Despegando con movilidad IPv6 (MIPv6)

Miguel Ángel Díaz Fernández, César Olvera Morales
{miguelangel.diaz, cesar.olvera}@consulintel
CONSULINTEL

Pedro García Segura
pedrogs@dif.um.es
Universidad de Murcia

Resumen*.El modelo de conectividad a Internet está evolucionando rápidamente hacia un enfoque basado en la movilidad de los usuarios gracias a la aparición de nuevos dispositivos portátiles y a la cada vez más extensa cobertura de las redes de acceso. Los operadores ven una fuente importante de ingresos en un servicio de movilidad basado en IPv6 (MIPv6) que permita a sus usuarios ser siempre alcanzables por terceros con independencia de la red en la que se encuentren. Sin embargo, aunque MIPv6 está estandarizado desde hace tiempo, aún quedan algunos flecos que es necesario resolver para permitir el despliegue a gran escala del servicio de movilidad.*

1 Introducción

Recientemente han empezado a aparecer todo tipo de dispositivos de red que permiten al usuario estar conectado a Internet en cualquier lugar gracias a las tecnologías inalámbricas. No solamente PCs portátiles sino también PDAs, consolas de juegos, e incluso recientemente teléfonos móviles celulares y muchos más que son difíciles de visionar en el presente.

Estos dispositivos van a empezar a cambiar el modelo de conectividad a Internet con el que se trabaja en el presente.

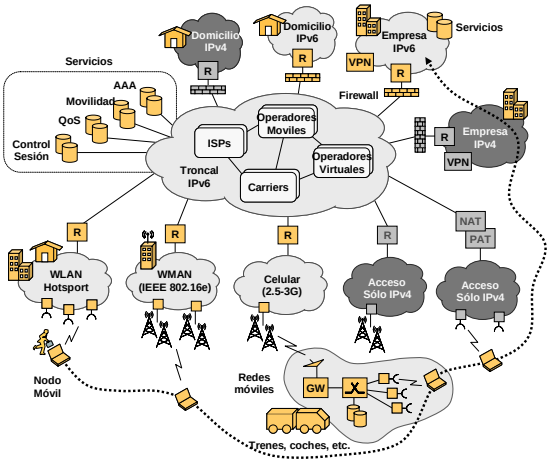

Figura 1. Escenario basado en movilidad IP

Actualmente cuando un usuario se desplaza viajando por distintas redes (*roaming*), cada una de las nuevas redes visitadas por las que pasa le proporciona una dirección IP diferente a la que poseía en la red anterior de la que proviene, por lo que el usuario no puede mantener una sesión de aplicación abierta durante el desplazamiento. Esto significa por ejemplo, que si el usuario tenía una conversación con otro usuario mediante voz sobre IP (VoIP), dicha conversación se corta en el momento en que el usuario móvil realiza el cambio de red.

El modelo actual de conectividad impide la aparición de nuevos servicios basados en el escenario de la figura 1, como la recepción en cualquier momento de mensajes multimedia; distribución de noticias; integración de comunicación vocal en aplicaciones; comunicaciones IP con servicios de seguridad; localización de flotas de autobuses, camiones; etc.

IETF desarrolló un nuevo modelo de conectividad a Internet que soluciona los problemas mencionados anteriormente. A esta tecnología se la conoce con el nombre de movilidad IP, la cual no es operativa sobre IPv4 por diversos motivos[1] pero gracias a IPv6 (el protocolo de red sucesor del actual IPv4) y sobre todo al protocolo de movilidad sobre IPv6 (MIPv6) [1] la puesta en práctica de un modelo de conectividad con soporte de movilidad del usuario parece más realista.

1.1 Funcionamiento básico de MIPv6

En MIPv6 se definen tres agentes diferentes: *Home Agent* (HA), *Mobile Node* (MN) y

[1] Sin ánimo de ser exhaustivo, algunos de los problemas que presenta MIPv4 son: necesidad del despliegue de un nodo especial en las redes visitadas (*Foreing Agent*); necesidad de autenticación entre el *Foreing Agent* y el *Home Agent* y entre el *Mobile Node* y el *Foreing Agent* basada en infraestructuras de AAA; uso de NATs debido a la escasez de direcciones IPv4 públicas, etc.

Correspondent Node (CN). El HA es un agente que se despliega en la red del operador que despliega el servicio de movilidad. Es el encargado de tener registrada la "verdadera posición" del nodo móvil. Por su parte, el MN es el dispositivo del usuario que cuando se encuentra en la red de su operador tiene una dirección IPv6 denominada *Home of Address* (HoA) y cuando se desplaza y se encuentra en una red visitada adquiere una dirección diferente, denominada *Care of Address* (CoA). Por último, el CN es un nodo que pretende contactar con el MN y que en principio si no sabe cual es su posición real trata de contactar usando la HoA del MN.

El funcionamiento básico de MIPv6 se muestra en la figura 2. Cuando el MN se encuentra en una red visitada lo primero que hace es enviar a su HA un mensaje de señalización para notificar su verdadera posición (1), es decir, informa de la dirección IPv6 que tiene en ese momento (CoA). El HA actualiza su base de datos para ligar la dirección que tendría el MN en la red del operador (HoA) con la que realmente tiene en ese momento (CoA).

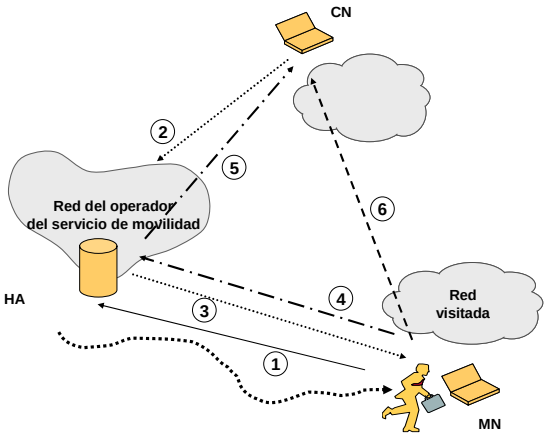

Figura 2. Funcionamiento básico de MIPv6

Cuando un CN quiere contactar con el MN (por ejemplo un usuario que quiere establecer una llamada de VoIP con el MN), lo que hace es intentar contactar con el MN a través de su HoA (2), ya que es la dirección fija conocida por el CN. Los paquetes enviados a la red del operador y dirigidos a la HoA del MN son interceptados por el HA, encapsulados en un paquete MIPv6 y re-dirigidos hacia la nueva dirección CoA que el nodo móvil tiene en la red visitada (3).

El MN contesta al CN encapsulando los paquetes de datos en un paquete MIPv6 y se lo envía al HA(4), el cual extrae el paquete original del paquete MIPv6 recibido y se lo envía al CN(5).

Si el CN tiene soporte MIPv6, entonces es posible que el MN contacte con el CN para informarle que su dirección IPv6 en el momento de estar en la red visitada es la CoA y no la HoA, de manera que el CN envía los paquetes de datos directamente a la CoA del nodo móvil (6). A este procedimiento se le denominada *Route Optimization* y es una mejora en el camino seguido por los paquetes puesto que no tienen que pasar por el HA, lo cual introduce retardos innecesarios. Si el CN no posee soporte MIPv6 entonces no es posible que el CN y el MN puedan comunicarse directamente usando la función *Route Optimization*.

Si el MN vuelve a cambiar de red, obtendrá una nueva CoA que deberá registrar en su HA con el fin de estar siempre alcanzable por cualquier CN que quiera comunicar con él.

1.2 Carencias de MIPv6

El mecanismo anteriormente descrito corresponde al protocolo estandarizado por IETF[1] y funciona de una manera efectiva y eficiente. Sin embargo para que el despliegue de MIPv6 a gran escala en un operador sea realizable es necesario aún cierto trabajo, como el que se está realizando en el proyecto IST ENABLE [13], para abordar diferentes aspectos de configuración de forma dinámica. En concreto, el protocolo de movilidad sobre IPv6 [1] solo proporciona la definición de los agentes involucrados en el soporte de movilidad, su funcionamiento y sus interacciones, lo cual es suficiente si pensamos en un despliegue experimental o a baja escala en el que participen muy pocos usuarios y donde la configuración de los agentes implicados es predominantemente manual. Sin embargo si pensamos en movilidad como servicio de producción en un operador el marco de estandarización actual no es suficiente.

Aún más escaso es el marco desarrollado para garantizar la seguridad en el servicio de movilidad. En el IETF se han desarrollado las pautas [2] para integrar IPsec (concretamente el uso de la cabecera ESP [10] de IPsec) en la señalización del servicio de movilidad (MIPv6), lo cual es beneficioso puesto que garantiza la confidencialidad y la integridad de las comunicaciones, pero es insuficiente puesto que no se menciona nada acerca de la distribución de las claves que serán utilizadas por el MN o por el HA para cifrar dichas comunicaciones.

Existen aún por tanto algunos problemas relacionados con la configuración dinámica de los nodos que intervienen en el servicio de movilidad que requieren una solución cuando un proveedor de servicios pretende desplegar el servicio de movilidad a gran escala, con centeneras o millares de usuarios, puesto que el marco de estandarización actual [1, 2, 3, 4, 5] no los contempla. A continuación se realiza una descripción de los principales problemas actuales y las soluciones consideradas por el proyecto ENABLE [13].

2 Inicializando el servicio de movilidad

Cuando un usuario inicia el servicio de movilidad está en disponibilidad de ser alcanzado siempre a través de la misma dirección IP (su HoA), incluso aunque se desplaza y se encuentre en otras redes diferentes a las de su operador. Sin embargo para que esto pueda llevarse a cabo es necesario realizar una serie de pasos destinados a la configuración automática y de forma dinámica del servicio de movilidad. A continuación se describen dichos procesos.

2.1 Autenticación y autorización del usuario

Cuando un proveedor piensa en el despliegue de movilidad, lo primero que debe afrontar es la identificación del usuario (autenticación) para posteriormente comprobar si dicho usuario tiene derecho a disfrutar del servicio de movilidad (autorización) y en su caso computar el tiempo que ha estado disfrutando del servicio para su posterior facturación. Estos son requisitos básicos no cubiertos tampoco por el marco de estandarización actual de MIPv6 y que el operador precisa para el despliegue de cualquiera de sus servicios comerciales. Este tipo de funciones se realizan habitualmente por medio de una infraestructura de AAA (*Authentication, Authorization and Accounting*), basada en los protocolos RADIUS [6] o Diameter [7].

2.2 Asignación del HA

Además de la autenticación, autorización y facturación del usuario, para la correcta configuración del servicio de movilidad el proveedor debe ser capaz de proporcionar diversos datos relacionados con la red del proveedor. En concreto, el proveedor debe proporcionar la *Home Network* (HN), es decir, el prefijo de la red a la que el usuario (en realidad el MN del usuario) pertenece de forma permanente mientras éste se encuentra desplazándose por otras redes. Además de la HN el MN debe ser configurado con la dirección IPv6 que tendrá dentro de la HN, es decir la *Home Address* (HoA). Para ello el proveedor podrá proporcionársela al MN mediante algún mecanismo no estandarizado aún, o alternativamente y gracias a las características de autoconfiguración de IPv6 [8], este podría ser capaz de crear su propia HoA una vez sabido el prefijo de la HN a la que pertenece.

Por otra parte, es lógico pensar que cuando un operador realice el despliegue a gran escala de este tipo de servicios, vaya a utilizar varios HAs con el fin, no solo de conseguir una redundancia del servicio ante eventuales averías de alguno de estos nodos, sino también para poder distribuir de una manera eficiente la carga de procesamiento de paquetes para atender a todos los usuarios demandantes del servicio. El estándar de MIPv6 [1] define un método básico para descubrir un HA una vez conocida la HN, el cual se basa en el uso de direcciones IPv6 de tipo *anycast* [9]. Sin embargo este método no permite un reparto equitativo de la carga de procesamiento entre los diversos HAs existentes, por lo que es mucho más recomendable la definición de un mecanismo que sea capaz de asignar un determinado HA al MN de un usuario cuando este solicita el inicio del servicio. Además dicho mecanismo debería ser capaz de reasignar al MN un nuevo HA en el caso de detectar que el que se le ha asignado inicialmente está sobrecargado o incluso se ha averiado.

2.3 Intercambio del material criptográfico

Como se ha descrito previamente, el uso de la cabecera ESP de IPsec [10] es uno de los métodos definidos en MIPv6 para la protección de los paquetes de señalización entre el MN y el HA[2]. Con este mecanismo se garantiza no solo la autenticación mutua de los nodos sino además se proporcionan herramientas para la encriptación de los paquetes intercambiados entre los nodos que utilizan el servicio de movilidad. Así pues con la protección de la señalización con IPsec además de confidencialidad se consigue garantizar que dichos paquetes no han sido modificados en el camino hasta llegar a nodo destino.

Pero para que IPsec funcione apropiadamente es necesario definir en ambos nodos (MN y HA) el

material criptográfico adecuado que permita establecer las asociaciones de seguridad (*security associations*, SAs) que IPsec maneja durante su funcionamiento en el nodo donde está implementada. De nuevo el estándar de MIPv6 no define ningún método en concreto para el intercambio del material criptográfico entre los nodos que permita el establecimiento de las SAs.

Una alternativa habitual es la configuración manual de las claves utilizadas en el establecimiento de las SAs, pero obviamente esta solución no es viable en el caso del despliegue de un servio a gran escala en un operador.

Alternativamente se puede emplear el protocolo IKE [11] como herramienta para la automatización del intercambio de claves y establecimiento de SAs. Sin embargo es un protocolo demasiado complejo y difícil de depurar como para ser usado en un entorno con millares de usuarios.

Finalmente, el uso de IKEv2[12] parece mucho más recomendable puesto que es un protocolo más simple, con posibilidades reales de ser implementado en dispositivos portátiles que se caracterizan por la escasez de recursos hardware (capacidad de procesamiento, memoria, etc.), aunque de nuevo no hay ninguna estandarización o recomendación de cómo integrar este protocolo en el servicio de movilidad.

2.4 *Bootstrapping* y sus escenarios

Los tres pasos anteriores son esenciales para que un MN pueda iniciar el servicio de movilidad y lo deseable es poder realizarlos de la manera más rápida posible con el fin de que el usuario no tenga que realizar largas esperas durante el inicio del servicio.

La mejor solución para ello es agrupar todos esos pasos en un procedimiento único mediante el cual el usuario no solamente se autentica frente al operador, sino que también se le informa de diversos parámetros de red (HN, HoA) necesarios para el inicio de la movilidad, se le asigna un HA y se establece el material criptográfico para el establecimiento de las SAs que permitan cifrar la señalización MIPv6.

A este procedimiento único se le conoce con el término de MIPv6 *bootstrapping* [14] y en el proyecto ENABLE [13] se ha estado trabajando para identificar los diferentes escenarios en los que se puede realizar el *bootstrapping*, los agentes que intervienen y el modo en el que interactúan.

El análisis del problema del *bootstrapping* comienza con la identificación de las entidades involucradas en el servicio de movilidad y las relaciones entre ellas. Las entidades identificadas son:

- ASA (*Access Service Authorizer*): es el operador de red que autentica a un nodo móvil y decide si está autorizado para recibir acceso a Internet. Los procesos de autenticación y autorización son gestionados por servidores AAA.

- ASP (*Access Service Provider*): es el operador de red que proporciona conectividad IP al nodo móvil. Antes de conceder el acceso a la red, el ASP debe recibir autorización del dominio Home del usuario, es decir, del ASA. Una vez el acceso ha sido autorizado, el ASP debe aplicar las políticas de servicio del ASA y, adicionalmente, las suyas propias, siempre que no entren en conflicto con las establecidas originalmente por el ASA.

- MSA (*Mobility Service Authorizer*): es el operador que autoriza el servicio de movilidad. Como en el caso del ASA, los procedimientos de autenticación y autorización son gestionados mediante servidores AAA del dominio al que pertenece el MSA.

- MSP (*Mobility Service Provider*): es el operador que proporciona el servicio de movilidad (por ejemplo, los *Home Agents*). Para autorizar el servicio, el MSP se pone en contacto con el MSA del usuario a través de su infraestructura AAA. Una vez confirmado que se ha concedido el servicio de movilidad al nodo móvil, el MSP debe aplicar las políticas de servicio requeridas por el MSA, además de las suyas propias (siempre que no entren en conflicto).

Todas estas entidades deben tener una relación de confianza y comunicarse entre ellas para autenticar y autorizar los servicios (por ejemplo, acceso a la red y movilidad). Por este motivo, se asume que hay acuerdos de itinerancia establecidos entre las entidades involucradas.

En base a las relaciones entre ASA, ASP, MSA y MSP, dos escenarios distintos han sido

identificados: el escenario separado (*split*) y el escenario integrado (*integrated*). Ambos escenarios se describen a continuación, según la figura 3.

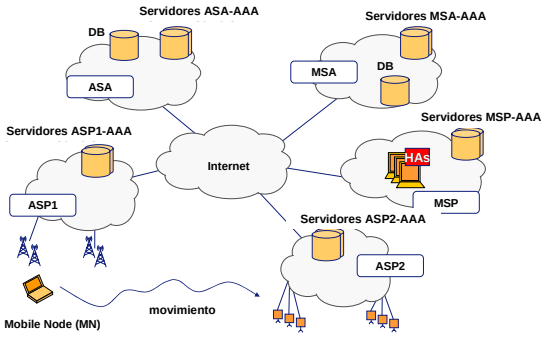

Figura 3. Escenarios de *bootstrapping* y entidades involucradas

En el caso del escenario *split*, el ASA y el MSA son entidades separadas. Un caso típico es un nodo móvil que obtiene conectividad a través de un *hotspot* (en un hotel, por ejemplo), pero hace uso de una tercera entidad, normalmente su operador, para obtener servicio global de movilidad. Esta separación implica que el servicio de movilidad debe ser autorizado por una entidad (MSA) distinta de la que autorizó el acceso a la red (ASA). El proceso de *bootstrapping* en este escenario comienza por el descubrimiento de la dirección del HA, que se realiza mediante consultas DNS. Un vez obtenida la dirección del HA, el nodo móvil debe crear las asociaciones de seguridad requeridas por MIPv6 y obtener una dirección en la red del HA, es decir la HoA. Para autorizar este proceso, el HA debe ser capaz de ponerse en contacto con los servidores AAA del MSA para autenticar al nodo móvil y requerir la autorización del servicio de movilidad. Por suerte, todo este proceso se puede llevar a cabo mediante el protocolo IKEv2, que permite autenticar las credenciales del nodo móvil mediante EAP (EAPoIKEv2), crear las asociaciones de seguridad para Mobile IPv6 y asignar una HoA mediante señalización IKEv2.

En el escenario integrado, el MSA y el ASA son la misma entidad, denominada MASA (*Mobility and Access Service Authorizer*). Un caso común de escenario integrado se da cuando el usuario tiene un contrato con un operador de movilidad que le proporciona tanto acceso a la red como servicios de movilidad. Los pasos necesarios para llevar a cabo el *boostrapping* de MIPv6 en este escenario son básicamente los mismos que en el caso del escenario *split*, con la diferencia de que el descubrimiento del HA no se realiza mediante DNS, sino con DHCPv6 o a través del canal EAP que se establece entre el nodo móvil y el servidor AAA del MASA durante la autenticación para el acceso a la red. Estos métodos de descubrimiento del HA son mucho más flexibles que el uso de DNS, y permiten al operador asignar un HA más cercano al usuario (es decir, uno situado en la red del ASP/MSP en lugar de la red del MASA), además de permitir el uso de algoritmos de balanceo de carga mucho más óptimos que los disponibles en caso de realizar la asignación mediante DNS.

Otra importante optimización se puede realizar en el escenario integrado cuando la red de acceso soporta EAP y el nodo móvil emplea un método EAP que deriva material criptográfico (por ejemplo, EAP-TLS). En ese caso, las claves derivadas por el método EAP tras la autenticación para el acceso a la red son conocidas por el nodo móvil y por el servidor AAA del MASA, y pueden ser empleadas para generar nuevas claves que permitan al nodo móvil usar una clave pre-compartida para la autenticación de los intercambios IKEv2, en lugar tener que realizar otra autenticación EAPoIKEv2 completa como en el resto de los escenarios. Esta optimización implica que la clave pre-compartida es transportada desde el servidor AAA del MASA al HA mediante el uso de una aplicación Diameter [7] específica.

3 Problemas de MIPv6 en las redes visitadas

Los problemas descritos en la sección anterior están relacionados con el inicio del servicio de movilidad, pero no son los únicos con los que un usuario se puede encontrar cuando se desplaza por diferentes redes.

En concreto existen dos obstáculos principales para que MIPv6 pueda funcionar: la presencia de *firewalls* que filtren los paquetes de tipo MIPv6 y la falta de soporte IPv6 en la red visitada por el usuario.

3.1 Atravesando los *firewalls*

En MIPv6 existen dos tipos de tráfico, el relacionado con la señalización que se encarga de iniciar y mantener el servicio de movilidad activo entre los agentes (HA-MN y CN-MN) y el tráfico de datos propiamente dicho que transporta los

datos de aplicación de la comunicación entre el CN y el MN[2].

El tráfico MIPv6 (tanto el tráfico de señalización como el tráfico de datos[3]) utilizan cabeceras de extensión IPv6 específicamente diseñadas para el servicio de MIPv6, lo cual puede representar un problema cuando existen *firewalls* instalados en cualquiera de las redes en las que se encuentran los nodos que intervienen en la movilidad (MN, HA y CN).

Esto es debido a que los *firewalls* pueden no tener soporte de MIPv6, es decir, no entender ni las cabeceras de extensión MIPv6 ni el tráfico que llevan. Por tanto dicho tráfico será directamente bloqueado e impedirá el funcionamiento del servicio de movilidad. En concreto, los problemas derivados de la presencia de *firewalls* sin soporte MIPv6 son básicamente tres:

1. El *firewall* no entiende los mensajes de señalización MIPv6 (BU, BA, CoTI, HoTI) y por tanto se descartan. Como consecuencia no se puede iniciar el servicio de movilidad.

2. El firewall no permite el paso de paquetes IPsec puesto que no es capaz de saber cual es su contenido. Como consecuencia los paquetes de señalización MIPv6 entre el MN y el HA no llegan a su destino y no se puede iniciar el servicio de movilidad.

3. El *firewall* no entiende los mensajes con cabeceras MIPv6 por lo que el tráfico de datos es descartado. Como consecuencia no es posible la comunicación entre el CN y el MN.

En función de si existen uno o varios *firewalls* y de la red en la que se encuentren (red del HA, red visitada por el MN o red del CN) se pueden presentar todos o un conjunto de los tres problemas anteriores.

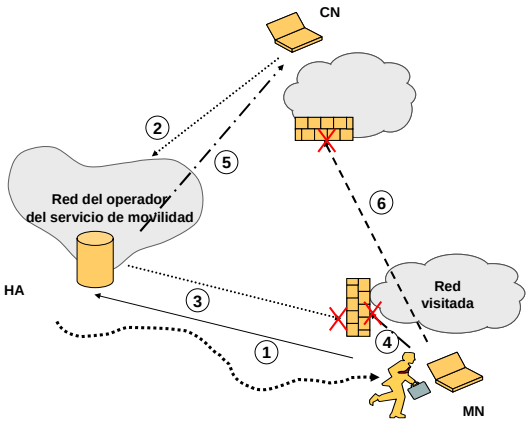

Figura 4. Efecto de los *firewalls* en MIPv6

En ENABLE se han analizado y evaluado diversas tecnologías como posibles soluciones para este problema (*Universal Plug and Play*, *STUN/TURN/ICE*, *Application Layer Gateways*, *Middlebox Communication*, *Simple Middlebox Control*, *NSIS and NAT/FW NSLP* y *Policy Based Networks*) y NSIS [15] apunta ser el protocolo más prometedor que ayudaría a solventar este problema.

La gran ventaja de NSIS frente al resto de tecnologías es que define una arquitectura y un protocolo de señalización que permite a los nodos que manejan tráfico MIPv6 informar a todos los *firewalls* que se deben atravesar hasta alcanzar el destino, del tipo de tráfico que están enviando y de sus características, con el fin de que los *firewalls* se configuren de forma apropiada para que ese tráfico sea cursado.

3.1 Funcionamiento en redes IPv4

Como su nombre indica, MIPv6 es un protocolo diseñado para funcionar sobre redes IPv6. Sin embargo aunque un operador de servicios decida realizar el despliegue de IPv6 en su red para proporcionar este tipo de conectividad a sus usuarios, no es una garantía de que el servicio de movilidad basado en IPv6 sea operativo en cualquier escenario en el que se encuentre el usuario en sus desplazamientos.

De hecho, es muy probable que durante un período de tiempo que es difícil de prever, existan otros operadores en los que no se realice el despliegue de IPv6 y por tanto sus redes sean solo IPv4.

---

[2] El tráfico de datos entre el CN y el MN puede ser intercambiado directamente entre estos dos nodos si el CN tiene soporte de MIPv6 y se usa la funcionalidad *Route Optimization* definida en [1] o bien puede ser enviado a través del HA por medio de túneles bidireccionales entre el HA y el MN si el CN no tiene soporte de MIPv6 o no se ha podido establecer señalización MIPv6 entre el CN y el MN.

[3] A excepción del tráfico de datos entre el CN y el HA cuando no se usa la *Route Optimization* definida en [1].

Esto supone un problema cuando un usuario del servido de movilidad debido a su desplazamiento se encuentra en este tipo de redes, puesto que al tener solo conectividad IPv4 el MN no será capaz de contactar con el proveedor del servicio de movilidad, es decir, con el HA.

Un despliegue real del servicio MIPv6 tiene que tener esta problemática presente y solucionarla de algún modo puesto que a pesar de que IPv6 hace tiempo que ha dejado de ser un protocolo experimental y empieza a estar desplegado en las redes de los operadores más importantes, es seguro que durante un período de tiempo indeterminado habrá otros operadores que no desplieguen este protocolo en sus redes.

En ENABLE se vislumbran dos aproximaciones distintas para dar solución a la problemática de que el MN esté conectado en una red IPv4 y quiera contactar con el HA (IPv6).

1. Utilizar el mecanismo de transición IPv6 *softwires* [16] para que el MN sea capaz de obtener conectividad IPv6 (a pesar de que esté conectado en una red IPv4) y posteriormente utilizar MIPv6 de forma normal como si estuviera conectado a una red IPv6 nativa.

2. Utilizar las extensiones del protocolo MIPv6 (DSMIPv6) que están siendo definidas en el IETF [17] con el fin de que el MN pueda encapsular los paquetes MIPv6 dentro de paquetes IPv4 para hacerlos llegar al HA.

Ninguna de las dos soluciones es lo suficientemente completa como para que sea la solución definitiva sin ningún género de dudas.

Con la solución basada en el uso de *softwires*, el MN que está situado en una red IPv4 contacta con un agente denominado *Softwires Concentrator* (SC) para establecer un túnel IPv6, es decir el MN envía paquetes IPv6 encapsulados en paquetes IPv4 al SC. *Softwires* está basado en el protocolo L2TP (tanto la versión 2, L2TPv2, como la versión 3 L2TPv3 que se acometerá en el futuro), que es un protocolo ampliamente extendido para el establecimiento de VPNs por lo que proporciona un buen soporte para la autenticación del usuario antes de establecer el túnel IPv6. Así pues en realidad la verdadera encapsulación del túnel IPv6 sería:

- IPv4-L2TP-PPP-IPv6-MIPv6 en el caso de que la implementación de L2TPv2 soporte la encapsulación directa sobre paquetes IPv4

- IPv4-UDP-L2TP-PPP-IPv6-MIPv6 en el caso de que la implementación de L2TPv2 no soporte la encapsulación directa sobre paquetes IPv4 o exista un *firewall* o NAT que no permita pasar los paquetes con el encapsulamiento anterior.

Una desventaja importante de esa solución es la sobrecarga que se establece en la comunicación entre el MN y el HA, puesto que los paquetes MIPv6 están encapsulados dentro de paquetes con varias cabeceras.

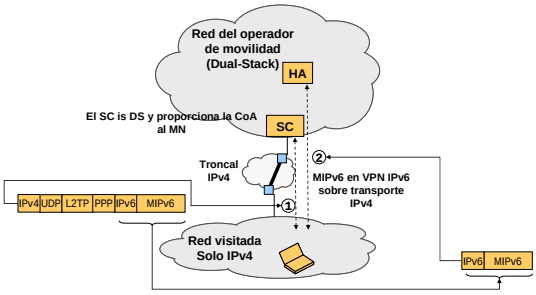

Figura 5. Solución IPv4-MIPv6 usando softwires

Sin embargo tiene una gran ventaja respecto a la otra solución: el HA puede estar ubicado en una red que solo sea IPv6, es decir no tenga conectividad IPv4. En este caso el MN podría utilizar el SC desplegado en otro proveedor (que tuviera tanto conectividad IPv4 como conectividad IPv6) para obtener conectividad IPv6 de él y una vez establecido el túnel IPv6 contactar con el HA.

Por otra parte, con la solución basada en DSMIPv6 se permite el registro en el HA de direcciones CoA tanto IPv4 como IPv6, lo posibilita que el MN pueda estar en una red solo IPv4 y contactar con el HA para registrar su posición. El tipo de encapsulamiento en DSMIPv6 depende del tipo de paquetes:

- IPv4-UDP-IPv6-MIPv6 en el caso de paquetes de señalización MIPv6

- IPv4-UDP-IPv6, en el caso de paquetes de datos entre el HA y el MN cuando hay NAT en la red visitada por el MN

- IPv4-IPv6, en el caso de paquetes de datos entre el HA y el MN y no hay un NAT en la red visitada por el MN

La gran ventaja de DSMIPv6 es la menor sobrecarga en los paquetes enviados, sobre todo los paquetes de datos, aunque esta solución obliga a que el HA (y por tanto el proveedor del servicio de movilidad) sea *dual-stack*, es decir, tenga tanto IPv4 como IPv6 en su red. No es una solución válida, por tanto, en el escenario en el que la red visitada por el MN sea solo IPv4 y la red del operador del servicio de movilidad (HA) sea sólo IPv6. Además tiene algunos inconvenientes más como la necesidad de que tanto el HA como el MN soporten extensiones especiales del protocolo MIPv6 (no es válida la especificación básica definida en [1]) y no permite el uso de la función *Route Optimization*, por lo que todo el tráfico entre el MN y un CN debe ser tunelizado y enviado al HA.

4 Proyecto ENABLE

ENABLE [13] es un proyecto IST cofinanciado por la UE cuyo objetivo principal es conseguir el despliegue a gran escala del servicio de movilidad de una manera eficiente y sobre entornos IPv6, teniendo también en cuenta la transición desde IPv4. Dentro del proyecto se abordan entre otros, los temas descritos anteriormente que aún están abiertos y no existe por tanto una solución estandarizada, contribuyendo para ello con diversos organismos de estandarización como IETF, 3GPP, etc.

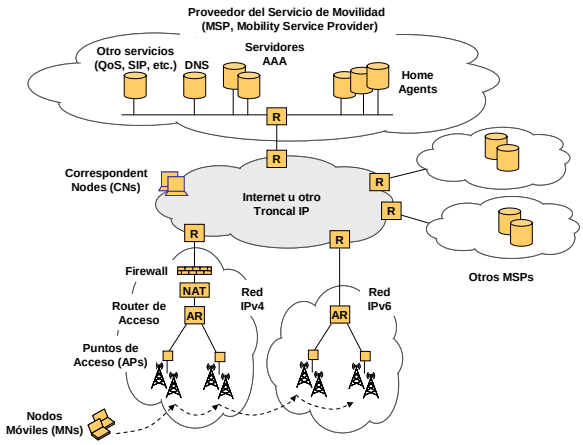

Figura 6. Arquitectura de referencia de ENABLE

Las principales áreas de trabajo del proyecto se centran en:

- Diseño de una arquitectura de referencias como la mostrada en la figura 6 que permita la integración de los diversos agentes involucrados en un servicio de movilidad real a gran escala.

- Mejora de MIPv6 para habilitar una movilidad transparente en grandes redes de producción con múltiples dominios administrativos, tipos de acceso heterogéneos y un número elevado de usuarios

- Enriquecimiento de MIPv6 básica con un conjunto de características avanzadas como QoS, *Fast Handover*, etc.

- Análisis de los objetivos y diseño de lo principios que permitan la evolución de MIPv6 a largo plazo.

La investigación que se está llevando a cabo con el proyecto ENABLE permitirá el despliegue del servicio de movilidad sobre IPv6 robusta que soporte posibles evoluciones futuras y un uso intensivo de la red con aplicaciones como multimedia (vídeo y audio), servicios de localización, emergencia, etc.

5 Conclusiones

El modelo de conectividad a Internet está evolucionando rápidamente a medida que empiezan a aparecer nuevos dispositivos portátiles y el despliegue de las redes de acceso se extiende cada vez más. El nuevo modelo basado en la movilidad de los usuarios en redes IPv6 se irá implantando en los próximos años debido a un diseño robusto y eficiente, que lo diferencia de su antecesor MIPv4.

Sin embargo aún existen algunos flecos en la estandarización de MIPv6 que necesitan ser abordados para ofrecer soluciones que permitan el despliegue a gran escala de MIPv6.

A medida que proyectos como ENABLE avancen en sus objetivos y una vez que se finalice el diseño de una arquitectura de referencia que solvente los problemas tratados en las secciones anteriores, los usuarios estarán en disposición de entrar en un nuevo mundo de servicios móviles.

Agradecimientos

Los autores agradecen a la Comisión Europea por la cofinanciación del proyecto ENABLE, donde se ha realizando este trabajo.

Referencias

[1] RFC3775 Johnson, D., Perkins, C., J. Arkko, “Mobility Support in IPv6”. Junio 2004

[2] RFC3776 Arkko, J., Devarapalli, V., F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”. Junio 2004

[3] RFC4225 Nikander, P., Arkko, J., Aura, T., Montenegro, G., E. Nordmark, “Mobile IP Version 6 Route Optimization Security Design Background”. Diciembre 2005

[4] RFC4283 Patel, A., Leung K., Khalil, M., Akhtar, H., K. Chowdhury, “Mobile Node Identifier Option for Mobile IPv6 (MIPv6)”. Noviembre 2005

[5] RFC4285 Patel A., Leung, K., Khalil, M., Akhtar, H., K. Chowdhury, “Authentication Protocol for Mobile IPv6”. Enero 2006

[6] RFC2865 Rigney, C., Willens, S., Rubens , A., W. Simpson “Remote Authentication Dial In User Service (RADIUS)”. Junio 2000

[7] RFC3588 Calhoun, P., Loughney, J., Guttman, E., Zorn, G., J. Arkko, “Diameter Base Protocol”. Septiembre 2003

[8] RFC2462 Thomson, S., T. Narten, “IPv6 Stateless Address Autoconfiguration”. Diciembre 1998

[9] RFC2526 Johnson, D., S. Deering, “Reserved IPv6 Subnet Anycast Addresses”. Marzo 1999

[10] RFC2406 Kent, S., R. Atkinson, "IP Encapsulating Security Payload (ESP)". Noviembre 1998

[11] RFC2409 Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)". Noviembre 1998

[12] RFC4306 C. Kaufman, “Internet Key Exchange (IKEv2) Protocol”. Diciembre 2005

[13] Proyecto ENABLE (Enabling efficient and operacional mobility in large heterogeneous IP networks). Proyecto IST co-financiazado por la UE. http://www.ist-enable.eu

[14] RFC4640 Patel, A., Giaretta, G., “Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)”. Septiembre 2006

[15] Stiemerling, M, Tschofenig, H., Aoun, C., E. Davies, “NAT/Firewall NSIS Signaling Layer Protocol (NSLP)”, Internet draft draft-ietf-nsis-nslp-natfw. Trabajo en curso. Octubre 2006.

[16] Storer, B., Pignataro, C., Dos Santos, M., Tremblay, J., B. Stevant, “Softwires Hub & Spoke Deployment Framework with L2TPv2”. draft-ietf-softwire-hs-framework-l2tpv2. Trabajo en curso

[17] Hesham Soliman, “Mobile IPv6 support for dual snack Hosts and Routers (DSMIPv6)”. draft-ietf-mip6-nemo-v4traversal. Trabajo en curso.

RESEÑA CURRICULAR

Miguel Ángel Díaz Fernández posee las titulaciones de Ingeniero Técnico Electrónico e Ingeniero Superior de Telecomunicación, ambas otorgadas por la Universidad Politécnica de Madrid. Su experiencia incluye programación en diferentes lenguajes orientados a objeto como C/C++ y Java así como lenguajes de modelación como UML. Desde 2.001 ha estado involucrado en diferentes proyectos de I+D relacionados con streaming de audio y video, voz sobre IP (VoIP), QoS, Movilidad, etc. En la actualidad desarrolla su actividad profesional en la empresa Consulintel como consultor en el diseño y despliegue de redes IP, principalmente IPv6, dando soporte a clientes tales como ISP y grandes empresas. Así mismo participa en diferentes proyectos IST y PROFIT de I+D, siendo sus áreas de interés aquellas que se centran en el protocolo IPv6, tales como despliegue de red, gestión, evaluación, QoS, transición etc.

Pedro García Segura es Ingeniero Técnico Informático y actualmente trabaja en el proyecto ENABLE siendo sus principales áreas de interés los relacionados con los aspectos que aborda el proyecto ENABLE (movilidad, *bootstrapping*, segurdad, etc.).

César Olvera Morales es Físico por la Universidad Nacional Autónoma de México - UNAM. De 1998 a 2001 trabajó en DGSCA-UNAM, coordinando el Laboratorio de Interoperabilidad, donde realizó investigaciones y pruebas de IPv6, QoS, Multicast, VoIP, MPLS, etc.; además de organizar conferencias y seminarios sobre estas tecnologías, y ser

conferencista en eventos nacionales e internacionales. Desde 2002 trabaja en Consulintel donde participa en varios proyectos de I+D de IST y PROFIT, y centrando sus tareas en consultorías, pruebas e instalación de IPv6 sobre temas como direccionamiento, encaminamiento, PLC, QoS, Multicast, Movilidad, etc. Además colabora con ETSI, IPv6 Forum, Spirent, Agilent, Ixia, Telelogic, Testing Tech, etc., en el diseño y conducción de pruebas de interoperabilidad, conformidad y prestaciones en dispositivos IPv6. También ha colaborado con el grupo de trabajo de v6ops de la IETF. Actualmente es estudiante de doctorado en la Universidad Politécnica de Madrid