Caracterización de IPv6

IPv6 Characterization

Carlos A. Castillo Medina
Ingeniero de Sistemas, candidato a magister en Ciencias de la Información y las Comunicaciones. Docente de la Universidad del Bosque y la Universidad Católica. Bogotá, Colombia.
Contacto: *cacm.castillo@gmail.com*

Felipe Forero Rodríguez
Ingeniero Electrónico, candidato a magister en Ciencias de la Información y las Comunicaciones. Asesor en escritura de textos científicos en Inglés de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia.
Contacto: *fforeror@udistrital.edu.co*

Fecha de recepción: 14 de noviembre de 2011
Clasificación del artículo: Revisión
Fecha de aceptación: 27 de noviembre de 2012
Financiamiento: Universidad Distrital Francisco José de Caldas

Palabras clave: calidad de servicio, IPv4, IPv6, seguridad en redes.

Key words: quality service, IPv4, IPv6, network security.

RESUMEN

El presente artículo tiene como finalidad hacer un recuento de lo que es el protocolo IPv6; desde la evolución de IPv4, que motivó el diseño de nuevas características, hasta los detalles que componen la nueva versión del protocolo de Internet. En las secciones principales del artículo se explican los inconvenientes de IPv4 que se resuelven al implementar IPv6, destacando los aspectos de seguridad, movilidad y calidad de servicio (QoS).

ABSTRACT

The present paper attempts to survey the current state of the network protocol called IPv6; starting from the evolution of IPv4 (which motivated the design of new features) to the details that are comprised in the new version of the Internet Protocol. The main sections explain the drawbacks of IPv4 that can be overcome by implementing IPv6, highlighting aspects such as security, mobility, and Quality of Service (QoS).

* * *

1. INTRODUCCIÓN

El Protocolo de Internet (IP) fue diseñado en los años setenta con el fin de interconectar nodos de una red militar del gobierno americano llamada ARPANET [1], que luego se extendió a interconectar redes públicas entre sí. Los creadores de Internet no predijeron, en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos [2]. Sin embargo, por su rápida difusión no fue posible la implementación en QoS (*Quality of Service.* Disponible en: http://tools.ietf.org/html/rfc2990) lo que significa que, si bien el protocolo hace su mejor esfuerzo en entregar un paquete a su destino, no se puede asegurar dicha entrega puesto que existe un porcentaje de paquetes que se pueden perder en la red, bien sea por tiempo o por errores [3]. No es que estuvieran equivocados, sino que las Tecnologías de la Información y Comunicación (TIC) han evolucionado de un modo mucho más explosivo de lo esperado. Por esto, la versión actual de IP (versión 4), está llegando a sus límites, con restricciones que impiden un adecuando crecimiento de la red y, por tanto, la creación e implementación de nuevas aplicaciones, con más posibilidades que las actuales [4]. El nacimiento de IPv6 viene a resolver las limitaciones de IPv4, además de integrar nuevas características que permitan entregar seguridad y confiabilidad en la transmisión de la información [5]. En este sentido, el presente artículo tiene como finalidad hacer un recuento de lo que es el protocolo IPv6, con sus principales características, destacando los aspectos de seguridad, movilidad y calidad de servicio (QoS).

2. UN POCO DE HISTORIA

A principios de los años setenta, dos científicos visionarios llamados Vinton Cerf y Robert Kahn, que trabajaban para la DARPA (Advanced Esearch Projects Agency) del Departamento de Defensa de los Estados Unidos, fueron los encargados de liderar un proyecto para interconectar los computadores de un cierto número de universidades distribuidas por todo el país, las cuales realizaban proyectos científicos informáticos de interés para la *Advanced Research Projects Agency* (DARPA), dicho proyecto fue llamado ARPANET. Este fue el inicio para el desarrollo de la arquitectura base y los protocolos que, en la actualidad, gobiernan la Internet. Teorías como la conmutación de paquetes, el manejo de redes heterogéneas y los enrutamientos sin conexiones, comenzaron a sucumbir entre los investigadores debido a las grandes bondades y potencialidades que estas características generaban; en este sentido, fue necesario analizar los siguientes puntos que son característicos de las redes de datos actuales [6]:

- La transmisión no siempre es fiable.
- La latencia no es cero.
- El ancho de banda no es infinito.
- La red no es segura.
- La topología de red puede cambiar.
- Existe un coste en las comunicaciones.
- La administración no siempre será centralizada.

Para el año 1974, se publicó el diseño básico del protocolo de Internt (IP) de Cerf – Kahn, convirtiéndose, junto con un protocolo de capa superior llamado TCP, en el punto de partida para la explotación y uso de las redes de interconexión. No fue sino hasta inicios de la década de los años 90, que la Internet y su protocolo base TCP/IP, inicio su proliferación y uso masivo, cuando, por primera vez, iniciaron operaciones dos compañías llamadas UUnet y Psinet como ISP (Internet Servi-

ce Provider) en los Estados Unidos, consiguiendo la tecnología, crecimientos exponenciales nunca previstos en tan poco tiempo. Desde entonces, el Protocolo IP, en su versión actual, 4 (IPv4), ha sido muy exitoso, por su diseño flexible y poderoso. Ha permitido que la Internet maneje redes heterogéneas, cambios bruscos en las tecnologías de hardware y aumentos enormes de escala [7].

La demanda actual de redes, en las páginas web en particular, correo electrónico, los servicios *peer-to-peer*, y el uso de dispositivos móviles, ha crecido mucho más allá de las expectativas de sus creadores. El despliegue y desarrollo de las tecnologías de redes y comunicaciones móviles ha superado la capacidad de IPv4 para proporcionar suficiente espacio de direcciones globalmente único [8].

De igual manera, con la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, sé ha presentado la necesidad de desarrollar extensiones o añadidos al protocolo original, como lo son, fundamentalmente, medidas para permitir: calidad de servicio (QoS) [9], seguridad [10], (IPSec) y movilidad [11]. Pero con el transcurrir del tiempo, la tecnología de redes ha madurado considerablemente, han surgido nuevas aplicaciones y nuevos protocolos. De manera, que el protocolo IP (IPv4) se quedó corto en el alcance de soportar estas nuevas tendencias tecnológicas. Tanto así, que ya se están presentando algunas limitaciones al funcionamiento de las redes actuales, como lo es, fundamentalmente, la inminente saturación del espacio de direcciones IP [12], por el abrupto crecimiento de la Internet, limitando el crecimiento de la misma; soporte inadecuado de las nuevas aplicaciones, ya que son más demandantes de factores como: tiempos de respuestas y disponibilidad de ancho de banda; y por último, la inminente necesidad de manejar altos grados de seguridad, pero de manera nativa, ya que IPv4 para manejar seguridad, se basa en protocolos (Patches) como IPSec (IP Security Protocol), SSL (Secure Sockets Layer) [13], SHTTP (Secure HyperText Transfer Protocol) [14], los cuales ninguno es un estándar [7].

Los esfuerzos para desarrollar un sucesor de IPv4 se inició en la década de 1990, dentro de la Internet Engineering Task Force (IETF) “El IETF es una comunidad abierta internacional encargado de la evolución de las arquitecturas de Internet y de sus normas. Un estándar de Internet que comienza como un proyecto de Internet, que generalmente se desarrolla durante la publicación de versiones sucesivas. A continuación, podrán ser publicados en documento de solicitud de comentarios (RFC). Algunos definen las normas IETF RFC, mientras que otros son documentos informativos o describir los protocolos experimentales”. El objetivo era resolver las limitaciones de espacio de direcciones, así como proporcionar una funcionalidad adicional. El IETF comenzó los trabajos en el año 1993, con un Protocolo de Internet de Nueva Generación (IPng) para investigar diferentes propuestas y hacer recomendaciones para futuras acciones.

El IETF recomienda IPv6 en el año 1994. (El nombre de IPv5 había sido asignado a un protocolo de secuencia experimental.) Su recomendación se especifica en el RFC 1752: *La Recomendación para Protocolo IP de Nueva Generación*. Después de esta, siguieron nuevas propuestas donde *The Internet Engineering Steering Group* aprobó la recomendación de IPv6 y redactó un Proyecto de Norma el 17 de noviembre de 1994. El RFC 1883: *Protocolo de Internet versión 6 (IPv6)*, el cual se publicó en 1995. El núcleo básico de protocolos IPv6 “Dos de los actuales grupos de trabajo IETF que se concentran en las operaciones y protocolos IPv6 son: El grupo de trabajo de operaciones de IPv6 (v6ops) y el grupo de trabajo de mantenimiento de IPv6 (6man)” se convirtió en un proyecto de norma IETF el 10 de agosto de 1998. Esto incluye RFC 2460, que sustituyó a RFC 1883. En pocas palabras, se puede decir que

IPv6 es un protocolo diseñado para manejar la tasa de crecimiento de Internet y para hacer frente a los exigentes requisitos de calidad de servicios, la movilidad y la seguridad de extremo a extremo [8].

Este nuevo Protocolo de Internet IPv6, se convierte en una evolución natural del protocolo anterior IPv4, más no es un cambio abrupto del mismo, ya que funciones que servían en IPv4 se mantuvieron y mejoraron en IPv6, y funciones que no servían se eliminaron, produciendo una serie de características determinantes en la mejora del protocolo anterior.

3. INICIOS DE IPV6

En diciembre de 1993, el RFC 1550 fue distribuido, titulado "IP: Next Generation (IPng)". Este RFC invitó a cualquier grupo interesado que sometiera comentarios con respecto a cualquier requisito específico para el IPng o cualquier factor dominante que se debería tener en cuenta en el momento de seleccionar IPng, en lo cual se obtuvo 21 respuestas que fueron sometidas, las cuales trataban diversos temas entre ellos: seguridad [15] y opinión de usuario corporativo [16]. El proyecto IPng detalló en el RFC 1726: "Criterio Técnico para elegir IP, la nueva generación de direcciones IP (IPng)", los siguientes 17 puntos a tener en cuenta [17]:

Escalabilidad: el protocolo de IPng debe permitir la identificación y la dirección de menos 1012 sistemas finales y de 109 redes individuales.

Flexibilidad topológica: la arquitectura del encaminamiento y los protocolos de IPng deben permitir muchas diversas topologías de la red.

Funcionamiento: los router de categoría normal debe poder procesar y remitir el tráfico de IPng a las velocidades de las cuales son capaces de utilizar, disponible comercialmente, a una velocidad rápida. Los hosts deben poder alcanzar las tazas de transferencia de datos con IPng que son comparables a las tazas de transferencia alcanzadas con IPv4, usando niveles similares de los recursos del hosts.

Rendimiento: deben poder procesar y remitir el tráfico de IPng a las velocidades capaces completamente de utilizar en los medios comercialmente disponibles, a altas velocidades. Los hosts deben poder alcanzar las tazas de transferencia de datos con IPng, que son comparables a las tazas de transferencia alcanzadas con IPv4, usando niveles similares de los recursos del hosts.

Servicio robusto: el servicio de red y sus protocolos asociados de los encaminamientos y del control deben ser robustos.

Transición: el protocolo debe tener un plan directo de la transición del IPv4 actual.

Independencia de los medios: el protocolo debe trabajar a través una red interna de diversos medios como LAN, WAN y MAM. Con velocidades individuales de acoplamiento extendiéndose de 1 bits por segundo hasta cientos de gigabits por segundo.

Servicio de Datagrama No fiable: el protocolo debe apoyar un servicio de entrega de datagrama no fiable.

Configuración, administración, y operación: el protocolo debe permitir la configuración y la operación fáciles y en gran parte distribuida. Se requiere la configuración automática de hosts y de routers.

Operación segura: IPng debe proporcionar una capa de red segura.

Nombramiento único: IPng debe asignar a cualquier objeto en global, un nombre único en la Capa IP de Internet.

Acceso y documentación: los protocolos que definen IPng, sus protocolos asociados, y los protocolos del encaminamiento, deben ser publicados en la pista RFCs de los estándares, estar libremente disponibles, y no requerir ningún honorario que licencia para la puesta en práctica.

Multicast: el protocolo debe permitir transmisiones de paquete unicast [18], y la transmisión del paquete de multicast [19].

Extensibilidad: el protocolo debe ser extensible; debe poder desarrollarse para resolver las necesidades futuras del servicio del Internet. Además, como IPng se desarrolla, debe permitir que diversas versiones coexistan en la misma red.

Servicio de Red: el protocolo debe permitir que la red asocie los paquetes a las clases particulares del servicio y provea de ellas los servicios especificados por esas clases.

Movilidad: el protocolo debe apoyar los hosts, las redes, y los internetworks móviles.

Protocolo de control: el protocolo debe incluir la ayuda elemental para soportar y probar las redes para eliminar los errores.

Redes privadas: IPng debe permitir que los usuarios construyan internetworks privados encima de la infraestructura básica del Internet, apoyando internetworks basados en IP y basados en no-IP.

4. TERMINOLOGÍA BÁSICA

Las siguientes definiciones son necesarias para entender correctamente la referencia al Protocolo IPv6, RFC 2460 [20]:

Address (Dirección): un identificador IPv6 para una interfaz de capa o un conjunto de interfaces

Node (Nodo): un dispositivo de la red que envía y recibe paquetes IPv6

Deprecated address (Dirección obsoleta): una dirección, asignado a una interfaz, cuyo uso no se recomienda, pero no está prohibido (por ejemplo, direcciones locales del sitio, tales como FEC0:: / 10). Una dirección obsoleta ya no se debe utilizar como dirección de origen en las nuevas tecnologías, pero los paquetes enviados desde o hacia las direcciones en desuso se entregan como se esperaba.

Router (Enrutador): un nodo que envía y recibe paquetes, y también acepta los paquetes y los envía en nombre de otros nodos.

Host: un nodo que puede enviar y recibir paquetes, pero no paquetes de reenvío para otros nodos.

Link (Enlace): una facilidad de comunicación o medio sobre el cual los nodos pueden comunicarse en la capa de enlace, es decir, la capa inmediatamente inferior a IPv6. Ejemplos de ello son: Ethernets (simple o un puente), Point-to-Point Protocol (PPP), X.25, Frame Relay, o modo de transferencia asíncrona (ATM) las redes, y de tres capas (o superior) túneles, como los túneles sobre IPv4 o IPv6.

Link MTU (MTU del Enlace): la unidad de transmisión máxima (MTU), es decir, tamaño de paquete en octetos, que puede ser transmitida sobre un enlace.

Path MTU (MTU de Camino): el mínimo vínculo MTU de todos los eslabones de una ruta entre un nodo fuente y un nodo destino.

Upper Layer (Capa Superior): una capa de protocolo inmediatamente encima IPv6. Ejemplos de ello son los protocolos de transporte como

el Transmission Control Protocol (TCP), y de datagramas de usuario Protocol (UDP) [21], protocolos de control, tales como: mensajes de Internet Protocolo de control (ICMP) [22], protocolos de enrutamiento como Open Shortest Path First (OSPF) [23], y conexión a internet o capa inferior-protocolos de ser en túnel a través (es decir, encapsulados en) IPv6, como intercambio de paquetes (IPX), AppleTalk, o IPv6.

Interface (Interfaz): el punto en el que un nodo se conecta a un enlace. Las direcciones IPv6 Unicast están siempre asociados con las interfaces.

Packet (Paquete): una cabecera IPv6 más carga útil.

Neighbors (Vecinos): los nodos conectados al mismo enlace.

5. MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6

Un aspecto muy importante desde que se inició el diseño de IPv6, fue el reconocimiento de que tendría que coexistir en la red con IPv4 durante un largo período de tiempo. Esto se debe al hecho de que existen millones de dispositivos, aplicaciones y servicios que no pueden ser desconectados ni tan siquiera por un momento [24]. Internet ha llegado a ser una infraestructura crítica, y no hay modo alguno de pararla, ni tan siquiera por una única noche, realizar una actualización y tener IPv6 funcionando en toda la Red. Es también fácil entender que aún cuando se pudiera hacer algo así, todavía habría dispositivos que no podrían ser actualizados para soportar IPv6, por ejemplo, en aquellos casos en los cuales el fabricante ha desaparecido y posiblemente no se tiene acceso al código existente en su interior para actualizarlo [25].

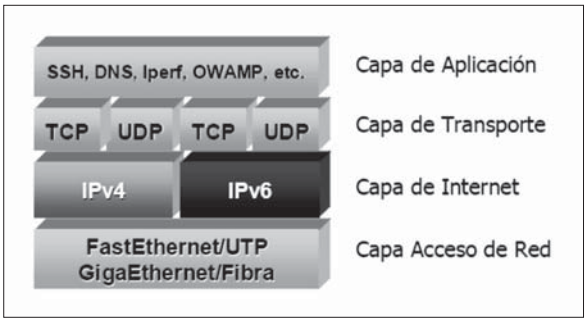

Figura 1. Modelo TCP/IP Double Snack
Fuente: elaboración propia.

Por este motivo, IPv6 ha sido diseñado junto a un conjunto de mecanismos de transición, los cuales permiten la coexistencia de ambos protocolos, IPv4 e IPv6, tanto tiempo como sea preciso, lo cual depende de innumerables factores, escenarios de red, sectores de negocio, etc [26]. Además, estos mecanismos de transición facilitan la integración de IPv6 en la red Internet existente hoy con IPv4 [27].

La problemática que implica en migrar a IPv6 la Internet actual, que está basada en IPv4, ha sido abordada a través de diversos mecanismos de transición [28]. El RFC 2893, describe dos aproximaciones (que pueden usarse separadas o en conjunto) para integrar gradualmente hosts y routers IPv6 dentro de un mundo IPv4: Double-Stack y Tunneling [29],[30]. El primer mecanismo se ve conceptualizado en el modelo TCP/IP de la figura 1, en donde los nodos IPv6 tienen, además, una completa implementación de IPv4 [31], [5].

El segundo mecanismo, es conocido como tunneling o tunelización [32], [33]. En éste, dos routers IPv6 que están interconectados a través de routers IPv4, se comunican entre sí utilizando paquetes IPv6 mediante establecimiento de un "túnel" entre ambos. El conjunto de routers IPv4 intermedios pasan a ser parte del túnel, como se muestra en la figura 2.

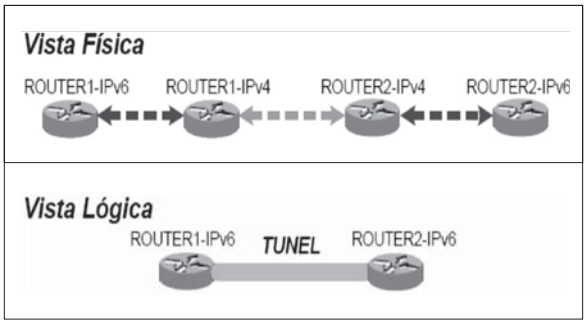

Figura 2. Vista física y lógica del modelo Tunneling
Fuente: elaboración propia.

6. PRINCIPALES DIFERENCIAS ENTRE IPv6 E IPv4

Consecuentemente, el diseño de IPv6 se presentó como una forma de mejorar Internet, con nuevas ventajas, además de la capacidad para expandir el espacio de direcciones, como: [34], [27]:

- *Autoconfiguración y reconfiguración sin servidores* ("enchufar y funcionar", "plug and play"): con esta característica, Internet se simplifica, en el sentido de que es más fácil conectar automáticamente cualquier dispositivo a la red [35]. No hay motivos para pedir a los usuarios que configuren nunca más los dispositivos, especialmente, considerando que los nuevos dispositivos no serán "sencillos" ordenadores con teclado y pantalla, sino electrodomésticos, dispositivos de todo tipo, sensores, entre otros; los cuales no tienen este tipo de interfaces para poder ser configurados. En IPv4 esto no se puede realizar, salvo que en la red se haya instalado un servidor (para el protocolo DHCP), lo que implica un coste superior para el propio servidor y su mantenimiento.
- *Mecanismos de movilidad más eficientes y robustos:* IPv6 ha sido diseñado bajo la perspectiva de un nuevo mundo "nómada". Usuarios y dispositivos tienen a movilizarse más que nunca. La conectividad es importante, incluso cuando las personas se desplazan, de tal forma que se puedan utilizar servicios mejorados, especialmente en entornos sin cables. IPv4 también permite movilidad, pero es muy ineficiente comparada con la movilidad en IPv6.
- *Seguridad extremo a extremo con autenticación y encriptación embebidas en la capa IP*: IPsec es el protocolo de seguridad, el mismo que en el caso de IPv4. La principal diferencia es que IPv4 no obliga al soporte de IPsec, lo que implica que no siempre está disponible. Además, en IPv4, debido al uso de NAT, a menudo no es posible utilizar IPsec extremo a extremo, salvo que se posean los conocimientos necesarios para configurar un túnel o VPN (Red Privada Virtual, Virtual Private Network), entre las dos estaciones que desean establecer dicha comunicación y se atraviesen los NAT. Este aspecto se describe en profundidad posteriormente en este mismo capítulo.
- *Cabecera con un formato mejorado e identificación de flujos*: los diseñadores del protocolo IPv6 sacaron provecho de los conocimientos adquiridos con la experiencia por el uso de IPv4 durante los últimos años, de forma que pudiera mejorarse la forma en que los datos se codifican para formar la cabecera del protocolo IPv6 y, consecuentemente, mejorar la operación de la red. Al mismo tiempo que la cabecera ha sido simplificada, se han agregado nuevas funcionalidades, siendo una de ellas la identificación de flujos, lo cual permitirá, en un futuro próximo, una mejor operación de los mecanismos de calidad de servicio (QoS) en Internet.
- *Soporte mejorado de multidifusión*: IPv6 incluye soporte mejorado de multidifusión (multicast), dado que se trata de una característica embebida en el protocolo, la cual es fundamental para el uso de redes de banda ancha para la distribución de contenidos.

- *Extensibilidad:* soporte mejorado para opciones / extensiones. Por último, pero no menos importante, IPv6 ha sido diseñado teniendo en cuenta las posibilidades para su crecimiento. No se desea repetir errores y llegar a la situación de descubrir, en unos pocos años, que, del mismo modo que se diseñó IPv4, de tal forma que ha llegado a ser un impedimento para la extensión de Internet, pueda ocurrir con IPv6. La forma en que IPv6 trabaja, permite incorporar nuevas características o piezas del protocolo (las que se denominan cabeceras de extensión), sin necesidad de actualizar todos los dispositivos de la red. Solo aquellos dispositivos que precisen usar determinadas extensiones tienen que ser actualizados, del mismo modo que, en la actualidad, todos los sistemas operativos y aplicaciones son frecuentemente actualizados, de una forma automática, transparente para el usuario.

Una lista resumida de las diferencias más relevantes entre IPv4 e IPv6 se encuentra en la figura 3.

7. DIRECCIONAMIENTO IPv6

Es descrito en el RFC 4291 [36]: *IP Version 6 Addressing Architecture*. Una dirección IPv6 tiene una longitud de 128 bits de largo y está escrita en notación hexadecimal separada por dos puntos (:). Está compuesta por ocho números distintos, representados por 16 bits cada uno y escritos en hexadecimal, un ejemplo de una dirección IPv6 sería:

2001:0db8:9095:02e5:0216:cbff:feb2:7474.

Vint Cerf (uno de los fundadores de la Internet) predice que con IPv6 "cada lámpara en la casa tendrá su número IP" [35]. Solamente el 15 % de espacio de direccionamiento está previsto para ser usado el 85 % restante está reservado para uso futuro.

Las direcciones IPv6 se dividen en tres grandes porciones de dirección: el prefijo de red, el identificador de subred y un identificador de host.

Property	IPv4	IPv6
Address size and network size	32 bits, network size 8-30 bits	128 bits, network size 64 bits
Packet header size	20-60 bytes	40 bytes
Header-level extension	limited number of small IP options	unlimited number of IPv6 extension headers
Fragmentation	sender or any intermediate router allowed to fragment	only sender may fragment
Control protocols	mixture of non-IP (ARP), ICMP, and other protocols	all control protocols based on ICMPv6
Minimum allowed MTU	576 bytes	1280 bytes
Path MTU discovery	optional, not widely used	strongly recommended
Address assignment	usually one address per host	usually multiple addresses per interface
Address types	use of unicast, multicast, and broadcast address types	broadcast addressing no longer used, use of unicast, multicast and anycast address types
Address configuration	devices configured manually or with host configuration protocols like DHCP	devices configure themselves independently using stateless address autoconfiguration (SLAAC) or use DHCP

Figura 3. Diferencias entre IPv6 e IPv4
Fuente: elaboración propia.

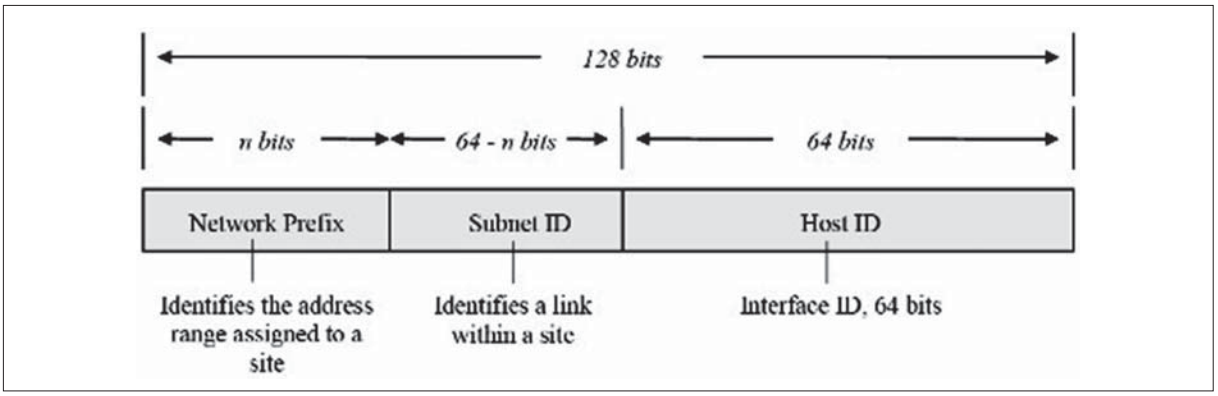

Figura 4. Formato de una Dirección IPv6

Fuente: elaboración propia.

El prefijo de red: es de los bits de orden superior de una dirección IP, utilizada para identificar una red específica y, en algunos casos, un tipo específico de la dirección véase la figura 7. Tipos de Direcciones IPv6.

El identificador de subred (ID): identifica un enlace de un sitio. El ID de subred es asignado por el administrador local del sitio, un sitio puede tener varios identificadores de subred. Esto se utiliza como un indicador para la red en la que se tienen varios host en su interior.

El identificador de host (ID host) es un identificador único para el nodo de la red en el que reside. Puede identificar una interfaz específica de un host. La figura 4 muestra el formato de dirección IPv6 con el prefijo de red, identificador de subred y un identificador de host.

De igual forma, el RFC 4291 también describe la notación de los prefijos de Red. Los prefijos de red son análogos, pero no equivalentes a la máscara de subred en IPv4. No existen máscaras de subred en IPv6, la notación de / es usada para identificar los bits que componen la longitud del prefijo de red. Un ejemplo sería:

2001:0db8:9095:02e5:0216:cbff:feb2:7474/**32**

Lo cual indica que la longitud del prefijo de red es de 32 bits. Los 96 bits restantes son asignados por el administrador local para relocalizar el ID de subred y el ID de host. Nuevamente, es importante tener claro que los ID de host son únicos y sirven para identificar una interfaz de un host. La figura 5 muestra dicha situación:

Las subredes dentro de una organización a menudo tienen prefijos de red de 64 bits (/ 64), dejando

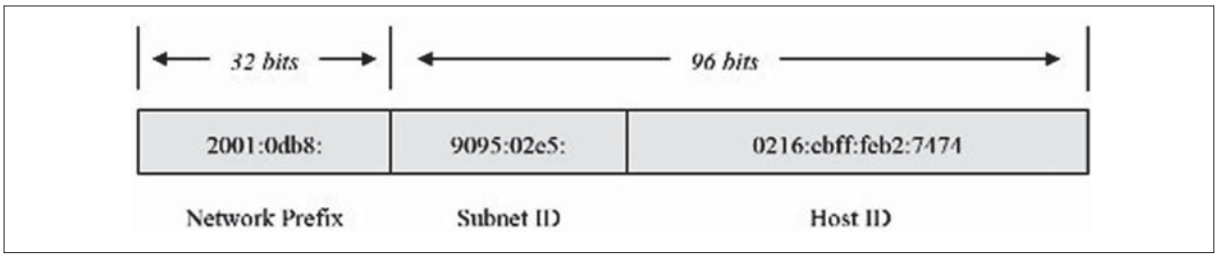

Figura 5. Formato de dirección IPv6 con prefijo de 32 bits

Fuente: elaboración propia.

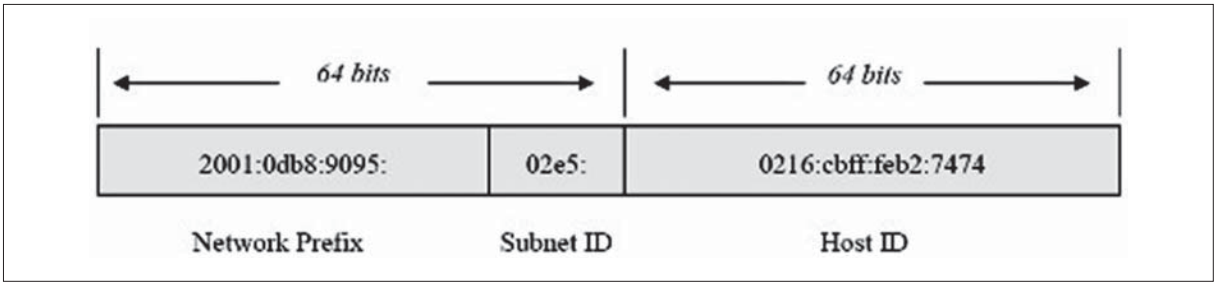

Figura 6. Dirección IPv6 con prefijo de 64 bots
Fuente: elaboración propia.

Address Type	Binary Prefix	IPv6 Notation	Uses
Embedded IPv4 address	00... 1111 1111 1111 1111 (96 bits)	::FFFF/96	Prefix for embedding IPv4 address in an IPv6 address
Loopback	00 ... 1 (128 bits)	::1/128	Loopback address on every interface (RFC 2460)
Global Unicast	001	2000::/3	Global unicast and anycast (allocated) (RFC 4291)
Global Unicast	01 - 1111 1100 0	4000::/2 - FC00::/9	Global unicast and anycast (unallocated)
Teredo	0010 0000 0000 0001 0000 0000 0000 0000	2001:0000::/32	Teredo (RFC 4380)
Nonroutable	0010 0000 0000 0001 0000 11 01 1011 1000	2001:DB8::/32	Nonroutable. Documentation purposes only. (RFC 3849)
6to4	0010 0000 0000 0010	2002::/16	6to4 (RFC 3056)
6Bone	0011 1111 1111 1110	3FFE::/16	Deprecated. 6Bone testing assignment. 1996 through mid 2006. (RFC 3701)
Link-local Unicast	1111 1110 10	FE80::/10	Link local unicast
Reserved	1111 1110 11	FEC0::/10	Deprecated. Formerly Site-local address space, unicast and unycast (RFC 3879)
Local IPv6 address	1111 110	FC00::/7	Unicast Unique local address space, unicast and unycast. (RFC 4193)
Multicast	1111 1111	FF00::/8	Multicast address space (RFC 4291)

Figura 7. Tipos de direcciones IPv6
Fuente: elaboración propia.

64 bits para la asignación a las interfaces de host. El ID de host debe seguir el formato suministrado por el EUI-64 (Extended Unique Identifier)[1]. La figura 6 muestra la distribución en este tipo de direcciones IPv6 [37]:

La figura 7 muestra los diferentes tipos de direcciones IPv6:

1 *IEEE EUI-64, Guidelines for 64-Bit Global Identier (EUI-64) Registration Authority*.

8. ALCANCE DE LAS DIRECCIONES IPV6

Cada interfaz puede tener naturalmente más de una dirección, según del alcance geográfico [38], como podemos ver en la figura 8:

Link Local: es la dirección local del interfaz con alcance de redes (LAN - Network Area Local), se puede designar o también obtenerla automáticamente componiéndose esta dirección con la

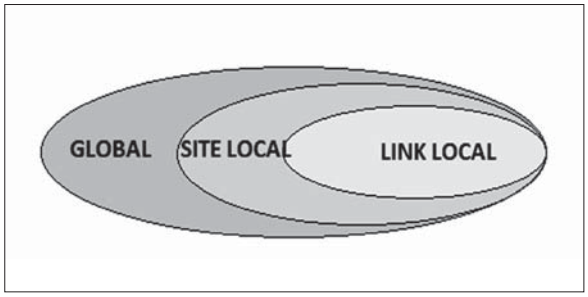

Figura 8. Alcance de las direcciones IPv6
Fuente: elaboración propia.

dirección MAC de la interfaz, de esta manera, estas direcciones no consumen ancho de banda para relacionar la dirección IP y MAC a través del protocolo ARP como sucede en IPv4, mejorando así el desempeño de la red.

Site Local: esta dirección tiene como alcance un campus o ciudad.

Global: es la dirección que tiene cada interfaz en internet, no son modificadas como sucede con (NAT) en IPv4 facilitando así la comunicación punto a punto entre dispositivos móviles en cualquier parte del mundo.

9. CABECERA DEL PROTOCOLO IPV6

Resumida en el costado derecho de la figura 9, la cabecera de un paquete IPv6 es, sorprendentemente, más sencilla que la del paquete IPv4. A esto se le suma que la funcionalidad del protocolo IPv6 es mucho mayor. La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o longitud. Sin embargo, para simplificar la vida de los enrutadores, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos:

El campo Versión: el campo Versión es de 4 bits de largo e identifica la versión del protocolo. Para IPv6, Versión = 6. Nótese que este es el único campo con una función y posición que es consistente entre IPv4 e IPv6. Todos los demás son diferentes de alguna forma. El tener este campo al comienzo del paquete permite una rápida identificación de la versión del IP y el paso de ese paquete al protocolo de proceso apropiado: IPv4 o IPv6.

El campo Traffic Class [39]: el campo Traffic Class es de 8 bits de largo y su intención para los

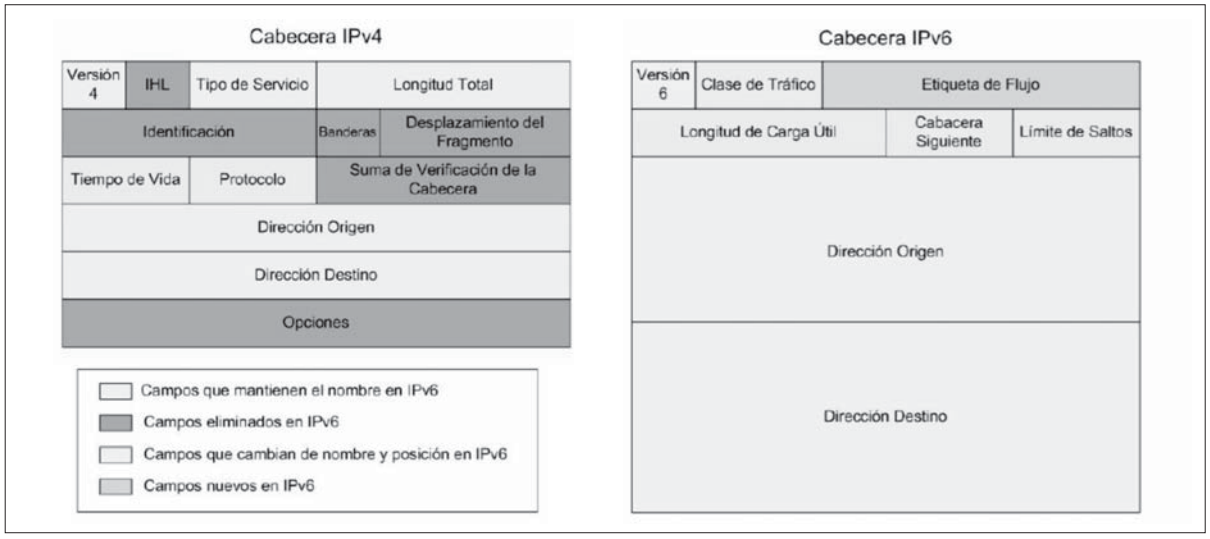

Figura 9. Cabecera de los protocolos IPv4 e IPv6
Fuente: elaboración propia.

nodos de origen, o nodos de reenvío, es identificar y distinguir entre diferentes clases o prioridades de paquetes IPv6. (En la primera publicación de la especificación IPv6, RFC 1883, este campo se llamaba Priority, reflejando su función. Mejoras en este trabajo lo renombraron como campo Class, con una longitud de 4 bits. Trabajo adicional en el IPNG Meeting, en el plenario de agosto 1997 de Munich, expandió este campo a 8 bits y redujo el campo Flow Label de 24 bits a 20. El nuevo término Traffic Class, definido en RFC 2460, identifica más el propósito de este campo). Este campo reemplaza las funciones que fueron proveídas por el campo Type of Service de IPv4, permitiendo la diferenciación entre categorías del servicio de transferencia de paquetes. Esta función es comúnmente referida como "Servicio de Diferenciación". En la actualidad, algunos experimentos están siendo conducidos en esta área de la tecnología, especialmente en soporte de transporte de señal dependiente del tiempo, como voz o video sobre IP. Estos tres requerimientos generales para el campo Traffic Class son stated en RFC 2460:

- Para paquetes que son originados en un nodo por un protocolo de capa más alta, ese protocolo de capa más alta especificaría el valor de los bits del campo Traffic Class. El valor por default es cero.
- Nodos que soportan una función particular que usa bits de Traffic Class pueden cambiar los valores de los bits en paquetes que ellos originan, reenvían o reciban. Sin un nodo no soporta esa función particular, no debe cambiar ninguno de los bits de Traffic Class.

Los protocolos de capa más alta no deben asumir que los valores de los bits de Traffic Class en un paquete recibido son los mismos valores que fueron originalmente transmitidos. En otras palabras, un nodo intermediario puede ser permitido a cambiar (y haber cambiado) los bits de Traffic Class en tránsito.

El campo Flow Label: el campo Flow Label es de 20 bits de longitud, y puede ser usado por un host para solicitar manejo especial para ciertos paquetes, como aquellos con una calidad de servicio de no default o de tiempo real. En esta primera versión de la especificación IPv6, RFC 1883, este campo era de 24 bits de longitud, pero cuatro de estos bits han sido ahora colocados en el campo Traffic Class, como se discutió en la sección anterior [40]. RFC 1809, "Usando el Campo Flow Label en IPv6", describe algunas de las investigaciones más tempranas en la materia, como el campo Class, Flow Label es sujeto de investigación actualmente y puede cambiar según la experiencia de la industria madura.

El campo Payload Field: el campo Payload Field es un entero no asignado de 16 bits que mide la longitud, dada en octetos, de la carga (ejemplo, el balance del paquete IPv6 que sigue al encabezado base de IPv6). Los encabezados de extensión opcional son considerados parte de la carga, junto con cualquier protocolo de capa más alta, como TCP, FTP y así. El campo Payload Length es similar al campo Total Length de IPv4, excepto que las dos medidas operan en diferentes campos. Payload Length (IPv6) mide los datos después del encabezado, mientras Total Length (IPv4) mide los datos y el encabezado. Las cargas más grandes de 65,535 son permitidas y son llamadas cargas Jumbo. Para indicar una carga jumbo, el valor de Payload Length está fijado en cero y la longitud de la carga actual es especificada en una opción que es cargada en la extensión del encabezado Hop-by-Hop.

El campo de Siguiente Cabecera (Next Header Field): el campo Next Header tiene 8 bits de longitud e identifica el encabezado inmediatamente siguiente del encabezado de IPv6. Este campo usa los mismos valores que el campo Protocol de IPv4. En la figura 10 se encuentran algunos ejemplos:

Value	Header
0	Hop-by-Hop Options
1	ICMPv4
4	IP in IP (encapsulation)
6	TCP
17	UDP
43	Routing
44	Fragment
50	Encapsulating Security Payload
51	Authentication
58	ICMPv6
59	None (No Next Header)
60	Destination Options

Figura 10. Valores posibles del campo Next Header

Fuente: elaboración propia.

Un paquete IPv6, que consiste en un paquete de encabezado IPv6 más su carga, puede consistir de cero, uno o más encabezado de extensión. Muchos de los encabezados de extensión también emplean un campo Next Header.

El campo Hop Limit: el campo Hop Limit tiene 8 bits de longitud, y va decreciendo en 1 por cada nodo que reenvía el paquete. Cuando Hop Limit se iguala a cero, el paquete es descartado y un mensaje de error es retornado. Este campo es similar al campo Time-to-Live (TTL) encontrado en IPv4, con una excepción clave. El campo Hop Limit (IPv6) mide el máximo de saltos (hops) que pueden ocurrir mientras el paquete es enviado por varios nodos. El campo TTL (IPv4) puede ser medido en saltos o segundos. Nótese que con Hop Limit usada en IPv6, la base del tiempo no está disponible más.

El campo Source Address: el campo Source Address es un campo de 128 bits que identifica el originador del paquete. El formato de este campo es más ampliamente definido en RFC 2373 [41].

El campo Destination Address: el campo Destination Address es un campo de 128 bits que identifica el destinatario que tiene la intención de recibir el paquete. Una importante distinción es que el destinatario que tiene la intención de recibir el paquete, puede no ser el destinatario final, como el Header Routing puede ser empleado para especificar la ruta que el paquete toma desde su fuente, a través de destinatario(s) intermedio(s), y así hasta su destinatario final.

10. SEGURIDAD EN IPV6

IPv6 incluye explícitamente la posibilidad de utilizar el modelo de seguridad IPsec (Internet Protocol Security) [42] que proporciona autenticidad, integridad y confidencialidad a las comunicaciones de extremo a extremo. IPsec es un conjunto de protocolos abiertos que tienen como fin proporcionar seguridad en las comunicaciones de la capa de red del modelo OSI (a la que pertenece el protocolo IPv6) y, de ese modo, a todos los protocolos de capas superiores [43], [44].

En IPv4, la implementación de IPsec se define en una especificación diferente a la del propio protocolo IPv4, por lo que la inclusión del protocolo se hace con mecanismos definidos fuera del mismo, mientras que, en IPv6, la propia arquitectura "extensible" del protocolo permite implementar IPsec de forma natural. Es importante reseñar que IPv6 habilita la posibilidad de usar IPsec, y no los mecanismos de cifrado y autenticación propios de IPsec.

IPsec tiene dos modos de funcionamiento que proporcionan distintos niveles de seguridad [45]:

Modo transporte: se cifra o autentica la carga útil, o payload, pero las cabeceras no se tienen en cuenta. Tiene como ventaja que se puede utilizar de extremo a extremo, pero tiene en contra que la información de las cabeceras, como la dirección IP de origen y destino, es visible.

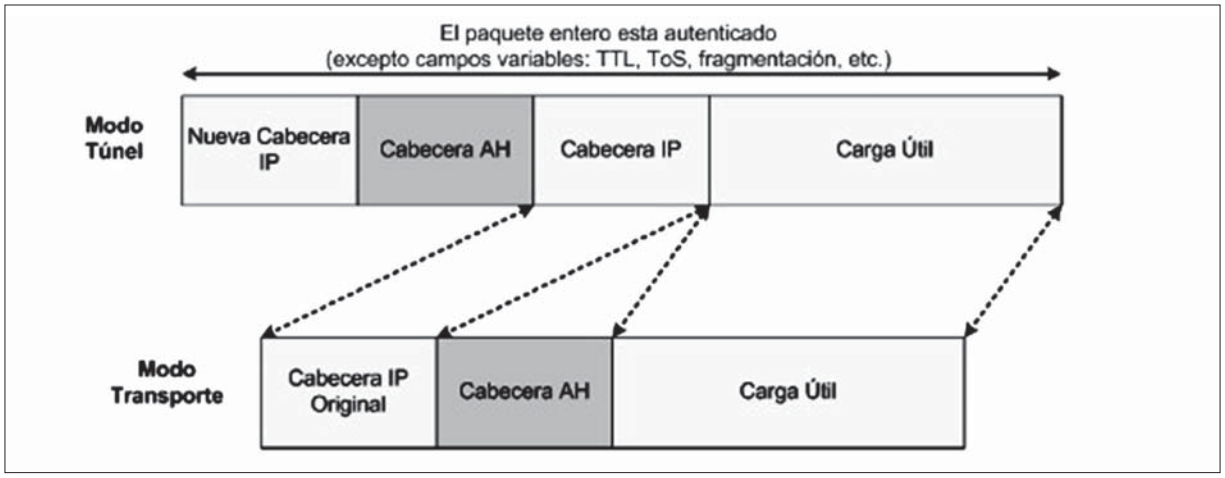

Figura 11. Implementación de AH en modo Túnel y en modo Transporte
Fuente: elaboración propia.

*Modo t*únel*:* una plataforma, o pasarela, encapsula el paquete original en otro paquete. Con ello se cifra o autentica el paquete original completo, pero se necesita de una plataforma que realice el túnel.

Además, IPsec tiene dos modos o protocolos de transferencia, que a su vez pueden funcionar en modo túnel o transporte:

AH (Authentication Header): proporciona autenticación, integridad y un servicio de anti-repetición opcional. Su ubicación se puede ver en la figura 11.

ESP (Encapsulating Security Payload): además de las ventajas anteriores proporciona confidencialidad. Su implementación se muestra en la figura 12.

En la práctica, el uso de IPsec es escaso debido, sobre todo, a la falta de un mecanismo generalizado y global de intercambio de claves. Por esta

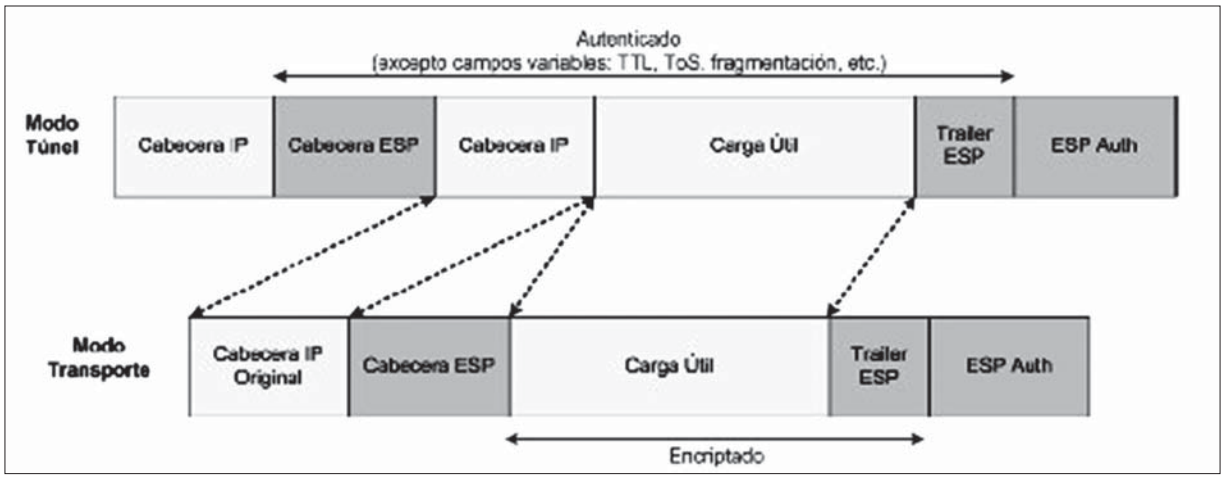

Figura 12. Implementación de ESP en modo Túnel y en modo Transporte
Fuente: elaboración propia.

razón, el uso de IPsec en IPv6 es, por el momento, similar al de IPv4, para conexiones preconfiguradas como, por ejemplo, las utilizadas en las VPN.

La solución futura para el problema anterior puede que se base en mecanismos externos como certificados transportados por DNS asegurado con DNSSEC[2].

11. MOVILIDAD EN IPV6

Concepto: se entiende por movilidad a la capacidad para que un nodo de la red mantenga la misma dirección IP, a pesar de que éste se desplace físicamente a otra área [46]. Es decir que, sin importar su ubicación, este pueda seguir siendo accesible a través de la misma dirección IP. Sin esta capacidad, los paquetes destinados a un nodo móvil no estarán posibilitados para llegar a destino mientras el nodo móvil se encuentre alejado de su vínculo principal (*home link*). Un nodo móvil bien podría seguir manteniendo la comunicación al ir cambiando su dirección IP cada vez que salta de proveedor a proveedor, pero esto trae aparejado el problema de ir perdiendo la conexión en las capas de transporte y superiores. Por eso, es necesario el estudio y desarrollo de protocolos que permitan movilidad a lo largo de varios tipos de redes, en distintas áreas geográficas [46] - [48].

Uso en IPv6: el soporte de movilidad es una característica muy tenida en cuenta en la implementación de IPv6, ya que se espera que una gran parte de la población requiera de servicios de movilidad durante el periodo de vida de IPv6. La definición del protocolo que permite movilidad en IPv6 está definido principalmente en RFC 3775: *Mobility Support in IPv6*, además de una gran variedad de escritos que aún no han sido aprobados por la IETF (Internet Engineering Task Force).

Funcionamiento general: un nodo móvil siempre pretenderá ser accesible desde su dirección principal, sin importar si éste se encuentra físicamente conectado al vínculo principal o ya sea que se encuentre geográficamente alejado [49]. La dirección principal o *home address* es, según lo expresado en [50], la dirección IP que le corresponde al nodo en el ámbito de su vínculo principal. Mientras el nodo se encuentra en su vínculo principal, los paquetes destinados a esa dirección principal son ruteados utilizando los mecanismos estándares de ruteo de Internet. Cuando el nodo se encuentra físicamente conectado a otro vínculo aún es accesible, por lo que se denomina una *care-of-address* (sin traducir de [50]). La cual es una dirección IP asociada al nodo móvil que contiene el prefijo de subred del vínculo externo. Un nodo móvil puede, llegado el caso, ser accedido por más de una *care-of-address*. El nodo móvil puede obtener la dirección en el vínculo externo mediante los mecanismos habituales de IPv6.

El proceso de asociación entre una dirección de tipo *care-of-address* de un nodo móvil y su dirección principal o *home address* se conoce como binding. Cuando el nodo móvil se encuentra alejado, éste registra su dirección de tipo *care-of-address* en el router de su vínculo principal (home-agent según [50]). Cualquier otro nodo que desee comunicarse con el nodo móvil tiene dos maneras para establecer un vínculo con el nodo móvil: la primera se menciona en [50], conocida como túnel bidireccional, no requiere soporte de movilidad IPv6 por parte del nodo que desee comunicarse (*correspondent node*). Los paquetes enviados por el *correspondent node* son enviados al router en el vínculo principal del nodo móvil. Y es este router (home-agent según

2 Domain Name System Security Extensions: Disponible en: https://www.iana.org/dnssec

[50]) quien, a su vez, lo envía al nodo móvil, ya que es el único que conoce su dirección en el vínculo externo. Para este túnel se utiliza encapsulación de IPv6.

La segunda, mencionada en [50], se conoce como routeo optimizado. Para este caso, se necesita que el nodo móvil registre su *binding* actual al *correspondent node*. De esta manera, los paquetes con destino al nodo móvil son ruteados de manera directa a la dirección de tipo *care-of-address* del nodo móvil. Cada vez que el *correspondent node* necesita enviar un paquete al nodo móvil, éste primero verifica por una entrada, conteniendo la dirección principal del nodo móvil en sus *cached bindings*, si encuentra una de estas entradas entonces, mediante una cabecera especial IPv6, ruteará de manera directa hacia el nodo móvil a través de la dirección tipo *care-of-address*.

12. CALIDAD DE SERVICIO EN IPv6

La calidad de servicio en IPv6, es un servicio más robusto que el provisto por datagrama llamados: Prioridad (priority –4 bits-) y Etiqueta de Flujo (Flow Label –24 bits-). Estos, son usados para que un host pueda identificar los paquetes, para el cual se requiere un manejo especial por parte de los routers IPv6. Esta capacidad es importante para el momento de soportar aplicaciones que requieren el menor grado de retardos, delay o alteraciones en el flujo. Estos tipos de aplicaciones son comúnmente descritas como aplicaciones multimedia o de tiempo real [51].

El enrutamiento basado en flujo, le podría dar a las interredes algunas de las características determinísticas asociadas con tecnologías de conmutación orientadas a conexión y circuitos virtuales telefónicos [52].

REFERENCIAS

[1] M. Del Rey, *Internet Protocol*, California: IETF. 1981, RFC 791.

[2] B. A. Forouzan, *Transmisión de Datos y Redes de Computadores,* Madrid-España : Mac Graw Hill, 2007.

[3] J. A. Mañas, *Mundo IP.* Madrid - España: Ediciones Nowtilus, 2004.

[4] A.Tanenbaum, *Redes de Computadoras,* México: Prentice Hall, 2003.

[5] J. Rodríguez Albornoz y R. Guerra Díaz, *Evaluación y Comparación de los Protocolos de Internet IPv4 e IPv6 en una Red Experimental WDM,* Valparaíso - España: Publicaciones Universidad Técnica Federico Santa María, 2005.

[6] P. A. Castillo Valdivieso, *Interoperabilidad de Redes Heterogeneas de Computadores,* 2005.

[7] E. F. Pinillos T, "Ip versión 6: La nueva Generación IP", *Revista Electrónica de Estudios Telemáticos*, pp. 50-57. 2008.

[8] Frankel, Sheila, et al., *Guidelines for the Secure Deploymen of IPv6*, Washington D.C.: U.S. Departament of Commerce, 2010.

[9] G. Huston, *Next Steps for the IP QoS Architecture,* California: IETF, 2000. RFC 2990.

[10] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol,* California: IETF, 1998. RFC 2401.

[11] C. Perkins, *P Mobility Support,* California: IETF, 1996, RFC 2002.

[12] V. Fuller, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy,* California: IETF, 1993. RFC 1519.

[13] K. E. B.Hickman, *The SSL Protocol,* California: W3O, 1994.

[14] E. Rescorla, *The Secure HyperText Transfer Protocol,* California: IETF, 1999, RFC 2660.

[15] A. Ghiselli, *INFN Requirements for an IPng,* California: IETF, 1994, RFC 1676.

[16] M. Vecchi, *IPng Requirements: A Cable Television Industry Viewpoint,* California: IETF, 1994, RFC 1686.

[17] D. Santana Yunes, *IPv6: Nueva Generación Protocolo de Internet,* Santo Domingo: Universidad Nacional Pedro Henríquez Ureña, 2004.

[18] G. Van de Velde, *IPv6 Unicast Address Assignment Considerations,* California : IETF, 2008, RFC 5375.

[19] H. Holbrook, *Source-Specific Multicast for IP,* California: IETF, 2006. RFC 4607.

[20] S. Deering, *Internet Protocol, version 6 IPv6. Specification,* S.l.: IETF, 1998, RFC 2460.

[21] J. Postel, *User Datagram Protocol,* California: IETF, 1980. RFC 768.

[22] *Internet Control Message ProtocoL,* California: IETF, 1981. RFC 792.

[23] J. Moy, *OSPF Version 2,* California: IETF, 1998. RFC 2328.

[24] J. Amoss and D. Monoli, *Handbook of IPv4 to IPv6 transition,* S.l: Auerbach Publications, 2008.

[25] J. Arkko, *IPv4 Run-Out and IPv4-IPv6 Co-Existence Scenarios,* California: IETF, 2009, Draft-arkko-townsley-coexistence-03.

[26] J. Curran, *An Internet Transition Plan,* California: IETF, 2008, RFC 5211.

[27] Euro6IX, *Ipv6: Legal Aspects of the new Internet Protocol,* Madrid: Euro6IX, 2005.

[28] R. Gilligan, *Transition Mechanisms for IPv6 Hosts and Routers,* California: IETF, 2000, RFC 2893.

[29] J. Arkko, *Guidelines for Using IPv6 Transition Mechanisms,* California: IETF, 2010. Draft-arkko-ipv6-transition-guidelines-01.

[30] G. Bajko, *Security On Demand for Mobile IPv6 and Dual-stack Mobile IPv6,* California: IETF, 2010, Draft-bajko-mext-sod-00.

[31] G. Tsirtsis, *Dual-Stack Mobile IPv4,* California: IETF, 2009. RFC 5454.

[32] R. Graveman, *Using IPsec to Secure IPv6-in-IPv4 Tunnels,* California: IETF, 2007. RFC 4891.

[33] M. Blanchet, *IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP),* California: IETF, 2010, RFC 5572.

[34] F. Baker, *IPv4 and IPv6 Greynets,* California: IETF, 2010, Draft-baker-v6ops-greynet-02.

[35] S. Krishnan, *Reserved IPv6 Interface Identifiers,* California: IETF, 2009, RFC 5453.

[36] R. Hinden, S. Deering, *IP Version 6 Addressing Architecture,* S.l.: IEFT, 2006, RFC 4291.

[37] G. Huston, *Administration of the IANA Special Purpose IPv6 Address Block,* California: IETF, 2006, RFC 4773.

[38] M. Blanchet, *Special-Use IPv6 Addresses,* California: IETF, 2008, RFC 5156.

[39] C. Partridge, *Using the Flow Label Field in IPv6,* California: IETF, 1995, RFC 1809.

[40] B. Carpenter, *Update to the IPv6 flow label specification,* California: IETF, 2010, Draft-carpenter-6man-flow-update-03.

[41] R. Hinden, *IP Version 6 Addressing Architecture,* California: IETF, 1998, RFC 2373.

[42] INTECO, *Informe sobre las Implicaciones de la Seguridad en la Implantación de IPv6,* Madrid- España: Ministerio de Industria, Turismo y Comercio, 2010.

[43] E. Vyncke, *Advanced Security for IPv6 CPE,* California: IETF, 2010, Draft-vyncke-advanced-ipv6-security.

[44] S. Yamamoto, *Softwire Security Analysis and Requirements,* California: IETF, 2009. RFC 5619.

[45] M. StJohns, *Common Architecture Label IPv6 Security Option (CALIPSO),* California: IETF, 2009, RFC 5570.

[46] C. Taffernaberry, A. Dantiacq, "IPv6: La siguiente Generación del Protocolo de Internet", en *Grupo de Investigación CODA-REC - Argentina* pp. 1 – 10, 2008.

[47] H. Soliman, *Hierarchical Mobile IPv6 (HMIPv6) Mobility Management,* California: IETF, 2008, RFC 4140.

[48] F. Le, *Mobile IPv6 and Firewalls: Problem Statement,* California: IETF, 2006, RFC 4487.

[49] R. Koodli, *Mobile Networks Considerations for IPv6 Deployment,* California: IETF, 2010, Draft-koodli-ipv6-in-mobile-networks.

[50] D. Johnson, R. Arkkon and C. Perkins, *Mobility Support in IPv6,* S.l.: IEFT, 2004.

[51] G. Van de Velde, *Local Network Protection for IPv6,* California: IETF, 2007, RFC 4864.

[52] T. Chown, *Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks,* California: IETF, 2006. RFC 4554.