Escuela Superior de Ingenieros
Universidad de Sevilla

Análisis de las extensiones a IPv6 Móvil para la mejora del proceso de "handover"

Proyecto Fin de Carrera
Ingeniería de Telecomunicación

Autor: David García Ternero
Tutor: Juan Antonio Ternero Muñiz

Sevilla, Enero de 2003

Índice General

Capítulo 1. Introducción

Hoy en día, estamos inmersos en un mundo de cambio. Las personas se desplazan de un sitio a otro constantemente, y desean estar comunicadas en cualquier momento y en cualquier lugar, ya sea paseando por un parque, en el coche o en un restaurante. Están saliendo a la luz nuevos dispositivos que satisfacen esa necesidad, y actualmente no es extraño ver aparatos como PDAs, teléfonos móviles o ordenadores portátiles que hacen posible este tipo de comunicación. Estas maquinas son cada vez más rápidas, más pequeñas y más funcionales. También han ido apareciendo en estos últimos años nuevas tecnologías de comunicación inalámbricas que dan soporte a este tipo de dispositivos. Las redes de área local inalámbricas pueden proporcionar un gran ancho de banda, pero están limitadas a un área geográfica pequeña. Por otra parte, tecnologías como GPRS o UMTS proporcionan cobertura en un área geográfica mucho mayor pero tienen como contrapartida un menor ancho de banda.

También se puede apreciar una nueva tendencia, y es la convergencia entre las tecnologías de transmisión de voz y de datos. Un punto fundamental para esta convergencia es el apoyo en un protocolo de transmisión común: el protocolo de Internet, IP. Este protocolo fue diseñado hace más de 20 años, por lo que la posibilidad de dispositivos móviles no fue tomada en cuenta.

Una dirección IP consta de dos partes, la parte que identifica a la subred y la parte que identifica al dispositivo. Los diferentes dispositivos de encaminamiento en Internet usan este prefijo de subred para entregar correctamente los paquetes a la subred adecuada, utilizando la parte de host para identificar al nodo al que van destinados los paquetes. Esta forma en la que los distintos dispositivos de encaminamiento manejan las direcciones, hace que el protocolo IP no se adapte bien a la movilidad. Si el nodo se mueve a un nuevo enlace, dentro de una nueva subred, el prefijo de subred cambia. Si el nodo no cambia su dirección IP, con un prefijo de subred que la identifique, la comunicación no es posible. Por lo tanto, el nodo necesita obtener una nueva dirección IP con un prefijo de subred válido.

Hay diversos métodos que permiten al nodo obtener una nueva dirección IP, como DHCP, pero estos métodos no permiten que se mantenga la misma sesión en la comunicación, por lo que el paso de una red a otra no se hace de una manera indetectable por el usuario, requisito que debería cumplir el protocolo que se encargue de la movilidad. Este protocolo es IP Móvil, y su versión basada en IPv6, llamada IPv6 Móvil.

Actualmente, esta tecnología es raramente usada, en parte porque hay poca necesidad para ella y en parte porque las implementaciones actuales, como MIPL, consumen una gran cantidad de ancho de banda, y requieren dos direcciones IP, algo que, en el caso de estar utilizándose las escasas direcciones IPv4, no se puede permitir. Sin embargo, IPv6 Móvil se espera que se convierta en una importante tecnología cuando las redes inalámbricas y IPv6 se extiendan ampliamente. Este protocolo permitirá el paso de una red inalámbrica de 3ª generación a un hot spot basado en Bluetooth o Wi-Fi (802.11b) de una manera totalmente transparente para el usuario.

1.1 **Objetivos del proyecto**

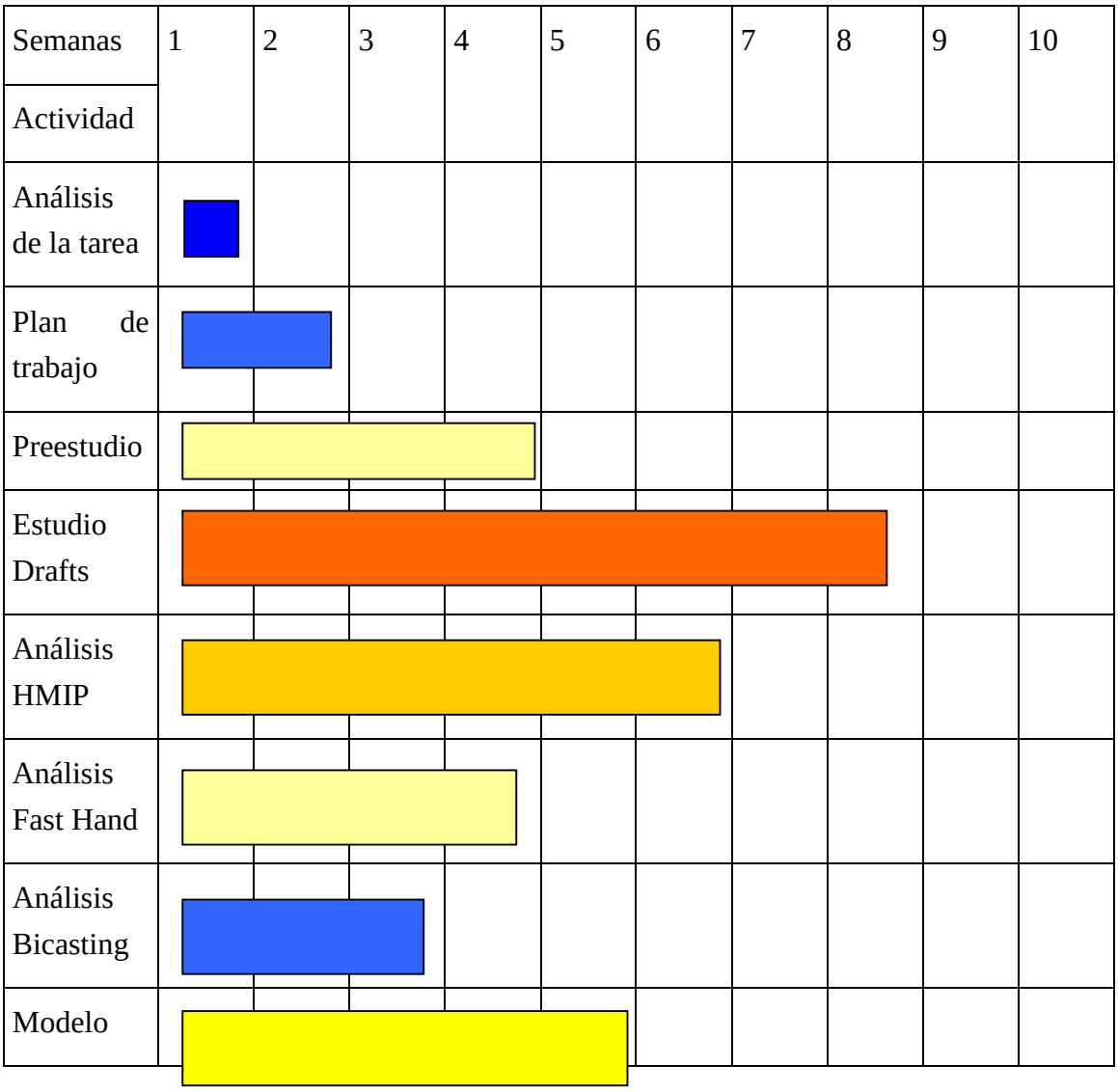
Este proyecto se basa en el estudio del protocolo IPv6 Móvil. Este protocolo asigna una nueva dirección IP válida al nodo que se encuentre fuera de su subred, y lo hace de manera que los protocolos de las capas superiores no son conscientes del cambio. Este protocolo también aprovecha las nuevas ventajas ofrecidas por IPv6, como las mejoras en las opciones de seguridad y movilidad, que se encuentran perfectamente integradas. En este proceso de cambio de subred, con el consiguiente cambio de dirección IP, o también llamado proceso de handover, el Nodo Móvil tiene que registrar su nueva dirección IP en su red propia, comunicación que puede llevar bastante tiempo, sobre todo en el caso de que el Nodo Móvil este lejos de su red habitual. Esta comunicación hace que el proceso de handover no sea indetectable por el usuario, lo que en ciertas ocasiones, como en el caso de estar utilizándose aplicaciones en tiempo real como voz o video, puede que no sea aceptable.

El objetivo del proyecto es analizar las nuevas extensiones al protocolo IPv6 Móvil, que son Fast Handover, Bindings Simultáneos e IPv6 Móvil Jerárquico, que tratan de minimizar el impacto del handover en las comunicaciones. Se estudiarán las

diferentes extensiones y se propondrán soluciones a las posibles deficiencias en el mismo. Se procederá también a la integración de las diferentes propuestas en una solución única, analizando las ventajas e inconvenientes de cada caso y centrándose siempre en el objetivo de dar soporte a aplicaciones en tiempo real como voz o video en el proceso de handover.

1.2 **Plan de trabajo**

El siguiente gráfico muestra el plan de trabajo seguido durante el proyecto, con las actividades programadas frente al numero de semanas dedicadas.



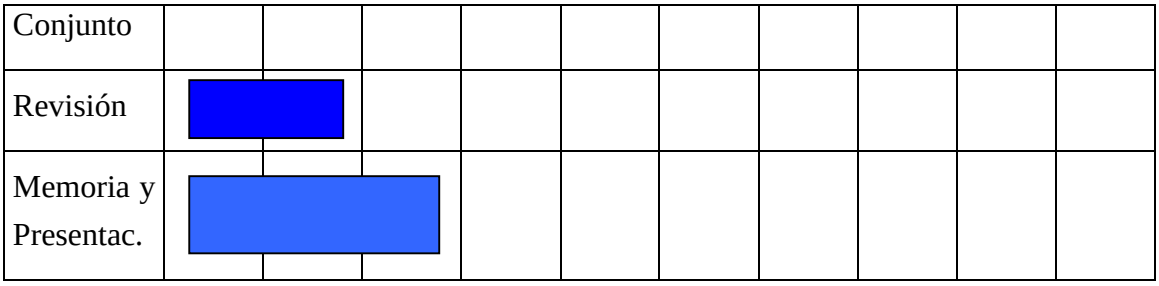


Figura 1: Esquema de trabajo seguido

1.3 Medios materiales

Para este proyecto se utilizaron ordenadores fijos y portátiles proporcionados por el IMIT, Departamento de Microelectrónica y Tecnología de la Información dentro del Real Instituto Tecnológico de Estocolmo, en Suecia. También se utilizaron las instalaciones de Ericsson, ya que fue el sponsor de este proyecto. La mayor parte del trabajo realizado se basa en el estudio y en el análisis teórico de diferente documentación, siendo parte fundamental de la misma el estudio de los drafts de la IETF. Por ello fue fundamental el acceso a Internet que permitió tanto la consulta de los drafts, como la búsqueda de nuevo material de estudio y la posibilidad de ponerse en contacto con personas que trabajaban en líneas de trabajo similares en universidades de todo el mundo

1.4 Organización de la memoria

La memoria está dividida en varios capítulos. A continuación se muestra un resumen de lo que se puede encontrar en cada apartado.

- Capítulo 1. Se hace una introducción al proyecto y los problemas que intenta resolver. Se explica el plan de trabajo seguido y los medios con los que se contó.
- Capítulo 2. Es una pequeña descripción de IPv6
- Capítulo 3. Se presenta el protocolo IPv6 Móvil.

- Capítulo 4, 5 y 6. Se presentan los drafts IPv6 Móvil Jerárquico, Fast Handover y Bindings Simultáneos.

- Capítulo 7. Se exponen una serie de propuestas que intentan solucionar los problemas existentes en IPv6 Móvil y mejorar las extensiones existentes. Se propone una integración de las extensiones y un protocolo de selección de MAP.

- Capítulo 8. Es una introducción a un producto comercial que utiliza los mismos métodos que IPv6 Móvil.

- Capítulo 9. Capítulo dedicado a las conclusiones generales y a la posible continuación del proyecto.

- En la parte final de la memoria aparece la bibliografía, un glosario de términos y dos apéndices con información sobre las aplicaciones en tiempo real y calidad de servicio.

Capítulo 2. Descripción de IPv6

2.1 Introducción

La Internet Engineering Task Force (IETF) empezó a estudiar ya en 1991 el problema del crecimiento de Internet y de la cantidad de direcciones IP que se necesitarían en un futuro. La necesidad de más direcciones IP fue algo que no cogió desprevenido a nadie, pero lo que si ha sorprendido es la necesidad de la utilización de estas direcciones en dispositivos tan dispares como teléfonos móviles y ordenadores portátiles. Actualmente, el éxito del despegue de este protocolo varía dependiendo del país. El mayor argumento para la migración de IPv4 a IPv6 es que el nuevo protocolo es capaz de proporcionar una mucha mayor cantidad de direcciones que el antiguo. Muchos países están sufriendo una gran escasez de direcciones IP, especialmente en Asia. Muchas compañías de esos países han solventado temporalmente este problema con el uso de servidores NAT (Network Address Translator), pero con el creciente número de usuarios de Internet, esta solución no es aceptable a largo plazo. Esta falta de direcciones no afecta por igual a todas las partes del mundo. Países como Estados Unidos no están muy a favor de la migración, ya que en un principio recibieron una gran cantidad de direcciones. Por ejemplo, un país con tantos habitantes como China, tiene menos direcciones IPv4 que algunas universidades de los Estados Unidos, como el MIT o Standford. En estos momentos se está viviendo cierto pesimismo sobre el despliegue de redes basadas en IPv6, debido sobre todo a que tanto las empresas como los ISPs (Internet Service Providers) no están muy dispuestas a afrontar la costosa remodelación de sus redes. Sin embargo, se están tomando muchas iniciativas, sobre por parte de empresas asiáticas, que están apostando por la migración a IPv6. Una cosa está clara, y es que IPv6 se convertirá es el estándar oficial en todo el mundo, la pregunta es cuándo.

2.2 Formato de las direcciones

La diferencia más importante con respecto a IPv4 es que IPv6 es capaz de proporcionar una cantidad mucho mayor de direcciones. Usa 128 bits en el espacio

de direcciones, en vez de los 32 bits que usa IPv4. Esto permitirá una densidad de $6*10^{23}$ direcciones por metro cuadrado de la tierra [STALLINGS], por lo que, aún con una asignación de direcciones muy ineficiente, este número parece ser más que suficiente. Las direcciones en IPv6 pueden ser de tres tipos diferentes: unicast, anycast y multicast.

Unicast. La dirección actúa como identificador de una única interfaz. Un paquete mandado a una dirección unicast es entregado a la interfaz definido por la dirección.

Anycast. Una dirección anycast hace referencia a varias interfaces, normalmente pertenecientes a nodos distintos. Un paquete mandado a una dirección anycast es entregado a una de las interfaces identificadas en esa dirección.

Multicast. Una dirección multicast también hace referencia a un grupo de interfaces. El paquete mandado a esa dirección es entregado a todas las interfaces identificados por la dirección

2.3 Formato de la cabecera

En IPv6, la base de la cabecera tiene una longitud fija, a la que se le pueden añadir varias extensiones. El tamaño de la cabecera fija es de 40 bytes, y cada extensión tiene un tamaño que tiene que ser múltiplo de 8 octetos.

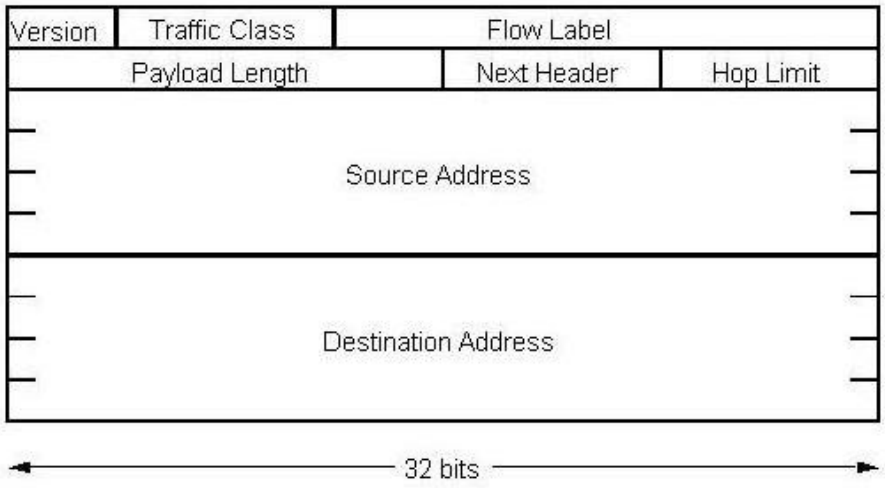


Figura 2: Cabecera fija en IPv6

Los campos en la cabecera IPv6 son los siguientes:

- Versión. (4 bits): Es la versión del protocolo. En este caso es 6.
- Clase de tráfico. (8 bits): Es el valor de prioridad para dicho paquete.
- Etiqueta de flujo. (20 bits): Puede ser usado para etiquetar a un conjunto de paquetes para los que se pide un tratamiento especial por parte de los routers.
- Longitud del paquete. (16 bits): Longitud del paquete exceptuando la cabecera, en octetos.
- Próxima cabecera. (8 bits): Identifica la próxima extensión que sigue a la cabecera fija.
- Limite de saltos (8 bits): Es el número de saltos restantes permitidos a este paquete. Es puesto a un determinado valor por el emisor y decrementado en 1 en cada salto.
- Dirección de origen-destino. (128 bits cada una): Las direcciones origen y destino del paquete.

Además de la cabecera fija, hay una serie de extensiones adicionales:

- Cabecera de opción salto a salto. Define opciones especiales para el procesamiento salto a salto del paquete.
- Cabecera de encaminamiento. Permite establecer un encaminamiento desde el origen.
- Cabecera de fragmentación. Proporciona información necesaria para la fragmentación y reensamblado.
- Cabecera de autentificación. Proporciona servicios de integridad y autentificación.

- Encapsulation Security Payload. Proporciona privacidad.
- Cabecera de opciones para el destino. Contiene información adicional que se examina únicamente en el nodo destino.

Capítulo 3. Descripción de IPv6 Móvil

3.1 Introducción

El protocolo IPv6 Móvil surge como una extensión al protocolo IPv6 para dar sopoerte a la movilidad. Esta sección describe el funcionamiento básico de este protocolo. Aparecen una serie de nuevos términos:

- Nodo Móvil: Es un nodo que tiene la capacidad de moverse de un enlace a otro.
- Home Network: Es la red donde el Nodo Móvil normalmente reside y donde se registra en el Home Agent
- Home Agent (HA): Es un nodo situado en la Home Network cuya función es coger los paquetes destinados al Nodo Móvil mientras éste esté en otra red, y mandárselos a la nueva localización.
- Correspondent Node (CN): Es el nombre que se le da a cualquier nodo genérico que se comunique con el Nodo Móvil.
- Foreign Network: Es una red, diferente a la Home Network, a la cual el Nodo Móvil puede acceder
- Home Address: Es la dirección del Nodo Móvil cuyo prefijo de subred pertenece a la Home Network.
- Care-of Address: Dirección que el Nodo Móvil obtiene en el nuevo enlace y cuyo prefijo de subred pertenece a la Foreign Network.
- Router de Acceso (RA): Es el último router en la jerarquía antes de llegar al Nodo Móvil.

El principio básico de este protocolo es el siguiente. Si el Nodo Móvil está en la Home Network, no tiene ningún problema para comunicarse con el Correspondent Node, ya que su dirección IP tiene un prefijo de subred válido. Pero si el Nodo Móvil entra en una red distinta, Foreign Network, la comunicación no será posible, ya que el prefijo de subred de su dirección IP no es correcto. Para que se establezca la comunicación, el Nodo Móvil obtiene una Care-of Address, con prefijo de subred válido, y registra está dirección en el Home Agent. Así, cuando el Correspondent Node quiera mandar un paquete al Nodo Móvil, y no es consciente de que ha cambiado de red, manda los paquetes a la Home Address del Nodo Móvil. Cuando el paquete llega a la Home Network, el Home Agent, lo intercepta, y los manda a la Care-of Address. El Nodo Móvil puede también registrar la Care-of Address en el Correspondent Node para habilitar así la comunicación directa. A continuación se describe con más detalle el protocolo IPv6 Móvil.

3. 2 Detección de cambio de enlace

El Nodo Móvil puede usar diferentes métodos para averiguar si se encuentra en un nuevo enlace. El primer método hace uso del protocolo IPv6 Neighbor Discovery, en donde se incluyen Router Discovery y Neighbor Unreachability Detection. El Nodo Móvil debe usar Router Discovery para descubrir nuevos routers dentro del nuevo enlace. Puede mandar el mensaje Router Solicitation o puede esperar a recibir los Router Advertisement, que son mandados a una dirección multicast de manera no solicitada. Basándose en la información recibida en el Router Advertisement, el Nodo Móvil mantiene una lista con todos los routers disponibles en el enlace, con información acerca de sus prefijos.

Cuando un Nodo Móvil se encuentra en la Foreign Network, selecciona un router de la lista de routers disponibles, y un prefijo para usar en la Care-of Address. Es importante que el Nodo Móvil sea capaz de detectar que el router seleccionado no está disponible, para así poder seleccionar otro. Para esto se utiliza Neighbor Unreachability Detection. Este mecanismo se basa en el envío por parte del Nodo Móvil del mensaje Router Solicitation y el recibo del mensaje Router Advertisement. Pero el Nodo Móvil no puede basarse solo en este mecanismo para averiguar que el router no está disponible, ya que el continuo envío de Router Solicitations podría

sobrecargar la red. Por lo tanto, mientras el Nodo Móvil esté recibiendo paquetes IPv6, sea del tipo que sea, se puede considerar que el router está disponible, sin necesidad de enviar Router Solicitations. De todas maneras, en el mensaje Router Advertisement se incluye el campo intervalo, que indica con que frecuencia el router va a mandar Router Advertisement sin solicitación previa.

3.3 Formación de una nueva Care-of Address

Después de que el Nodo Móvil haya detectado de que ha entrado en una nueva subred y ha encontrado un nuevo router disponible, el Nodo Móvil debe formar una nueva Care-of Address, usando uno de los prefijos anunciados en el Router Advertisement. Las especificaciones dicen que no se podrán registrar en el Home Agent más de una Care-of Address por segundo. El Nodo Móvil podrá formar más de una Care-of Address, pero sólo una podrá ser registrada en el Home Agent.

Para la formación de la Care-of Address, el Nodo Móvil puede usar Stateless Address Autoconfiguration o Stateful Address Autoconfiguration (como DHCPv6). En el caso de que el Nodo Móvil tenga que mandar paquetes para la formación de la dirección, debe usar un tipo especial de dirección, local al enlace, como dirección origen, en vez de su Home Address. En el caso de utilizar Stateless Address Autoconfiguration, esta dirección se formará uniendo el prefijo de subred con un identificador único del nodo, basado en la dirección MAC.

Después de formar la nueva Care-of Address, el Nodo Móvil debe efectuar Duplicate Address Detection (DAD) para asegurarse de la unicidad de la dirección. DAD manda un paquete Neighbor Solicitation para asegurarse de que esta dirección no se encuentra actualmente en uso. Si esto es así, no se recibirá ninguna respuesta a este mensaje. En cambio, si la dirección está siendo usada, el nodo que la usa responderá con un paquete Neighbor Advertisement, indicando que un nodo con esa dirección se encuentra en la red. Sin embargo, hacer esto representa un balance entre seguridad, sobrecarga de la red y tiempo, ya que el efectuar DAD requiere el envío de paquetes sobre lo que puede ser una red lenta, como es el caso de una red inalámbrica. Este método causa también un retraso en la utilización de la nueva Care-of Address, por lo que se podría retrasar de manera inaceptable el proceso de

handover. Se recomienda por tanto la realización del DAD en paralelo con la utilización de la dirección por parte del Nodo Móvil.

3.4 Mandando Binding Updates al Home Agent

Una vez que el Nodo Móvil haya formado la nueva Care-of Address, tiene que proceder al registro de la dirección en el Home Agent. El Nodo Móvil manda un paquete a su Home Agent conteniendo una opción Binding Update. Está opción viene incluida en la extensión de movilidad, definida en el nuevo protocolo IPv6. Este Binding Update hará una asociación entre la Home Address y la Care-of Address, por lo que todos los paquetes que lleguen a la Home Network destinados al Nodo Móvil, podrán ser interceptados por el Home Agent y ser redireccionados hasta la Care-of Address. Mientras el Nodo Móvil este fuera de su Home Network, su Home Agent participará en DAD para defender su dirección contra Stateless Address Autoconfiguration realizado en la Home Network.

El paquete Binding Update contendrá también el tiempo por el cual será válida la asociación entre las direcciones. Un Binding Update mandado al Home Agent sólo se diferenciará al mandado al Correspondent Node en que el campo que indica el registro en el Home Agent estará activado. Los Binding Updates al Home Agent deben de ser contestados con un Binding Acknowledgement, confirmando la llegada del Binding Update. Este paquete informa si la asociación se ha realizado con éxito y la posible causa del fallo, en el caso de que la asociación no sea posible.

3.5 Mandando Binding Updates a los Correspondent Nodes

Una vez que el Nodo Móvil haya obtenido la Care-of Address, puede enviar un Binding Update a los diferentes Correspondent Nodes, vinculando la Care-of Address con la Home Address. De esta manera, el Correspondent Node almacena en una cache, la Binding Cache, la Home Address de los Nodos Móviles junto con la Care-of Address. En el caso de que quiera mandar un paquete a algún Nodo Móvil, primero mira en la tabla para ver si hay alguna Care-of Address asociada a ese nodo, para así habilitar la comunicación directa, en vez de tener que enviar los paquetes a la Home Network, optimizando así la ruta seguida por los paquetes. Este Binding

Update tiene también un tiempo de vida, por lo que el Correspondent Node, cuando vea que el tiempo esté a punto de expirar, puede mandar un Binding Solicitation al Nodo Móvil, solicitando el envío de un Binding Update.

Los Binding Updates al Correspondent Node no necesitan responderse con Binding Acknowledgement. Es necesario solamente si así se indica en el paquete Binding Update.

3.6 Enviando y recibiendo paquetes en la Foreign Network

Cuando el Nodo Móvil quiera mandar paquetes una vez que se encuentre en la Foreign Network, debe poner como dirección origen la Care-of Address. Esto se requiere para evitar los problemas de routers que no dejan pasar el tráfico de nodos que no tengan una dirección que no pertenezca a la red en la que se encuentran. Para que el procedimiento permanezca transparente a las capas superiores, se incluye la Home Address del Nodo Móvil en la opción Home Address.

El Nodo Móvil podrá recibir paquetes por uno de los métodos siguientes:

- Los paquetes mandados por un Correspondent Node que no tenga entrada para el Nodo Móvil en la Binding Cache, serán enviados a la Home Address del Nodo Móvil. Una vez llegados a la Home Network, estos paquetes serán interceptados por el Home Agent y serán encapsulados usando un túnel hacia la Care-of Address. El Nodo Móvil al recibir este tipo de paquetes, debe enviar un Binding Update, para proceder a la comunicación directa.

- Si el Correspondent Node tiene una entrada en la Binding Cache, los paquetes serán enviados a la Care-of Address directamente. Para esto se utiliza la opción de IPv6 de encaminamiento, en donde se establece la Home Address como último salto.

Una vez que el Nodo Móvil llega a la Home Network, este debe mandar un Binding Update al Home Agent para indicarle deje de interceptar los paquetes destinados al Nodo Móvil. En este Binding Update aparecerá la Home Address como Care-of Address.

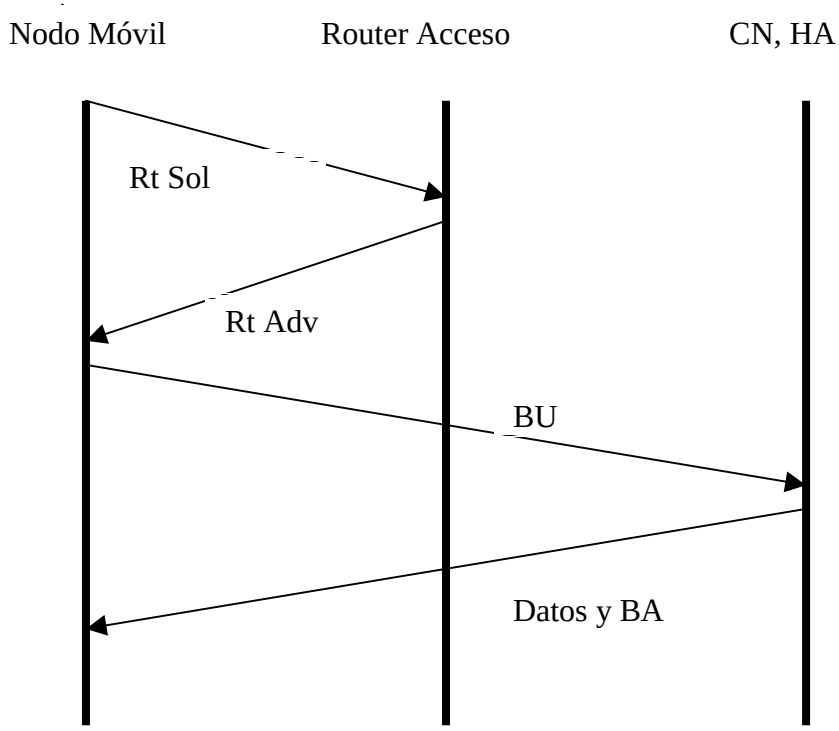


Figura 3: Flujo de paquetes en IPv6 Móvil

3.7 Seguridad

La seguridad es una de las tareas más difíciles a la hora de diseñar de una red. A pesar de que un análisis detallado de todos los riesgos a la seguridad y las posibles soluciones está fuera del objetivo del proyecto, en este apartado se presenta una introducción de los riesgos más importantes que se pueden presentar al usar MIPv6, y algunas de las soluciones propuestas.

Los posibles riesgos a la seguridad de MIPv6 son:

Riesgos de los Binding Updates mandados al Home Agent:

- El atacante puede que asocie la Home Address de un nodo con una Care-of Address que no pertenece a dicho nodo. El nodo víctima no recibirá los paquetes destinados a él ya que los paquetes se redirigiran a otra Care-of Address. El atacante podrá de esta manera recibir los paquetes que iban destinados al Nodo Móvil.

- Si el atacante asocia la Home Address del Nodo Móvil con la Care-of Address de otro nodo víctima, este último recibirá paquetes que no quiere, siendo esto una amenaza a la confidencialidad, disponibilidad y negación de servicio.

Riesgos de los Binding Updates a los Correspondent Nodes:

- El nodo atacante puede asociar su Care-of Address con la Home Address de la víctima, por lo que los paquetes dirigidos a la víctima serán mandados al atacante.

- El atacante puede unir la Care-of Address de la víctima con la Home Address del atacante, por lo que paquetes mandados en respuesta a paquetes mandados por el atacante se mandarán a la víctima, pudiéndose ocasionar problemas de negación de servicio.

- Un nodo atacante puede mandar una gran cantidad de Binding Updates a un Corresponent Node. Si el procesamiento de cada Binding Update consume una cierta cantidad de recursos, esto puede ser usado para causar negación de servicio.

- El atacante puede también mandar un antiguo Binding Update, por lo que los paquetes son mandados ahora a la antigua localización del nodo víctima.

La protección de los Binding Updates mandados al Home Agent y Correspondent Node requieren soluciones de seguridad distintas. El Nodo Móvil y el Home Agent se conocen mutuamente, y tienen una asociación de seguridad para autentificar los mensajes, por lo que en este caso se puede utilizar Ipsec Encapsulation Security Payload (ESP). Estos mensajes requieren control de integridad, correcto orden de entrega y protección ante el envío de paquetes antiguos, o replay attack.

IPv6 Móvil no confía únicamente en IPv6 para la protección contra los replay attack, por lo que proporciona sus propios mecanismos de defensa dentro de los Binding Updates y Binding Acknowledgement. Un campo con un número de secuencia asegura el correcto orden de entrega de los paquetes, utilizandose un esquema de ventana para dichos números de secuencia.

La protección de los Binding Updates mandados a los Correspondent Nodes es un problema mucho más difícil de solucionar. Se espera que IPv6 Móvil tenga un uso global, por lo que construir una infraestructura de autentificación es una tarea poco factible. Los Binding Updates mandados al Correspondent Node se protegen utilizando el método de Return Routability (RR). Cada Correspondent Node tiene una clave secreta (Kcn), que no comparte con ninguna otra entidad, por lo que no se requiere ningún mecanismo de intercambio de claves. Kcn puede ser un valor fijo o se puede actualizar regularmente. El Nodo Correspondiente puede generar un nuevo Kcn cada vez que arranca, para evitar así la necesidad de un almacenamiento seguro.

La señalización en RR es la siguiente:

- Cuando el Nodo Móvil quiere efectuar una optimización en el encaminamiento, es decir, mandar un Binding Update al Correspondent Node, manda un mensaje llamado Home Test Init (HoTI) al Correspondent Node. Este mensaje contiene la Home Address del Nodo Móvil. Este mensaje es mandado a través del Home Agent utilizando un túnel.

- El Nodo Móvil manda un mensaje llamado Care-of Test Init (CoIT) al Correspondent Node. Este mensaje se manda en paralelo con el mensaje

HoTI. Este mensaje contiene la Care-of Address del Nodo Móvil, y es mandado directamente al Correspondent Node.

- El Correspondent Node responde mandando un mensaje Home Test (HoT) al Nodo Móvil. Cuando el Correspondent Node recibe el mensaje HoTI, genera una cookie usando Kcn y la Home Address. Esta cookie se le manda al Nodo Móvil a través del Home Agent, probándose así que el Nodo Móvil puede recibir paquetes mandados a su Home Address.

- El Correspondent Node manda un Care-of Test (CoT) al Nodo Móvil. Este mensaje incluye una cookie generada usando Kcn y la Care-of Address. Este mensaje es mandado directamente al Nodo Móvil.

- El Nodo Móvil manda un Binding Update al Correspondent Node. Para ello ha tenido que esperar la llegada de los mensajes HoT y CoT, ya que tienen las cookies necesarias para el envío del Binding Update. Con estas cookies forma una clave válida para la sesión, que utilizará junto con el Binding Update, la Care-of Address y la Home Address para elaborar un código de autentificación. El Correspondent Node, que tiene información suficiente para reconstruir la clave de sesión, es ahora capaz de verificar el Binding Update mandado por el Nodo Móvil. Una vez que el mensaje ha sido verificado, se procede a la inclusión de una entrada con la Care-of Address en la binding cache.

Este protocolo evita que un Binding Update contenga direcciones pertenecientes a diferentes nodos. El Correspondent Node manda las cookies a través del Home Agent y directamente a la Care-of Address. Lo primero asegura que la cookie llegará a la Care-of Address que aparezca en la cache del Home Agent, asociación que se pude suponer correcta, ya que fue creada usando una asociación segura, Ipsec.

El Nodo Móvil necesita esas dos cookies para mandar un Binding Update que pueda ser aceptado por el Correspondent Node. Si la Home Address y la Care-of Address pertenecen a nodos distintos, el Nodo Móvil no recibirá las dos cookies por lo que su Binding Update no será aceptado por el Correspondent Node.

Este protocolo protege también contra ataques de respuesta, ya que los Binding Updates tienen por sí mismo un número de secuencia. También protege

contra la integridad, ya que el Binding Update no puede modificarse, ya que entonces el mensaje de autentificación no sería correcto. También protege contra ataques de negación de servicio, ya que el Correspondent Node no tiene que almacenar ningún estado de Binding Updates que no sean correctos.

Un problema de este protocolo es que pueda que sea lento, ya que requiere un intercambio de información entre el Nodo Móvil y el Correspondent Node, directamente y a través del Home Agent, y todo esto antes de poder mandar el Binding Update.

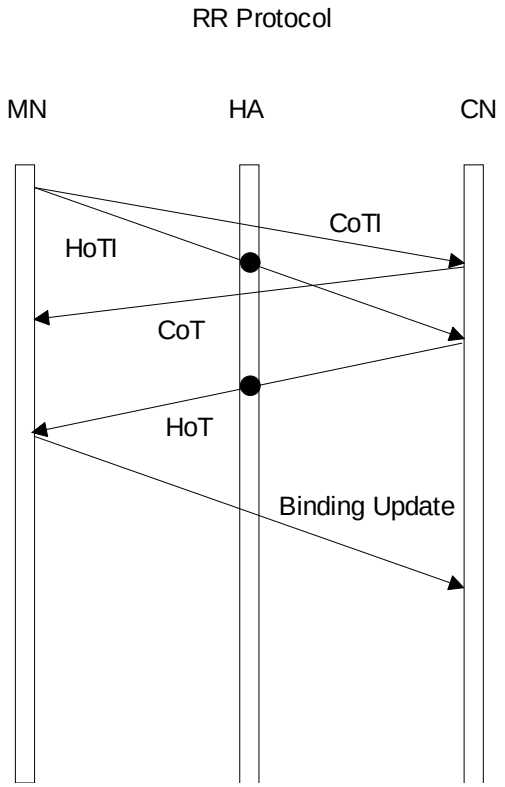


Figura 4 : Protocolo RR

3.8 Diferencias con IPv4 Móvil

El diseño de IPv6 Móvil se ha beneficiado de la experiencia acumulada en el desarrollo de IPv4 Móvil, y aprovecha las ventajas que brinda el hecho de utilizar IPv6. Los dos protocolos comparten muchas características, pero IPv6 Móvil está plenamente integrado en IPv6, y ofrece una gran cantidad de mejoras. A continuación se expone una lista con las principales diferencias entre los dos protocolos.

- No hay necesidad de utilizar routers especiales en la Foreign Network, como en el caso de los Foreign Agents en IPv4 Móvil.
- El soporte para la optimización del camino es una parte fundamental del protocolo, en vez de una serie de extensiones no integradas.
- Se ha eliminado el problema de IPv4 Móvil con los routers que hacían Ingress Filtering.
- La mayoría de los paquetes que se mandan al Nodo Móvil utilizan la cabecera de encaminamiento de IPv6, en vez de encapsulamiento IP, por lo que se reduce la sobrecarga debido a las cabeceras.
- IPv6 Móvil no depende de la capa 2, ya que usa Neighbor Discovery, en vez de ARP, por lo que se mejora la robustez del protocolo.

Capítulo 4. Fast Handover

4.1 Introducción

Durante el handover, se produce un periodo de tiempo durante el cual el Nodo Móvil no puede mandar o recibir paquetes debido a la falta de conexión de nivel 2 y 3. En algunos casos, este periodo de tiempo puede ser mayor que lo admitido para el soporte de aplicaciones en tiempo real, o aplicaciones sensibles al retraso de los paquetes. El draft de Internet, Fast Handover para IPv6 Móvil [FASTHO] , describe mejoras al protocolo IPv6 Móvil, cuyo principal objetivo es reducir el periodo de tiempo en el que se producen pérdidas de paquetes, dando a IPv6 Móvil soporte para aplicaciones en tiempo real.

El periodo de tiempo en el que el Nodo Móvil está sin conexión depende de multiples factores, siendo los más importantes los que se muestran a continuación:

- El elemento que realiza la decisión acerca del handover, que puede ser la red o el Nodo Móvil.
- La cantidad de información disponible acerca de las distintas entidades que intervienen en el proceso de handover, por ejemplo, el conocimiento de la dirección IP del nuevo Router de Acceso.
- El soporte que la capa 2 proporciona a la capa 3.
- Cuánto tiempo antes puede saber el Nodo Móvil que está a punto de entrar en una nueva red.
- La cantidad de tiempo que se emplea en realizar procedimientos como Neighbor Discovery, Duplicate Address Detection (DAD) o Stateful Address Autoconfiguration.

4.2 Tipos de Fast Handover

Se han definido dos diferentes mecanismos dentro de Fast Handover. El primero se llama Handover Anticipativo o Predictivo. En este tipo, se inicia el handover de la capa 3 cuando el Nodo Móvil tiene todavía conexión de nivel 2 en el antiguo enlace. En este escenario, o el Nodo Móvil o el Router de Acceso tienen que tener información acerca de la proximidad de un nuevo handover, y de la nueva subred a la que se va a entrar. El segundo tipo de handover es el Basado en Túnel. En este caso el Nodo Móvil espera a tener conexión de nivel 2 en el nuevo enlace, o incluso depués, para hacer el handover de nivel 3. Los paquetes llegan al nuevo enlace y se dirigen a la antigua Care-of Address hasta que el Nodo Móvil efectúe el handover de la capa 3. En este proyecto nos centraremos en el caso de Handover Anticipativo.

Handover Anticipativo. Este tipo de handover conlleva iniciar el handover de la capa 3 mientras todavía se tiene conexión de capa 2 en el antiguo enlace. Dos casos se pueden dar, dependiendo de si es el Nodo Móvil o Router de Acceso quien tiene la información del posible nuevo handover. En el caso de Handover Iniciado por la red, el antiguo Router de Acceso tiene la información de que el Nodo Móvil está a punto de realizar un handover y acerca de la red a donde se va a desplazar. Esta información es requerida antes de establecer conexión de nivel 2 en el nuevo enlace. Es el Router de Acceso antiguo quien inicia la señalización con el Nodo Móvil y con el nuevo Router de Acceso para empezar el handover de nivel 3. En el caso de Handover Iniciado por el Nodo Móvil, es este nodo quien tiene la información sobre la posibilidad del nuevo handover y quien inicia el proceso de señalización.

4.3 Mensajes que intervienen en el handover

Los siguientes mensajes se utilizan en Fast Handover:

- Router Solicitation Proxy. Este mensaje es mandado por el Nodo Móvil al Router de Acceso, en el caso de Handover Iniciado por el Nodo Móvil, para solicitar un mensaje Proxy Router Advertisement. Este mensaje indica al Router de Acceso que se está a punto de producir un cambio de red.

- Proxy Router Advertisement. Este paquete es el que comienza el proceso de señalización en el caso de Handover Iniciado por la Red, y es el que el Router de Acceso manda en respuesta al Router Solicitation proxy. En este mensaje se manda el prefijo de la subred en la que se está a punto de entrar, para que el Nodo Móvil pueda formar la nueva Care-of Address usando Stateless Address Autoconfiguration.

- Handover Initiation. Este es un mensaje mandado por el antiguo Router de Acceso al nuevo Router de Acceso. Se incluye en este mensaje la dirección de nivel 2 del Nodo Móvil, para ayudar al nuevo Router de Acceso a reconocer al Nodo Móvil cuando éste se conecte. Se incluye también la antigua Care-of Address, para que sea posible la redirección de los paquetes aún en el caso de que la nueva Care-of Address no sea válida. Y por ultimo, se incluye la nueva Care-of Address, formada utilizando Stateless Address Autoconfiguration y que será la dirección que el Nodo Móvil usará cuando esté en el nuevo enlace.

- Handover Ackowledgement. Este mensaje lo manda el nuevo Router de Acceso al antiguo en respuesta al mensaje Handover Initiation. El objeto de este mensaje es informar al antiguo Router de Acceso si la nueva Care-of Address ha sido aceptada.

- Fast Neighbour Advertisement. Este paquete es mandado por el Nodo Móvil al nuevo Router de Acceso para indicarle que ha llegado ya al nuevo enlace.

- Fast Binding Update. Este paquete es mandado por el Nodo Móvil al antiguo Router de Acceso relacionando la antigua Care-of Address con la nueva. De esta manera el antiguo Router de Acceso puede empezar la redirección de los paquetes que llegan destinados a la antigua Care-of Address al nuevo enlace.

- Fast Binding Acknowledgement. Este paquete se manda en respuesta al Fast Binding Update para indicar si la asociación de direcciones se ha efectuado de manera satisfactoria.

4.4 Flujo de paquetes

Primeramente, es el Nodo Móvil o el Router de Acceso quién detecta que el Nodo Móvil está a punto de realizar un cambio de red. En el caso de que sea el Nodo Móvil, este manda un Router Solicitation Proxy al Router de Acceso, que responde con un Proxy Router Advertisement. Este paquete se manda en primer lugar si es el Router de Acceso quién detecta que el Nodo Móvil va a entrar en una nueva red. El Proxy Router Advertisement puede indicar una de las siguientes posibilidades:

- El antiguo Router de Acceso no tiene información acerca del nuevo Router de Acceso, y responderá diciendo que el nuevo punto de enlace es desconocido.

- Puede ocurrir que el nuevo enlace esté controlado bajo el mismo Router de Acceso, el antiguo. En este caso el paquete indicará que el nuevo punto de enlace es conocido y que está bajo el control del mismo Router de Acceso. Esto puede ocurrir en el caso de que el Nodo Móvil se encuentre situado en una red inalámbrica, y se proceda a un cambio de celda, pero aún perteneciendo al mismo Router de Acceso.

- Si el nuevo punto de enlace es conocido y el antiguo Router de Acceso tiene información sobre él, la respuesta indica que el nuevo enlace es conocido. Este mensaje contiene también la Care-of Address que el Nodo Móvil debe utilizar en el nuevo enlace, o información sobre el prefijo de subred necesario para formar la Care-of Address.

A continuación el antiguo Router de Acceso pasa a verificar que es posible el handover utilizando la Care-of Address previamente formada. Para eso manda el mensaje Handover Initiation al nuevo Router de Acceso, que contiene la nueva y la antigua Care-of Address. Puede que ocurra que el mensaje anterior no disponga de una nueva Care-of Address, por lo que, en este caso, el nuevo Router de Acceso busca una nueva para el uso por parte del Nodo Móvil. En el caso de que el mensaje sí disponga de una nueva Care-of Address, el nuevo Router de Acceso pasa a validar dicha dirección.

El nuevo Router de Acceso responde al antiguo con un mensaje Handover Acknowledgement, conteniendo la nueva Care-of Address o el resultado de la comprobación de si la nueva Care-of Address propuesta por el antiguo Router de Acceso es válida. El momento en el que el antiguo Router de Acceso manda el Proxy Router Advertisement al Nodo Móvil depende de si se está usando Stateless o Stateful Address Configuration. En el caso de Stateful, el antiguo Router de Acceso obtiene una nueva Care-of Address a través del nuevo Router de Acceso al recibir el mensaje Handover Acknowledgement, como se describió anteriormente, así que el antiguo Router de Acceso debe esperar a recibir el mensaje Handover Acknowledgement antes de poder transmitir el Proxy Router Advertisement al Nodo Móvil. En el caso de utilizar Stateless Address Autoconfiguration el antiguo Router de Acceso puede mandar el Proxy Router Advertisement antes de recibir el Handover Acknowledgement.

Tan pronto como el Nodo Móvil recibe el Proxy Router Advertisement y obtiene una nueva Care-of Address, manda, antes de terminar la conexión de nivel 2 en el antiguo enlace, un Fast Binding Update al antiguo Router de Acceso, vinculando la nueva y la antigua Care-of Address. En respuesta al Fast Binding Update, el antiguo Router de Acceso manda un Fast Binding Acknowledgement al Nodo Móvil. Este paquete es mandado tanto al nuevo enlace como al antiguo y especifica el tiempo de validez del túnel establecido por el antiguo Router de Acceso entre este nodo y la nueva Care-of Address. El antiguo Router de Acceso espera la llegada del Fast Binding Update para empezar a mandar los paquetes a través del túnel al nuevo enlace, por lo que el Nodo Móvil debe esperar hasta el momento en que esté a punto de moverse realmente al nuevo enlace para mandar el Fast Binding Acknowledgement.

Cuando el Nodo Móvil llega al nuevo enlace y establece una nueva conexión de nivel 2, manda un Fast Neighbour Advertisement para avisar al nuevo Router de Acceso de que ya ha llegado al nuevo enlace, y que ya puede proceder a la entrega de paquetes destinados a él.

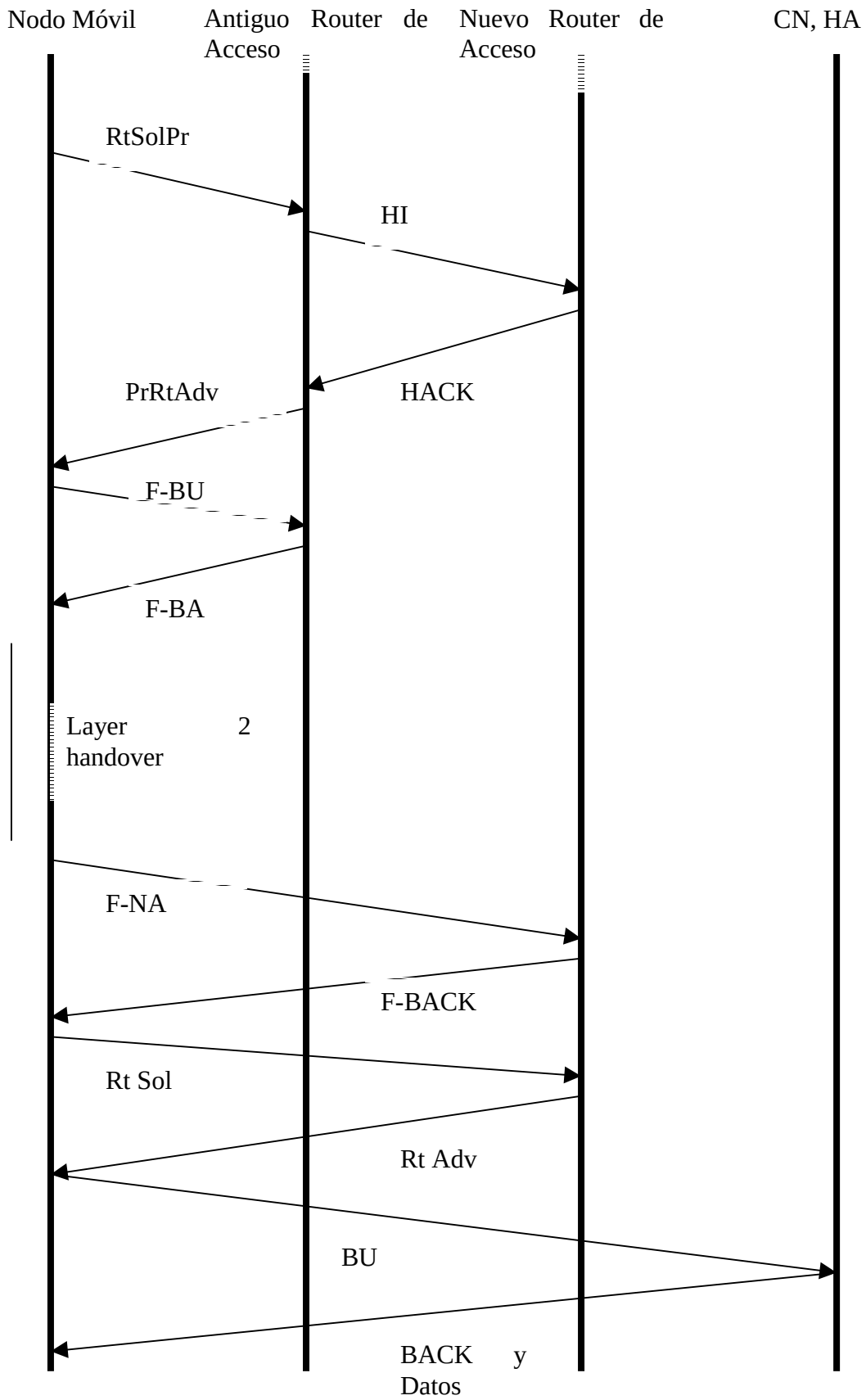
El antiguo Router de Acceso es responsable de la retransmisión de los paquetes que van destinados a la antigua Care-of Address del Nodo Móvil, hasta la nueva subred. Si el Handover Acknowledgement indica que el nuevo Router de Acceso acepta la nueva Care-of Address, el antiguo Router de Acceso retransmite los paquetes hasta la nueva Care-of Address. Si el nuevo Router de Acceso rechaza la

dirección, el antiguo Router de Acceso establece un túnel para la retransmisión de los paquetes hasta el nuevo Router de Acceso. En ambos casos, el antiguo Router de Acceso no empieza la retransmisión de los paquetes hasta que no ha llegado el Fast Binding Update.

Una vez que el Nodo Móvil llega al nuevo enlace y mandado el Fast Neighbour Advertisement, el Nodo Móvil sigue con los mismos pasos que el caso de un handover con IPv6 Móvil, que son el mandar el Router Solicitation, o esperar al Router Advertisement, y mandar el Binding Update al Home Agent y al Correspondent Node.

En este protocolo los triggers de nivel 2 cumplen un papel muy importante. Son los que deben informar al Nodo Móvil o al antiguo Router de Acceso de que se va a proceder a entrar en una nueva red. También deben informar al Nodo Móvil o al nuevo Router de Acceso de que el Nodo Móvil ha entrado en una nueva subred.

La sigiente figura (figura 5) muestra el flujo de señales en Fast Handover:


Nodo Móvil
Antiguo Router de Acceso
Nuevo Router de Acceso
CN, HA
RtSolPr
HI
PrRtAdv
HACK
F-BU
F-BA
Layer 2 handover
F-NA
F-BACK
Rt Sol
Rt Adv
BU
BACK y Datos

Capítulo 5. Bindings Simultáneos

5.1 Introducción

Fast Handover es una extensión al protocolo IPv6 Móvil que tiene como objetivo minimizar la interrupción de servicio al efectuar el handover. La extensión de Bindings Simultáneos [BICASTING] introduce una nueva mejora en el protocolo Fast Handover para minimizar el periodo de pérdida de paquetes. Una de las tareas a la hora de efectuar el handover es estimar el momento adecuado en el que se debe empezar la redirección de los paquetes desde el Router de Acceso antiguo hasta el nuevo enlace. Si la redirección se hace demasiado pronto o demasiado tarde con respecto al momento en el que el Nodo Móvil llega al nuevo enlace, se producen pérdidas de paquetes. La nueva funcionalidad introducida por la extensión de Bindings Simultáneos permite que el antiguo Router de Acceso retransmita los paquetes a varias localizaciones al mismo tiempo como son el antiguo enlace y el posible o los posibles nuevos enlaces.

Por lo tanto, el principal objetivo de la extensión Bindings Simultáneos es reducir el periodo de pérdida de paquetes y eliminar la ambigüedad de tiempo en relación a cuándo se debe proceder a la retransmisión de paquetes al nuevo enlace. Esto permite el desacoplo del handover de las capas 2 y 3, ya que no importa cuándo el Nodo Móvil hace el handover de la capa 2. El handover de la capa 3 se realiza previamente y los paquetes llegan a los dos enlaces, el nuevo y el antiguo, por lo que no se producen periodos de pérdidas.

5.2 Descripción

La única modificación con relación a los mensajes utilizados en Fast Handover es que se añade una nueva bandera al paquete Fast Binding Update, la bandera de Bindings Simultáneos.

Hay dos tipos de Bindings Simultáneos. El primero es el llamado Bicasting, que es el utilizado cuando se está tratando con aplicaciones sensibles a la pérdida de paquetes. Por este mecanismo, se mandan dos flujos de paquetes, uno hacia la red en la que actualmente se encuentra el Nodo Móvil, y el otro hacia la posible futura red. El segundo tipo de Binding Simultaneo es el llamado N-casting, en el que en vez de dos flujos de paquetes, se establecen varios. Esto se utiliza para evitar el fenómeno de movimiento de "Ping-Pong", en el que el Nodo Móvil se desplaza una y otra vez de un punto de acceso a otro con gran rapidez. Mandando los paquetes a todos los posibles routers de acceso se soluciona el problema.

Cuando un nodo recibe un Fast Binding Update con la bandera de Bindings Simultáneos activada, se debe de crear una nueva entrada en el Binding Cache para esta Care-of Address, pero sin reemplazar a ninguna de las entradas anteriores. Este paquete tiene también un campo llamado tiempo de vida de bicasting. Cuando este tiempo se acaba, el nodo tiene que dejar de mandar paquetes a la antigua dirección, borrando así la entrada para la antigua Care-of Address.

El inconveniente de esta solución es que si todos los paquetes se transmiten a varias localizaciones al mismo tiempo, esto puede causar congestión en la red, por lo que se debe decidir qué paquetes deben utilizar este método.

Capítulo 6. IPv6 Móvil Jerárquico

6.1 Introducción

El protocolo IPv6 Móvil ha sido diseñado para proporcionar movilidad a los usuarios que la requieren, siendo esta transparente a los protocolos de las capas superiores. Para conseguir esta trasparencia en la movilidad, el Nodo Móvil obtiene una nueva Care-of Address en cada punto de acceso, teniendo esta dirección un prefijo que define la exacta localización de la red en la que está situado el nodo, permitiendo así la correcta entrega de los paquetes por parte de los routers que conforman Internet. Sin embargo, uno de los objetivos más importantes de este protocolo, una movilidad transparente y no detectable por el usuario, se compromete por una falta de un rapido handover.

El Nodo Móvil tiene que obtener una nueva Care-of Address en cada nuevo enlace, y registrar esta dirección en el Home Agent, que puede que este bastante lejos del Nodo Móvil. Por esta razón, a veces, y dependiendo de la distancia relativa entre el Home Agent y el Nodo Móvil, handovers indetectables por el usuario no son posibles, debido a la gran cantidad de tiempo empleado en el proceso de mandar el Binding Update al Home Agent, proceso durante el cual las comunicaciones se interrumpen. Este punto ha sido objetivo de muchas críticas, y se han propuesto diferentes soluciones. La mayoría de estas nuevas mejoras propuestas intentan eliminar la dependencia con la distancia en el proceso de handover

Una de estas soluciones propuestas es IPv6 Móvil Jerárquico [HMIPv6]. Este nuevo draft, elaborado por Mobile-IP Working Group de la IETF (Internet Engineering Task Force) presenta algunas extensiones a los protocolos IPv6 Móvil y Neighbor Discovery, y trata de reducir los Binding Updates al Home Agent y Correspondent Node. Se utiliza un nuevo nodo, el llamado MAP (Mobility Anchor Point), que puede encontrarse a cualquier nivel en la jerarquía de routers, incluido el Router de Acceso. El funcionamiento de IPv6 Móvil Jerárquico, HMIPv6 está basado en los conceptos de Care-of Address regional y dominios del MAP. El dominio de un MAP está formado por todos los routers de acceso que anuncian la presencia de un MAP en concreto. Un Nodo Móvil en un dominio MAP tiene una

Care-of Address local, con el prefijo de red del enlace en el que se encuentra en ese momento. Tiene también una Care-of Address regional, válida en todo el dominio MAP. Cada vez que el Nodo Móvil tiene que efectuar un handover dentro del dominio MAP, sólo tiene que obtener una nueva link Care-of Address, específica para cada subred, y mandar un Binding Update al MAP, uniendo la Care-of Address regional con la link Care-of Address. El Binding Update al Correspondent Node y al Home Agent es sólo necesario cuando el Nodo Móvil sale fuera del dominio MAP. En este caso, el Nodo Móvil tiene que mandar un Binding Update a dichos nodos uniendo la Home-address con la nueva Care-of Address regional.

El MAP actúa como un Home Agent en el ámbito local. Recibe todos los paquetes que el Home Agent y el Correspondent Node han mandado a la Care-of Address regional y los manda a la Care-of Address local del Nodo Móvil. Es importante resaltar que cada Nodo Móvil dentro del dominio MAP tiene una única y exclusiva Care-of Address regional.

El concepto de MAP es simplemente una extensión al protocolo MIPv6. El Nodo Móvil puede elegir si utilizar o no HMIPv6 así como puede dejar de utilizar un cierto MAP en cualquier momento. Todo esto proporciona gran flexibilidad al funcionamiento del protocolo.

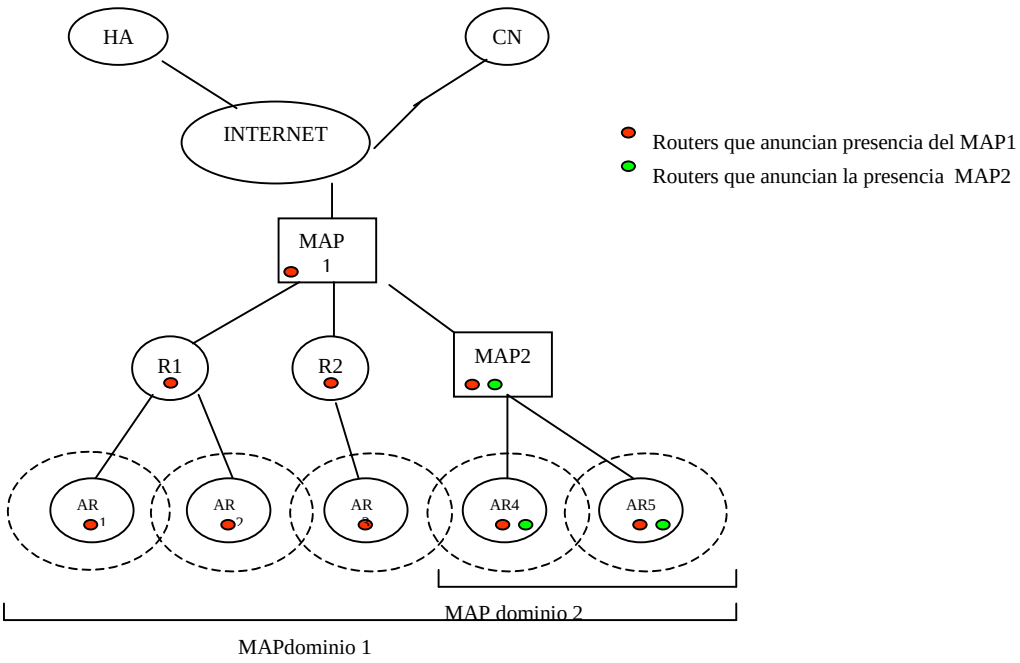


Figura 6: Ejemplo de arquitectura MAP

6.2 Extensiones de IPv6 Móvil

En el paquete Binding Update, se añade una nueva bandera, la bandera M, que indica registro en el MAP. Cuando un Nodo Móvil se registra en un MAP, la bandera M del correspondiente Binding Update debe activarse, para distinguirse de un registro en el Home Agent, o un Binding Update mandado a un Correspondent Node.

Se han introducido también nuevas extensiones en el Neighbor Discovery. Se han añadido nuevos campos y banderas a los paquetes que componen el Neighbor Discovery Protocol, formando así la opción MAP. Los campos más importantes dentro de esta opción son los siguientes:

- Distancia. Es un capo formado por un entero de 4 bits indicando la distancia desde el MAP hasta el nodo que recibe el paquete Router Advertisement. La distancia debe ponerse a 1 si el MAP y el Nodo Móvil están situados en el mismo enlace. Este número no debe ser interpretado como número de saltos, aunque el único requerimiento es que este valor sea interpretado consistentemente dentro del mismo dominio.

- Preferencia. Indica el valor de preferencia del MAP, indicado por un número del 1 al 15. Un valor de 15 representa la preferencia más baja, y puede ser usado por ejemplo, para indicar que el MAP está sobrecargado y que no puede soportar más tráfico.

- Dirección Global. Es una de las direcciones globales del MAP. La longitud del prefijo de subred debe ser de 64 bits.

- Tiempo de Vida. Este valor indica la validez de la dirección del MAP, y por consecuencia, el tiempo para la que la Care-of Address regional es válida.

- Distintas banderas indicando el modo de funcionamiento, modo básico o extendido, y cómo se forma la Care-of Address.

6.3 Funcionamiento de IPv6 Móvil Jerárquico

En esta sección se describirá cómo el Nodo Móvil obtiene la dirección del MAP y cómo los routers de acceso pueden descubrir los MAPs que están activos en un dominio en un determinado momento.

El MAP debe distribuir diferente información, como su dirección global, en la cual el prefijo de subred viene incluido. Está información es transmitida usando paquetes de Neighbour Discovery. Cuando el Nodo Móvil recibe este paquete, ya tiene toda la información para formar una nueva Care-of Address regional.

En estos paquetes hay también información acerca de la distancia a la que se encuentra el MAP y la preferencia. El valor que aparece en el campo distancia puede ser muy útil, ya que permite que el Nodo Móvil seleccione el MAP más lejano, reduciéndose la posibilidad de que salga del dominio MAP. El valor del campo preferencia puede ser utilizado por el MAP para indicar que en ese momento no se encuentra disponible, indicándolo así con un valor de 15.

En este paquete aparece también información acerca del modo de operación del MAP, básica o extendida.

Descubrimiento Dinámico del MAP se basa en la propagación de la opción MAP desde el MAP hasta el Nodo Móvil, a través de ciertos interfaces de los distintos routers de la jerárquía, previamente configurados manualmente para tal efecto. Cada router de la jerarquía debe incrementar en uno el valor del campo distancia después de recibir la opción MAP. Si el router era también un MAP, éste debe mandar su propia opción MAP en el mismo paquete.

Si el Nodo Móvil recibe información de diferentes MAP, éste se encuentra situado dentro de varios dominios MAP al mismo tiempo, y puede obtener una Care-of Address regional válida para cada uno de los MAPs, aunque sólo una de esas direcciones puede registrarse en el Home Agent.

6.4 Operaciones del Nodo Móvil

6.4.1 Modo Básico

En el modo básico el Nodo Móvil tiene dos direcciones, una Care-of Address regional y una on-link Care-of Address, o Care-of Address local. La Care-of Address

regional se forma combinando el prefijo de subred del MAP, que aparece en la opción MAP, con el identificador de interfaz del Nodo Móvil.

Deben configurarse dos nuevas direcciones cuando el Nodo Móvil se traslada a otro dominio MAP, una Care-of Address regional, con el prefijo de subred del nuevo MAP, y una on-link Care-of Address, con el prefijo de subred del enlace en el que se encuentra en ese momento el Nodo Móvil. Ambas direcciones se obtienen utilizando Stateless Address Autoconfiguration.

Más tarde, el Nodo Móvil manda un Binding Update al MAP, uniendo la Care-of Address regional con la Care-of Address local (on-link Care-of Address). El MAP tiene la opción de, a continuación, realizar un DAD, (Duplicate Address Detection), para la Care-of Address regional. Con este procedimiento se evita que se estén utilizando direcciones iguales. Si esa dirección no se está utilizando en ese momento, el MAP devuelve un BA al Nodo Móvil, indicando que el registro y la unión de las direcciones se ha completado correctamente. En el caso de que se produzca algún error en el proceso, el MAP devuelve un BA con el correspondiente código de error. El Nodo Móvil debe esperar al BA enviado por el MAP antes de proceder al registro de ninguna dirección en su Home Agent. Después de recibir el BA, el Nodo Móvil manda Binding Update al Home Agent y a los Correspondent Nodes, emparejando la Care-of Address regional con la Home Address.

De esta manera, el Home Agent y el Correspondent Node mandan los paquetes destinados al Nodo Móvil a la Care-of Address regional de dicho nodo. Estos paquetes llegan al MAP, que los intercepta utilizando proxy Neighbor Advertisement, y los envía por medio de un túnel a la Care-of Address local del Nodo Móvil, que procede a continuación a desencapsular dichos paquetes.

6.4.2 Modo extendido

Este modo funciona prácticamente igual que el modo básico. La diferencia es que, en este caso, el Nodo Móvil manda el Binding Update al MAP relacionando la Care-of Address local con la Home Address. El Binding Update mandado al Home

Agent y Correspondent Node asocia la Care-of Address regional con la Home Address.

Este modo de operación puede ser usado en diferentes escenarios, aunque el caso más destacable es el de las redes móviles. Puede darse el caso de una red móvil formada por un router móvil y varios nodos móviles. Si el router móvil, que actúa como MAP, no puede asignar una Care-of Address regional a cada uno de los nodos, podría dar a todos los nodos móviles la misma Care-of Address regional. En este tipo de escenario, es probable que la Care-of Address regional, que ha sido asignada a todos los nodos, sea la Care-of Address obtenida por el router móvil, y que las Care-of Address locales de los nodos móviles no sean topológicamente correctas.

Para estos casos, HMIPv6 en modo extendido se adapta perfectamente a las necesidades del problema. El Nodo Móvil registra la Care-of Address local y la Home Address en el router móvil, que está actuando como MAP, y también registra la Care-of Address regional, que es la misma para todos los nodos, y la Home Address en el Home Agent y Correspondent Node.

Por lo tanto, cuando el Home Agent o Correspondent Node quieren mandar un paquete al Nodo Móvil, primero se lo mandan a la Care-of Address regional, que es la Care-of Address topologicamente correcta del router móvil. Éste, dependiendo de la Home Address del paquete recibido, mandará dicho paquete a la Care-of Address local del Nodo Móvil correspondiente, atendiendo a la relación de direcciones que aparezca en su Binding Cache.

Este modo de operación puede tener varias ventajas con respecto al modo básico de funcionamiento. Para simplificar el funcionamiento, solo un modo de operación es válido al mismo tiempo.

En el modo básico, los paquetes son interceptados por el MAP y son encapsulados de nuevo. En el modo extendido, el MAP primero desencapsula el paquete y lo vuelve a encapsular de nuevo, por lo que sólo se requiere una cabecera IPv6 adicional, en contra de las dos cabeceras IPv6 necesarias en el modo básico. Si la compresión de cabecera no está siendo utilizada, esto puede ser un importante punto a tener en cuenta.

En el modo básico, el Nodo Móvil tiene que esperar al BA, y éste es mandado normalmente después de haberse efectuado un DAD con la Care-of

Address regional por parte del MAP. En el modo extendido, esto no es necesario, ya que el Nodo Móvil registra la Home Address en el MAP, no la Care-of Address regional. Si se espera que el Nodo Móvil realice muchos inter-MAP handovers, este modo de operación debería tomarse en cuenta.

6.5 Descripción del flujo de paquetes

El esquema de la figura 7 muestra el flujo de paquetes en HMIPv6

- El Nodo Móvil, al entrar en el dominio de un nuevo Router de Acceso espera a recibir el paquete Router Advertisement.

- Cuando el Nodo Móvil ha recibido el paquete Router Advertisement, ya puede configurar sus nuevas direcciones, on-link Care-of Address y Care-of Address regional, esta última en el caso de que haya ocurrido un inter-MAP handover. Estas direcciones se forman utilizando Stateless Address Autoconfiguration, uniendo el prefijo anunciado en el paquete Router Advertisement con un identificador único, basado en la dirección MAC. Ahora el Nodo Móvil puede mandar el Binding Update al MAP, relacionando la Care-of Address local con la Care-of Address regional, en el modo básico, y la Care-of Address local con la Home Address en el modo extendido.

- En el modo básico, el MAP debe efectuar DAD con la recién formada Care-of Address regional, en el caso de que un inter-MAP handover ocurra. A continuación, el MAP manda un BA al Nodo Móvil. En el caso de un Intra-MAP handover, el handover termina en este momento.

- Cuando el Nodo Móvil recibe el BA, puede mandar el Binding Update al Home Agent y Correspondent Node.

- A continuación, el Home Agent y Correspondent Node pueden mandar paquetes al nuevo MAP, incluido el paquete BA.

A continuación se muestra un gráfico con el flujo de paquetes en HMIPv6 en el caso normal.

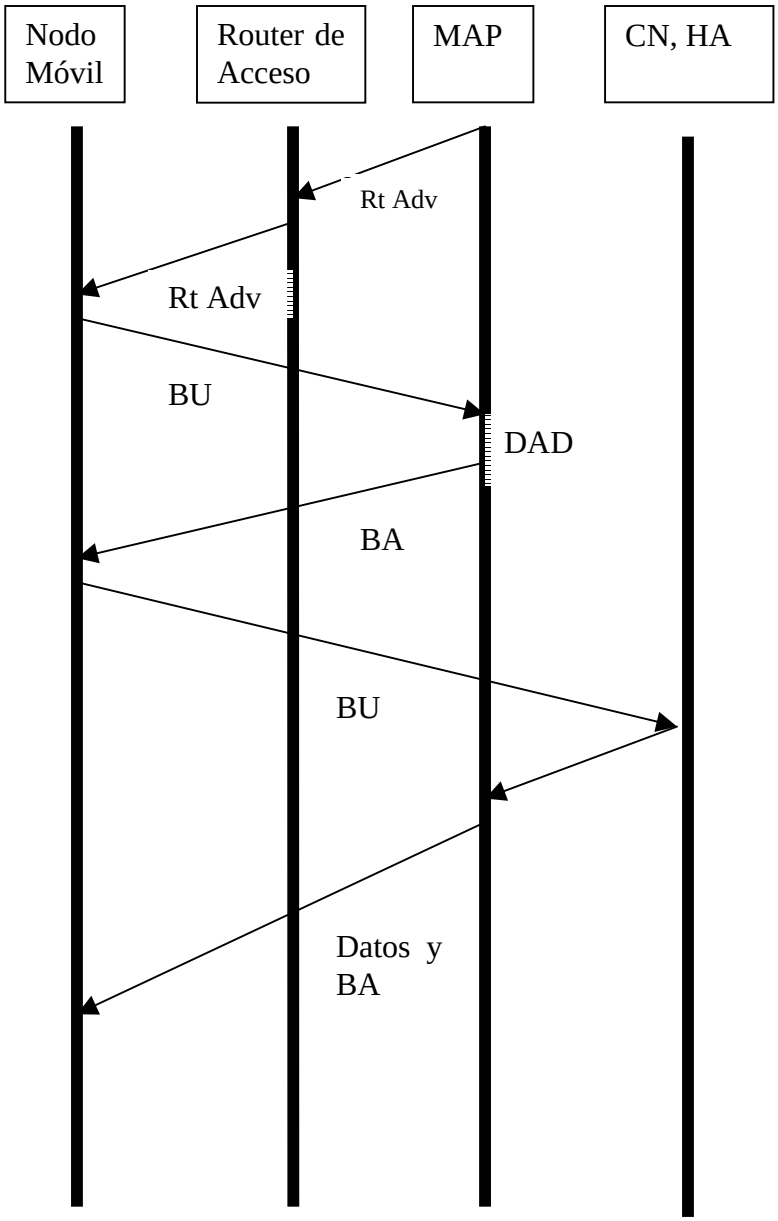


Figura 7. Diagrama de flujo de HMIPv6 en el caso normal

Con este esquema de handover, hay periodos de tiempo en los que se producen pérdidas de paquetes. A continuación se muestra una cantidad aproximada del tiempo en el que se producen dichas perdidas, aunque hay que tener en cuenta que estas cantidades nos dan sólo una idea del orden de magnitud de tiempo, por lo que no se deben tomar como valores de referencia.

Para el caso de un Intra-MAP handover (handover dentro del mismo MAP):

- Tiempo 1: Paquetes en vuelo desde el MAP hasta el Nodo Móvil. (1-2 ms).

- Handover de la capa 2. (100 ms). Este tiempo dependerá en gran medida de la tecnología que se esté empleando en la capa 2. En esta estimación de tiempo se ha considerado que en el nivel 2 se está utilizando una Wireless LAN IEEE 802.11 b.

- Tiempo para mandar un Binding Update. (50-1500 ms). Este tiempo puede llegar a ser importante. Es el tiempo que tarda el Nodo Móvil en darse cuenta de que ha entrado en una nueva red y de obtener los prefijos necesarios para formar las Care-of Address. Como no se está utilizando ningún trigger de nivel 2, el conocimiento de que se ha entrado en una nueva red depende unicamente del paquete Router Advertisement, mandado por el Router de Acceso por lo que finalmente, este tiempo depende de la frecuencia en la que estos paquetes son mandados, llegando a ser de hasta 1.5 segundos según las especificaciones.

- Tiempo hasta que el MAP recibe el Binding Update. (1-2 ms) Este tiempo suele ser pequeño, ya que normalmente el MAP se encuentra situado cerca del Nodo Móvil, aunque por supuesto, esto depende también de otros factores como el tipo de enlace, la congestión, etc…

- Tiempo que tarda el MAP en efectuar el DAD. (0-2000 ms). Aunque efectuar el DAD no es obligatorio, sí aparece como recomendable en las especificaciones, y puede llegar a durar del orden de segundos.

Por lo que haciendo balance de los tiempos de pérdidas, se obtiene una previsión optimista de unos 150 ms y otra pesimista de 3.6 segundos. Hay que reseñar que este último valor es tan grande debido fundamentalmente a dos factores, el DAD y la espera del Router Advertisement.

En el caso de un Inter-MAP handover:

En el caso de un Inter-MAP handover, al tiempo que tarda en caso de Intra-MAP, hay que añadir:

- Tiempo que tarda el Nodo Móvil en recibir el BA por parte del nuevo MAP. (1-2 ms).
- Tiempo que tarda el Home Agent y Correspondent Node en recibir el Binding Update . (2.5-75 ms) Este valor tiene este amplio rango porque depende de la distancia a la que se encuentre el Nodo Móvil del Home Agent. Este valor puede ser del orden de los 75 ms en el caso de que el paquete tenga que atravesar un enlace transoceánico.

Capítulo 7. Mejoras propuestas

7.1 IPv6 Móvil Jerárquico

7.1.1 Optimización del flujo de mensajes

El tiempo que el Nodo Móvil emplea en efectuar el handover se puede reducir si se toman en cuenta las siguientes consideraciones.

Para que el Nodo Móvil sepa que ha llegado a una nueva subred, debe esperar a recibir el paquete Router Advertisement. Esto puede que conlleve bastante tiempo, ya que el tiempo mínimo que tiene que esperar un router para mandar un Router Advertisement es de 3 segundos, según el protocolo Neighbour Discovery. Por esta razón, el draft de MIPv6 recomienda reducir este tiempo a un mínimo de 0.05 segundos, y a un máximo de 1.5 segundos. El tiempo que tarda el Nodo Móvil en darse cuenta de que ha llegado a una nueva red depende fundamentalmente de este parámetro. Se puede conseguir una considerable mejora en este respecto si el Nodo Móvil puede recibir información de la capa inferior a la capa 3, la capa 2. Esta información vendría dada en forma de triggers, señal que la capa 2 manda a la capa superior para indicarle que algún hecho ha ocurrido o está a punto de ocurrir, como por ejemplo, que se está a punto de abandonar un enlace, o que se acaba de iniciar una conexión de nivel 2 en un nuevo enlace. Con esta información, no habría necesidad de esperar al Router Advertisement, por lo que la detección de que se ha entrado en un nuevo enlace no depende del parámetro de espaciamiento temporal de dichos paquetes, que puede ser del orden de magnitud de segundos [JONASWILLEN]. Esta optimización depende por tanto de que el Nodo Móvil reciba unos triggers procedentes de la capa 2 informando que se ha establecido conexión en un nuevo enlace. Justo después de recibir este trigger, el Nodo Móvil manda un paquete de Router Solicitation.

En el caso de un Inter-MAP handover, después de recibir el paquete de Router Advertisement, el Nodo Móvil manda un Binding Update al antiguo MAP, uniendo la anterior Care-of Address regional con la recién formada Care-of Address local. El antiguo MAP puede ahora redirigir los paquetes dirigidos a la antigua Care-

of Address regional a la nueva Care-of Address local, reduciéndose así el periodo de perdida de paquetes.

El MAP puede emplear una gran cantidad de tiempo en la realización del DAD, con valores que pueden alcanzar hasta 5 segundos. Este tiempo pasa a no tener importancia si el paquete nombrado en el punto anterior se mandó. También el MAP puede mandar el BA al Nodo Móvil y efectuar el DAD en paralelo, aunque si se sigue esta opción, una gran cantidad de tiempo se malgasta si finalmente la nueva Care-of Address regional no pasa el DAD. Este mismo procedimiento puede también emplearse en el caso de que se quiera realizar un DAD con la nueva Care-of Address local en el nuevo link. El Nodo Móvil puede mandar el Binding Update a la vez que se efectúa el DAD.

Otro método a utilizar para reducir el tiempo que se tarda en efectuar un DAD es que el MAP tenga una caché interna con una lista de todos las Care-of Address regionales utilizadas en un momento determinado. El MAP puede determinar si la Care-of Address regional está en uso en cierto momento, y esto requeriría muy poco tiempo comparado con el DAD. En este caso, el MAP esperaría al resultado del chequeo para mandar el BA.

El Nodo Móvil puede mandar un Binding Update al Home Agent y Correspondent Node al mismo tiempo que manda el Binding Update al MAP. En este caso, el Nodo Móvil no espera el resultado del DAD y se puede producir una considerable perdida de tiempo si finalmente la dirección no pasa el DAD.

Siguiendo esta optimización se reduce drásticamente el periodo de tiempo en el que se producen pérdidas de paquetes, quedando casi únicamente el tiempo que tarda el Nodo Móvil en hacer un handover de la capa 2, que se estimo en unos 100 ms. Está reducción en el tiempo de perdida de paquetes es debido al hecho de que no fue necesario esperar al Router Advertisement, para lo que se utilizó un trigger de la capa 2. La otra reducción significativa viene dada por el hecho de que no se gasta tiempo en realizar un DAD, sino que se emplea uno de los métodos explicados anteriormente, siendo probablemente el de la caché el más eficaz.

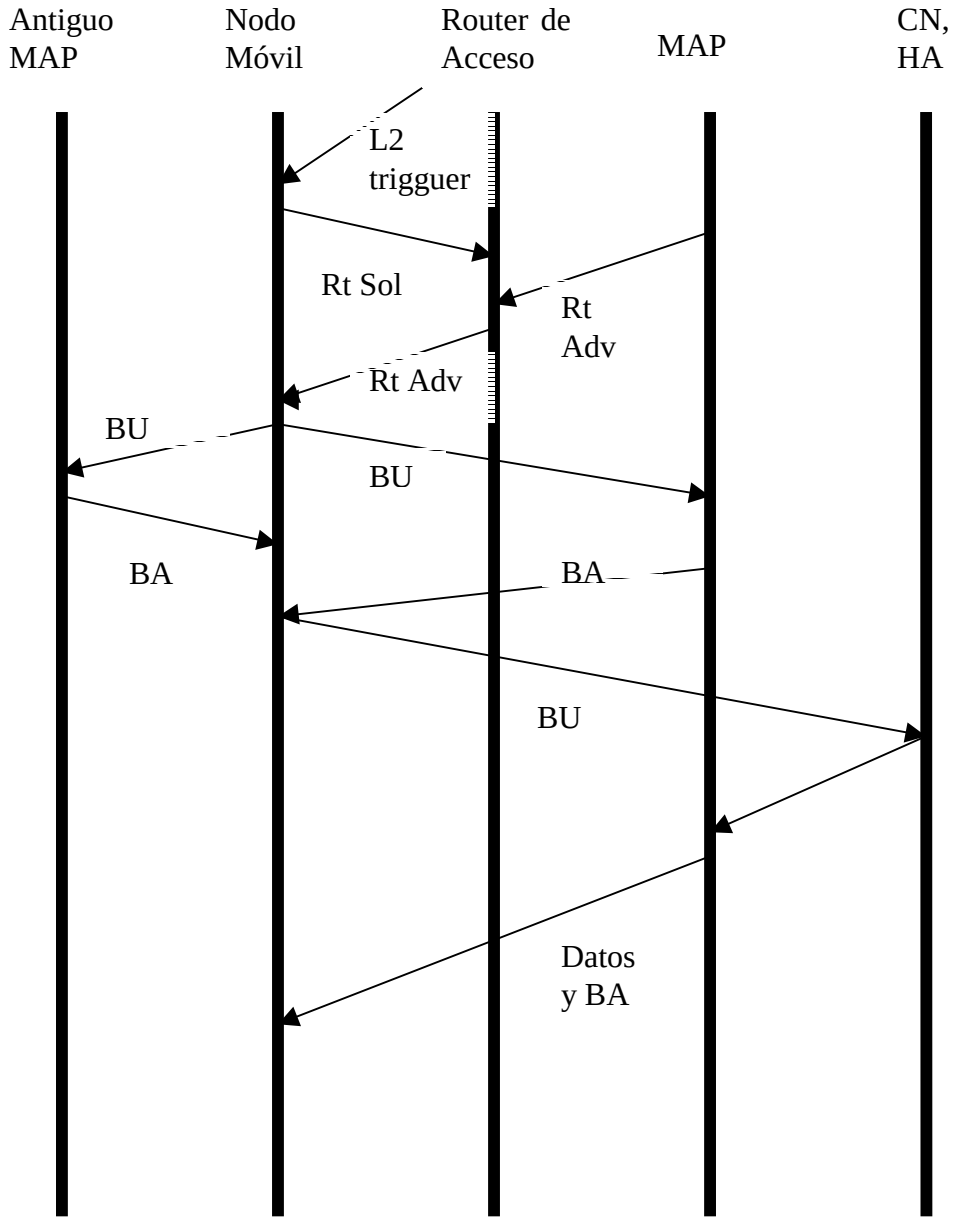


Figura 8. Diagrama de flujo de HMIPv6 mejorado

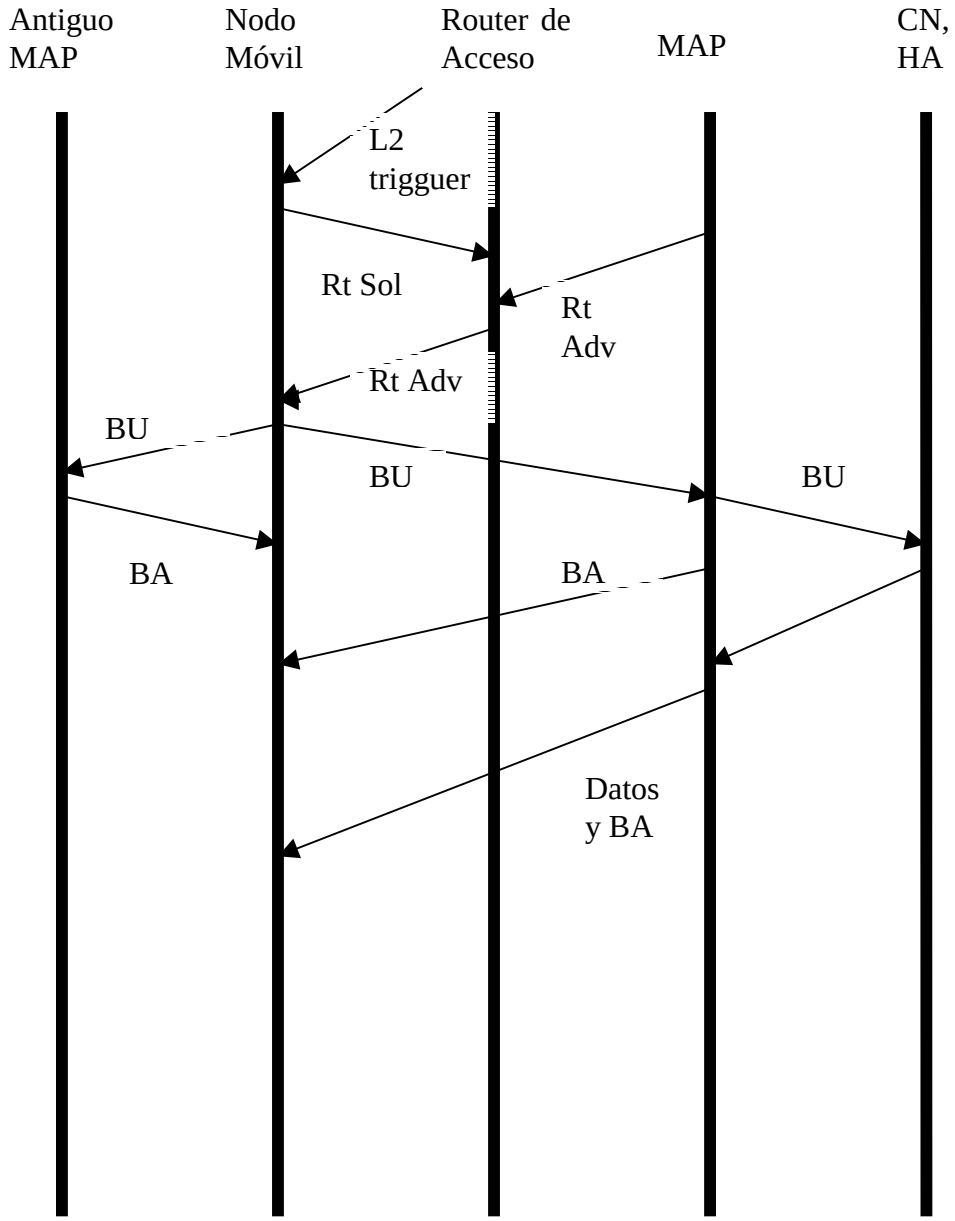


Figura 9 Diagrama de flujo mejorado con Binding Update directo al Home Agent y Correspondent Node

7.1.2 Conclusiones

El uso de HMIPv6 en vez de MIPv6 puede traer muchas ventajas, aunque por supuesto, no todo es bueno. Hay también algunas desventajas que deben tenerse en consideración. A continuación se enumeran las ventajas y desventajas derivadas del uso de HMIPv6 en relación con MIPv6.

7.1.2.1 Ventajas

- Reduce el número de Binding Update mandados al Home Agent y Correspondent Node. En el caso de Intra-MAP handover, sólo es enviado un Binding Update, el que se manda al MAP, en comparación con el caso de MIPv6, en el cual es necesario un Binding Update para el Home Agent y para Correpondent Node. En HMIPv6 sólo es necesario mandar el Binding Update al Home Agent y al Correspondent Node en el caso de inter-MAP handover. Si este tipo de handover no es muy frecuente, hay una considerable reducción del número de paquetes mandados, que en algunos casos, como por ejemplo, el de un canal inalámbrico, puede significar una gran ventaja al dejar libre ancho de banda, que en este tipo de enlaces es un recurso escaso.

- El uso de HMIPv6 puede reducir el tiempo de handover. El Binding Update tiene que ir sólo desde el Nodo Móvil al MAP. En el caso de un handover en MIPv6, el Binding Update tiene que llegar hasta el Home Agent o el Correspondent Node, que puede que esté lejos del Nodo Móvil. En el caso de inter-MAP handover es necesario mandar un Binding Update al Home Agent y Correspondent Node, pero si se mandó un Binding Update al antiguo MAP relacionando la antigua Care-of Address regional con la nueva Care-of Address local, el antiguo MAP puede empezar a redireccionar los paquetes que llegan a la antigua Care-of Address regional a la nueva Care-of Address local. Con este procedimiento, el periodo de tiempo en el que se producen pérdidas de paquetes se reduce.

- HMIPv6 es independiente de la tecnología subyacente en las capas inferiores. El único requerimiento es el uso de triggers de nivel 2 en la versión mejorada.

- Este nodo es adecuado para implementar control de acceso.

- En el caso de intra-MAP handover, sólo el camino desde el MAP hasta el Nodo Móvil cambia. Esto puede ser importante cuando se usan protocolos de Calidad de Servicio basados en la reserva de recursos a través del camino desde el Correspondent Node al Nodo Móvil. Si solamente esta parte del camino cambia, sólo es necesario reservar nuevos recursos en la parte nueva del camino, dejando el resto tal como estaba, por lo que el proceso de establecer un nuevo camino con todos los recursos reservados se acelera.

7.1.2.2 Desventajas

- Puede ser un punto de congestión. Todas las comunicaciones dentro del dominio MAP pasan a través del MAP, lo cuál puede deteriorar el rendimiento de las comunicaciones. En el algoritmo propuesto en el draft para elegir el MAP, se selecciona el más lejano en la jerarquía, lo cuál significa que este MAP puede tener un gran número de Nodos Móviles en su dominio. Para solucionar este problema, un campo en la opción MAP del Router Advertisement indica la disponibilidad del MAP, indicándo con un valor de 15 que el MAP no está disponible en ese momento. Anteriormente se propuso un algoritmo para solventar este problema, y otras soluciones han ido apareciendo con el mismo propósito. [MIPV6 MOBMANAGEMENT]

- El MAP se convierte en un punto único de fallo. Debido a que todas las comunicaciones pasan por el MAP, el fallo de éste acarrearía la interrupción de todas las comunicaciones con los Nodos Móviles dentro de su dominio. El uso de dominios MAP solapados puede solucionar este problema.

- El inter-MAP handover puede llevar mucho tiempo si los dos dominios MAP están topologicamente lejos.

7.2 Integración de los drafts.

7.2.1 Introducción

Se han propuesto diferentes métodos para mejorar el funcionamiento del protocolo IPv6 Móvil. El mayor defecto de este protocolo es que hay un periodo grande de tiempo en el proceso de handover durante el cual se producen pérdidas de paquetes. Esto ocurre porque el Nodo Móvil tiene que comunicarse con el Home Agent o el Correspondent Node, que pueden encontrarse bastante lejos. Esta comunicación retrasa significativamente el proceso de handover, y pueden aparecer periodos de tiempo en lo que el servicio se interrumpe. Este comportamiento puede que no sea tolerable para aplicaciones en tiempo real.

Para mejorar el comportamiento de IPv6 Móvil frente al handover se han propuesto diversas extensiones, como son las descritas anteriormente, IPv6 Móvil Jerárquico, Fast Handover y Bindings Simultáneos. Estos protocolos tratan de solventar el problema de la pérdida de paquetes, cada uno utilizando diferentes métodos. Pero estos protocolos tienen también varias desventajas, por lo que se hace ncesaria una combinación de estos protocolos para mejorar el comportamiento ante el handover y disminuir las desventajas de cada protocolo por separado.

HMIPv6 introduce un nuevo nodo, el MAP. El Nodo Móvil puede comunicarse con el MAP en vez del Home Agent y Correspondent Node, haciendo el proceso de Handover mucho más rápido. También reduce el ancho de banda utilizado en el enlace inalámbrico, debido a que en el caso de intra-MAP handover, sólo se tiene que mandar un Binding Update al MAP, a diferencia de MIPv6, en el que se tiene que enviar un Binding Update al Home Agent y al Correspondent Node. Pero a pesar de estas grandes mejoras, hay un periodo grande de tiempo en el que se producen pérdidas de paquetes. Esto es debido al hecho de que el handover de la capa 3 empieza después de haberse completado el handover de la capa 2. Aunque se ha propuesto en este documento, un método para reducir el tiempo de handover, es necesaria la combinación con otros protocolos que intentan realizar el handover de la capa 3 antes de que termine el handover de la capa 2.

Esto lo realiza el protocolo Fast Handover. En este protocolo, el Nodo Móvil obtiene una nueva Care-of Address local para el nuevo Router de Acceso cuando

todavía tiene conexión con el antiguo Router de Acceso. Cuando el Nodo Móvil llega al nuevo enlace y establece la conexión de nivel 2, puede restablecer la comunicación, ya que ya tiene una Care-of Address local válida para ese enlace. Mientras el Nodo Móvil manda un Binding Update al Home Agent y al Correspondent Node, los paquetes que llegan al router de acceso antiguo son redireccionados hasta la nueva Care-of Address local.

El hecho de que tenga que mandar un nuevo Binding Update al Home Agent y al Correspondent Node en cada Handover, aunque no implique pérdida de paquetes, hace que se malgaste una gran cantidad de ancho de banda, recurso escaso en enlaces inalámbricos.

Otra desventaja importante del Fast Handover es que requiere la sincronización de la redirección de los paquetes con el paso del Nodo Móvil de una red a otra. Si la redirección se hace demasiado pronto, se produce pérdida de paquetes, ya que éstos llegan al nuevo enlace y el Nodo Móvil no esta allí todavia. Si la redirección se realiza demasiado tarde, el Nodo Móvil llega al nuevo enlace y no recibe ningún paquete. Para solucionar este problema se propone el uso de Bicasting y de un buffer para almacenar los paquetes que llegan al nuevo Router de Acceso.

Con el uso de Bicasting, el antiguo Router de Acceso redirecciona los paquetes a la nueva Care-of Address local y al mismo tiempo sigue mandando paquetes a la antigua Care-of Address local permitiendo el desacoplamiento con el handover de la capa 2, y el momento del movimiento del Nodo Móvil al nuevo enlace. Es necesario un buffer para guardar los paquetes mandados al nuevo enlace, y que el Nodo Móvil no ha podido recibir al estar efectuando el handover de nivel 2.

7.2.2 Esquema Propuesto

Con todo lo expuesto anteriormente, cabe la posibilidad de obtener un mejor funcionamiento de MIPv6 con una solución que integre los tres protocolos mencionados. El esquema propuesto consiste en utilizar el MAP para reducir la comunicación con el Home Agent y Correspondent Node, junto con Fast Handover y Bicasting. Sin embargo, ahora es en el MAP donde se realiza la redirección de los paquetes, en vez de en el Router de Acceso antiguo. El MAP utiliza Bicasting y manda los paquetes a la antigua y a la nueva Care-of Address local. Los paquetes que

llegan al nuevo enlace antes de que lo haga el Nodo Móvil se guardan en un buffer para su posterior entrega.

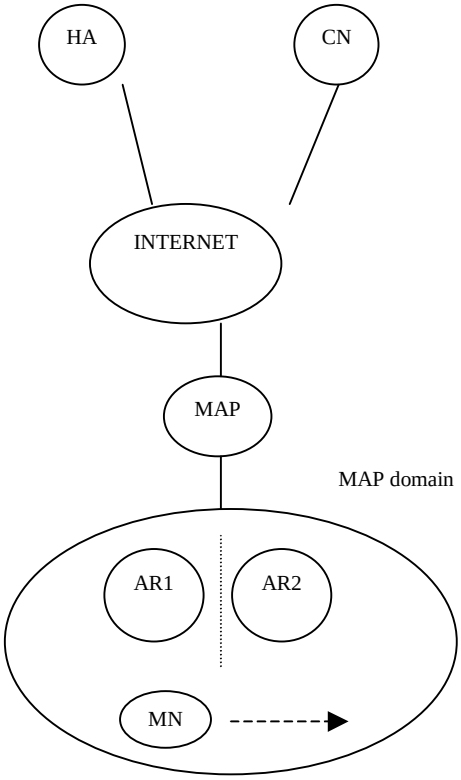


Figura 10: Esquema de la arquitectura propuesta.

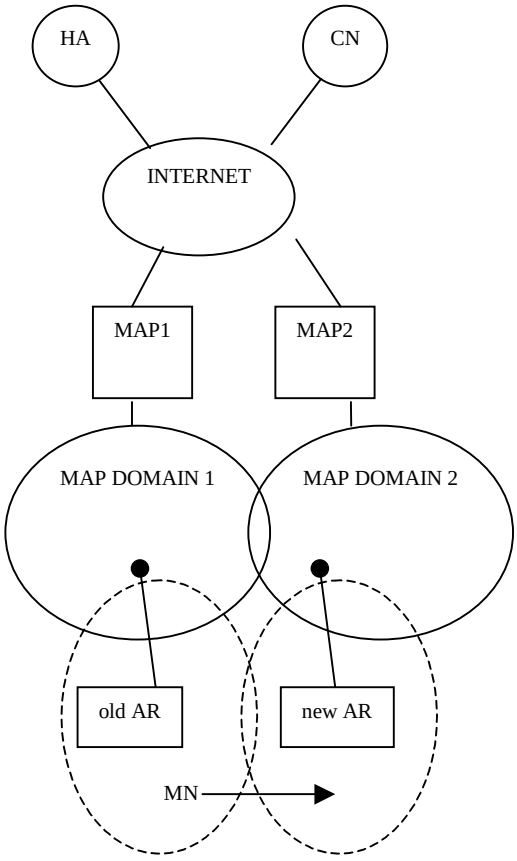


Figura 11: Esquema con dos MAPs

En las siguientes líneas se explica con más detalle la integración propuesta de los distintos protocolos.

El proceso empieza cuando el Nodo Móvil está todavía en el enlace previo, conectado al Router de Acceso antiguo, y se aproxima a la zona de cobertura dentro del dominio del nuevo Router de Acceso. El Nodo Móvil recibe un trigger

procedente de la capa 2, informando que el nuevo enlace estará disponible en un corto periodo de tiempo, y que se está a punto de entrar en el proceso de handover. Por lo tanto, es necesaria algún tipo de coordinación con la capa 2.

Cuando el Nodo Móvil recibe el trigger de la capa 2, manda un paquete Router Solicitation Proxy (RtSolPr) al Router de Acceso antiguo informándole de que está a punto de ocurrir un nuevo handover, y suministrándole también la identidad del nuevo Router de Acceso.

A continuación el Router de Acceso antiguo manda un paquete Router Advertisement Proxy (RtAdvPr) al Nodo Móvil, informándole del prefijo de subred del enlace en el que el Nodo Móvil está a punto de entrar. Si es el Router de Acceso antiguo el que recibe el trigger de la capa 2, en vez del Nodo Móvil, estamos en el caso del handover iniciado por la red, y el Router de Acceso antiguo manda un RtAdvPr al Nodo Móvil sin esperar a recibir el RtSolPr.

El Router de Acceso antiguo debe tener información acerca de los prefijos de subred de los routers de acceso contiguos a él. Una vez que el Nodo Móvil recibe el prefijo de subred del nuevo Router de Acceso, incluido en el RtAdvPr, ya puede formar una nueva Care-of Address local usando Stateless Address Autoconfiguration. La porción de red de la nueva dirección es el prefijo del nuevo enlace, y la parte del host es un número basado en la dirección MAC.

Después de esto, es necesario un nuevo paquete, el Iniciador. El Router de Acceso antiguo tiene que informar al MAP acerca del posible handover. Este paquete debe contener información que permita al MAP mandar un mensaje Handover Initiate (HI) al nuevo Router de Acceso, por lo que la antigua Care-of Address local, la nueva y la dirección del nuevo Router de Acceso deben incluirse en este paquete. El Router de Acceso antiguo debe por tanto conocer el MAP con el que el Nodo Móvil está registrado, y su dirección, para poder mandar el paquete Iniciador a dicho MAP. Esta información debe proporcionarla el mensaje RtSolPr.

Cuando el MAP recibe el paquete Iniciador, manda un mensaje HI al nuevo Router de Acceso, incluyendo en este paquete la recién formada Care-of Address local. El nuevo Router de Acceso comprueba si esa dirección se está utilizando en ese mismo momento, efectuando un DAD, proceso que puede llevar un cierto tiempo. Por lo tanto, este DAD se puede efectuar por medio de tablas en las que el

Router de Acceso mantiene las direcciones usadas en ese momento. Usando este procedimiento se acorta significativamente este tiempo.

Con el resultado de la comprobación de duplicidad de la dirección, el nuevo Router de Acceso manda un mensaje HACK al MAP, indicando cómo redireccionar los paquetes. Si la comprobación tuvo éxito, los paquetes son redirigidos desde el MAP hasta la nueva Care-of Address local. Si el resultado de la comprobación no tuvo éxito, el MAP redirige los paquetes al nuevo Router de Acceso.

Para empezar el proceso de redirección de paquetes, el Nodo Móvil manda un Fast Binding Update al MAP, relacionando la Care-of Address regional con la nueva Care-of Address local. Este Fast Binding Update utilizará Bindings Simultáneos, por lo que el MAP, a partir de ese momento, manda un Fast BA al nuevo y al antiguo enlace, y empieza a realizar bicasting, mandando los paquetes tanto al nuevo enlace como al antiguo. Con este método no es necesaria la coordinación de la capa 2 con la 3, y no es necesario conocer el momento exacto del cambio de red, ya que el MAP está mandando los paquetes a los enlaces antiguos y nuevos, evitándose así la pérdida de paquetes.

Cuando los paquetes llegan al nuevo Router de Acceso, puede ocurrir que el Nodo Móvil no se encuentre todavía allí. Aún estando allí, puede que el Nodo Móvil este efectuando todavía el handover de la capa 2, por lo que no le es posible recibir los paquetes. Por lo tanto se requiere la solución de un buffer que guarde los paquetes que llegan para evitar así su pérdida. Una vez que el Nodo Móvil llega al nuevo enlace, éste manda un mensaje llamado Fast Neighbour Advertisement, cuya función es anunciar al nuevo Router de Acceso su presencia en el nuevo enlace. Cuando el nuevo Router de Acceso recibe dicho paquete, empieza a mandar al Nodo Móvil los paquetes que tenía almacenado en el buffer.

En el caso de Stateful Address Autoconfiguration, el nuevo Router de Acceso manda en el mensaje HACK una Care-of Address local válida al MAP, y es este último nodo quien manda el Router Advertisement Proxy al Nodo Móvil, no el Router de Acceso antiguo, proporcionando en este mensaje la nueva Care-of Address local. Por lo tanto, el mensaje RtAdvPr es mandado por el MAP después de recibir el HACK.

Cuando el Nodo Móvil establece conexión en el nuevo enlace, debe mandar el Router Solicitation como en el caso normal de HMIPv6. Es necesario un trigger de

la capa 2 para informar al Nodo Móvil de que ya ha establecido una conexión de nivel 2. Entonces el nuevo Router de Acceso manda un Router Advertisement al Nodo Móvil, en donde viene incluido la opción MAP. El Nodo Móvil verifica entonces la lista de MAPs disponibles en ese momento en el enlace, y determina si ha entrado en un nuevo dominio MAP. El Nodo Móvil puede recibir varias opciones MAP, y tiene la posibilidad de elegir entre los diferentes MAPs disponibles, seleccionando finalmente uno de ellos.

El Nodo Móvil tiene que saber si la nueva Care-of Address mandada en el Fast Binding Update es válida, o en cambio, no es válida, por lo los paquetes se están mandando a través de un túnel desde el MAP hasta el nuevo Router de Acceso. Esta información debe ser proporcionada por el F-Back.

Si el Nodo Móvil permanece en el mismo dominio MAP y la nueva Care-of Address local es válida, el proceso de handover finaliza al recibir el Nodo Móvil el mensaje Router Advertisement, mandado por el nuevo Router de Acceso. Si la nueva Care-of Address no es una dirección válida, el Nodo Móvil debe de continuar la comunicación a través del túnel. Si el Nodo Móvil cambia de dominio MAP, debe proceder con los pasos normales de registro al igual que en el caso de HMIPv6. Debe mandar un Binding Update al MAP relacionando la nueva Care-of Address local con la nueva Care-of Address regional, formada previamente con el prefijo de subred del nuevo MAP, incluido en el mensaje Router Advertisement. Si el MAP está trabajando en modo extendido, en vez de en modo básico, el Binding Update relaciona la nueva Care-of Address local con la Home Address. El nuevo MAP manda a continuación el BA al Nodo Móvil. El proceso termina con el Binding Update mandado al Correspondent Node y Home Agent relacionando la Care-of Address regional con la Home Address.

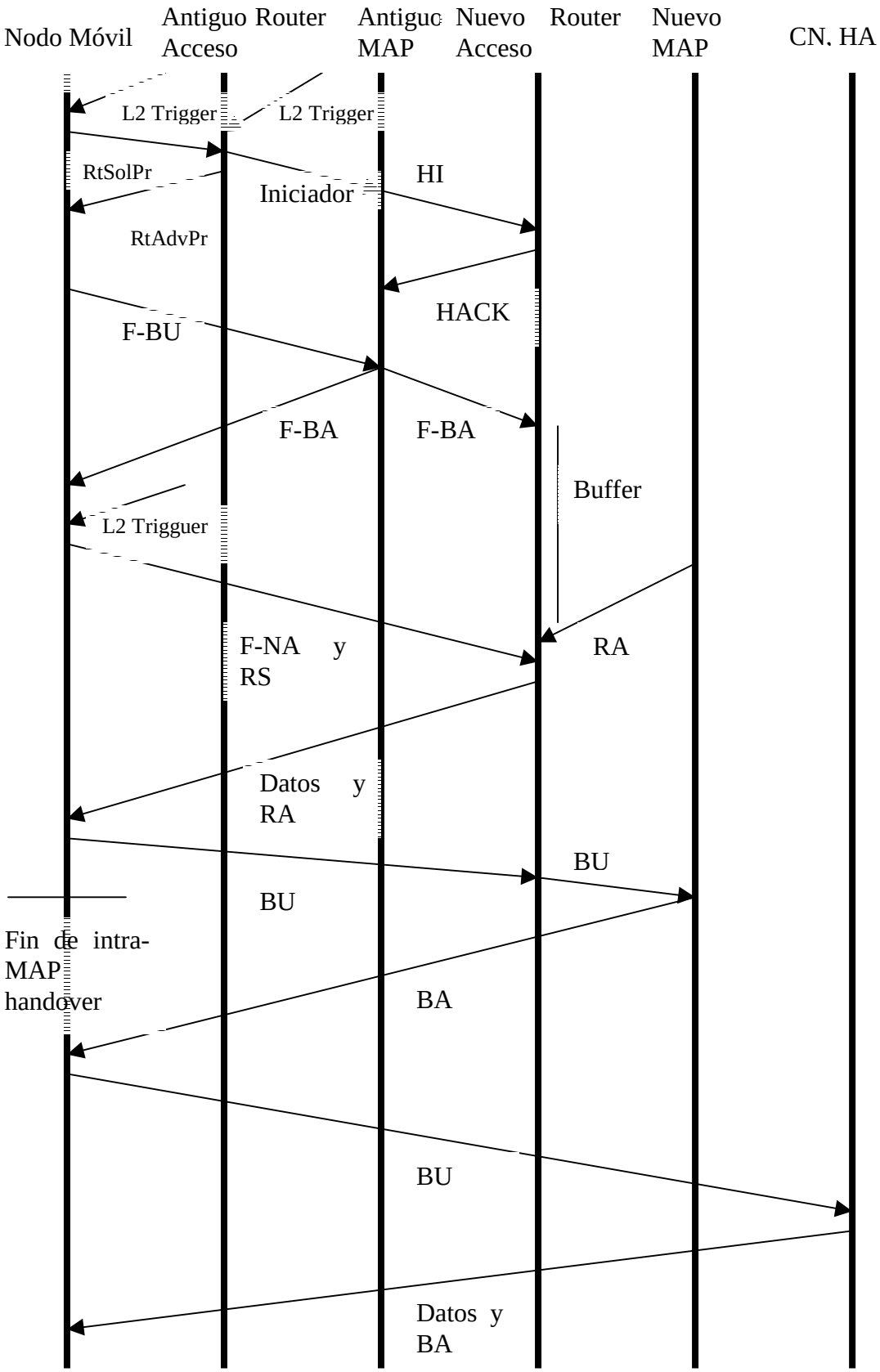

Nodo Móvil
Antiguo Router Acceso
Antiguo MAP
Nuevo Router Acceso
Nuevo MAP
CN, HA
L2 Trigger
L2 Trigger
RtSolPr
Iniciador
HI
RtAdvPr
HACK
F-BU
F-BA
F-BA
Buffer
L2 Trigguer
F-NA y RS
RA
Datos y RA
BU
BU
Fin de intra-MAP handover
BA
BU
Datos y BA

Figura 12. Flujo de paquetes en Integración de los 3 protocolos

7.2.3 Periodo de pérdida de paquetes

El principal objetivo del protocolo propuesto es intentar minimizar el periodo de pérdidas de paquetes, pero de todas maneras, puede que haya algunas pérdidas. Deben tenerse en cuenta dos hechos importantes, el handover de nivel 2 y el buffer. Antes de efectuar el handover de la capa 2, este protocolo efectúa el handover de la capa 3. El MAP transmite los paquetes a la nueva Care-of Address local y a la antigua. Este método hace que no haga falta una coordinación entre el handover de la capa 2 y el de la capa 3, ya que el Nodo Móvil puede permanecer en el enlace previo después de mandar el Fast Binding Update, sin producirse pérdidas de paquetes. La utilización de Bicasting permite que no haga falta una sincronización entre las conexiones de nivel 2 y 3, ya que los paquetes están llegando a los dos enlaces simultáneamente. Durante el handover de la capa 2, la comunicación se interrumpe, aunque los paquetes que llegan durante ese periodo de tiempo no se pierden, ya que quedan almacenados en el buffer. Pero si el handover de nivel 2 tarda más tiempo que lo que el buffer puede almacenar, entonces si se pueden producir pérdidas de paquetes. Este buffer puede hacerse más grande, y ser capaz de almacenar una gran cantidad de paquetes, pero esto es totalmente inútil en el caso de que se estén utilizando aplicaciones en tiempo real, como transporte de voz o video. El máximo retraso de extremo a extremo recomendable en la transmisión de voz a través de Internet es de 150 ms [DELAY_END_TO_END]. Por esta razón, y sin considerar factores como el retraso de propagación, el retraso del codec, de serialización, etc... estos 150 ms imponen una restricción a la máxima cantidad de tiempo que el buffer debe ser capaz de almacenar, suponiendo que estamos en el caso de la transmisión de voz. Al considerar lo anterior, el máximo tiempo que el handover de la capa 2 debe durar para que no se produzcan pérdidas de paquetes son 150 ms. De todas maneras, éste es el mejor comportamiento que se puede esperar de la capa 3, ya que no hay ningún otro periodo de pérdidas de paquetes debido a la señalización de la capa 3. También se puede producir una pequeña pérdida de paquetes si la capa 2 se desconecta justo después de que el Nodo Móvil mande el Fast Binding Update. Hay

un pequeño espacio de tiempo, hasta que el Fast Binding Update llega al MAP y los paquetes son redirigidos, en los que es posible que se produzca pérdida de paquetes, pero esta cantidad de tiempo es muy pequeña, y teniendo en cuenta que los modernos DSPs pueden corregir hasta 30 ms de pérdidas en voz, este periodo de pérdidas no debe tenerse en cuenta.

7.2.4 Retraso de redirección.

Si estamos en el caso de aplicaciones en tiempo real, como voz sobre IP, el retraso máximo recomendable de extremo a extremo debe ser de 150 ms, tal como se ha mencionado anteriormente. En el proceso de handover, el retraso de extremo a extremo en el nuevo enlace tiene que cumplir también con los requerimientos de tiempo. Este protocolo trata de evitar la pérdida de paquetes utilizando la técnica del redireccionamiento de los paquetes. Si esta redirección añade un retraso extra superándose así el total de 150 ms, los paquetes que llegan después de este tiempo corren el riesgo de ser descartados por excesivo retraso, por lo que en ese caso, se estaría dando una nueva forma de pérdida de paquetes. Por esta razón, es importante que, si se quiere que el retraso de redirección traiga consigo una pérdida de paquetes, el camino de redirección se optimice. Esto se consigue utilizando el MAP como punto desde el cuál se realiza la redirección, en vez del antiguo Router de Acceso, no teniendo entonces que bajar por la jerarquía de routers para tener que subir de nuevo, obteniéndose así un camino más directo.

7.2.5 Conclusiones

Desde el punto de vista de la pérdida de paquetes, con la integración de Fast Handover, Bicasting y HMIPv6 no se obtiene un mejor resultado que en el caso de la integración de Fast Handover y Bicasting unicamente. Pero el tiempo de handover, el tiempo que se tarda en mandar mensajes de señalización y el Home Agent y Correspondent Node tienen las direcciones necesarias para comunicarse con el Nodo Móvil se reduce. Si se utiliza Fast Handover y Bicasting, cada vez que el Nodo Móvil llega a un nuevo enlace, éste debe mandar Binding Update al Home Agent y

Correspondent Node, que puede llegar a tardar bastante tiempo y ocupar ancho de banda. Además, durante el handover, los paquetes que llegan al nuevo enlace se redireccionan desde el antiguo Router de Acceso, por lo que puede que el camino de redirección no sea el optimo, pudiéndose producir pérdidas de paquetes debido a un excesivo retraso añadido por la redirección.

En el caso de la integración de los tres protocolos, la posibilidad de pérdida de paquetes es la misma. Si consideramos el caso de un Intra-MAP handover, el proceso termina cuando el Nodo Móvil recibe el Router Advertisement, y no se necesitan mandar más Binding Update adicionales, ni al MAP ni al Home Agent y Correspondent Node. El único Binding Update que se necesita ya se mandó desde el antiguo enlace. Por lo tanto, en el caso de Inter-MAP handover, el proceso tarda el mismo tiempo que en el caso de HMIPv6. Hay una mejora también en el camino de redirección. Los paquetes no se redirigen en el router de accceso, sino en el MAP, nodo que se encuentra más arriba en la jerarquía de routers. De este modo se consigue un camino más directo y además se estable el posible camino definitivo, no uno temporal como en el caso Fast Handover. En el caso de Inter-MAP handover esto es un punto a tener en cuenta, ya que los paquetes deben redireccionarse desde el antiguo MAP hasta el nuevo enlace, por lo que en este caso si puede que se produzca un retraso extra. En este caso, el camino no está optimizado, ni tampoco es el camino final. También son necesarios los Binding Update al Home Agent y al Correspondent Node, así como al MAP.

La optimización del camino es un punto importante a tener en cuenta cuando se utilizan protocolos de QOS (calidad de servicio) basado en la reserva de recursos a través del camino, como RSVP. Usando la integración de los tres protocolos en el caso de intra-MAP handover, sólo es necesaria la reserva de más recursos en el camino desde el MAP hasta el Nodo Móvil. Si utilizamos únicamente Fast Handover, hay un periodo de tiempo en el que se utiliza un camino temporal, lo que puede causar problemas a los protocolos de QOS.

La solución propuesta integrando los tres protocolos tiene también ciertos problemas. El buffer que se necesita en el nuevo Router de Acceso puede que traiga problemas de escalabilidad, por lo que el tamaño de este buffer es un aspecto a considerar. Para aplicaciones en tiempo real, no es necesario un buffer de gran tamaño, teniendo este la capacidad para almacenar unos 150 ms, en el caso de aplicaciones de voz. Otro buffer que puede tener problemas de escalabilidad es el

que se utiliza para asegurar que las direcciones no están duplicadas. Esto puede causar problemas si están registrados en el mismo buffer un gran número de nodos.

Usando la combinación de los tres protocolos, el periodo de pérdida de paquetes es más pequeño que si usamos simplemente HMIPv6, pero es el mismo que si utilizamos Fast Handover y Bicasting. El ancho de banda utilizado, sin embargo es menor en la solución propuesta que en el caso de Fast Handover, y es elimado el retraso de redirección en el caso de Intra-MAP handover, que se espera que sea en la mayoría de los casos. Esta propuesta hereda los problemas derivados de HMIPv6 como son que el MAP se convierte en un único punto de fallo, y un punto de congestión.

La conclusión final es que si el handover que con más frecuencia ocurre es el intra-MAP, la inclusión de HMIPv6 a Fast Handover y Bicasting puede mejorar el rendimiento del protocolo, ya que el camino utilizado es el camino final, se consume menos ancho de banda y los paquetes redirigidos no sufren un retraso extra.. El periodo de pérdidas de paquetes es reducido al mínimo, pero no hay nuevas ventajas comparado con el caso de Fast Handover y Bicasting.

Si el handover más frecuente es el inter-MAP handover, no se producen mejoras comparados con Fast Handover y Bicasting. Además los problemas de escalabilidad, de punto de congestión y de fallo, permanecen en este protocolo.

7.3 Mejoras en el protocolo de selección del MAP

7.3.1 Protocolo Actual

El MAP anuncia su presencia utilizando el paquete Router Advertisement. En este paquete el MAP incluye su prefijo de subred, el campo preferencia y el campo distancia. El prefijo de subred se incluye para permitir al Nodo Móvil formar una nueva Care-of Address regional, usando Sateless Address Autoconfiguration. Esta nueva dirección se forma concatenando el prefijo de subred del MAP con un identificador único basado en la dirección MAC. Es necesario efectuar DAD en la

dirección o algún otro mecanismo, como la utilización de tablas, que verifique que la dirección recién formada no está siendo utilizada en ese momento

El valor indicado en el campo distancia indica la distancia desde el MAP hasta el Nodo Móvil, y no es necesariamente el número de saltos. Cuando un Nodo Móvil entra en un nuevo enlace, recibe el paquete Router Advertisement, cuya opción MAP contiene la lista de todos los MAPs disponibles en dicho enlace, con la correspondiente información de cada MAP.

Si el MAP con el que el Nodo Móvil se estaba comunicando no aparece en la lista de MAPs, se tiene que proceder a la elección de un nuevo MAP de entre los disponibles en el enlace, que son aquellos que aparecen en la lista. Sólo se puede registrar un único MAP en el Home Agent y el Correspondent Node. Para seleccionar un MAP el Nodo Móvil actúa de la siguiente manera: Primero clasifica los diferentes MAPs en función del valor que aparece en el campo distancia. El Nodo Móvil tendra preferencia por el MAP que tenga un mayor valor en el campo distancia, ya que mientras más lejano esté el MAP, menor será la posibilidad de que se efectúe un handover entre dos MAPs distintos. A continuación el Nodo Móvil pasa a seleccionar el MAP más lejano en la jerarquía, a menos que su valor en el campo preferencia sea de 15, lo que significará que el MAP no está disponible, quizás debido a la congestión de dicho nodo. En este caso, el Nodo Móvil pasa a seleccionar el siguiente MAP de la lista, de nuevo comprobando que su valor no es de 15. Otros valores distintos de este campo no se utilizan en este protocolo.

7.3.2 Posibles mejoras

El problema del punto único de fallo del MAP puede solucionarse si en cada enlace estuvieran disponibles varios MAPs. Usando este simple protocolo para seleccionar el MAP, todos los Nodos Móviles dentro de un mismo enlace seleccionarán el mismo MAP, el más lejano en la jerarquía. El problema del punto de congestión permanece ya que aunque varios MAPs estén disponibles, sólo será seleccionado uno por todos los Nodos Móviles, quedando el resto sin utilizar.

Sería bastante útil la posibilidad de poder seleccionar no sólo un único MAP para cada Nodo Móvil, sino varios MAPs, pudiendo depender del Correspondent Node con el que se está comunicando en dicho momento. El protocolo mejorado para

la elección de un MAP deberá elegir el mejor MAP para comunicarse con un cierto Correspondent Node, teniendo por lo tanto la posibilidad de tener varios MAPs para comunicarse con distintos Correspondent Nodes.

El Nodo Móvil debe darse cuenta cuándo la comunicación directa con el Correspondent Node es mejor que la comunicación a través del MAP. Si el Correspondent Node está más cerca que el MAP del Nodo Móvil, no aporta ninguna ventaja el hecho de utilizar HMIPv6 o la integración de los tres protocolos. Por lo tanto, esta situación deberá de ser detectada por el protocolo de selección del MAP, y proceder a la comunicación directa cuando se cumplan los requisitos.

La velocidad del Nodo Móvil también debe de tenerse en cuenta, ya que si ésta es muy alta, hay más posibilidades de que el Nodo Móvil efectúe un handover entre los diferentes MAPs, situación que debe ser evitada, ya que consume una gran cantidad de tiempo y recursos. En estos casos, es recomendable elegir el MAP más alejado en la jerarquía, evitando así los inter-MAP handover. Si la velocidad del Nodo Móvil no es muy alta, o no está en movimiento, se debe seleccionar para la comunicación el MAP más cercano en la jerarquía.

Es necesario mejorar también la utilización del campo preferencia. El rango entero, de 1 a 15 se debe utilizar para indicar la sobrecarga del MAP, no sólo el valor 15. Si un MAP está menos congestionado que otro en cierto momento, debe de tener preferencia a la hora de la selección. Con esto, debe ser posible la distribución de carga entre los diferentes MAPs.

7.3.3 Solución propuesta.

A continuación se expone una propuesta para el algoritmo de selección del MAP usando HMIPv6 o la integración de éste con Fast Handover y Bicasting.

Cuando el Nodo Móvil llega al nuevo enlace, éste recibe el paquete Router Advertisement, incluyendo la opción MAP, que contiene una lista de todos los MAPs disponibles en ese momento, incluyendo las opciones de distancia, preferencia y el prefijo de subred.

En el caso de estar utilizando HMIPv6, el Nodo Móvil forma una nueva Care-of Address local, y manda un Binding Update a todos los MAPs con los que se estaban comunicando en el antiguo enlace. Estos Binding Update relacionan las antiguas Care-of Address regionales con la nueva Care-of Address local. Se evita así la pérdida de paquetes, ya que los antiguos MAPs pueden empezar a redireccionar los paquetes a la nueva Care-of Address local. En el caso de utilizar la integración de los protocolos, se mandarían Fast Binding Updates a los antiguo MAPs cumpliendo la misma función.

El siguiente paso es determinar si los MAPs que el Nodo Móvil estaba utilizando en el antiguo enlace siguen disponibles en este momento. Si lo están, al haber mandado ya el Binding Update, el proceso de handover termina aquí. Sin embargo, si uno o más de un MAP de los que el Nodo Móvil estaba utilizando anteriormente no se encuentran disponibles en ese momento, se tiene que proceder a la selección de MAPs, seleccionándose para cada Correspondent Node el MAP más conveniente de entre los varios que están disponibles. Pero, el Nodo Móvil sólo necesita seleccionar un MAP para los Correspondent Node cuyos MAPs no se encuentran disponibles en el nuevo enlace. Esto se realiza para conseguir una reducción en la señalización ya que sólo cuando un MAP que estaba en uso no está ya disponible, el Nodo Móvil busca un nuevo MAP para sus Correspondent Nodes.

A continuación, el Nodo Móvil obtiene una lista de los Correspondent Nodes que no tienen MAP en el nuevo enlace. Hay que tener en cuenta que no se producen pérdidas de paquetes ya que el Nodo Móvil mandó un Binding Update a todos los antiguos MAP.

En este punto es necesaria la introducción de nuevos paquetes. El paquete Test se manda a cada uno de los Correspondent Nodes que se han quedado sin MAP. Este paquete contiene la Home Address y la Care-of Address local del Nodo Móvil, y la dirección de todos los MAPs disponibles en el nuevo enlace. El Nodo Móvil activa un temporizador por cada paquete Test que manda.

Cuando el Correspondent Node recibe el paquete Test, manda un nuevo paquete, el Test Acknowledgement a cada una de las direcciones de los MAPs incluidas en el paquete Test y otro paquete para la Care-of Address local. Estos paquetes van desde el Correspondent Node al Nodo Móvil a través de los diferentes MAPs contando el número de saltos que emplea hasta llegar al MAP. Finalmente los

paquetes llegan al Nodo Móvil, que ahora sabe el número de saltos desde un determinado Correspondent Node a todos los MAPs. En el caso del paquete Test Acknowledgement mandado directamente a la Care-of Address local, el número de saltos indica la distancia para una comunicación directa desde el Correspondent Node al Nodo Móvil.

Cuando el Nodo Móvil recibe un Test Acknowledgement, éste detiene un temporizador asociado a este MAP y Correspondent Node. Una vez recibido este paquete, el Nodo Móvil tiene conocimiento de la distancia desde el Correspondent Node a cada MAP, y también del tiempo que tarda un paquete en ir desde el Correspondent Node hasta el Nodo Móvil pasando por un determinado MAP.

Después de esto, el Nodo Móvil tiene que decidir si es mejor una comunicación directa con el Correspondent Node, o hacerlo a través del MAP. Para lograr esto, el Nodo Móvil hace una lista con todos los MAPs, colocando primero en la lista los MAPs que se encuentren más lejos. Está clasificación se hace basándose en la información que aparece en el campo distancia, incluido en el Router Advertisement. El Correspondent Node se incluye también en la lista, y su posición depende del valor indicado en el mensaje Test Acknowledgement que tomó el camino directo. Si el último nodo en la lista es el Nodo Correspondiente, todos los MAPs se encuentran más lejos que el Correspondent Node, por lo que se procede a la comunicación directa, ya que el uso de MAP no reportaría ninguna ventaja. Si el Correspondent Node no es el último en la lista, hay otros MAPs más cercanos al Nodo Móvil. En este caso, los MAPs que están más lejos que el Nodo Correspondiente no se toman en cuenta para la elección, y los restantes entran a formar parte del algoritmo para seleccionar cuál es el mejor MAP para comunicarse con un determinado Correspondent Node.

La velocidad del Nodo Móvil se debe tener en cuenta. En este caso, el MAP situado más lejos en la jerarquía es el preferible. Otro factor importante es la distancia del Correspondent Node al MAP. El Nodo Móvil preferirá el MAP con la mínima distancia al Correspondent Node, seleccionando así el MAP que por la topología de la red esté más cerca del Correspondent Node. Esta información viene dada en el paquete Test Acknowledgement. Es importante tomar una decisión teniendo en cuenta la congestión actual del MAP, información que es suministrada por el campo preferencia del paquete Router Advertisement. Haciendo esto es posible distribuir la carga entre los diferentes MAPs. Hay que considerar también

que el tiempo que los paquetes tardan en llegar al Correspondent Node y volver de nuevo al Nodo Móvil. Esto proporciona información acerca de que camino es mejor para comunicarse con cierto Correspondent Node, teniendo en cuenta otros factores además de la distancia, como el ancho de banda disponible, la congestión del enlace, etc... Puede ser que el MAP más lejos del Correspondent Node sea el que cuente con mejores condiciones en términos de velocidad del enlace, por ejemplo.

La expresión propuesta para la selección del mejor MAP es la siguiente, seleccionándose el MAP que obtenga un mayor valor:

X1*velocidad*distancia1 –X2*distancia2 – X3*carga –X4*timer

Las cantidades X1, X2, X3 y X4 se necesitan para ponderar los diferentes valores de las variables, pudiendo de esta manera dar más valor a unas variables que a otras. El termino velocidad es la velocidad del Nodo Móvil. Distancia 1 es la distancia desde el MAP al Nodo Móvil. Distancia 2 es la distancia del Correspondent Node al MAP. Carga es el valor que aparece en el campo preferencia en el Router Advertisement. Timer es el tiempo que tarda el paquete Test en ir al Correspondent Node y al Test Acknowledgement volver a través del MAP. El signo positivo indica que cuanto mayor sea la cantidad, mejor, mientras que el signo negativo indica lo contrario, que cuanto menor sea la cantidad, mejor.

Una vez que el Nodo Móvil ha seleccionado el MAP adecuado para cada Correspondent Node, manda un Binding Update a los distintos MAPs, relacionando la Care-of Address local con la Care-of Address regional. En este protocolo, el Home Agent es tratado como si fuera un Correspondent Node más.

7.3.4 Conclusiones

En este apartado se trata de solucionar dos de los problemas que aparecen con la utilización de MAPs, el punto de congestión y el punto único de fallo. Para solucionar esto, se propone una arquitectura con varios MAPs. Por esta razón, es necesario un algoritmo mejorado para la selección del MAP. Este algoritmo es capaz de distribuir la carga entre varios MAPs y también es capaz de seleccionar el mejor MAP para cada Correspondent Node. También detecta cuándo una comunicación directa con el Correspondent Node es preferible. No se producen pérdidas de

paquetes, ya que se mando un Binding Update al antiguo MAP, que procede a la redirección de los paquetes al nuevo enlace.

Pero este protocolo tiene también un problema importante. La señalización aumenta de manera considerable en el caso de que se tengan que registrar nuevos MAPs.

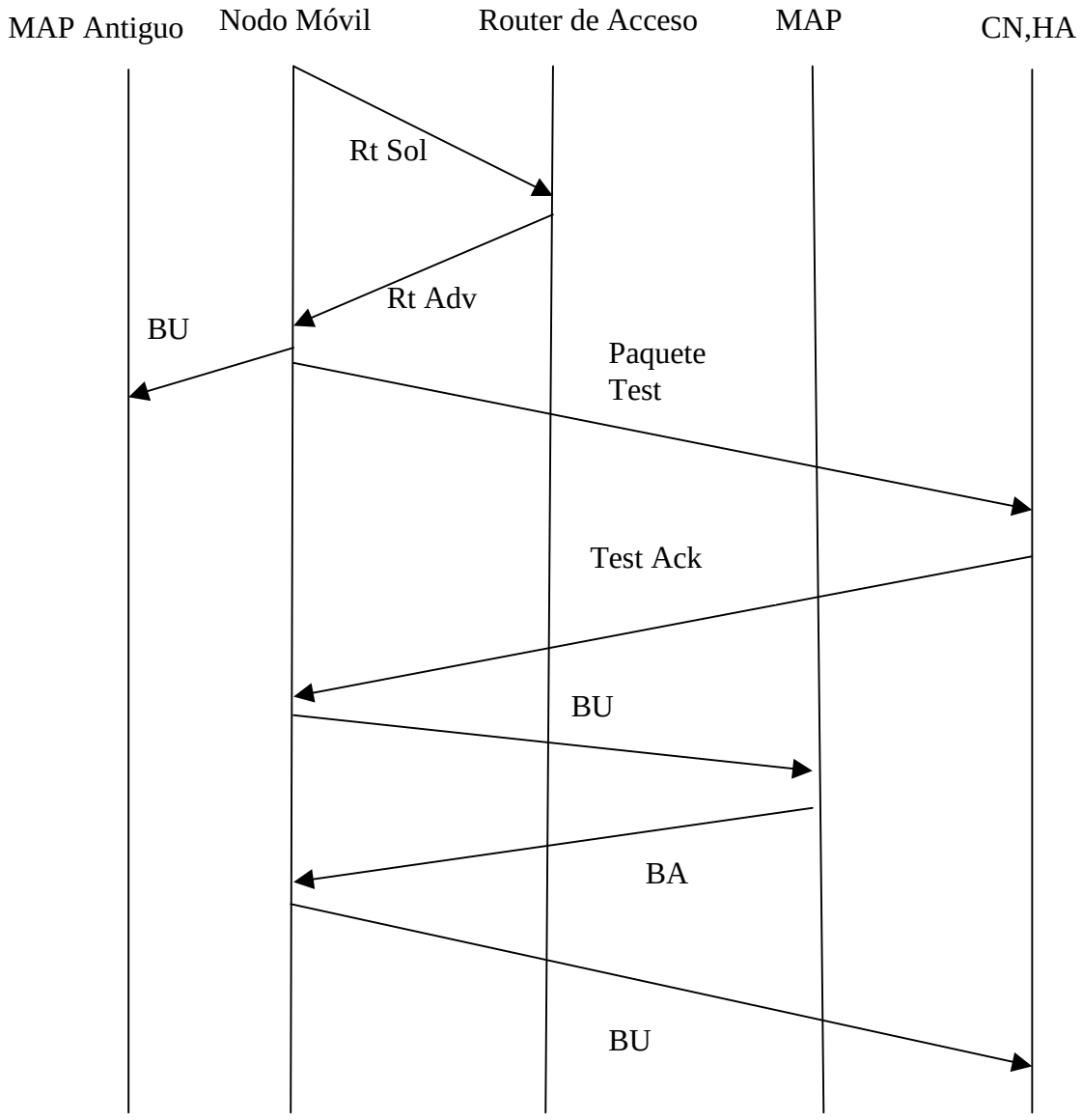


Figura 13: Flujo de Señales

7.4 Resultados generales

El principal objetivo de este proyecto es el analizar los tres drafts propuestos para mejorar IPv6 Móvil, como son Fast Handover, Bindings Simultáneos y IPv6 Móvil Jerárquico, y hacer una integración de los tres drafts y encontrar si con estos protocolos, o una combinación de ellos, es posible conseguir soporte para aplicaciones en tiempo real, como voz o video, en el proceso de handover.

En el diseño original de IPv6 Móvil es difícil conseguir dar soporte a aplicaciones en tiempo real, ya que el Nodo Móvil tiene que comunicarse con el Home Agent y el Correspondent Node durante el proceso de handover. Estos nodos pueden que se encuentren lejos del Nodo Móvil, por lo que el proceso de intercambio de mensajes puede ser bastante lento. Durante este periodo de tiempo, se produce pérdida de paquetes, o estos son enrutados de una manera no óptima. También hay que tener en cuenta que la señalización de nivel 3 se produce después de que se complete el handover de nivel 2, por lo que en ese periodo de tiempo los paquetes se pierden. Por lo tanto, el rendimiento del handover en IPv6 Móvil es muy dependiente del tiempo que tarda el handover de la capa 2. Extensiones como Fast Handover permiten el desacoplo de las dos capas, pudiéndose producir el handover de nivel 3 incluso antes que el de nivel 2.

Uno de los mayores problemas de IPv6 Móvil, la detección del movimiento, se ha resuelto con la introducción de triggers de nivel 2, que anuncian al Nodo Móvil de que ha entrado en un nuevo enlace. Con esta solución se evita la dependencia del handover con la frecuencia a la que se mandan los Router Advertisement.

Si se considera el caso de Fast Handover únicamente, éste es capaz de proporcionar propiedades de tiempo real si y solo si se cuenta con una adecuada coordinación con el handover de la capa 2. Si esta coordinación no es posible, se pueden producir pérdidas de paquetes, ya que el flujo de paquetes puede llegar al nuevo enlace antes de que lo haga el Nodo Móvil. Este problema se soluciona con la introducción de Bicasting, lo cual elimina la necesidad de coordinación entre la capa 2 y la 3, ya que el handover de la capa 2 puede ocurrir cuando sea, ya que hay un flujo de paquetes llegando al antiguo enlace y al nuevo al mismo tiempo. Sigue siendo necesario en este caso la utilización de triggers de nivel 2.

La combinación de Fast Handover con Bindings Simultáneos puede soportar aplicaciones en tiempo real, pero deben tomarse en cuenta diversas consideraciones. A pesar de que no es necesaria la coordinación con el handover de nivel 2, sí es necesario que la capa 2 cumpla con una serie de requerimientos. El primero sigue siendo la necesidad de triggers que informen al Nodo Móvil de que está a punto de efectuar un handover. Segundo, es necesario que el handover de nivel 2 dure menos que una determinada cantidad de tiempo, ya que en ese periodo de tiempo, los paquetes que llegan al nuevo enlace deben guardarse en un buffer para evitar que se pierdan. Si durante el handover de la capa 2 llegan más paquetes que los que el buffer puede guardar, se produce pérdida de paquetes. No es una solución posible el hacer el buffer mayor, ya que el retraso acumulado por los paquetes almacenados en el buffer se haría demasiado grande para el caso de aplicaciones en tiempo real. Otro problema a tener en cuenta es el retraso de redirección. Fast Handover está basado en la redirección de los paquetes desde el Router de Acceso antiguo hasta el nuevo. Si el retraso que el nuevo camino de redirección introduce es demasiado grande, el retraso total de extremo a extremo puede ser en este caso mayor que el máximo permitido al utilizar aplicaciones en tiempo real, por lo que esos paquetes se descartan. Este retraso es probablemente pequeño, siempre y cuando la red se haya construido adecuadamente.

IPv6 Móvil Jerárquico es capaz de soportar aplicaciones en tiempo real, pero se pueden obtener mejoras importantes al utilizar el esquema modificado propuesto en este trabajo, sobre todo en el caso de que se produzcan handovers entre distintos MAPs. Se requieren algunos requerimientos de la capa 2. El primero es que el handover de la capa 2 debe permanecer tan pequeño como sea posible, ya que durante este tiempo los paquetes se pierden. Es necesaria también la utilización de triggers de nivel 2. Sin embargo, la utilización de IPv6 Móvil Jerárquico tiene una serie de inconvenientes, los principales son que puede convertirse en un único punto de fallo y de congestión. Esto se puede solucionar con la solución propuesta para la mejora del protocolo de selección de MAPs.

En el caso de que se integren los tres protocolos, se obtienen diversas ventajas. La primera con respecto al uso de Fast Handover es que se reduce la señalización durante el handover. También se obtiene un camino optimizado en la redirección, por lo que se elimina el riesgo de retraso de redirecćon. El periodo de pérdidas de paquetes es el mismo que con Fast Handover, pero es el mejor rendimiento que podemos esperar de la capa 2. Sin embargo, en el caso de Inter-

MAP handover, no se introduce ninguna mejora a Fast Handover. La integración también requiere el uso de triggers de nivel 2.

En resumen, usando IPv6 Móvil Jerárquico junto con Fast Handover y Bicasting se puede dar soporte a aplicaciones en tiempo real en el proceso de handover, aunque el soporte de la capa 2 sigue siendo necesario.

Capítulo 8. Soluciones alternativas

Están apareciendo diferentes productos que intentan dar solución a los mismos problemas que IPv6 Móvil. Entre estos productos se encuentran Hawaii, de Lucent Technologies y Mobility 4.0 de NetMotion [NETMAGAZINE]. En este capítulo se expondrá resumidamente esta última solución, ya que es la que más éxito está consiguiendo en los mercados.

El software vendido por NetMotion proporciona en este momento la mayoría de las funciones que IPv6 Móvil plantea proporcionar en un futuro. Además de dar soporte al handover entre diferentes subredes (handover horizontal) y entre diferentes tecnologías (handover vertical) [IP_QoS_IN_MOBILE_ENV], Mobility es capaz de mantener una sesión aún cuando se entre en espacios de baja o nula cobertura o incluso si desconectamos el aparato. Ponen como ejemplo el caso de que una persona en un aeropuerto de Estados Unidos, procediendo a la descarga de material por Internet mediante un hospot IEEE 802.11b (Wi-Fi) puede desconectar su equipo, coger un vuelo a Europa y una vez allí reanudar la misma descarga mediante GPRS. Está situación sería también útil en situaciones como el paso por debajo de un puente, o a través de un túnel, lugares que normalmente carecen de cobertura.

Todo esto se consigue dirigiendo todo el tráfico a través de un servidor proxy, situado en la Home Network, normalmente la LAN de la compañía. Por una parte, el servidor hace un seguimiento de los Nodos Móviles, y manda el tráfico destinado para ellos a través de un túnel. Por el otro lado, proporciona una dirección IP virtual fija, empleando técnicas como alterar el tamaño de ventana de TCP para que todo el proceso sea transparente a los protocolos de las capas superiores. Por lo tanto este software emplea una técnica muy parecida a la empleada por IPv6 Móvil, el tener una Care-of Address válida para cada enlace y una dirección fija, por la cual se comunican los demás nodos con la participación del servidor proxy.

Además del servidor proxy, lo que sería equivalente al Home Agent en IPv6 Móvil, cada Nodo Móvil requiere un cliente que automáticamente selecciona la mejor conexión disponible.

Dirigir todos los paquetes a través del servidor proxy tiene dos claros inconvenientes. El primero es que consume ancho de banda en la Home Network, y el segundo es que añade retraso a los paquetes. Sin embargo, la mayoría de las tecnologías inalámbricas tienen una tasa de transmisión tan baja que no debería causar ningún problema en los potentes enlaces de la Home Network. El retraso que se añade a los paquetes puede ser un problema más serio, aunque NetMotion asegura que el retraso introducido es equivalente a un solo salto. Para aplicaciones en tiempo real como Voz sobre IP (VoIP), los usuarios pueden elegir entre la comunicación por medio del proxy o la conexión directa.

El software Mobility puede funcionar teóricamente sobre cualquier tipo de capa física, aunque trabaja mejor con tecnologías que pueda reconocer, como RDSI, DSL o fibra óptica. Es capaz de compensar y reconocer una gran cantidad de redes inalámbricas, como Bluetooth, infrarrojos, HomeRF y todo tipo de IEEE 802.11. Soporta también redes WAN inalámbricas, como CDMA, GSM y tecnologías de 3ª generación.

Capítulo 9. Conclusiones

9.1 Conclusión general

El objetivo principal del proyecto fue el análisis e integración de las distintas extensiones propuestas para la mejora del handover en IPv6 Móvil. Se han analizado por separado cada una de las extensiones y se ha llegado a un modelo conjunto, que es capaz de dar soporte a aplicaciones en tiempo real en el proceso de handover. Se ha analizado esta solución, con sus ventajas e inconvenientes, exponiendo ciertos requerimientos, como los triggers de nivel 2.

Además, se ha propuesto un modelo para la mejora e IPv6 Móvil Jerárquico, junto con un nuevo protocolo de selección de MAP, que intenta remediar los mayores inconvenientes del uso de esta extensión.

9.2 Trabajos futuros

A continuación se presentan los posibles puntos a tratar en una futura continuación del proyecto.

- Estudiar con más detalle el soporte que la capa 2 es capaz de proporcionar y analizar las distintas tecnologías disponibles en dicha capa.

- Dar solución teórica a una serie de problemas que quedaron pendientes, como por ejemplo la posibilidad de eliminar el paquete Fast Binding Update en el caso de utilizar Fast Handover. El antiguo Router de Acceso tiene toda la información necesaria para efectuar el handover, por lo que este paquete no introduce ninguna nueva información, y en el caso de estar utilizando Bicasting, no se necesita la coordinación con la capa 2 por lo que este paquete pierde toda su utilidad.

- Posibilidad de establecer un banco de pruebas con IPv6 Móvil, con el uso del software disponible en este momento, como es MIPL o USAGI.

- Realización de una simulación con software como Network Simulator 2 (NS-2), que actualmente tiene unas extensiones, Mobiwan (Inria, Francia), que cubren IPv6 Móvil y IPv6 Móvil Jerárquico.
- Ampliación del estudio en las áreas de seguridad y calidad de servicio.

10. Bibliografía

[3G/4G WIRELESS]
"Providing Application-level QOS in 3G/4G wireless systems: A comprehensive framework based on multi-rate cdma", F.Fitzek, A.Koepsel, A. Wolisz, M. Krishnam, M. Reisslein. Technical University of Berlin and Arizona State University.

[ACTNETW_MOB MULTIMEDIA]
"Componet-based Active networks for mobile multimedia systems", S.Schmid. J.Finney. A.C Scott, and W.D Sheperd. Lancaster University. UK.

[BICASTING]
"Simultaneous Bindings for Mobile IPv6 Fast Handoffs", version 1. Karim El Malki, Hesham Soliman, Ericsson Radio Systems, November 2001.

[COMPMOB]
"Comparison of IP Micromobility Protocols", Campbell, Gomez, Kim, Wan, Turanyi, Valko

[DELAY_END_TO_END]
"End-to-end dealy analysis for interactive services on a large-scale IP network", Michel Mandjes ..

[DEPLOYIPV6]
"Deploying IPv6", Alain Durand (Sun Microsystems), February 2001,

[FASTHO]
"Fast Handovers for Mobile IPv6", Dommety G., Yegin A., Perkins C, Tsirtsis G., El-Malki K., Khalil M., Internet Draft, October 2002

[GSMNET]
"Overview of the Global System for Mobile Communications", John Scourias:,

[GSMOV]
"GSM Overview", Unknown author,

[HIER_TOPOLOGY]
"Mechanisms and hierarchical topology for fast handover in wireless IP networks", Antoine Stephane. A.H Aghvami, King's College London.

[HMIPv6]
"Hierarchical MIPv6 mobility management (version 07), Karim El Malki, Hesham Soliman, Ericsson Radio Systems and Claude Casteluccia, Ludovic Bellier, INRIA, Internet draft, October 2002.

[IP_QoS_IN_MOBILE_ENV]
"Enabling IP QOS in Mobile Environments", Victor Marques, Rui Aguiar.. Universidade de Aveiro.

[IPMMOBP]
"IP Micro-Mobility Protocols Campbell", Gomez-Castellanos

[IPV6]
"RFC 2460 – Internet Protocol, Version 6 (IPv6) Specification". S. Deering (Cisco), R. Hinden (Nokia), December 1998, Available at http://www.ietf.org.

[IPV6GAININGGROUND]
"Is IPv6 Finally Gaining Ground?", George Lawton, August 2001,

[JONASWILLÉN]
M.Sc. Thesis "Introducing IPv6 and Mobile IPv6 into an IPv4 wireless Campus network", Jonas Willén, Telecommunication System Lab at the Department of Microelectronics and Information Technology, 27th February 2002

[MIP_UNPLUGGED]
"Mobile IP, the Internet Unplugged", James D.Solomon, 1998, Prentice Hall.

[MIPV6]
"Mobility Support in IPv6 - version 20", David B. Johnson and Charles Perkins, Juary 2003

[MIPV6_MOBMANAGEMENT] "A study on Mobile IPv6 based mobility management architecture", Tsuguo Kato, Fujitsu, 2001.

[MOBCONTHAND]
"Mobile Controlled handover in wireless LANs", Attila Weyland, University of Bern.

[NEIGHB]
"Neigbor Discovery for IP Version 6", RFC 2461

[NETMAGAZINE]

"Network Magazine" November 2002.

[NEXTGEN]
"Next-generation Wireless Internet Protocol Networks", Aura Ganz,

[STALLINGS]

"Comunicaciones y Redes de Computadores". William Stallings. Prentice Hall.

[UMTSOV]
"UMTS Overview (OH-slides)", Nour ElKadri, Jean Nehme,

[VOICETRANSMISSION_WLAN] "Voice transmission in an IEEE 802.11 WLAN based access network", Andreas Köpsel, Adam Wolisz. Telecommunication Network Group. Technical University of Berlin

[VOICEQUALITY]"Voice Quality in converging telephony and IP networks", The Internet Engineering Consortium, Web proforum tutorials.

[VOIP TUTORIAL]
"Voice over IP tutorial", CommWeb.com, 2001.

Apéndice 1. Glosario de términos

aAR	anchor Access Router
AP	Access Point
AR	Access Router
BACK	Binding Acknowledgement
BU	Binding Update
CN	Correspondent Node
CoA	Care-of Address
DAD	Duplicate Address Detection
F-Back	Fast Binding Acknowledgement
F-BU	Fast Binding Update
F-NA	Fast Neighbor Advertisement
HA	Home Agent
HACK	Handover Acknowledgement
HI	Handover Initiate
HTT	Handover To Third
MAP	Mobility Anchor Point
MN	Mobile Node
nAR	new Access Router
nCoA	new Care-of Address
oAR	old Access Router
oCoA	old Care-of Address
PrRtAdv	Proxy Router Advertisement
QoS	Quality of Service
RtAdv	Router Advertisement
RtSol	Router Solicitation
RtSolPr	Router Solicitation Proxy

Apéndice 2. Aplicaciones en tiempo real

2.1 Introducción

La tendencia actual en el mercado de las comunicaciones señala una convergencia de todo tipo de transmisiones, tanto de voz como de datos, en un mismo protocolo de red, tanto para redes fijas como inalámbricas. El uso de la tecnología IP soluciona algunos de los problemas de compatibilidad que se producen entre tecnologías distintas, pero al mismo tiempo, los mecanismos de calidad de servicio no están plenamente adaptados a la movilidad entre las diferentes tecnologías.

Idealmente, una aplicación en tiempo real, como Voz sobre IP, debe ser capaz de moverse a través de una red fija, una Wireless LAN o una red UMTS. En este escenario tienen que producirse varios y diferentes handovers: handovers entre tecnologías diferentes (handover vertical) y handover entre celdas de la misma tecnología (handover horizontal). Estos handovers tienen que producirse de una manera transparente al usuario, y para esto, el handover debe hacerse en un periodo corto de tiempo, y sin interferir en la comunicación en curso.

El nuevo grado de libertad que las comunicaciones inalámbricas proporcionan ha convertido a este tipo de dispositivos en extremadamente populares. El cliente típico de este tipo de aplicaciones espera que los servicios ofrecidos por las redes fijas sean ofrecidos también por las redes inalámbricas, y quiere que no haya distinción entre los dos tipos de comunicación. Esto supone un gran esfuerzo, ya que en la comunicación inalámbrica todos los servicios tienen que ofrecerse a través de enlaces con una gran tasa de error, y que sufren con gran frecuencia desvanecimientos. La gran variedad de aplicaciones que existe requiere diferentes tratamientos con respecto a la calidad de servicio. Algunas de las aplicaciones en auge son las siguientes:

- Datos: WWW, FTP, E-mail.
- Transacciones: WWW Seguro.

- Networking: NFS.
- Tiempo Real: Videoconferencia, Voz sobre IP.
- Streaming: Video bajo demanda.
- Juegos.

Los servicios de Voz sobre IP están incrementando su fama debido a sus ventajas con respecto al precio. La videotelefonía se consideró durante mucho tiempo como una aplicación emergente, sin embargo, su elevado precio y sus grandes requerimientos técnicos han evitado hasta ahora su despegue.

En las aplicaciones de streaming, el audio y el video se ejecutan a la vez que se produce la descarga. Las aplicaciones de video bajo demanda son capaces de proporcionar servicios de aprendizaje a distancia, películas bajo demanda y retransmisión de eventos importantes. Deben resolverse varios problemas para la mejora de la transmisión de video. En primer lugar, los actuales algoritmos de compresión de video admiten pocos errores en la transmisión, y en segundo lugar, hay una falta de mecanismos que proporcionen una adecuada calidad de servicio. Es necesaria una mejora tanto en el backbone como en el bucle de abonado para que puedan proporcionar calidad de servicio al streaming de video. También es necesario que se mejoren los mecanismos de compresión de video para hacer frente al retraso y al jitter (diferencia entre los retrasos de distintos paquetes). MPEG-4 es un estándar para la codificación y el transporte de audio y video sobre distintos tipos de redes. La IETF ha desarrollado el protocolo de reserva de recursos RSVP, para proporcionar calidad de servicio a los flujos de datos en redes IP. Otra manera de evitar la congestión de la red es reducir el número de saltos del streaming, con el uso de servidores proxy cerca del cliente.

Últimamente estamos asistiendo a una explosión de juegos interactivos a través de Internet. El mayor problema técnico es el de predecir y reducir el retraso de los paquetes a través de la red. Para que un juego multijugador sea realista, los movimientos que un jugador hace en su ordenador tienen que quedar inmediatamente reflejados en la pantalla del otro jugador. En un sistema multijugador en el que los participantes se encuentren relativamente cerca, es normal que se retarde unos 30-40

ms los movimientos de los jugadores para compensar el retraso de la red. Recientes estudios que han investigado el tráfico de los juegos por Internet han llegado a la conclusión de que este tipo de juegos no necesita unos grandes requerimientos en cuanto a ancho de banda, aunque los requerimientos en cuanto el retraso son bastante exigentes, en torno a los 100 ms.

En la siguiente tabla se muestran varias aplicaciones junto con los requerimientos de ancho de banda, pérdidas y retraso.

Tipo	Tipo	Tipo	Ancho de Banda (Kbps)	Pérdidas(%)	Retraso (ms)
Datos		FTP	Sin límite	0	TCP timer
Real Time	Audio	Voz	Menos que 64	0.0001	Menos que 300
Real Time	Audio	Voz sobre IP	10-64	0.05	Menos que 300
Real Time	Video	MPEG-4	Menos que 2000	0.01	Menos que 40
Real Time	Video	H.320	Menos que 64	0.0001	Menos que 40
Non Real Time	Audio	CD	150	0.0001	Longitud del buffer
Non Real Time	Video	MPEG-4	Sin límite	0	Longitud del buffer
Juegos		Estrategia	20	0-0.01	500 ms
Juegos		Acción	20	0-0.0001	100 ms
Network Service		NFS	Sin límite	0	-

Tabla 1 Requerimientos en términos de ancho de banda, retraso y pérdidas para varias tipos de aplicaciones

2.2 Integración de las tecnologías de voz y datos

La integración de las tecnologías de voz y datos es interesante tanto para los proveedores de servicio como para las empresas. A los proveedores de acceso les atrae la idea del bajo costo de los modelos existentes. El coste de voz sobre IP se estima que es entre un 20 y un 50 por ciento más barata que los tradicionales servicios de voz basados en la conmutación de circuitos. También están interesados por otro tipo de ahorros, los asociados a la reducción del coste de mantenimiento y un control de la red más eficiente.

La integración de las tecnologías de voz y datos se ha acelerado enormemente debido a las presiones de proveedores y consumidores. En el lado de la demanda, los clientes están invirtiendo en infraestructura de red para aprovechar aplicaciones integradas como las de voz. Por el lado de los proveedores, éstos están aprovechando los avances de tecnología, estándares y tecnología de red.

Avances recientes en la tecnología están permitiendo la integración de las tecnologías de voz y datos. Por ejemplo, los nuevos Procesadores Digitales de Señal han permitido el procesamiento de señales analógicas en el dominio digital, cosa que era impensable hace sólo unos años. Estos potentes procesadores ofrecen una tremenda capacidad de proceso, permitiendo el muestreo, la digitalización y la compresión de las señales en tiempo real. Los nuevos procesadores pueden manejar hasta cuatro conversaciones de voz al mismo tiempo, y está previsto aumentar el rendimiento a corto plazo. Estas tecnologías reducen el coste y la complejidad del desarrollo de nuevos productos, y favorecen la implantación de soluciones de voz sobre enlaces de datos.

En otras áreas se han podido apreciar los avances de la tecnología de los codec de voz. Anteriormente, se asumía que la calidad de la voz disminuiría a la vez que se disminuye el ancho de banda con una relación lineal. Ahora es posible obtener un sonido de una calidad razonable con una fracción de ancho de banda que se requería anteriormente. Y más importante, esos nuevos algoritmos se han incorporado a los estándares para permitir la interoperabilidad de voz comprimida.

La tecnología de transmisión de datos ha mejorado hasta el punto de que la voz puede ser mandada de una manera segura. En los últimos años, el crecimiento del tráfico de voz ha sido pequeño, mientras que el tráfico de datos ha crecido de una manera exponencial. El resultado es que el tráfico de datos supera al tráfico de voz en muchas redes. Además, la importancia relativa del tráfico de datos ha crecido, ya

que más y más empresas y organizaciones están basando sus negocios en la ubicuidad de sus datos. Esta creciente importancia de las redes de datos ha forzado a un cambio fundamental en la forma en la que las redes se diseñan y se construyen. Los típicos esquemas basados en best-effort, sin garantía de servicio, han dado paso a avanzados esquemas que ofrecen calidad de servicio a un amplio rango de aplicaciones.

2.3 Voz sobre IP

Voz sobre IP (VoIP) se empezó a desarrollar hace pocos años. A diferencia de voz sobre Frame Relay o voz sobre ATM, voz sobre IP es una solución de nivel 3, y puede por tanto ser enrutado sobre cualquier tipo de infraestructura de red, incluido Frame Relay y ATM. La calidad sin embargo puede que sea la peor de entre las tecnologías de voz paquetizadas, ya que la calidad de servicio no puede garantizarse en este tipo de redes. Protocolos como TCP son insensibles al retraso, pero deben retransmitir los paquetes que se pierden debidos a colisiones o congestión. La voz, sin embargo, es mucho más sensible al retraso que a la pérdida de paquetes. Además de la congestión del tráfico, la calidad de servicio proporcionada depende de los protocolos de las capas inferiores, que ignoran la existencia de los paquetes de voz.

Las tecnologías de Voz sobre IP usan para la transmisión de voz los paquetes RTP sobre IP, y soportan una gran variedad de codecs de compresión.

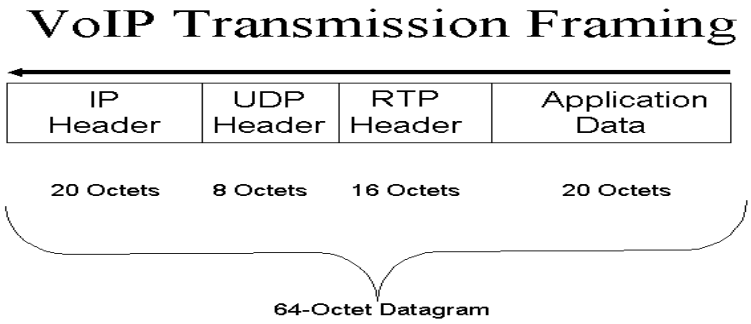


Figura 14: Paquete RTP

Después de que la voz se haya comprimido y convertido a datos, el próximo paso es pasarlos a un flujo de RTP (Real Time Protocol), para la transmisión a través de Internet. Los diseñadores de red deben tener en cuenta tanto el ancho de banda como el retraso a la hora de diseñar las redes. El ancho de banda disponible es crítico, y viene determinado no sólo por los codecs utilizados, sino por la sobrecarga originada por las cabeceras IP, y otros factores. El ancho de banda es una cuestión especialmente crítica en el caso de caros enlaces WAN. El retraso viene determinado por el retraso de propagación, (velocidad de la luz), el retraso de serialización, que es causado por la puesta en los buffers de los paquetes por los dispositivos que atraviesa, y por el retraso de paquetización.

El ancho de banda de una conversación de voz sobre IP depende de una variedad de factores. El primer es el codec empleado en la codificación puede ser tan pequeño como de 3 o 4 Kbps hasta 64 Kbps. Los paquetes de voz son muy pequeños, y típicamente no contienen más de 20 bytes de información.

Voice Activity Detection (VAD) se usa en el origen para regular el flujo de paquetes parando la transmisión si el nivel de voz analógica cae por debajo de un determinado umbral. Esto tiene el resultado de reducir el ancho de banda consumido a la mitad, ya que una persona permanece en silencio aproximadamente la mitad del tiempo.

Otra herramienta usada por los ingenieros de diseño de red es la compresión de las cabeceras RTP, ya que la gran parte de la información contenida en esas cabeceras está duplicada o es redundante.

La calidad de la voz se puede ver afectada fundamentalmente por dos factores, que son la pérdida de paquetes y el retraso. La pérdida de paquetes hace que se produzcan pequeñas interrupciones y saltos en la comunicación. Los modernos DSPs pueden corregir hasta 30 ms de voz perdida. Cada paquete de voz sobre IP contiene unos 20 ms de muestras de voz, por lo que, teniendo en cuenta la corrección del DSP, sólo puede perderse un paquete de voz.

El retraso de los paquetes puede causar que se degrade la calidad de la conversación, en el caso de retraso de extremo a extremo, o pérdida de paquetes, en el caso, de retraso variable o jitter. Si el retraso de extremo a extremo es demasiado grande, (unos 250 ms), la conversación empieza a resultar extraña. Si se produce jitter, hay un riesgo de que se produzca un llenado del buffer en el receptor. El

tamaño de este buffer suele ser de unos 20 a 50 ms, y se utiliza para que la voz se vaya reproduciendo al ritmo correcto, y no se produzcan interrupciones.

El estándar G.114 de la International Telecommunications Union (ITU) establece un retraso máximo de extremo a extremo de 150 ms, aunque se ha demostrado que son igualmente admisibles retrasos de 200 ms.

Actualmente, el jitter es el mayor impedimento para la transmisión de voz sobre Internet. Una típica llamada de voz sobre IP atravesará muchos enlaces diferentes, con una gran diferencia en los retrasos. Como resultado, la calidad de la voz sobre Internet sigue siendo pobre. Los sistemas que están apareciendo se caracterizan por tener un gran buffer en recepción, lo que puede añadir retrasos de hasta 1 segundo.

En un futuro, cuando los proveedores de acceso a Internet mejoren las características de calidad de servicio de sus redes, las soluciones de voz sobre IP se harán muy populares e incluso será un servicio añadido gratuito, que vendrá dado por la conexión a Internet.

Apéndice 3. Calidad de Servicio

Históricamente, las redes basadas en IP han sido capaces de proporcionar un servicio de entrega sencillo y de máximo esfuerzo a todas las aplicaciones que permitían estas redes. El servicio de mejor esfuerzo trata a todos los paquetes de igual forma, sin niveles de servicio, requerimientos, reservas o garantías. Aunque la cabecera de IPv4 está equipada con campos que pueden especificar nivel de preferencia y tipo de servicio, en general esta información se ha ignorado por los dispositivos de encaminamiento. El estilo de mejor esfuerzo ha funcionado en general bien: los usuarios pueden tolerar algún retardo y la variabilidad en la velocidad de los datos (jitter) para el correo electrónico, transferencia de ficheros o navegación web. Pero las necesidades de los usuarios han cambiado, con aplicaciones que requieren tratamiento en tiempo real, como voz o video. Para este tráfico sensible al retardo, la técnica del mejor esfuerzo sólo funciona bien cuando hay abundantes recursos de red desde un extremo de Internet al otro. El único esquema de interconexión diseñado desde un principio para dar soporte a este tipo de aplicaciones es ATM. Sin embargo, la confianza en ATM significa o bien construir una segunda infraestructura de interconexión para el tráfico en tiempo real, o reemplazar la existente basada en IP, las cuales son alternativas costosas.

De esta forma, existe una fuerte necesidad de ser capaz de soportar una gran variedad de tráfico con una gran variedad de requisitos en cuanto a la calidad de servicio (Quality of Service, QoS) dentro de una arquitectura TCP/IP. Un mecanismo de QoS traduce una petición de servicio, como por ejemplo, una llamada de teléfono por Internet, en un conjunto de características de tráfico para ese servicio, como el rendimiento, el retardo, la variación de retardo, pérdidas y tasa de errores. El mecanismo de QoS debe ser capaz de medir estas características de tráfico y utilizar técnicas de encaminamiento y de tratamiento de colas para conseguirlo. Algunos mecanismos de QoS también tratan de obtener recursos de la red (capacidad y memoria de almacenamiento) suficientes para garantizar estas características. El requisito fundamental es incorporar es incorporar una nueva funcionalidad a los dispositivos de encaminamiento y un medio para solicitar un servicio basado en QoS

para un conjunto de redes. Para satisfacer este requisito, la IETF está desarrolando una serie de estándares bajo la denominación general de Arquitectura de Servicios Integrados (ISA), pensado para proporcionar transporte de QoS sobre redes basadas en IP.

La calidad de servicio (QoS) se refiere a la capacidad de la red de proporcionar mejores servicios a determinado tráfico. El primer objetivo de la calidad de servicio es proporcionar algún tipo de prioridad, como ancho de banda dedicado, retraso y jitter controlado, y características de pérdidas mejoradas. Es importante que el proporcionar prioridad a un flujo no vaya a producir el fallo del resto de las comunicaciones.

Fundamentalmente, la calidad de servicio permite dar un mejor servicio a ciertos flujos de paquetes. Esto se consigue elevando la prioridad de los paquetes de un flujo o bajando la prioridad de los paquetes de otro flujo. Cuando se usan herramientas para el control de la congestión, se intenta elevar la prioridad de un flujo, colocando los flujos en colas diferentes y dando distinto tratamiento a cada cola. Las herramientas que se usan para evitar la congestión, eliminan los paquetes de prioridad más baja. Herramientas basadas en la política a seguir, como RED, dan prioridad a un flujo, limitando el ancho de banda disponible para otros flujos. Se procede al descarte de los paquetes cuando se sobrepasen la cantidad establecida de ancho de banda. Herramientas de optimización del enlace dan preferencia a pequeños flujos en detrimento de grandes flujos. Otras herramientas, como RSVP, reservan recursos que sólo podrán ser usados por ese flujo.

En el caso de voz sobre IP, la calidad de la voz se ve afectada en gran medida por el retraso y el jitter, por lo que es necesaria la implementación de mecanismos de calidad de servicio a la hora de diseñar una red.

Los elementos para proporcionar una buena calidad de servicio incluyen acciones ante la pérdida de paquetes, el retardo, el jitter y la utilización eficiente del ancho de banda. A continuación se definen una serie de herramientas definidas para lograr el objetivo de proporcionar calidad de servicio:

- Herramientas basadas en la política a seguir. Proporciona la posibilidad de la limitación de la tasa de transmisión de paquetes, a menudo simplemente eliminando los paquetes que exceden un determinado límite umbral previamente establecido. Estas herramientas basadas en la política se pueden

aplicar tanto en el flujo de salida como en el de entrada de un dispositivo. Ejemplos de esta herramienta son RED (Ramdom Early Detection) y WRED (Weighted RED).

- Herramientas basadas en el uso de buffers. Proporciona la capacidad para el control tanto de los flujos de salida como de entrada de un dispositivo, pero a diferencia de los métodos basados en la eliminación de los paquetes, estas herramientas proceden al almacenamiento temporal de los paquetes en un buffer. Estos métodos añaden retardo y jitter debido al empleo del buffer.

- Herramientas basadas en la reserva de recursos a través del camino. Permiten la reserva de recursos en el camino que un paquete toma desde el origen hasta el destino. Un ejemplo de este tipo de herramientas es RSVP (Resource Reservation Protocol).

- Herramientas basadas en colas. Se emplean diferentes colas para la transmisión de diferentes tipos de aplicaciones, como voz y datos. Permiten dar prioridad a los paquetes sensibles al retraso, a favor de paquetes no sensibles. Ejemplos son Weighted Fair Queuing y IP RTP.

- Herramientas basadas en el empleo de etiquetas. Se emplean etiquetas que se incluyen en los paquetes para así poder identificar a aquellos que requieren un tratamiento especial.

- Herramientas basadas en la fragmentación. Permiten el dividir paquetes de gran tamaño en paquetes más pequeños. Esto es fundamental en el caso de que un pequeño paquete sensible al retraso tenga que esperar a la transmisión de uno grande. Permite a los pequeños paquetes de voz intercalarse entre los espacios de los paquetes grandes fragmentados. Los paquetes grandes son reensamblados por el router al otro lado del enlace por lo que el procedimiento es transparente a la aplicación de datos

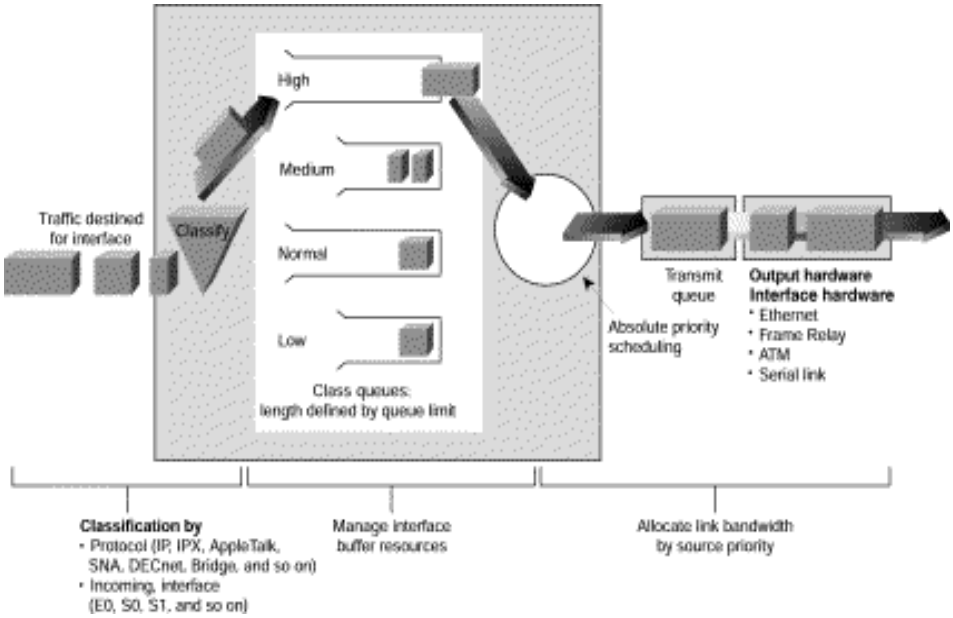


Figura 15: Planificación por medio de colas