Arquitecturas de indirección: HIP

Alberto Los Santos Aransay, albertolsa@gmail.com

1. INTRODUCCIÓN

En el presente documento se pretende reseñar la problemática que entraña el direccionamiento en Internet y explicar los conceptos en que se basan dos de las iniciativas que tratan de resolver estas carencias. Los servicios en Internet han evolucionado, y es necesario implementar diversas mejoras para poder cubrir sus necesidades.

En el siguiente capítulo veremos un breve resumen de la estructura de Internet, junto con los problemas de direccionamiento detectados. En los capítulos 3 y 4 veremos dos de las soluciones disponibles, *Layered Names* y *Host Identity Protocol* (HIP), respectivamente. Por último, en el capítulo 5 se dispone de las conclusiones.

2. INTERNET

Internet nació con el objetivo de proveer una arquitectura junto con unos protocolos que diesen la posibilidad de unir en una única red todas las redes heterogéneas existentes en la época. Se definió la arquitectura TCP/IP basada fundamentalmente en tres protocolos: IP, TCP y UDP. Mientras que el protocolo IP se diseñó con la misión exclusiva de encaminar paquetes entre los extremos, el control de la comunicación extremo a extremo es realizado por los protocolos TCP y UDP. Para poder realizar esta función, cada equipo conectado a la red se identifica por una dirección única (al menos a priori, veremos después que esto no es totalmente correcto), conocida como dirección IP. El protocolo IP se diseñó utilizando direcciones de 32 bits, que permiten identificar hasta unos 4.000.000.000 ordenadores diferentes. En los 70 parecía imposible que el mundo llegase a tener tal cantidad de ordenadores.

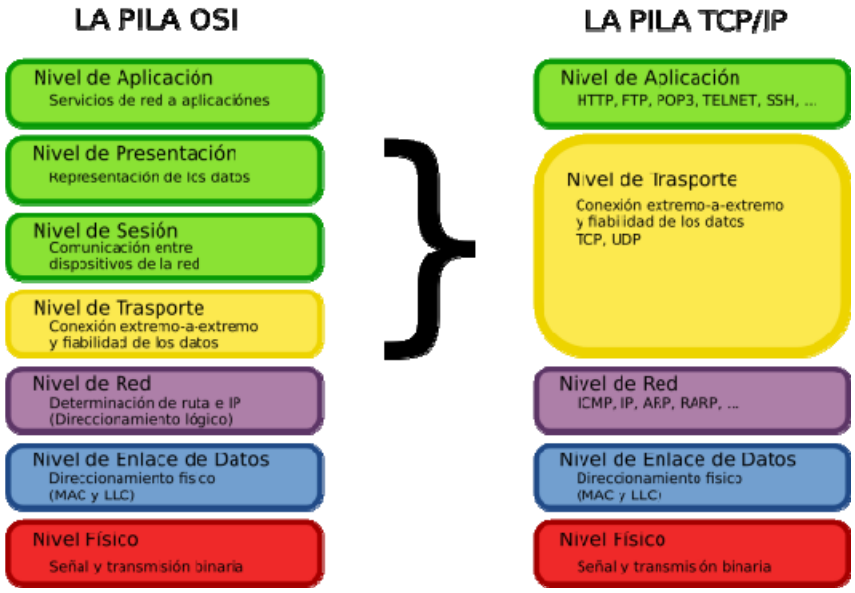

Fig. 1: Modelo OSI frente a TCP/IP [1]

Los tres elementos principales que forman parte de Internet son: los nodos de la red (los cuales intercambian la información), las infraestructuras de transporte de paquetes, y los servicios o aplicaciones. Como ya se ha explicado, cada nodo se puede identificar a través de al menos una dirección IP, pero además se puede alcanzar mediante nombres DNS (Domain Name System). DNS es una base de datos distribuida que ofrece un mapeo entre nombres (asignados jerárquicamente) y servicios o máquinas en Internet.

2.1 Problemas de direccionamiento en Internet

Desde sus inicios, Internet ha ido cambiando, y de igual manera las aplicaciones que sustenta también han evolucionado. Si inicialmente pretendía ser una red de compartición de información y datos estáticos, cada vez las necesidades por parte de las aplicaciones han ido haciéndose más exigentes. Además, debido al tremendo éxito de la red, los planteamientos iniciales no han sido suficientes, denotando ciertas carencias. En esta sección se pretenden resumir los principales problemas relacionados con el direccionamiento actual en Internet.

- Espacios de nombres: Internet está compuesto por dos espacios de nombres, direcciones IP y nombres DNS. Las direcciones IP son usadas tanto para referenciar las interfaces de red como los nombres de las localizaciones de los servicios o equipos (información necesaria para hacer llegar los paquetes a su destino). Además, las distintas interfaces de los dispositivos disponen de distintas direcciones IPs, y estas IPs pueden variar cada vez que el terminal se conecta a la red. Los espacios de nombres actuales acarrean tres problemas:

· La reasignación dinámica de direcciones no puede ser gestionada directamente.

· El anonimato no se puede ofrecer de forma consistente y confiable.

· No se provee de autenticación para sistemas y datagramas.

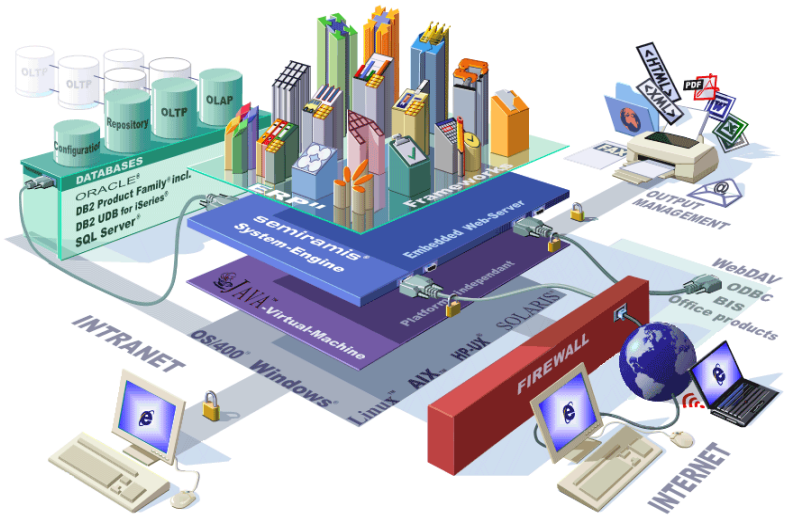

Fig. 2: Capas software de un ordenador actual, conectado a Internet a través de un Firewall [2]

- Limitación en el número de direcciones IP: Debido al gran número de equipos y aplicaciones en la red, se han tenido que introducir nuevos elementos en la estructura. Una de las soluciones ha sido el uso de NAT (Network Address Translator) y NAPT (Network Address Port Translation), de esta forma una IP pública es compartida por varios equipos. Un dispositivo NAT recibe las conexiones TCP o los paquetes IP que vienen de la red privada y los reencamina hacia la Internet pública como si fuesen suyos. Los paquetes de respuesta los recibe el dispositivo NAT, que los reencamina hacia el otro extremo de la comunicación dentro de la red privada utilizando una tabla de encaminamiento donde figuran todas las comunicaciones en curso. La introducción de NAT obliga a renunciar al paradigma extremo a extremo de las aplicaciones de Internet, que pasan a tener un dispositivo intermediador entre los extremos. Desde dentro de una red privada, es decir desde detrás de un NAT, sólo se puede acceder como cliente a algunos servicios de la Internet pública, como Web o correo electrónico.

Además de NATs, se han introducido otros elementos intermedios, como por ejemplo, los firewalls, proxys y cachés transparentes, que introducen aún más problemas para el diseño y correcto funcionamiento de muchas aplicaciones.

3. LAYERED NAMES

Para solventar los problemas detallados en el capítulo anterior, numerosas iniciativas y estudios se pueden encontrar en la literatura. Por citar algunas: PIP [4], IPv6 [5], Dynamic Networks [6], Active Networks [7], Nimrod [8], Smart Packets [9]. Algunas de estas soluciones se centran en proponer mejoras a la arquitectura básica, mientras que otras pretenden un rediseño profundo.

En este capítulo detallaremos la solución referenciada en la asignatura, titulada "A Layered Naming Architecture for the Internet" [10]. Este sistema está basado en el uso de un espacio de nombres de cuatro capas: descriptores a nivel de usuario (palabras claves, direcciones e-mail, etc.), identificadores de servicios (SIDs), identificadores de terminal (EIDs) y direcciones IP. De esta forma se consigue:

1. Independizar la ruta de los servicios (dirección IP o URL) de su situación en la red o dominio DNS, por lo que pueden ser fácilmente migrados o replicados en otras máquinas.
2. Abordar más fácilmente la movilidad y el multi-homing (multi-dominio).
3. Permitir introducir elementos intermedios (NATs, firewalls, etc.) en la red, sin impedir a priori, el funcionamiento de todos los servicios

A través de la Figura 3 se puede ver el funcionamiento básico del sistema. Imaginemos que una aplicación quiere acceder a un servicio, que en este caso es un servidor Web. La aplicación usaría la capa de resolución SID, para a partir del servicio obtener una o más triplas (EID, transporte, puerto). Si además el servicio se refiere a un objeto en concreto, por ejemplo una web, y no un servicio general, la capa de resolución SID devolvería la ruta de la misma. A partir de las triplas, se comunicaría con los respectivos EIDs. La capa de resolución EID, transforma el identificador en una o más IPs (IPs múltiples pueden ser devueltas en caso de que un identificador lógico represente una colección de máquinas físicas, cada una con su IP, o a hosts multi-dominio).

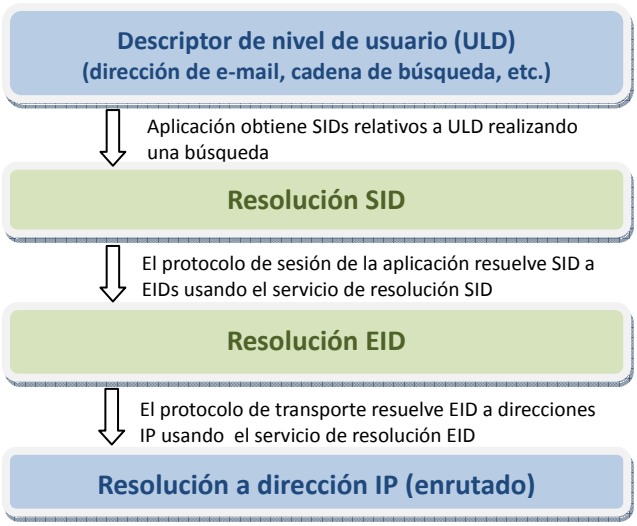

Fig. 3: Capas de nombres propuestas en la solución

La solución detallada por los autores se basa en la combinación de otras propuestas ya existentes. De la propuesta Host Identification Protocol (HIP) [11], que será explicada en el próximo capítulo, se incorpora la idea de desacoplar las capas de transporte y red, para conseguir movilidad y multi-dominio. De UIP (Unmanaged Internet Protocol) [12], recogen el concepto de usar este mismo desacoplamiento para solucionar los problemas que ocasiona el uso de direccionamiento privado, como el producido por el uso de NATs. De i3 (Internet Indirection Infrastructure) [13] integran la idea de las indirecciones en función del emisor. Además, de SFR (Semantic-Free Referencing) [14] se recoge la idea de utilizar identificadores planos, es decir, que no tienen relación con el objeto al que identifican. Por último de HIP y UIP, de nuevo, incorporan el uso de identificadores planos para los terminales. Por último, para solventar la resolución de los nombres planos, se necesita una infraestructura escalable, que está basada en DHTs (Distributed Hash-Tables).

4. HIP: HOST IDENTITY PROTOCOL

Host Identity Protocol (HIP) surge con la idea de ofrecer una alternativa para separar el identificador del localizador. Este protocolo, desarrollado por IETF [15], es especificado junto un espacio de nombres propio. Tal y como se ha tratado anteriormente, Internet tiene dos espacios de nombres principales: las direcciones IP y los nombres DNS. El propuesto, llamado identidad de Host (HI), intenta cubrir un hueco importante entre ambos, usando nombres criptográficos.

Un nombre en el espacio de nombres Host Identity es señalado mediante un HI, y representa un identificador único y global para cualquier sistema basado en IP. Un mismo sistema puede tener varios HIs, unos públicos y otros anónimos. Cualquier sistema debe autentificar su identidad, por él mismo o a través de una entidad certificadora (como DNSSEC [16]). Estos identificadores aportan dos características: Permiten desacoplar las capas de red y transporte, y al ser el mismo HI una clave pública, se puede usar para autenticar en protocolos de seguridad como IPsec. Los HIs públicos deben ser almacenados en servidores DNS o en directorios LDAP[1], para ser intercambiados.

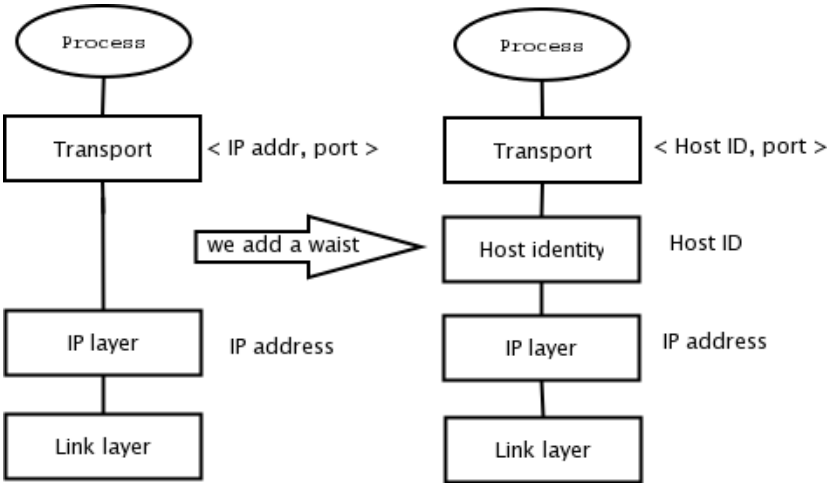

Fig. 4: Incorporación de la capa HI en la arquitectura de HIP

Otro de los elementos característicos de HIP es el Host Identity Tag (HIT), una representación de 128-bit de cada HI, creada calculando su hash criptográfico. Al usar un hash de longitud fija, se le facilita el trabajo al protocolo de codificación, y además la identidad se presentará siempre de forma consistente independientemente del algoritmo criptográfico usado. En los paquetes HIP, los HITs identifican el origen y destino del paquete, por lo que cada HIT debe ser único.

Con esta arquitectura, los nombres de los terminales y de los localizadores son distintos. Las IPs continúan actuando como localizadores, pero los HIs son ahora los identificadores de los nodos. Hay que reseñar que un HI puede ser alcanzable a través de diferentes interfaces. Además, las asociaciones en la capa de transporte se realizan hacia HIs y no a direcciones IPs. En Internet es posible que un mismo terminal aloje diferentes servicios, con HIP cada uno de estos servicios o nodos podría disponer de un HI único.

HIP, al desacoplar las capas de transporte y red, y ligar las comunicaciones a los HI, ofrece un grado de movilidad entre redes y multi-dominio sin apenas coste estructural, permitiendo conectar nodos entre NATs. Un mecanismo importante para facilitar la comunicación con nodos móviles es el de *rendezvous* [17] (aunque se podrían usar DNS dinámicos [18]). Este mecanismo depende de una infraestructura de *rendezvous* que el nodo móvil debe mantener continuamente actualizada con su dirección o direcciones IP actuales. Los nodos deben confiar en el mecanismo de *rendezvous* para mantener sus direcciones HIT e IP mapeadas.

[1] LDAP (Lightweight Directory Access Protocol o Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

En la imagen inferior se describe un caso para el uso de HIP con DNS. En el lado del cliente (izquierdo), la aplicación envía una petición DNS al servidor DNS. Este último responde con un HI (FQDN[2]->HI) en vez de una IP. En el segundo paso, otra búsqueda es hecha en la capa HI por el demonio HIP. Así, HIs son traducidas en direcciones IP (HI->IP) para la entrega de la capa de red. El protocolo de transporte envía un paquete conteniendo el HI del servidor, y la capa HI reemplaza el HI con la correspondiente IP del servidor. La capa de red transmite este paquete con la cabecera IP. Así el tradicional conjunto de datos {protocolo, IP origen, puerto origen, IP destino, puerto destino} se convierte en {protocolo, HI fuente, puerto fuente, IP destino, puerto destino. HIP usa un modo especial ESP (Protocolo Encapsulating Security Payload) de IPsec llamado Bound End-to-End Tunnel (BEET), para transportar el tráfico.

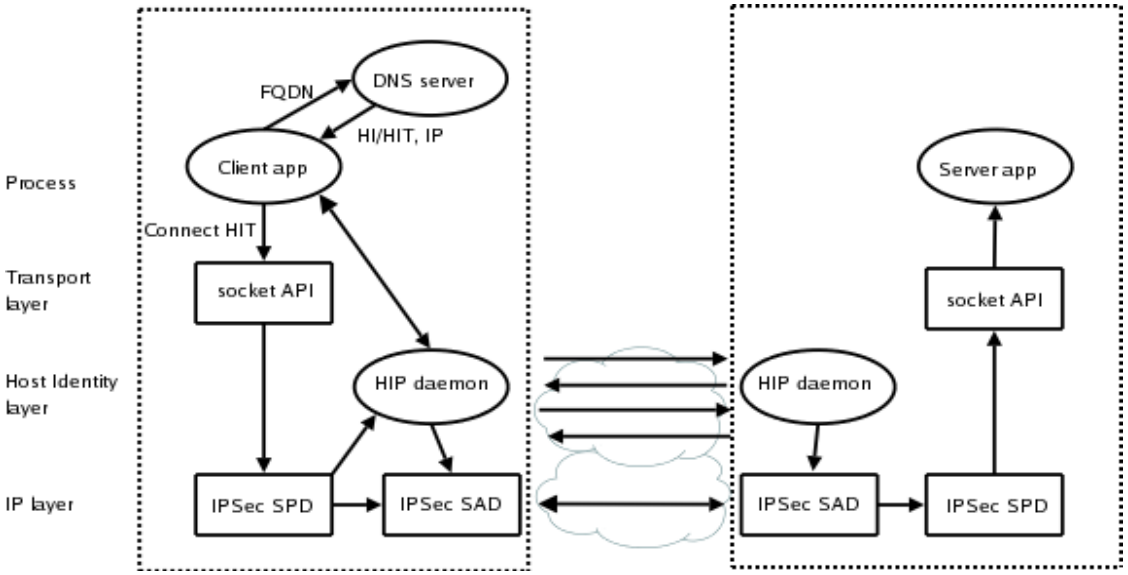

Fig. 5: Ejemplo de funcionamiento de HIP con servidores DNS

HIP se aprovecha de HI para proveer de autenticación segura a hosts y realizar un intercambio de clave rápida para IPsec. Además es capaz de reducir la exposición a diferentes ataques y caídas en los servicios. El protocolo además es efectivo para evitar posibles ataques por inundación de mensajes, ya que HIP incluye un mecanismo de comprobación de direcciones, donde la disponibilidad de cada nodo es chequeada antes de permitir el intercambio de grandes cantidades de tráfico.

CONCLUSIONES

Internet desde su diseño inicial ha ido evolucionando, para cada vez soportar más tráfico, nodos y aplicaciones. Con este aumento de usuarios y necesidades, diversos problemas han aparecido, relacionados con la seguridad, movilidad, dimensionado… En este trabajo se ha tratado de exponer las limitaciones que tiene la arquitectura actual basada en dos espacios de nombres, direcciones IP y DNS.

Para solventar los problemas que adolece Internet, han surgido multitud de propuestas. En este trabajo nos hemos centrado en estudiar dos: Host Identity Protocol (HIP) y Layered Names, ambos enfocados al diseño de nuevas arquitecturas que introducen capas extra que desacoplan el identificador del recurso de su localización (capas de Transporte e IP). La segunda propuesta incluye a HIP en su framework, junto con otras soluciones como UIP, i3, SFR y DHT, para en definitiva conseguir movilidad, multi-dominio, conectividad entre hosts públicos y privados (evitando NATs, firewalls, proxy…), mayor seguridad en las comunicaciones, etc.

Las soluciones planteadas parecen ser efectivas y útiles, pero también acarrean ciertos problemas. Uno de ellos es la pérdida de semántica al usar identificadores planos. Esta característica es muy versátil, pero

[2] Un FQDN (Fully Qualified Domain Name) es un nombre que incluye el nombre del terminal y el nombre de dominio asociado a ese equipo, por ejemplo: si el terminal se llama «pc1» y el nombre de dominio «uvigo.com», el FQDN será «pc1.uvigo.com».

impide que el usuario pueda asociar el nombre a un recurso concreto, haciendo además que pueda no confiar en el mismo sin la intervención de terceros (autoridades certificadoras).

Hemos dejado para el final el mayor problema que suponen estas soluciones. En general, nuevas capas en la arquitectura significan, al menos, cambios en el software de los principales nodos de la red. En las soluciones detalladas en el documento como mínimo es necesario introducir una infraestructura que resuelva los distintos identificadores hasta llegar al nivel IP. Esto puede suponer un gran impedimento, como sucede con IPv6,el cual, aún siendo una solución aceptada por la mayor parte de la comunidad, todavía no está totalmente desplegada ya que supone una inversión por parte de muchas entidades – principalmente de los ISPs (Internet Service Providers) - que en ciertos casos no están dispuestos a asumir, o tienden a retrasar. Esto puede dar una idea de lo problemático que puede ser introducir una "mejora" en la red de redes.

REFERENCIAS

[1] Imagen extraída de: http://albertjh.cymaho.com/wp-content/uploads/2008/06/tcp_ip_frentea_iso.png

[2] Imagen extraída de: http://cachanilla.itmexicali.edu.mx/~chong/arqweb/ArqWeb.gif

[3] Quemada, J. "Hacia una Internet de nueva Generación", Enero de 2004.

[4] Francis, P. "A near-term architecture for deploying PIP". *IEEE Network*, 7(6):30–27, 1993.

[5] Deering, S. y Hinden, R." Internet Protocol, Version 6 (IPv6)", Dec. 1998. RFC 2460.

[6] O'Malley, S. W. y Peterson, L. L. "A dynamic network architecture". *ACM Transactions on Computer Systems*, 10(2):110–143, Mayo 1992.

[7] Tennenhouse, D. L., Smith, J. M., Sincoskie, D., Wetherall, D. J.y Minden, G. J." A Survey of Active Network Research". *IEEE Communications Magazine*, 35(1):80–86, 1997.Asd

[8] Castineyra, I., Chiappa, N. , y Steenstrup, M. "The Nimrod routing architecture", August 1996. RFC 1992.

[9] Schwartz, B., Jackson, A. W., Strayer, W. T., Zhou, W., Rockwell, R. D. y Partridge, C. "Smart packets: applying active networks to network management". *ACM Transactions on Computer Systems*, 18(1):67–88, Feb. 2000.

[10] Balakrishnan, H., Lakshminarayanan K., Ratnasamy, S., Shenker, S., Stoica, I. y Walfish, M. "A Layered Naming Architecture for the Internet". In ACM SIGCOMM 2004, Portland, OR, Septiembre 2004.

[11] Moskowitz, R. y Nikander, P. "Host Identity Protocol (HIP) Architecture". IETF RFC, Mayo 2006.

[12] Ford, B. "Unmanaged Internet Protocol: taming the edge network management crisis". In *2nd ACM Hotnets Workshop*, Cambridge, MA, Noviembre 2003.

[13] Stoica, I., Adkins, D., Zhuang S., Shenker, S., y Surana, S. "Internet indirection infrastructure". In *ACM SIGCOMM*, Pittsburgh, PA, Agosto 2002.

[14] Walfish, M., Balakrishnan, H., y Shenker, S. "Untangling the Web from DNS". In *1st USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI '04)*, San Francisco, CA, Marzo 2004.

[15] The Internet Engineering Task Force (IETF) web: http://www.ietf.org/

[16] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, Marzo 2005.

[17] Laganier, J. y Eggert, L. "Host Identity Protocol (HIP) Rendezvous Extension". Abril 2008. RFC 5204.

[18] Vixie, P., Thomson, S., Rekhter, Y., y J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, Abril 1997.