará con el MAG correspondiente, esto depende de si ya existe un túnel bidireccional (creado a partir de otra sesión de movilidad de algún otro MN). Enseguida el LMA crea una ruta de los prefijos asignados sobre el túnel respectivo para que sepa por donde transmitir el tráfico dirigido al prefijo asociado a cierta sesión de movilidad. Los campos contenidos en el mensaje PBA se observan en la figura 6.11.

| **Encabezado IPv6**<br><br>Origen: LMAA<br>Destino: Proxy-CoA | **Encabezado de Movilidad**<br>BA (P) | **Opciones de Movilidad**<br>MNI, HNP, Indicador de Handoff, Tipo de tecnología de acceso. [Fecha y hora, Identificador de capa de enlace del MN, Dirección de enlace local] |
|---|---|---|

Figura 6.11 Mensaje PBA

Una vez que el MAG recibe el mensaje PBA lo procesa para saber si fue aceptado o no el registro del MN, si el registro fue exitoso, el MAG configura uno de los puntos del túnel que formará con el LMA (en caso de que aplique) y se auto-configura para mandar por dicho túnel todos los paquetes que reciba de parte del MN destinados a un nodo dentro o fuera del dominio PMIPv6. Con la información recibida el MAG puede simular la información del enlace local respectivo y enviar un mensaje RA al MN para anunciarle el prefijo que le fue asignado y el valor de MTU que debe utilizar (reflejando la existencia del túnel formado entre el MAG y el LMA). Es preferible que el MAG y el LMA periódicamente corroboren que no han existido cambios en el valor de la MTU a fin de que puedan emplear correctamente un valor actual y sean capaces de mantener la eficiencia en la entrega de los mensajes. Finalmente para reflejar el correcto registro del MN, el MAG crea una entrada en su estructura de datos BUL.

El MN configura su interfaz (o interfaces) a través de stateless o stateful (según las políticas de la red) para adquirir una dirección (o varias) del prefijo de red recibido. Opcionalmente cuando el tiempo de registro del MN esté por terminarse el MAG podrá mandar un mensaje PBU al LMA para solicitarle que extienda dicho lapso de tiempo sin embargo, antes de esto el MAG deberá asegurarse de que el MN aún

continua presente en su red a través de mecanismos como: eventos de capa de enlace (depende de la tecnología de acceso), notificación del LMA, NUD, etc. El LMA a su vez se encargará de prolongar y actualizar la entrada correspondiente en su BC y transmitir un mensaje PBA al MAG para informarle el nuevo periodo de tiempo que le ha sido asignado al MN.

b) *El MN se desplaza dentro de un mismo dominio PMIPv6* (figura 6.12): cuando un MN se mueve en un único dominio PMIPv6 (cambiando solamente de MAG) conserva los mismos datos que obtuvo de su primer registro en el dominio.

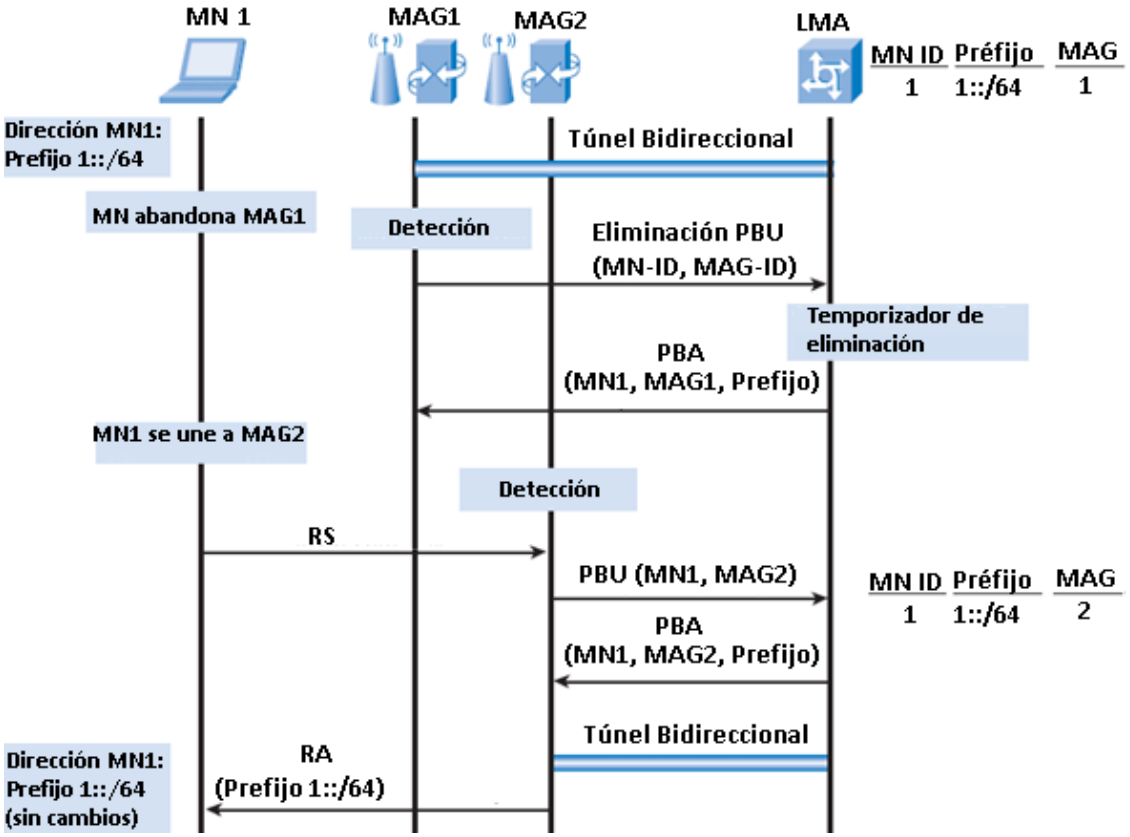



Figura 6.12 Desplazamiento de MN dentro del mismo dominio PMIPv6

Si el MN se desplaza a una ubicación distinta por ejemplo cambiando de un MAG1 a un MAG2 (ambos pertenecientes al mismo dominio PMIPv6) pasará cierto tiempo hasta que el MAG1 se percate de dicho evento, tras lo cual transmitirá un mensaje PBU al LMA solicitándole que elimine el registro correspondiente (colocando el campo Tiempo de vida en 0).

Enseguida que el LMA reciba ese mensaje identifica la sesión de movilidad asociada a dicho MN y espera un cierto tiempo antes de realizar alguna acción (temporizador) mientras tanto, elimina todos los paquetes que reciba destinados a ese MN. Por su parte cuando el MN se desplaza físicamente no deberá percatarse

que ha pasado del MAG1 al MAG2 pero, este último si debe estar consciente de ello e inmediatamente tendrá que enviar un mensaje PBU al LMA para informarle de la nueva ubicación del MN (valor mayor a 0 en el campo Tiempo de vida).

En PMIPv6 existe un inconveniente en el mensaje PBU enviado por el MAG2 ya que éste desconoce el valor que debe contener el campo Número de Secuencia para que el LMA acepte el mensaje, para ello existen 2 posibles soluciones: obtener los valores de secuencia de un dispositivo que almacene políticas de red o emplear el campo Fecha y hora. Este campo se basa en el manejo y comparación de la hora del MAG y el LMA de tal forma que si la diferencia de tiempo que existe entre la hora de envío del MAG y la hora de recepción del LMA está dentro de cierto rango definido, se acepta el mensaje PBU, de lo contrario se descarta.

Si el LMA no recibe ningún mensaje PBU antes de que expire el temporizador, asume que el MN se encuentra en un nuevo dominio realiza lo siguiente: elimina la sesión de movilidad, libera el prefijo asociado a tal MN y consulta si el tiempo de expiración del túnel ha sido alcanzado (en caso de haber sido creado dinámicamente); si existen otros MNs que hacen uso del túnel que mantiene con el MAG1, lo deja intacto pero, en caso contrario lo elimina (a menos claro que haya sido creado de forma permanente).

Si el temporizador aún no expira, el LMA recibe ese mensaje PBU y en vez de eliminar la entrada correspondiente de su BC (sesión de movilidad) actualiza la asociación que tiene con tal MN, adicionalmente también verifica si ya tiene configurado el punto final del túnel con el MAG2 (debido a un registro anterior de otro MN), de ser así ya no crea un túnel, de lo contrario procede a configurarlo. Después de esto el LMA transmite al MAG2 un mensaje PBA para informarle el estado de la asociación del MN y las acciones a realizar.

Ahora el MAG2 transmite un mensaje RA donde anuncia el prefijo asociado al MN, provocando que este último se mantenga al margen de los mensajes de movilidad mientras se desplaza dentro del dominio.

Por su parte el LMA también transmite un mensaje PBA al MAG1 para informarle que deje de anunciar el enlace local del MN.

Con la serie de acciones realizadas anteriormente, todas las comunicaciones en curso del MN continúan funcionando y todo sin que éste se percate siquiera que se está moviendo dentro de un dominio PMIPv6.

Ya se conocen los 2 eventos más representativos de PMIPv6 ahora se procederá a describir la manera en que el MN sigue comunicándose con algún CN (figura 6.13):

- El CN manda paquetes dirigidos al MN.
- Cuando el LMA haya registrado o actualizado la asociación del MN entonces, podrá recibir los paquetes destinados a dicho nodo y consultar su BC para determinar el túnel que debe utilizar para reenviarlos. Es precisamente gracias a la existencia de tal túnel que es posible llevar a cabo la entrega final de los paquetes, en la encapsulación que se lleva a cabo (usualmente IPv6 en IPv6) los puntos finales del túnel son las direcciones: LMAA (del LMA) y Proxy-CoA (del MAG).
- Una vez que el MAG correspondiente remueve el encabezado exterior, consulta su BUL para conocer la interfaz por la que debe enviar los paquetes destinados al MN.

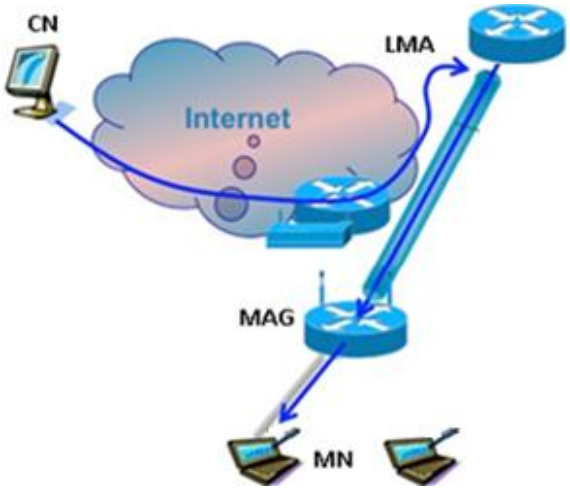



Figura 6.13: Comunicación de CN a MN en PMIPv6

Particularmente aquellos CNs que estén dentro del mismo dominio que el MN, en algunos casos podrán enviarle sus paquetes directamente sin que tengan que ser interceptados por el LMA, es decir, no es necesario que los paquetes se encapsulen y sean enviados a través de un túnel sino que simplemente pueden ser mandados al MAG donde se encuentre el MN; pese a esto el desarrollo de tal comunicación depende de las políticas de la red, por ejemplo: manejo de la seguridad, cobro de servicio, etc.

Otro punto a contemplar es que PMIPv6 puede permitir a los MNs poseer diferentes direcciones, ya sea porque el LMA le asigne diferentes prefijos al enlace local del MN o porque el MN posee varias interfaces conectadas simultáneamente al mismo dominio (el LMA asigna una sesión de movilidad distinta por interfaz). Cualquiera que sea el caso cada sesión de movilidad debe ser representada por una entrada diferente en la BC para mantener registros distintos asignados a cada MN. Precisamente por esa capacidad de

multihoming es necesario distinguir entre los distintos indicadores de handover que suelen presentarse en PMIPv6 (tabla 6.4).

Tabla 6.4 Indicadores de Handover en PMIPv6 [32]

| Valor | Descripción |
|---|---|
| 0 | Reservado para uso futuro. |
| 1 | Asociación mediante una nueva interfaz: se crea una nueva sesión de movilidad. |
| 2 | Handover entre diferentes interfaces del MN: para acceder a la red el MN cambia su interfaz. |
| 3 | Handover entre diferentes MAGs de la misma interfaz del MN: existe una sesión de movilidad. |
| 4 | Handover de estado desconocido: el MAG es incapaz de determinar si existe una sesión de movilidad actual asociada a un MN. |
| 5 | Handover de estado no cambiante: se solicita una renovación de una sesión de movilidad de un MN. |

Debido a la existencia de los indicadores antes mencionados, es necesario que existan ciertos mecanismos de transferencia de contexto entre los MAGs del dominio, por ejemplo se puede hacer uso de un nodo que almacene políticas de perfiles del dominio PMIPv6, en cuyo caso la información a guardar sería la siguiente:

- El identificador de cada MN.
- La dirección LMAA del LMA.
- El prefijo de red asignado a cada interfaz de los MNs (opcional).
- El tiempo de vida asignado a cada prefijo de red.
- Los procedimientos de auto-configuración soportados en el dominio PMIPv6 (stateless, stateful o ambos).

Otro punto a tomar en cuenta es que PMIPv6 además de brindar sus servicios en las redes IPv6 también lo hace con las redes IPv4 (véase el RFC 5844 [33]), capacidad que sin duda lo convierte en un candidato bastante atractivo y con mucho potencial por delante. Lograr esto implica que el MN adquiera una dirección IPv4 HoA a través de la cual sea posible intercambiar tráfico de señalización sobre una red IPv4 por lo tanto, dentro del dominio PMIPv6 el LMA y los correspondientes MAGs deben tener una dirección IPv4 configurada (IPv4-LMAA y IPv4-Proxy CoA respectivamente). En la figura 6.14 se aprecian los elementos que interactúan dentro de PMIPv6 para lograr operar en una red IPv4, y algo sumamente representativo es la flexibilidad que adquieren los MNs porque pueden obtener una dirección HoA en IPv4 o IPv6, es decir, tienen la posibilidad de recibir alguna de ellas o inclusive ambas, dependiendo únicamente de sus propias capacidades y del soporte de las redes en que se encuentren.

Hasta el momento se han mencionado las formas en que el MN adquiere su dirección HoA en IPv6 no obstante, para IPv4 se puede recurrir a una configuración estática, un servidor DHCP, IKEv2, etc. A pesar de estas diferencias que existen es importante conocer que todas las direcciones HoA que sean asignadas a una interfaz del MN serán administradas por una sola sesión de movilidad, independientemente de si son direcciones IPv4 o IPv6, por ejemplo en aquellos casos donde el MN posea varias interfaces será necesario que el LMA tenga una entrada diferente para cada una de ellas en su BC.

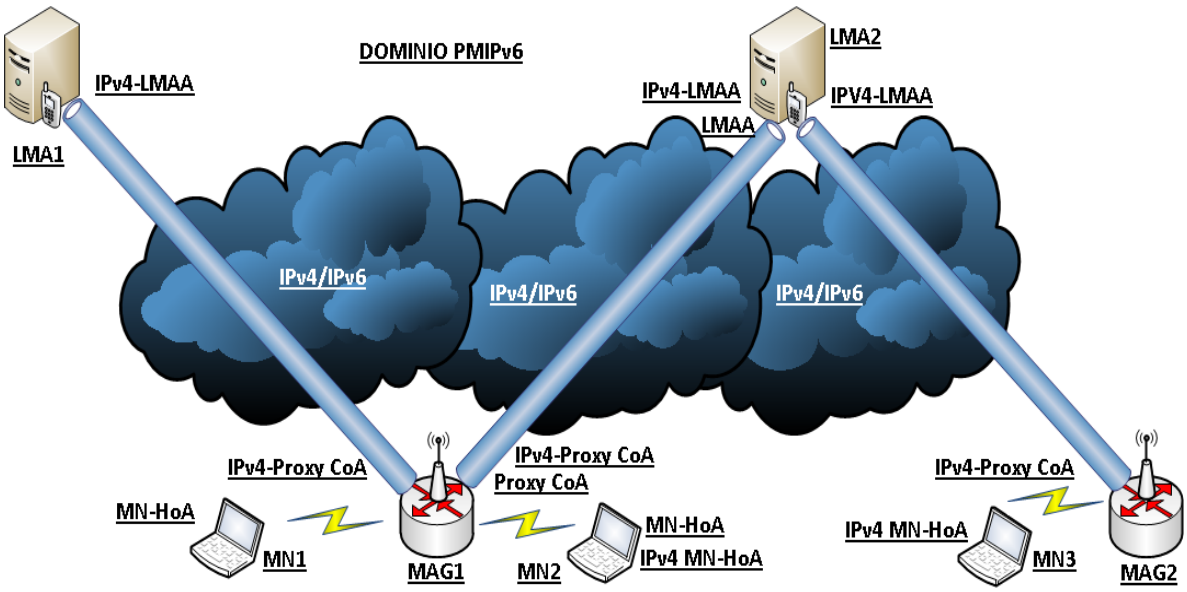



Figura 6.14 Soporte de IPv4 en PMIPv6

Es necesario tener bien en claro que independientemente de la versión de IP usada en el dominio PMIPv6, el protocolo que se utiliza es PMIPv6 por lo tanto, cuando un MN entra por primera vez a un cierto dominio y adquiere una dirección HoA en IPv4 sucede algo muy similar a lo que acontece con IPv6, es decir, el MN conserva dicha dirección durante toda su estancia en el dominio y no se percata de que al desplazarse dentro de éste va cambiando de MAGs. Específicamente cuando un MN utilice IPv4 para su configuración de red el LMA necesita almacenar nueva información:

- ⇒ La dirección IPv4 HoA asignada a alguna de las interfaces del MN (según aplique).
- ⇒ La máscara de red a utilizar.
- ⇒ La dirección IPv4 perteneciente al ruteador por defecto del MN.

Finalmente no se debe olvidar que actualmente existen muchos agentes maliciosos en la red que pueden llevar a cabo un sinfín de ataques, y teniendo esto en mente es que se necesitan proteger los mensajes de movilidad intercambiados entre el MAG y el LMA, por ejemplo al usar IPSec en modo transporte se puede proporcionar autenticación e

integridad, y adicionalmente al manejarlo en modo túnel se llega a tener confidencialidad en el resto de las comunicaciones.

Dado que las interacciones que se llevan a cabo entre el LMA y el MAG son una tarea crítica es necesario que ambos se identifiquen y autentiquen, de esta forma se logra que el LMA únicamente permita solicitudes de registro de MAGs autorizados, y al mismo tiempo éstos tienen la certeza de que el LMA con que se comunican es auténtico. Algunas propuestas contemplan el uso de servidores de Autenticación Autorización y Contabilidad, AAA por sus siglas en inglés (Authentication, Authorization and Accounting) o algún servidor que contenga las políticas de uso del dominio PMIPv6. Adicionalmente para evitar que se produzca un rastreo del MAG donde se localiza cada MN habrá que plantear el uso de identificadores temporales, dando oportunidad a que todos los MNs puedan tener una identidad distinta cada vez que se tengan que autenticar.

## 6.5 MIPv6 CON SOPORTE PILA DUAL

En lo que va del capítulo todas las mejoras de la movilidad que se han visto se basan exclusivamente en IPv6 (excepto PMIPv6) sin embargo, debido a que actualmente esa versión de IP no es ampliamente utilizada no es posible que los dispositivos utilicen de un día para otro únicamente direcciones IPv6 por ello, se pensó en desarrollar MIPv6 con soporte Pila Dual, DSMIPv6 por sus siglas en inglés (Dual Stack MIPv6). Esta mejora se específica en el RFC 5555 [34] y permite a MIPv6 funcionar en ruteadores y hosts con soporte dual, es decir, hace posible que tanto el MN como el HA soporten MIPv6 a través de IPv4, IPv6 o ambos.

El presente escenario permite al MN utilizar IPv4 o IPv6 en la asignación de su dirección CoA y en el prefijo que adquiere, lo cual es posible porque el MN al crear un túnel con su HA puede estar en una red IPv6 o IPv4 (con la excepción de cuando el MN regresa a su red local y viene de una red IPv4) pero, sin tener que utilizar simultáneamente MIPv4 y MIPv6.

Si el MN se encuentra en una red que sólo soporta IPv4 debe conocer la dirección IPv4 de su HA, ya sea que la tenga pre-configurada o la descubra a través del servicio DNS (necesita conocer al nombre de su HA). Por su parte cuando el MN está en una red con soporte de IPv6 podrá hacer uso de las funcionalidades adicionales de MIPv6, por ende es aconsejable que ante una red con soporte de IPv4 e IPv6 preferentemente se elija IPv6 aunque, también se puede plantear la posibilidad de tener una dirección HoA para ambas versiones de IP. En la figura 6.15 se presentan algunos ejemplos.

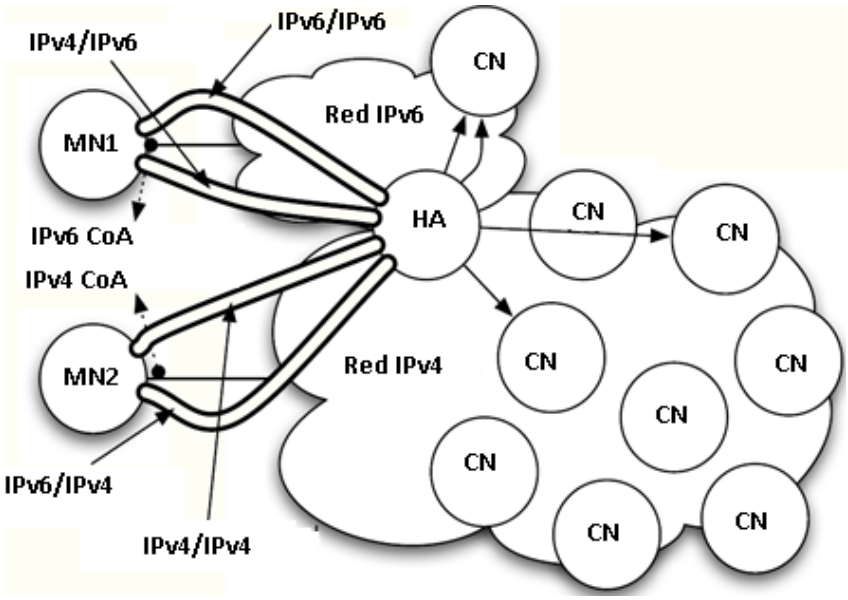



Figura 6.15 MIPv6 en nodos con soporte dual

Evidentemente tener soporte de MIPv6 en hosts y ruteadores duales trae consigo una gran complejidad en las comunicaciones móviles, de manera que hoy en día únicamente se soportan los siguientes casos (figura 6.16) [34]:

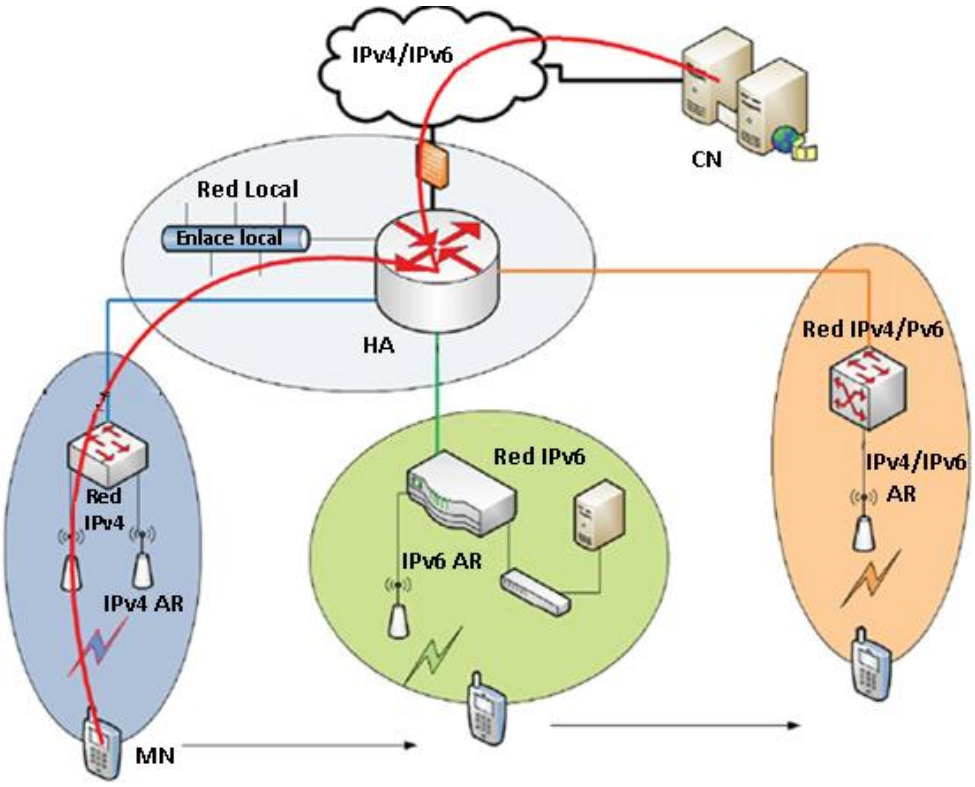



Figura 6.16 Casos soportados por MIPv6 en nodos duales

a) *Red Foránea ofrece conectividad IPv6:* el MN adquiere una dirección CoA en la red IPv6 donde se encuentra actualmente y opcionalmente puede incluir en su mensaje BU la opción Home Address IPv4.

   Si el HA del MN está de acuerdo con tal opción crea 2 entradas en su BC (una para IPv4 y otra para IPv6) asociadas a la dirección IPv6 del MN. El HA debe incluir las opciones que acepta en el mensaje BA que transmita para que el MN pueda saber si fue aceptado o no el uso de una dirección IPv4. Si el HA aceptó la opción anterior recibe paquetes dirigidos a la dirección HoA del MN y se los envía a su posición actual a través de un túnel IPv4/IPv6 ó IPv6/IPv6.

b) *Red Foránea ofrece conectividad IPv4:* ya que el MN únicamente puede adquirir una dirección IPv4 CoA (su HA también necesita tener configurada una dirección IPv4) y una dirección IPv4 HoA (ya asignada o solicitando alguna a su HA), deberá remover las entradas relacionadas a cualquier CN no obstante, antes de que todo esto acontezca el HA necesita conocer si se emplea o no NAT en la red actual del MN, dependiendo de ello existen 2 opciones:

   1) No existe NAT: el MN obtiene una dirección única y global de la red foránea, lo cual implica que transmitirá un mensaje BU a la dirección IPv4 de su HA usando una encapsulación IPv6/IPv4. El MN utiliza su dirección IPv6 HoA en la opción Home Address y su dirección IPv4 en el campo Opción IPv4 CoA; adicionalmente el MN puede colocar la opción Home Address IPv4.

      El HA crea las entradas correspondientes en su BC según las opciones que haya recibido y las políticas de uso con que haya sido configurado, posteriormente envía un mensaje BA al MN informándole de los registros que ha creado, por ejemplo: si acepta la dirección IPv4 HoA del MN o le asigna una dirección IPv4 HoA, el mensaje BA incluye la opción Acuse de Recibo de Dirección IPv4.

      El MN al recibir el mensaje BA sabe si sus asociaciones fueron o no exitosas. Finalmente cuando el HA reciba paquetes dirigidos a la dirección HoA del MN (IPv4 o IPv6) podrá enviárselos correctamente a su dirección IPv4 CoA.

   2) Existencia de NAT: el MN obtiene una dirección privada de la red foránea por lo tanto, para lidiar con la presencia de NAT usa un túnel que encapsule paquetes IPv6 a través de UDP e IPv4, es decir, todos los paquetes destinados al MN que el HA reciba tendrán como origen y destino lo siguiente(según corresponda): dirección IPv6 HoA del MN, dirección IPv6 del CN; posteriormente estos paquetes se encapsulan a través de UDP e IPv4 (en ese orden) tomando como

origen y destino dirección IPv4 del HA y dirección IPv4 CoA del MN (según la dirección de las comunicaciones).

Debido a que hoy en día es muy usual que las redes hagan uso de NAT en IPv4, resulta interesante conocer el escenario donde el MN se ubica en una red con esa característica porque ello implica que el MN necesita descubrir dicha condición en su red actual mediante lo siguiente:

i. El MN transmite un mensaje BU a su HA realizando una encapsulación primero en UDP y posteriormente en IPv4.

ii. Al recibir este mensaje el HA compara la dirección origen del encabezado IPv4 con la dirección contenida en el campo de la Opción IPv4 CoA, el que las direcciones coincidan es un indicio para el HA de que no se está usando NAT, de no ser así el HA debe enviar un mensaje BA con el campo Opción de Detección NAT para indicarle al MN que se detectó el uso de NAT en su red IPv4.

iii. El MN al recibir el mensaje BA conoce el tipo de encapsulación a emplear y actualiza sus entradas correspondientes en su BUL. De esta manera es como el MN y su HA comienzan a intercambiar paquetes encapsulados en UDP y en IPv4. Después de cierto tiempo el MN debe renovar sus asociaciones para indicarle a su HA que aún necesita el soporte de movilidad (ambos negocian los tiempos a usar o es el HA quien indica un determinado lapso de tiempo).

    Opcionalmente el MN puede solicitarle a su HA que encapsulen los paquetes que vayan a intercambiar entre sí a través de UDP independientemente de si se haya detectado o no el uso de NAT pero, la decisión de aceptar o no dicha solicitud es de su HA. Es importante tener esto en mente porque está prohibido usar una encapsulación UDP cuando el MN está en una red IPv6.

Cuando el MN se desplace a otra red o simplemente ya no desee disfrutar del soporte de MIPv6 tendrá que eliminar los registros correspondientes que posea y al mismo tiempo informarle a su HA acerca de ello, en tales circunstancias las principales consideraciones a seguir son:

- Si el MN tiene registrada una dirección IPv4 HoA, debe quitar el campo Opción Home Address IPv4 en el próximo mensaje BU que le envíe a su HA.
- El MN en estricto orden debe eliminar primero el registro de su dirección IPv4 HoA (si es que la tiene) y posteriormente el registro asociado a su dirección IPv6 HoA.

Cuando el MN desea eliminar todos los registros que posee con su HA basta con que envíe un mensaje BU colocando un valor de 0 en el campo Tiempo de vida.

Para entender mejor el formato de los mensajes implicados en MIPv6 con soporte pila dual se presentan a continuación los casos más representativos:

a) Mensaje BU enviado por el MN a su HA (figura 6.17).

| **Encabezado IPv4** Origen: HoA Destino: HA | **Encabezado UDP** (Cuando así se requiera) | **Encabezado IPv6** Origen: HoA Destino: HA | **Encabezado ESP** Modo Transporte | **Encabezado de Movilidad** BU | **IPv4 HoA** | **IPv4 CoA** |
|---|---|---|---|---|---|---|

Figura 6.17 Mensaje BU en DSMIPv6

b) Mensaje BA enviado por el HA al MN (figura 6.18).

| **Encabezado IPv4** Origen: HA Destino: HoA | **Encabezado UDP** (Cuando así se requiera) | **Encabezado IPv6** Origen: HA Destino: HoA | **Encabezado ESP** Modo Transporte | **Encabezado de Movilidad** BA | **IPv4 Ack** | **NAT** |
|---|---|---|---|---|---|---|

Figura 6.18 Mensaje BA en DSMIPv6

c) El CN recibe paquetes cuando el MN está en una red IPv4 (figura 6.19).

| **Encabezado IPv4** Origen: CoA Destino: HA | **Encabezado UDP** (Cuando así se requiera) | **Encabezado IPv6** Origen: HoA Destino: CN | **Encabezado de Protocolos de capas superiores** |
|---|---|---|---|

Figura 6.19 Mensaje de comunicación del MN a CN en DSMIPv6

d) Envío de paquetes del CN a la red IPv4 donde está el MN (figura 6.20).

| **Encabezado IPv4** Origen: HA Destino: CoA | **Encabezado UDP** (Cuando así se requiera) | **Encabezado IPv6** Origen: CN Destino: HoA | **Encabezado de Protocolos de capas superiores** |
|---|---|---|---|

Figura 6.20 Mensaje de comunicación del CN al MN en DSMIPv6

Hasta el momento con los escenarios antes vistos es claro que las funcionalidades de MIPv6 que el MN utiliza dependen del tipo de red en que se encuentre, por ejemplo: cuando el MN se ubica en una red con soporte IPv6 podrá hacer uso de Optimización de Ruta, DHAAD, etc., procesos que no se pueden realizar cuando la red en que está solamente soporta IPv4 a pesar de ello, es evidente que MIPv6 con soporte pila dual amplía en la medida de lo posible las facilidades y capacidades de movilidad del MN sin agregar mayor complejidad de la necesaria al proceso de comunicación.

Por último se hablará de algunos de los aspectos de seguridad que deben ser considerados a fin de mantener el mismo nivel de protección (o al menos similar) en las comunicaciones del MN, ya sea que éste se encuentre en una red IPv4 o IPv6. Para alcanzar dicho objetivo habrá que contemplar lo siguiente:

⇒ Es recomendable que los mensajes de movilidad sean protegidos a través de IPSec en modo túnel (empleando IKEv2 para establecer las SAs). Se aprecia este escenario en la figura 6.21.

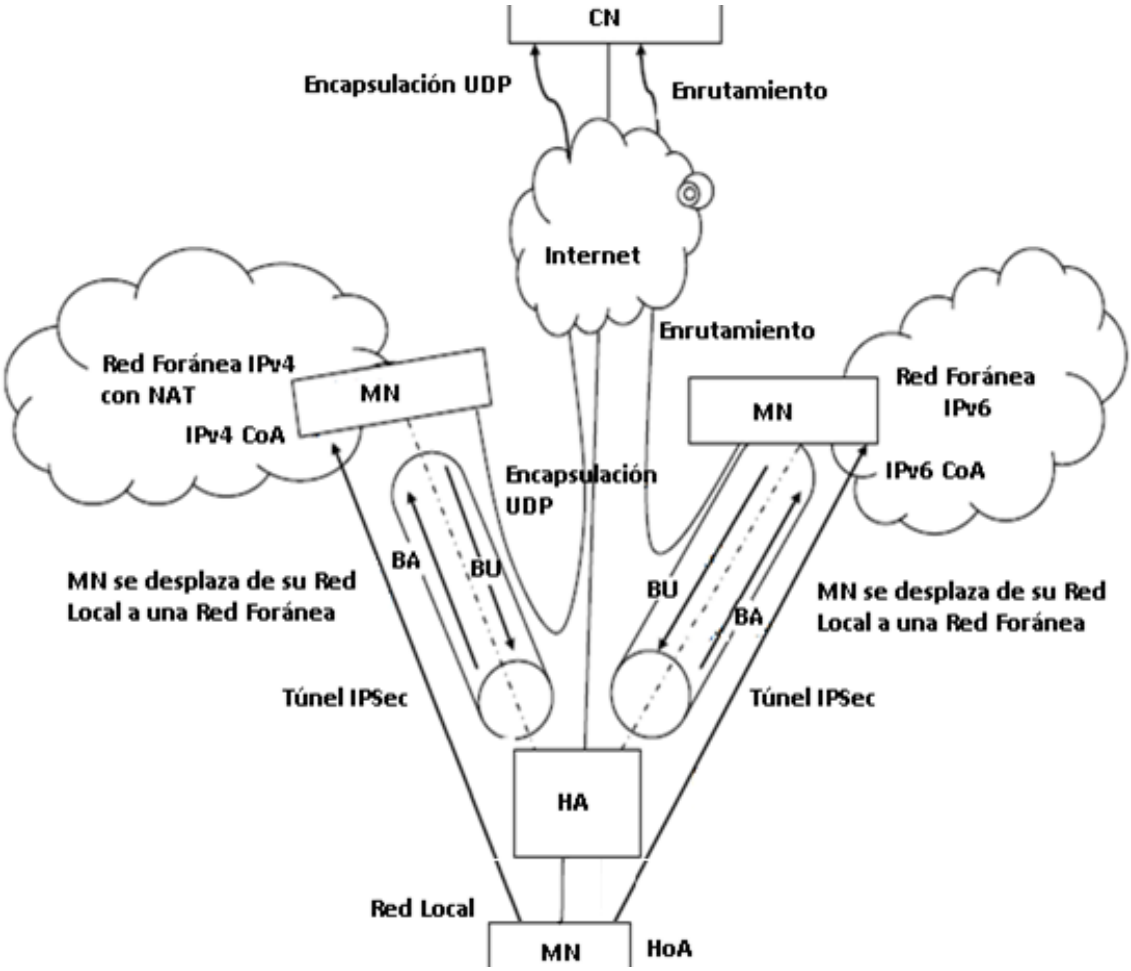



Figura 6.21 Uso de IPsec en DSMIPv6

⇒ Para que el HA pueda aceptar la dirección IPv4 HoA del MN primero tiene que relacionarla con la respectiva dirección IPv6 HoA.

⇒ Debido a que el contenido del encabezado IPv4 no es autenticado por el HA pueden existir varios problemas de seguridad por ende, es necesario que los paquetes sean autenticados con base a la dirección IPv6 HoA del MN.

## 6.6 MOVILIDAD DE RED

Ya se mencionó anteriormente que delegar las funciones de movilidad a la red (en vez de al host) es más productivo y resulta bastante beneficioso, particularmente existe además de PMIPv6 una mejora denominada Movilidad de Red, NEMO por sus siglas en inglés (Network Mobility) que funciona siguiendo un principio similar. La idea surgió pensando en permitir a todos los nodos de una red (ya sea que tengan o no soporte de MIPv6) mantener sus sesiones de forma ininterrumpida mientras la red en la que se encuentran se desplaza físicamente y por ende experimenta un cambio en su punto de acceso (para más detalles remítase al RFC 3963 [35]). Antes de continuar es necesario familiarizarse con ciertos términos de NEMO (tabla 6.5).

Tabla 6.5 Elementos de NEMO

| Elemento | Descripción |
|---|---|
| Ruteador de Acceso | AR por sus siglas en inglés (Access Router): es el ruteador conectado al MR que usualmente le proporciona acceso a Internet |
| Ruteador Móvil | MR por sus siglas en inglés (Mobile Router): ruteador encargado de proporcionar el soporte de movilidad a toda la red. |
| Interfaz de egreso | Interfaz o grupo de interfaces que el MR usa para enviar paquetes de alguno de sus nodos de red hacia algún CN que se encuentra en otra red. Esta interfaz está unida a la red local del MR o a una red foránea, según sea el caso. |
| Interfaz de ingreso | Interfaz o grupo de interfaces que el MR utiliza para mandar un paquete hacia uno de los nodos de su red. |
| Nodo de Red Móvil | MNN por sus siglas en inglés (Mobile Network Node): cualquier nodo localizado dentro de la red administrada por el MR. Los nodos se clasifican como:<br>Nodo Fijo Local, LFN por sus siglas en inglés (Local Fixed Node): nodo originario de la red móvil que no tiene soporte de MIPv6.<br>Nodo Móvil Local, LMN por sus siglas en inglés (Local Mobile Node): nodo móvil con soporte de MIPv6 que pertenece a la red móvil.<br>Nodo Móvil Visitante, VMN por sus siglas en inglés (Visited Mobile Node): nodo con soporte de MIPv6 que está de visita en la red móvil. |
| Entidad Corresponsal | CE por sus siglas en inglés (Correspondent Entity): nodo (CN o Ruteador Corresponsal) con el que el MR o algún MNN establece una optimización de ruta. |
| Prefijo de Red Móvil | MNP por sus siglas en inglés (Mobile Network Prefix): conjunto de prefijos IPv6 que se asignan al MR (por parte de un HA) para que éste los anuncie en la red donde vaya a dar soporte de movilidad. |
| Agente Local | Ruteador capaz de soportar NEMO que puede registrar a un MR. |

La diferencia que existe entre NEMO y MIPv6 se aprecia fácilmente en la figura 6.22.

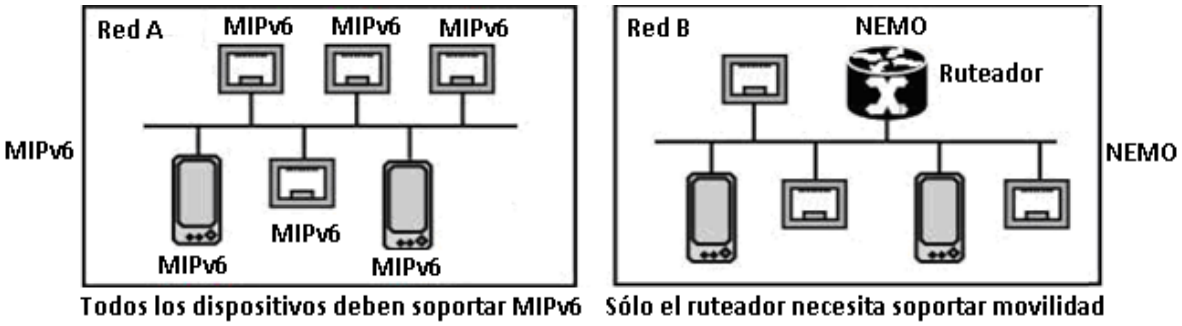



Figura 6.22 Diferencia entre MIPv6 y NEMO

MIPv6 es muy similar a NEMO aunque específicamente en este último es necesario que exista en la red un Gateway por defecto denominado MR, precisamente este ruteador al detectar que está en una red foránea manda un mensaje BU a su HA para registrarse (figura 6.23). Se adicionan al mensaje BU las siguientes características:

- Bandera R activada: indica que el ruteador tiene soporte de MR.
- Prefijos asignados al MR.
- HoA: dirección IPv6 permanente asignada al MR (puede poseer una dirección HoA por cada prefijo recibido por su HA).
- CoA: dirección que el MR adquiere mientras se encuentra en una red foránea.

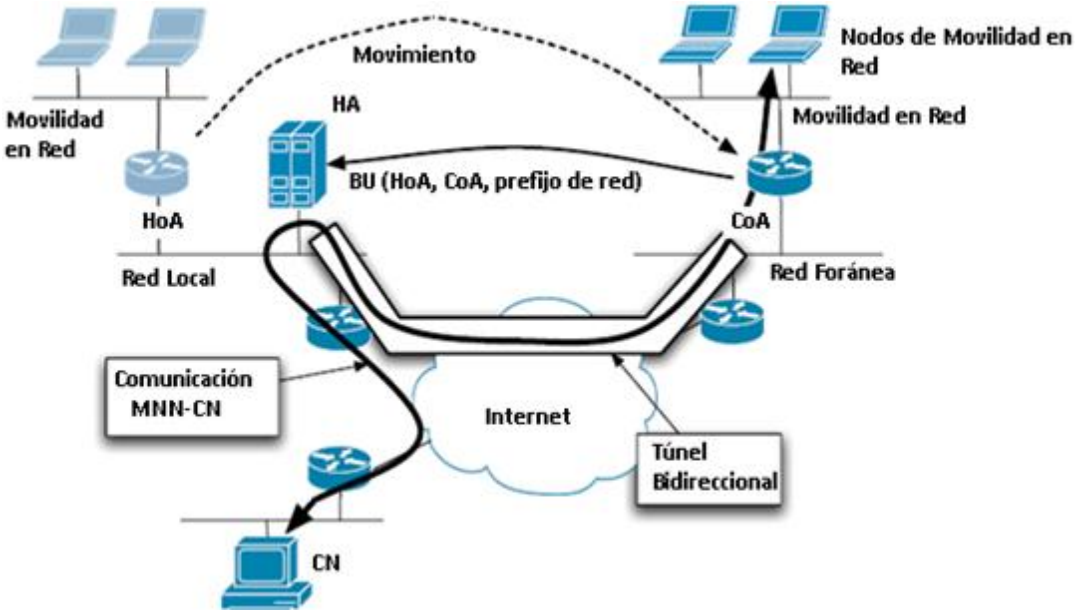



Figura 6.23 Registro del MR

El HA a su vez manda un mensaje BA a la dirección CoA respectiva indicando si tiene o no soporte para registrar a un nodo con capacidad de MR, si posee dicho soporte el estado del mensaje es menor a 128, en caso contrario el MR necesita ejecutar el proceso DHAAD para conocer algún HA en su red local que posea ese soporte (el MR primero tiene que

eliminar su registro anterior antes de intentar registrarse con otro HA). Si el registro no es exitoso el HA le indica al MR la causa de la falla, los estados se muestran en la tabla 6.6.

Tabla 6.6 Nuevos estados de MR

| Estado | Descripción |
|---|---|
| 140 | Operación de Ruteador Móvil no permitida: el HA no soporta registrar MRs. |
| 141 | Prefijo inválido: uno o varios prefijos de los recibidos son inválidos. |
| 142 | Prefijo no autorizado: uno o más prefijos no pueden usarse con la dirección HoA. |
| 143 | Prefijos faltantes: no existe suficiente información para configurar al MR. |

Cuando el registro es satisfactorio se forma un túnel bidireccional entre el MR y su HA (figura 6.24), siendo este último el encargado de recibir todos los paquetes destinados a los prefijos asignados al MR y enviarlos a través del túnel a la dirección CoA correspondiente. El MR recibe tales paquetes por su interfaz de egreso y verifica que se dirijan a direcciones que pertenezcan a uno de los prefijos de red que le fueron asignados; de no cumplirse esto elimina los paquetes, de lo contrario los transmite por su interfaz de ingreso respectiva.

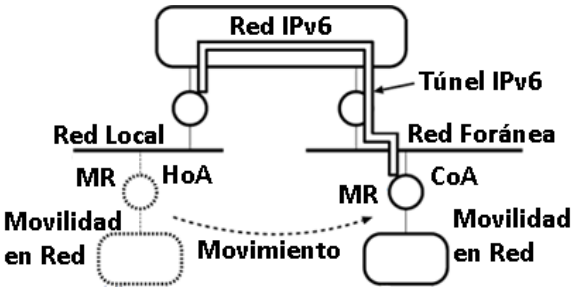



Figura 6.24 Movimiento del MR

Para hacer uso del túnel es necesario llevar a cabo una encapsulación (figura 6.25) de manera que las comunicaciones desde/hacia algún CN se mantengan ininterrumpidas.

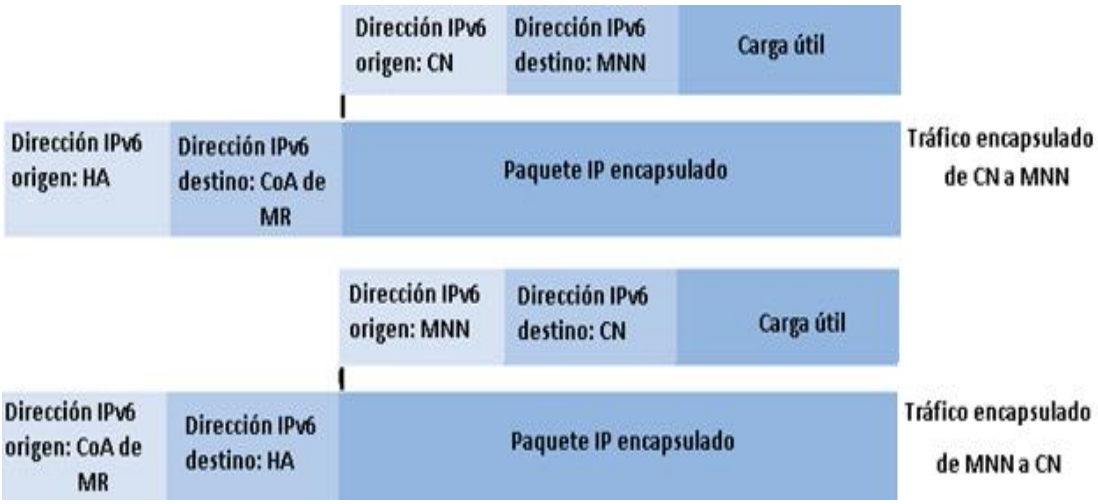



Figura 6.25 Encapsulación en NEMO

El túnel creado puede considerarse como una interfaz de túnel si existe un protocolo de ruteo activado dentro de éste, de ser así los mensajes BU que el MR mande a su HA no deben contener información acerca de los prefijos que tiene asignados porque son los mensajes de los protocolos de ruteo los encargados de informar de cualquier cambio que ocurra en los prefijos asignados al MR. Para aquellos casos donde no se esté utilizando un protocolo de ruteo existen 2 modos principales en que el HA puede conocer los prefijos asignados a cierto MR (figura 6.26) [35]:

a) *Modo implícito:* los mensajes BU que el MR transmite a su HA no contienen la opción Prefijo de Red Móvil porque el HA determina dicha información con base a otros mecanismos, por ejemplo mediante una configuración manual realizada con anterioridad.

b) *Modo explícito:* el MR en sus mensajes BU contiene la opción Prefijo de Red Móvil para informar a su HA los prefijos que tiene asignados. A su vez el HA para mantener dicha información debe almacenarla en su BC (tabla de prefijos).

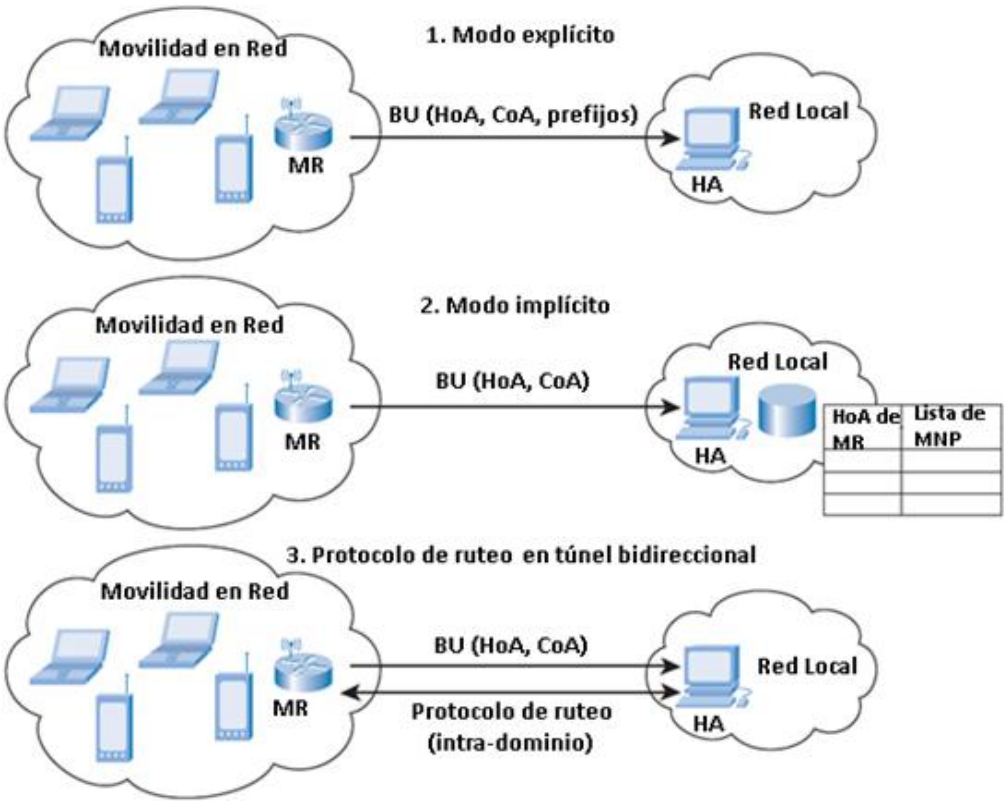



Figura 6.26 Envío de información de MNP

Hasta ahora se han descrito todos aquellos elementos que permiten al MR registrarse y obtener la información que necesita para funcionar sin embargo, una vez que el MR esté en una red foránea es necesario que desarrolle las siguientes conductas:

- Por su interfaz de egreso el MR podrá responder a los mensajes NS que reciba pero, no deberá enviar mensajes RA no solicitados ni responder a ningún mensaje RS. El MR únicamente debe usar los mensajes RA que reciba en su interfaz de egreso para llevar a cabo tareas como: autoconfiguración, elección de su ruteador por defecto y la detección de cuando se haya desplazado a otra red.

- Por su interfaz de ingreso el MN debe transmitir mensajes RA y responder los mensajes RS (para evitar que lo elijan como ruteador por defecto necesita colocar 0 en el campo Tiempo de vida). Adicionalmente el MR puede mandar mensajes de algún protocolo de ruteo por su interfaz de ingreso para comunicar dicha información a algún MR que esté en la red donde da soporte de movilidad.

Como se mencionó con anterioridad el MR da soporte de movilidad a los diferentes tipos de nodos dentro de una red porque existe la posibilidad de que un MR esté en determinado tiempo dentro de la red de otro MR, situación que comúnmente se denomina NEMO anidada. En esos casos el MR interno se denomina sub-MR y la red a la que da soporte de movilidad es sub-NEMO; mientras tanto el MR principal es llamado root-MR o parent-MR y su red se denomina root-NEMO o parent-NEMO (figura 6.27).

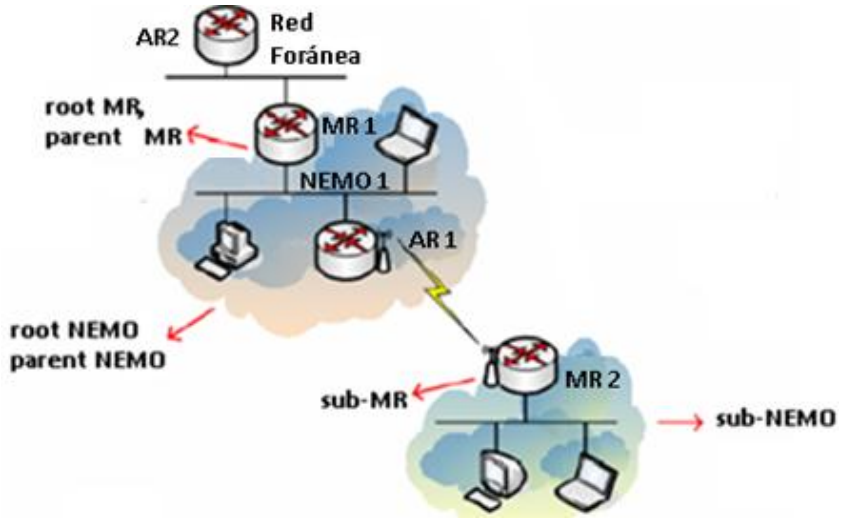



Figura 6.27 NEMO anidada

Un caso interesante ocurre cuando en una NEMO anidada la red root-NEMO se desplaza físicamente y se ubica dentro de alguna de sus redes sub-NEMO, situación que ocasiona que esta última se convierta en la root-NEMO y por ende ambas redes se quedan temporalmente sin conectividad. La figura 6.28 muestra una situación que hoy en día no es muy común sin embargo, se tiene que evaluar la manera de eficientar las comunicaciones en NEMO ya que aún no se ha definido una comunicación con optimización de ruta (analóga a MIPv6) precisamente por esto, suele presentarse un fenómeno conocido como “Ruta Pinball”: en las comunicaciones desarrolladas entre un

MNN (ubicado en una NEMO anidada) y algún CN los paquetes pasan por más de un HA antes de poder ser entregados a su destinatario final (figura 6.28).

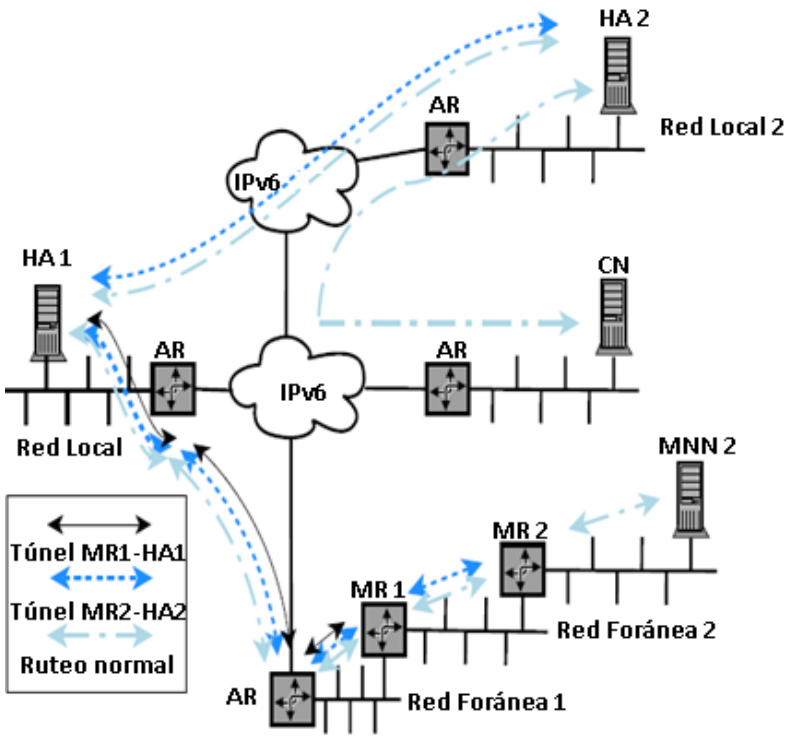



Figura 6.28 Fenómeno de "Ruta Pinball"

Es evidente que actualmente existen varios inconvenientes que se llegan a presentar en una NEMO anidada, algunos de los cuales son:

- ✓ *Aumento del procesamiento de paquetes:* debido a que se realizan varias encapsulaciones la carga útil de los paquetes tiende a disminuir, además se requiere de un mayor tiempo de procesamiento por parte de los HAs para desarrollar tareas de: encapsulación, fragmentación, re-ensamblado, cálculo de la MTU, etc., elementos que en determinado momento pueden llegar consumir la mayoría de sus recursos disponibles o incluso agotarlos por completo.

- ✓ *Cuellos de botella y aumento en fallas de enlaces:* ya que no hay una comunicación directa entre un MNN y algún CN existe una mayor probabilidad de que alguno de los enlaces por los que pasan los paquetes llegue a congestionarse o inclusive experimente una falla, circunstancias que a su vez producen que los paquetes se retrasen o descarten.

- ✓ *Incremento de la latencia:* dificulta el uso de aplicaciones en tiempo real porque aplicaciones muy sensitivas no toleran el tiempo de retraso que se genera.

Con todo lo comentado es indudable que se necesitan considerar diversos elementos para poder tomar una correcta decisión de donde realizar la optimización de ruta, habrá que recordar que el propósito que se persigue es obtener las mayores ventajas posibles (en sencillez, rendimiento y tiempo) sin agregar nuevos problemas de seguridad y lidiando al mismo tiempo con las dificultades de su correcta implementación en redes foráneas donde existan diferentes políticas de uso.

En lo que respecta a la seguridad en NEMO, el MR debe realizar un filtrado en su interfaz de ingreso para asegurarse de que todos los paquetes que vaya a mandar posean una dirección origen que pertenezca a los prefijos de red que está anunciando, y al mismo tiempo debe descartar aquellos paquetes que estén usando alguna dirección que haya sido asignada a alguna de sus interfaces (situación sospechosa que puede ser un indicio de un posible ataque).

Por su parte el HA necesita verificar que los paquetes que reciba a través del túnel bidireccional creado con algún MR pertenezcan a uno de los prefijos asignados a dicho MR, de no cumplirse esto sencillamente puede descartar tales paquetes. Estas medidas aunque sencillas son bastante útiles y se implementan para evitar que algún nodo malicioso trate de llevar a cabo algún ataque en representación de un MR o MNN auténtico.

Adicionalmente, es aconsejable autenticar a los nodos que interactúan en NEMO para asegurarse que las entidades participantes son realmente quienes dicen ser, además el empleo de algún protocolo de seguridad refuerza la seguridad al brindar confidencialidad, privacidad e integridad en las comunicaciones. Desarrollos presentes involucran el uso del Descubrimiento Seguro de Vecinos, SEND por sus siglas en inglés (Secure Neighbor Discovery) y Direcciones Generadas Criptográficamente, CGAs por sus siglas en inglés (Cryptographically Generated Addresses). Habrá que esperar si son opciones viables a utilizar en NEMO o si es necesario explorar otras futuras alternativas.

Naturalmente no se describieron todas las mejoras en Movilidad IP que existen, a lo largo de este capítulo, porque se realizan desarrollos constantemente y nuevas mejoras aparecen, algunas con ideas totalmente nuevas y otras como una combinación de las principales, por ejemplo realizando una combinación de FMIPv6 y HMIPv6 surge FHMIPv6.

En el presente capítulo se trató de abarcar las mejoras más significativas que han aparecido a lo largo de los años, ya que la aportación de cada una de éstas ha contribuido notablemente a explorar características diferentes, explotar nuevas capacidades e incluso ofreciendo formas de brindar el soporte de Movilidad IPv6 totalmente distintas.

Ideas seguirán llegando, conceptos continuarán apareciendo, investigaciones conllevarán a increíbles e insólitas propuestas, pero al final lo único realmente importante es: "movilidad", y sólo unos cuantos afortunados comprenderán la complejidad de su sencillez, mientras que el resto de las personas únicamente la disfrutará y la hará parte de su vida.

Antes de finalizar este capítulo, a fin de sintetizar las características principales de las mejoras existentes de la Movilidad IPv6, se presenta la tabla 6.7 donde se realiza una comparación de los protocolos de administración de Movilidad IPv6 tratados en este capítulo.

Tabla 6.7 Protocolos de administración de Movilidad IPv6

| Característica | MIPv6 | FMIPv6 | HMIPv6 | PMIPv6 | NEMO | DSMIPv6 |
|---|---|---|---|---|---|---|
| Baja latencia en Handover | N | Y | N | Y | N | N |
| Baja sobrecarga por señalización | N | N | Y | Y | Y | N |
| Optimización de ruta | Y | N | N | N | N | - |
| Privacidad de ubicación | N | N | Y | Y | Y | N |
| Soporte en redes IPv4 e IPv6 | N | N | N | Y | N | Y |
| Movilidad delegada a host (H), red (R) | H | H | H | R | R | H |

# Capítulo 7

## Estado actual y futuro de la

## Movilidad IP

*Users will also begin using their mobile devices to control and manage other Internet enabled appliances (kitchen equipment, entertainment equipment, etc.) - Vint Cerf*

## 7.1 INTRODUCCIÓN

Cada día que pasa hay más y más investigaciones, propuestas y desarrollos en torno a las comunicaciones móviles, todo con el propósito de dar respuesta a las exigencias cada vez más demandantes, los usuarios ya son más delicados, se dan su lugar, comienzan a ser intransigentes, intempestivos, estrictos en lo que desean, con una postura firme en sus convicciones y todo para sentirse con más libertad, llenos de autonomía, deseando utilizar cada vez más servicios en todo momento y desde cualquier lugar.

Precisamente hoy en día una de las posturas que está tomando mayor fuerza es la convergencia de redes, una unión que es independiente de ambientes fijos o móviles, y por la tendencia que actualmente se observa es muy probable que tal unificación se base en el protocolo de Internet o IP, reconociéndolo como el bloque fundamental de las comunicaciones. Justamente por toda esta serie de acontecimientos en las siguientes secciones se hablará del estado actual y futuro de la movilidad IP.

## 7.2 REDES 3G

A finales del siglo pasado se observó que las capacidades de las redes 2G comenzaban a ser insuficientes y se pensó en crear la siguiente generación de redes que permitiera satisfacer los requisitos de los usuarios. Fue así como en el año 2000 la Unión Internacional de Telecomunicaciones, ITU por sus siglas en inglés (International Telecommunications Union) [36] terminó de definir IMT-2000.

IMT-2000 es la norma para las comunicaciones inalámbricas de Tercera Generación (comúnmente conocidas como redes 3G) y desde su diseño se pensó en mantener una compatibilidad con los sistemas existentes, razón por lo que no había que hacer excesivas inversiones. Las redes 3G no se limitan a proporcionar una mayor velocidad de transferencia (2Mbps en ambientes fijos y 384Kbps en ambientes móviles), su creación va más allá al permitir utilizar nuevos sistemas y servicios, situación que indudablemente contribuyó al crecimiento en la cantidad de usuarios y áreas de cobertura disponibles. Más que estandarizar una tecnología con IMT-2000 lo que se pretendió fue definir las características que una red debe cumplir para ser considerada una red 3G, algunas de las más sobresalientes son:

- Transmisión simétrica/asimétrica.
- Ancho de banda dinámico.
- Soporte de conmutación de paquetes y de circuitos.
- Calidad de voz similar a una conexión fija.
- Servicio internacional entre distintos operadores.

### 7.2.1 PROYECTO ASOCIACIÓN DE TERCERA GENERACIÓN (3GPP)

Para tratar de apoyar el trabajo desarrollado en torno a IMT-2000, en 1998 se fundó el Proyecto Asociación de Tercera Generación, 3GPP por sus siglas en inglés (3rd Generation Partnership Project) con el objetivo de extender las capacidades de las redes GSM (2G). Los miembros fundadores fueron [37]:

- ARIB (Association of Radio Industries and Businesses): Japón
- ATIS (Alliance for Telecommunications Industry Solutions): Estados Unidos
- CCSA (China Communications Standards Association): China
- ETSI (European Telecommunications Standards Institute): Europa
- TTA (Telecommunications Technology Association): Corea del Sur
- TTC (Telecommunications Technology Committee): Japón

En ese mismo año se creó 3GPP2 para impulsar la siguiente fase de desarrollo de las redes CDMA (2G). Entre sus miembros fundadores se encuentran [38]:

- ARIB (Association of Radio Industries and Businesses): Japón
- CCSA (China Communications Standards Association): China
- TIA (Telecommunications Industry Association): Estados Unidos
- TTA (Telecommunications Technology Association): Korea
- TTC (Telecommunications Technology Committee): Japón

La figura 7.1 ayuda a comprender mejor las diferencias y relaciones que existen entre las generaciones de redes:

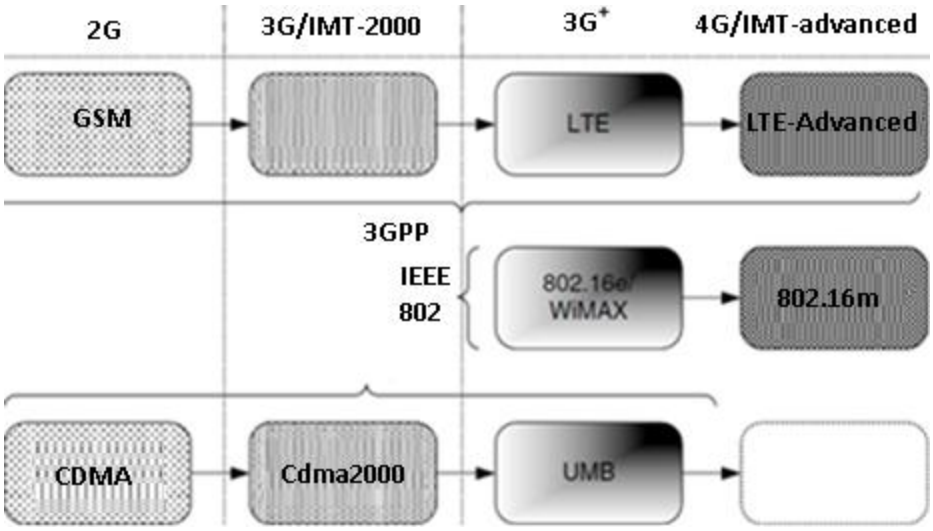



Figura 7.1 Comparativo de generaciones de redes

### 7.2.2 MOVILIDAD IP

Tratándose de movilidad IP es MIPv4 la opción más utilizada actualmente debido a que ha sido estandarizada por la IETF y por varias otras organizaciones, tales como 3GPP2, el foro de WiMAX, etc.

Hoy en día cada vez más es común observar a MIPv4 implementado en redes CDMA, situación que en gran medida se debe a que IPv4 aún sigue siendo la versión IP más empleada a nivel mundial (en comparación con IPv6). En lo que respecta a las redes WiMAX se consideró dentro de su estructura soportar PMIPv4 aunque, también da soporte a clientes con Movilidad IP, CMIP por sus siglas en inglés (Client Mobile IP). En ambos casos (redes WiMAX y 3GPP2) se realizaron adaptaciones y mejoras a sus elementos existentes de red para incorporar las funciones de Agente Local o Agente Proxy de Movilidad con el fin de mantener el nivel de seguridad de las comunicaciones y la transparencia al experimentar un cambio de redes (remítase al RFC 5563).

Otros casos consideran el uso de FMIPv6 en redes 3G (específicamente en CDMA2000) para lidiar con la criticidad de algunos servicios como la voz donde se requiere que exista una mínima pérdida de paquetes, evitando al mismo tiempo que no se presente una degradación considerable en los servicios del usuario. Esta idea fue contemplada en el RFC 5271 aunque, en la actualidad no es muy común observar su empleo en un ambiente empresarial o por parte de algún proveedor de servicios.

En lo que respecta a la relación de IPv6 en las redes 3G fue en el año 2002 que se llevaron a cabo las primeras recomendaciones (RFC 3314), se discutieron varios aspectos de su uso, y se tomaron en cuenta consideraciones que deberían hacerse para su empleo futuro. El tiempo transcurrió y no fue hasta el año 2005 cuando se comenzó a discutir el proceso de transición que se llevaría a cabo en tales redes (RFC 4215), se hablaba ya de los mecanismos de transición viables, los escenarios contemplados, elementos de seguridad, etc. Finalmente debido al incremento masivo de las conexiones inalámbricas de banda ancha un acontecimiento reciente sucedió el presente año 2012, se elaboró un documento (RFC 6459) en el que se describe el soporte de IPv6 en las redes que forman parte de 3GPP, principalmente se contempló el empleo de conexiones pila dual, administración de direcciones IPv4 e IPv6, etc.

Teniendo todos estos sucesos en mente es claro que habrá que esperar unos años más para que la Movilidad IP tenga más presencia en las redes 3G, o al menos en las redes que no pertenecen al proyecto 3GPP. Enseguida se describe la situación actual de MIP en las redes 3G para llegar a entender el papel que juega este protocolo en dichos ambientes, y las dificultades que tendrá que enfrentar para hacerse de un lugar.

### 7.2.3 SITUACIÓN ACTUAL

No es de extrañarse que las redes 3G hayan tenido que sufrir constantes mejoras y modificaciones para incrementar el nivel de los servicios brindados a los usuarios, particularmente ha sido la integración de elementos adicionales que ha traído consigo una mayor complejidad. Precisamente pensando en mantener un ambiente de competitividad, 3GPP desarrolló una visión denominada Evolución de Arquitectura de Sistema, SAE por sus siglas en inglés (System Architecture Evolution) con el objetivo de crear nuevos radios de acceso a la red y reducir al mismo tiempo el número de configuraciones a realizar por parte de los usuarios. Para hacer esto posible se contempló la creación de un Núcleo de Paquetes Evolucionado, EPC por sus siglas en inglés (Evolved Packet Core) a través del cual se pudiera soportar una movilidad continua no solamente por medio de las redes pertenecientes a 3GPP sino también, a través de aquellos radios de acceso que no lo son, tales como WiMAX, CDMA2000, WLAN, etc.

Se visualiza la estructura de SAE en la figura 7.2.

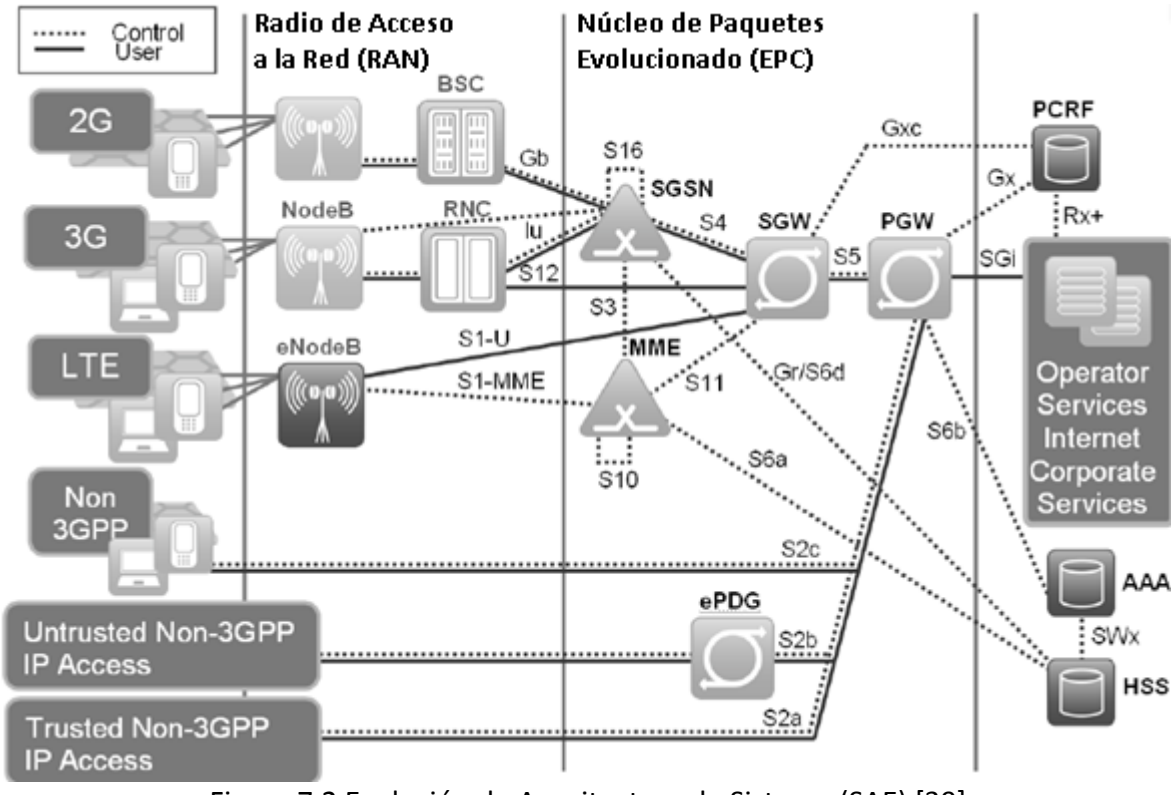



Figura 7.2 Evolución de Arquitectura de Sistema (SAE) [39]

Definitivamente todo comienza a tomar sentido sobre todo cuando se habla de temas como: visión basada en IP, Redes de Próxima Generación, etc. Sin fines de entrar en detalle es importante conocer al menos los elementos más importantes observados en la

figura 7.2, ya que con esto se mejorará el panorama de la movilidad en las redes 3G. En la tabla 7.1 se enuncian los elementos más representativos de SAE:

Tabla 7.1 Elementos de SAE [40]

| Elemento | Descripción |
|---|---|
| Nodo B Evolucionado | eNB por sus siglas en inglés (Evolved Node B): nodo lógico encargado de manejar una o varias células de red, desarrollando funciones como: administrar los recursos de radio (configuración, admisión, modificación y liberación), compresión/descompresión del encabezado IP, cifrado de los datos del usuario, etc. |
| Entidad de Administración de Movilidad | MME por sus siglas en inglés (Mobility Management Entity): entidad principal del plano de control que permite a los usuarios moverse de forma transparente por la red, ocupándose de establecer el soporte para acceder a la red actual, movilidad, rastreo de los usuarios (ingreso y egreso), autenticación, seguridad, etc. |
| Gateway de Red de Paquete de Datos | PGW por sus siglas en inglés (Packet Data Network Gateway): une a varios tipos de redes (ruteo y renvío entre las redes propuestas por 3GPP y el resto de las redes). Se encarga de asignar direcciones IP a los usuarios (IPv4, prefijo IPv6 o ambos), realizar el filtrado de paquetes, determinar políticas de QoS de la red, etc. |
| Función de Políticas y Reglas de Cargo | PCRF por sus siglas en inglés (Policy and Charging Rule Function): negocia las políticas de QoS con una red externa y determina la forma en que los paquetes son considerados (respecto a cargos al usuario). |
| Servidor Local de Suscripción | HSS por sus siglas en inglés (Home Suscriber Server): contiene una base de datos de los usuarios de la red a través de la cual se conocen los servicios a los que cada uno de estos tiene derecho. |
| Gateway de Servicio | SGW por sus siglas en inglés (Serving Gateway): es controlado por uno o más MMEs y le permite al usuario moverse libremente dentro de una red que forma parte de 3GPP (actúa como Mobility Anchor de capa 2). Adicionalmente reenvía paquetes entre el eNB y algún PGW o SGSN. |
| Gateway de Acceso | AGW por sus siglas en inglés (Access Gateway): brinda acceso a redes confiables que no son parte de 3GPP, y gestiona la movilidad en capa 2 mientras los usuarios se mueven dentro de dichas redes. |
| Gateway Mejorado de Paquetes de Datos | ePDG por sus siglas en inglés (Enhanced Packet Data Gateway): garantiza un acceso seguro a los usuarios que pasan del EPC a una red que no pertenece a 3GPP y que además no es confiable. |

Finalmente en la tabla 7.2 se encuentra una breve descripción de las interfaces de SAE.

Tabla 7.2 Interfaces de SAE [40]

| Interfaz | Descripción |
|---|---|
| LTE-Uu | Interfaz aérea que existe entre el usuario y el eNodeB. |

| | |
|---|---|
| X2 | Cuando se presenta un handover entre células vecinas y no se recurre al EPC, la señalización se realiza a través de esta interfaz. |
| S1-MME | Transmite tráfico de señalización (procedimientos de seguridad, administración de contexto) ante el acceso y salida de usuarios. |
| S1-U | Se usa para intercambiar paquetes IP del usuario. |
| S10 | Permite realizar transferencias de contexto de los usuarios. |
| S6a | Por medio de ésta el MME recupera del HSS la información de suscripción de un usuario (QoS, handover, localización, etc.) o en su defecto envía actualizaciones al HSS para brindarle nueva información de algún usuario. |
| S11 | Permite comunicar a un MME con uno o varios SGWs para crear nuevas sesiones, administrándolas (modificar, eliminar y cambiar) y estableciendo los recursos necesarios. |
| S5 | Existe entre un SGW y un PGW cuando ambos pertenecen a la misma red, es decir, al no presentarse roaming. |
| S8 | Es similar a la interfaz S5 con la diferencia de que el SGW está en la red visitada y el PGW en la red local (existe roaming) por lo tanto, adicionalmente en esta interfaz se desarrollan funciones de seguridad entre operadores. |
| S9 | Se encuentra entre un hPCRF y un PCRF (para casos de roaming) y se usa para aplicar en la red visitada políticas de control dinámicas de la red local. |
| S12 | Encapsula los datos directamente entre el SGW y un radio de acceso a la red. |
| S3 | Transfiere la información cuando se realiza un handover entre diferentes tipos de redes. |
| S4 | Le permite al SGW tomar el rol de GGSN. |
| S7 | Admite que el PGW pregunte por el nivel de QoS que se configurará en el SAE, y le permite al PCRF solicitar la configuración del SAE con un QoS adecuado. |
| S16 | A fin de realizar transferencias de contexto de los usuarios comunica a dos SGSNs cuando se trabaja con accesos 2G/3G. |
| S2a | Se encuentra entre un AGW (en una red confiable que no forma parte de 3GPP) y un PGW (contemplando casos de roaming y no roaming) para permitir movilidad dentro de un acceso confiable que no pertenece a 3GPP. |
| S2b | Existe entre un ePDG y un PGW, y contempla casos de roaming y no roaming |
| S2c | Permite dar soporte de control y movilidad entre el equipo del usuario y un PGW, para roaming y no roaming, en redes confiables o no confiables (sea que pertenezcan o no a 3GPP). |
| SGi | A través de ésta el PGW envía/recibe información hacia/desde una red externa (de algún otro operador de red) por medio de direcciones IPv4 o IPv6. |
| Gx | Comunica a un PGW con un PCRF para definir políticas de QoS, filtrado, control de cargos, etc. |
| Gxc | Tiene una función similar a la interfaz Gx pero, se localiza entre un SGW y un PCRF cuando se emplea PMIPv6 en las interfaces S5 o S8. |
| Rx+ | Facilita el intercambio de políticas e información de cargo entre el PCRF y otros operadores de red. |

Actualmente en las redes definidas por 3GPP es muy común encontrar que la movilidad es realizada a través del Protocolo de Encapsulación GPRS, GTP por sus siglas en inglés (GPRS Tunneling Protocol). Este protocolo es el encargado de manejar la movilidad en la capa de enlace en las redes de 3GPP y debido a la flexibilidad y características que posee se ha convertido en un éxito en ambientes móviles de gran escala en este tipo de redes. Entre las tareas que lleva a cabo se encuentran:

- Administración de movilidad: comprende mensajes para identificar a los usuarios, manejar la transferencia de los datos ante handovers, conocer el estado de los elementos de la red, etc.
- Administración de encapsulación: involucra la creación y eliminación de las sesiones de los usuarios, permitiendo a estos últimos mantener los requerimientos de los servicios que estén usando e inclusive planteando el uso de ambientes multi-homing.
- Funciones específicas de servicio: integra mejoras y optimizaciones para el manejo de handovers y el manejo de negociaciones de QoS.
- Transferencia: realiza la transmisión de los datos de cada usuario junto con la información de contexto asignada a cada sesión.
- Mantenimiento del sistema: a fin de mejorar la robustez del sistema administra las rutas, maneja errores y contempla casos de recuperación y restauración de algún elemento de la red.

Concretamente GTP es un protocolo propietario de encapsulación utilizado en las redes GPRS y UMTS como mecanismo para proveer soporte de movilidad basada en red, es decir, GTP al contrario de MIP no necesita estar soportado en cada estación móvil sino que, son los propios elementos de la red los que se encargan de manejar la movilidad, capacidad que sin duda resulta una oferta atractiva a los operadores de redes celulares. Para su funcionamiento GTP posee 2 componentes principales: el plano de control (GTPv2-C) le permite administrar los túneles que la red establece con cada usuario, definiendo las rutas que seguirán los datos; el plano de usuario (GTPv1-U) representa un mecanismo de encapsulación para transportar el tráfico de los usuarios. Actualmente dependiendo de las funciones que se desarrollen dentro del SAE se utilizan varias interfaces, mismas que a su vez transportan la señalización de protocolos como GTP, PMIPv6, MIPv4, DSMIPv6, GRE, IKEv2, IPSec, etc., en la figura 7.3 se presenta un ejemplo de esto.

Claramente GTP es el protocolo dominante para manejar la movilidad en las redes del proyecto 3GPP sin embargo, ante la llegada de EPC para brindar soporte de movilidad en las redes que no forman parte de dicho proyecto fue necesario explorar otras opciones, alternativas que permitieran a los usuarios pasar de una red definida por 3GPP a una red que no lo es (todo de forma transparente y sin que se vieran interrumpidas sus comunicaciones y servicios). Los principales candidatos propuestos en 2009 corresponden a las mejoras de MIP observadas en la tabla 7.3.

Tabla 7.3 Mejoras de MIP integradas a redes del proyecto 3GPP

| Descripción | Movilidad basada en host (DSMIPv6, MIPv4) | Movilidad basada en red (PMIPv6) |
|---|---|---|
| Dependencia de las capacidades de la red de acceso | Alto | Bajo |
| Sobrecarga en la interfaz del usuario por la movilidad | Existe | No existe |
| Consumo de batería | Alto | Bajo |
| Impacto en las terminales | Soporte de IKEv2, DSMIPv6 o MIPv4 | No existe |
| Impacto en la red de acceso | Sobrecarga por el establecimiento de túneles bidireccionales | Las funciones de LMA y MAG están soportadas en las entidades de red. |

Antes de entrar en detalle de los elementos mostrados en la tabla 7.3, será importante comentar que los accesos por las redes que no forman parte de 3GPP se clasifican en confiables y no confiables. En el primer caso las medidas de seguridad de la red externa son equivalentes a las existentes en una red de 3GPP, por lo que únicamente se necesita una coordinación para conceder el acceso al usuario; para el segundo caso a fin de garantizar que el usuario acceda de forma segura al SAE es necesario incluir a un nodo que autentique y provea un acceso confiable.

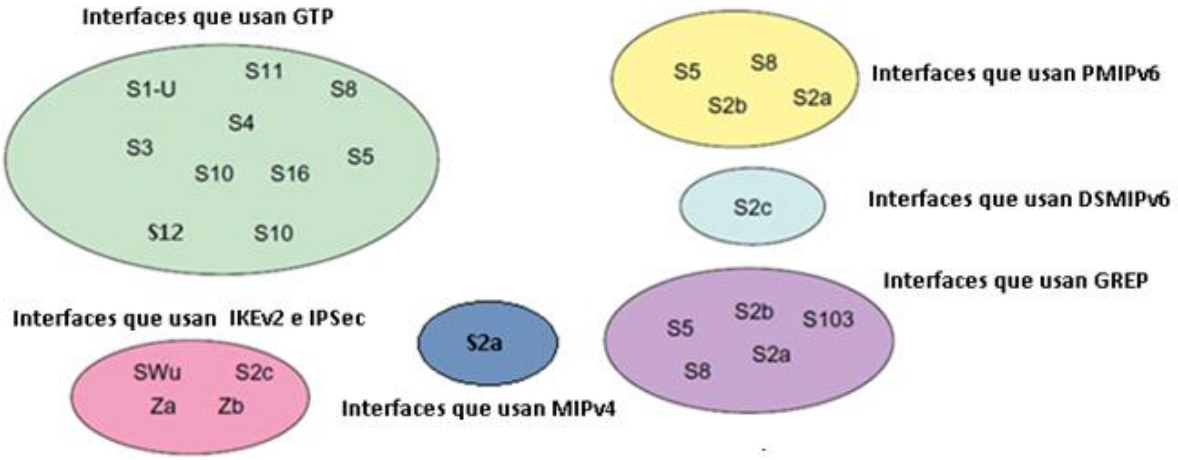



Figura 7.3 Interfaces principales de SAE

Dentro del SAE en algunas interfaces puede existir cualquiera de las mejoras de MIP antes mencionadas, e inclusive varias de ellas llegan a estar presentes. Con el propósito de comprender mejor las opciones antes descritas se presenta una descripción de cada caso:

a) *MIPv4 (modo FA):* esta opción suele emplearse en redes confiables que no pertenecen a 3GPP, tales como WiMAX y redes definidas por 3GPP2, específicamente de los modos de empleo de MIPv4 se recurre únicamente a la asignación de direcciones CoA (modo FA) porque permite a los operadores de red no agotar su espacio de direcciones IPv4. En el SAE generalmente el HA se encuentra en el PGW y el rol de FA es asumido por el punto de acceso a la red confiable que no es de 3GPP (véase figura 7.4).

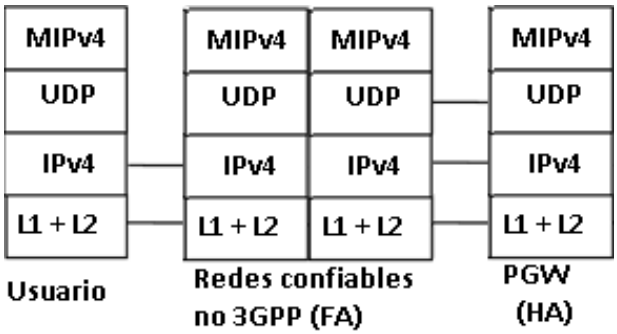



Figura 7.4 Elementos de MIPv4 en SAE

Tomando en cuenta lo anterior se enuncian a continuación las acciones que se presentan entorno al usuario y su FA (figura 7.5):

1. Descubrimiento de FA: el usuario manda un mensaje Solicitud de Agente para conocer el FA de la red donde se encuentra.

2. Registro inicial: el usuario usa un identificador (NAI) para enviar un mensaje de Solicitud de Registro a su HA (a través del FA recién descubierto).

3. Renovación: mientras el usuario permanezca en esa red antes de que expire el tiempo de su registro deberá renovar la asociación con su HA.

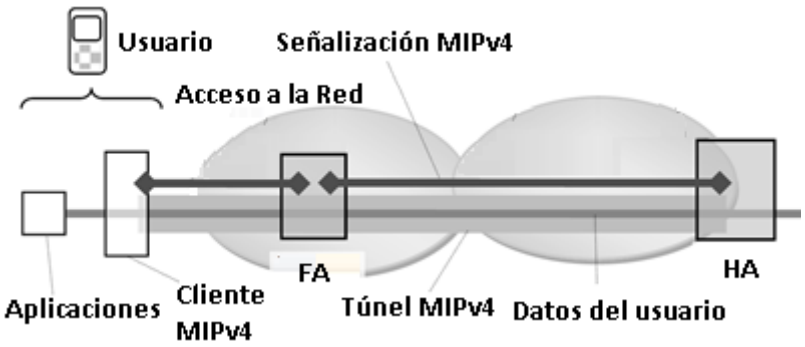



Figura 7.5 Interacción usuario-FA en MIPv4

b) *DSMIPv6:* particularmente el HA puede ser estar contenido en el PGW o en un nodo diferente de la red (ya sea que esté detrás del GGSN o del ePDG). Se observa un ejemplo en la figura 7.6.

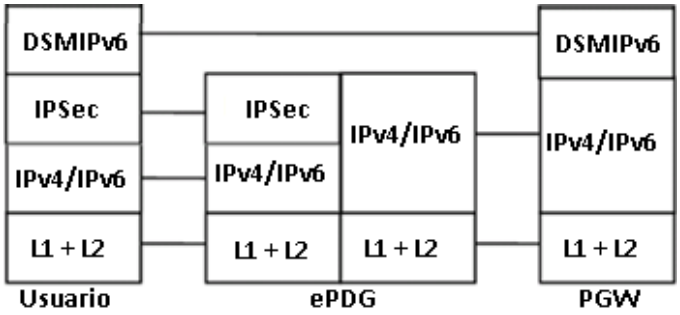



Figura 7.6 Elementos de DSMIPv6 en SAE

Para que se proporcione un soporte de DSMIPv6 existe todo un proceso involucrado, de modo que para su correcto funcionamiento se necesitan desarrollar las siguientes actividades:

1) Descubrimiento de HA: cada usuario que recién haya ingresado a la red debe conocer a su HA, para ello existen 3 opciones: tener una configuración estática con los parámetros del operador, realizar una consulta DNS preguntando por el identificador del HA, preguntar por la dirección del HA a un servidor DHCPv6.

2) Establecimiento de SAs: en aquellos casos donde el usuario se encuentre en una red no confiable que no sea parte de 3GPP se utilizará IKEv2 para establecer un túnel IPSec, o en su defecto se puede usar la extensión EAP. Ambas opciones son suficientes para proteger el tráfico de señalización de DSMIPv6, se ilustra un ejemplo en la figura 7.7.

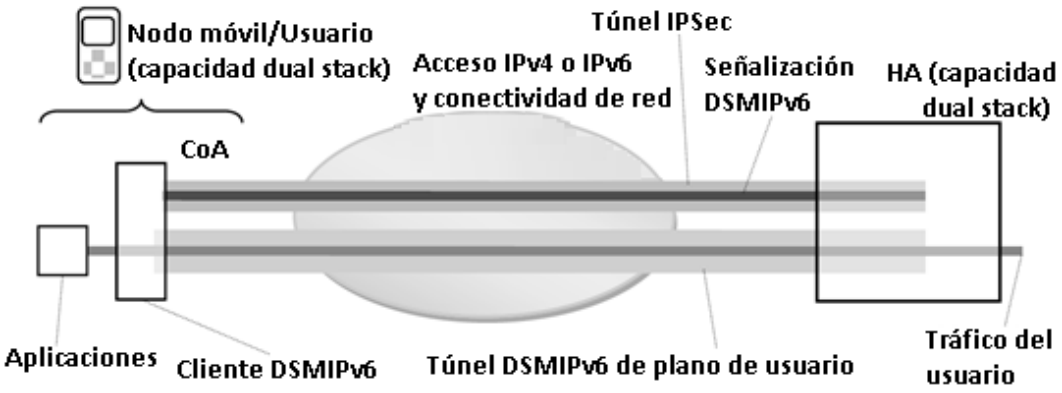



Figura 7.7 Interacción usuario-HA en DSMIPv6

3) Asignación de prefijo IPv6 local: ya que el usuario necesita un prefijo de red IPv6 el HA deberá asignárselo aunque, opcionalmente el dispositivo del usuario

puede emplear una configuración estática adquirida con anterioridad (caso que no es práctico ni muy común).

4) Detección del enlace de la red local: el usuario realiza esta acción para determinar si se encuentra o no en su red local.

5) Asociación inicial de registro: se realiza el intercambio de mensajes BU y BA entre el usuario y su HA para realizar el registro correspondiente. En este paso el usuario opcionalmente puede recibir alguna dirección IPv4 por parte de su respectivo HA.

c) *PMIPv6:* es el candidato más prometedor para cumplir con las funciones de GTP entre el PGW y alguna red confiable que no pertenezca a 3GPP, lo que pretende es que los cambios sean menores y que se tenga poco impacto en la infraestructura de las redes actuales. La figura 7.8 proporciona una idea general de su uso.

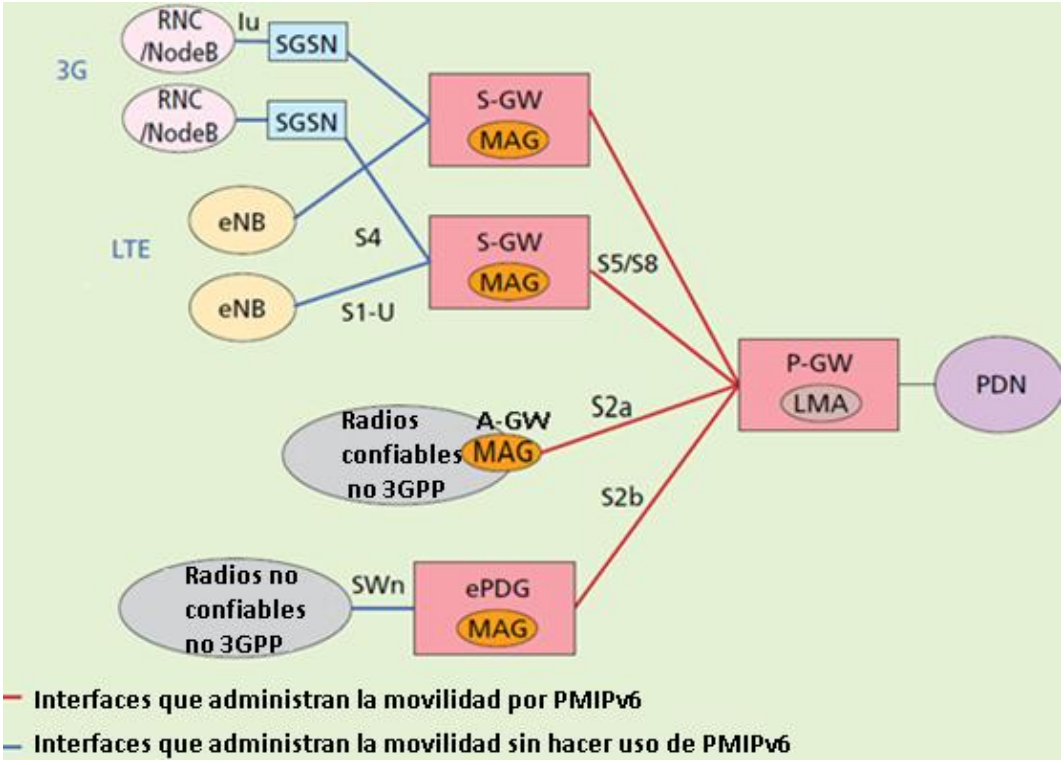



Figura 7.8 Interfaces involucradas para PMIPv6 en SAE

En cada una de las interfaces donde se maneja PMIPv6 habrá que realizar diversas consideraciones porque los dominios de enrutamiento en los que puede ubicarse el usuario llegan a ser distintos. Para lidiar con estas situaciones PMIPv6 se auxilia de túneles (a través de GRE) que le faciliten manejar indistintamente direcciones IPv4 o IPv6.

En la figura 7.8 se aprecian claramente los 2 usos principales de PMIPv6: proveer una asistencia a GTP (S5/S8), y actuar como un protocolo de movilidad en redes que no pertenecen a 3GPP (S2a, S2b). En este último caso es posible diferenciar 2 casos distintos, redes confiables o no confiables, en las primeras se ubican simplemente a los elementos MAG y LMA (figura 7.9).

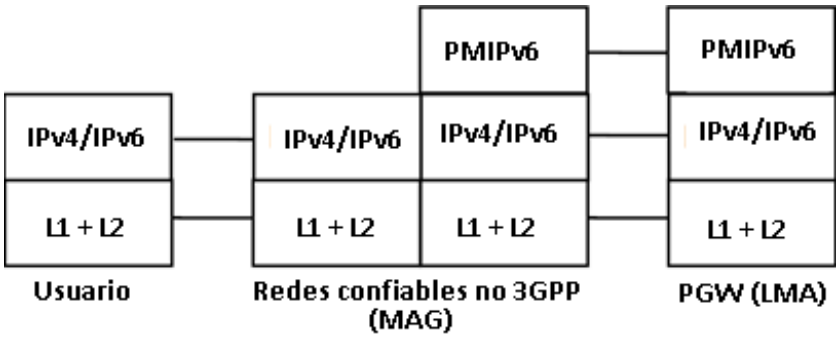



Figura 7.9 Estructura de PMIPv6 en interfaz S2a de SAE

Por su parte el involucrar a redes no confiables adicionalmente requiere de la presencia del ePDG para proporcionar un acceso seguro y confiable a los usuarios (figura 7.10).


Figura 7.10 Estructura de PMIPv6 en interfaz S2b de SAE

Para los casos antes descritos existen 2 tipos de handover que suelen presentarse en PMIPv6: no optimizados y optimizados. En el primer tipo, no se usan recursos de la red origen para preparar a la red destino porque el dispositivo del usuario durante el handover puede tener activo más de un radio al mismo tiempo no obstante, habrá que considerar que el uso de radios duales afecta el consumo de la batería del dispositivo e inclusive algunas veces puede llegar a presentarse cierta interferencia; en el segundo tipo la red origen se encarga de preparar los recursos que el usuario usará en la red destino (a través de un túnel), este tipo es muy recurrente cuando el usuario no puede transmitir y recibir simultáneamente en las redes origen y destino, es decir, el dispositivo del usuario únicamente puede tener activo un radio durante el handover.

Gracias al diseño y funcionamiento de PMIPv6 se puede eliminar el soporte de movilidad en los dispositivos de los usuarios, situación que sin duda trae varias ventajas tanto para

los usuarios finales como para los operadores de red, por ejemplo: existen menores demandas de procesamiento en los móviles, se presenta una disminución en el uso de las interfaces de radio, se optimizan los recursos de la red (menos señalizaciones), existen mejoras en el rendimiento de las comunicaciones durante el handover, se brinda mayor privacidad a los usuarios, etc.

Claramente PMIPv6 está logrando obtener un papel más activo en las redes 3G, y para hacer esto posible sus capacidades deben ser lo más cercanas a GTP porque con ello, se logrará postular como una opción que asista a dicho protocolo en brindar movilidad en las redes que forman parte de 3GPP. En la tabla 7.4 se muestran los principales mensajes de señalización de PMIPv6 que le permiten desarrollar su funcionamiento.

Tabla 7.4 Mensajes de señalización en PMIPv6

| Mensaje de señalización | Dirección | Descripción |
|---|---|---|
| Proxy Binding Update (PBU) | MAG -> LMA | Comprende actividades de registro (creación, extensión y eliminación). |
| Proxy Binding Acknowledgment (PBA) | LMA -> MAG | Informa el estado de las solicitudes que recibe. |
| Binding Revocation Indication (PBR) | LMA -> MAG | Notificación que revoca una asociación o incluso varias. |
| Binding Revocation Acknowledgment (BRA) | MAG -> LMA | Confirma el estado de una revocación. |

Resulta evidente que los mensajes de la tabla 7.4 aún no son suficientes para que PMIPv6 pueda ofrecer todo el soporte que posee GTP no obstante, a lo largo de los años la IETF han definido nuevas mejoras que le permitan a PMIPv6 alcanzar su máximo potencial, algunas de estas características se describen en RFCs y otras aún se encuentran como propuestas (tabla 7.5).

Tabla 7.5 RFCs y Drafts recientes de PMIPv6

| RFC/Draft | Descripción |
|---|---|
| 5779 (2010) [41] | Define la interacción de PMIPv6 y un servidor AAA (Diameter) con el fin de desarrollar un mecanismo de autenticación y acceso a la red. |
| 5844 (2010) [33] | Añade extensiones a PMIPv6 para darle soporte de IPv4, es decir, el usuario puede adquirir una dirección IPv4 o encontrarse en una red que únicamente use dicho protocolo y seguir disfrutando de movilidad. |
| 6058 (2011) [42] | Permite a PMIPv6 manejar mensajes de señalización periódicos para detectar fallas y optimizar el rendimiento ante handovers (se disminuyen retrasos y pérdidas). |
| 6475 (2012) [43] | Se define una base de datos (MIB) a través de la cual se monitorean y controlan las funciones del LMA y el MAG. |
| 6572 (2012) | Plantea usar RADIUS como el servidor AAA dentro del dominio PMIPv6. |

| | |
|---|---|
| 6705 (2012) [45] | Añade una mejora para optimizar la entrega de paquetes dentro de un domino PMIPv6. |
| 6757 (2012) [46] | Adiciona un identificador que le permite al MAG informar al LMA cierta información sobre la red en donde actualmente se ubica el MN. |
| wlan-03-applicability-03 [47] | Propone el empleo de PMIPv6 en redes WLAN. Se trata de no agregar complejidad y tener una administración centralizada. |
| pmipv6-flowmob-04 | Da soporte para que los usuarios puedan conectarse al mismo dominio PMIPv6 a través de diferentes interfaces. [49] |
| pmip6-qos-01 [48] | Propone brindar soporte de QoS a los usuarios mientras se desplazan dentro de un dominio PMIPv6. |
| pmip6-authiwk-05 [49] | Presenta el uso de identificadores y mecanismos de autenticación (802.1x) para proveer a los usuarios un acceso seguro a las redes WLAN. |
| pmip-nemo-01 [50] | Sugiere adicionar NEMO a PMIPv6 para que los dominios PMIPv6 sean capaces de dar servicio a MRs. |

No cabe duda que las propuestas siguen llegando e ideas revolucionarias comienzan a emerger por todos los continentes y todo ello, contribuirá a que PMIPv6 se convierta en un protocolo robusto y maduro; a pesar de esto hoy en día aún no es muy clara la participación que tendrá en las redes 4G, las cuales están cada vez más y más cerca.

## 7.3 REDES 4G

Los servicios que ahora demandan los usuarios rompen con los paradigmas de lo convencional al punto de alcanzar niveles insospechados, y fue el día en que se percibió esa nueva realidad que surgió la necesidad de buscar una forma de ir más allá de las capacidades que ofrecen las redes 3G; precisamente en dichas capacidades anheladas es donde las redes 4G comienzan a jugar un papel importante: hacer frente a la demanda del mercado móvil y al surgimiento de una nueva clase de usuarios.

Nuevamente el concepto ABC comienza a retomar fuerza con las redes 4G porque ya es más viable alcanzar tan bastas exigencias, ejemplo de ello son las mejoras que poseen este tipo de redes que son:

- ✓ Proveer servicios de banda ancha.
- ✓ Optimización en el uso de los recursos.
- ✓ Interoperabilidad entre distintos tipos de redes.
- ✓ Uso de múltiples antenas (MIMO).
- ✓ Redes basadas en conmutación de paquetes.

A pesar de las innovaciones que se adicionan a 4G aún existen ciertos retos que limitan su progreso pero, son las ideas y aportaciones provenientes de investigaciones lo que da pauta a solucionar esos desafíos. Para entender mejor a las redes 4G se verán en las siguientes secciones los organismos que las impulsan, las tecnologías propuestas y la forma en que se espera alcanzar una movilidad completa (conocida comúnmente bajo el término "seamless mobility").

### 7.3.1 TELECOMUNICACIONES MÓVILES INTERNACIONALES AVANZADAS (IMT-ADVANCED)

Falta poco para que las redes 3G sean insuficientes para la mayoría de la población mundial, afortunadamente este evento ya desde hace varios años fue previsto por la ITU y por ello decidió definir las especificaciones de las Telecomunicaciones Móviles Internacionales Avanzadas, IMT-Advanced por sus siglas en inglés (International Mobile Telecommunications-Advanced) [51]. Se realizaron estudios de nuevos diseños de tecnologías, estimaciones del uso de frecuencias, principios de estandarización y un análisis del mercado móvil. En la figura 7.2 se aprecia la evolución de una red 3G a una red 4G. En el año 2008 los miembros de la ITU y algunas otras organizaciones decidieron comenzar a dar forma a la estructura del IMT-Advanced, un año más tarde de todas las tecnologías propuestas únicamente quedaron algunos candidatos. Finalmente para el año 2010 solamente 2 tecnologías pudieron ser incluidas dentro del primer borrador del IMT-Advanced: LTE-Advanced por parte de 3GPP (versión 10) y WirelessMAN-Advanced a través de la IEEE 802.16 (grupo m). Ambas tecnologías se aprecian en la figura 7.11.

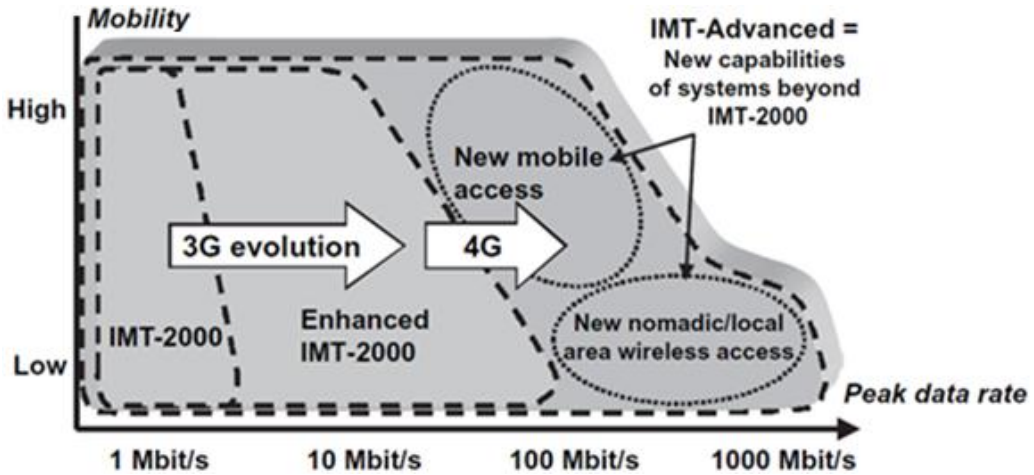


Figura 7.11 Evolución de las redes 3G y 4G

En los primeros meses del presente año (2012) la ITU dio a conocer su decisión de permitir el libre uso del término "4G", razón por la cual muchos proveedores de telefonía celular y demás organizaciones suelen utilizarlo indistintamente no obstante, para que una red

llegue a considerarse como "4G" necesita cumplir con una serie de requerimientos, mismos que se especifican en el IMT-Advanced y son las siguientes:

- Capacidad de roaming a nivel mundial.
- Compatibilidad de servicios con las redes fijas.
- Servicios de movilidad de alta calidad.
- Capacidad de interconexión con otros radios de acceso.
- Uso de equipos en todo el mundo de manera indistinta.
- Facilidad de empleo de equipos, servicios y aplicaciones.
- Alta uniformidad de funcionalidad a nivel mundial, siendo flexible para soportar un gran número de servicios y aplicaciones.
- Mayor velocidad de transferencia (100Mbps-alta movilidad, 1Gbps-baja movilidad).

Hoy en día no existen operadores que hagan uso de LTE-Advanced sin embargo, es relativamente sencillo pasar a dicha fase desde una red LTE, ya sea desde entornos de investigación hasta ambientes de producción, el desarrollo de LTE comienza a extenderse cada vez más a nivel mundial, de acuerdo a la Asociación Global de Proveedores Móviles, GSA por sus siglas en inglés (Global Mobile Suppliers Association) el estado de LTE es bastante prometedor (figura 7.12).

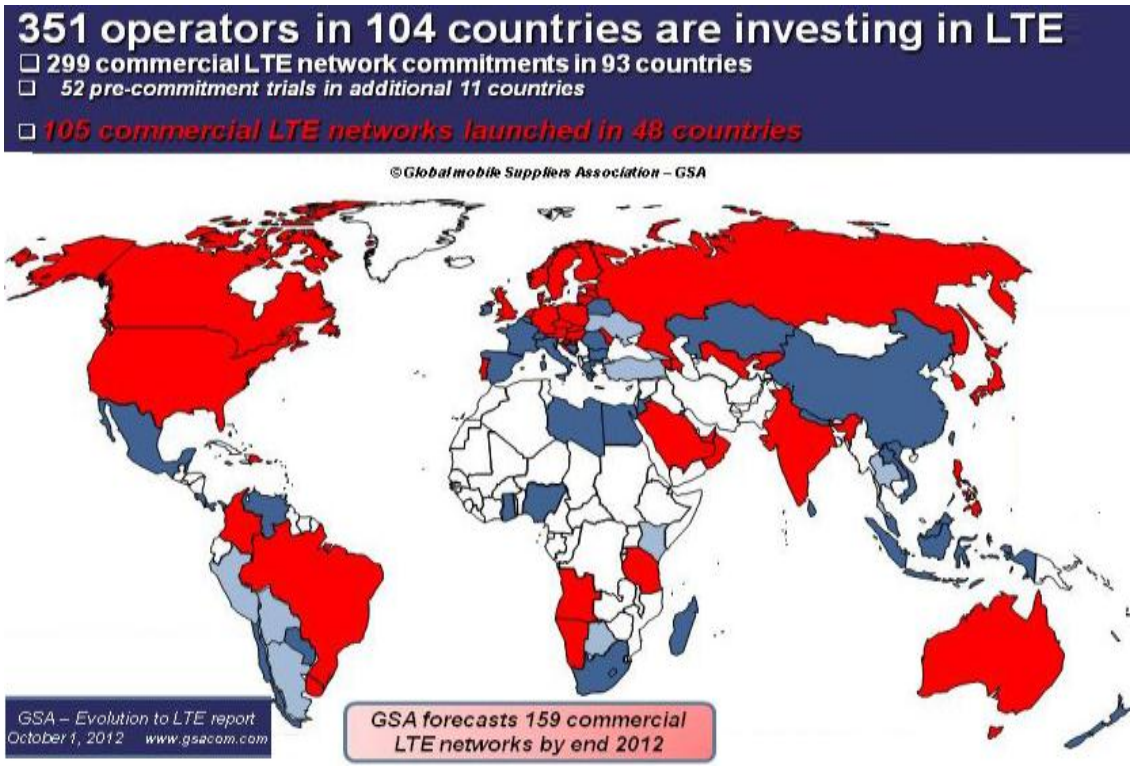



Figura 7.12 Estado de las redes LTE a nivel mundial [52]

Una situación similar ocurre con las redes WirelessMAN-Advanced ya que actualmente únicamente existen redes WiMAX. De acuerdo a datos del Foro WiMAX el desarrollo presente de este tipo de redes sigue aumentado alrededor de todo el mundo (figura 7.13).


| REGION | DEPLOYMENTS | COUNTRIES |
|---|---|---|
| CALA | 120 | 33 |
| Africa | 117 | 43 |
| Asia-Pacific | 98 | 23 |
| Eastern Europe | 86 | 21 |
| Western Europe | 77 | 18 |
| North America (USA/Canada) | 56 | 2 |
| Middle East | 29 | 10 |
| Total Deployments Tracked | 583 | 150 |
| Total Countries with WiMAX Deployments | | |

Figura 7.13 Estado de las redes WiMAX [53]

Para este año se espera mucho de LTE-Advanced y 802.16m porque las investigaciones que se realizan en torno a ambos desarrollos traerán mejoras significativas en el rendimiento y eficiencia de los servicios, tratando siempre de ganar puntos y simpatía con los proveedores restantes que aún no toman partido.

### 7.3.2 MOVILIDAD IP

Es indudable que existe una relación entre las diferentes tasas de transferencia y el nivel de movilidad (figura 7.11) no obstante, en dicha correspondencia hay un elemento adicional, el tiempo de interrupción debido a la presencia de un handover. Naturalmente la duración debe ser la mínima posible y dependiendo de las características en que se desarrolle, se han planteado las siguientes situaciones:

- El dispositivo del usuario conserva la misma frecuencia y banda: el tiempo no debe exceder de los 27.5ms

- La banda se mantiene pero, no la frecuencia: adicionalmente se designan 12.5ms para la asignación de la nueva frecuencia.
- No se mantiene ni la frecuencia ni la banda: el tiempo total asignado es de 60ms.

Particularmente debido a que las redes 4G se conforman por redes heterogéneas, se han desarrollado a lo largo de estos años estudios sobre el impacto y los efectos que produce trabajar bajo estos ambientes, lo que conlleva principalmente a evaluar efectos como:

- *Cambios en las condiciones de red:* cada red suele encontrarse bajo una serie de condiciones diferentes, lo que ocasiona que al pasar de una red a otra se lleguen a presentar ciertas variaciones, por ejemplo pérdida de paquetes, tiempos retraso, congestión de enlaces, etc.
- *Calidad de experiencia:* mientras el usuario se desplaza en redes heterogéneas, desde su perspectiva personal, debe experimentar la misma calidad en el uso de los servicios a los que recurre.

Para lograr una completa movilidad en las redes 4G los dispositivos de los usuarios necesitan ser capaces de pasar entre diferentes tecnologías de acceso de manera transparente. Pensando en ello se han planteado propuestas que involucran el uso de antenas inteligentes que den oportunidad a que los dispositivos se auto-configuren en el modo apropiado según lo vayan necesitando no obstante, para lograrlo se requerirán de los siguientes elementos:

- *Administración de ubicación:* este proceso comprende 2 etapas, la primera permite a la red descubrir la posición actual de cada usuario (por medio de actualizaciones periódicas de su ubicación) y llevar a cabo el procedimiento correspondiente de registro y autenticación en la nueva red; en la segunda se realiza una consulta a la red para conocer la ubicación actual del usuario. Algunos elementos que hay que considerar para lograr una correcta administración son [54]:
  - Paging: es una especie de mecanismo de broadcast a través del cual la red distribuye información a todos los nodos que estén dentro de su alcance.
  - Direccionamiento: involucra la asignación de direcciones a los dispositivos de los usuarios, lo que podría verse dificultado por la presencia de varios operadores de red.
  - Estructura de Bases de Datos: comprende el almacenamiento y distribución de la información de los usuarios, no importa que se utilice un manejo

centralizado, distribuido o hibrido, habrá que encontrar la opción que ofrezca un mejor rendimiento.

- Tiempo de actualización de ubicación: para definir los tiempos correspondientes hay que tomar en cuenta si se trata con una configuración dinámica o estática, es decir, se tienen que conjugar los perfiles definidos por la red y aquellos elegidos por los usuarios.

- *Administración de handover:* su objetivo es mantener las comunicaciones de los usuarios con el mismo nivel de calidad mientras se desplazan entre varias redes. Esta administración resulta bastante compleja pero, al mismo tiempo es muy importante porque en las redes 4G la existencia de handovers llega a ser muy común, tanto horizontales como verticales, específicamente la dificultad comienza a presentarse porque para estos últimos por ejemplo se puede pasar de una red pequeña con gran ancho de banda a una red más grande con un ancho de banda menor, o viceversa.

Con todo lo que se ha descrito hasta el momento es evidente que a pesar de que IPv6 se ve como el candidato ideal a utilizarse en las redes 4G, aún no es definitivo saber si MIP o alguna de sus mejoras pudieran desarrollarse dentro de este tipo de redes, sobre todo porque hasta el momento no responden completamente a los requerimientos de aplicaciones críticas basadas en tiempo real; aún así es probable que se recurran a técnicas que impliquen handovers rápidos, eficiencia en el enrutamiento, uso de buffers, mejoras en la detección y predicción de movimiento, etc.

Actualmente, estrictamente hablando aún no existen redes “4G” en el ámbito comercial porque los operadores todavía están realizando cambios en sus infraestructuras a pesar de ello, este proceso llevará cierto tiempo y ocurrirá de manera gradual, comenzado por supuesto con las grandes ciudades del mundo.

Dada la naturaleza propia de una red 4G (ambientes heterogéneos) se han realizado algunos estudios en FMIPv6 y HMIPv6. En el primer caso se han obtenido resultados aceptables en handovers horizontales y es posible reducir la latencia total; mientras que en el segundo caso se reduce el grado de señalización requerido debido a que se administra la movilidad localmente. Han surgido varias investigaciones y propuestas para la formación de una solución que combine ambas extensiones no obstante, esto podría aumentar la complejidad de la implementación, por lo que aún no existe algo concreto.

Hace algunos años se realizó una propuesta interesante que comprendía el uso de una técnica “*bi*-casting”, ésta demandaba que varias estaciones base mantuvieran la información del usuario hasta que finalizara el handover, reduciendo por lo tanto la

latencia implicada pero, forzando a un mayor uso de recursos. Dicha técnica también conocida como HMIP-Bv6 se asocia al siguiente proceso (figura 7.14):

- La capa de enlace del MN se percata de la presencia de un próximo handover y envía una notificación a la capa de red, enseguida dicha capa prepara al MN para mandar un mensaje BU y adiciona una extensión a través de la cual solicita a su MAP que almacene temporalmente los paquetes destinados al MN.

- El MAP recibe el mensaje y manda su respuesta (BA) indicando que ya ha comenzado a almacenar los paquetes dirigidos al MN.

- La capa de red del MN procesa el mensaje BA y le informa a la capa de enlace que lleve a cabo el proceso de handover, enseguida la capa de enlace establece una conexión con la nueva red y le notifica de tal evento a la capa de red. A continuación la capa de red configura la nueva dirección CoA y con ello el MN se encuentra listo para enviar un mensaje BU a su MAP, en dicho mensaje se anexa la solicitud al MAP para comunicarle que envíe a la dirección actual (CoA) del MN todos los paquetes que estén destinados a dicho dispositivo.

- Cuando el MAP inspecciona el nuevo mensaje BU deja de almacenar los paquetes dirigidos al MN y le envía todos los paquetes que tenga almacenados.

- En aquellos casos donde el MN se mueva a otro MAP, simplemente deberá mandar un mensaje BU a su antiguo MAP (después de asociarse correctamente con su nuevo MAP) solicitándole que le envíe a su MAP actual todos los paquetes que haya almacenado hasta el momento.

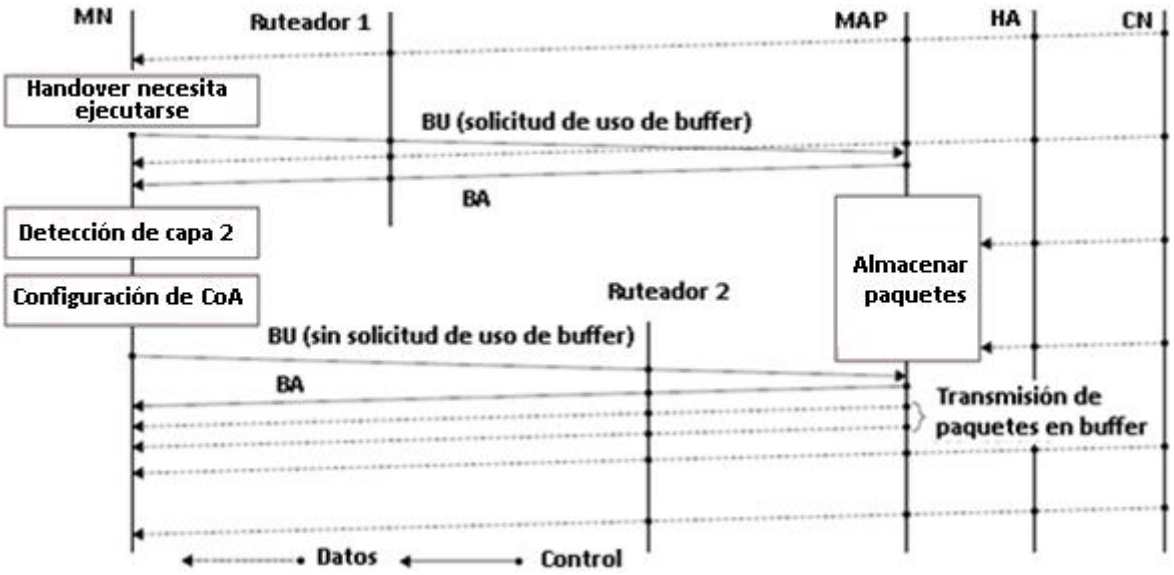



Figura 7.14 Proceso en la señalización de HMIP-Bv6

### 7.3.3 SITUACIÓN ACTUAL

A lo largo de la historia, la demanda del tráfico móvil ha ido en aumento a tal grado que hoy en día es necesario ofrecer velocidades de transferencia altas y confiables, para hacer esto posible ha sido preciso mejorar los siguientes elementos: transferencias pico, eficiencia promedio, espectro y capacidad. En la figura 7.15 se ilustra la evolución de demanda en bps y la capacidad [55].

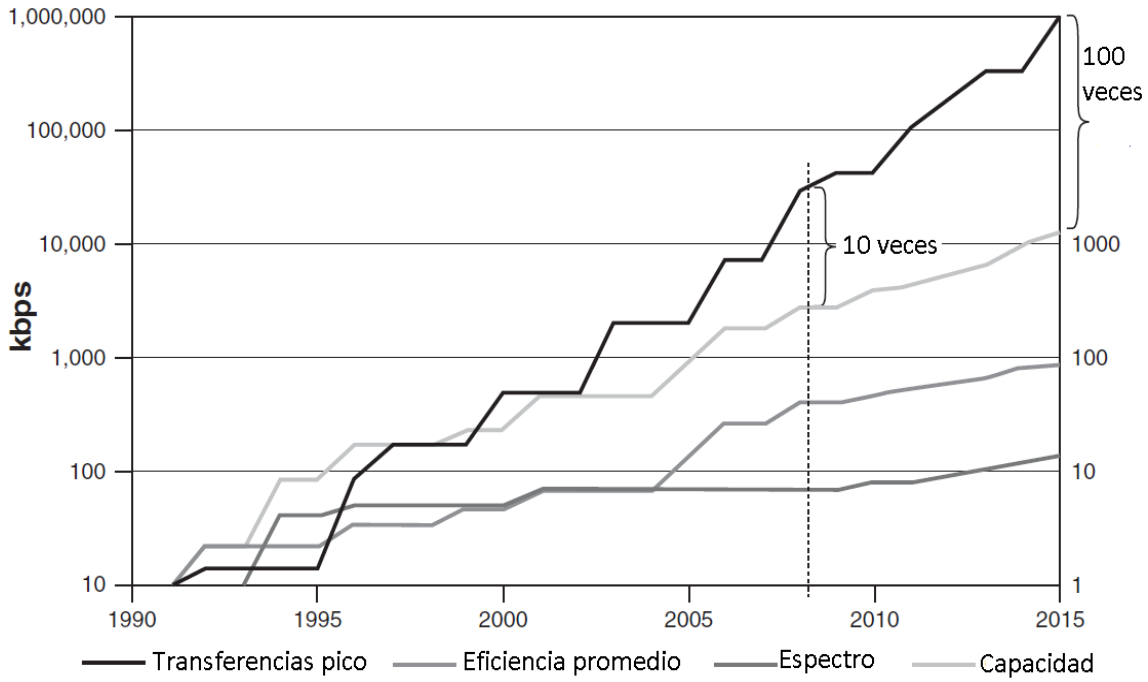



Figura 7.15 Evolución de la demanda de tráfico móvil

Las redes 4G sin duda representan el límite de la competitividad, y esto no es de extrañarse si se toma en cuenta que algunas de sus características más representativas son: QoS, seguridad, movilidad, conmutación de paquetes, velocidades de transmisión de banda ancha, administración de los recursos de red, y además se considera el uso de una red basada en IP, AIPN por sus siglas en inglés (All IP Network); si además se recuerda el agotamiento próximo e inminente de las direcciones IPv4 por lo tanto, no sería extraño que la presencia de AIPN llegue a estar fundamentada en IPv6, no solamente por la gran cantidad de direcciones que posee sino también por sus ventajas y características competitivas (no existe necesidad de NAT, ofrece auto-configuración de dispositivos, QoS, etc.).

No hay que perder de vista que para llegar a una red 4G fue necesario atravesar varias generaciones, cada una de las cuales resultó ser muy superior a su predecesora porque las exigencias de la sociedad de su época así lo demandaban. En la tabla 7.6 se presentan algunas de las características propias de cada generación.

Tabla 7.6 Generaciones de redes celulares

| | 1G | 2G | 2.5G | 3G | 4G |
|---|---|---|---|---|---|
| Tipo de conmutación | - | De circuitos | De paquetes | De circuitos y de paquetes | De paquetes |
| Velocidad de transmisión | - | 9.5 – 14.4 kbps | 64 – 144 kbps | 384 kbps – 2 Mbps | 100 Mbps – 1 Gbps |
| Norma | AMPS, TACS, etc. | TDMA, CDMA, GSM | GPRS, EDGE, 1xRTT | WCDMA, CDMA-2000 | LTE-Advanced, 802.16m |
| Servicios | Telefonía móvil | Voz digitalizada | SMS, datos en paquetes | Información, multimedia | Gran cantidad de servicios y aplicaciones |
| Núcleo de la red | PSTN | PSTN | PSTN y red de paquetes | Red de paquetes | Internet |
| Handoff | Horizontal | Horizontal | Horizontal | Horizontal | Horizontal y vertical |

En la actualidad dentro de las tecnologías consideradas por el IMT-Advanced como redes 4G, MIP por el momento no figura, además las 2 tecnologías candidatas definen únicamente la capa física y la capa de enlace por lo tanto, no serán ellas las encargadas de tratar la capa de red. Tras realizar esta aclaración sólo resta conocer la manera en que estas tecnologías manejan la movilidad y el handover [55]:

- *WirelessMAN-Advanced:* en WiMAX es muy común la existencia de handovers no anticipados y pensando en ir más allá para 802.16m, se planteó la posibilidad de contemplar handovers anticipados porque en estas redes será muy común experimentar handovers verticales (incluye el paso a una red LTE, 802.11, CDMA-2000, etc.) y horizontales, esta última opción se integra de 2 fases:

  - Adquisición de topología de red: cada estación base mediante mensajes de broadcast anuncia periódicamente las estaciones base vecinas que existen, con esta información el dispositivo del usuario mide la intensidad de dichas señales para facilitar en un futuro la elección de posibles destinos, al terminar la medición el dispositivo móvil adquiere la información arrojada y comprueba el destino más adecuado.

  - Ejecución de handover: si la intensidad de la señal de una estación base vecina excede el límite definido en la decisión de handover el dispositivo del usuario envía una solicitud de handover, en cuyo caso la estación base actual renvía el mensaje a todas las posibles estaciones base solicitándoles que cumplan con los

recursos necesarios y el nivel QoS esperado. Enseguida el dispositivo móvil manda un mensaje a su estación base para confirmar o cancelar el handover: en caso de continuar tendrá que negociar con la estación base destino la autorización, autenticación y registro. Opcionalmente la estación base puede comunicarse con la estación base destino para proporcionarle los datos del usuario y de esta forma minimizar la latencia implicada en las comunicaciones.

En lo que respecta a los handovers anticipados, esta capacidad es opcional y dependerá de las políticas con las que esté configurada la red WirelessMAN-Advanced. Hoy en día únicamente existen 2 opciones disponibles:

- Handover de Macro-Diversidad, MDHO por sus siglas en inglés (Macro-Diversity Handover): al presentarse un handover el dispositivo del usuario recibe simultáneamente la señal de varias estaciones base y elige a una de éstas como su nuevo punto de acceso.

- Conmutación Rápida de Estaciones Base, FBSS por sus siglas en inglés (Fast Base Station Switching): disminuye la latencia implicada porque durante un handover el dispositivo móvil no lleva a cabo el proceso del handover, simplemente se comunica con una estación base (anchor) y le indica de su desplazamiento a una nueva estación base.

- *LTE-Advanced*: también emplea handovers anticipados aunque, dependiendo específicamente del tipo de redes involucradas contempla soportar 3 tipos de handover [54]:

  - Intra-Handover: el handover ocurre dentro de la misma red LTE, es decir, se conserva la MME y el SGW pero, cambia el eNB.

    Cada dispositivo móvil mide la calidad e intensidad de la señal y envía un reporte de esos datos a su eNB, éste a su vez procesa la información y decide si hay que preparase para un próximo handover, de ser así manda una solicitud a un eNB vecino. La petición puede o no ser aceptada dependiendo de los recursos que posea en ese momento, si no acepta habrá que elegir a otro eNB, en caso contrario el eNB vecino envía un mensaje de respuesta con la información que requerirá el dispositivo del usuario para unirse a su nueva red.

    Al recibir el mensaje el dispositivo móvil ejecuta el handover con la información que le fue transmitida pero, trata de mantener la frecuencia que esté usando en ese momento, sin que ello cause alguna interferencia en su nueva red. Finalmente el usuario se une a su nueva red y manda un mensaje al SGW y PGW

para informarles de su nueva ubicación. Adicionalmente el nuevo eNB manda un mensaje al antiguo eNB para informarle que libere los recursos destinados al dispositivo del usuario.

- Inter-Handover: se presenta el handover entre varias redes LTE. Existe un cambio de MME, pudiendo o no conservarse el mismo SGW.

  La solicitud de handover es realizada por el eNB actual y es dirigida a su MME, ésta al percatarse de que el eNB destino es administrado por otra MME debe comunicarle dicha solicitud. Posteriormente el MME destino le informa la situación a su eNB respectivo para que reserve los recursos necesarios (autenticación, preparación de contexto, etc.) y posteriormente envía un mensaje de regreso al eNB actual. Por su parte el dispositivo móvil termina de asociarse con el eNB destino (recibirá del antiguo eNB los paquetes que vayan dirigidos al usuario). Finalmente el eNB antiguo libera los recursos asociados al dispositivo del usuario.

- Heterogéneo: el handover involucra distintos tipos de redes. Tanto LTE como LTE-Advanced definen la señalización necesaria aunque, adicionalmente se contempla apoyar de la norma 802.21 [56]

WirelessMAN-Advanced y LTE-Advanced han contemplado utilizar la opción que ofrece 802.21, Handover Independiente del Medio, MIH por sus siglas en inglés (Media Independent Handover), como un recurso a través del cual lleven a cabo handovers horizontales y verticales aunque, son estos últimos en los que más asistencia proporciona. El objetivo de MIH es definir extensiones que faciliten y optimicen el desarrollo de handovers entre redes, independientemente del radio de acceso utilizado (802.11, 802.16, Ethernet, redes celulares, etc.) y es su propio diseño el elemento que le permite abarcar 2 de las 3 fases del handover (figura 7.16).

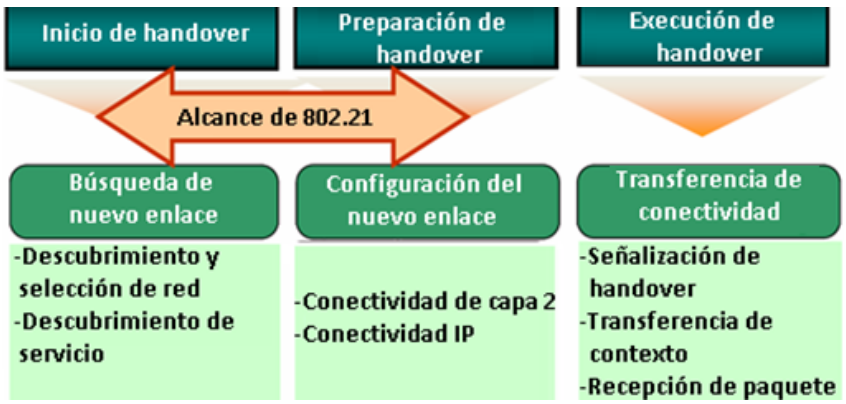



Figura 7.16 Handover Independiente del Medio

Para cumplir con su propósito el protocolo 802.21 emplea varios elementos, y es a través de las interacciones de éstos que logra desarrollar sus capacidades, se enlistan a continuación los elementos más representativos (figura 7.17).

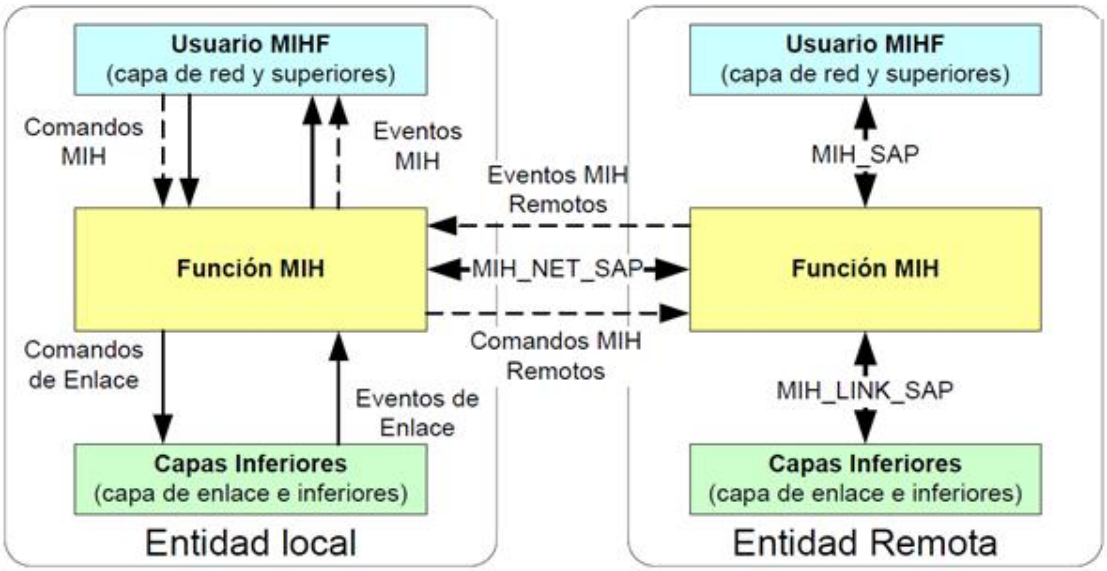



Figura 7.17 Elementos de MIH

- *Función MIH:* entidad lógica que proporciona una interfaz genérica entre las diferentes tecnologías de acceso y las capas superiores, su principal función es coordinar el intercambio de información y comandos entre los dispositivos involucrados en tomar y ejecutar la decisión de realizar un handover.

- *Usuario MIHF:* representa a la entidad que administra la movilidad, la cual se encarga de tomar la decisión de realizar un handover.

- *Puntos de Acceso de Servicio:* proveen al usuario MIHF acceso a servicios a través de los cuales puede recolectar información relacionada con el handover y enviar comandos para controlar la capa de enlace o de red durante el handover. Los 3 principales servicios que brinda MIH son:

  - El servicio de Eventos: facilita la detección de handover al identificar ciertos eventos que denoten cambios de estado en la capa física y de enlace (modificaciones en parámetros, eventos de transmisión), etc.

  - El servicio de Comandos: involucra la transmisión de comandos de las capas superiores a las inferiores para conocer el estado de los enlaces y mejorar el rendimiento del handover (controlar o configurar el móvil). Los comandos se mandan desde el usuario a la función MIH y desde dicha función a la capa de enlace e inferiores.

- El servicio de Información: optimiza la realización del handover porque le permite a la función MIH obtener información de su entorno, los datos incluyen información de las redes disponibles (tipo o tecnología de red, información específica de la red de acceso y del punto de acceso), mapas de sus redes vecinas y la identificación de los servicios disponibles en las capas superiores.

Debido a todos los alcances e implicaciones que tiene el uso del protocolo 802.21 en la actualidad existen varios grupos principales de trabajo que son:

- Grupo A: suministra integridad a los datos y protección anti-respuesta, reduce la latencia que se presenta durante la autenticación y el re-establecimiento de llaves, etc.
- Grupo B: realiza correcciones y provee extensiones para soportar enlaces unidireccionales, optimización de handovers verticales, etc.
- Grupo C: optimiza handovers de un solo radio entre redes heterogéneas.
- Grupo D: se encarga de administrar soluciones de grupos multicast, incluyendo mecanismos para desarrollar de manera segura las comunicaciones.

Ante la gran variedad de opciones que existen no hay que perder de vista que los elementos a contemplar son diversos, sobre todo si se considera que en un futuro próximo habrá millones y millones de dispositivos móviles conectados a las redes 4G, y todos deberán de ser capaces de disfrutar de los servicios que deseen, cuidando sobre todo que no pase lo que actualmente acontece en las redes 3G: se contrata un servicio de alta calidad pero, por la demanda existente no se disfruta de los niveles máximos prometidos sino que únicamente se accede con una calidad medianamente aceptable.

## 7.4 REDES DE PRÓXIMA GENERACIÓN (NGN)

Debido a las nuevas realidades que experimenta la industria de las telecomunicaciones existe una necesidad imperativa de llegar a una convergencia de redes. Es probable que al comenzar a unir varios de los elementos referidos en este capítulo es como será posible hacer frente a la demanda progresiva de nuevos servicios multimedia, soportando el crecimiento y la expansión desmesurada del tráfico digital que se aproxima.

Por fortuna se pudo imaginar que una situación así aparecería en un determinado momento, y surgió la idea de contemplar una Red de Siguiente Generación, NGN por sus siglas en inglés (Next Generation Network) [58]. Este término fue acuñado por la ITU y suele usarse para referirse a la evolución de las redes actuales hasta llegar a la

convergencia de las mismas por lo tanto, el concepto NGN es el siguiente paso; una red de conmutación de paquetes basada en IP que ofrece QoS y que además permite que el transporte sea totalmente autónomo, es decir, los servicios ofrecidos son absolutamente independientes de la tecnología de transporte que se emplee. De acuerdo a la ITU la arquitectura de una NGN se encuentra dividida en los siguientes estratos (figura 7.18).

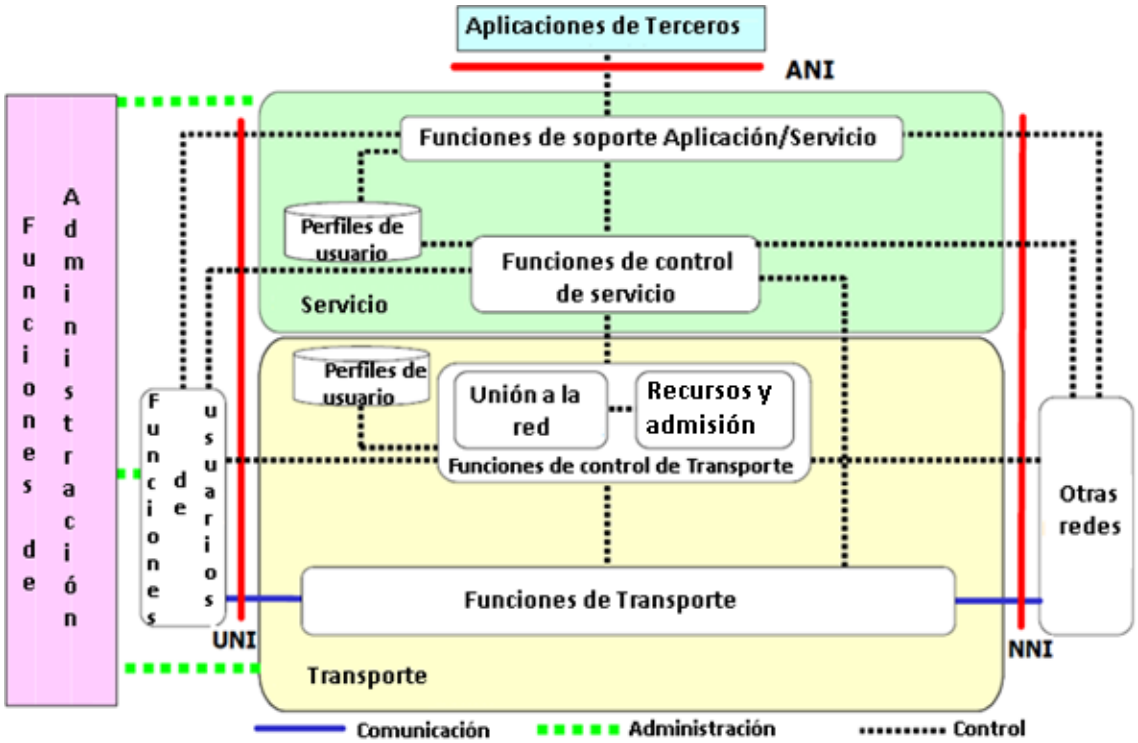



Figura 7.18 Arquitectura de una Red de Próxima Generación

- *Servicios:* almacena los perfiles de los usuarios, incluyendo los respectivos servicios que utilizan. Es con esta información que se logra controlar y administrar los servicios de la red para habilitar los servicios y aplicaciones que están permitidos a los usuarios finales.

- *Transporte:* se encarga de la administración de acceso a la red con el objetivo de interconectar una gran variedad de accesos e interfaces. Adicionalmente proporciona una conectividad basada en IP (soportando QoS) y administra el control de admisión de las sesiones móviles y el tráfico de los usuarios: video, voz, datos, etc.

Dentro de la misma arquitectura existen funciones que incluyen:

- *Aplicaciones:* tiene como tarea controlar las sesiones, administrar las políticas a través de la red, incluyendo servicios como DNS, DHCP, RADIUS, VPN, etc.

- *Administración:* para el estrato de servicios asegura que se entreguen servicios con la suficiente calidad a los usuarios finales, mientras que para el estrato de transporte asigna los recursos necesarios para garantizar niveles óptimos en seguridad, confiabilidad, disponibilidad y QoS.

Es evidente que la integración de los elementos anteriores son los que hacen que NGN sea particularmente única, permitiéndole poseer características como:

- Conmutación basada en paquetes.
- Movilidad generalizada.
- Capacidades transparentes de banda ancha con QoS.
- Soporte de múltiples tecnologías de última milla.
- Independencia entre las funciones de servicio y transporte.
- Convergencia de servicios entre redes fijas y móviles.
- Red basada en IP (AIPN).
- Soporte de una gran variedad de servicios con diferentes requerimientos.

Seguramente una de las características que más llama la atención es la movilidad generalizada, siendo una particularidad que permite a usuarios y dispositivos acceder a servicios independientemente de su cambio de ubicación, desplazándose entre diversos ambientes. Bajo estas circunstancias la disponibilidad depende de distintos factores, tales como: acuerdos de nivel de servicio, capacidades de las redes locales y visitadas, etc., y todo ello gracias a la convergencia de los mundos fijo y móvil.

Con la intervención conjunta de un número impresionante de dispositivos, interfaces, módulos, etc., lo que se espera con NGN es ir más allá de lo inimaginable, llegando a disfrutar de una amplia gama de servicios que estarán a disposición de cualquier persona, independientemente del dispositivo que se use, lugar y tiempo en que se utilice, servicio que se emplee, operador contratado, etc. Sencillamente ya nada será igual, lo único seguro es que se vivirá en un mundo donde la realidad estará por encima de la ficción.

# Capítulo 8

## Propuesta de MIPv6 en RedUNAM

*Omnipotent, Omnipresent, Omniscient. Who is like you? Easy, Nothing, No one - Anonymous*

## 8.1 CASOS DE ESTUDIO CONSULTADOS

Ya se han contemplado un sinfín de aspectos de MIPv6 comenzado desde su funcionamiento general y culminando con las mejoras hechas. Con todo ello es evidente que para los próximos años aún existen muchos retos a enfrentar para lograr un despliegue a mayor escala. Teniendo como base lo anterior fue que se decidió realizar la consulta de algunos casos de estudio, principalmente esta tarea se desarrolló con base a información de varios socios del proyecto europeo 6NET, de forma que los ejemplos más representativos del estudio de MIPv6 fueron:

A. *Fraunhofer Fokus (Alemania):* realizaron varias pruebas que contemplaban la descarga de audio y navegación Web. Los proyectos a los que recurrieron contemplan a KAME y MIPL.

   Un dato interesante es que en todas las pruebas nunca hicieron pasar al MN de una red foránea a su red local y además, no emplearon ningún mecanismo de seguridad para el tráfico intercambiado.

B. *Universidad Lancaster (Reino Unido):* esta universidad desarrolló su propia implementación de MIPv6, por lo tanto fue necesario que realizaran esfuerzos conjuntos con varios investigadores para poder lograr una interoperabilidad con otras implementaciones.

   El objetivo principal de su escenario fue investigar las interacciones que existen entre múltiples redes donde se hace uso de MIPv6. Los proyectos a los que recurrieron fueron MIPL, Microsoft MIPv6 Technical Preview, Cisco Ohanami EFT y KAME.

   Para las pruebas que hicieron únicamente en algunos casos se empleó IPSec (a través de una configuración manual) porque no todos los desarrollos de MIPv6 soportaban su uso.

C. *Universidad de Oulu (Finlandia):* las pruebas que llevaron a cabo se concentraron en investigar el uso de MIPv6 en redes heterogéneas (802.11 y 802.15.1) para conocer lo que ocurría en las comunicaciones al presentarse un handover.

## 8.2 ESCENARIOS CONTEMPLADOS

Una vez finalizada la consulta de los casos de estudio anteriores se prosiguió a la definición de los escenarios contemplados para las pruebas a realizar. En las siguientes secciones se explican las tareas efectuadas en torno a MIPv6.

### 8.2.1 MAQUETA DE PRUEBAS

Para llevar a cabo las pruebas de Movilidad IPv6 como primera opción se consideró el uso de equipo físico, para ello se realizó una búsqueda de aquellos dispositivos que permitieran plantear un escenario viable. Las alternativas encontradas fueron:

1) *Cisco Systems:* tiene una amplia gama de ruteadores que soportan la funcionalidad de Home Agent (es necesario tener un IOS superior o igual a 12) pero, actualmente no cuenta con todas las características de MIPv6, por ejemplo no se puede usar en conjunto con IPSec.

2) *Juniper:* soporta MIPv4 de forma parcial porque únicamente ha desarrollado la funcionalidad de HA, es decir, hoy en día carece de la funcionalidad de FA. En lo que respecta a MIPv6 aún no tiene ningún desarrollo.

3) *Nokia:* posee un controlador que tiene la capacidad de soportar PMIPv6, a pesar de ello está orientado más hacia un entorno comercial porque se basa en el uso de infraestructura de un operador de telefonía.

Con base en las opciones anteriores y a la factibilidad de implementación, se decidió contactar a algún partner o distribuidor de Cisco Systems. Luego de concretar una cita para exponer nuestros requerimientos se acordó esperar alguna propuesta por parte de sus representantes para determinar el equipo a utilizar y las condiciones bajo las cuales se trabajaría, desafortunadamente no se recibió propuesta alguna y luego de reintentar en varias ocasiones comunicarse nuevamente con ellos, se descartó la opción de hacer uso de su equipo.

Finalmente la solución para crear la maqueta de pruebas involucró el uso de varias máquinas con software libre. Teniendo esto en mente los dispositivos y sus respectivas funcionalidades quedaron de la siguiente manera:

- ✓ Dispositivo con funcionalidad de Home Agent
- ✓ Dispositivo con funcionalidad de Mobile Node
- ✓ Dispositivo con funcionalidad de Correspondent Node

Para utilizar MIPv6 sobre un medio inalámbrico se necesitaron de 2 Access Point que reenviaran el tráfico recibido desde/hacia el HA/MN (según fuera el caso), es decir, estos dispositivos simplemente actuaron como “bridge” y no necesitaron de una dirección IP para desempeñar su función ni en su interfaz cableada ni en la parte inalámbrica.

Respecto al cableado usado para la interconexión de los dispositivos se optó por emplear 4 cables UTP para Fast Ethernet (categoría 5).

El siguiente paso fue encontrar implementaciones de MIPv6, en la tabla 8.1 se presentan las más representativas que han surgido a lo largo de los años.

Tabla 8.1 Implementaciones de MIPv6

| | MIPL | Cisco | Microsoft | KAME | HP-UX |
|---|---|---|---|---|---|
| Plataforma | Linux 2.6.8.1 | Cisco IOS | 2000/XP/CE | FreeBSD | HP-UX-11i |
| Modo de operación | MN/HA/CN | HA/CN | MN/HA/CN | MN/HA/CN | MN/HA/CN |
| Protocolo ND | ✓ | ✓ | ✓ | ✓ | ✓ |
| Encabezado de Enrutamiento (Tipo 2) | ✓ | ✓ | ✓ | ✓ | ✓ |
| DHAAD | ✓ | ✓ | ✓ | ✓ | ✓ |
| Administración de Asociaciones | ✓ | ✓ | ✓ | ✓ | ✓ |
| Opción Home Address | ✓ | ✓ | ✓ | ✓ | ✓ |
| Detección de movimiento | Anuncios de Ruteador | N/A | Anuncios de Ruteador | Anuncios de Ruteador | N/A |
| IPSec | ✓ | X | ✓ | ✓ | ✓ |
| Intercambio de llaves | Manual | No | Manual | Manual | X |
| Incorporación de MIPv6 | X | ✓ | X | ✓ | X |
| Número de parches | 1 | 0 | 1 | 0 | 1 |
| Configuración | Archivos de configuración | Línea de comandos | Línea de comandos | Archivos de configuración | Archivos de configuración |
| Licencia | GNU | Comercial | Comercial | GNU | Comercial |

Para la selección de la implementación quedó descartado HP-UX por no contar con el equipo y sistema operativo que se requería para su uso por lo tanto, los elementos de la maqueta quedaron de la siguiente manera:

⇒ Para el Home Agent existen 2 implementaciones:

- *Proyecto KAME:* trabaja sobre NetBSD y FreeBSD. Es necesario considerar que las fuentes oficiales dejaron de estar disponibles (el paquete debe ser descargado en páginas de terceros) [59]

- *Proyecto USAGUI* (UniverSAl playground for IPv6): funciona sobre GNU/Linux. Actualmente la continuación de este proyecto es UMIP [60]

Es importante mencionar que adicionalmente del paquete para MIPv6 es necesario utilizar otro paquete que permita proveer la funcionalidad para anunciar direcciones y prefijos IPv6. Para lidiar con esta situación en GNU/Linux existe el paquete radvd [61] (para BSD se denomina rtadvd).

⇒ Para el MN se tiene la misma situación que para el Home Agent.

⇒ Algo similar ocurre con el CN aunque adicionalmente existe una implementación en el sistema operativo Windows XP (al no ser interoperable con UMIP la opción quedó descartada).

Debido a los tiempos en que fueron creados los proyectos antes mencionados, se eligió a UMIP dado que es el desarrollo más reciente y existe más información al respecto, además continuamente se le sigue dando soporte por parte de los desarrolladores.

Dentro del diseño de la maqueta de pruebas el direccionamiento del espacio IPv6 utilizado fue el siguiente: se trabajó bajo una red aislada e interna de manera que el segmento principal de red que se utilizó fue 2001:db8::/48. Se ilustra en la figura 8.1 la manera en que los prefijos IPv6 se asignaron a los enlaces.

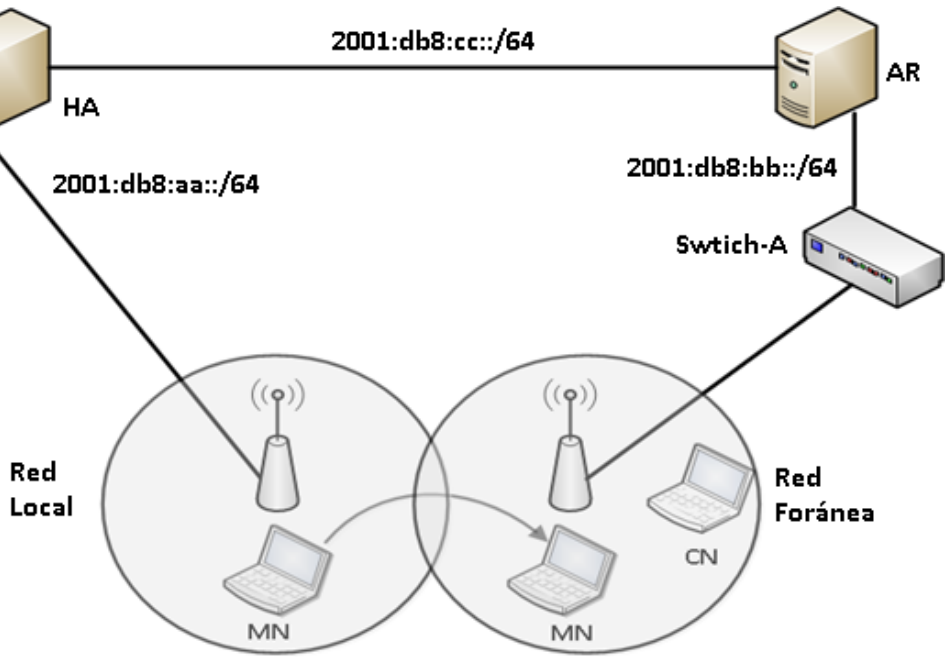



Figura 8.1 Maqueta de pruebas de MIPv6 utilizada

A continuación en la tabla 8.2 se resumen los componentes empleados.

Tabla 8.2 Elementos de la maqueta de pruebas

| Elemento | Nombre | Sistema Operativo | Implementación de MIPv6 | Función | Dirección IPv6 |
|---|---|---|---|---|---|
| Ruteador de Acceso | AR | GNU/ Debian | - | Ruteador | Interfaz con HA 2001:db8:cc::2/64 |
| Agente Local | HA | GNU/ Fedora | USAGUI umip 0.4 | | Home Address 2001:db8:aa::1/64 Interfaz con AR 2001:db8:cc::1/64 |
| Nodo Móvil | MN | | | Envío, recepción | HoA 2001:db8:aa::10/64 |
| Nodo Corresponsal | CN | Windows XP | - | | Interfaz con AR 2001:db8:bb::100/64 |
| Access Point | AP A | - | - | Bridge | - |
| | AP B | - | - | | - |
| Switch | Switch-A | Cisco IOS | - | Conmutador | - |

En los anexos D y E se mencionan los aspectos más representativos de las pruebas realizadas con el equipo físico y la experiencia que resultó de cada uno de los diferentes tipos de tráfico intercambiados. Es importante aclarar que lo más importante de esto fue la conducta observada porque a través de ella fue posible conocer la madurez actual de MIPv6.

### 8.2.2 SIMULADORES

La segunda opción contempló el empleo de algún simulador. Actualmente aquellos que ofrecen un desarrollo más sólido de MIPv6 son los siguientes:

i. *OPNET:* posee un buen soporte de Movilidad IPv6 aunque se requiere de una licencia para utilizarlo. A pesar de que se puede obtener una prueba gratuita únicamente se tiene disponible para su descarga la versión 9, pero es a partir de su versión 14 que se encuentra la funcionalidad requerida.

ii. *OMNeT++:* actualmente es el desarrollo más reciente que se encuentra disponible de Movilidad IPv6 sin embargo, no es posible hacer uso de IPSec para proteger las comunicaciones [62].

En un principio se trató de comparar las características que ambos simuladores ofrecían desafortunadamente no fue posible conseguir la versión 14 de OPNET o la licencia correspondiente que se necesitaba por lo tanto, los esfuerzos subsecuentes se concentraron solamente en el segundo simulador.

OMNeT++ es un paquete de simulación de código abierto que puede ser usado para fines académicos (no existe necesidad de conseguir una licencia). Por sí mismo no posee las características que se requerirán y por ello fue necesario hacer uso de un modelo de simulación que funcionara con OMNeT++, denominado xMIPv6 [63]

El modelo xMIPv6 está basado en el RFC 3775 y es importante conocer esto porque a que a mediados del año pasado (2011) la IETF remplazó dicho documento por el RFC 6275, afortunadamente las pruebas a las que ha sido sometido dicho modelo ratifican sus características.

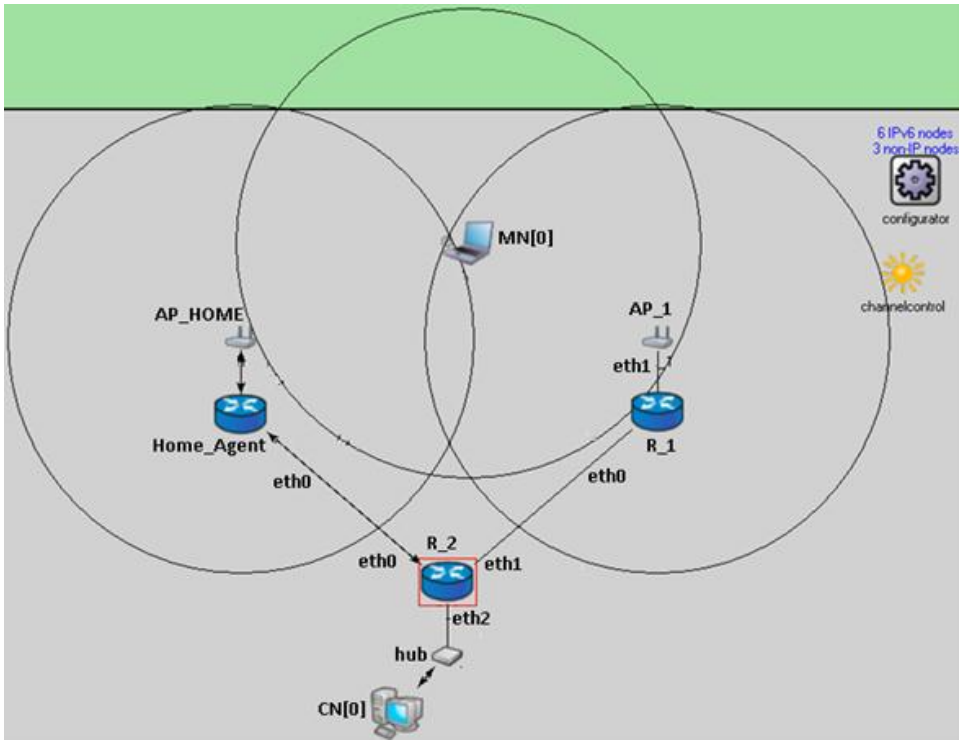



Figura 8.2 Topología de la red de pruebas con OMNeT++

En la figura 8.2 se encuentra el diagrama de la topología de red bajo la cual se realizaron las pruebas con OMNeT++, la idea sobre la que se trabajó en la simulación involucró al MN experimentando un handover, es decir, el MN se trasladó de su red local a una red foránea. Como se observa en la tabla 8.3 existieron 7 elementos representativos.

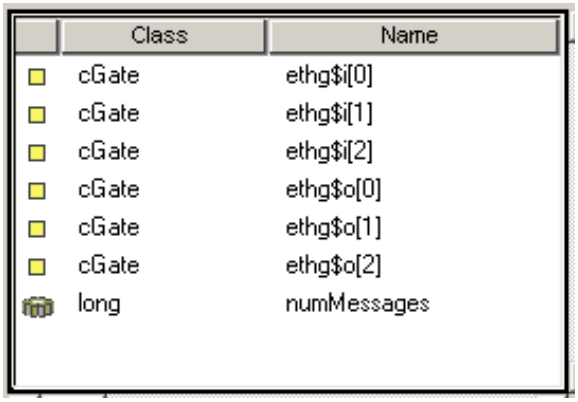
Tabla 8.3 Direcciones en los elementos de la simulación con OMNeT++

| Elemento | Interfaz | Dirección IPv6 | Dirección MAC |
|---|---|---|---|
| MN[0] | wlan | HoA →aaaa:0:1:0:aaa:ff:fe00:11<br>CoA →aaaa:1:1:0:aaa:ff:fe00:11 | 0A-AA-00-00-00-08 |
| AP_HOME | wlan | No aplica | 10-AA-00-00-00-01 |
| | eth0 | | 10-AA-00-00-00-02 |

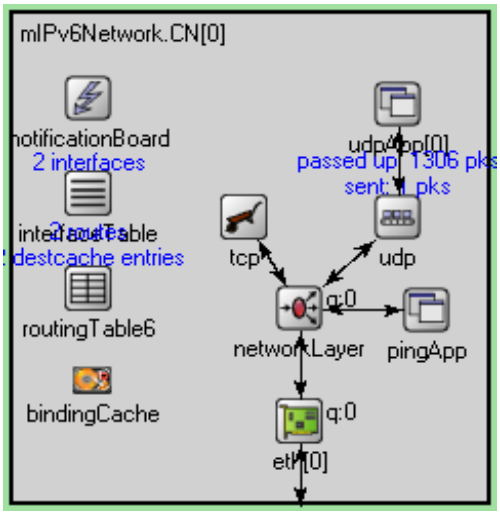
| | | | |
|---|---|---|---|
| Home_Agent | eth0 | aaaa::aaa:ff:fe00:1 | 0A-AA-00-00-00-01 |
| | eth1 | aaaa:0:1:0:aaa:ff:fe00:2 | 0A-AA-00-00-00-02 |
| R_2 | eth0 | aaaa:2::aaa:ff:fe00:5 | 0A-AA-00-00-00-05 |
| | eth1 | aaaa:2:1:0:aaa:ff:fe00:6 | 0A-AA-00-00-00-06 |
| | eth2 | aaaa:2:2:0:aaa:ff:fe00:7 | 0A-AA-00-00-00-07 |
| CN[0] | eth0 | aaaa:2:2:0:aaa:ff:fe00:9 | 0A-AA-00-00-00-09 |
| R_1 | eth0 | aaaa:1::aaa:ff:fe00:3 | 0A-AA-00-00-00-03 |
| | eth1 | aaaa:1:1:0:aaa:ff:fe00:4 | 0A-AA-00-00-00-04 |
| AP_1 | wlan | No aplica | 10-AA-00-00-A1-01 |
| | eth0 | No aplica | 10-AA-00-00-A1-02 |

La tabla anterior pertenece a una configuración automática que se obtuvo al agregar un módulo de configuración de OMNeT++ denominado “FlatNetworkConfigurator”. Se utilizó dicho módulo debido a que resulta bastante útil y práctico en redes de pruebas, y además permite fácilmente que cada dispositivo adquiera una dirección IPv6 automáticamente.

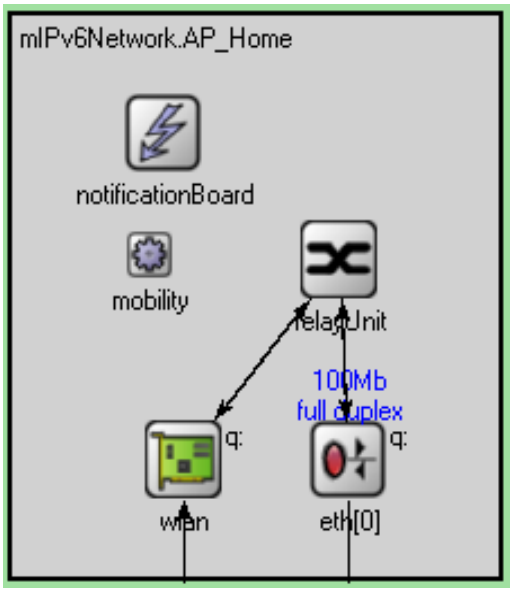
Cada uno de los elementos listados con anterioridad está conformado por una serie de sub-módulos, siendo la interacción que existe entre ellos lo que permitió que los dispositivos llevaran a cabo sus procesos que van desde manejar tablas de ruteo, adquirir sus direcciones (IPv6 y MAC), hasta el manejo de las estructuras de almacenamiento que permiten el funcionamiento de MIPv6. Es importante mencionar que los elementos que tuvieron soporte de MIPv6 son: HA, MN y CN; en la figura 8.3 se aprecia con claridad dicha situación y al mismo tiempo se presentan los sub-módulos que integraron a cada uno de los dispositivos utilizados.



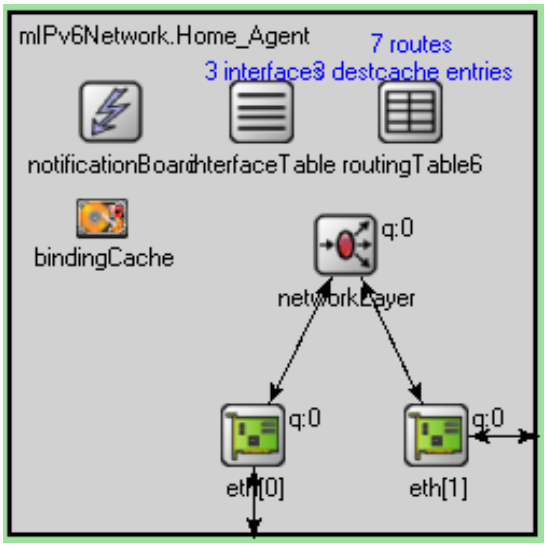

Hub



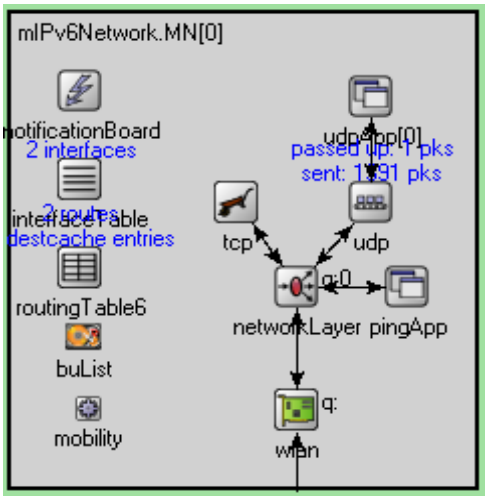

Correspondent Node



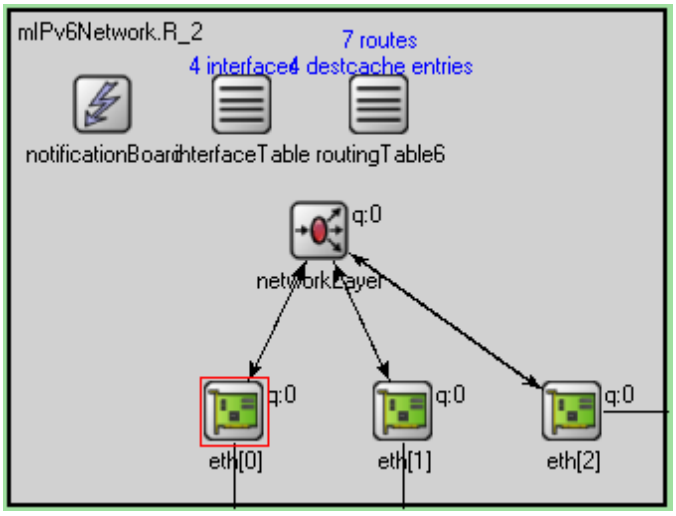

Access Point




Agente Local




Nodo Móvil




Ruteador de Acceso

Figura 8.3 Elementos utilizados en la simulación con OMNeT++

## 8.3 ASPECTOS A CONSIDERAR EN LAS PRUEBAS

En capítulos pasados se definieron las características e influencia del handover en las comunicaciones móviles, teniendo esos datos en mente fue que se prosiguió a definir los aspectos considerados en las pruebas. Básicamente en los escenarios planteados existió un medio alámbrico y uno inalámbrico, y en dicho ambiente se realizó un intercambio de diferentes tipos de tráfico por medio de varios protocolos, los casos manejados trataron de ser desarrollados bajo las mismas circunstancias sin embargo, existieron algunas modificaciones en unos de ellos. La tabla 8.4 muestra un breve resumen que describe los escenarios de las pruebas realizadas.

Tabla 8.4 Escenarios de pruebas realizadas

| Tráfico | Dispositivos |
|---|---|
| 1. Intercambio de echos ICMPv6. | ⇒ MN a CN<br>⇒ CN a MN |
| 2. Modelo UDP cliente-servidor | ▪ MN: servidor<br>▪ CN: cliente |
| 3. Modelo TCP cliente-servidor | ✓ MN: cliente<br>✓ CN: servidor |

Antes de detallar los escenarios de la tabla anterior es importante mencionar que adicionalmente en cada uno de estos se agregó una variable que contempló el cambio en la velocidad de desplazamiento del MN; los valores que se consideraron fueron elegidos por las capacidades y limitaciones propias de xMIPv6. Se presentan en la tabla 8.5 las diferentes velocidades utilizadas.

Tabla 8.5 Velocidades de desplazamiento del MN

| Movimiento | Velocidad [metro/segundo] |
|---|---|
| Antes, durante y después del Handover | 1 |
| | 2 |
| | 5 |
| | 8 |
| | 10 |

### 8.3.1 TRÁFICO ICMPV6

Para este tráfico en particular únicamente se realizó el intercambio de mensajes echo de ICMPv6 (solicitud y respuesta), situación que suele ser muy cotidiana al hacer un ping a cierta dirección IPv6.

La comunicación entre el CN y el MN se desarrolló con la particularidad de que el intercambio de mensajes fue simultáneo, es decir, del CN al MN y viceversa, la transmisión del tráfico ICMPv6 comenzó cuando el MN se encontraba en su red local y fue a través de MIPv6 que pudo seguir enviando y recibiendo dicho tráfico al pasar a una red foránea. Es importante aclarar que para cualquier tipo de tráfico es necesario que el MN comience su desplazamiento desde su red local hacia cualquier otra red foránea por lo tanto, el MN no puede iniciar MIPv6 desde una red foránea. La tabla 8.6 resume las características bajo las cuales se planteó este escenario

.Tabla 8.6 Características en el escenario del tráfico ICMPv6

| Tráfico | Características |
|---|---|
| ICMPv6 | Tamaño: 32[Bytes] |
| | Tiempo de inicio: 10[s] |
| | Tiempo de término: 120[s] |
| | Intervalo entre envíos: 0.5[s] |
| | Tiempo de vida: 32 saltos |

### 8.3.2 TRÁFICO UDP

Se recurrió al uso de un modelo cliente/servidor aunque a diferencia del escenario anterior, no se realizó de manera simultánea ya que xMIPv6 únicamente permite que para una simulación un nodo se comporte como cliente o como servidor por lo tanto, para el primer caso el MN fue el servidor mientras que el CN actuó como cliente, y en el segundo caso se invirtieron sus funciones.

En la transmisión de tráfico UDP se consideraron diferentes tamaños de un stream de video almacenado en el servidor. Las características más representativas de este tráfico se presentan en la tabla 8.7.

Tabla 8.7 Características en el escenario del tráfico UDP

| Tráfico | Características |
|---|---|
| UDP | a) Servidor |
| | Tamaño del stream de video: 2, 5, 10, 20, 50, 100[MB] |
| | Longitud de datagramas: 1250[Bytes] |
| | Puerto de escucha: 3088 |
| | Intervalo entre envíos: 0.01[s] |
| | b) Cliente |
| | Puerto local: 9999 |

### 8.3.3 TRÁFICO TCP

Para el tráfico TCP también se utilizó un modelo cliente/servidor sin embargo, a diferencia de los casos anteriores (UDP, ICMPv6) existieron ciertos cambios debido a la naturaleza de este protocolo.

Únicamente se decidió transmitir un archivo con un tamaño de 10MB porque existen algunas limitantes en el módulo TCP al ser utilizado con xMIPv6, se optó entonces por no variar el tamaño del archivo contenido en el servidor y solamente se cambió el tamaño de la Ventana Anunciada del Receptor, RWND por sus siglas en inglés (Receiver Window). Las características más representativas de este tráfico se visualizan en la tabla 8.8.

Tabla 8.8 Características en el escenario del tráfico TCP

| Tráfico | Características |
|---|---|
| TCP | Ventana inicial habilitada |
| | Tamaño de la Ventana Anunciada: 6500 (serie 1), 20000 (serie2), 35000 (serie 3), 50000 (serie 4), 65000 (serie 5) [Bytes] |
| | Tamaño del MSS: 1220 [Bytes] |
| | a. Servidor |
| | Puerto de escucha: 80 |
| | Intervalo entre envíos: 0.01 [s] |
| | b. Cliente |
| | Puerto local: 1100 |
| | Longitud de solicitud: 200 [Bytes] |
| | Longitud de respuesta: 10 [MB] |

## 8.4 RESULTADOS

Con los resultados obtenidos fue más clara la comprensión de MIPv6: su influencia, alcance, así como las limitaciones que actualmente posee. Enseguida se describe lo acontecido en los escenarios antes descritos.

### 8.4.1 TRÁFICO ICMPV6

Como se recodará se plantearon diferentes velocidades del MN, a pesar de ello en esta sección se analiza más a detalle el primer caso (1[m/s]) y del resto por cuestiones prácticas se presenta únicamente un resumen de los datos obtenidos (las gráficas respectivas están en el anexo A).

En este primer escenario se transmitieron mensajes echo de ICMPv6 (solicitudes y respuestas) del MN al CN y simultáneamente en la dirección contraria. Tal y como se ilustra en la figura 8.4, el comportamiento durante los primeros segundos fue muy parecido al presentado en un ambiente inalámbrico, cuestión entendible porque en ese lapso de tiempo el MN permaneció dentro del área de cobertura de su punto de acceso original (localizado en su red local), posteriormente a ello comenzó a suscitarse un repentino aumento en los tiempos de respuesta en ambas direcciones de la comunicación establecida entre el MN y el CN, conducta que se atribuye principalmente a lo siguiente:

- El MN al salir de su red local pasó al área de cobertura de un nuevo punto de acceso perteneciente a una red foránea por lo tanto, el móvil no solamente tuvo la necesidad de adquirir temporalmente una dirección IPv6 secundaria (CoA), mientras se encontró en tal segmento de red, sino que además siguió conservando su dirección IPv6 primaria (HoA).

- El hecho de que el CN también tuviera soporte de MIPv6 causó que los paquetes destinados al MN se mandaran directamente a su nueva dirección CoA, es decir, durante el handover existió un mayor retraso en el restablecimiento de las comunicaciones por el desarrollo del mecanismo Return Routability. Adicionalmente para mantener activas las conexiones de los mensajes intercambiados se emplearon encabezados de extensión, por ejemplo:

  - Cuando el MN envió un paquete al CN tuvo que colocar su dirección CoA como dirección origen y su dirección HoA dentro del encabezado de Opciones de Destino. Mientras tanto el CN al recibir el paquete intercambió las direcciones HoA y CoA para mantener intacta la comunicación en las capas superiores.

  - Por su parte el CN colocó la dirección CoA del MN como dirección destino y la dirección HoA fue almacenada en el Encabezado de Enrutamiento Tipo 2; esta situación ocasionó que el MN realizara el cambio respectivo de las direcciones antes de pasar la información a la capa inmediata superior.

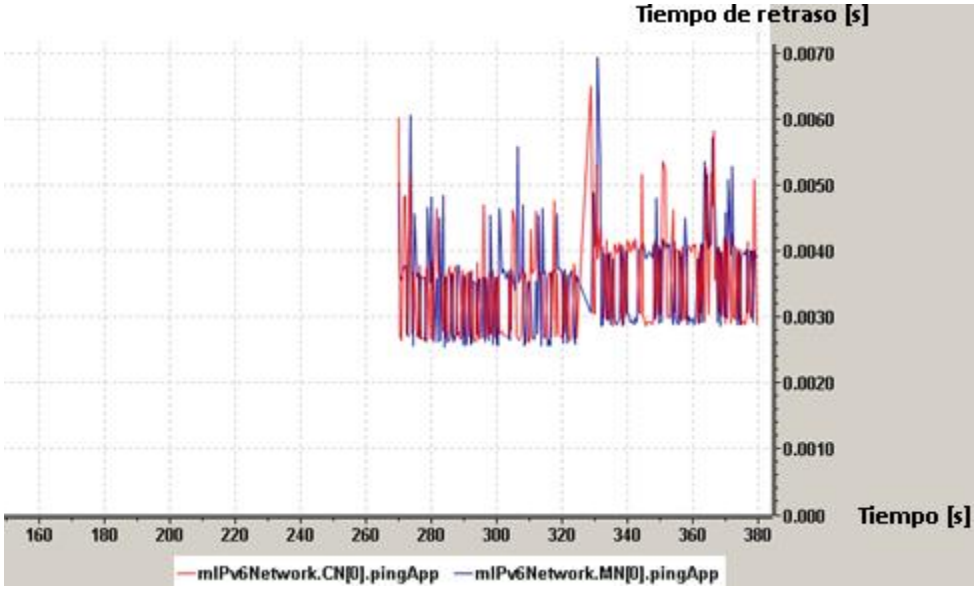



Figura 8.4 ICMPv6 y Retardo de ida y vuelta

También es posible apreciar que alrededor de los 324.5 [s] se llevó a cabo el handover y por ende se interrumpió temporalmente la entrega total de paquetes, de un total de 220 solicitudes transmitidas por ambas entidades existió una pérdida de 7 de ellas. Algunas de las causas atribuidas a estas conductas fueron:

- La pérdida de los paquetes transmitidos por el MN ocurren porque este último conoce en todo momento la ubicación precisa del CN no obstante, al experimentar el handover existió una fracción de tiempo en que no pudo seguir enviándole mensajes porque no tenía ninguna asociación con algún punto de acceso,

careciendo de esa forma de una configuración válida para seguir transmitiendo exitosamente.

- Por otro lado el CN experimentó una pérdida de los paquetes enviados porque a pesar de tener una configuración válida en todo momento, en un principio tuvo que esperar a que el HA registrará exitosamente al MN, y fue hasta ese momento que pudo participar en el mecanismo Return Routability para tener la capacidad de comunicarse directamente con la nueva dirección IPv6 (CoA) del MN. Es precisamente hasta ese instante en que volvió a reanudarse la transmisión.

Se muestra en la tabla 8.9 el resumen con los resultados obtenidos.

Tabla 8.9 Mensajes ICMPv6 transmitidos y recibidos

| Tráfico ICMPv6 | Paquetes enviados | Paquetes recibidos |
|---|---|---|
| MN a CN y CN a MN | 220 | 213 |

De la tabla anterior se obtiene el porcentaje de pérdida del tráfico ICMPv6 (figura 8.5).

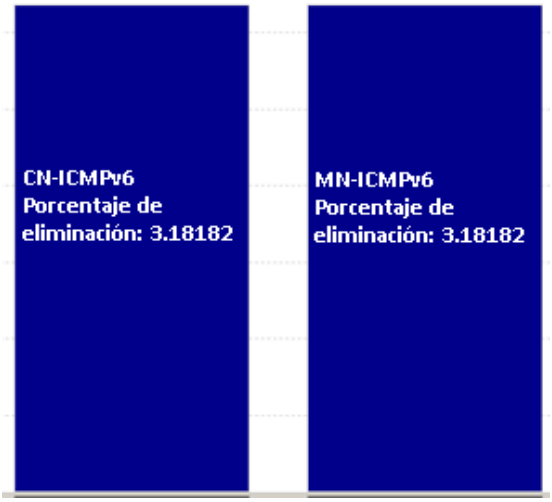



Figura 8.5 Porcentaje de mensajes ICMPv6 eliminados

La tabla 8.10 ilustra los resultados presentados para el resto de las velocidades.

Tabla 8.10 Resultados de tráfico ICMPv6 a diferentes velocidades

| Dirección de tráfico | Descripción | Velocidad (m/s) 2 | 5 | 8 | 10 |
|---|---|---|---|---|---|
| MN a CN y CN a MN | ICMPv6 Enviados / Recibidos | 220 / 213 | 220 / 213 | 220 / 212 | 220 / 212 |
| | Pérdida total (%) | 3.181818 | 3.181818 | 3.636363 | 3.636363 |

De la tabla anterior se observa que conforme se incrementó la velocidad con que se desplazaba el MN aumentó gradualmente el porcentaje de pérdida de los paquetes en ambos sentidos (del MN al CN y viceversa), inclusive a pesar de que los tiempos en que el MN experimentó el handover fueron menores. Posiblemente la causa principal de esta pérdida se atribuya a que la detección de movimiento del MN no le permitió percibir rápidamente que se encontraba en una nueva red, de manera que el MN trató de seguir usando su dirección HoA y no fue hasta que descubrió que estaba en otra red que comenzó a adquirir una nueva dirección IPv6 válida.

### 8.4.2 TRÁFICO UDP

En este segundo escenario se recurrió a la transmisión de un stream de video a través del protocolo UDP, principalmente se desarrollaron 2 secciones donde CN y MN intercambiaron los papeles cliente/servidor.

#### MODELO CLIENTE-SERVIDOR (SERVIDOR-MN, CLIENTE-CN)

Este modelo muestra los detalles obtenidos cuando el MN se desplaza a 1[m/s] y del resto de las velocidades se presenta un resumen (las gráficas están en el anexo B). Los resultados conseguidos se describen en función del tamaño del stream de video transmitido: 2, 5, 10, 20, 50 y 100 [MB], el resumen de los resultados está en la tabla 8.11.

Tabla 8.11 Resumen de datagramas perdidos (MN-servidor)

| Tamaño del stream [MB] | Número de datagramas perdidos | Datagramas perdidos (%) |
|---|---|---|
| 2 | 171 | 10.190703 |
| 5 | | 4.076281 |
| 10 | | 2.038383 |
| 20 | | 1.019191 |
| 50 | | 0.4076864 |
| 100 | | 0.203845 |

El número total de datagramas perdidos para cada caso fue el mismo independientemente del tamaño del stream, esto se debe a que para todos los casos planteados el MN experimentó el handover durante el mismo tiempo y por ende la repercusión fue la misma. Los porcentajes de pérdida llegaron a ser diferentes únicamente porque se realizó una variación en el tamaño del stream a pesar de ello, en esencia el efecto en las comunicaciones del usuario fue igual en un determinado periodo de tiempo y después de eso se restableció la transmisión. Con base en lo anterior se percibe la dependencia que existe entre el tiempo en que el usuario está en el área donde cambia su punto de acceso y el número de datagramas perdidos.

Se comentó recientemente que el proceso en el cambio de direcciones realizado causó un procesamiento adicional de cada paquete a pesar de ello, es a través de esta tarea que se logró mantener una comunicación que ya estaba establecida, por lo tanto es esencial. En la figura 8.6 se observa un comportamiento donde se aprecia que existió un incremento constante en los tiempos de entrega de los datagramas, primero se presentó una ausencia de transmisiones y posteriormente unos segundos más tarde, (justo después de que finalizó el evento de handover) se manifestó un retraso distintivo y generalizado de 0.0004[s] (al mantenerse constante resulta significativo aunque no es representativo si tomamos en consideración que se trata de microsegundos).

Por otro lado, es importante aclarar que en todos los escenarios planteados existió una superposición parcial de las señales, es decir, el punto de acceso de la red local estaba próximo al punto de acceso de la red foránea. La existencia de este ambiente favoreció sustancialmente el que se presentara una mínima pérdida de tráfico, para aquellos casos donde no exista una zona de cobertura de alguna de las 2 señales (local o foránea) es indudable que exista una degradación significativa en la comunicación, y dependiendo del tipo de aplicación y su sensibilidad, puede o no mantenerse la conexión inicial.

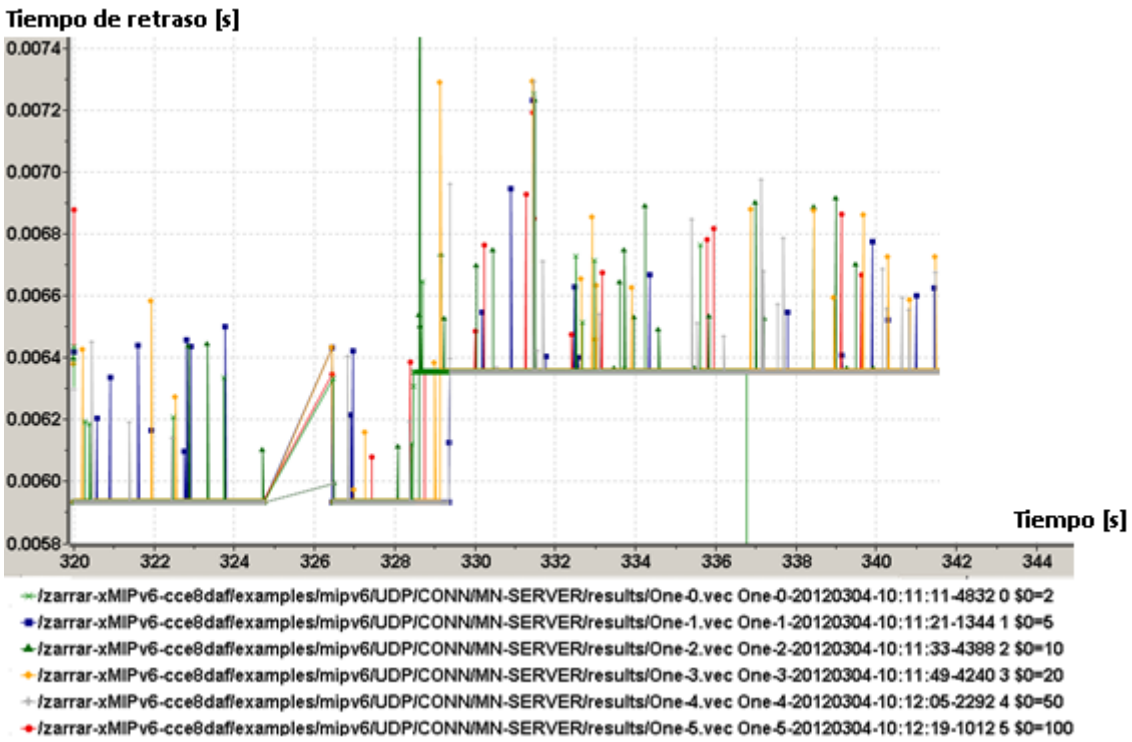


Figura 8.6 Tráfico UDP (MN-servidor)

En la figura anterior para cada uno de los tamaños de streams transmitidos se muestra el comportamiento de los tiempos de respuesta antes, durante y después de que el MN experimentó un handover (aproximadamente 5[s]).

En la tabla 8.12 se observan los resultados obtenidos en aquellas situaciones donde se desarrolló un incremento en la velocidad de desplazamiento del MN, particularmente se distingue una tendencia que depende principalmente de la variación de velocidad que experimenta el mismo, es decir, a medida que éste aumentaba su velocidad se presentó un mayor número de datagramas perdidos, a pesar de ello la relación que se presentó no es directamente proporcional pero sí lo suficientemente clara como para acentuar que este comportamiento se debe a la detección de movimiento que lleva a cabo el MN. Lo comentado recientemente deja en evidencia que uno de los retos que actualmente enfrenta MIPv6 es el desarrollo de un algoritmo más robusto que permita detectar de una manera más eficiente el movimiento, es precisamente dicha capacidad lo que hará posible que el MN perciba con mayor rapidez su condición, adquiera prontamente su dirección CoA y realice el intercambio de mensajes de registro.

Tabla 8.12 Tráfico UDP en función de la velocidad de desplazamiento (MN-servidor)

| Datagramas | Tamaño [MB] | Velocidad (m/s) | | | |
|---|---|---|---|---|---|
| | | 2 | 5 | 8 | 10 |
| $\frac{\text{Enviados}}{\text{Recibidos}}$ | 2 | $\frac{1678}{1506}$ | $\frac{1678}{1508}$ | $\frac{1678}{1507}$ | $\frac{1678}{1504}$ |
| Pérdida (%) | | 10.250297 | 10.131108 | 10.190703 | 10.369487 |
| $\frac{\text{Enviados}}{\text{Recibidos}}$ | 5 | $\frac{4195}{4024}$ | $\frac{4195}{4025}$ | $\frac{4195}{4024}$ | $\frac{4195}{4021}$ |
| Pérdida (%) | | 4.076281 | 4.052443 | 4.076281 | 4.147794 |
| $\frac{\text{Enviados}}{\text{Recibidos}}$ | 10 | $\frac{8389}{8220}$ | $\frac{8389}{8216}$ | $\frac{8389}{8218}$ | $\frac{8389}{8214}$ |
| Pérdida (%) | | 2.014542 | 2.062224 | 2.038383 | 2.086065 |
| $\frac{\text{Enviados}}{\text{Recibidos}}$ | 20 | $\frac{16778}{16607}$ | $\frac{16778}{16605}$ | $\frac{16778}{16606}$ | $\frac{16778}{16603}$ |
| Pérdida (%) | | 1.013231 | 1.031112 | 1.025151 | 1.043032 |
| $\frac{\text{Enviados}}{\text{Recibidos}}$ | 50 | $\frac{41944}{41774}$ | $\frac{41944}{41771}$ | $\frac{41944}{41772}$ | $\frac{41944}{41771}$ |
| Pérdida (%) | | 0.405302 | 0.412454 | 0.410070 | 0.417222 |
| $\frac{\text{Enviados}}{\text{Recibidos}}$ | 100 | $\frac{83887}{83717}$ | $\frac{83887}{83714}$ | $\frac{83887}{83715}$ | $\frac{83887}{83712}$ |
| Pérdida (%) | | 0.202653 | 0.206229 | 0.205037 | 0.208613 |

## MODELO CLIENTE-SERVIDOR (SERVIDOR-CN, CLIENTE-MN)

Ahora que se conocen los efectos producidos en la transmisión del stream de video por la variación de diferentes parámetros es momento de describir el comportamiento que se

suscitó al intercambiar los roles en las comunicaciones, el MN (cliente) solicita el stream de video al CN que actúa como servidor. En la tabla 8.13 se presentan los resultados que se obtuvieron al trabajar con estos nuevos roles (la velocidad del MN es 1[m/s]).

Tabla 8.13 Resumen de datagramas perdidos (CN-servidor)

| Tamaño del stream [MB] | Número de Datagramas perdidos | Datagramas perdidos (%) |
|---|---|---|
| 2 | 389 | 23.182359 |
| 5 | 445 | 10.607866 |
| 10 | 457 | 5.447609 |
| 20 | 410 | 2.443676 |
| 50 | 423 | 1.008487 |
| 100 | 424 | 0.505441 |

Bajo este escenario después de casi 5[s] de experimentar el handover comenzó a restablecerse la entrega exitosa de los datagramas (instante en que el MN se pudo comunicar directamente con el CN). En comparación con el caso anterior, se destaca un comportamiento en particular donde los datagramas presentan tiempos de entrega menores: al estar el MN en una red foránea el retraso general de cada paquete es aproximadamente de tan sólo 0.0001 [s], cifra que representa aproximadamente 4 veces menos tiempo que el caso anterior (figura 8.7).

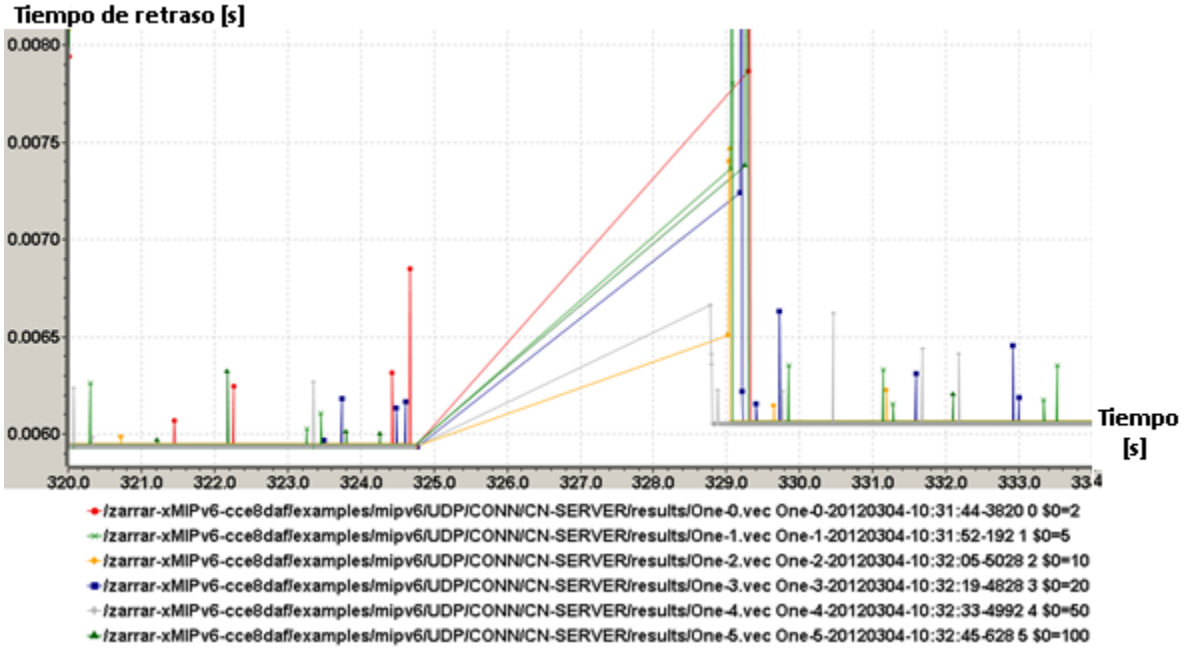


Figura 8.7 Tráfico UDP (CN-servidor)

Finalmente en la tabla 8.14 se encuentran los resultados obtenidos con las diferentes velocidades manejadas para el MN. Al realizar una comparación con la tabla 8.10 es claro

que en este ambiente existió un mayor número de datagramas perdidos, más del doble. Para entender esta situación es necesario considerar lo siguiente:

Al ser el CN el servidor simplemente se dedica a entregar los datagramas a la dirección HoA del MN aun cuando este último deja de tener una asociación con algún punto de acceso. Es precisamente esto lo que ocasiona una pérdida mayor de datagramas porque el CN no está consciente de que acontece dicho evento y simplemente sigue enviando datagramas en todo momento. Esta situación difiere del ejemplo anterior porque bajo ese ambiente por un instante el MN (servidor) se percata de que no está asociado a ningún punto de acceso, y es hasta que adquiere una configuración válida que comienza a enviar nuevamente los datagramas a la dirección del CN.

Tabla 8.14 Tráfico UDP en función de la velocidad de desplazamiento (CN-servidor)

| Datagramas | Tamaño [MB] | Velocidad (m/s) | | | |
|---|---|---|---|---|---|
| | | 2 | 5 | 8 | 10 |
| Enviados / Recibidos | 2 | 1678 / 1299 | 1678 / 1284 | 1678 / 1310 | 1678 / 1260 |
| Pérdida (%) | | 22.58641 | 23.48033 | 21.93087 | 24.91060 |
| Enviados / Recibidos | 5 | 4195 / 3771 | 4195 / 3740 | 4195 / 3767 | 4195 / 3728 |
| Pérdida (%) | | 10.10727 | 10.84625 | 10.20262 | 11.13230 |
| Enviados / Recibidos | 10 | 8389 / 7965 | 8389 / 7938 | 8389 / 7961 | 8389 / 7921 |
| Pérdida (%) | | 5.054237 | 5.376087 | 5.101919 | 5.578734 |
| Enviados / Recibidos | 20 | 16778 / 16375 | 16778 / 16327 | 16778 / 16349 | 16778 / 16310 |
| Pérdida (%) | | 2.401954 | 2.688043 | 2.556919 | 2.789367 |
| Enviados / Recibidos | 50 | 41944 / 41540 | 41944 / 41492 | 41944 / 41515 | 41944 / 41476 |
| Pérdida (%) | | 0.963189 | 1.077627 | 1.022792 | 1.115773 |
| Enviados / Recibidos | 100 | 83887 / 83483 | 83887 / 83435 | 83887 / 83458 | 83887 / 83419 |
| Pérdida (%) | | 0.481600 | 0.538820 | 0.511402 | 0.557893 |

### 8.4.3 TRÁFICO TCP

Para finalizar con las pruebas de simulación únicamente resta describir lo que aconteció con el tráfico TCP. Esencialmente se planteó el uso de un cliente que solicitara

la descarga de un archivo a un servidor; enseguida se presentan las 2 secciones principales en donde se hizo el cambio de roles entre el MN y el CN para desempeñar la función de cliente/servidor.

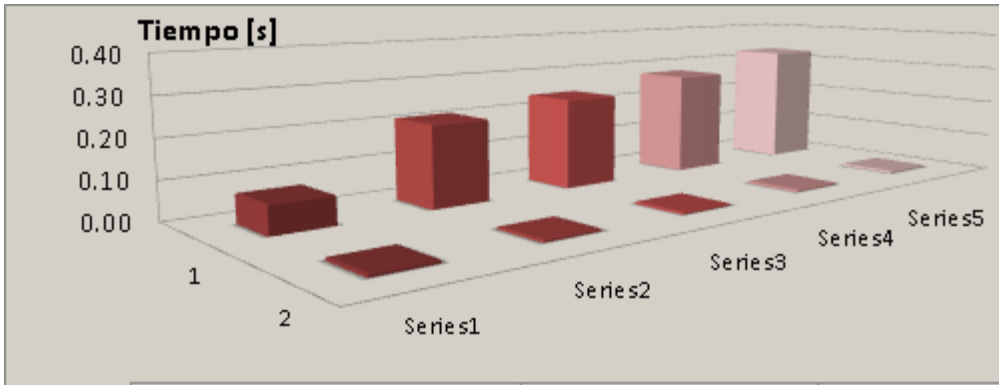
## MODELO CLIENTE-SERVIDOR (SERVIDOR-MN, CLIENTE-CN)

Bajo este escenario el CN realizó una solicitud para descargar un archivo del MN de manera que para cada escenario fue posible manejar uno de los siguientes tamaños en la variable RWND: 6500, 20000, 35000, 50000 y 65000 [Bytes]. Cabe precisar que las diferencias que se presentaron en los tiempos fueron mínimas y existen un sinfín de factores en juego adicionales que no se contemplaron (dignos de ser desarrollados en futuras líneas de investigación); por estas razones las siguientes aseveraciones no son totalmente terminantes.

Es posible apreciar en la figura 8.8 un fragmento de las comunicaciones desarrolladas, específicamente de lo que ocurrió cuando el MN pasó de su red local a una red foránea. A primera vista no existe una particularidad distintiva no obstante, al seguir observando la totalidad de los casos fue posible encontrar un comportamiento en el intercambio del tráfico TCP.


Figura 8.8 Tráfico TCP (MN-servidor)

Al mantener la misma velocidad en el MN y manipular el tamaño de RWND, una de las primeras cosas percibidas fue: mientras el valor de RWND aumentaba se presentó un incremento en el rango de los tiempos de retraso, es decir, existe cierta una relación entre ambas variables porque en el momento en que se amplió RWND se suscitó al mismo tiempo un aumento en el valor máximo de retraso. En la figura 8.9 se observa un ejemplo de esta relación.




| | 1 Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0744896023 | 0.0086608048 | 6500 |
| Series2 | 0.2144750630 | 0.0067783084 | 20000 |
| Series3 | 0.2429457854 | 0.0064609943 | 35000 |
| Series4 | 0.2783107877 | 0.0065209983 | 50000 |
| Series5 | 0.3276218857 | 0.0067980744 | 65000 |

Figura 8.9 Tiempos de retraso en TCP (MN-Servidor)

Por su parte, cuando se añadió mayor velocidad al desplazamiento del MN, los tiempos de retraso presentaron la misma relación aunque con la diferencia de que se comenzaron a acercar los tiempos que existían entre ellos (excepto en el primer valor de RWND), es decir, para un valor A y B de RWND, la diferencia en sus tiempos de retraso respectivos fue cada vez más pequeña al aumentar la velocidad en el MN (remítase al Anexo C).

Otro de los aspectos de interés fue el tiempo de transferencia del archivo, para este caso al conservar una velocidad constante en el MN existió una tendencia donde al incrementar el valor de RWND se observó una disminución en el tiempo de transferencia, es decir, con un menor valor en la variable RWND se presentó un mayor tiempo en la transmisión del archivo, por su parte montos más grandes en RWND hicieron alusión a una disminución en el tiempo de descarga del archivo. Esta situación se ejemplifica claramente en la figura 8.10.

Al momento de involucrar un cambio en la velocidad de desplazamiento del MN, los resultados mostraron que conforme aumentaba dicha velocidad comenzó a existir una modificación en la relación anterior, es decir, que el desplazamiento fuera más rápido ocasionó que se incrementaran los tiempos asociados a la transferencia del archivo. Se puede consultar el Anexo C para observar con mayor claridad la evolución de estas conductas.

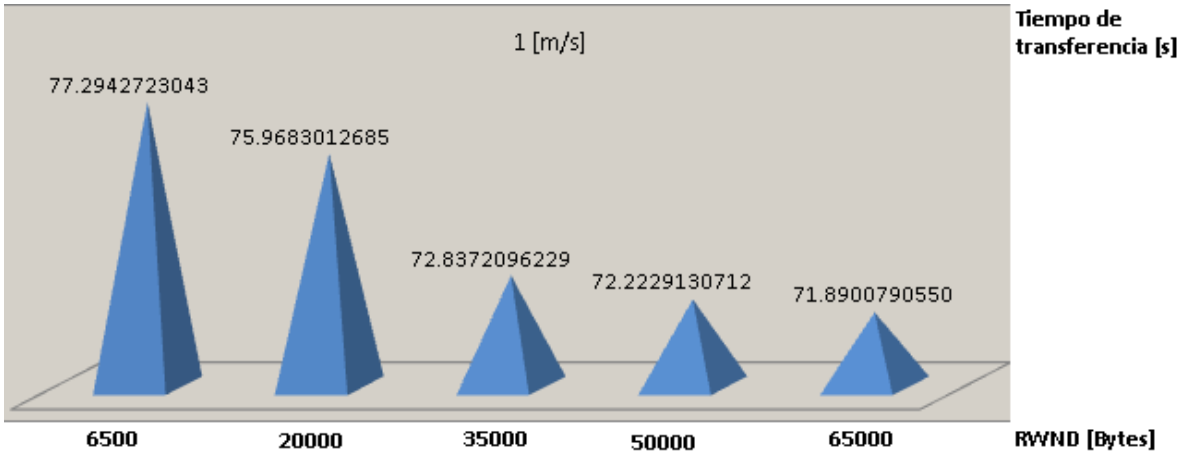



Figura 8.10 Tiempos de transferencia en función del valor RWND (MN-Servidor)

## MODELO CLIENTE-SERVIDOR (SERVIDOR-CN, CLIENTE-MN)

Una vez descritos los resultados que se desarrollaron en la transmisión del archivo y la variación presentada al manejar distintos tamaños de la variable RWND, únicamente resta considerar el comportamiento que se produjo al cambiar los roles en las comunicaciones: el MN (cliente) solicitó la descarga de un archivo al CN (servidor). Cuando se examina la figura 8.11 se aprecia que existe una particularidad en comparación con el caso anterior (MN-Servidor), los tiempos de retraso son menores.

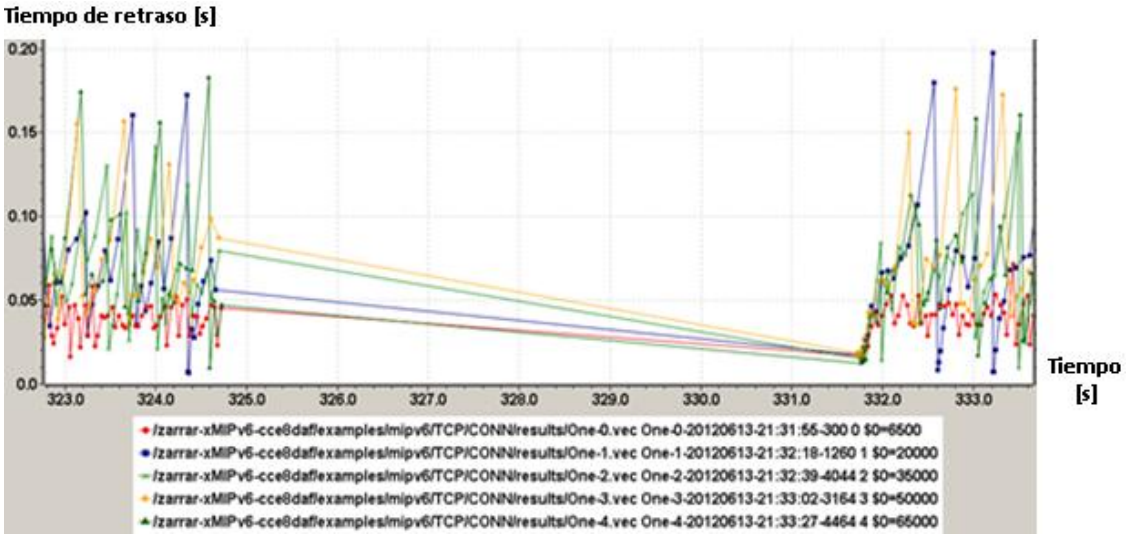
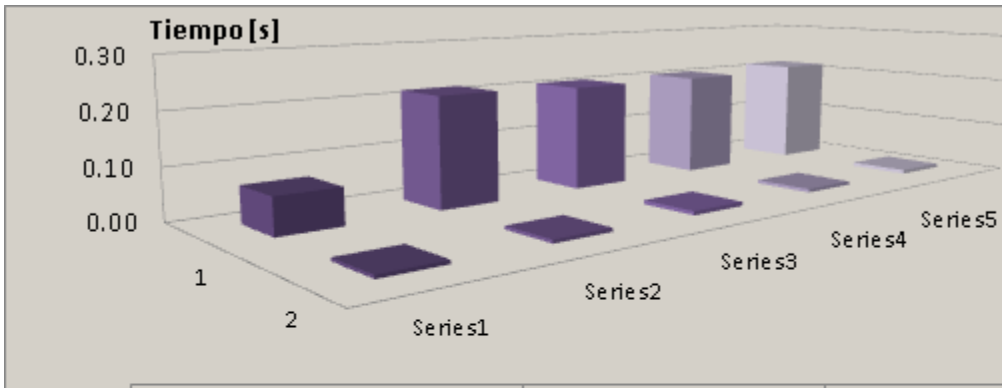



Figura 8.11 Tráfico TCP (CN-servidor)

Al mantener una velocidad constante en el MN y realizar una variación en el valor de RWND se obtuvieron los comportamientos mostrados en la figura 8.12, en dicha ilustración con claridad se percibe una disminución generalizada en los tiempos de retraso de las comunicaciones (fueron más notorios aquellos casos que poseen un valor más alto en la variable RWND). Habrá que tomar en cuenta que TCP al ser un protocolo confiable

maneja diversos mecanismos para controlar la congestión y el flujo de las comunicaciones, y son particularmente dichos elementos los que ocasionan que exista un mayor número de factores detonantes de ciertos comportamientos, es decir, TCP propicia un entorno que en definitiva aumenta el nivel de complejidad implicado en la interpretación de los resultados; aunque estas cuestiones no entran dentro del alcance del presente trabajo.




| | 1 Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0704441773 | 0.0064309891 | 6500 |
| Series2 | 0.2153344232 | 0.0067780619 | 2000 |
| Series3 | 0.2077276762 | 0.0076296582 | 35000 |
| Series4 | 0.2068062538 | 0.0067980199 | 50000 |
| Series5 | 0.2145060348 | 0.0075268291 | 65000 |

Figura 8.12 Tiempos de retraso en TCP (CN-Servidor)

Al momento de incrementar la velocidad en el desplazamiento del MN se siguió manteniendo una conducta muy similar a la antes descrita: menores tiempos de retraso y una diferencia muy cercana en dichos tiempos para diferentes valores de RWND, es decir, dado un tamaño A y B de RWND con una velocidad de B o C existen tiempos de retraso muy cercanos. Algo similar ocurre cuando se compara este comportamiento con el caso anterior (MN-servidor) aunque evidentemente en este escenario los tiempos de retraso fueron más cercanos entre sí.

Para finalizar con TCP únicamente resta describir lo que acontece en los tiempos de transferencia. A diferencia del caso anterior (MN-Servidor), bajo el actual escenario los tiempos permanecieron cercanos entre sí: al conservar una misma velocidad en el MN y cambiando el valor de RWND el impacto en los tiempos de transferencia fue mínimo, situación que conlleva a observar un mejor equilibrio para el caso donde el CN es el servidor y el MN el cliente. Se observa un ejemplo de los resultados en la figura 8.13.

En lo que concierne al incremento en la velocidad de desplazamiento del MN se mantuvo una relación similar al caso anterior (valores cercanos entre sí) aunque se presentó un

ligero aumento en los tiempos totales de transferencia. Evidentemente esta conducta es diferente de aquella que se observó cuando el MN fue el servidor, porque bajo esas condiciones los tiempos totales se incrementaron de manera generalizada, mientras tanto en este escenario para una velocidad A y B, en tiempos de transferencia C y D los valores obtenidos guardan una gran cercanía entre sí. En el anexo C se encuentra el resto de las figuras que ilustran esta serie de comportamientos.

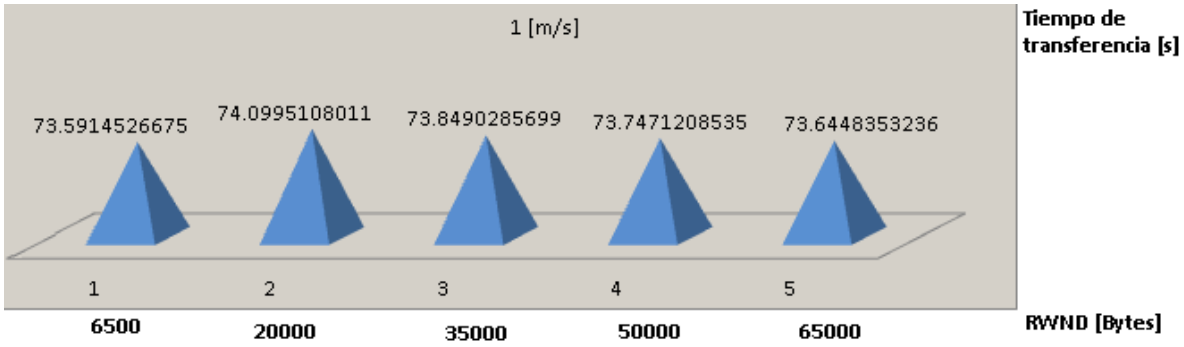



Figura 8.13 Tiempos de transferencia en función del valor RWND (CN-Servidor)

## 8.5 PROPUESTA DE USO EN REDUNAM

En la actualidad es innegable que las tendencias de movilidad que se experimentan involucran una gran variedad de ámbitos, y como era de esperarse, algunos de ellos la necesitan con mayor urgencia. A pesar de esto resulta evidente que las exigencias demandadas son diferentes en cada caso particular por ejemplo: alguien conectado a una red inalámbrica que desea verificar el estado de su correo electrónico no tiene que disfrutar de una conexión permanente no obstante, algunas actividades como realizar una llamada telefónica mediante VoIP, descargar un stream de video, etc. requieren que su conexión se mantenga constante mientras están en movimiento, y por lo tanto requieren disfrutar de una movilidad en todo momento porque de lo contrario se interrumpiría la continuidad de los servicios que estén empleando en ese momento.

Antes de abordar la propuesta que se realizó se presentan algunas de las cifras más significativas que muestran el crecimiento y situación del ciclo escolar 2011-2012 de la UNAM (para mayor información véase el portal de estadísticas de la UNAM):

- 324,413 alumnos
- 36,750 académicos
- 66,000 computadoras conectadas a RedUNAM

RedUNAM está conformada por una infraestructura de alta tecnología en la que switches de capa 3 y ruteadores, se interconectan por medio de enlaces de fibra óptica para brindar conectividad entre dependencias del campus C.U., foráneas, y hacia Internet. Particularmente en RedUNAM (como en cualquier otra red) se llegan a distinguir 3 clases

principales de tráfico: datos, voz y video, por lo tanto para que esta red pueda transmitir cada uno de éstos cuenta con una infraestructura que le permite atender las distintas actividades que se realizan a diario, por ejemplo de acuerdo al informe realizado en el 2011 por la Dirección General de Cómputo y Tecnologías de Información y Comunicación (DGTIC) "Resumen de Iniciativa y Beneficios impulsadas por DGTIC", el crecimiento de RedUNAM ha ido en aumento, tal y como lo muestran los siguientes datos:

- Casi 25000 líneas telefónicas.
- Acceso a Internet 1 (I1) de 900Mbps.
- Acceso a Internet 2 (I2) de 1Gbps directamente a Estados Unidos, de 64Mbps por la red de CUDI (Corporación Universitaria para el Desarrollo de Internet) y de 1Gbps por RI3.

Con base en la información recopilada se decidió plantear una propuesta de uso lo más verosímil posible, para ello fue necesario tomar en cuenta las pruebas realizadas y los resultados obtenidos con el simulador y con la maqueta. Adicionalmente, a la par de contemplar la madurez y desarrollo mostrado por MIPv6, también se tomaron en cuenta las recomendaciones hechas por la Unión Internacional de Telecomunicaciones, ITU por sus siglas en inglés (International Telecommunications Unit); enseguida la tabla 8.15 presenta un panorama más claro sobre las exigencias que demandan los distintos tipos de tráfico.

Tabla 8.15 Requerimientos de tráfico de acuerdo a la ITU

| Tráfico | Retraso [ms] | Jitter [ms] | Ancho de banda [Mbps] | Paquetes perdidos |
|---|---|---|---|---|
| Voz | 150 | <=30 | <=33% del enlace | 2 % |
| Video Interactivo | 150-200 | <=10 | 2-15 | 0.05% |
| IPTV | 150 | <=50 | <2.75 (definición estándar)<br><9 (alta definición) | $<10^{-6}$ |
| Video bajo demanda | | | | |
| Conferencias multimedia | >400 | | <=.460 por video llamada | 1% |

Para definir la propuesta fue importante considerar que es principalmente en DGTIC donde se localiza el control de la mayoría de los servicios ofrecidos por RedUNAM, en consecuencia es posible encontrar áreas como : Centro de Información de RedUNAM (NIC-UNAM), Centros de Operación de la Red (NOC), Centro de Operación de Videoconferencia (VNOC), Telefonía, Red Inalámbrica Universitaria (RIU), etc.

Al contemplar todos los elementos antes mencionados se llegó a una resolución para la propuesta de uso de MIPv6: enfocarse únicamente en la RIU. Esta decisión también se vio influenciada por el hecho de que dicha red constituye un escenario inalámbrico propicio para el uso de MIPv6 en la parte de datos, condición que no es así con los tráficos sensibles al retraso y en tiempo real.

A través de la RIU y por medio de distintos dispositivos móviles es posible acceder a Internet desde diferentes áreas de Ciudad Universitaria, desafortunadamente a partir de la migración realizada en los servidores de las cuentas de correo de comunidad UNAM se ha tenido la necesidad de realizar los registros de acceso a la RIU de manera personal en el Centro de Atención a Usuarios (CAU). Hoy en día debido al incremento del número y variedad de dispositivos utilizados por los usuarios, ha sido necesario brindar un acceso de hasta 3 dispositivos distintos bajo una misma cuenta de registro, dicha situación en gran medida se debe al número de usuarios que utilizan teléfonos inteligentes o tabletas para conectarse a la RIU. De acuerdo a estimaciones realizadas por el CAU cerca de un 60% de los usuarios que piden alguna clase de asesoría utilizan este tipo de dispositivos.

Para cumplir su misión la RIU cuenta con una infraestructura que contempla el uso de controladoras, facilitando así la administración y resolución de problemas, esta situación es más que comprensible si se considera que hasta el día de hoy se tienen cerca de 1000 Access Points distribuidos por las dependencias y facultades de la UNAM. En la figura 8.14 se muestra la estructura general de la RIU y en ella se puede apreciar la distribución de las controladoras.

Para la propuesta en primera instancia se investigaron las capacidades de las controladoras que actualmente se emplean en la RIU y para ello fue necesario familiarizarse con la marca Aruba Networks, específicamente con su equipo Aruba Controller 6000. La información más relevante de Aruba se concentra en su arquitectura denominada MOVE (Mobile Virtual Enterprise), gracias a ésta la controladora de Aruba provee una movilidad a través de toda una red e inclusive llega a presentar un tiempo de handoff de tan sólo unos milisegundos por lo tanto, las aplicaciones sensibles al retraso como voz, video, etc. no experimentan una degradación significativa en su rendimiento. Para lograr estos resultados el sistema de Aruba (ArubaOS) integra el soporte de Proxy Mobile IP, capacidad que se encuentra basada en una modificación del RFC 3344 y que permite que los usuarios no necesiten de ninguna clase de software especial en sus dispositivos para disfrutar de movilidad dentro de una red.

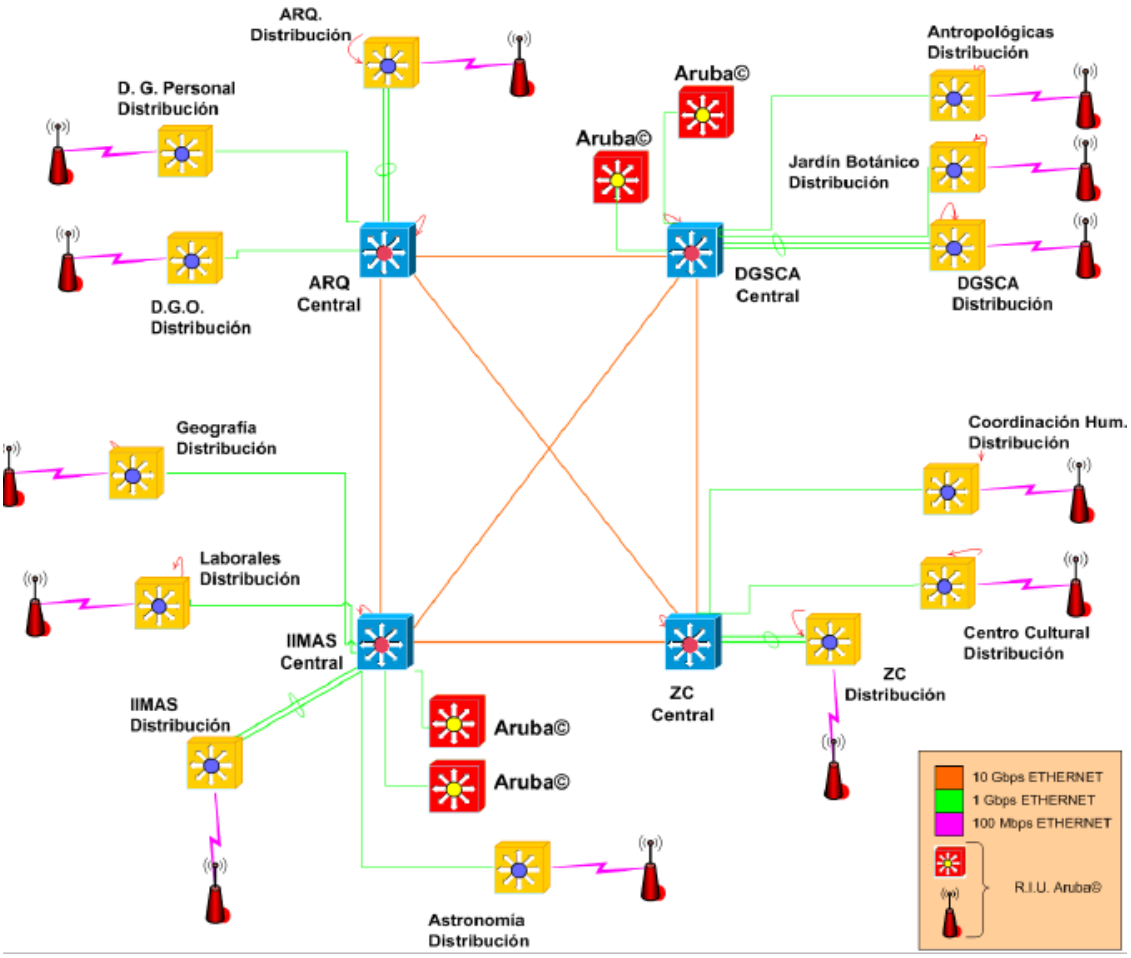



Figura 8.14 Estructura de la RIU

Aruba tiene un soporte un tanto limitado para IPv6, inclusive fue hasta su versión ArubaOS 6.3.1 (enero de 2012) que integró la funcionalidad a sus controladoras para que transmitieran mensajes RA. Después de consultar varias listas de correo realizados por algunos clientes inconformes de Aruba, se pudo conocer que inclusive el habilitar IPv6 ha provocado que la movilidad IPv4 deje de funcionar, por lo tanto esta situación claramente deja en evidencia que la movilidad en capa red para IPv6 aún no ha sido implementada o por lo menos no ha sido puesta a disposición de los clientes de Aruba. Por la inconformidad mostrada por este mal funcionamiento el personal de Aruba se ha comprometido a reparar este fallo dentro de los próximos meses no obstante, tentativamente la implementación de Movilidad IPv6 podría ser dada a conocer hasta la primera mitad del próximo año 2013.

Dada la situación actual de Aruba es claro que MIPv6 tendrá que esperar hasta el próximo año, afortunadamente es muy probable que su solución también permita manejar la movilidad basada en red lo cual constituye un punto a favor que sin duda podrá ser aprovechada al máximo por administradores de red y usuarios. Debido a esta situación de

aquí en adelante únicamente se describirán los cambios necesarios a realizar para tener un acceso inalámbrico a través de IPv6. En lo que respecta al uso de Movilidad IPv6 se necesitará esperar a que la solución sea ofrecida en las siguientes versiones de las controladoras de Aruba porque hasta el momento no existe un comunicado oficial que así lo informe.

En lo que respecta a la RIU, el primer paso que se tendría que dar es contar con el soporte más estable de IPv6, y para ello es necesario llevar a cabo una actualización en todas las controladoras a la versión ArubaOS 6.3.1. Otros de los elementos que habrá que tomar en cuenta es lo siguiente: el acceso a la RIU está basado en el uso de un servidor RADIUS, que junto con una base de datos, hacen posible que un usuario auténtico logre disfrutar del servicio inalámbrico, desafortunadamente la versión actual de dicho servidor no soporta el uso de IPv6 y por ello es necesario actualizarlo a una versión más reciente (Free-RADIUS a partir de su versión 2 ya tiene ese soporte) [64]; esta limitante pone de manifiesto que son varios los elementos que hay que contemplar antes de lograr poder ofrecer IPv6 de manera inalámbrica en la RIU.

Los pasos anteriores suenan sencillos pero en realidad llevan tras de sí un sinfín de consideraciones por ejemplo: claramente tomar una decisión así no es nada fácil sobretodo porque debe existir una necesidad que así lo amerite y todo un proceso para llevarlo a cabo de manera gradual. Si bien es cierto que la transición hacia esta nueva versión de IP es inminente también lo es el hecho de que necesita haber una convivencia gradual de IPv4 e IPv6, sobretodo porque no todos los usuarios tienen consigo teléfonos inteligentes o tabletas que soporten IPv6.

Con base en los elementos antes descritos es claro que será necesario considerar un pequeño escenario piloto donde pueda apreciarse el funcionamiento del acceso inalámbrico a través de IPv6. Podría ser DGTIC la primera dependencia en que fuera posible el ver reflejada esta capacidad porque recientemente se adquirieron varios switches capa 3 que permiten soportar IPv6 de forma nativa; concretamente el Laboratorio de Tecnologías Emergentes de Redes (NETLab [65]) de la DGTIC, sin duda sería uno de los lugares estratégicos que formen parte de esa primera fase, porque este sitio guarda una estrecha relación con el estudio e impulso de IPv6, condición que sin duda podría dar pauta a tener una mejor estimación de su funcionalidad y utilidad.

La decisión de brindar acceso inalámbrico por IPv6 e IPv4 a través de la RIU en el resto de las dependencias de la UNAM seguramente dependerá en gran medida de la experiencia y resultados obtenidos en DGTIC, datos que en definitiva llegarán a constituir una base más solida de una futura propuesta.

# Conclusiones

Gracias al estudio realizado en esta tesis en torno a la Movilidad IPv6 (MIPv6) no sólo fue posible conocer el funcionamiento de dicho protocolo y sus características más representativas, sino que además se pudo contemplar su uso en simulaciones y ambientes operativos. Desafortunadamente, no se pudo llevar a cabo la comparación con su respectiva versión en IPv4 (MIPv4) porque no se contó con el equipo y software necesario no obstante, los resultados obtenidos permitieron cumplir con los objetivos planteados en un inicio.

Para las pruebas de MIPv6 realizadas con el simulador OMNeT++ habrá que tener presente que trabajar bajo dichas condiciones en determinados momentos llega a distar en cierta medida de la experiencia observada en ambientes reales. Para los diferentes tipos de tráfico transferidos en general las principales conductas mostradas en las simulaciones fueron:

- Durante la interrupción de la transmisión de tráfico ICMPv6 y UDP entre el MN y CN existió cierta pérdida de información, conducta que no se presentó en TCP por ser un protocolo confiable.

- Debido a que la capa de transporte no está consciente de lo que ocurre en la capa de red, existió una complejidad adicional para determinar los efectos que produce MIPv6 en el tráfico TCP; propiamente en las comunicaciones no es posible distinguirlos de los efectos ocasionados por el control de flujo y congestión durante el handover.

- Mientras más rápido se desplazaba el MN, mayor fue la pérdida de paquetes durante el handover, este resultado se asocia con la detección de movimiento porque este proceso aún no es lo suficientemente rápido e involucra distintos mecanismos, los cuales contribuyen a que el MN demore su asociación en una red foránea.

Por su parte, el escenario construido en la maqueta de pruebas permitió que se llegará a las siguientes aseveraciones:

- El emplear MIPv6 para manejar la movilidad en la capa de red no es la mejor selección porque cada nodo en la red debe contar con dicho soporte, por lo tanto es preferible delegar dicha responsabilidad a la red, de manera que es más recomendable hacer uso de alguna de las mejoras en Movilidad IP que existen

como lo es el caso de Proxy MIPv6, ya que además de brindar la característica antes mencionada también puede funcionar en redes IPv4.

- A pesar de que el uso de la movilidad en la capa de red debería ser transparente para las capas superiores, existen todavía algunas diferencias en las transmisiones de acuerdo al tipo de tráfico que se envía o recibe. Esta situación se observó por ejemplo al regresar el MN a su red local cuando ciertas aplicaciones con soporte IPv6 dejaban de transmitir información, tal como ocurrió con Filezilla para FTP.

- El soporte actual de MIPv6 va en crecimiento, pero lamentablemente hoy en día no está preparado para satisfacer las más demandantes expectativas de los usuarios. Este aspecto se pudo corroborar al hacer uso de MIPv6-tester, aplicación mediante la cual se obtuvo el tiempo estimado que transcurrió durante el handover que fue de 8.947[s]; aunque este lapso es aceptable para algunos servicios lo cierto es, que es inaceptable para aplicaciones basadas en tiempo real o sensitivas al retraso.

En lo que respecta a la propuesta de uso de MIPv6 en RedUNAM, se centró la atención en la Red Inalámbrica Universitaria (RIU), desafortunadamente en la actualidad las controladoras de dicha red pertenecen a equipos de la marca Aruba Networks y éstos aún no tienen soporte de MIPv6; por lo tanto, los esfuerzos por el momento sólo se concentran en proponer algunas etapas mediante las cuales la RIU podrá brindar un acceso inalámbrico no sólo por IPv4 sino también por IPv6:

- Primera etapa: comprende el periodo de tiempo necesario para evaluar los requisitos de la RIU a fin de tener el soporte necesario para brindar IPv6 de forma inalámbrica. Esta etapa necesitará realizar la actualización de las controladoras de red a la versión ArubaOS 6.3.1, además se requerirá migrar el servidor RADIUS a una versión más reciente que cuente con el soporte de IPv6, por ejemplo FreeRadius 2.

- Segunda etapa: incluye la designación de un sitio de pruebas piloto, se propone al laboratorio NETLab, localizado en la DGTIC, como un lugar estratégico para las pruebas del uso de MIPv6, porque es el lugar en la UNAM donde se ha estudiado a fondo IPv6.

- Tercera etapa: contempla el análisis de los resultados que se lleguen a obtener en el uso del acceso inalámbrico mediante IPv6 en el NETLab. A través de estos resultados es que se conocerá la viabilidad de su implementación a una mayor escala y posiblemente de pie a la selección de nuevos sitios de uso.

Hasta el día de hoy, al hablar de la implementación de MIPv6 se llegan a relacionar ciertas palabras en relación a su estado, tales como: infante, inmaduro, novicio, etc., sin embargo, también es posible asociar elementos como crecimiento, avances, ascenso, y ciertamente aún tiene la oportunidad de dar grandes saltos que lo lleven al éxito, porque actualmente no es capaz de satisfacer las más demandantes expectativas de los usuarios.

Las implementaciones actuales de MIPv6 a pesar de tener ya varios años en desarrollo aún no cuentan con el suficiente soporte, e inclusive características adicionales que se han ido añadiendo a algunas de ellas complican la resolución de problemas porque no se cuenta con suficiente información al respecto. Por otra parte, su integración con IPSec ha dificultado su implementación por las grandes dificultades que se llegan a formar, por lo que habrá que esperar que las nuevas propuestas de seguridad mejoren esta situación y reviertan esa desfavorable condición

Es indudable que el estado actual de MIPv6 dependerá en gran medida de los avances que se logren obtener en PMIPv6, ya que hasta el momento ésta representa la única propuesta que podría satisfacer los requerimientos de los usuarios más exigentes, aún con ello no se debe pasar por alto que también será necesario que surjan otras alternativas de seguridad que brinden un nivel aceptable de protección, ya que este aspecto se ha convertido en un elemento crítico en las comunicaciones, no sólo móviles.

Ante todo, agradezco a mis compañeros del laboratorio de NETLab por el apoyo brindado durante las pruebas, y al Ingeniero Azael por el préstamo del equipo, ya que sin ellos no habría podido terminar con las pruebas llevadas a cabo y con este trabajo de tesis.

# Referencias


[1] Paulkner Christina, Ciccarelli Patrick, 2004, “Network Foundations”, San Francisco, Sybex.

[2] Curricula Cisco CCNA Exploration v4.

[3] Mobility in Wireless Networks, International Conference on Communication Technology.

[4] Handoff in Wireless Networks, Workshop on Future Wireless Systems.

[5] R. Stewart, Ed., “Stream Control Transmission Protocol”, RFC 4960. Septiembre 2007. <http:www.ietf.org/rfc/rfc4960.txt>

[6] A. Ford, C. Raiciu, M. Handley, S. Barre, J. Iyengar, “Architectural Guidelines for Multipath TCP Development”. Marzo 2011. <http:www.ietf.org/rfc/rfc6182.txt>

[7] MSOCKS: An Architecture for Transport Layer Mobility, Wireless IEEE Internation Symposium on Systems

[8] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “SIP: Session Initiation Protocol”. Junio 2002. <http:www.ietf.org/rfc/rfc3261.txt>

[9] Visual Networking Index, Cisco Systems. http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html

[10] IBSG de Cisco, http://www.cisco.com/web/about/ac79/index.html

[11] Instituto de Ingenieros Eléctricos y Electrónicos: http://www.ieee.org/index.html

[12] ARIN Regional Internet Registrie, https://www.arin.net/knowledge/rirs.html

[13] Fuerza de Trabajo de Internet, http://www.ipv6tf.org/

[14] Hagen Silvia, 2002, “IPv6 Essentials”, Beijing O´Really.

[15] Iljitsch van Beijnum, 2006, “Running IPv6”. California, Apress.

[16] S. Thomson, T. Narten, T. Jinmei , “IPv6 Stateless Address Autoconfiguration”, RFC 4862, Septiembre 2007. <http:www.ietf.org/rfc/rfc4862.txt>

[17] T. Narten, E. Nordmark, W. Simpson, H. Soliman, “Neighbor Discovery for IP version 6 (IPv6)”, RFC 4861, Septiembre 2007. <http:www.ietf.org/rfc/rfc4861.txt>

[18] A. Conta, S. Deering, M. Gupta, Ed., “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, RFC 4443, Marzo 2006. <http:www.ietf.org/rfc/rfc4443.txt>

[19] J. Manner, Ed., M. Kojo, Ed., “Mobility Related Terminology”, RFC 3753, Junio 2004. <http:www.ietf.org/rfc/rfc3753.txt>

[20] C. Perkins, Ed., “IP Mobility Support for IPv4”, RFC 5944, Noviembre 2010. <http:www.ietf.org/rfc/rfc5944.txt>

[21] C. Perkins, Ed., D. Johnson, J. Arkko, “Mobility Support in IPv6“, RFC 6275, Julio 2011. <http:www.ietf.org/rfc/rfc6275.txt>

[22] Vyncke Eric, Hogg Scott, 2009, “IPv6 Security”, Indianapolis, Cisco Press.

[23] A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, “Authentication Protocol for Mobile IPv6”, RFC 4285, Enero 2006. <http:www.ietf.org/rfc/rfc4285.txt>

[24] A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, “Mobile Node Identifier Option for Mobile IPv6 (MIPv6)”, RFC 4283, Noviembre 2005. <http:www.ietf.org/rfc/rfc4283.txt>

[25] B. Aboba, M. Beadles, J. Arkko, P. Eronen, “The Network Access Identifier”, RFC 4282, Diciembre 2005. <http:www.ietf.org/rfc/rfc4282.txt>

[26] S. Kent, “Security Architecture for the Internet Protocol”, RFC 4301, Diciembre 2005. <http:www.ietf.org/rfc/rfc4301.txt>

[27] S. Kent, “IP Encapsulating Security Payload (ESP)”, RFC 4303, Diciembre 2005. <http:www.ietf.org/rfc/rfc4303.txt>

[28] S. Kent, “IP Authentication Header”, RFC 4302, Diciembre 2005. <http:www.ietf.org/rfc/rfc4302.txt>

[29] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, “Internet Key Exchange Protocol Version 2 (IKEv2)”, RFC 5996, Septiembre 2010. <http:www.ietf.org/rfc/rfc5996.txt>

[30] R. Koodli, Ed., “Mobile IPv6 Fast Handovers”, RFC 5568, Julio 2009. <http:www.ietf.org/rfc/rfc5568.txt>

[31] H. Soliman, C. Castelluccia, K. ElMalki, L. Bellier, “Hierarchical Mobile IPv6 (HMIPv6) Mobility Management”, RFC 5380, Octubre 2008. <http:www.ietf.org/rfc/rfc5380.txt>

[32] S. Gundavelli, Ed., V. Devarapalli, K. Chowdhury, B. Patil, “Proxy Mobile IPv6”, RFC 5213. <http:www.ietf.org/rfc/rfc5213.txt>

[33] R. Wakikawa, S. Gundavelli, “IPv4 Support for Proxy Mobile IPv6”, RFC 5844, Mayo 2010. <http:www.ietf.org/rfc/rfc5844.txt>

[34] H. Soliman, Ed., “Mobile IPv6 Support for Dual Stack Hosts and Routers “, RFC 5555, Junio 2009. <http:www.ietf.org/rfc/rfc5555.txt>

[35] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, “Network Mobility (NEMO) Basic Support Protocol”, RFC 3963, Enero 2005. <http:www.ietf.org/rfc/rfc3963.txt>

[36] Telecomunicaciones Móviles Internacionales, http://www.itu.int/ITU-R/

[37] Proyecto Asociación de Tercera Generación (3GPP), http://www.3gpp.org/

[38] Proyecto 2 de Asociación de Tercera Generación (3GPP2), http://www.3gpp.org/

[39] Sultana Shabnamm, Olsson, Magnus 2009, “SAE and the Evolved Packet Core”, Great Britain, Elseiver.

[40] Adibi Sasan, Mobasher Amin, 2010, “Fourth Generation Wireless Networks”, New York, Information Science Reference

[41] J. Korhonen, Ed., J. Bournelle, K. Chowdhury, A. Muhanna, U. Meyer, “Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server”, RFC 5779, Febrero 2010. <http:www.ietf.org/rfc/rfc5779.txt>

[42] M. Liebsch, Ed., A. Muhanna, O. Blume, “Transient Binding for Proxy Mobile IPv6”, RFC 6058, Marzo 2011. <http:www.ietf.org/rfc/rfc6058.txt>

[43] G. Keeni, K. Koide, S. Gundavelli, R. Wakikawa, “Proxy Mobile IPv6 Management Information Base”, RFC 6475, Mayo 2012. <http:www.ietf.org/rfc/rfc6475.txt>

[44] F. Xia, B. Sarikaya, J. Korhonen, Ed., S. Gundavelli, D. Damic, “RADIUS Support for Proxy Mobile IPv6”, RFC 6572, Junio 2012. <http:www.ietf.org/rfc/rfc6572.txt>

[45] S. Krishnan, R. Koodli, P. Loureiro, Q. Wu, A. Dutta, “Localized Routing for Proxy Mobile IPv6”, RFC 6705, Septiembre 2012. <http:www.ietf.org/rfc/rfc6705.txt>

[46] S. Gundavelli, Ed., J. Korhonen, Ed., M. Grayson, K. Leung, R. Pazhyannur, “Access Network Identifier (ANI) Option for Proxy Mobile IPv6”, Octubre 2012. <http:www.ietf.org/rfc/rfc6757.txt>

[47] S. Gundavelli , “Applicability of Proxy Mobile IPv6 Protocol for WLAN Access Networks”, draft gundavelli-netext-pmipv6-wlan-applicability-04, Octubre 2012

[48] M. Liebsch, P. Seite, H. Yokota, J. Korhonen, S. Gundavelli , “Quality of Service Option for Proxy Mobile IPv6”, draft liebsch-netext-pmip6-qos-01, Octubre 2012

[49] Proxy Mobile IPv6 Extensions to Support Flow Mobility, “Proxy Mobile IPv6 Extensions to Support Flow Mobility”, draft-ietf-netext-pmipv6-flowmob-05, Octubre 2012

[50] A. Petrescu, C. Janneteau, “Network Mobility with Proxy Mobile IPv6”, draft-petrescu-netext-pmip-nemo-01, Julio 2012

[51] Telecomunicaciones Móviles Internacionales avanzadas, http://www.itu.int/ITU-R/

[52] Asociación de Proveedores móviles Globales, http://www.gsacom.com/

[53] Foro WiMAX, http://www.wimaxforum.org/

[54] Ratasuk Rapeepat, Gosh Amitabha 2011, “Essentials of LTE and LTE-A”, Cambridge University Press

[55] Taha Adb-Elhamid, Najah Abu Ali 2012, “LTE, LTE-Advanced and WiMAX”, India, Wiley

[56] IEEE 802.21, http://www.ieee802.org/21/

[57] Redes de Próxima Generación, http://www.ngn-enabled.com

[58] Redes de Próxima Generación, http://www.itu.int/en/ITU-T/gsi/ngn/Pages/default.aspx

[59] Proyecto KAME, http://www.kame.net/

[60] Proyecto UMIP, http://www.umip.org/

[61] Demonio Anuncio de Ruteador, http://www.litech.org/radvd/

[62] Librería de simulación OMNeT++, http://www.omnetpp.org/

[63] Modelo de simulación xMIPv6, https://github.com/zarrar/xMIPv6

[64] Cruz Placido Carolina Geraldin, Jaime López Cisneros, “Implementación de IPv6 en la Red Inalámbrica Universitaria”, 2012.

[65] Laboratorio de Tecnologías Emergentes de Redes, http:// www.netlab.unam.mx

# Anexos

## *ANEXO A: Resultados tráfico ICMPv6 con diferentes velocidades del MN*

A continuación se presentan las gráficas obtenidas para el tráfico ICMPv6: Retardo de ida y vuelta.

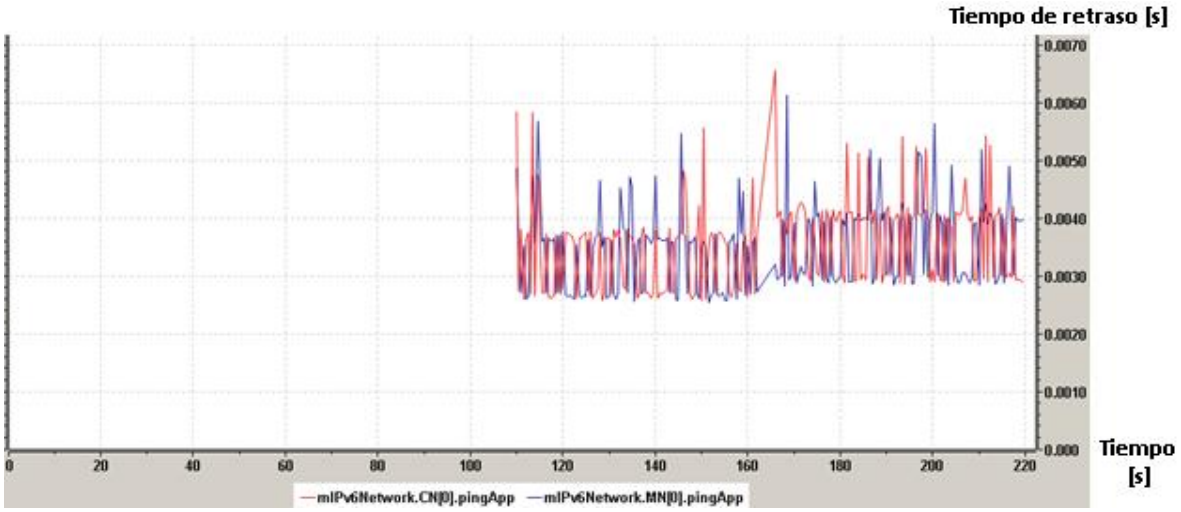



Figura I. ICMPv6, retardo de ida y vuelta (2[m/s])

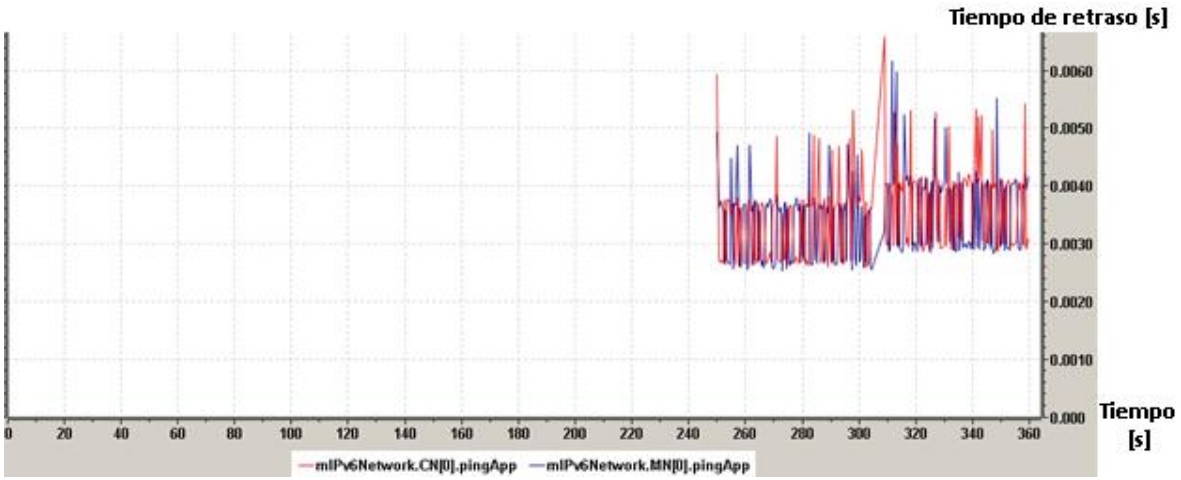



Figura II. ICMPv6, retardo de ida y vuelta (5[m/s])

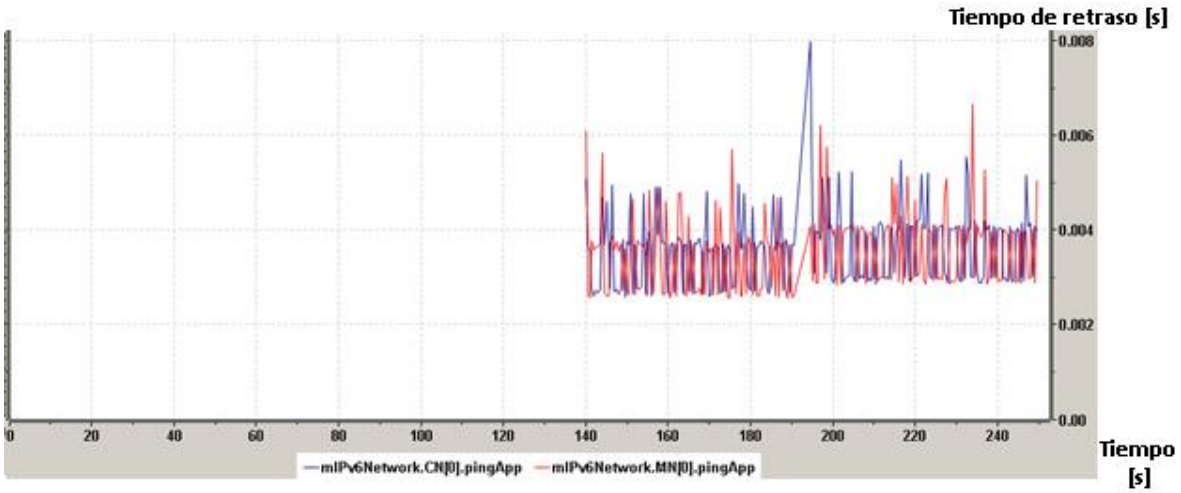



Figura III. ICMPv6, retardo de ida y vuelta (8[m/s])

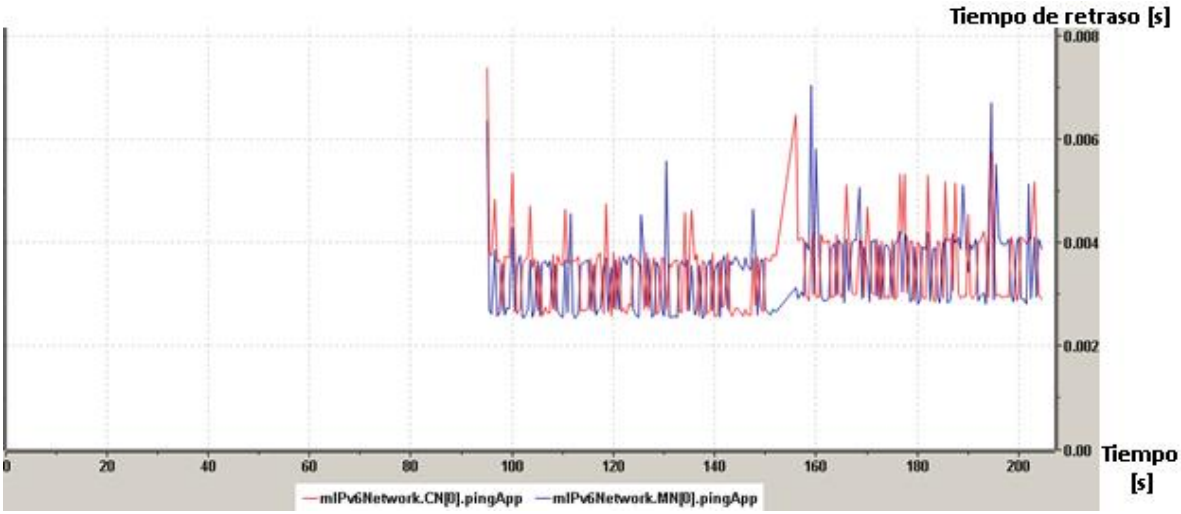



Figura IV. ICMPv6, retardo de ida y vuelta (10[m/s])

# *ANEXO B: Resultados tráfico UDP con diferentes velocidades del MN*

Enseguida se observa el comportamiento obtenido en el tráfico UDP a diferentes velocidades del MN.

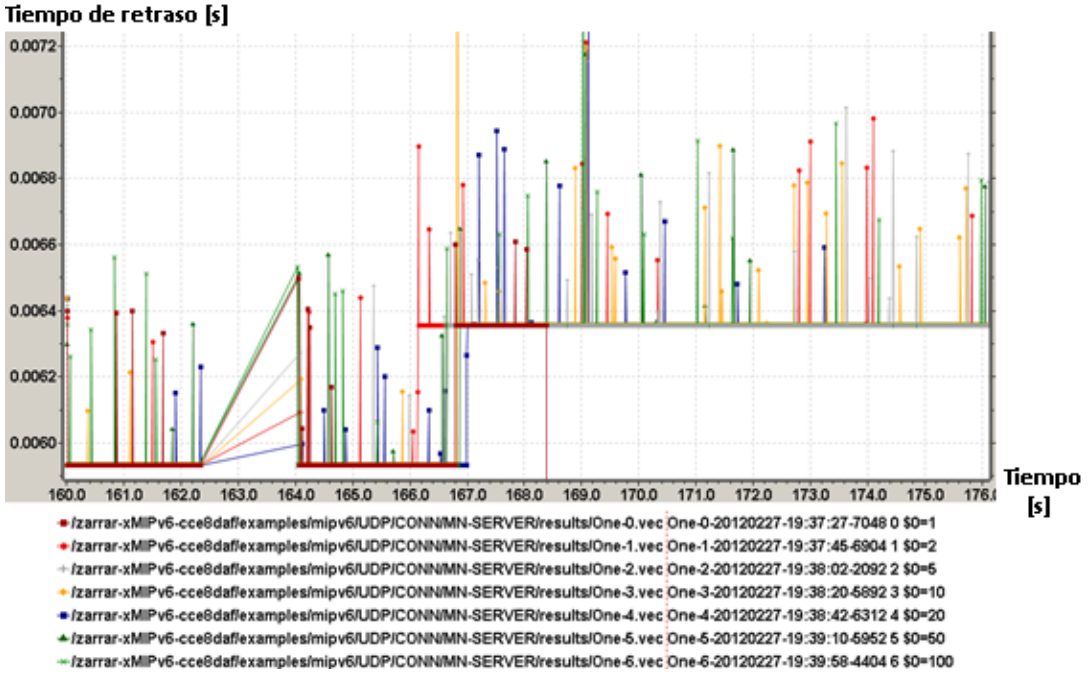



Figura V. Tráfico UDP (2[m/s])

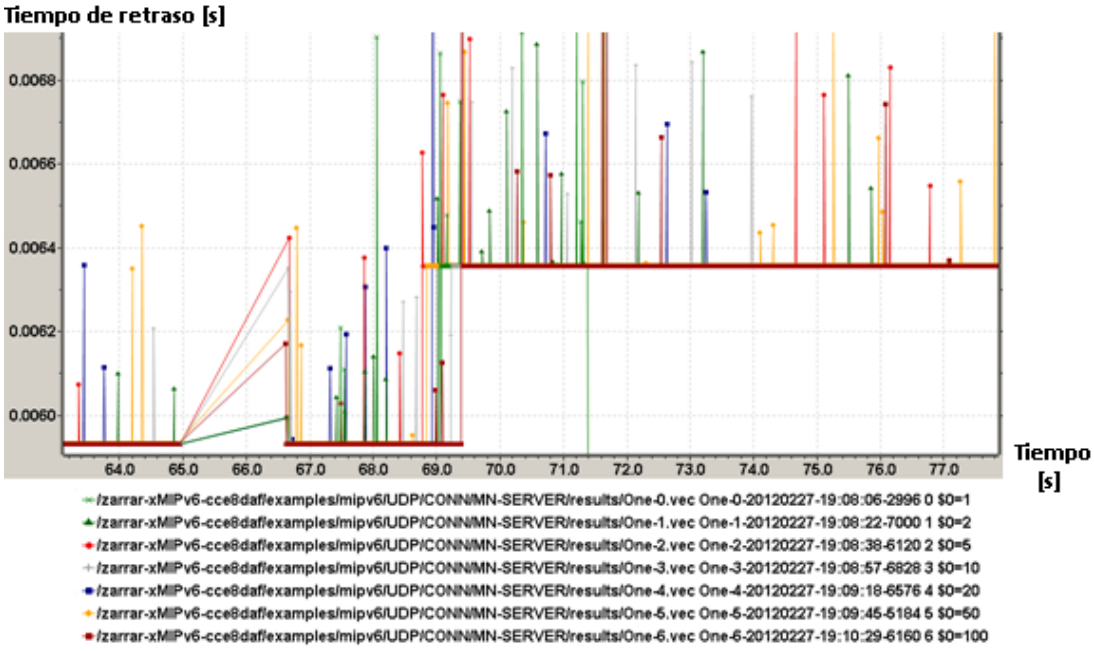



Figura VI. Tráfico UDP (5[m/s])

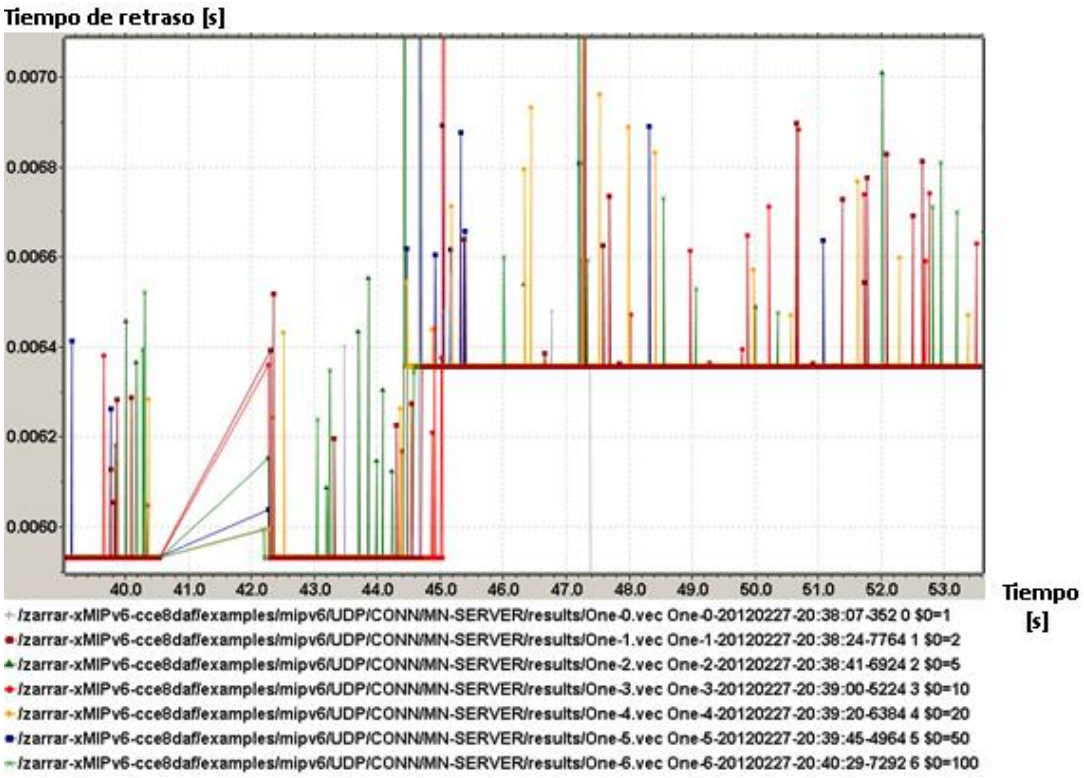



Figura VII. Tráfico UDP (8[m/s])

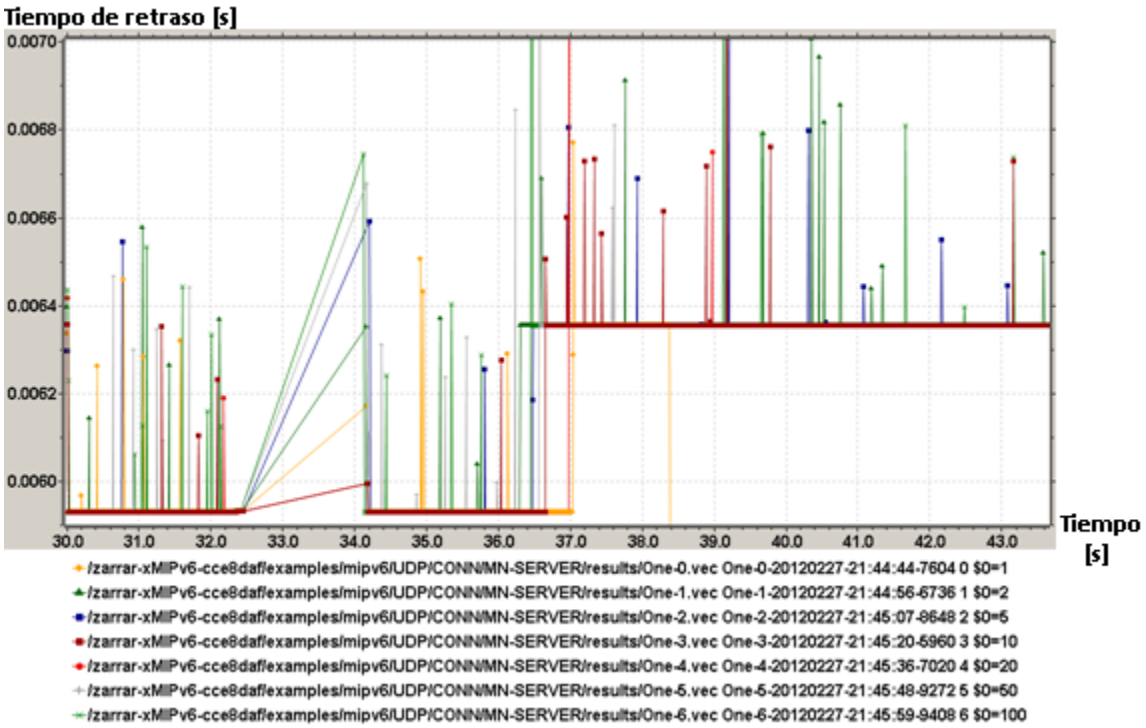
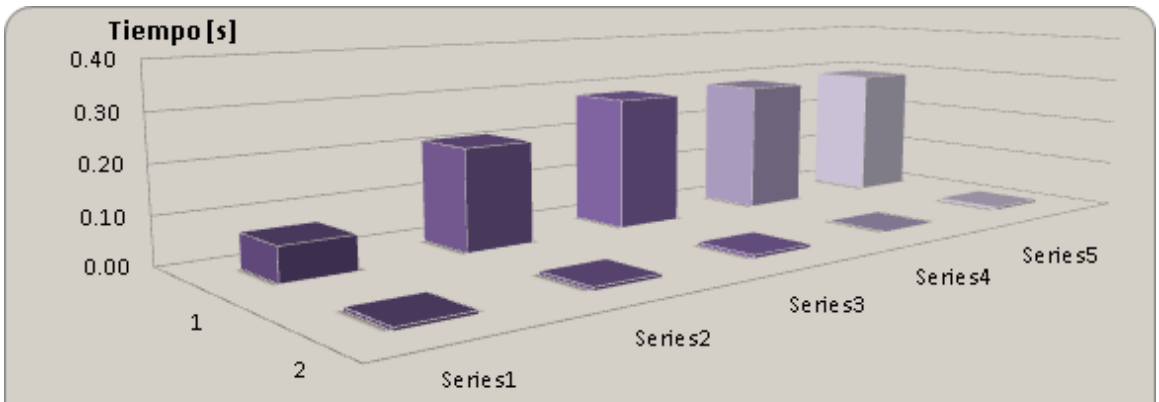



Figura VIII. Tráfico UDP (10[m/s])

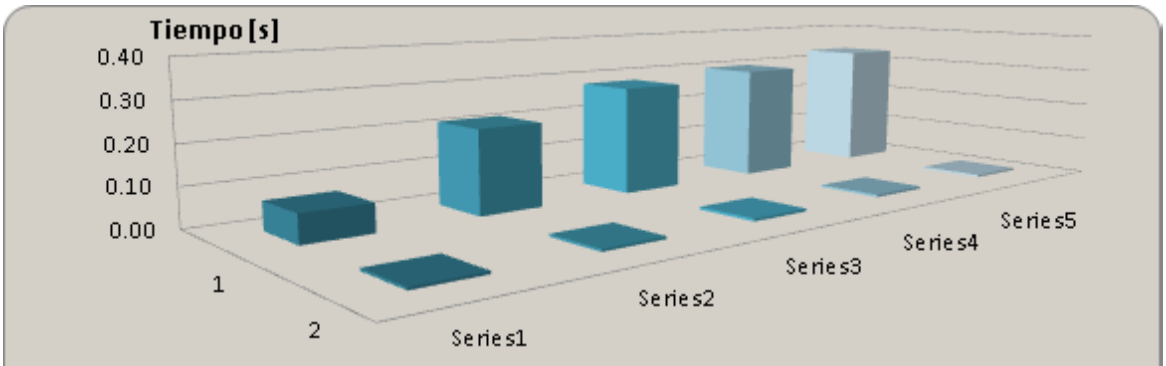
# *ANEXO C: Resultados tráfico TCP con diferentes velocidades del MN*

Las gráficas que representan el comportamiento del tráfico TCP a las diferentes velocidades del MN son las siguientes:



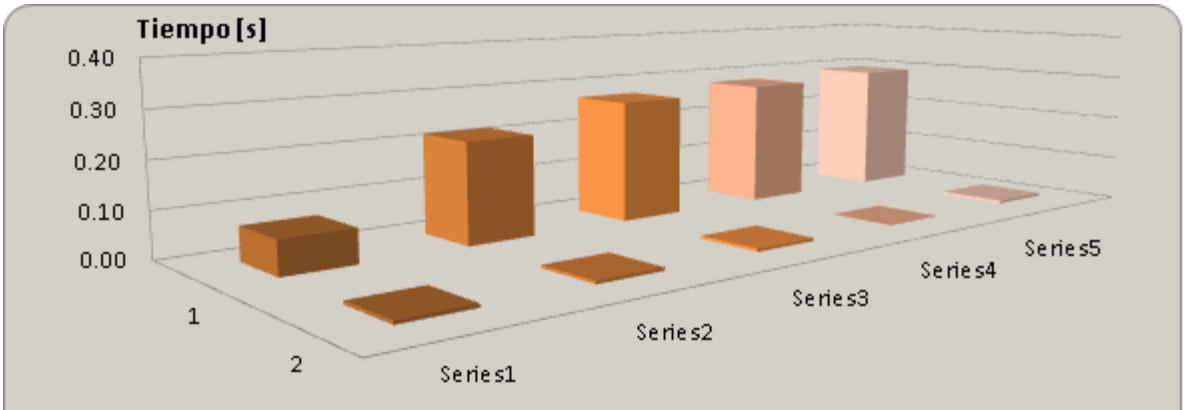

| | 1 Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0711587266 | 0.0064404102 | 6500 |
| Series2 | 0.2132039998 | 0.0067782147 | 20000 |
| Series3 | 0.2819496761 | 0.0069663114 | 35000 |
| Series4 | 0.2836530157 | 0.0008769171 | 50000 |
| Series5 | 0.2883895304 | 0.0064204200 | 65000 |

Figura IX. TCP, Tiempos de retraso, MN servidor (2[m/s])



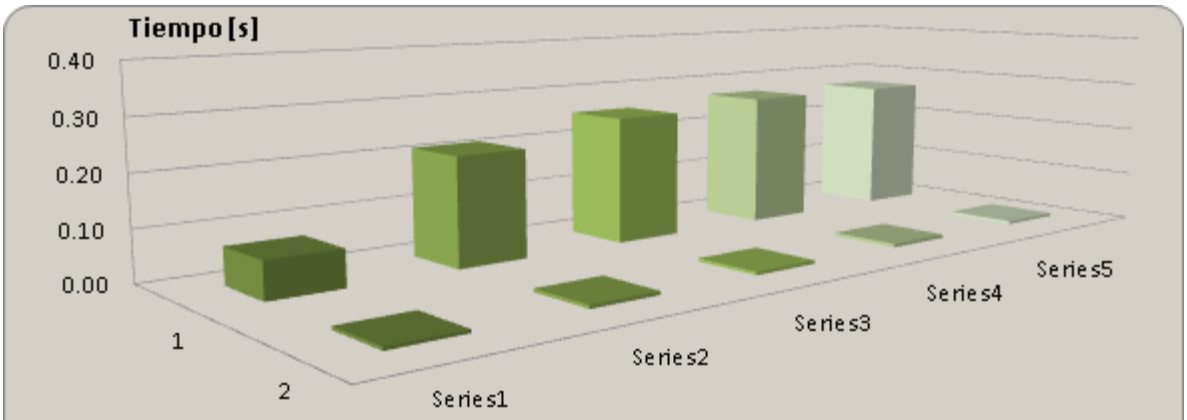

| | 1 Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0714567018 | 0.0064405611 | 6500 |
| Series2 | 0.2144011970 | 0.0064806523 | 20000 |
| Series3 | 0.2810532950 | 0.0069840999 | 35000 |
| Series4 | 0.2997408121 | 0.0065006747 | 50000 |
| Series5 | 0.3325822284 | 0.0064205892 | 65000 |

Figura X. TCP, Tiempos de retraso, MN servidor (5[m/s])




| | 1 Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0730580845 | 0.0074663764 | 6500 |
| Series2 | 0.2184181231 | 0.0064405686 | 20000 |
| Series3 | 0.2691781983 | 0.0065004300 | 35000 |
| Series4 | 0.2796944203 | 0.0009163581 | 50000 |
| Series5 | 0.2918072613 | 0.0068174512 | 65000 |

Figura XI. TCP, Tiempos de retraso, MN servidor (8[m/s])




| | 1 Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0718619582 | 0.0065203185 | 6500 |
| Series2 | 0.2136470578 | 0.0067777467 | 2000 |
| Series3 | 0.2545714232 | 0.0064203211 | 35000 |
| Series4 | 0.2686675524 | 0.0069182569 | 50000 |
| Series5 | 0.2690665240 | 0.0064005242 | 65000 |

Figura XII. TCP, Tiempos de retraso, MN servidor (10[m/s])

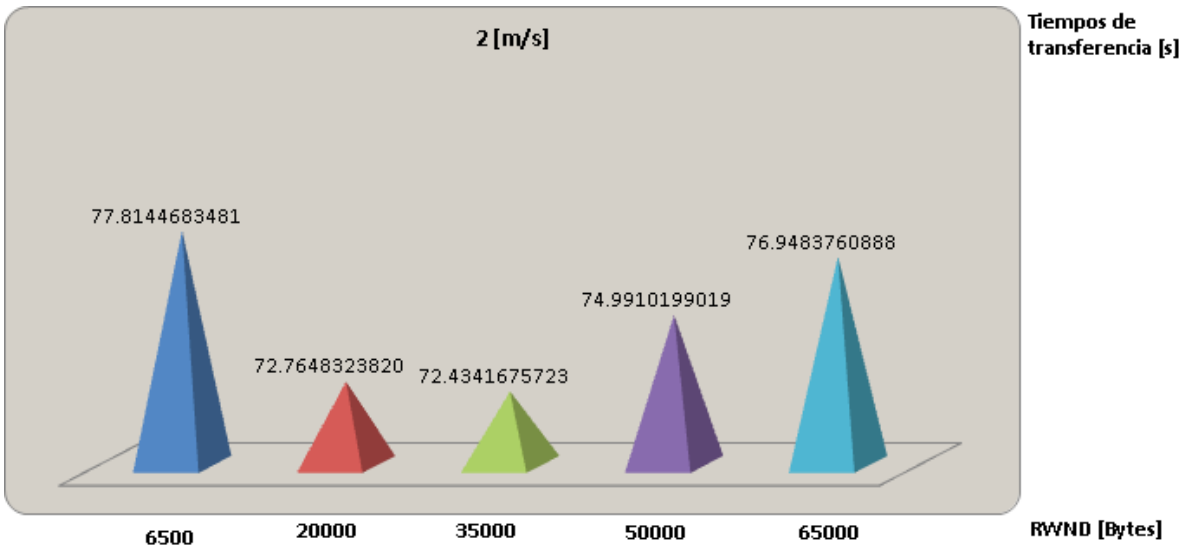



Figura XIII. TCP, Tiempos totales de transferencia, MN servidor (2[m/s])

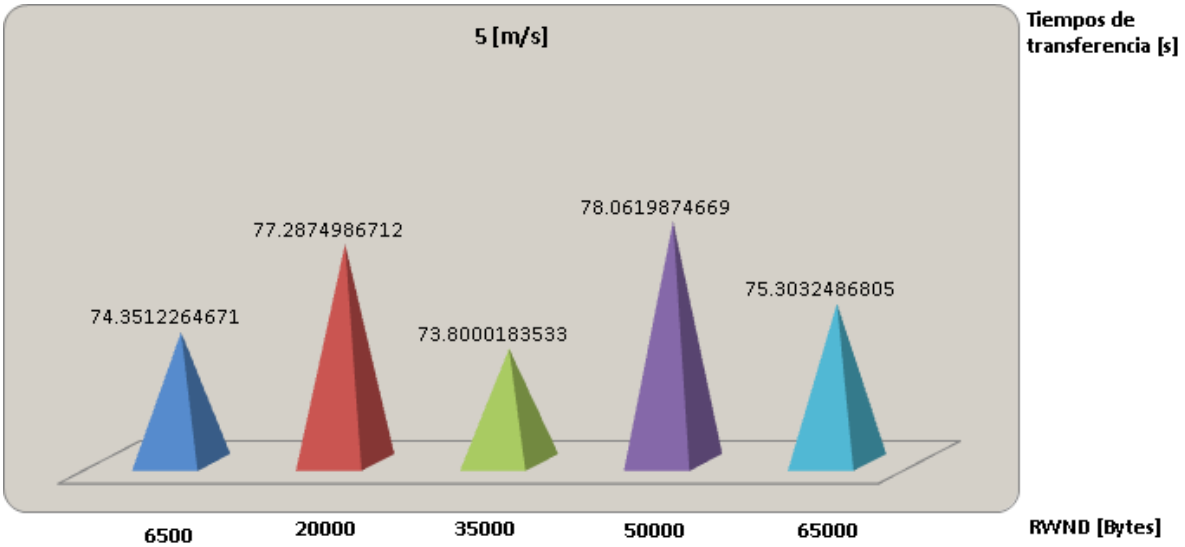



Figura XIV. TCP, Tiempos totales de transferencia, MN servidor (5[m/s])

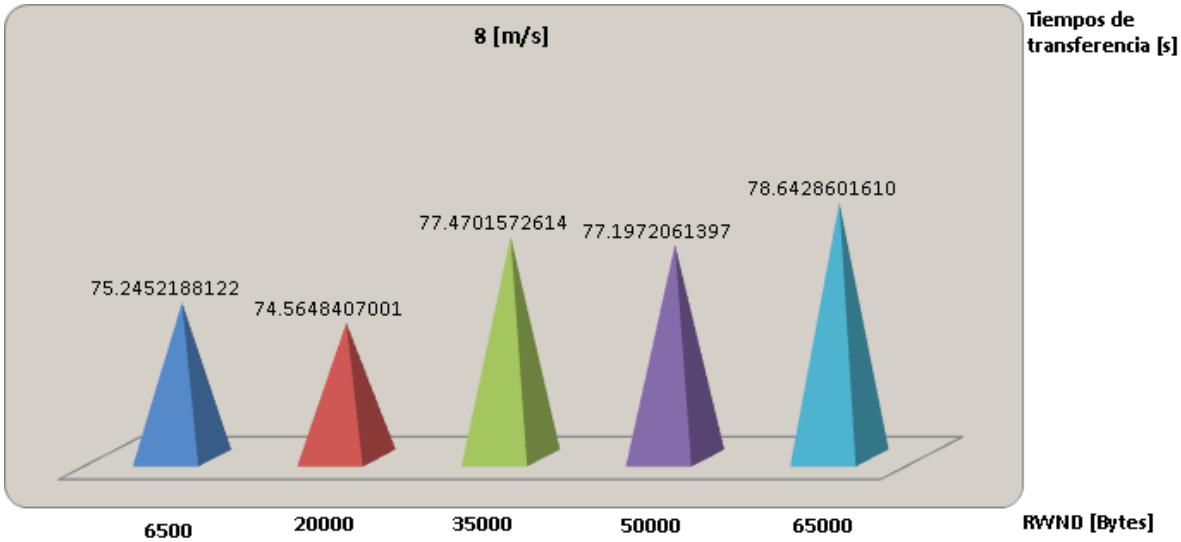



Figura XV. TCP, Tiempos totales de transferencia, MN servidor (8[m/s])

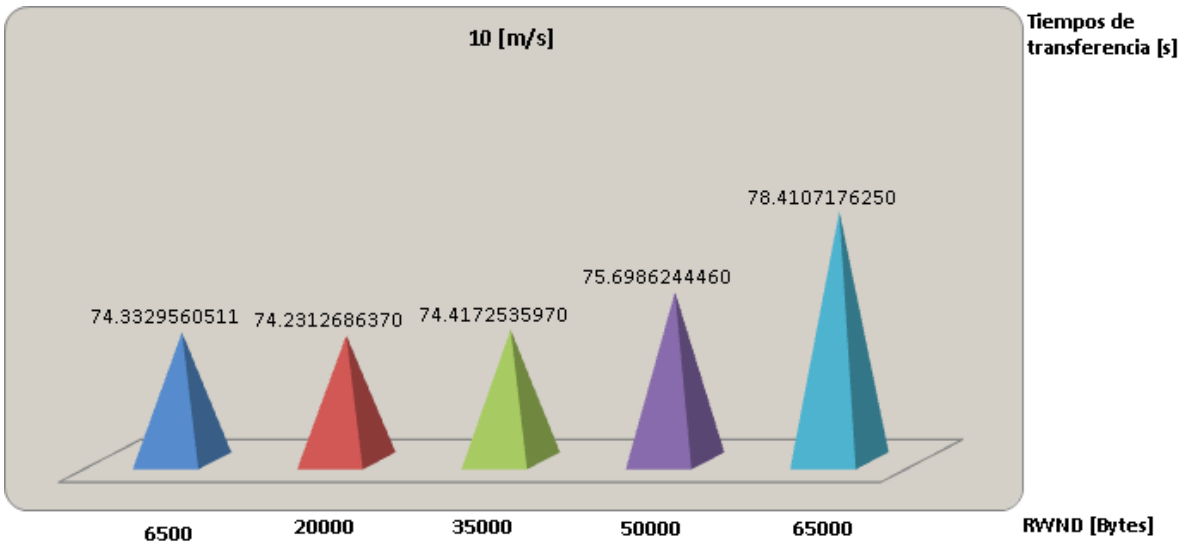
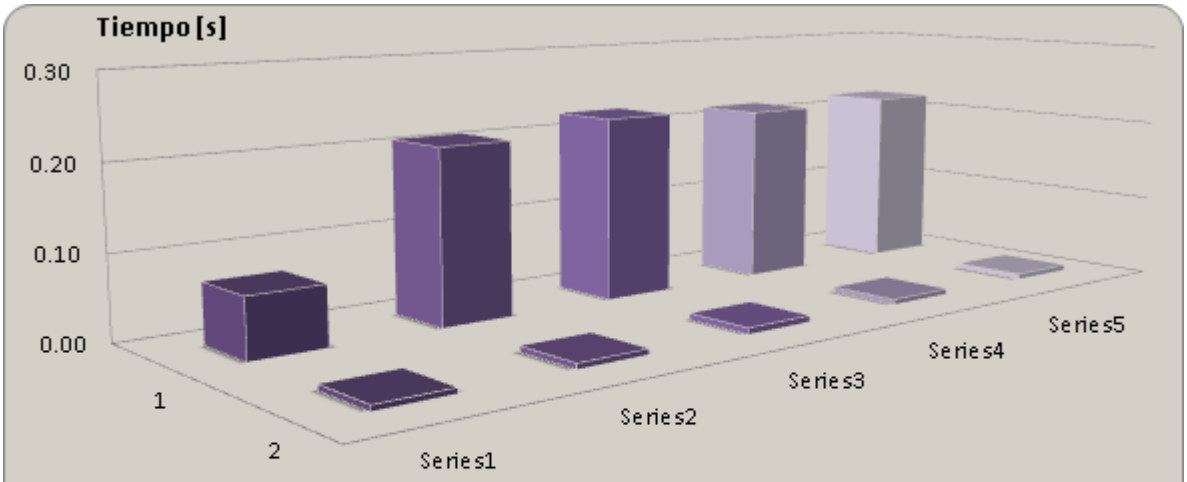
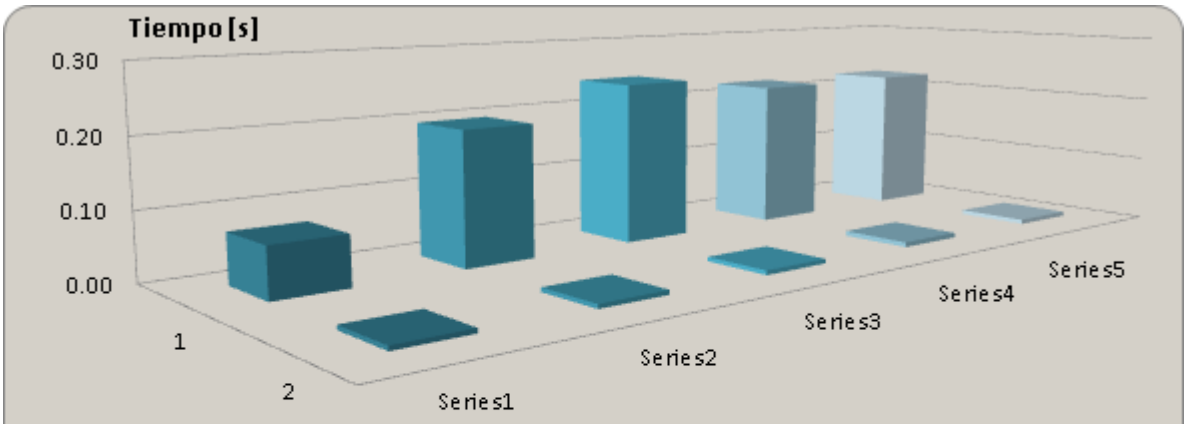



Figura XVI. TCP, Tiempos totales de transferencia, MN servidor (10[m/s])



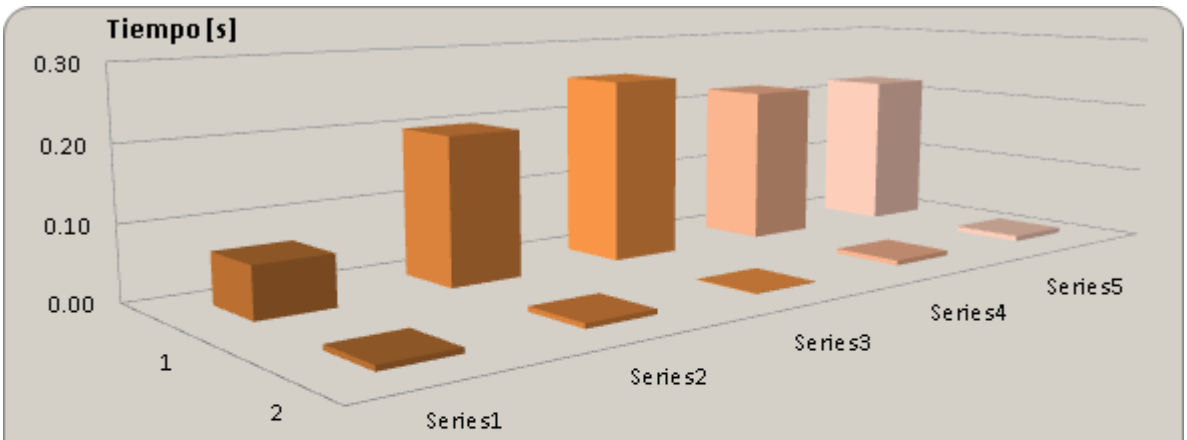

| | 1 Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0708380591 | 0.0065104539 | 6500 |
| Series2 | 0.2078940473 | 0.0067782305 | 20000 |
| Series3 | 0.2228129298 | 0.0075898606 | 35000 |
| Series4 | 0.2153547701 | 0.0064904481 | 50000 |
| Series5 | 0.2183452670 | 0.0067780856 | 65000 |

Figura XVII. TCP, Tiempos de retraso, MN cliente (2[m/s])



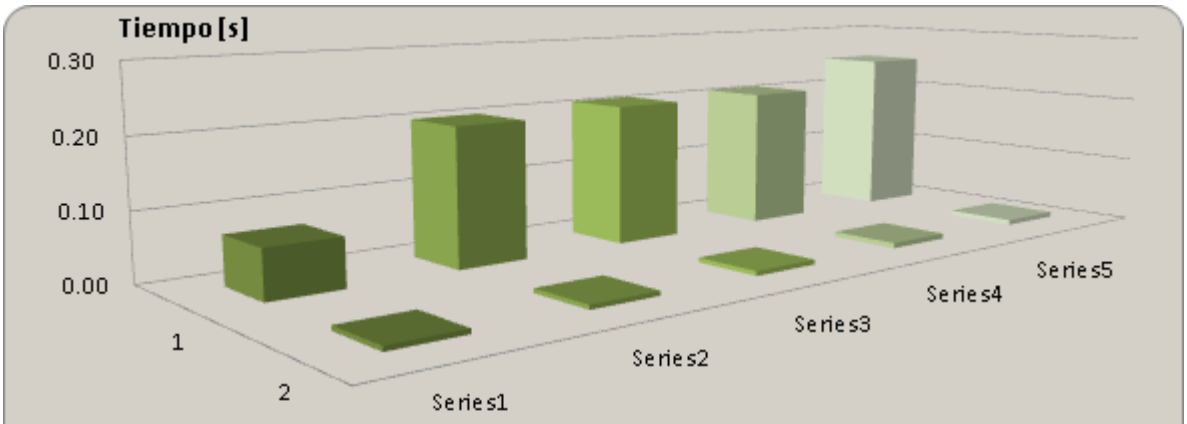

| | 1 Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0734857602 | 0.0064505487 | 6500 |
| Series2 | 0.1970683249 | 0.0064705549 | 20000 |
| Series3 | 0.2421301917 | 0.0064305580 | 35000 |
| Series4 | 0.2200734101 | 0.0072063918 | 50000 |
| Series5 | 0.2217080933 | 0.0064906206 | 65000 |

Figura XVIII. TCP, Tiempos de retraso, MN cliente (5[m/s])




| | 1 ´Máximo | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0680042157 | 0.0071064160 | 6500 |
| Series2 | 0.1991099635 | 0.0068176828 | 20000 |
| Series3 | 0.2528521688 | 0.0011161738 | 35000 |
| Series4 | 0.2202410892 | 0.0068576828 | 50000 |
| Series5 | 0.2201923300 | 0.0074239466 | 65000 |

Figura XIX. TCP, Tiempos de retraso, MN cliente (8[m/s])




| | 1 Máxino | 2 Mínimo | RWND [Bytes] |
|---|---|---|---|
| Series1 | 0.0708710005 | 0.0068382041 | 6500 |
| Series2 | 0.2022175026 | 0.0065104880 | 20000 |
| Series3 | 0.2092296332 | 0.0068582041 | 35000 |
| Series4 | 0.2094622864 | 0.0076899950 | 50000 |
| Series5 | 0.2503164576 | 0.0076241611 | 65000 |

Figura XX. TCP, Tiempos de retraso, MN cliente (10[m/s])

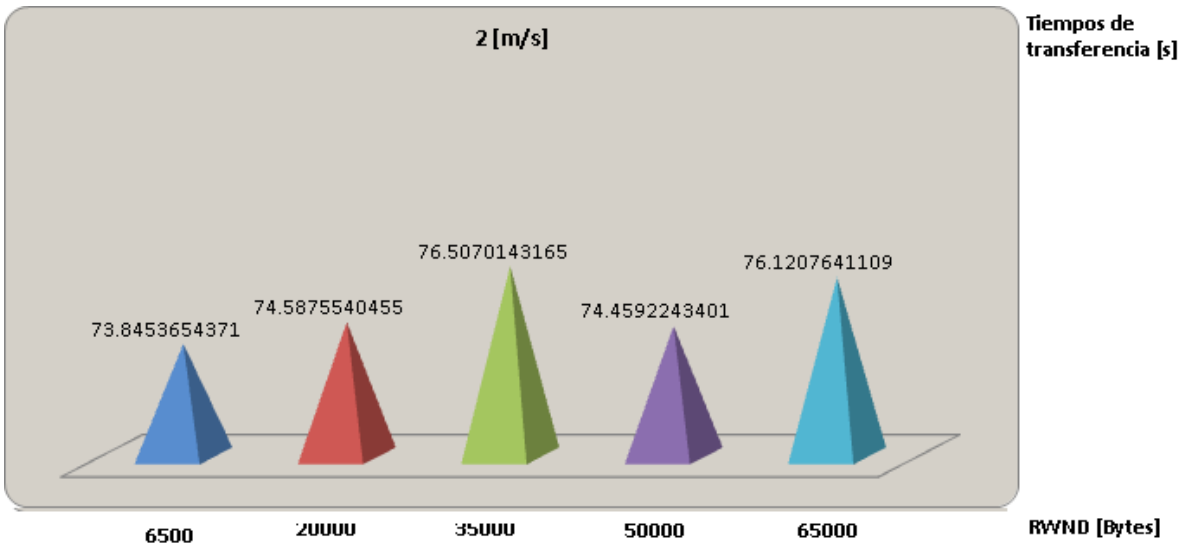



Figura XXI. TCP, Tiempos totales de transferencia, MN cliente (2[m/s])

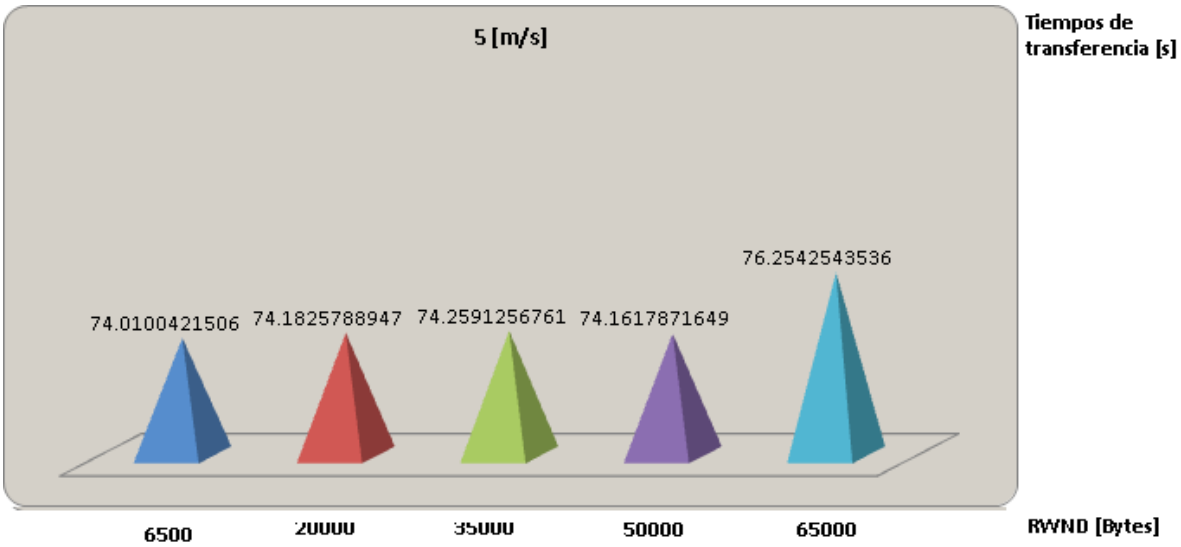



Figura XXII. TCP, Tiempos totales de transferencia, MN cliente (5[m/s])

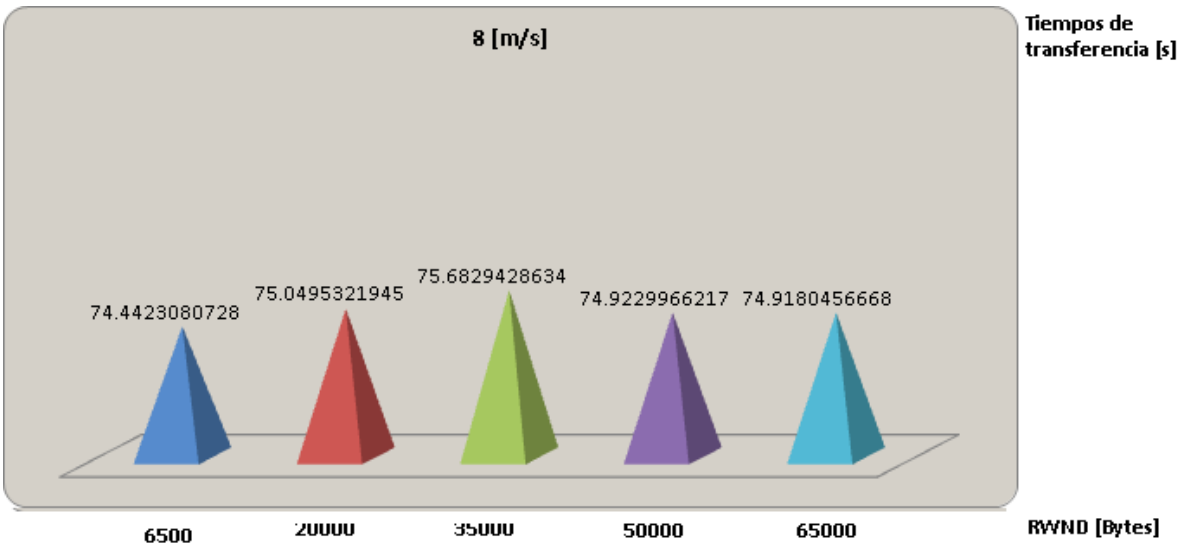



Figura XXIII. TCP, Tiempos totales de transferencia, MN cliente (8[m/s])

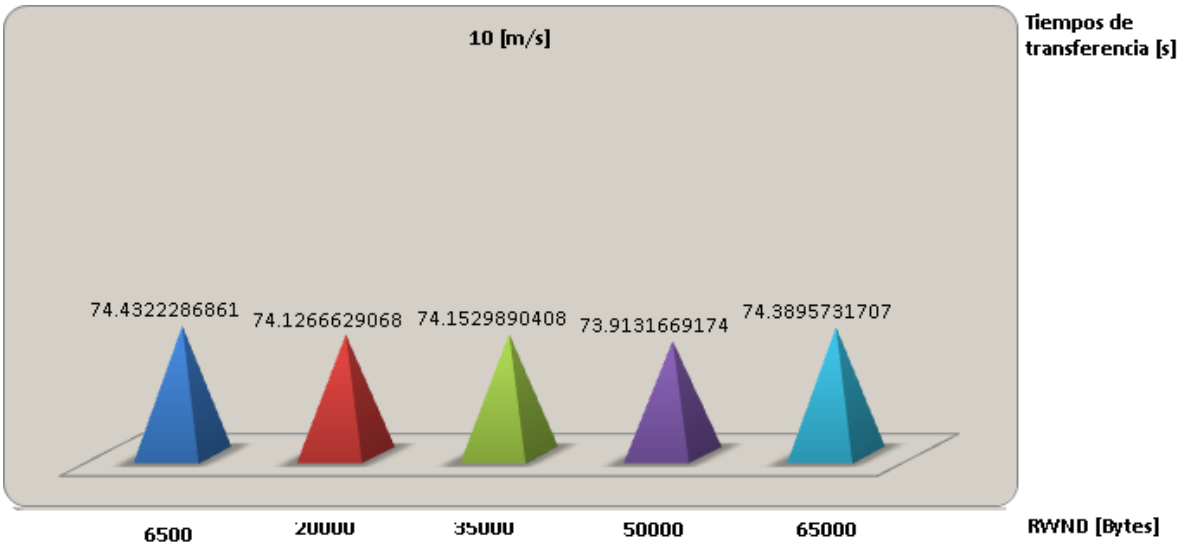



Figura XXIV. TCP, Tiempos totales de transferencia, MN cliente (10[m/s])

# *ANEXO D: Preparación de la Maqueta de Pruebas*

Ya se mencionó en el capítulo 8 que para la maqueta de pruebas se recurrió al uso del proyecto USAGUI-UMIP no obstante, es importante aclarar que para poder utilizar el paquete correspondiente para el desarrollo de MIPv6 fue necesario contar con varias opciones habilitadas en el Kernel de Linux, por ejemplo en el MN, CN y HA las opciones requeridas fueron las siguientes:

```
CONFIG_EXPERIMENTAL=y
CONFIG_SYSVIPC=y
CONFIG_PROC_FS=y
CONFIG_NET=y
CONFIG_INET=y
CONFIG_IPV6=y
CONFIG_IPV6_MIP6=y
CONFIG_XFRM=y
CONFIG_XFRM_USER=y
CONFIG_XFRM_ENHANCEMENT=y
CONFIG_XFRM_SUB_POLICY=y
CONFIG_INET6_XFRM_MODE_ROUTEOPTIMIZATION=y
```

Adicionalmente para el HA y MN también se requirió:

```
CONFIG_IPV6_TUNNEL=y
CONFIG_IPV6_ADVANCED_ROUTER=y
CONFIG_IPV6_MULTIPLE_TABLES=y
```

Para el MN además fue necesario habilitar:

```
CONFIG_IPV6_SUBTREES=y
CONFIG_ARPD=y
```

Si se desea utilizar IPSec entre el MN y su HA las opciones requeridas contemplan:

```
CONFIG_NET_KEY=y
CONFIG_NET_KEY_MIGRATE=y
CONFIG_INET6_ESP=y
CONFIG_INET6_XFRM_MODE_TRANSPORT
CONFIG_INET6_XFRM_MODE_TUNNEL
CONFIG_CRYPTO_HMAC
CONFIG_CRYPTO_SHA1
CONFIG_CRYPTO_DES
```

Se instalaron los siguientes paquetes para armar la maqueta de la figura 8.1 (capítulo 8):

```
gcc (4.4.4), flex (2.5.35), bison (2.4.1), make (3.81)
```

Adicionalmente para el AR y el HA también se necesitó:

```
quagga (0.99), radvd 1.6), wireshark (1.2)
```

En caso de que se quiera emplear IPSec, el MN y su HA requieren:

```
ipsec-tools (0.7)
```

En el HA y MN (opcionalmente en el CN) también habrá que descargar el paquete proporcionado en el proyecto USAGUI-UMIP:

```
umip (0.4-2)
```

Después de la compilación del Kernel se ejecutó el script "chkconf_kernel.sh" (anexado en umip) para verificar que las opciones en el Kernel hubieran sido activadas correctamente. Debido a que todo estuvo en orden se procedió a la instalación del paquete umip. Durante la correspondiente instalación se utilizó el modo terminal (--enable-vt) para que se pudiera consultar el contenido de las estructuras de datos correspondientes en el MN y su HA; desde la línea de comandos se ejecutaron los siguientes comandos:

```
./config --enable-vt
make
make install
```

Una vez que se tuvo todo instalado de manera correcta se procedió a entrar en los respectivos archivos de configuración. Enseguida se explican las configuraciones realizadas en el AR, MN y HA.

Para el HA se especificaron los parámetros que le permitieran registrar a aquellos hosts que también tuvieran instalado el paquete de umip. Para hacer esto posible únicamente se empleó el siguiente archivo de configuración.

*mip6.conf*

```
#Funcionalidad de HA y registro de eventos
NodeConfig HA;
DebugLevel 10;
#Optimización de ruta con otros MNs y CNs. Cuando se utiliza la optimización únicamente hay que habilitar la siguiente línea
DoRouteOptimizationCN disabled;
```

```
DoRouteOptimizationMN disabled;
#Definir interfaz involucrada en movilidad
Interface "eth0";
#Definición de políticas de nodos permitidos
BindingAclPolicy 2001:db8:aa::10 allow;
DefaultBindingAclPolicy deny;
#Opción de integración con IPSec. Al utilizarlo esta opción hay que habilitar la siguiente línea
UseMnHaIPsec disabled;
#Desactivar capacidad de administración de movilidad
KeyMngMobCapability disabled;
#No comentar las siguientes líneas al utilizar IPSec
#IPsecPolicySet {
#       HomeAgentAddress 2001:db8:aa::1;
#       HomeAddress 2001:db8:aa::10/64;
#       IPsecPolicy HomeRegBinding UseESP 1 2;
#       IPsecPolicy MobPfxDisc UseESP 5 6;
#       IPsecPolicy TunnelHomeTesting UseESP 7 8;
#}
```

Para desarrollar sus funciones el HA también requirió de un paquete (radvd) que le permitiera anunciar la capacidad que poseía para registrar a los MNs, fue así que para el HA también se necesitó configurar un archivo donde se anunciara el prefijo IPv6 que sería utilizado para la red local. Se muestran a continuación el archivo respectivo:

*radvd.conf*

```
interface eth0
{
        AdvSendAdvert on;
         MinRtrAdvInterval 1;
         MaxRtrAdvInterval 3;
         AdvIntervalOpt on;
         AdvHomeAgentFlag on;
         AdvHomeAgentInfo on;
         HomeAgentLifetime 1800;
         HomeAgentPreference 10;
         prefix 2001:db8:aa::1/64
         {
                 AdvOnLink on;
                 AdvAutonomous on;
                 AdvRouterAddr on;
         };
};
```

El HA desarrolló un comportamiento de ruteador y por ello tuvo que ser capaz de enrutar paquetes a través de sus interfaces. Para brindar una comunicación por IPv6 entre segmentos se utilizó al protocolo de ruteo RIPng por lo tanto, para el HA y el AR se configuraron los respectivos archivos.

*ripng.conf*

```
hostname localhost
!
router ripng
 network eth2
 network eth0
 redistribute kernel
 redistribute connected
 redistribute static
!
line vty
!
```

*zebra.conf*

```
hostname localhost
!
interface eth0
 ipv6 address 2001:db8:aa::1/64
 no ipv6 nd suppress-ra
 ipv6 nd prefix 2001:db8:aa::/64
!
interface eth2
 ipv6 address 2001:db8:cc::1/64
 ipv6 nd suppress-ra
 ipv6 nd prefix 2001:db8:cc::/64
!
interface lo
!
ipv6 forwarding
!
line vty
!
```

El siguiente archivo de configuración de IPSec permitió realizar la protección de los mensajes de movilidad. Particularmente a través del uso de ESP fue posible autenticar y cifrar la información de movilidad no obstante, únicamente se empleó una configuración manual y el archivo quedó idéntico tanto en el MN como en su HA.

*sa.conf*

```
#Eliminar entradas existentes
flush;
spdflush;
#Definir políticas: modo->transporte|tunel, cifrado->des-cbc, autenticación->hmac-sha1
##BU de HoA de MN a HA
add 2001:db8:aa::10 2001:db8:aa::1 esp 1
        -u 1
        -m transport
```

```
        -E des-cbc "BindingU"
        -A hmac-sha1 "Solicitud-registro_1" ;
#BA HA a HoA de MN
add 2001:db8:aa::1 2001:db8:aa::10 esp 2
        -u 2
        -m transport
        -E des-cbc "BindingA"
        -A hmac-sha1 "Respuesta_registro_1" ;
#Datos de HoA de MN a HA
#add 2001:db8:aa::10 2001:db8:aa::1 esp 3
#       -u 3
#       -m tunnel
#       -E des-cbc "MOBILE-TEST"
#       -A hmac-sha1 "test-key" ;
#Datos de HA a HoA de MN
#add 2001:db8:aa::1 2001:db8:aa:10 esp 4
#       -u 4
#       -m tunnel
#       -E des-cbc "MOBILE-TEST"
#       -A hmac-sha1 "test-key" ;
#MPS de HoA de MN a HA
add 2001:db8:aa::10 2001:db8:aa::1 esp 5
        -u 5
        -m transport
        -E des-cbc "SolPrefi"
        -A hmac-sha1 "Solicitud_de_prefijo" ;
#MPA de HA a HoA de MN
add 2001:db8:aa::1 2001:db8:aa::10 esp 6
        -u 6
        -m transport
        -E des-cbc "ResPrefi"
        -A hmac-sha1 "Respuesta_de_prefijo" ;
#HoTI de HoA de MN a HA
add 2001:db8:aa::10 2001:db8:aa::1 esp 7
        -u 7
        -m tunnel
        -E des-cbc "TestHoTI"
        -A hmac-sha1 "Mensaje-HomeofTestIn" ;
#HoT de HA a HoA de MN
add 2001:db8:aa::1 2001:db8:aa::10 esp 8
        -u 8
        -m tunnel
        -E des-cbc "Test_HoT"
        -A hmac-sha1 "Mensaje-Home_of_Test" ;
```

En el AR se presentó un caso muy parecido al del HA, con la excepción de que no se instaló el paquete de umip. Sus archivos de configuración quedaron de la siguiente manera:

*radvd.conf*

```
interface eth0
{
        AdvSendAdvert on;
        AdvManagedFlag off;
       AdvOtherConfigFlag off;
        MinRtrAdvInterval 1;
        MaxRtrAdvInterval 3;
        prefix 2001:db8:cc::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
                AdvValidLifetime 300;
         AdvPreferredLifetime 120;
        };
};
```

*ripng.conf*

```
hostname quagga-router
!
router ripng
 network eth0
 redistribute connected
 redistribute static
 redistribute kernel
!
line vty
!
```

*zebra.conf*

```
hostname quagga-router
!
interface eth0
 ipv6 address 2001:db8:cc::1/64
 ipv6 nd suppress-ra
 ipv6 nd prefix 2001:db8:cc::/64
!
interface eth1
 ipv6 address 2001:db8:bb::1/64
 no ipv6 nd suppress-ra
 ipv6 nd prefix 2001:db8:bb::/64
!
interface lo
!
ipv6 forwarding
!
```

```
line vty
!
```

En lo que concierne al MN, únicamente se requirió de un archivo de configuración mediante el cual se especificó su dirección y sus capacidades de registro ante el HA.

*mip6.conf*

```
#Funcionalidad de MN y registro de eventos
NodeConfig MN;
DebugLevel 10;
#Activar optimización de handover
OptimisticHandoff disabled;
#Optimización de ruta con otros MNs y CNs. Cuando se utiliza la optimización únicamente hay que habilitar las siguientes líneas
DoRouteOptimizationCN disabled;
DoRouteOptimizationMN disabled;
#Duración del registro con HA
MnMaxHaBindingLife 600;
#Activar cuando se utilice optimización de ruta
UseCnBuAck disabled;
#Descartar HA con problemas en sus parámetros
MnDiscardHaParamProb enabled;
#Definir interfaz involucrada en movilidad
Interface "wlan0" {
        MnIfPreference 1;
}
#Direcciones de interfaz adjunta a red local
MnHomeLink "wlan0" {
        HomeAgentAddress 2001:db8:aa::1;
        HomeAddress 2001:db8:aa::10/64;
}
#Al utilizar IPSec habilitar la siguiente línea
UseMnHaIPsec disabled;
#No comentar las siguientes líneas al usar IPSec
#IPsecPolicySet {
#       HomeAgentAddress 2001:db8:aa::1;
#       HomeAddress 2001:db8:aa::10/64;
#       IPsecPolicy HomeRegBinding UseESP 1 2;
#       IPsecPolicy MobPfxDisc UseESP 5 6;
#       IPsecPolicy TunnelHomeTesting UseESP 7 8;
#}
```

Al llevar a cabo la prueba del uso de IPSec se requirió del archivo “sa.conf”.

Con la finalidad de disminuir el tiempo implicado en la configuración de los elementos de la maqueta de pruebas se prepararon los siguientes scripts:

*Home_Agent.sh*

```
#!/bin/bash
#Actuar como ruteador y HA
echo 1 > /proc/sys/net/ipv6/conf/all/proxy_ndp
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
echo 0 > /proc/sys/net/ipv6/conf/all/autoconf
echo 0 > /proc/sys/net/ipv6/conf/all/accept_ra
echo 0 > /proc/sys/net/ipv6/conf/all/accept_redirects
#Configurar reglas provisionales de IPv6
ip6tables -F
ip6tables –A INPUT –p all –j ACCEPT
ip6tables –A OUTPUT –p all –j ACCEPT
ip6tables –A FORWARD –p all –j ACCEPT
#Iniciar los demonios correspondientes
/etc/init.d/zebra start
/etc/init.d/ripngd start
/etc/init.d/radvd start
#En caso de no utilizar IPSec comentar la siguiente línea
setkey -f /etc/sa.conf
#Iniciar el demonio de umip
mip6d -c /etc/mip6d.conf
```

*Mobile_Node.sh*

```
#!/bin/bash
#Actuar como host ipv6
echo 0 > /proc/sys/net/ipv6/conf/wlan0/forwarding
echo 1 > /proc/sys/net/ipv6/conf/wlan0/autoconf
echo 1 > /proc/sys/net/ipv6/conf/ wlan 0/accept_ra
echo 1 > /proc/sys/net/ipv6/conf/ wlan 0/accept_redirects
#Configurar HoA
ifconfig wlan 0 inet6 add 2001:db8:aa::10/64
#Configurar reglas provisionales de IPv6
ip6tables -F
ip6tables –A INPUT –p all –j ACCEPT
ip6tables –A OUTPUT –p all –j ACCEPT
#Iniciar los demonios correspondientes
#En caso de no utilizar IPSec comentar la siguiente línea
setkey -f /etc/sa.conf
#Iniciar el demonio de umip
mip6d -c /etc/mip6d.conf
```

Finalmente es importante mencionar que para utilizar los scripts anteriores en otros entornos de prueba será necesario cambiar los nombres de las interfaces correspondientes y las direcciones IPv6 que se deseen utilizar. De la misma forma es conveniente verificar las rutas donde se encuentran los archivos de configuración.

# *ANEXO E: Maqueta de Pruebas y resultados obtenidos*

Debido a que en un principio no se contaba con APs la topología de la maqueta de pruebas contempló únicamente el uso de una red cableada con cables UTP. La figura XV presenta la interconexión que se realizó entre los distintos dispositivos.

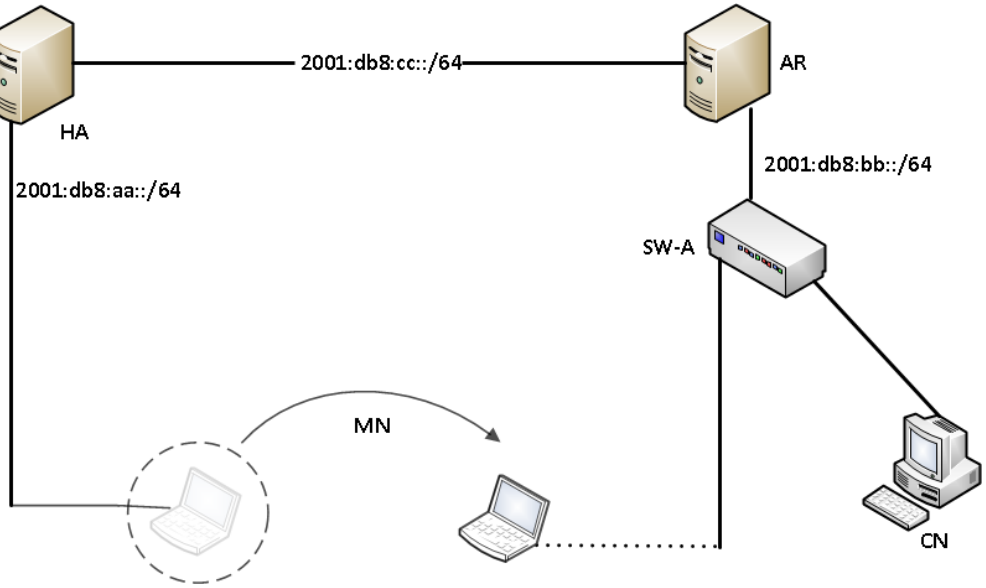



Figura XV. Primera topología de la maqueta de pruebas

Una vez confirmado el funcionamiento del protocolo, MIPv6, (intercambio de mensajes de registro del MN) se procedió a utilizar 2 APs en la maqueta de pruebas. La topología final se muestra a continuación (figura XVI).

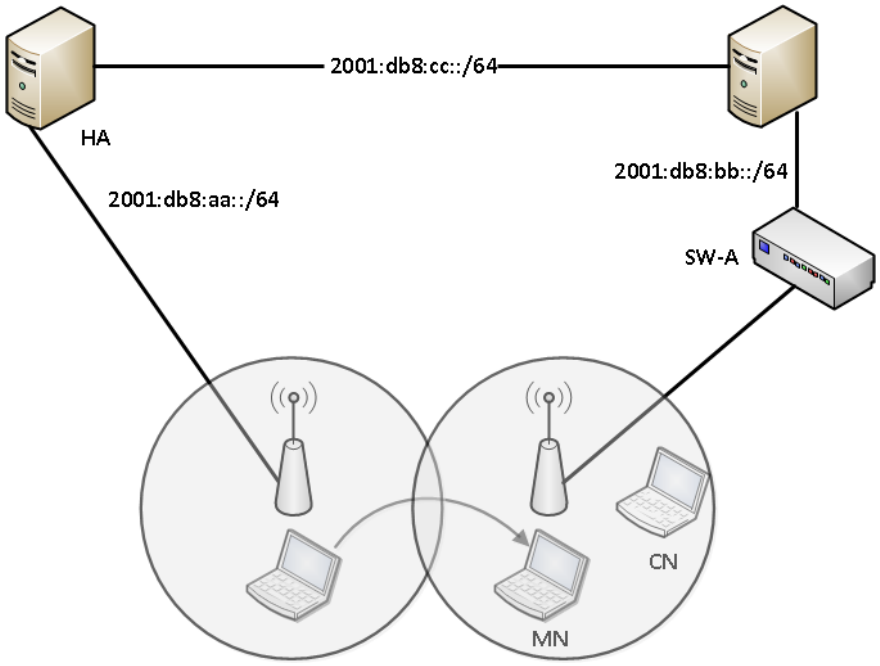



Figura XVI. Topología final de la maqueta de pruebas

Cuando el MN se encontraba en su red local únicamente tenía asignada una dirección IPv6 HoA; posteriormente, al recibir un mensaje RA adquirió otra dirección IPv6. La información de la interfaz inalámbrica del MN quedó de la siguiente forma (figura XVII).

```
[root@FED gio]# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:21:5D:8C:BD:1E
          inet addr:169.254.4.1  Bcast:169.254.4.255  Mask:255.255.255.0
          inet6 addr: 2001:db8:aa::10/64 Scope:Global
          inet6 addr: 2001:db8:aa:0:221:5dff:fe8c:bd1e/64 Scope:Global
          inet6 addr: fe80::221:5dff:fe8c:bd1e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10325 (10.0 KiB)  TX bytes:13036 (12.7 KiB)
```

Figura XVII. Interfaces del MN en red local

En la figura XVIII se presentan las rutas IPv6 definidas hasta ese momento en el MN.

```
[root@FED gio]# route -A inet6 -n
Kernel IPv6 routing table
Destination                    Next Hop                   Flags Metric Ref    Use Iface
2001:db8:aa::/64               ::                         U     256    35       0 wlan0
fe80::/64                      ::                         U     256    0        0 wlan0
::/0                           fe80::21a:a0ff:fe2e:4487   UGDA  1024   0        0 wlan0
::1/128                        ::                         U     0      6        1 lo
2001:db8:aa::10/128            ::                         U     0      0        1 lo
2001:db8:aa:0:221:5dff:fe8c:bd1e/128 ::                  U     0      0        1 lo
fe80::221:5dff:fe8c:bd1e/128   ::                         U     0      0        1 lo
ff02::1/128                    ff02::1                    UC    0      38       0 wlan0
ff02::9/128                    ff02::9                    UC    0      3        0 wlan0
ff02::fb/128                   ff02::fb                   UC    0      8        0 wlan0
ff00::/8                       ::                         U     256    0        0 wlan0
```

Figura XVIII. Rutas IPv6 del MN en red local

Al desplazar el MN a una red foránea cambió la información de sus interfaces, y se creó una nueva interfaz virtual de uso exclusivo para la Movilidad IPv6 (figura XXIX).

```
ip6tnl1   Link encap:UNSPEC  HWaddr 20-01-0D-B8-00-BB-00-00-00-00-00-00-00-00-00-00
          inet6 addr: 2001:db8:aa::10/128 Scope:Global
          inet6 addr: fe80::221:5dff:fe8c:bd1e/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP  MTU:1460  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

wlan0     Link encap:Ethernet  HWaddr 00:21:5D:8C:BD:1E
          inet addr:169.254.5.1  Bcast:169.254.5.255  Mask:255.255.255.0
          inet6 addr: 2001:db8:bb:0:221:5dff:fe8c:bd1e/64 Scope:Global
          inet6 addr: fe80::221:5dff:fe8c:bd1e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

Figura XXIX. Interfaces del MN en red foránea

Las rutas IPv6 respectivas del MN (estando en la red foránea) también se vieron afectadas (figura XXX).

```
[root@FED gio]# route -A inet6 -n
Kernel IPv6 routing table
Destination                    Next Hop                   Flags Metric Ref    Use Iface
2001:db8:aa::1/128             2001:db8:aa::1             UC    0      1        1 ip6tnl1
::/0                           ::                         U     128    0        0 ip6tnl1
2001:db8:aa::10/128            ::                         U     256    0        0 ip6tnl1
2001:db8:bb::/64               ::                         U     256    0        0 wlan0
fe80::/64                      ::                         U     256    0        0 wlan0
fe80::/64                      ::                         U     256    0        0 ip6tnl1
::/0                           fe80::21a:a0ff:fe0d:ac3e   UG    1008   2        1 wlan0
::1/128                        ::                         U     0      7        1 lo
2001:db8:aa::10/128            ::                         U     0      1        1 lo
2001:db8:bb::/128              ::                         U     0      0        1 lo
2001:db8:bb:0:221:5dff:fe8c:bd1e/128 ::                  U     0      1        1 lo
fe80::/128                     ::                         U     0      0        1 lo
fe80::221:5dff:fe8c:bd1e/128   ::                         U     0      0        1 lo
fe80::221:5dff:fe8c:bd1e/128   ::                         U     0      0        1 lo
ff02::1/128                    ff02::1                    UC    0      51       0 wlan0
ff02::2/128                    ff02::2                    UC    0      2        0 wlan0
```

Figura XXX. Rutas IPv6 del MN en red foránea

Al desplazar el MN a una red foránea se llevó a cabo el registro correspondiente (figuras XXXI y XXXII).

```
191 639.123346 2001:db8:aa::10 2001:db8:aa::1 MIPv6 110 Binding Update
⊞ Ethernet II, Src: Sony_03:e6:b2 (00:1d:ba:03:e6:b2), Dst: 3com_ab:30:99 (00:60:08:ab:30:99)
⊟ Internet Protocol Version 6, Src: 2001:db8:cc:0:21d:baff:fe03:e6b2 (2001:db8:cc:0:21d:baff:fe03:e6b2), Dst: 2001:db8:aa::1 (2001:db8:aa::1)
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 56
    Next header: IPv6 destination option (0x3c)
    Hop limit: 64
    Source: 2001:db8:cc:0:21d:baff:fe03:e6b2 (2001:db8:cc:0:21d:baff:fe03:e6b2)
    [Source SA MAC: Sony_03:e6:b2 (00:1d:ba:03:e6:b2)]
    Destination: 2001:db8:aa::1 (2001:db8:aa::1)
  ⊟ Destination Option
      Next header: Mobile IPv6 (0x87)
      Length: 2 (24 bytes)
      PadN: 4 bytes
      Option Type: 201 (0xc9) - Home Address Option
      Option Length: 16
      Home Address: 2001:db8:aa::10 (2001:db8:aa::10)
⊟ Mobile IPv6 / Network Mobility
    Payload protocol: IPv6 no next header (0x3b)
    Header length: 3 (32 bytes)
    Mobility Header Type: Binding Update (5)
    Reserved: 0x00
    Checksum: 0x8380
  ⊟ Binding Update
      Sequence number: 19077
      1... .... .... .... = Acknowledge (A) flag: Binding Acknowledgement requested
      .1.. .... .... .... = Home Registration (H) flag: Home Registration
      ..0. .... .... .... = Link-Local Compatibility (L) flag: No Link-Local Address Compatibility
      ...0 .... .... .... = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility
      .... 0... .... .... = MAP Registration Compatibility (M) flag: No MAP Registration Compatibility
      .... .0.. .... .... = Mobile Router (R) flag: No Mobile Router Compatibility
      .... ..0. .... .... = Proxy Registration (P) flag: No Proxy Registration
      .... ...0 .... .... = Forcing UDP encapsulation (F) flag: No Forcing UDP encapsulation
      .... .... 0... .... = TLV-header format (T) flag: No TLV-header format
      Lifetime: 15 (60 seconds)
  ⊟ Mobility Options
      Mobility Options: PadN (1)
      PadN: 2 bytes
      Mobility Options: Alternate Care-of Address (3)
      Alternate care-of address: 2001:db8:cc:0:21d:baff:fe03:e6b2 (2001:db8:cc:0:21d:baff:fe03:e6b2)
```

Figura XXXI. Captura de tráfico BU de red foránea del MN al HA

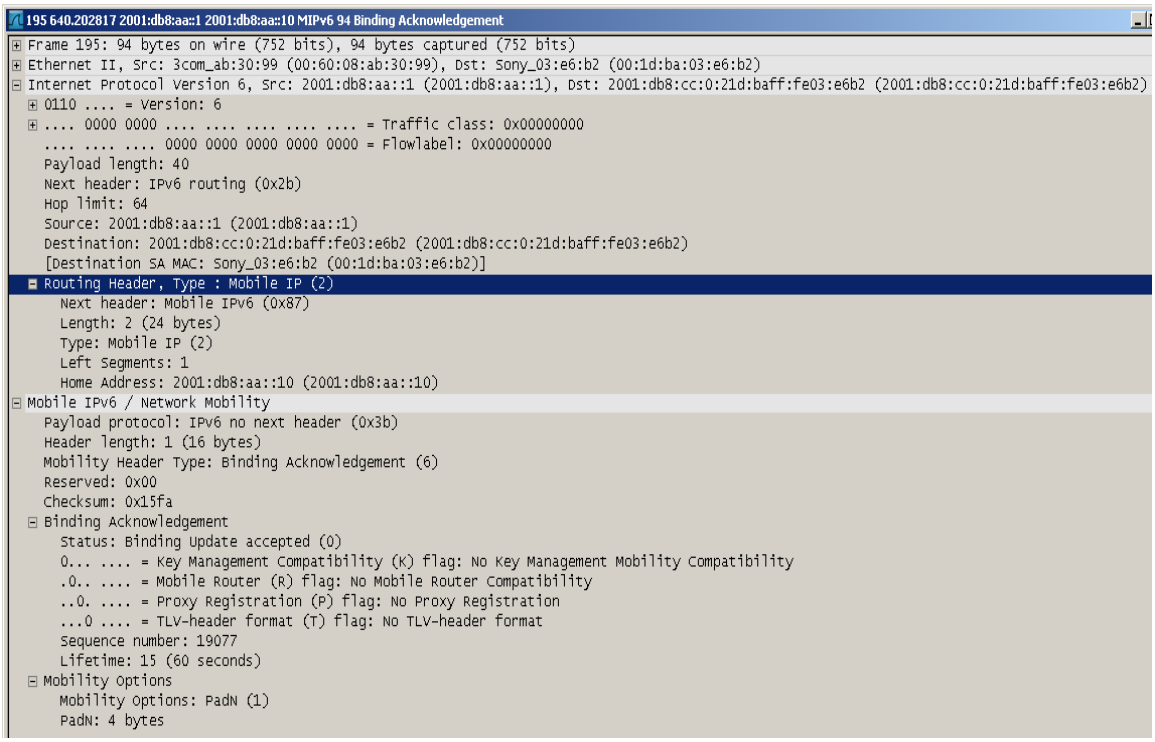



Figura XXXII. Captura de tráfico BA del HA a red foránea del MN

Mientas el MN permaneció en la red foránea pudo seguir comunicándose con un CN, no se realizó una optimización de ruta debido a que el CN no tenía soporte de MIPv6. Al momento de regresar al MN a su red local se necesitó anunciar dicho evento al HA (figuras XXXIII y XXXIV).

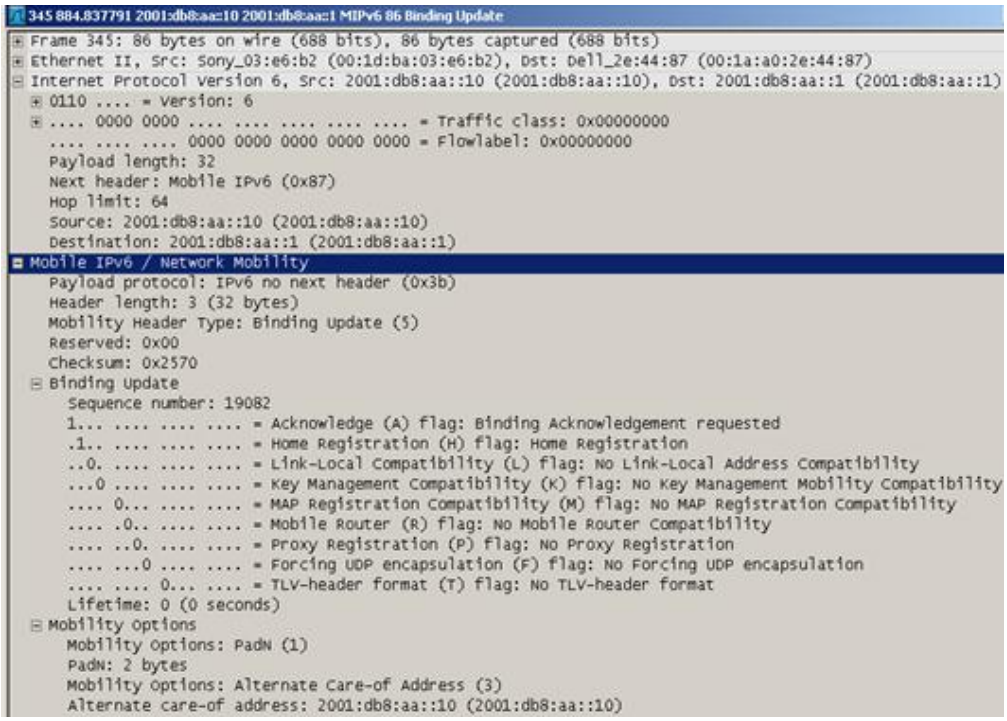



Figura XXXIII. Captura de tráfico BU del MN al regresar a su red local

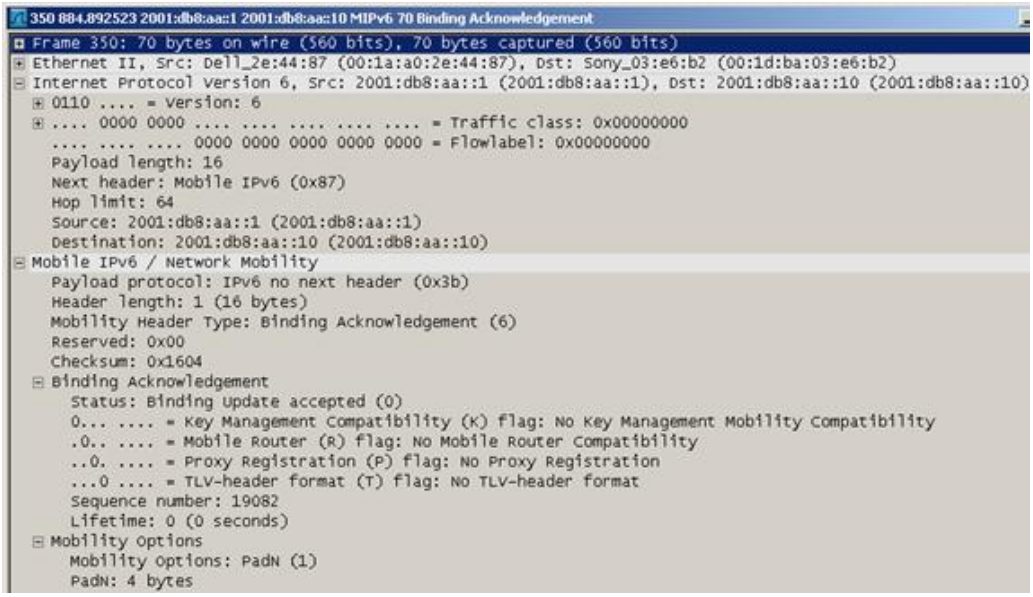



Figura XXXIV. Captura de tráfico BA del HA a red foránea del MN

Las rutas de IPv6 del MN al regresar a su red local se modificaron nuevamente porque al estar en dicha red ya no requiere del soporte de Movilidad IPv6 (figura XXXV).


Figura XXXV. Rutas IPv6 del MN al regresar a su red local

La información de las interfaces del MN también se vio afectada, al regresar a su red local el MN pasó nuevamente las direcciones de su interfaz virtual a su interfaz inalámbrica (figura XXXVI).

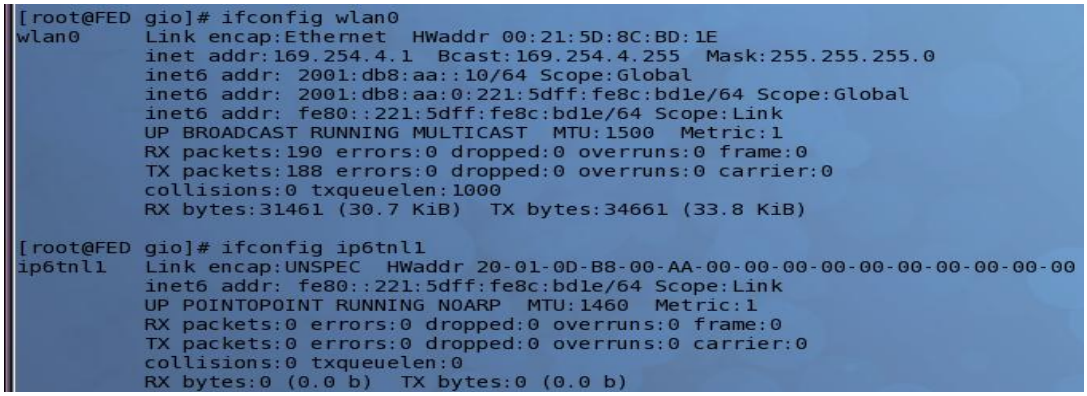



Figura XXXVI. Interfaces del MN de regreso a red local

En lo que respecta al contenido de las estructuras de datos utilizadas, se puede apreciar el contenido de cada una de éstas en las siguientes figuras.

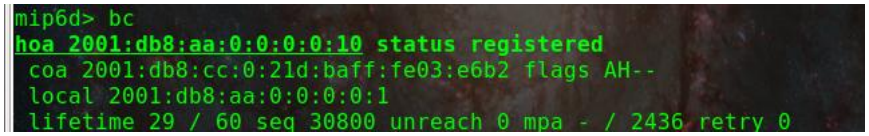



Figura XXXVII. Estructura de datos del Binding Cache en HA


Figura XXXVIII. Estructura de datos del Home Agent List en HA

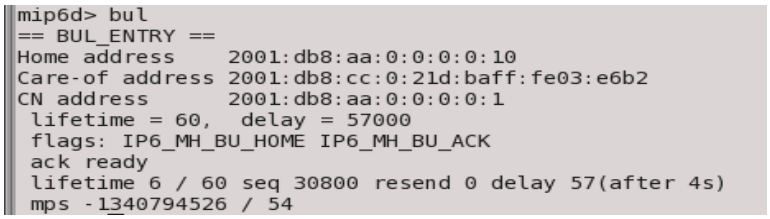



Figura XXXIX. Binding Update List en MN

Respecto a los logs generados, los resultados más representativos se muestran en las siguientes figuras. El HA se configuró con la dirección anycast definida para MIPv6 y de ahí en adelante tomó una función de proxy; es decir, se encargó de crear un túnel hacia la dirección CoA actual del MN para enviar y recibir a través de éste los paquetes destinados a la dirección HoA del MN. Para hacer esto posible el HA necesitó procesar los mensajes BU recibidos de parte del MN, y de ser el caso enviar el mensaje BA correspondiente, modificando según aplique, el túnel creado con anterioridad (figura XL):

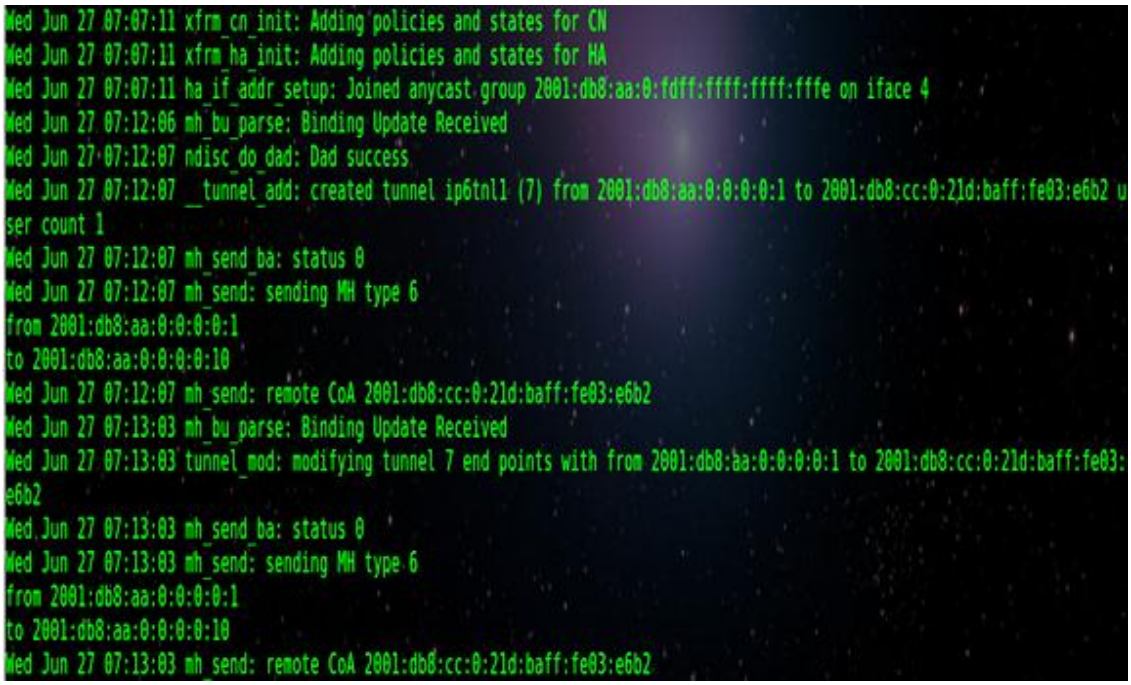



Figura XL. Información del proceso umip en HA

En cuanto al MN, el móvil detectó si se encontraba en su red local o en una red foránea al recibir y procesar los mensajes RA de la red de su ubicación actual. Cuando tal información resultaba ser diferente, sabía que había dejado su red local, por el contrario, cuando la información coincidió con el prefijo anunciado en su red local, supo que ya no se encontraba en una red foránea (figura XLI).

```
Wed Jun 27 07:06:29 xfrm_cn_init: Adding policies and states for CN
Wed Jun 27 07:06:29 xfrm_mn_init: Adding policies and states for MN
Wed Jun 27 07:06:29 conf_home_addr_info: HoA address 2001:db8:aa:0:0:0:0:10
Wed Jun 27 07:06:29 conf_home_addr_info: HA address 2001:db8:aa:0:0:0:0:1
Wed Jun 27 07:06:29 __tunnel_add: created tunnel ip6tnl1 (8) from 2001:db8:aa:0:0:0:0:10 to 2001:db8:aa:0:0:0:0:1 user count 1
Wed Jun 27 07:06:29 conf_home_addr_info: Home address 2001:db8:aa:0:0:0:0:10
Wed Jun 27 07:06:29 flag_hoa: set HoA 2001:db8:aa:0:0:0:0:10/128 iif 8 flags 12 preferred_time 4294967295 valid_time 4294967295
Wed Jun 27 07:06:29 conf_home_addr_info: Added new home_addr_info successfully
mip6d[1884]: Interface 1 (lo):type 772 unsupported
mip6d[1884]: Interface 2 (tunl0):type 768 unsupported
Wed Jun 27 07:06:29 __md_discover_router: discover link on iface eth0 (6)
Wed Jun 27 07:06:32 md_change_default_router: add new router fe80:0:0:0:21a:a0ff:fe2e:4487 on interface eth0 (6)
Wed Jun 27 07:06:32 md_update_router_stats: Adding CoA 2001:db8:aa:0:21d:baff:fe03:e6b2 on interface (6)
Wed Jun 27 07:06:34 mn_addr_do_dad: DAD succeeded!
Wed Jun 27 07:06:34 mn_addr_do_dad: address = 2001:db8:aa:0:0:0:0:10
Wed Jun 27 07:06:34 mn_move: 1775
Wed Jun 27 07:06:34 mn_move: in home net
Wed Jun 27 07:06:34 mv_hoa: move HoA 2001:db8:aa:0:0:0:0:10/64 from iface 8 to 6
Wed Jun 27 07:06:34 md_update_router_stats: Adding CoA 2001:db8:aa:0:21d:baff:fe03:e6b2 on interface (6)
Wed Jun 27 07:06:37 md_update_router_stats: Adding CoA 2001:db8:aa:0:21d:baff:fe03:e6b2 on interface (6)
Wed Jun 27 07:07:27 md_update_router_stats: Adding CoA 2001:db8:aa:0:21d:baff:fe03:e6b2 on interface (6)
Wed Jun 27 07:07:29 md_update_router_stats: Adding CoA 2001:db8:aa:0:21d:baff:fe03:e6b2 on interface (6)
Wed Jun 27 07:07:31 md_expire_router: expiring router fe80:0:0:0:21a:a0ff:fe2e:4487 on iface eth0 (6)
Wed Jun 27 07:07:36 __md_discover_router: discover link on iface eth0 (6)
Wed Jun 27 07:07:36 md_change_default_router: add new router fe80:0:0:0:260:8ff:feab:3099 on interface eth0 (6)
Wed Jun 27 07:07:36 md_update_router_stats: Adding CoA 2001:db8:cc:0:21d:baff:fe03:e6b2 on interface (6)
Wed Jun 27 07:07:37 md_update_router_stats: Adding CoA 2001:db8:cc:0:21d:baff:fe03:e6b2 on interface (6)
Wed Jun 27 07:07:38 mn_move: 1775
Wed Jun 27 07:07:38 mn_move: in foreign net
Wed Jun 27 07:07:38 mv_hoa: move HoA 2001:db8:aa:0:0:0:0:10/128 from iface 6 to 8
Wed Jun 27 07:07:38 mn_send_home_bu: 792
Wed Jun 27 07:07:38 mn_get_home_lifetime: CoA lifetime 86399 s, HoA lifetime 86390 s, BU lifetime 60 s
Wed Jun 27 07:07:38 process_first_home_bu: New bule for HA
Wed Jun 27 07:07:38 bul_add: Adding bule
== BUL_ENTRY ==
Home address    2001:db8:aa:0:0:0:0:10
Care-of address 2001:db8:cc:0:21d:baff:fe03:e6b2
CN address      2001:db8:aa:0:0:0:0:1
 lifetime = 60,  delay = 1500
 flags: IP6_MH_BU_HOME IP6_MH_BU_ACK
Wed Jun 27 07:07:38 mn_send_home_bu: New bule for HA
Wed Jun 27 07:07:38 mh_send: sending MH type 5
from 2001:db8:aa:0:0:0:0:10
to 2001:db8:aa:0:0:0:0:1
Wed Jun 27 07:07:38 mh_send: local CoA 2001:db8:cc:0:21d:baff:fe03:e6b2
Wed Jun 27 07:07:38 bul_update_timer: Updating timer
== BUL_ENTRY ==
Home address    2001:db8:aa:0:0:0:0:10
Care-of address 2001:db8:cc:0:21d:baff:fe03:e6b2
CN address      2001:db8:aa:0:0:0:0:1
 lifetime = 60,  delay = 1500
 flags: IP6_MH_BU_HOME IP6_MH_BU_ACK
Wed Jun 27 07:07:38 tunnel_mod: modifying tunnel 8 end points with from 2001:db8:cc:0:21d:baff:fe03:e6b2 to 2001:db8:aa:0:0:0:0:1
Wed Jun 27 07:07:38 __tunnel_mod: modified tunnel iface ip6tnl1 (8)from 2001:db8:cc:0:21d:baff:fe03:e6b2 to 2001:db8:aa:0:0:0:0:1
Wed Jun 27 07:07:39 mn_recv_ba: 1044
Wed Jun 27 07:07:39 mn_recv_ba: Got BA from 2001:db8:aa:0:0:0:0:1 to home address 2001:db8:aa:0:0:0:0:10 with coa 2001:db8:cc:0:21d:baff:fe03:e6b2 and statu
 0
```

Figura XLI. Información del proceso umip en MN

Se observa ahora lo acontecido cuando se inició una comunicación (echo-request y echo-reply) desde el HA hacia las direcciones HoA y CoA del MN (figura XLII).

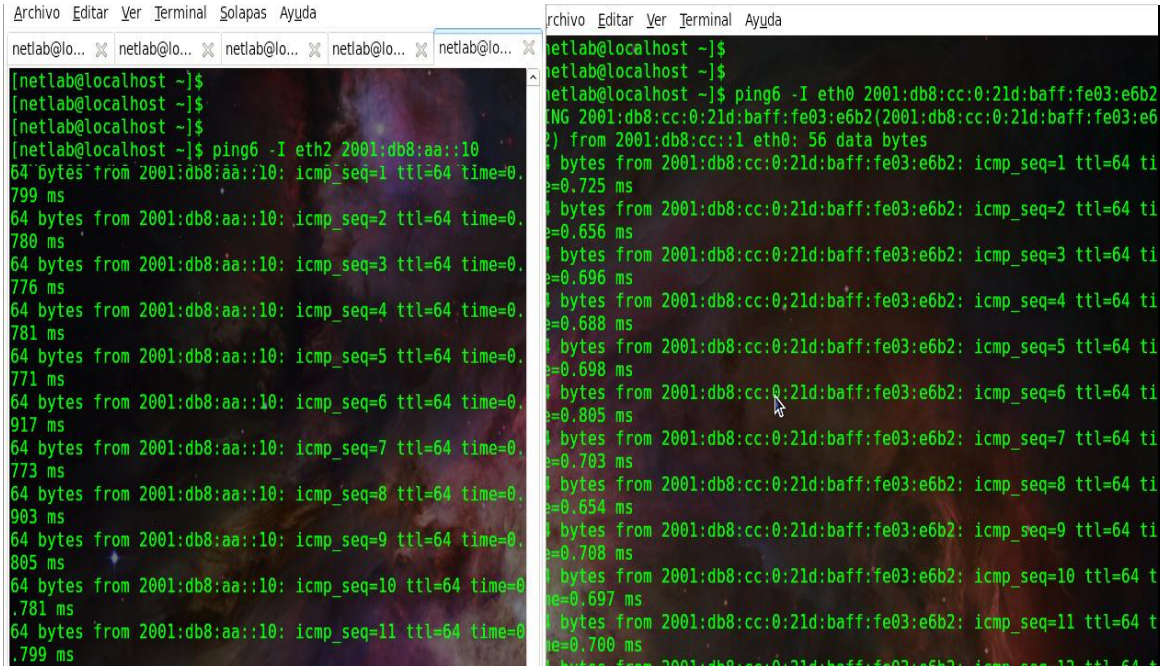



Figura XLII. Resultados de paquetes ICMPv6 del HA al MN

Para observar el comportamiento del tráfico UDP, mediante el programa VLC se decidió realizar la transferencia de un video, mientras el MN se desplazaba de su red local hacia una red foránea, se transmitió el stream hacia la dirección del CN. Estando en dicha red el MN siguió con la transmisión del video, inclusive cuando volvió a su red local (figuras XLIII y XLIV).

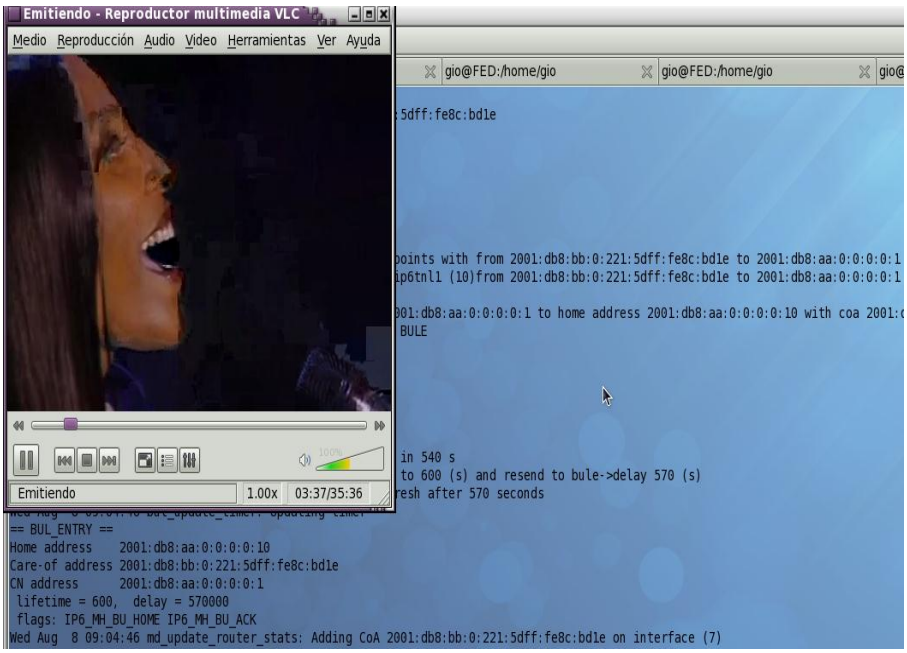



Figura XLIII. Transferencia de un video desde el MN hacia el CN

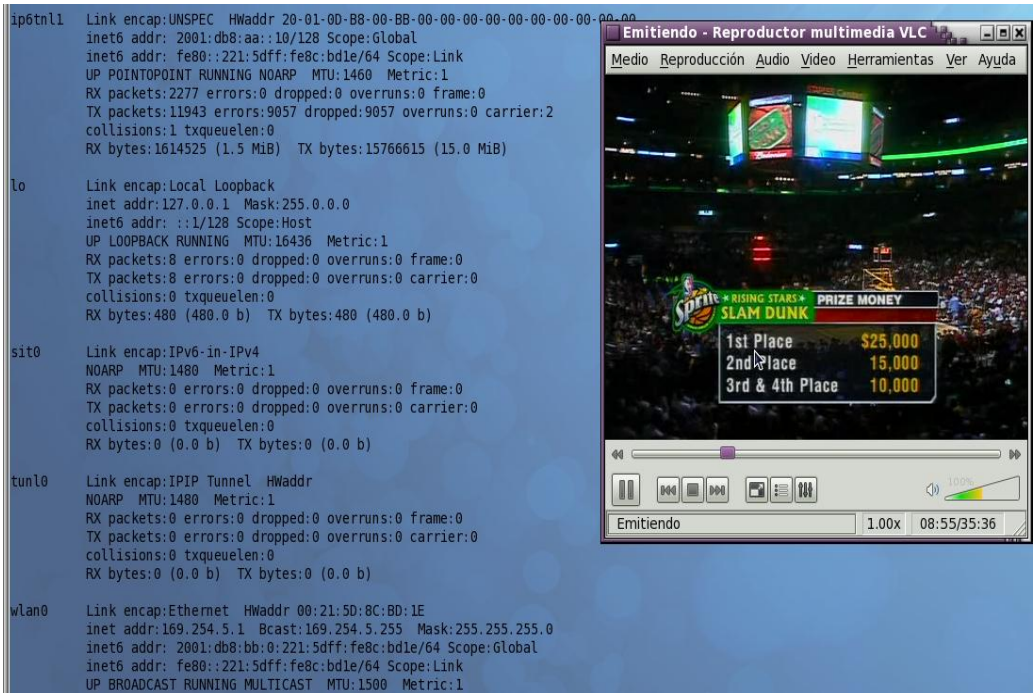



Figura XLIV. Recepción del video en el CN desde el MN

En cuanto al tráfico TCP el uso de Filezilla (aplicación FTP con soporte de IPv6) permitió crear una relación cliente/servidor en FTP, el MN fue el cliente y el CN el servidor (figuras XLV y XLVI).

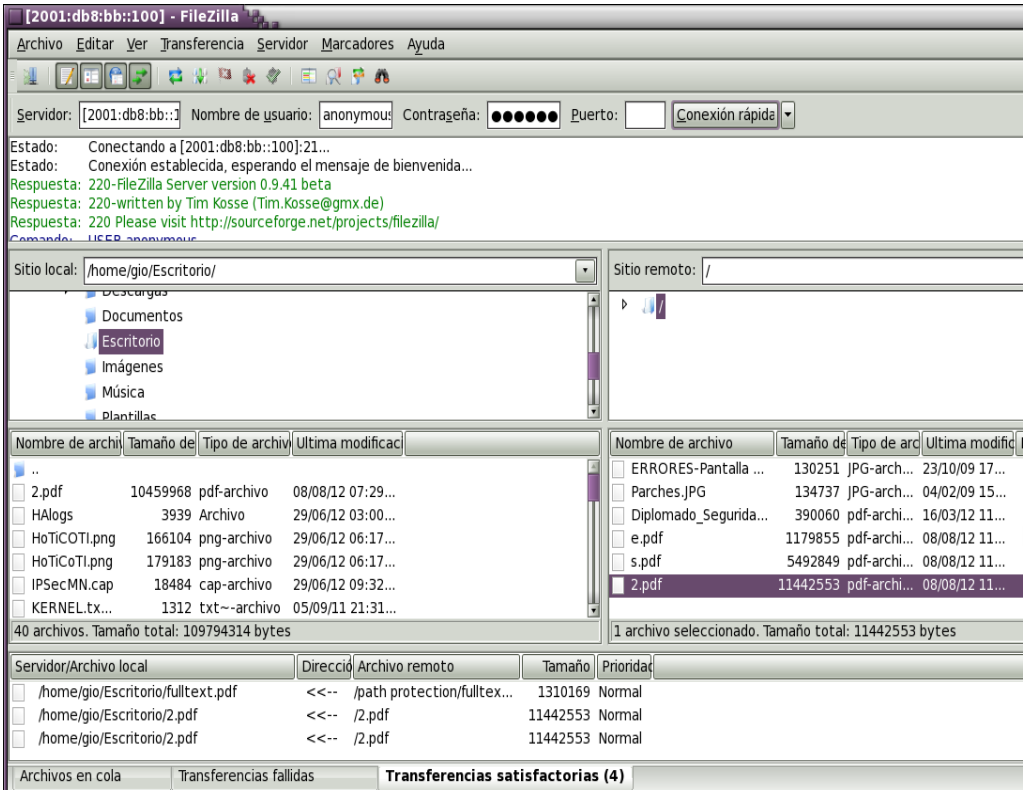



Figura XLV. CN actuando como servidor FTP

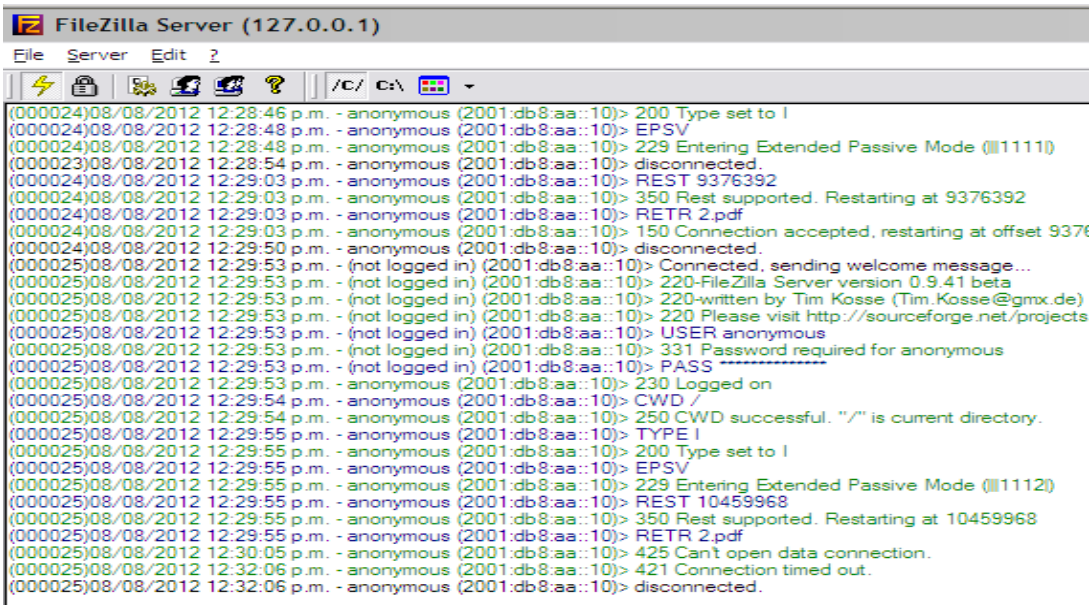



Figura XLVI. MN funcionado como cliente FTP

En la siguiente figura se observa la conexión TCP que se estableció en el CN com FTP (figura XLVII).

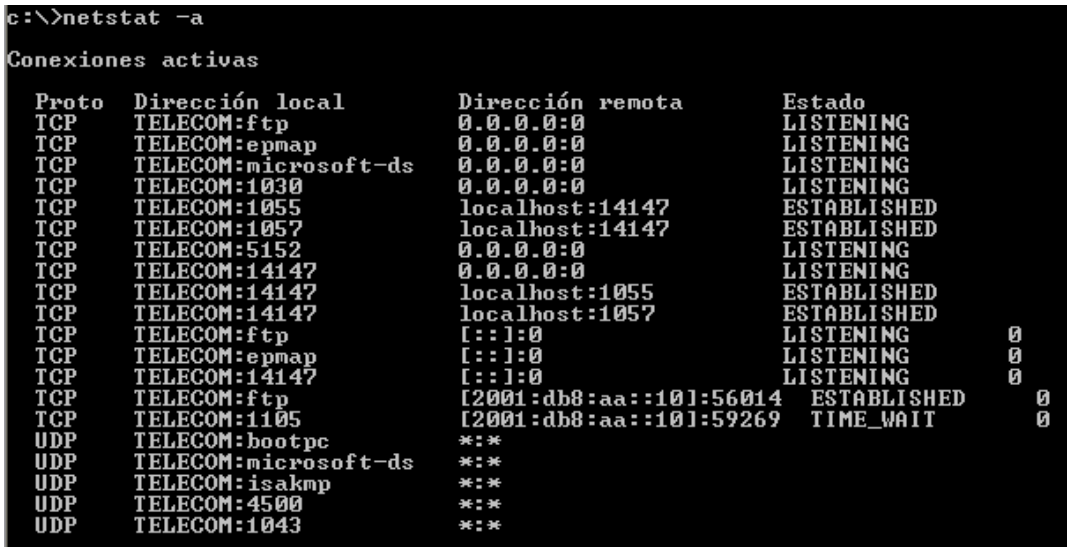



Figura XLVII. Conexión FTP establecida en el servidor

Adicionalmente se empleó una herramienta desarrollada para medir las capacidades de MIPv6 (MIPv6 tester), mediante ésta el CN (servidor) transmitió tráfico UDP hacia el MN (cliente). Durante la transmisión llevada a cabo el tráfico se vio temporalmente pausado y se reanudó después de que el MN se asoció a la red foránea. Particularmente uno de los rasgos más interesantes observados fue que el handover presentado resultó de cerca de 9 segundos En las siguientes imágenes se presentan las respectivas capturas de pantalla (figuras XLVIII Y XLIX).

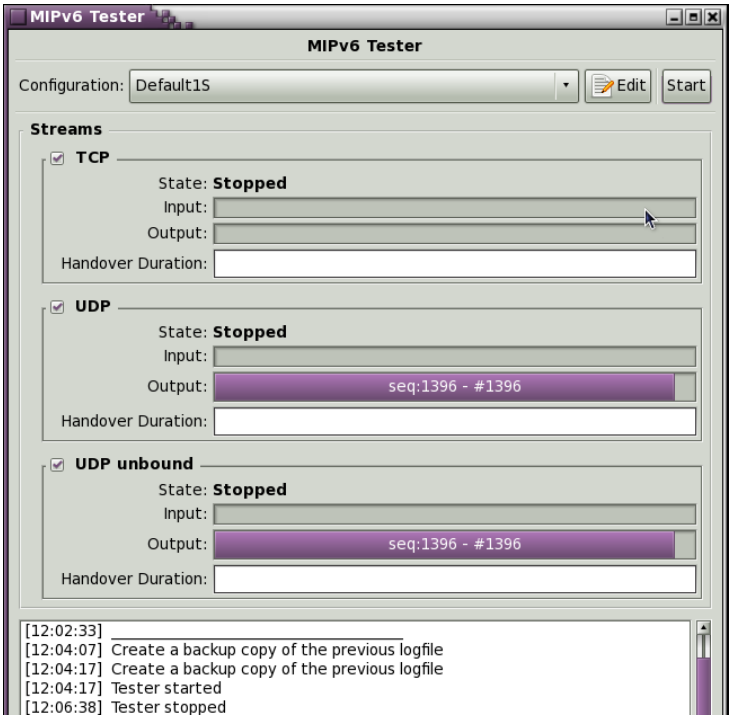



Figura XLVIII. CN (servidor) ejecutando MIPv6 Tester

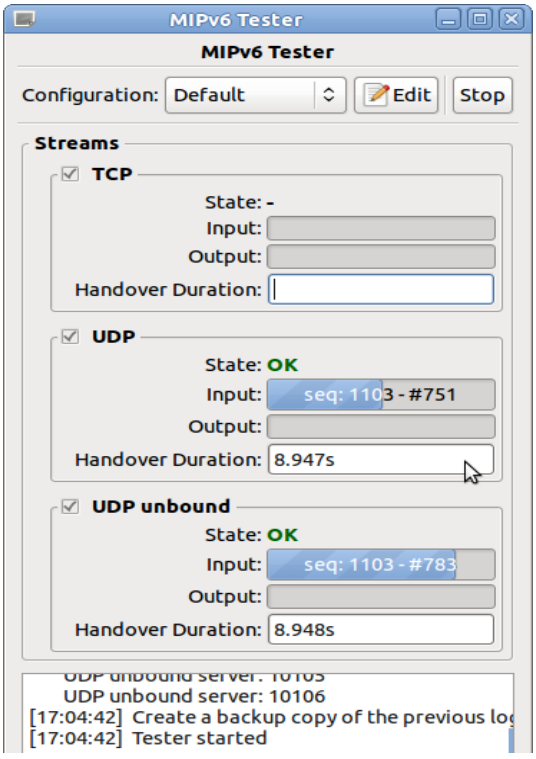



Figura XLIX. MN (cliente) ejecutando MIPv6 Tester

Finalmente se decidió emplear IPSec únicamente con fines demostrativos en el tráfico correspondiente al registro, es decir los mensajes BU y BA fueron cifrados para ocultar su información de posibles atacantes que pudieran hacer uso de algún sniffer.

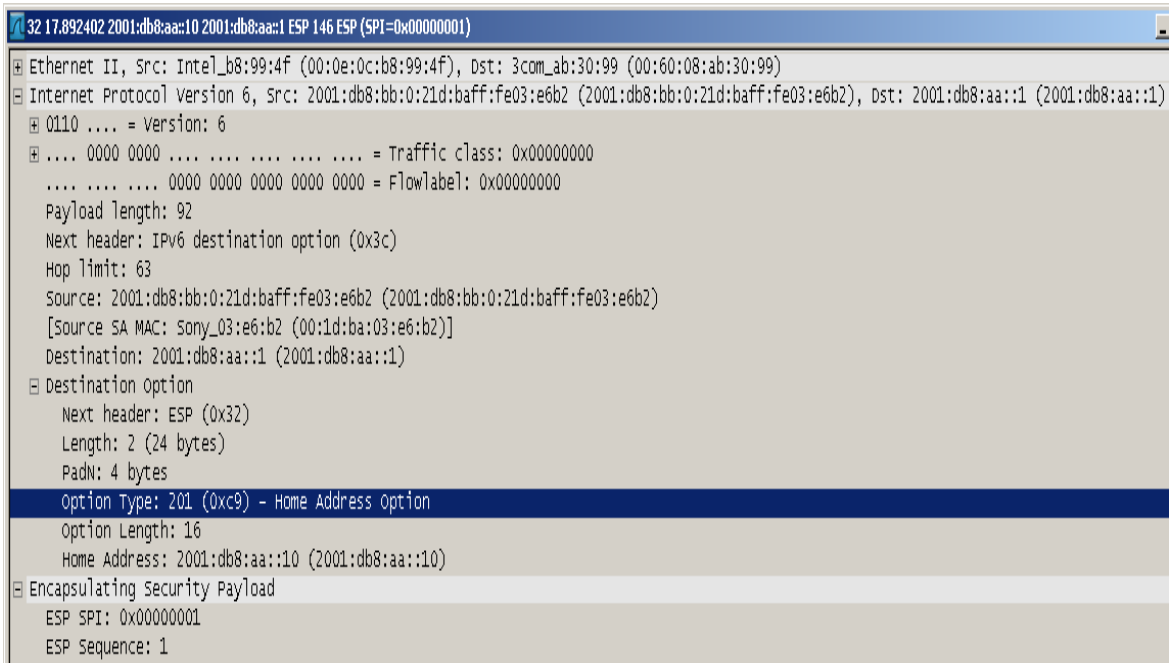



Figura XL. Captura de tráfico BU protegido por IPSec

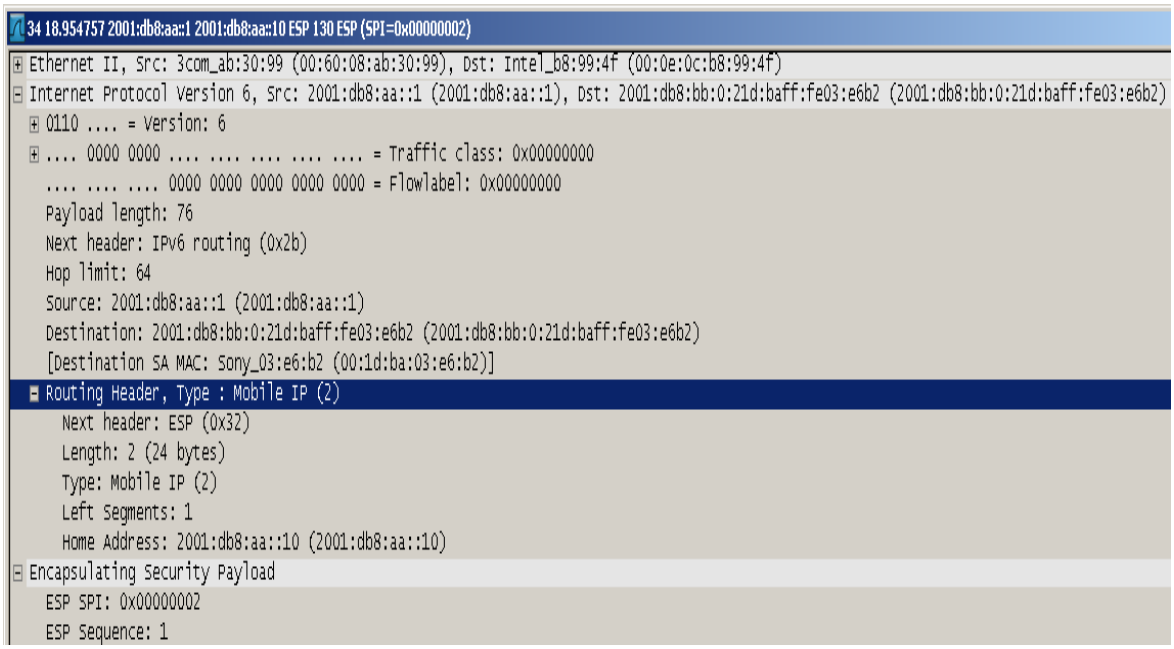



Figura XLI. Captura de tráfico BA protegido por IPSec