SHIM6: Más que Tolerancia a Fallos en IPv6

Marcelo Bagnulo[*], Alberto García-Martínez[†], Arturo Azcorra[†]

[*]Huaweii Labs at UC3M, [†]U. Carlos III de Madrid, Avda. de la Universidad 30, Leganés 28911.

email: {marcelo, alberto, azcorra}@it.uc3m.es

***Abstract* — SHIM6 es un protocolo definido para preservar las comunicaciones en caso de fallos entre nodos configurados con múltiples direcciones IPv6. En esta propuesta de póster presentamos varias propuestas desarrolladas por los autores con el objeto de obtener otras propiedades adicionales a las inicialmente previstas para SHIM6. Estas propiedades son independencia del proveedor en la conexión a Internet, mejora en la privacidad en las comunicaciones y tolerancia a fallos para nodos móviles.**

I. INTRODUCCIÓN

Existe un consenso creciente en que el modelo de encaminamiento interdominio basado en BGP, en uso para IPv4, presentará pronto importantes problemas operativos debido a su limitada escalabilidad. Un gran número de problemas surgen del hecho de que cualquier red que requiera ser alcanzable por varios proveedores debe ser anunciada en BGP para poder beneficiarse de capacidades de tolerancia a fallos o de ingeniería de tráfico. Por un lado, esto limita el acceso a los beneficios de la conectividad a través de múltiples proveedores (escenario conocido como *multihoming*) para redes de pequeño tamaño que no disponen de los recursos para gestionar una red BGP. Por otro lado, aquellas redes de pequeño o mediano tamaño que se aventuran a esta gestión hacen que el número de entradas en la tabla de encaminamiento sea muy elevado, y en general contribuyen a una alta variabilidad de esta información al no disponer de personal con capacidades técnicas acordes con los requisitos de gestión de BGP. No es necesario incidir en la importancia de encontrar mecanismos que permitan combinar un correcto funcionamiento de Internet con un acceso a mejores calidades en la conectividad para redes cada vez más pequeñas (pequeñas empresas, usuarios residenciales), de una forma que no se requieran configuraciones complejas.

Para mantener la escalabilidad del sistema de encaminamiento, el IETF (Internet Engineering Task Force, www.ietf.org) propone para las redes IPv6 el uso de direcciones *Provider Aggregatable*. Así, las redes *multihomed* pueden obtener varios prefijos a partir del rango de direccionamiento de sus proveedores. En esta configuración, los proveedores (ISPs) sólo anuncian su propio prefijo en el sistema de encaminamiento, por lo que un nodo en una red *multihomed* dispone de varias direcciones, una por cada ISP, cada una permitiendo la comunicación a través del proveedor del que han sido delegadas.

La gestión de múltiples direcciones en un equipo da lugar a ciertas dificultades a la hora de obtener tolerancia a fallos. Es especialmente problemático el mantenimiento de una comunicación establecida cuando ocurre un fallo en el camino determinado por las direcciones en uso, ya que es necesario utilizar una dirección IPv6 alternativa. El cambio de direcciones IPv6 debe hacerse de forma transparente con respecto a las capas de transporte y aplicación, ya que estas capas utilizan en muchos casos a las direcciones IP para identificar los participantes de una comunicación. El grupo de trabajo SHIM6 del IETF está especificando un conjunto de protocolos extremo a extremo que permiten por un lado modificar las direcciones IPv6 utilizadas por una comunicación en curso de forma transparente para las capas superiores [1], y de forma segura, y por otro un protocolo que permita a los nodos que se comunican detectar la existencia de fallos en el camino [2].

En el póster que proponemos pretendemos presentar no sólo los aspectos básicos de funcionamiento del protocolo SHIM6, ilustrando cómo ofrece tolerancia frente a fallos en los caminos utilizados, sino otros usos más avanzados, propuestos por los autores, que surgen de la facilidad de SHIM6 para separar en las direcciones IPv6 las funciones de identificación en las capas superiores de los extremos, y de etiqueta para el reenvío de los paquetes entre los routers. Los servicios avanzados que modificaciones apropiadas de SHIM6 permiten conseguir son:

- **Independencia del proveedor**. Actualmente, cuando una red *multihomed* cambia alguno de sus proveedores, las direcciones, que estaban asociadas con ese ISP deben ser cambiadas en un proceso que se conoce como *renumerado*. Este proceso es muy costoso en términos de ajuste de la configuración, y delicado, lo que resulta de facto en una situación en la que los clientes están cautivos de sus proveedores. El uso de un dispositivo dedicado *proxy SHIM6* junto con el uso de direcciones IPv6 independientes del proveedor permite una configuración que sustituye con ventaja el uso de NATs con direcciones privadas [3].
- **Privacidad en las comunicaciones**. Es posible extender la arquitectura SHIM6 para que los extremos que se comunican varíen dinámicamente los localizadores utilizados en una secuencia suficientemente grande [4]. De esta forma, se dificulta en gran medida la capacidad de un nodo espía para reconstruir un flujo a partir de paquetes capturados en puntos arbitrarios de Internet. Esta solución ofrece un compromiso en la protección ofrecida y los recursos requeridos frente al uso de cifrado en las comunicaciones (IPsec, TLS/SSL, etc.).
- **Tolerancia a fallos para nodos móviles**. El protocolo MIPv6 (Mobile IP) no permite obtener el máximo beneficio de la disponibilidad de múltiples conexiones. Por ejemplo, no permite mantener comunicaciones IPv6 cuando hay fallos

en el acceso a la Home Address. Una combinación apropiada de SHIM6 y de MIPv6 permite obtener un escenario que sólo pierde la comunicación si fallan todos los caminos posibles entre los nodos que se comunican [5].

II. EL PROTOCOLO SHIM6

SHIM6 establece una correspondencia entre los *identificadores*, las direcciones IP presentadas hacia los niveles superiores, que se mantienen constantes a lo largo de una comunicación, y los *localizadores* incluidos en los paquetes que viajan por la red. Al poder variar los localizadores, se permite que paquetes de una misma comunicación puedan tomar diferentes caminos hacia un destino dado. Para gestionar esta correspondencia, los nodos que se comunican deben haber intercambiado las direcciones que actúan como identificadores y localizadores, dando lugar a un estado llamado *contexto SHIM6*.

La capa SHIM6 se coloca dentro de la capa de red por encima de las funciones de encaminamiento de IP (determinación del interfaz de salida para un paquete, etc.), y por debajo de funciones como fragmentación, o IPsec.

La capacidad del protocolo SHIM6 para asociar varios localizadores a un identificador abre la puerta a ataques en los que una identidad pueda ser asociada a un localizador no legítimo. Para evitar estos ataques se ha propuesto el uso de CGA [6] (Cryptographically Generated Addresses) y HBA [7] (*Hash Based Addresses*, *Direcciones Basadas en Hash*). Las CGA son direcciones IPv6 que incorporan dentro del identificador de interfaz de 64 bits un hash de una clave pública del nodo. Esta estructura permite al dueño de la clave privada asociada demostrar su propiedad de la CGA. Cuando se desea informar a otro nodo acerca de los diferentes localizadores disponibles, estos localizadores son firmados con la clave privada del nodo, garantizando su asociación con el nodo cuya IP es la CGA. Por otro lado, las HBA incorporan dentro del identificador de interfaz un *hash* de los prefijos disponibles en un nodo con múltiples direcciones. Como resultado, se genera un conjunto de direcciones, una para cada prefijo, ligadas criptográficamente entre sí para impedir que un localizador no legítimo se pueda asociar al conjunto. Un nodo remoto puede verificar si una dirección alternativa está ligada o no a la dirección HBA que se utilizó inicialmente para establecer la comunicación mediante la ejecución de un simple hash.

El protocolo SHIM6 [1] crea y gestiona el contexto SHIM6 asociado a las comunicaciones establecidas entre dos nodos. En el ejemplo posterior se ilustra el intercambio de información requerido para establecer un contexto SHIM6. El mensaje I1 indica la voluntad de una de las partes (con el rol de *iniciador*) de establecer el contexto asociado a las comunicaciones establecidas entre un par de identificadores dado del iniciador y correspondiente, utilizando para ello un par de localizadores (que puede ser igual al par de identificadores). Los identificadores serán bien CGA o HBA. El nodo correspondiente responde con un mensaje R1. La información intercambiada en estos mensajes incorpora valores aleatorios (*nonces* y *validators*) que se utilizan para proteger frente a ataques de denegación de servicio. Los mensajes I2 y R2 se utilizan a continuación para intercambiar la información de los localizadores alternativos. En el momento de la recepción de estos mensajes, los nodos validan los localizadores según el procedimiento definido por el tipo de mecanismo de seguridad utilizado (CGA o HBA).

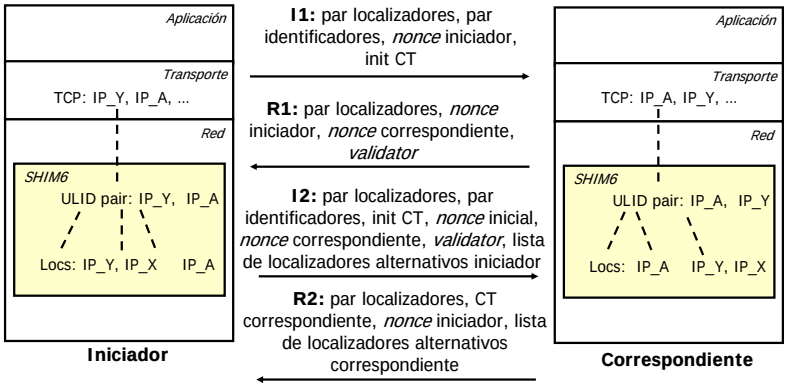

Fig. 1. Establecimiento del contexto SHIM6

Una vez establecido el contexto SHIM6, las comunicaciones pueden ser derivadas a otros caminos alternativos definidos por los posibles pares de localizadores conocidos por los nodos que se comunican. Si los paquetes de datos no utilizan el par de identificadores como localizadores, se incluye una cabecera de extensión que incorpora una etiqueta de contexto (Context Tag) que permite al receptor del paquete identificar el par de identificadores original y reconstruirlo antes de pasar la información a niveles superiores.

La detección de fallos (definida en el protocolo REAP, [2]), se basa en el análisis de la secuencia de intercambio de los paquetes entre los nodos que han establecido la comunicación, y si estos no son suficientes, y sólo en ciertas ocasiones, en la generación de paquetes específicos para comprobar la conectividad. Cuando un nodo detecta un fallo, inicia una fase exploratoria en la que envía paquetes de prueba por diferentes caminos alternativos para identificar pares de localizadores que estén operativos, de modo que la comunicación utilice estos nuevos localizadores.

III. INDEPENDENCIA DEL PROVEEDOR

El uso de un dispositivo intermedio (*middlebox*) para la implantación de SHIM6 permite obtener una serie de beneficios, tales como la facilidad de cambio de proveedor, facilidad para aplicar políticas de ingeniería de tráfico en el tráfico entrante y saliente de la red de forma centralizada, además de ser una forma fácil de hacer partícipes a nodos antiguos de los beneficios de SHIM6. En esta configuración, todos los nodos de una red son configurados exclusivamente con unas direcciones IPv6 que aúnen las propiedades de ser únicas globalmente y por otro lado no tengan que ser retornadas al cambiar de proveedor, tales como las direcciones Local IPv6 Unicast (RFC 4193).

Cuando un nodo interno (sin SHIM6 habilitado) desea comunicarse con otro nodo localizado en una red distinta servida también por un P-SHIM6, típicamente inicia una petición al DNS para resolver las direcciones asociadas al nodo de destino. En el DNS se habrá almacenado un nuevo tipo de registro en el que se representa la dirección independiente del proveedor del destino, así como localizadores asociados al mismo nodo (en este caso sí dependientes del proveedor). El nodo P-SHIM6 intercepta esta petición, la almacena para uso futuro, y devuelve al nodo iniciador de la comunicación sólo un registro AAAA conteniendo la dirección independiente del proveedor correspondiente al destino. Cuando el iniciador envía un paquete de datos, la configuración del encaminamiento hace que este paquete se encamine hacia el P-SHIM6. El P-SHIM6 inicia entonces la fase de establecimiento de contexto SHIM6 utilizando como identificadores las direcciones independientes del proveedor, como localizador destino uno de los devueltos en la anterior petición al DNS. El mensaje I1 es interceptado en la red de destino por el P-SHIM6 correspondiente, que es el que se encarga de representar al nodo remoto en la negociación del contexto SHIM6. El resultado es que los proxies utilizan el protocolo SHIM6 para intercambiar localizadores de forma segura, para detectar fallos en las comunicaciones, y para derivar los paquetes por un camino alternativo, de forma transparente para los nodos que se comunican.

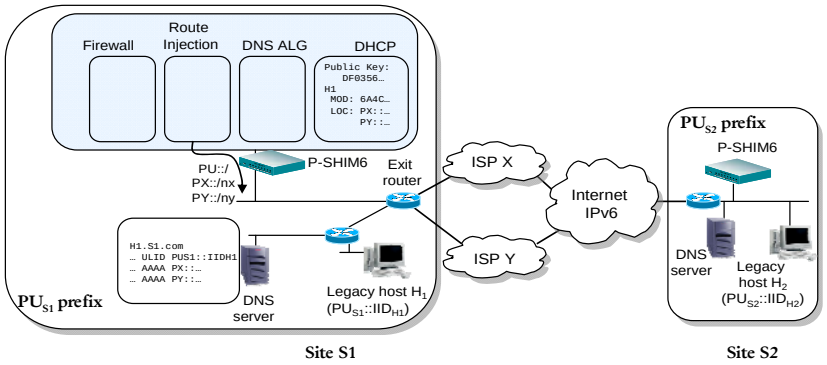

Fig. 2. Ejemplo de arquitectura basada en Proxy SHIM6 (P-SHIM6)

En el caso de que las redes cambien de proveedor, la configuración a actualizar está concentrada en el P-SHIM6, en el DNS, y en los routers de salida conectados a los proveedores, pero no es necesario actualizar otra configuración interna de la red. Otro beneficio es que el P-SHIM6 determina los caminos utilizados para cada comunicación por medio de la selección de los localizadores, por lo que éste es el único punto a configurar para establecer una política de Ingeniería de Tráfico determinada. Finalmente, el uso de P-SHIM6 permite incorporar capacidades de SHIM6 a nodos antiguos.

IV. PRIVACIDAD EN LAS COMUNICACIONES

En este caso proponemos la modificación de SHIM6 para obtener cierta privacidad en las comunicaciones IPv6 mediante la variación de ciertos parámetros (entre ellos las direcciones IP) para los paquetes que pertenecen a una comunicación dada. De esta forma se dificulta de forma notable la capacidad de un nodo colocado en un punto intermedio de la comunicación para identificar los paquetes pertenecientes a una comunicación determinada, impidiendo la reconstrucción del flujo de contenidos, o la determinación de su duración o del número de bytes intercambiados. Este modo de funcionamiento puede complementarse con el uso de IPsec para obtener una seguridad superior (un nodo espía tiene dificultades hasta para determinar que paquetes pertenecen a la comunicación – a parte de no conocer los contenidos), o como una alternativa de bajo coste computacional al cifrado. La variación propuesta para la provisión de privacidad se basa en el uso de secuencias pseudoaleatorias para el identificador de interfaz de la dirección, para la etiqueta de contexto SHIM6 y para otros parámetros que pueden ser relevantes para desvelar información sobre la comunicación (por ejemplo, número de puertos, etc.). Las secuencias pseudoaleatorias están basadas en semillas que se intercambian de forma secreta durante el establecimiento de contexto, de forma que ambos nodos participantes, y sólo esos nodos, conocen la lista ordenada de valores a ser utilizados. A partir del momento en el que uno de los nodos decide avanzar en la secuencia de valores, los paquetes generados por él incorporan los nuevos parámetros. Cuando el interlocutor recibe el primer paquete con los nuevos parámetros, interpreta de forma implícita que él también debe avanzar en la secuencia. Para proteger el intercambio de las semillas, se modifica el establecimiento de contexto SHIM6 para incluir una negociación Diffie-Hellman de claves.

V. TOLERANCIA A FALLOS EN COMUNICACIONES MÓVILES

El protocolo MIPv6 puede ser utilizado en escenarios multihomed, en los que pueden existir distintos proveedores en la red hogar (Home Network), distintos proveedores en la red remota (Visited Network), o incluso distintas redes remotas accesibles a través de distintos niveles de enlace en el nodo móvil. En todos estos casos pueden existir varios caminos distintos entre el nodo móvil y el nodo correspondiente con el que tiene establecida una comunicación. No obstante, a pesar de ello, hay muchos casos para los que la especificación de MIPv6 no permite mantener una comunicación establecida en caso de fallo de alguno de los enlaces. Un ejemplo para esto es cuando la comunicación se ha establecido utilizando una dirección concreta de la red hogar (una HoA) para el nodo móvil. Si en este caso se cae el proveedor al que pertenece esa dirección, MIPv6 no permite la recuperación de la comunicación a pesar de que el Home Agent (HA) puede estar accesible a través de otra dirección. Otra limitación de MIPv6 es la de no disponer de un mecanismo que detecte los fallos en los caminos en uso.

Es posible combinar SHIM6 con MIPv6 para obtener una mayor tolerancia a fallos, en este caso sin requerir modificaciones en ninguno de los dos protocolos. La arquitectura propuesta en este caso es colocar en los nodos móvil y correspondiente la ejecución de SHIM6 encima de MIPv6 (en un esquema conceptual en el que el nivel de enlace se coloca abajo, y el nivel de aplicación encima de todo). De esta forma, un nodo móvil podrá tener configuradas en el nivel SHIM6 varias direcciones, por ejemplo varias HoAs (si dispone de varios HAs, o un HA es accesible a través de varios proveedores), o algunas direcciones recibidas en la red visitada. MIPv6 puede mantener el estado correspondiente para cada una de las HoAs disponibles, respondiendo al chequeo periódico de seguridad conocido como *Return Routability*, y utilizando mensajes

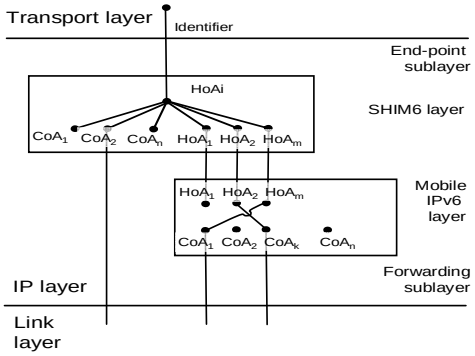

Fig. 3. Combinación de SHIM6 y MIPv6 para mejorar la tolerancia a fallos.

de Binding Update con el HA. De esta forma el HA conoce en cada momento a qué CoA está asociada cada HoA del nodo.

Supongamos que un nodo correspondiente desea iniciar una comunicación con un nodo que está fuera de su red hogar. El nodo correspondiente típicamente obtendrá en el DNS alguna de las direcciones asociadas al nodo móvil, en concreto una de sus HoAs. El primer paquete de datos llegará al HA del nodo móvil, y este lo redirigirá al nodo móvil. Al recibir el nodo móvil este paquete, iniciará un establecimiento de contexto SHIM6 utilizando la HoA como identificador local. El nodo correspondiente debe tener activa la subcapa SHIM6 de forma que el contexto se podrá establecer. Mientras no haya fallos, SHIM6 mantendrá la HoA como dirección del nodo móvil, posiblemente utilizando facilidades de optimización de rutas. No obstante, si hay un fallo para el camino utilizado, REAP lo descubrirá, y SHIM6 iniciará un procedimiento de exploración de caminos alternativos que resultará en la recuperación de la comunicación a través de otra HoA del nodo móvil, o una dirección adquirida de la red visitada.

De esta forma, MIPv6 se utiliza para establecer la comunicación, y para evitar condiciones de carrera en el caso de que dos nodos móviles que se comuniquen se movieran a la vez (los nodos se encuentran en los Has de cada uno), pero SHIM6 facilita la detección de los fallos y gestiona la recuperación de los mismos incluso si los fallos afectan al acceso al HA.

REFERENCIAS

[1] E. Nordmark, M. Bagnulo, “SHIM6: Level 3 Multihoming Shim Protocol for IPv6”, draft-ietf-shim6-proto-08, May 2007.

[2] J. Arkko, I. van Beijnum, “Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming”, draft-ietf-shim6-failure-detection-07, December 2006.

[3] M. Bagnulo, A. García-Martínez, A. Azcorra. “Fault Tolerant Scalable Support for Network Portability and Traffic Engineering”. *5th International Conference on Wired/Wireless Internet Communications (WWIC)*, Coimbra, PT. Lecture Notes in Computer Science. May 2007. Aceptado, pendiente de publicación.

[4] M. Bagnulo, A. García-Martínez, A. Azcorra. “An Architecture for Network Layer Privacy”. *2007 IEEE International Conference on Communications (ICC 2007)*. Glasgow, UK. Junio 2007. Aceptado, pendiente de publicación.

[5] M. Bagnulo, A. García-Martínez, A. Azcorra. “IPv6 Multihoming Support in the Mobile Internet”. *IEEE Wireless Communications*. Aceptado, pendiente de publicación.

[6] Aura, T., "Cryptographically Generated Addresses (CGA)", *6th Information Security Conference (ISC'03)*, Bristol, UK, October 2003.

[7] M. Bagnulo, A. García-Martínez, A. Azcorra. “Efficient Security for IPv6 Multihoming”. *ACM Computer Communications Review*, pp 61-68. Vol. 35, nº 2. Abril 2005.